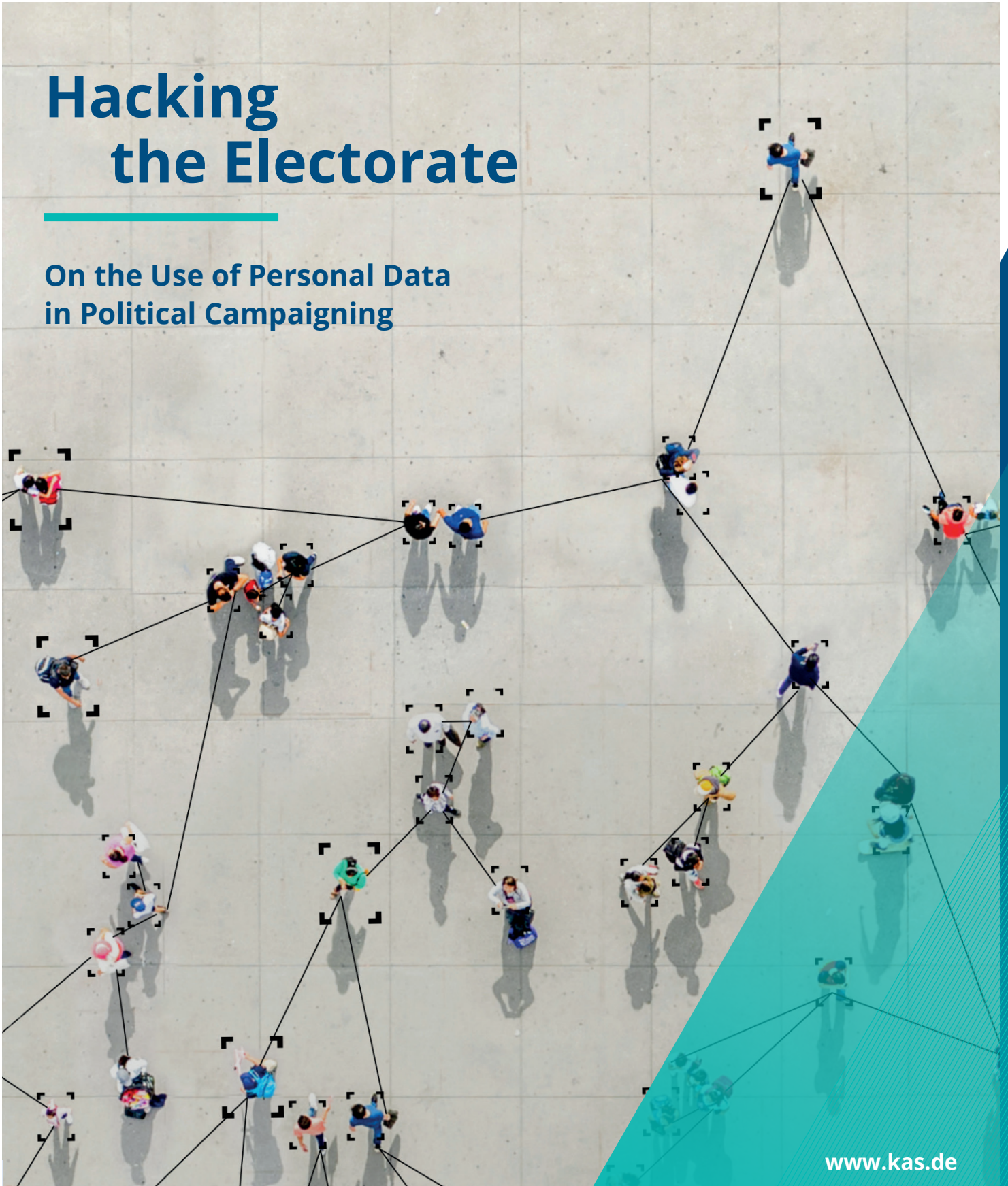


Hacking the Electorate

On the Use of Personal Data
in Political Campaigning



Legal notice

Publisher:

Konrad-Adenauer-Stiftung e. V. 2020, Berlin

Cover photo: © iStock/Orbon Alija

Chapter marker: p. 10 © Adobe Stock/Gorodenkoff;

p. 28 © Adobe Stock/Alexander; p. 38 © Shutterstock/mrmohock

Design and typesetting: yellow too, Pasiak Horntrich GbR

The print edition of this publication was printed by

copy print Kopie & Druck GmbH, Berlin.

Printed in Germany.

Produced with financial support from the Federal Republic of Germany.



The text of this publication is licensed under the terms of
“Creative Commons Attribution-ShareAlike 4.0 International”, CC BY-SA 4.0
(available at: <https://creativecommons.org/licenses/by-sa/4.0/legalcode.de>).

ISBN 978-3-95721-772-1

Hacking the Electorate

On the Use of Personal Data
in Political Campaigning

At a Glance

- › Although data-driven political campaigning is not a new phenomenon, the tools used, the amount of data accessible, and the potential capacity to influence voters represent a new and challenging scenario for the rule of law.
- › With the arrival of participatory and social web, Internet users can now generate data in a complex network and without any obligation to the pursuit of objectivity or journalistic standards as pillars for content creation.
- › People in different countries are increasingly getting informed and learning about political candidates and other political issues through social networks.
- › In recent years political parties and campaigners around the world have invested heavily in online advertising, demonstrating all the potential to reach more people in an efficient, targeted, and accessible way.
- › Firms like Cambridge Analytica gather massive amounts of individual data, process these data to identify and forecast even more intimate individual details, and use these profiles and forecasts to personalize political messaging, such as social media advertising, to guide tactical campaign decisions.
- › If voters do not understand how their data are being used to influence them, they will not be able to exercise their legal rights in relation to that information and the strategies being applied.
- › Current practices of unauthorized personal data processing are boosting misinformation and 'digital astroturfing strategies', capable of influencing citizens with even greater precision.
- › The possibility of bridging electoral regulation and the legal frameworks for campaign activities involving personal data depends on many factors.
- › This lack of uniformity or misinterpretation of the GDPR's guidance in the context of elections may lead to differences in the level of personal data protection within Member States and potentially influence other regions negatively.
- › The effectiveness of data protection regulation depends on the capacity and institutional articulation of the different stakeholders involved.
- › Data protection regulations are fully applicable to political campaigns and have the ability to assist in reducing the instrumental use of personal data, while also avoiding the impact of misinformation and computational propaganda used for the purpose of political manipulation.

- › A data protection approach can sum up strategically with other efforts, helping to reduce misinformation in electoral campaigns by sanctioning the illegal processing of personalized data, serving as an effective and useful legal instrument in the present context.
- › On the one hand, it is the role of public institutions through its resolutions and sanctions, to reinforce compliance and the effectiveness of the GDPR guidelines. On the other hand, it is the duty of political parties and campaigners to comply with legal requirements, having full responsibility, transparency, and good faith in the processing of voters' personal data.
- › Unauthorized processing of personal data, along with misinformation techniques and unfair use of bots, profiles, deep fakes, and others, undermines voters' confidence and the integrity of political processes and should be viewed by institutions as threats to democracy.



Eduardo Magrani

Ph. D. in Law and Fellow at the Konrad-Adenauer-Stiftung e. V. in Germany, on the European and International Cooperation Program for Global Innovation Policy, Digitalization, and Artificial Intelligence (EIZ-Fellow für Globale Innovationspolitik, Digitalisierung und Künstliche Intelligenz. Europäische und Internationale Zusammenarbeit). Professor of Law and Technology and Intellectual Property at FGV Law School (Getulio Vargas Foundation), IBMEC and Pontifical Catholic University of Rio de Janeiro (PUC-Rio) in Brazil. President of the National Institute for Data Protection in Brazil. Author of the Digital Culture Trilogy in Brazil "Democracy, Hyperconnectivity and Ethics: a trilogy on digital culture," concerning philosophy of technology, digital democracy, data protection, innovation, cybersecurity, and artificial intelligence.

Table of Contents

Abstract	6
Introduction	7
1. Hacking the Electorate	10
The echo-chamber/filter-bubble effect	13
The Brazilian experience: election campaign in 2018	15
2. Compliance with data protection regulations on elections	28
3. Enhancing effectiveness and bridging the gaps	38
Final Considerations	50

Abstract

The continuous interaction between intelligent devices, online platforms, sensors, and people points to the increasing volume of data being produced, stored, and processed, increasingly changing our daily lives in various aspects. The context of hyperconnectivity can bring economic benefits to the State and companies, as well as convenience to consumers. On the other hand, this new reality brings significant challenges in the spheres of democratic processes, especially in the context of political campaigning. The potential harm that can be caused by political manipulation strategies through the unauthorized use of data is exponential when we consider how new technologies are being used altogether. For a social order whose cohesion is based on the rule of law, sovereignty, and consent of its citizens, this represents an unprecedented challenge, and the way democracies will approach this challenge represents a key factor for political systems. Recent years' experiences indicate how digital technology can undermine and destabilize democracy. Misinformation, algorithmic manipulation, behavioral micro-targeting, and social bots are some of the techniques currently used, and these are based most of the times on unauthorized processing of personal data. More importantly, these elements can be used differently in each region, built upon cultural, technological, and personal habits. Considering this context, it is extremely important that privacy and data protection regulations are made effective and strengthened. In the European Union, the General Data Protection Regulation (GDPR) brings a robust legal framework, which has inspired many other countries' regulations in this matter. In spite of that, there are some differences between data protection regulations that must be highlighted, with the purpose of identifying how they can be reinforced and correctly interpreted for the context of political campaigning. This research paper intends to compare the GDPR with the Brazilian General Law on Data Protection (LGPD), investigating how both regulations are applicable in the context of personal data usage in political campaigns. The justification for bringing the Brazilian scenario into this analysis is twofold: (i) the GDPR was the main pillar for the LGPD's drafting, although the latter has some differences in regard to compliance that should be considered; and (ii) Brazilian politics is experiencing some major episodes of misinformation and digital astroturfing strategies for political manipulation that are relevant to be addressed and further understood. Finally, this paper will also offer a critical analysis of the effectiveness of both regulations and suggest possible solutions.

Introduction

Political parties and campaigners have used different communication practices and technologies over time. Now with the rapid development of new digital technologies and communication tools, political campaigning has become increasingly sophisticated. Although data-driven political campaigning is not a new phenomenon, the tools used, the amount of data accessible, and the potential capacity to influence voters represent a new and challenging scenario for the rule of law.¹

The possibility of gathering huge databases of citizens, containing thousands of pieces of information that provide the full picture of who they are, where they live, what they do, and what is happening around them, can bring several benefits to parties and political campaigners. Millions of e-mail addresses, phone numbers, and other personal data, such as the ones gathered through donations, at rallies, and through merchandise, allow political campaigners to obtain very sensitive information about specific target groups and voters. In recent years, political parties and campaigners around the world have invested heavily in online advertising, demonstrating all the potential to reach more people in an efficient, targeted, and accessible way, sometimes for a fraction of the cost of more traditional methods.²

Advertising and political manipulation strategies are not new, but there is no precedent for targeting people in such intimate detail and on the scale of entire populations.³ It represents both a gain of scale and effectiveness. It should be handled carefully and always on a legal basis, with transparency, fairness, and accountability. A potential infringement of the personal data protection right in democratic processes, such as election campaigns, can considerably affect other fundamental rights. It poses a real threat to citizens' ability to make their own independent decisions or even their right of opinion, undermining the fundamental value of dignity, which underpins all human rights. The public is entitled to expect political advertising to be done in accordance with the law. Furthermore, all political parties and campaigners need to comply with the same data protection and electoral rules, regardless of the method or new technological developments.⁴

Unauthorized personal data processing, along with misinformation and digital astroturfing techniques, undermines voters' trust and the integrity of political processes, and shall be considered as threats to democracy.⁵ Citizens can only make genuinely informed choices about whom to vote for if they are certain that their decisions have not been unfairly influenced. That is why trust and confidence in the integrity of democratic processes should not be weakened.^{6 7}

Taking into consideration the importance of personal data processing in this context, part of the potential abuses and risks arising from its misuse may be mitigated by the application of robust legal frameworks, such as the European and the Brazilian general data protection regulations (respectively the "GDPR" and the "LGPD"). Both regulations are applicable to political campaigning and can reduce the instrumental use of personal data for unfair political manipulation. Harmonizing general privacy and data

protection regulations with electoral laws has the power to ensure effective mechanisms to guarantee rights and duties related to personal and sensitive data, helping to foster a healthy, legal and ethical environment in election periods.⁸

However, the connection between electoral regulation and the legal frameworks for campaign activities involving personal data is still under development. As much as there are strong foundations on both sides, general data protection regulations, such as the GDPR and the LGPD, did not yet accumulate significant application and jurisprudence in order to guarantee a perfectly clear guideline for compliance and accountability. It is still being debated how exactly these regulations should be applicable in practice for a range of activities. Extending this protection to campaigns is still a goal to be pursued, and is being substantially debated by specialists in the field, courts, and data protection entities.⁹

The effectiveness of data protection regulation depends on the capacity and institutional articulation of the different stakeholders. Activities concerning personal data usage in political campaigns will demand a close look not only by public entities, such as judicial courts and data protection authorities, who will have to harmonize interpretation and set up adequate guidance, but also by the private sector in helping to prevent manipulation and misinformation practices.¹⁰

Considering cultural and normative idiosyncrasies, through the analysis of both the European and the Brazilian data protection regulations and their potential effects on political campaigning, it is evident that there is a need for parties, campaigners, courts, data protection authorities, and private companies to commit to the privacy of users, reacting to the side effects and threats posed by technology to democratic institutions and their citizens' rights, in both contexts.

-
- 1 Information Commissioner's Office (ICO) (2018), "Investigation into the use of data analytics in political campaigns: a report to Parliament," <https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf>, access September, 2019.
 - 2 Information Commissioner's Office (ICO) (2018), "Investigation into the use of data analytics in political campaigns: a report to Parliament," <https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf>, access September, 2019.
 - 3 European Data Protection Supervisor (2018), "Opinion 3/2018 EDPS Opinion on online manipulation and personal data," https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf, access October, 2019.
 - 4 See <https://privacyinternational.org/case-study/763/case-study-profiling-and-elections-how-political-campaigns-know-our-deepest-secrets>, access October, 2019.
 - 5 As recent evidence shows, voters do not grasp the hidden existence of personal data uses, undermining the system of democracy through computational propaganda. See Samuel C. Woolley and Philip N. Howard (2017), *Computational Propaganda Worldwide*, University of Oxford, <http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf>, access October, 2019.
 - 6 ICO (2019), "Guidance on political campaigning: Draft framework code for consultation," <https://ico.org.uk/media/about-the-ico/consultations/2615563/guidance-on-political-campaigning-draft-framework-code-for-consultation.pdf>, access December, 2019.
 - 7 Kaltheuner, Frederike (2018), "It's about human dignity and autonomy," *Digital Society Blog*.
 - 8 The compliance with relevant legal frameworks, such as general data protection regulations, has effects on parties, candidates, and political marketing consultants, as well as their suppliers who, alongside internet platforms, must be subject to accountability, oversight, and sanctions in the event of legal noncompliance. The traditional and specific ruling for political campaigning is in most cases either outdated or ineffective, by not reflecting modern campaigning practices. The importance of processing personal data in compliance with data protection laws during political campaigning is crucial to maintaining elections' integrity and voters' autonomy, as well as trust in the use of their information. See ICO (2019), "Guidance on political campaigning: Draft framework code for consultation," <https://ico.org.uk/media/about-the-ico/consultations/2615563/guidance-on-political-campaigning-draft-framework-code-for-consultation.pdf>, access December, 2019.
 - 9 Britto, Cruz et al. (2019), "Internet e eleições no Brasil: Diagnósticos e recomendações," *InternetLab*.
 - 10 Britto, Cruz et al. (2019), "Internet e eleições no Brasil: Diagnósticos e recomendações," *InternetLab*.



1. Hacking the Electorate

Micro-targeting, bots, and misinformation
as new challenges to democracy

The Federal Trade Commission (FTC) in the USA, America's consumer protection agency, has agreed to impose a record fine on Facebook – \$5 billion, the largest privacy fine in the FTC's history. The settlement stems from the investigation into the company's privacy practices related to the Cambridge Analytica (CA) scandal. The CA case exposed how personal data was misused to micro-target and potentially manipulate swing voters in the US' election in 2016.¹¹

Cambridge Analytica stated that it had up to 5,000 data points related to each US' voter, collected through individuals' profiles, websites, Twitter messages, Facebook profiles, and Instagram pictures. By applying 'psychographic analytics' to its dataset, it claimed to be able to attest the kind of person each voter was, including a relatively accurate assessment of individual needs and fears, and how they were likely to behave.¹²

Psychometrics (or psychographic analytics) focuses on measuring psychological traits, intending to assess human beings based on five personality features: openness, conscientiousness, extroversion, agreeableness, and neuroticism. Based on these five traits it is possible to assess important and sensitive information about an individual, that may be used for different purposes. Before the Internet and the spread of social networks, one of the main challenges for effective psychometrics was exactly the difficulty in gathering all the necessary data, which depended on comprehensive and highly personal questionnaires. This challenge was overcome due to online platforms and user engagement on social networks.¹³ Nowadays, psychometrics is largely used for different purposes, including electoral campaigning.

Although there are some disagreements on the effectiveness of psychometrics' practices, recent research in the field of computational propaganda and sociology state that individuals' mental profiles can be precisely anticipated from the trails they leave while on the web. Studies on the impact of micro-targeting in advertising suggest that psychological micro-targeting can be used covertly to attract up to 40% more clicks and up to 50% more purchases. Findings also state that marketers can attract up to 63 percent more clicks and up to 1,400 more conversions in advertising campaigns on Facebook when matching products and marketing messages to consumers' personality characteristics.¹⁴

This type of evaluation derived from digital interactions reinforces the importance of understanding the degree to which the use of big data and psychometrics can influence the activities of large groups of individuals.¹⁵ This might not be the only reason for the specific 2016 US election outcome, but there are indications that it was a useful contribution¹⁶, and not only in the US. More recently, Facebook has agreed to pay £500,000 for failing to keep UK users' personal information from organizations like Cambridge Analytica (CA). The Information Commissioner's Office (ICO) said Facebook had let a "genuine break" of the law occur, and did not take sufficient steps to prevent apps from collecting data in contravention of data protection law.^{17 18}

According to the ICO:¹⁹

Our investigation found that between 2007 and 2014, Facebook processed the personal information of users unfairly by allowing application developers access to their information, without sufficiently clear and informed consent, and allowing access even if users had not downloaded the app, but were simply 'friends' of people who had. Facebook also failed to keep the personal information secure because it failed to make suitable checks on apps and developers using its platform.

Besides the notoriety of the CA scandal and outputs in the US and UK, analyzing the internet-based big data economy and political usages, the conclusion is that this phenomenon is not just about one company or restricted to exceptional episodes in specific regions. Recent studies have shown evidence that this is happening worldwide, where non-authorized personal data is massively processed by companies, parties, and campaigners seeking behavioral manipulation, with the capacity for unfairly influencing election results using individualized, high-impact messages. Furthermore, this practice is becoming even more effective and more manipulative by the use of misinformation and digital astroturfing techniques.

According to the European Data Protection Board:²⁰

Political parties, political coalitions, and candidates increasingly rely on personal data and sophisticated profiling techniques to monitor and target voters and opinion leaders. In practice, individuals receive highly personalized messages and information, especially on social media platforms, on the basis of personal interests, lifestyle habits, and values. Predictive tools are used to classify or profile people's personality traits, characteristics, mood, and other points of leverage to a large extent, allowing assumptions to be made about deep personality traits, including political views and other special categories of data. The extension of such data processing techniques to political purposes poses serious risks, not only to the rights to privacy and to data protection, but also to trust in the integrity of the democratic process.²¹

Despite increased efforts by web platforms²² to counter these effects²³, according to Oxford's new report, the use of these techniques by governments around the world is growing and the strategies are no longer limited to large countries. Smaller States can easily set up Internet operations as well, using not only personal information, but combining this with the potential of bots²⁴, targeted misinformation, fake profiles, and hired "trolls."

Researchers at the Oxford Internet Institute built a case-based analysis of computational propaganda²⁵ in order to better understand its global reach. It was found that in the last two years, the number of countries with political disinformation campaigns more than doubled to 70, with evidence of at least one political party or governmental entity in each of those countries engaged in manipulation of social media. The World Economic Forum recently listed the spread of misinformation online as among the top 10 perils to society. Research has found that social media favors sensationalist content, regardless of whether the content has been fact-checked or is from a reliable source.²⁶

Oxford researchers said governments are increasingly opting for social media to curtail human rights, undermine political opponents, and suppress dissent, including in countries like Azerbaijan, Zimbabwe, and Bahrain. The report also states that in Tajikistan, university students were recruited to set up fake accounts and share pro-government views.^{27 28 29 30} Through mixing real news with misinformation and unconstrained Internet content, target voters find messages on many pages reinforcing their perspectives without knowing that they are some of the only people in the world that are getting such messages, nor are they aware that they are targets of political campaigning.^{31 32 33}

Researchers concluded that most of the government-linked disinformation efforts were domestically focused; but at least seven countries are trying to influence views outside their borders: China, India, Iran, Pakistan, Russia, Saudi Arabia, and Venezuela. Political advertisements were aimed at creating images, videos, or other content pieces designed to take advantage of the algorithms of social networks and their amplifying power – leveraging the viral potential on each platform.^{34 35}

Internet platforms are often lacking sufficient transparency in their informational and algorithmic clipping, giving consumers a false idea that information has a neutral and free flow. But in some cases users are interacting in filter bubbles looking at a digital reality provided by algorithmic filtering tailored specifically to them, considering their needs, wishes, fears, and weaknesses based on their personal data. Algorithm filtering in online environments allows a degree of customization and targeting on a much larger scale, which tends to accelerate with the increase of the Internet of Things scenario, given that with more and more intelligent devices connected around us, we will have even more personal data being collected, stored, processed, and transferred.^{36 37}

The echo-chamber/filter-bubble effect

The so called echo chamber/filter bubble³⁸ effect is related to a defined set of data produced by all the algorithmic mechanisms used to make an invisible edition aimed at the customization of online navigation.³⁹ It is content customization made by Internet platforms/applications to enhance both users' experience and ads revenue for its companies.⁴⁰

Filtering has emerged as a necessity and is often considered welcome, generating a great deal of comfort for the user, who quickly and efficiently finds, in most cases, the information or any other content that he wants to access. This is Netflix's business model, for instance, which allows the user to have at his disposal a collection of movies based solely on his profile through the suggestion of personalized titles and filters, in order to improve his experience. The same convenience and experience enhancement argument is applicable for Google's search engine, Facebook's timeline, Instagram, LinkedIn, Amazon, and many other platforms and applications where the business model is based on ads, micro targeting, and the profiling of users.⁴¹

Beyond convenience and user experience, the problem lies in the form and in the excess of filtering, both by the companies and by the individuals themselves, who, unconsciously, restrict themselves and move away from contradictory perspectives,

impoverishing the value of the debate in the virtual public sphere⁴². Consequently, filter bubbles can limit users to an algorithmic prediction that only provides specific targeted content based on personal data processing.⁴³ This creates a problem in accessing the information that should be seen to enrich the democratic debate.⁴⁴ From another perspective, the internet user, when navigating the most well-known sites, is today the target of a torrent of targeted advertising that signifies the commercial interest behind this filtering and personalization mechanism.⁴⁵

Shaping digital platforms into tailored reality spaces, can generate echo chambers and filter bubbles, isolating people from what they eventually need to see. This effect can be perceived as damaging to the debate and the formation of consensus in the connected public sphere, since it can restrict access to information, as well as the autonomy of individuals, potentially increasing polarization and radicalization of discourses.^{46 47 48}

There are though divergences concerning the real effect that filter bubbles and echo chambers⁴⁹ represent today on social platforms and also in the political context. Inaccurate generalization must be avoided in order to permit a more complex analysis.⁵⁰ As Simon Hegelich states, users aren't in fact in a 'bubble':⁵¹ "They are actually communicating different topics in various networks and deciding at any time when to discuss ideas that go beyond their own ideological confines. Nevertheless, as Hegelich put it, "while every user in principle has the option to look up the original source of the information and consume unbiased information, this again requires a switch to rational logic. The architecture of social networks does not prevent this from happening, but Facebook, Twitter, etc. are designed for private exchanges between friends where, as a matter of principle, homophily is welcomed (...)."⁵²

So despite the fact that there are still some divergences⁵³ concerning the impact of echo chambers and filter bubbles, as well as its variations in different countries and sociotechnical contexts, its existence and importance are well highlighted by many scholars and researchers. Although empirical evidence is still being consolidated to support stronger concerns about filter bubbles, as personalization technology improves⁵⁴, and personalized news content becomes people's main information source, problems for our democracy can arise.⁵⁵

According to Michela Del Vicario et Al.:⁵⁶

Users tend to aggregate in communities of interest, which causes reinforcement and fosters confirmation bias, segregation, and polarization. This comes at the expense of the quality of the information and leads to proliferation of biased narratives fomented by unsubstantiated rumors, mistrust, and paranoia. According to these settings, algorithmic solutions do not seem to be the best options for breaking such a symmetry.

According to Dr. Judith Moeller, Prof. Dr. Natali Helberger⁵⁷

It cannot be denied that, as a result of the proliferation of profiling and targeting practices, the way news is distributed as well as consumed has changed, and profoundly so. A growing number of users (also) consume news content via large, highly personalized information intermediaries or platforms – platforms that do not share the edi-

torial ethos and commitment to diversity that traditional, quality news outlets adhere to. Particularly those parts of the population for whom these platforms are the main gateways to information do risk, if not ending up in filter bubbles, then at least having only limited access and to a strongly filtered, and potentially biased towards popular (mainly US and UK based) information sources. In addition, the multiplication of informational content and sources online do create the need for new ways of curating and filtering news content.

In light of the above, the idea that Internet infrastructure as a public sphere has the potential to allow the discussions to be strong enough to reach different segments and different interest groups, replicating through the various networks of people who make up society, may be an increasingly distant reality.⁵⁸ This is due to the fact that the expressions can be often restricted to networks of people with common interests and communication channels designed by the platform holders to reinforce this effect.⁵⁹ The consequence of this has the potential to lead towards a fragmentation and polarization of the public debate⁶⁰, creating more fertile ground for political manipulation.⁶¹

The Brazilian experience: election campaign in 2018

Similar to the Donald Trump campaign in 2016, the Brazilian election campaign in 2018 in Brazil also revealed that messages were massively sent through social media platforms to influence the electorate.⁶² Political manipulation through misinformation, algorithmic manipulation, behavioral micro-targeting, and social bots⁶³ have been widely used and mostly based on unauthorized processing of personal data, taking advantage also of national idiosyncrasies and cultural aspects.

Brazil is the largest country in Latin America with a population of approximately 208 million people. Although 66% of Brazilians have access to the Internet, 49% access the Internet only through mobile phones.⁶⁴ According to a survey conducted by Consumer Watch, the main reason for Brazilians to access the Internet is to use social networks. Brazil is one of the countries that uses the most social platforms. 39% of national Internet users check their social networks more than 10 times a day, being online on average five hours a day, mainly browsing social networks.⁶⁵

While Facebook and Twitter were massively used in the US electoral campaign, in Brazil WhatsApp played a major role.⁶⁶ WhatsApp has become one of the most important weapons for computational propaganda and misinformation in the Brazilian political scenario. Facilitated accessibility to the platform through zero-rating practices helped WhatsApp's user penetration rate in the country. Facebook was the first app to circumvent the net neutrality⁶⁷ rules in Brazil, and today WhatsApp is the most used chat app in Brazil (120 million users).⁶⁸

Despite belonging to the same economic group as Facebook, WhatsApp brings a new layer of challenges. It has a different role as an instantaneous messaging platform, and its messages feature end-to-end encryption. Therefore, although it guarantees better protection of user's privacy and personal data, at the same time it is also more difficult to investigate and moderate content since even the company itself does not have direct access to the content of the messages (*a priori*).⁶⁹ The intricacies of the

platform made thus harder for the massive electoral content to be flagged or even to assure candidates that the platform would not be used for illicit purposes, such as unfair political advertising, propagation of hate speech, or false facts spread by automatized processes.⁷⁰

Although WhatsApp does not allow any advertising, marketing companies offer political campaigning services exclusively for the messaging app. Ongoing investigations in Brazil are showing that third party companies, dedicated to political marketing campaigns, acted in the last election campaign in Brazil, targeting groups with the purpose of political manipulation, not only disrespecting the terms of use of the platform, through its techniques of mass messaging to spread misinformation (which is prohibited by the platform), but also using unauthorized databases, disrespecting best practices of data protection.⁷¹ As a common practice, they collect voter data, such as phone numbers at events, and from there build up broadcast lists that can reach 20,000 users to send an average of 10 messages per day to each user in the messaging app.⁷²

Based on GDPR standards, the possibilities of any personal data processing, even when based on “publicly available personal data” and used in the electoral context, must be carefully addressed, taking into account what happened in specific situations such as the abovementioned CA case. Even though there can be exemptions for consent, in many cases, the processing can be considered illegal by not taking fundamental compliance steps, such as informing the data subject about the processing and guaranteeing basic data protection principles and rights.^{73 74 75 76}

On October 2019, WhatsApp, for the first time, admitted massive messaging on its platform, with automated systems (bots)⁷⁷ hired by companies, during the last presidential election campaign in Brazil. The acknowledgment was made by the messaging platform’s Public Policy officer, Ben Supple, who explained that there was a “breach of the terms of use” that prohibit the automation and massive sending of content.⁷⁸ Nevertheless, one year before, in October 2018, a Brazilian newspaper⁷⁹ had already revealed that marketing companies were hired to send out mass political messages, also containing misinformation⁸⁰ content.⁸¹ The strategy became public when the press disclosed that there were contracts of around R\$ 12 million for mass sending of messages and also purchasing of third party databases. Names, birth dates, and identification numbers of national and foreign elderly people were also used to register cell phone chips without their consent, for the purpose of mass generating messages on WhatsApp from these numbers and targeting recipients based on their income and geographic region.⁸²

The growth of robot-led action thereupon represents a real danger to public debate, representing hazards to democracy itself, interfering with the process of consensus-building in the public sphere, and in choosing representatives and government agendas.⁸³ Confirming the thesis of risk to democracy, the Directorate for Public Policy Analysis (DAPP) of FGV (Getulio Vargas Foundation) disclosed illegitimate interference in the online debate during the 2018⁸⁴ election⁸⁵ and in public debates in general.⁸⁶ Scheduled accounts for mass postings have become a tool for manipulating social media debates. In the course of the electoral race of 2018, automated accounts were responsible for 12.9% of interactions on Twitter.^{87 88 89 90}

A former employee of one of the companies (Yacows) who coordinated the messaging process, claimed to have used a list with information of ten thousand people to illegally access their personal data to send the messages, with the intent of circumventing the filtering of numbers put in place by WhatsApp. The use of robots was also declared, with the confession that for each 50 messages there was a 10-second pause to also try to circumvent the WhatsApp block.^{91 92} Up to 300,000 WhatsApp accounts may have been used to automate broadcasts of disinformation and coordinate non-reported political advertising to thousands of WhatsApp groups.^{93 94 95 96}

Due to disclosures by the press, investigations are examining the involvement of politicians, parties, and supporters concerning misinformation and political manipulation. The investigations are exposing important facts and testimonials. At the same time, they reveal the complex circumstances especially the judicial system is facing in the fight against misconduct within digital campaigning.^{97 98 99 100 101 102}

The new model of data-driven campaigning poses a systemic and institutional challenge that cannot be solved quickly and needs a combination of political and regulatory approaches. Stronger data protection is certainly part of the answer¹⁰³: properly enforcing Europe's General Data Protection Regulation, which has international reach, and using it as a model in other countries, could help to mitigate the extent of data-mining and profiling used for political manipulation.¹⁰⁴ In the words of Iva Nenadić, "the efficiency of online micro-targeting depends largely on data and profiling. Therefore, if effectively implemented, the GDPR should be of use here by preventing the unlawful processing of personal data."¹⁰⁵

According to the Privacy International Organization:¹⁰⁶

Where data is generated, individuals should be able to find out which companies hold what kinds of data about them. Profiling generates highly sensitive inferences and predictions about people's personality, behavior, or beliefs. (...) Companies that have accumulated years of sensitive data on billions of people around the world may be able to change people's actual behavior at scale. (...) Individuals should be able to access these inferences and predictions about them, in order to effectively challenge them, or to ask for profiles to be deleted.

Personal data is key to this debate. Echoing the words of Linda Risso:¹⁰⁷ "It is clear that lawmakers are lagging behind and that there is an increasingly wider gap between the current status of technology and the focus of the law."¹⁰⁸ Therefore it is crucial that national governments come to grips quickly with the ethical and legal challenges posed by social media, computational propaganda, and data protection.¹⁰⁹ Since 2017, EU data protection rules mean that personal data can only be processed in certain situations and under certain conditions. However, the question of how this will work in practice remains open."^{110 111 112 113}

1. Hacking the Electorate

- 11 "The most important source of the data was Facebook. Via a third-party app, Cambridge Analytica improperly obtained data from up to 87 million Facebook profiles – including status updates, likes, and even private messages, and individually micro-target messages to influence their behavior." Westby, Joe (2019), "The Great Hack: Cambridge Analytica is just the tip of the iceberg", Amnesty Tech, <https://www.amnesty.org/en/latest/news/2019/07/the-great-hack-facebook-cambridge-analytica/>, access January 2020.
- 12 According to Christopher Wylie, one of Cambridge Analytica's co-founders and whistleblower: "We exploited Facebook to harvest millions of people's profiles and built models to exploit what we knew about them and target their inner demons." See <https://www.theverge.com/2018/3/20/17138854/cambridge-analytica-facebook-data-trump-campaign-psychographic-microtargeting>, access January, 2020.
- 13 'Not having a Facebook account did not provide protection – the litany of available data sources is not limited to Facebook, and the analysis can easily apply to other points of personal preference. In addition, every website with the Facebook logo is linked to Facebook, allowing for tracking of non-members as well as members who might not have opted in for the service. There are many similar sources of online tracking – for instance, web beacons – most of which are tied to "cookies" that can be used across websites, and access can be sold to interested buyers.' Isaak; Mina J. Hanna (2018), "User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection," IEEE Computer Volume: 51 Issue: 8, <https://ieeexplore.ieee.org/abstract/document/8436400>, access August, 2018.
- 14 Grassegger, Hannes, and Krogerus, Mikael (2017), "The Data That Turned the World Upside Down," Motherboard, https://www.vice.com/en_us/article/mg9vvn/how-our-likes-helped-trump-win, access October, 2019.
- 15 S. C. Matz, M. Kosinski, G. Nave, D. J. Stillwell (2017), "Psychological targeting in digital mass persuasion," National Academy of Sciences, See also Moon, Y. (2016), "Personalization and personality: Some effects of customizing message style based on consumer personality," Journal of Consumer Psychology, Elsevier.
- 16 Because of the many factors involved in the process of political manipulation, from cultural to technological and psychological/idiosyncratic factors, it is still difficult to attest with clear certainty exactly how it happened and how many people were manipulated through these techniques. Empirical research examining specifically online communication processes and outcomes is still scant.
- 17 Youyou, Wu et al. (2015), "Computer-based personality judgments are more accurate than those made by humans," PNAS. <https://www.bbc.com/news/technology-45976300>, access October, 2019.
- 18 Information Commissioner's Office (ICO) (2018), "Investigation into the use of data analytics in political campaigns: a report to Parliament," <https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf>, access September, 2019.
- 19 Information Commissioner's Office (ICO) (2018), "Investigation into the use of data analytics in political campaigns: a report to Parliament," <https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf>, access September, 2019.
- 20 European Data Protection Board (2019), "Statement 2/2019 on the use of personal data in the course of political campaigns," https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-03-13-statement-on-elections_en.pdf, access January, 2020.
- 21 The European Council adopted a set of policies requiring political parties to adhere to EU data protection rules. European Council (2019), "EP elections: EU adopts new rules to prevent misuse of personal data by European political parties," <https://www.consilium.europa.eu/en/press/press-releases/2019/03/19/ep-elections-eu-adopts-new-rules-to-prevent-misuse-of-personal-data-by-european-political-parties/>, In: Chester, J. & Montgomery, K. C. (2019), "The digital commercialization of US politics – 2020 and beyond," Internet Policy Review, 8(4).
- 22 WhatsApp for instance limited the number of members of each group to 256, and the number of messages following to five at a time. WhatsApp also implemented the need of authorization to be added in a specific WhatsApp group and deleted nearly 1.5 million accounts in the last Brazilian elections that were to some extent engaging in the automatization of content, or any other malpractice. Google, for its part, will stop giving advertisers the ability to target election ads using data such as public voter records and general political affiliations. Facebook, for its part, stated that it will remove deepfakes. Twitter decided in October that it simply would not accept any more political propaganda. Google, for its part, determined in November that anyone who wanted to hire political advertising in the United States (including for YouTube) would no longer be able to target the publication to users filtered by ideological preference. See <https://piaui.folha.uol.com.br/materia/o-algoritmo-da-agera/>. See <https://www.zdnet.com/article/whatsapp-banned-nearly-half-a-million-accounts-during-brazilian-elections/>. See <https://faq.whatsapp.com/en/30046788/?lang=en>. See <https://mobile-reuters-com.cdn.ampproject.org/c/s/mobile.reuters.com/article/amp/idUSKBN1XU2WT>. See https://link.estadao.com.br/noticias/empresas,facebook-passara-a-remover-videos-falsos-e-deepfakes-da-rede-social,70003146938?utm_source=facebook:newsfeed&utm_medium=social-organic&utm_campaign=redes-sociais:012020:e&utm_content=::&utm_term=, access February, 2020.
- 23 One issue that should not be overlooked in this context is the importance of educational and training work on the phenomenon of online misinformation. According to a survey conducted by the company

- Kaspersky, which went deeper in understanding how Latin America deals with fake news: On average, 70% of Latin Americans do not know how to identify or are not sure whether they can differentiate if news on the internet is false or true. By nationality, the citizens least able to recognize false news are Peruvians (79%), followed by Colombians (73%) and Chileans (70%). Further back are Argentines and Mexicans, with 66%, and then Brazilians (62%). See https://veja.abril.com.br/tecnologia/62-dos-brasileiros-nao-sabem-reconhecer-uma-noticia-falsa/amp/?__twitter_impression=true&fbclid=IwAR0hLFm_NOT-v61xTWYDazqY4Oi_Uf_HFUCnlkqyDJf6A1zjwNdfGIUGM8gE, access February, 2020.
- 24 "Bots, the automated programs integral to the spread of computational propaganda, are software intended to perform simple, repetitive, robotic tasks. They are used to computationally enhance the ability of humans to get work done online. Social media bots are automated identities that can perform mundane tasks like collect information, but they can also communicate with people and systems. They are deployed to perform legitimate tasks like delivering news and information. They also are used for more malicious activities associated with spamming and harassment. Whatever their uses, they are able to rapidly deploy messages, interact with other users' content, and effect trending algorithms – all while passing as human users. Political bots, social media bots used for political manipulation, are also effective tools for strengthening online propaganda and hate campaigns. One person, or a small group of people, can use an army of political bots on Twitter to give the illusion of large-scale consensus." Woolley, Samuel, and Howard, Philip (2017), "Computational Propaganda Worldwide," University of Oxford, <http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf>, access February, 2020.
 - 25 Woolley, Samuel and Howard, Philip (2017), "Computational Propaganda Worldwide," University of Oxford, <http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf>, access February, 2020.
 - 26 Woolley, Samuel, and Howard, Philip (2017), "Computational Propaganda Worldwide," University of Oxford, <http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf>, access February, 2020.
 - 27 'Governments and parties are using "cyber troops" to shape public opinion, including networks of bots to amplify messages, groups of "trolls" to harass political dissidents such as journalists and activists, and fake social media accounts to misrepresent the number of people engaged on an issue. Governments are spreading disinformation in order to discredit political opponents, hide opposing views, and even intervene in foreign affairs.' Alba, D. and Satariano, A. (2019), "At Least 70 Countries Have Had Disinformation Campaigns", NY Times.
 - 28 "Ultimately, if these capabilities are as powerful as the companies and their customers claim, they pose a real threat to our ability to make our own autonomous decisions or even our right to opinion, undermining the fundamental value of dignity that underpin all human rights. Advertising and propaganda aren't new, but there is no precedent for targeting individuals in such intimate depth, and at the scale of whole populations." Westby, Joe (2019), "The Great Hack: Cambridge Analytica is just the tip of the iceberg, Amnesty Tech, <https://www.amnesty.org/en/latest/news/2019/07/the-great-hack-facebook-cambridge-analytica/>, access January 2020.
 - 29 Isaak; Mina J. Hanna (2018), "User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection," IEEE Computer Volume: 51 Issue: 8, <https://ieeexplore.ieee.org/abstract/document/8436400>, access August, 2018.
 - 30 Woolley, Samuel and Howard, Philip (2017), "Computational Propaganda Worldwide," University of Oxford, <http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf>, access February, 2020.
 - 31 Risso, Linda (2017), "Harvesting Your Soul? Cambridge Analytica and Brexit," Akademie der Wissenschaften und der Literatur, http://www.adwmainz.de/fileadmin/user_upload/Brexit-Symposium_Online-Version.pdf#page=75, access December, 2019. See also Samuel C. Woolley and Philip N. Howard (2017), Computational Propaganda Worldwide, University of Oxford, <http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf>, access October, 2019. See also Funke D. and Flamini, D. (2019), "A guide to anti-misinformation actions around the world," <https://www.poynter.org/ifcn/anti-misinformation-actions/>, access December, 2019.
 - 32 Bradshaw, S. Howard, P. (2019), "The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation," University of Oxford, <https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf>, access December, 2019.
 - 33 Funke D. and Flamini, D. (2019), "A guide to anti-misinformation actions around the world," <https://www.poynter.org/ifcn/anti-misinformation-actions/>, access December, 2019.
 - 34 Alba, D. and Satariano, A. (2019), "At Least 70 Countries Have Had Disinformation Campaigns," NY Times.
 - 35 Samuel C. Woolley and Philip N. Howard (2017), Computational Propaganda Worldwide, University of Oxford, <http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf>, access October, 2019.

1. Hacking the Electorate

- 36 Bayer, J. et al. (2019), "Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States. European Parliament," [http://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU\(2019\)608864_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU(2019)608864_EN.pdf), access February, 2020.
- 37 Anderson, J. and Rainie, L. (2017), "The Future of Truth and Misinformation Online," Pew Research Center, [web/imagining/surveys/2017_survey/Future_of_Info_Environment_Elon_University_Pew_10-18-17.pdf](http://www.pewresearch.org/internet/2017/07/11/future-of-truth-and-misinformation-online/), access February, 2020.
- 38 Pariser, E. (2011), "The Filter Bubble: What the Internet is Hiding from You," Penguin Press.
- 39 Magrani, Eduardo (2014), "Democracia Conectada," Jurua, <https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/14106/Democracia%20conectada.pdf?sequence=1&isAllowed=y>, access September, 2019.
- 40 'Cookies are, in a nutshell, access data that consist of the "digital footprints" left when passing through and manifesting through online environments.' Wu, Tim (2011), "The Master Switch: The Rise and Fall of Information Empire," Vintage.
- 41 Magrani, Eduardo and Medeiros, R. (2019), "The public sphere forged in the era of fake news and filter bubbles: the Brazilian experience of 2018," *Cyber law*.
- 42 Magrani, Eduardo (2014), "Democracia Conectada," Jurua, <https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/14106/Democracia%20conectada.pdf?sequence=1&isAllowed=y>, access September, 2019.
- 43 Morozov, E. (2013), "To Save Everything, Click Here: The Folly of Technological Solutionism," *Public Affairs*.
- 44 Borgesius, Z. et al. (2016), "Should we worry about filter bubbles?," *Internet Policy Review*, 5(1).
- 45 Magrani, Eduardo and Medeiros, R. (2019), "The public sphere forged in the era of fake news and filter bubbles: the Brazilian experience of 2018," *Cyber law*.
- 46 A peremptory statement in this direction would require further study, so that the specific approach of this point would go beyond the limits of this study.
- 47 "Many people are unaware that filter bubbles even exist. More than 60% of Facebook users are entirely unaware of any curation on Facebook at all, believing instead that every single story from their friends and followed pages appeared in their news feed." Hern, A. (2017), "How social media filter bubbles and algorithms influence the election. The Guardian. <https://www.theguardian.com/technology/2017/may/22/social-media-election-facebook-filter-bubbles>, access October, 2019.
- 48 Allred, K. (2018), "The Causes and Effects of 'Filter Bubbles' and how to Break Free," Medium, <https://medium.com/@10797952/the-causes-and-effects-of-filter-bubbles-and-how-to-break-free-df6c-5cbf919f>, access October, 2019.
- 49 This debate is also diffculted by the divergent concepts around both terms. See Bruns, A. (2019), "Filter Bubbles and Echo Chambers: Debunking the Myths," Medium, <https://medium.com/dmrc-at-large/are-filter-bubbles-real-3be22bd9230e>, access October, 2019. See also Moeller, J., & Helberger, N. (2018), "Beyond the filter bubble: Concepts, myths, evidence, and issues for future debates," University of Amsterdam, https://www.ivir.nl/publicaties/download/Beyond_the_filter_bubble__concepts_myths_evidence_and_issues_for_future_debates.pdf, access October, 2019.
- 50 Bruns, A. (2019), "Are Filter Bubbles Real?," *Digital future series*.
- 51 Hegelich, S. and Shahrezaye, M. (2017), "Disruptions to political opinion: Political debate in the age of echo chambers and filter bubbles," KAS Facts and Findings n 253, https://www.kas.de/documents/252038/253252/7_dokument_dok_pdf_49188_2.pdf/d3741812-3abb-c52a-fe75-658665e274d7?version=1.0&t=1539649011639, access October, 2019.
- 52 Hegelich, S. and Shahrezaye, M. (2017), "Disruptions to political opinion: Political debate in the age of echo chambers and filter bubbles," KAS Facts and Findings n 253, https://www.kas.de/documents/252038/253252/7_dokument_dok_pdf_49188_2.pdf/d3741812-3abb-c52a-fe75-658665e274d7?version=1.0&t=1539649011639, access October, 2019.
- 53 "Such moral panics distract us from more important matters, as Sebastian Meineck has put it, it is only when the tale of the filter bubble bursts that the debate about the transformation of the public sphere can get started. This debate will need to examine whether societies around the world, from Australia to Brazil, from Germany to the United States, are becoming increasingly polarized, or whether such polarization is simply becoming more visible; (...) these transformations severely disrupt and sometimes paralyze existing political systems and undermine fundamental societal consensus. But it will also need to recognize that such transformations are not fueled simply by surface factors such as the communication technologies and platforms preferred by these new political actors and their established opponents, respectively – rather, they are an expression of far more fundamental social, economic, societal, and political challenges. This does not mean that search and social media platforms are free of fault, of course – indeed, at present there is an acute need to compel them (through regulatory or other means) to do more to remove extremist accounts, prevent the circulation of disinformation, and open themselves to independent scholarly scrutiny. On the specific question of filter bubbles, however, they appear largely free of blame." Bruns, A. (2019), "Filter bubble," *Internet Policy Review*.

- 54 Because of the many factors involved in the process of political manipulation, from cultural to technological and psychological/idiosyncratic factors, it is still difficult to attest with clear certainty exactly how and how many people were influenced. Empirical research examining specifically online communication processes and outcomes is still scant. Echoing the words of Zuiderveen et al.: “Empirical research into the extent of personalized communication, and its effects on access to diverse information, can serve as a reality check. Empirical research can help to adjust the priorities in public policy, and to identify areas in which we simply do not know enough to make any conclusive policy statements. (...) if personalization technology improves, and personalized news content becomes people’s main information source, problems for our democracy could indeed arise, as our review of empirical studies of media effects has shown.” Zuiderveen Borgesius, F. J. & Trilling, D. & Möller, J. & Bodó, B. & de Vreese, C. H. & Helberger, N. (2016), “Should we worry about filter bubbles?,” *Internet Policy Review*, 5(1).
- 55 Zuiderveen Borgesius, F. J. & Trilling, D. & Möller, J. & Bodó, B. & de Vreese, C. H. & Helberger, N. (2016), “Should we worry about filter bubbles?,” *Internet Policy Review*, 5(1).
- 56 Del Vicario, Michela et al. (2016), “The spreading of misinformation online,” *Proceedings of the National Academy of Sciences of the United States of America*, <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4725489/>, access October, 2019.
- 57 Moeller, J., & Helberger, N. (2018), “Beyond the filter bubble: Concepts, myths, evidence, and issues for future debates,” University of Amsterdam, https://www.ivir.nl/publicaties/download/Beyond_the_filter_bubble_concepts_myths_evidence_and_issues_for_future_debates.pdf, access October, 2019.
- 58 “Facebook conducted a massive psychological experiment on 689,003 users, manipulating their news feeds to assess the effects on their emotions. Facebook has the ability to make you feel good or bad, just by tweaking what shows up in your news feed. They relied on an automated system that identified positive or negative words based on an electronic dictionary. They reduced the positive content in some users’ news feeds, finding that when the positive content was reduced, a larger percentage of words in people’s status updates were negative and a smaller percentage were positive. When negativity was reduced, the opposite pattern occurred. The authors found that these results suggest that the emotions expressed by friends, via online social networks, influence our own moods, constituting, to our knowledge, the first experimental evidence for massive-scale emotional contagion via social networks and providing support for previously contested claims that emotions spread via contagion through a network.” McNeal, G. (2014), “Facebook Manipulated User News Feeds to Create Emotional Responses,” <https://www.forbes.com/sites/gregorymcneal/2014/06/28/facebook-manipulated-user-news-feeds-to-create-emotional-contagion/#10567b1039dc>, access October, 2019. See also Ryan, C. (2013), “Digital Market Manipulation,” University of Washington School of Law Research Paper No. 2013–27.
- 59 As Cass Sunstein states, bubble filters would be a serious risk to the potential of the connected public sphere due to the lack of contact with dissenting opinions and the polarization of discourses leading to radicalism. This would be a problem with trends not to its resolution, but to its aggravation, from the sophistication of content customization algorithms. Sunstein, C. (2011), “*Republic.com 2.0.*,” Princeton University Press. See also Sunstein, C. (2001), “*Republic.com*,” Princeton University Press.
- 60 Individuals have an important responsibility in this context, for reducing their own personal filter bubbles. By understanding and managing customization features, cookies gatherings, and targeted ads on websites, we can limit the effect that algorithms have on our content.
- 61 Magrani, Eduardo and Medeiros, R. (2019), “The public sphere forged in the era of fake news and filter bubbles: the Brazilian experience of 2018,” *Cyber law. A peremptory statement in this direction would require further study, so that the specific approach of this point would go beyond the limits of this study.*
- 62 See <https://www1.folha.uol.com.br/poder/2019/10/whatsapp-admite-envio-massivo-ilegal-de-mensagens-nas-eleicoes-de-2018.shtml>, access October, 2019.
- 63 According to the results presented on the study “Computational Power: Automated Use of WhatsApp in the Elections,” concerning the use of bots and WhatsApp in Brazilian 2018 elections, it states: “We specifically identified that there are strong elements of the use of automation to power the distribution of information among different groups on WhatsApp. We also identified that there is coordinated action among different members in their activities in the networks of discussion groups on WhatsApp. (...) about 56% of Brazilian voters said their choices of candidates for president were influenced by social networks. Thus, there are hypotheses that point to the effectiveness of this strategy, especially in the first round, even if, to different extents and with different strategies, all candidates have made use of digital campaigns. There is still little understanding of the use of automation and computational power to influence election decisions,” Machado, Caio e Konopacki, Marco (2018), “Computational Power: Use of Automation on WhatsApp in the Elections; A study on the use of automation tools to boost political campaigns digitally in the 2018 Brazilian elections,” ITS Rio.
- 64 Casaes, D. and Córdova, Y. (2019), “Weaponized Information in Brazil: Digitizing Hate,” Policy Brief No. 63. Toda, https://toda.org/assets/files/resources/policy-briefs/t-pb-63_casaes-and-cordova_weaponised-information-in-brazil.pdf, access January, 2019.

1. Hacking the Electorate

- 65 Casaes, D. and Córdova, Y. (2019), "Weaponized Information in Brazil: Digitizing Hate," Policy Brief No. 63. Toda, https://toda.org/assets/files/resources/policy-briefs/t-pb-63_casaes-and-cordova_weaponised-information-in-brazil.pdf, access January, 2019.
- 66 WhatsApp has become a particularly powerful campaigning instrument. Easy to use, end-to-end encrypted and facilitating the sharing of messages to large groups, WhatsApp has been extremely popular in countries like India (Hickok, 2018), Brazil, and other countries in the Global South. However, WhatsApp not only allows parties to tailor messages to precise groups, it also offers anonymity, thus making it easy to misrepresent a sender's identity with the predictable and widespread concerns about the delivery of "fake news" and hate-inciting messages. Rafael Evangelista and Fernanda Bruno (2019) demonstrate the pernicious use of WhatsApp in Brazil for the spread of racist, misogynistic, and homophobic messages (...). Their analysis suggests that WhatsApp relies upon a more trusting relationship between group members than is apparent within other social media. It therefore produces a more susceptible medium for the spread of misinformation.' See Bennett, C. J. & Lyon, D. (2019), "Data-driven elections: implications and challenges for democratic societies," *Internet Policy Review*, 8(4). See also: Evangelista, R., & Bruno, F. (2019), "WhatsApp and political instability in Brazil: targeted messages and political radicalization," *Internet Policy Review*, 8(4).
- 67 Net neutrality is the principle of equal treatment of all data packages sent over the internet, irrespectively of their content, origin, destination, and type of equipment used to access it. 'Zero-rating' is when an ISP applies a price of zero to the data traffic associated with a particular application or class of applications based on commercial agreement or a unilateral decision of an internet service provider that results in some content being exempted from end users' monthly data cap.
- 68 Casaes, D. and Córdova, Y. (2019), "Weaponized Information in Brazil: Digitizing Hate," Policy Brief No. 63. Toda, https://toda.org/assets/files/resources/policy-briefs/t-pb-63_casaes-and-cordova_weaponised-information-in-brazil.pdf, access January, 2019.
- 69 Gollatz, K. and Jenner, L. (2018), "Hate Speech und Fake News – Zwei verwobene und politisierte Konzepte," HIIG.
- 70 Martins, B and Varon, J. (2018), "Data and elections in Brazil," *Coding Rights*.
- 71 There are also ongoing investigations in the electoral courts concerning non-declared payments and contracts related to mass messaging and misinformation in the electoral campaign of 2018.
- 72 Also, bots have been used to boost penetration on filter bubbles enhancing the capacity to send a massive numbers of messages online, attacking opponents and forging discussions. They manipulate debates, produce and circulate false news, and influence public opinion by posting and replicating messages on a prominent scale. Many bots have reproduced hashtags on Twitter and Facebook that gain eminence by messaging automated posts in order to strangle sudden debates on a particular topic. Martins, B and Varon, J. (2018), "Data and elections in Brazil," *Coding Rights*.
- 73 Ruediger, M. (2019), "Robots, Social Networks and Politics in Brazil: Study on Illegitimate Interference in the Public Debate on the Web, Risks to Democracy and the Electoral Process of 2018," FGV, <http://dapp.fgv.br/en/robots-social-networks-politics-fgv-dapp-study-points-illegitimate-interference-public-debate-web/>, access July, 2019.
- 74 By interfering in discussions, robots are directly reaching political and democratic processes through the influence of public opinion. Cordova Y. and Doneda, D. (2017), "A Place for the Robots in the Elections," JOTA, <https://www.jota.info/opiniao-e-analise/artigos/um-lugar-para-os-robos-nas-eleicoes-20112017>, access March, 2018.
- 75 Magrani, Eduardo and Medeiros, R. (2019), "The public sphere forged in the era of fake news and filter bubbles: the Brazilian experience of 2018," *Cyber law*.
- 76 See <https://observa2018.com.br/posts/debate-influenciado-por-robos-volta-a-crescer-e-chega-a-104-das-discussoes-sobre-os-presidenciais-no-twitter/>, access October, 2018.
- 77 It is important to note that automated accounts can also confer positive aspects of life on social networks. Chatbots, for instance, streamline customer service and, in some cases, even help consumers process their requests and get more information. Nevertheless, an increasing number of robots act with spiteful purposes in the public sphere. Social bots (social robots) are accounts controlled by software, which artificially generate content and establish interactions with non-robots. They attempt to imitate human behavior and to pass as such in order to interfere in legitimate and voluntary debates and produce forged (not organic) discussions. Institute of Technology and Equity (2017), "Experts Explain How the Robot can Influence the Debate in Networks," *Medium*, <https://medium.com/@tecnoequidade/especialistas-explicam-como-o-robô-pode-influenciar-o-debate-nas-redes-3a844f911849>, access October, 2017.
- 78 The study of the use of robots already clearly establishes the adverse potential of this practice for political dispute and public debate. One of the most apparent conclusions in this sense is the concentration of these actions in poles located at the extreme of the political spectrum, artificially promoting a radicalization of the debate in the bubble filters and, thereupon, undermining potential bridges of dialogue between the different constituted political fields. Therefore, robots can not only circulate misinformation,

- which can have damaging effects on society, but also can actively prevent users from informing themselves appropriately. Magrani, Eduardo and Medeiros, R. (2019), "The public sphere forged in the era of fake news and filter bubbles: the Brazilian experience of 2018," *Cyber law*.
- 79 See <https://www1.folha.uol.com.br/poder/2018/10/empresarios-bancam-campanha-contra-o-pt-pelo-whatsapp.shtml>, access January, 2020.
- 80 Another kind of misinformation technique that is increasing in practice and creating a major concern are "deepfakes." It is a new way to produce misinformation much more sophisticated. Deepfakes are fake videos or audio recordings that look and sound just like the real person. Technologies already allow the recording of audio with imitation almost similar to the voice of people and the editing of videos in which the face of an individual who has never been in the situation appears as a participant. If in the daily scenario of non-public people, this is already extremely harmful to a person's reputation and image, this risk grows exponentially when we talk about public people. Audio and edited videos can be used, for instance, to defame the image of a certain candidate to an electoral position. On October 23, 2018 in Brazil, a video was circulated on the internet (mainly on WhatsApp) in which, supposedly, the candidate for governor of the state of São Paulo, João Doria (PSDB), appeared in intimate scenes with women. Five days after the second round of elections, the circulation of a video in this sense is enormously damaging to the image of the candidate, especially when it is considered that Doria is a defender of traditional family values. The then-candidate filed for an investigation in Electoral Court. Initially, the investigations in relation to the video found that it was assembled or simulated: an expert report stated that the face of the candidate was wrongly inserted into the video, putting him in a situation in which he did not participate. Subsequently, a new report confirmed the accuracy of the video. In short, two technical reports with two contradictory statements. After the video was released, the voting preferences surveys showed some variation in the percentage points of each candidate. According to Datafolha's survey on October 25, 2018, Doria had 52% of the votes, while on the 27th of that month it had fallen to 49%. Considering the intensity of the campaigns in the days immediately preceding the elections and the profusion of information that is disclosed, we cannot affirm that the video was directly responsible for this fall. The fact is that the disclosure of this deep fake, accompanied by expert reports that did not indicate the same result, was not enough to prevent the victory of the candidate, who won with 51.77% of the valid votes. Note, however, that we can affirm that this kind of video can be an important factor to be faced with in the final moments of a campaign. Moreover, reality itself is called into question, and what is true or false is no longer known. This creates a mental confusion in the electorate, which happens to believe in one side without any solid ground, relying on narratives. All being questionable, the human desire for an answer grasps at any clue of truthfulness, previous bias, or even self-deception. The joint use of deepfakes with microtargeting and artificial intelligence, without proper and robust regulation to control it, is already one of the major concerns for upcoming elections. Magrani, Eduardo and Medeiros, R. (2019), "The public sphere forged in the era of fake news and filter bubbles: the Brazilian experience of 2018," *Cyber law*.
- 81 Pablo Ortellado (2018), "Bias on the Internet Does Not Seem to Be Caused by Bubbles," *Folha de São Paulo*, <https://www1.folha.uol.com.br/colunas/pablo-ortellado/2018/02/polarizacao-na-internet-nao-parece-ser-causada-pelas-bolhas.shtml>, access, October 2018. See also Mello, P. (2018), "Entrepreneurs Campaign Against the PT by WhatsApp," *Folha de São Paulo*, <https://www1.folha.uol.com.br/poder/2018/10/empresarios-bancam-campanha-contra-o-pt-pelo-whatsapp.shtml>, access October, 2018.
- 82 Magrani, Eduardo and Medeiros, R. (2019), "The public sphere forged in the era of fake news and filter bubbles: the Brazilian experience of 2018," *Cyber law*.
- 83 Bots account for more than 50% of internet traffic around the world. Some bots are intended, for example, to require accountability of politicians, to root out gender inequality, or to help organize the (many) daily tasks of their users. Other bots are aimed at spreading lies to influence conversations in the public sphere, a phenomenon that has been gaining global scale since 2014. These bots are out there and hardly anyone knows how they work, who develops them, and who they are funded by. See <https://g1.globo.com/rs/rio-grande-do-sul/noticia/pesquisa-demonstra-que-repercussao-do-cancelamento-do-queermuseu-foi-insuflada-por-robos-na-internet.ghtml>, access March, 2017.
- 84 Ruediger, M. (2019), "Robots, Social Networks and Politics in Brazil: Study on Illegitimate Interference in the Public Debate on the Web, Risks to Democracy and the Electoral Process of 2018," FGV, <http://dapp.fgv.br/en/robots-social-networks-politics-fgv-dapp-study-points-illegitimate-interference-public-debate-web/>, access July, 2019.
- 85 Ruediger, M. (2019), "Robots, Social Networks and Politics in Brazil: Study on Illegitimate Interference in the Public Debate on the Web, Risks to Democracy and the Electoral Process of 2018," FGV, <http://dapp.fgv.br/en/robots-social-networks-politics-fgv-dapp-study-points-illegitimate-interference-public-debate-web/>, access July, 2019.
- 86 Ruediger, M. (2019), "Robots, Social Networks and Politics in Brazil: Study on Illegitimate Interference in the Public Debate on the Web, Risks to Democracy and the Electoral Process of 2018," FGV, <http://dapp.fgv.br/en/robots-social-networks-politics-fgv-dapp-study-points-illegitimate-interference-public-debate-web/>, access July, 2019.

1. Hacking the Electorate

- 87 In 2014, the first presidential election in which the robots played a more meaningful role, the interference was similar. The bots accounted for more than 10% of interactions on Twitter. Formerly during the impeachment process of previous President Dilma Rousseff, robots were responsible for 20% of the debate between the supporters of Dilma. In the second round of the 2014 elections, 20% of the interactions in favor of Aécio Neves were brought forth by robots. See Ruediger, M. (2019), "Robots, Social Networks and Politics in Brazil: Study on Illegitimate Interference in the Public Debate on the Web, Risks to Democracy and the Electoral Process of 2018," FGV, <http://dapp.fgv.br/en/robots-social-networks-politics-fgv-dapp-study-points-illegitimate-interference-public-debate-web/>, access July, 2019.
- 88 "Twitter claims that, since June 2017, it has detected a daily average of 130,000 accounts that attempted to manipulate trending topics through social bots. The social network claims that there are about 16 million fake or spam accounts. Experts estimate a higher number. The dynamics are known as "botnet," or network of robots, when profiles act in a synchronized manner, with the same performance – one posts and others retweet, or respond, or publish something similar. The general rules of the platform state that it is not allowed to use Twitter services in order to artificially amplify or suppress information or to engage in behavior that manipulates or harms people's experience on Twitter. According to the social network, accounts that violate these rules can be punished with reduced viewing, removed from the Twitter search engine and even banned." See <https://apublica.org/2019/12/como-funciona-um-perfil-robot-no-twitter/>, access January, 2020.
- 89 "The detection through machine learning occurs by coding the behavior patterns from the collection of metadata. In this way, the system is able to automatically identify humans and robots based on the behavioral pattern of the profile. User metadata is considered one of the most predictable aspects of human and robot differentiation and can contribute to better understanding how sophisticated robots work. Identifying these robots or hacked accounts, however, is difficult for these systems. In addition, the constant evolution of robots causes the system, built from a static database, to become less accurate over time. However, it allows you to process a large number of complex correlations and patterns, as well as analyze a large number of accounts. The most efficient identification mechanisms combine different aspects of these approaches, exploring multiple dimensions of profile behavior, such as activity and time patterns. These systems take into account, for example, that real users spend more time on the network exchanging messages and visiting the content of other users, such as photos and videos, while robots' accounts spend their time searching profiles and sending friendship requests." Ruediger, M. (2019), "Robots, Social Networks and Politics in Brazil: Study on Illegitimate Interference in the Public Debate on the Web, Risks to Democracy and the Electoral Process of 2018," FGV, <http://dapp.fgv.br/en/robots-social-networks-politics-fgv-dapp-study-points-illegitimate-interference-public-debate-web/>, access July, 2019.
- 90 Magrani, Eduardo and Medeiros, R. (2019), "The public sphere forged in the era of fake news and filter bubbles: the Brazilian experience of 2018," *Cyber law*.
- 91 Simões, M. (2018), "Pro-Bolsonaro Groups on WhatsApp Orchestrate Fake news and Personal Attacks on the Internet, Research Says," *El País*, https://brasil.elpais.com/brasil/2018/10/23/politica/1540304695_112075.html?id_externo_rsoc=FB_BR_CM&fbclid=IwAR05Mw9zXzmjDbYv5OkjAm1hVipWBURMCPyiOORlaxSsy_qNxEjzrpHKxfQ, access October, 2018.
- 92 See <https://observa2018.com.br/posts/fraude-nas-urnas-e-kit-gay-tem-maior-impacto-que-outras-noticias-falsas-em-twitter-facebook-e-youtube/>, access October, 2018.
- 93 Gianetti, E. (2005), "Lies We Live By: The Art of Self-deception," *Companhia das Letras*.
- 94 There are project bills in the Brazilian National Congress that seek to criminalize the disclosure of false facts/fake news, such as Bill No. 9973/2018, 10292/2018, 9931/2018 and 9532/2018 in the House of Representatives. Senate Bill No. 246/2018 is broader and seeks to insert in the Civil Framework of the Internet "measures to combat the disclosure of fake content or offensive Internet applications." In addition, there are groups intended to accomplish fact-checking. But in a scenario where everything is questionable, the profusion of true and false information could lead to the so-called context of "infocalypse," as stated by Prof. Aviv Ovadya, jeopardizing the possibility of consensus on a rational and democratic basis. That is why we affirm above that it is essential to guarantee a minimum level of consensus on reality and a respect for fundamental ethical principles. An exhaustive enumeration and detailed presentation of all bills on the subject would require its own study and would go beyond the limits of this article. See <https://www.uol/noticias/especiais/ele-previu-o-apocalipse-das-noticias-falsas.htm>, access January, 2020.
- 95 See <https://www1.folha.uol.com.br/poder/2018/12/fraude-com-cpf-viabilizou-disparo-de-mensagens-de-whatsapp-na-eleicao.shtml>. See also <https://www1.folha.uol.com.br/poder/2018/10/empresarios-bancam-campanha-contra-o-pt-pelo-whatsapp.shtml> See also <https://www1.folha.uol.com.br/poder/2018/10/entenda-as-irregularidades-envolvendo-uso-do-whatsapp-na-eleicao.shtml>, access January, 2020.
- 96 See <https://riotimesonline.com/brazil-news/brazil/whatsapp-admits-to-illegal-mass>, access November, 2019.
- 97 Facebook, which has been under increasing pressure to do more to tackle misinformation, announced an update of WhatsApp in January that reduced the number of times users can forward a single message to five. See <https://www.theguardian.com/world/2019/oct/29/europe-accuses-facebook-of-being-slow-to-remove-fake-accounts>, access January, 2020. See also <https://www.theguardian.com/>

- technology/2019/jan/21/whatsapp-limits-message-forwarding-fight-fake-news. See also https://politica.estadao.com.br/blogs/estadao-verifica/limite-de-encaminhamento-no-whatsapp-nao-consegue-frear-desinformacao-na-plataforma-aponta-pesquisa/?amp&__twitter_impression=true&fbclid=IwAR1X_aDEg7Mlz_0OoCE1piZHkO_TyyMQVgyw9SH-hT4Vc37Lbfj5By6JumU, access January, 2020.
- 98 See https://www.theguardian.com/world/2019/oct/30/whatsapp-fake-news-brazil-election-favoured-jair-bolsonaro-analysis-suggests?CMP=share_btn_fb, access January, 2020.
- 99 According to Yasodora Cordova and Diego Casaes in a recent report about the Brazilian context: “Brazilians do everything over WhatsApp, since it’s “free.” From music classes to e-commerce and medical appointments, the app became central to the functioning of business and family life, especially for the most vulnerable communities. Brazilian citizens are some of the highest social media users in the world, second only to the Philippines. Citizens, however, are often limited by the content they receive via WhatsApp, and therefore, they lose the context and the opportunity to check for different versions online or expand their knowledge. The fact that everything going through WhatsApp is free of internet charges makes it easy for people to spread audios or YouTube videos (that open inside WhatsApp). Due to this design, WhatsApp can be considered a conduit to disinformation in many formats, but is especially harmful for audio and videos. Together, YouTube and WhatsApp formed a pipeline of misinformation, spreading conspiracy theories, campaign material, and political propaganda throughout Brazil.” Casaes, D. and Córdova, Y. (2019), “Weaponized Information in Brazil: Digitizing Hate,” Policy Brief No.63 Toda, https://toda.org/assets/files/resources/policy-briefs/t-pb-63_casaes-and-cordova_weaponised-information-in-brazil.pdf, access January, 2019.
- 100 Evangelista, R. & Bruno, F. (2019), “WhatsApp and political instability in Brazil: targeted messages and political radicalization,” *Internet Policy Review*, 8(4), access October, 2018. In the words of Rafael Evangelista and Fernanda Bruno: Although WhatsApp does not provide a service for micro-targeting audiences, there is evidence that third party companies, dedicated to non-political marketing campaigns, provided that kind of service in the context of elections, sometimes using illegal databases. (...) The case of use of WhatsApp in Brazilian elections shows how a surveillant structure was built on top of a group message service that allegedly uses cryptography to protect its user’s privacy.”
- 101 See https://www.theguardian.com/world/2019/oct/30/whatsapp-fake-news-brazil-election-favoured-jair-bolsonaro-analysis-suggests?CMP=share_btn_fb, access January, 2020.
- 102 “*Internet Policy Review*, 8(4).” See also Cesarino, L. (2019), “On Digital Populism in Brazil,” *PoLAR: Political and Legal Anthropology Review*, <https://polarjournal.org/2019/04/15/on-jair-bolsonaros-digital-populism/>, access January, 2020.
- 103 Recently, The European Commission “has recognized the exposure of citizens to online disinformation and micro-targeting of voters based on the unlawful processing of personal data as one of the major challenges for European democracies. In a response, the EC has put in place several measures to formulate a European approach. (...) The Commission’s guidance on the application of the GDPR in the electoral context (EC, 2018d) underlines that it “applies to all actors active in the electoral context,” including European and national political parties, European and national political foundations, platforms, data analytics companies, and public authorities responsible for the electoral process. Any data processing should comply with the GDPR principles, such as fairness and transparency, and for specified purposes only.” See Nenadić, I. (2019), “Unpacking the European approach to tackling challenges of disinformation and political manipulation,” *Internet Policy Review*, 8(4). See also: European Commission (2018), “Free and fair European elections – Factsheet, State of the Union,” https://ec.europa.eu/commission/presscorner/detail/en/IP_18_5681. See also: European Commission (2018), “Commission guidance on the application of Union data protection law in the electoral context: A contribution from the European Commission to the Leaders’ meeting in Salzburg,” https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-data-protection-law-electoral-guidance-638_en.pdf, access January, 2019.
- 104 Westby, J. (2019), “The Great Hack: Cambridge Analytica is just the tip of the iceberg,” *Amnesty Tech*, <https://www.amnesty.org/en/latest/news/2019/07/the-great-hack-facebook-cambridge-analytica/>, access January, 2019.
- 105 Westby, J. (2019), “The Great Hack: Cambridge Analytica is just the tip of the iceberg,” *Amnesty Tech*, <https://www.amnesty.org/en/latest/news/2019/07/the-great-hack-facebook-cambridge-analytica/>, access January, 2019.
- 106 See <https://privacyinternational.org/learning-topics/data-and-elections>, access January, 2019.
- 107 Risso, Linda (2017), “Harvesting Your Soul? Cambridge Analytica and Brexit,” *Akademie der Wissenschaften und der Literatur*, http://www.adwmainz.de/fileadmin/user_upload/Brexit-Symposium_Online-Version.pdf#page=75, access December, 2019.
- 108 “Policymakers should be required to stay abreast of fast-moving innovations in the technology and marketing industries, identifying the uses and abuses of digital applications for political purposes, such as the way that WhatsApp was deployed during recent elections in Brazil for computational propaganda.” In: Chester, J. & Montgomery, K. C. (2019), “The digital commercialization of US politics – 2020 and beyond,” *Internet Policy Review*, 8(4), access January, 2019.

- 109 "It is fair to say that regulators have been generally slow to appreciate the complex variety of risks posed by data-driven campaigning. Until relatively recently, for example, most DPAs had not taken an active interest in the processing of personal data within the electoral process in their respective countries. There was some earlier guidance and rulings on political campaigning in the UK (ICO, 2014) and a series of rulings in France (CNIL, 2012). In most EU countries, and others in which political parties are regulated by data protection law, rulings relate to quite narrow issues, prompted by individual complaints about the actions of particular parties and candidates during specific electoral contests. Similarly, elections regulators have typically been more concerned with the transparent and efficient running of elections, together with questions about electoral financing, than they have with concerns about the processing of personal data on the electorate." See Bennett, C. J. & Lyon, D. (2019), "Data-driven elections: implications and challenges for democratic societies," *Internet Policy Review*, 8(4).
- 110 European Commission, "Commission proposes high level of privacy rules for all electronic communications and updates data protection rules for EU institutions," http://europa.eu/rapid/press-release_IP-17-16_en.htm, access January, 2019.
- 111 Samuel C. Woolley and Philip N. Howard (2017), *Computational Propaganda Worldwide*, University of Oxford, <http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf>, access October, 2019.
- 112 Lane, Julia, et al. (eds.) (2014), "Privacy, Big Data, and the Public Good: Frameworks for Engagement," Cambridge.
- 113 European Commission proposes high level of privacy rules for all electronic communications and updates data protection rules for EU institutions. 2017. See http://europa.eu/rapid/press-release_IP-17-16_en.htm, access January, 2019.



2. Compliance with data protection regulations on elections

A comparative analysis between the EU and Brazil (GDPR vs. LGPD)

In order to analyze the application of personal data regulations to electoral processes in Brazil and the EU, this section explores the most relevant similarities and differences between the European General Data Protection Regulation (GDPR) and the Brazilian General Data Protection Law (“Lei Geral de Proteção de Dados Pessoais” – LGPD). The following considerations explore how these intricate systems determine the limits of candidates’ and parties’ data processing capabilities in each jurisdiction, while also presenting relevant normative instruments related specifically to electoral processes.

The Brazilian general data protection law was widely based on the EU’s general data protection regulation. Thus, there are many similarities between the two. Firstly, there are overlaps between the general principles in both laws. The GDPR lists, in Article 5, six principles relating to the processing of personal data. The LGPD lists, in Article 6, ten principles. Both provide the core values of specific and clear purposes, transparency, quality (accuracy) of data, safety, accountability, lawfulness, and fairness. The head of the Brazilian article on principles reads:

Art. 6th Personal data processing activities shall observe good faith and the following principles...

The “good faith” (boa-fé) mentioned could be interpreted as being analogous to the fairness principle of the GDPR. “Boa-fé” is a general civil law principle in Brazil. Its explicit mention at the caput of the article relating to the principles of personal data processing strengthens its role as an interpretative axis when applying the law. In practice, this means taking into consideration the context of data collection in order to determine the reasonably expected and fair uses of the data. This is what jurists describe as “contextual privacy”¹⁴:

In summary, the contextual privacy theory consists, therefore, in considering that the data subject has legitimate expectations (of privacy) about how their data shall appropriately flow. Data traffic, thus, does not occur in a vacuum, but under a set of circumstances that determine its integrity.

Besides many similarities, as the aforementioned fairness principle, there are, however, instances where the two regulations differ. One such case is the definition of joint controllers. Joint controllers are described in Article 26 of the GDPR, which reads:

Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.

It is important to note that the same dataset may have many distinct controllers, when they use it for distinct purposes, or joint controllers, when they jointly decide on the purposes of processing¹⁵. The Brazilian law, on the other hand, does not have

2. Compliance with data protection regulations on elections

an explicit category of joint controllers. Controllership is still determined based on the capacity to decide on the purposes of processing, but there is no mention of joint controllership. The law does, however, hint at it in one instance.

In Article 42, II, the LGPD states that the controllers directly involved in a processing activity shall be jointly responsible for any violations. This article suggests joint controllership by stating that distinct actors may be bundled under the effects of the law, an interpretation that should be considered when determining the governance structure of political campaigning efforts. In such instances it is especially true due to another piece of law on the liability of candidates and political parties. Brazilian law n. 9.504/1997 states, in Article 6th, § 5th:

§ 5th Candidates and their parties are jointly and severally liable for fines resulting from electoral propaganda...

Thus, the LGPD is fully applicable to the personal data processing carried out by both parties and candidates, as well as their campaign structures. In Brazilian law, this is further stressed by political parties' characterization as private associations, that is, entities falling under the same general legal regime as private companies and non-governmental organizations.

Controllership is a crucial issue in both regulations, since the controller is responsible for the implementation of a broad set of requirements and is ultimately liable for any violations. Determining the controller of personal data can be a challenge in practice, which is, finding the person(s) with the ability to substantially decide the purposes and means of processing. In the context of political campaigns, this can prove a complex assessment:

The role as data controller or data processor has to be assessed in each individual case. In the electoral context, a number of actors can be data controllers: political parties, individual candidates and foundations are, in most instances, data controllers; platforms and data analytics companies can be (joint) controllers or processors for a given processing depending on the degree of control they have over the processing concerned; national electoral authorities are controllers for the electoral registers¹¹⁶.

Besides controllers, political campaigns must also pay attention to two more entities involved in the personal data processing relationships. Data processing is conducted by a "processor" (GDPR; called an "operator" in the LGPD), which executes the will and strategy of the controller. Whereas the controller has substantial decision power, the processor merely implements the planned processing activities. The other one is the Data Protection Officer (DPO, in the GDPR, and "Encarregado" in the Brazilian law), who serves as a communication channel between the data subject, the Data Protection Authority, and the company or organization.

The roles of the processor and the DPO are very different. The processor is involved in the processing activities and has the technical background necessary to implement the decisions of the controller, acting under their orders. The DPO, on the other hand, has been described as "the manifestation of the supervisory authority in an organization¹¹⁷." This role should ideally be independent from the controller and processor in

order to conduct a comprehensive assessment of the data processing activities and inform the authority and data subjects of any issues when necessary¹¹⁸.

Although similar in concept, the DPO and the “Encarregado” are designed slightly differently in the GDPR and LGPD. One main distinction is that appointing an “Encarregado” is generally mandatory and its waiver requires further specification by the Brazilian Data Protection Authority (Art. 41, § 3, of the LGPD). The GDPR, on the other hand, lists the cases when the DPO is necessary, although it is considered good practice to appoint one¹¹⁹.

Brazilian law has, to a limited extent, dealt with personal data in electoral campaigns before the LGPD. One example relates to the sharing of data with third parties. Under Article 7th, I and § 5th, of the LGPD, if data were collected and processed based on consent and needed to be communicated to another controller, this would require a new act of specific consent by the data subject. If based on any of the other legal basis, duties of transparency and accountability, and all rights of the subject and principles of law, would still be applicable, but no previous communication to the subject would be required. This would mean carefully registering the transfer and its purposes and, depending on the case, but preferably in a Data Protection Impact Assessment (DPIA)¹²⁰ report. In case legitimate interest is the lawful base for processing, it is recommended to do a Legitimate Interest Assessment (LIA)¹²¹.

However, previous to the LGPD there already was Article 57-E of law n. 9.504/97 (Political Parties Regulation), enacting a prohibition on the sharing or buying of contact information lists for political propaganda purposes. The article states:

Art. 57-E. The persons listed in Art. 24 are forbidden to utilize, donate or cede electronic registers of their clients, in favor of candidates, parties or party groupings.

§ 1st It is forbidden to sell electronic address registers.

With this general prohibition on contact information sharing, the scenario is further complicated. “Electronic registers” (“cadastro eletrônico”) may not be communicated by a list of entities, including foreign entities or governments; public administration offices; public service contractors; trade unions; nonprofits that receive foreign funding; non-governmental organizations that receive public funding; among others. Private companies in general were added to this list following a decision by the Supreme Court on case ADI 4650, dealing with private donations to political campaigns¹²². On top of that, any commercialization of electronic address registers is prohibited.

The GDPR doesn’t explicitly touch on data commercialization. However, an interpretation according to the regulation’s rules and principles orders that a controller processes personal data according to the initially intended purposes¹²³. That means transfer of data – be it through a donation or sale – to third parties should meet the original purpose of data collection.

In practice, these considerations mean political campaigns should be careful about the source of their data and who has access to it. If the initial collection of data was made directly by the campaign, through online or physical subscription, all future uses of

2. Compliance with data protection regulations on elections

the information – including e-mail marketing and profiling – should be disclosed to the data subject. If the initial collection of data was not related to political campaigning, e. g., if a candidate has contact information on his constituents in order to aid them with specific issues in the regular exercise of his political attributions, one should ask if any further uses would be reasonably expected by the data subject¹²⁴. This goes for both the European and Brazilian contexts. In Brazil, on top of that, political campaigns should not accept donations of or buy contact lists, as that is explicitly forbidden by electoral law.

The previously described case of political messages spread via WhatsApp during Brazilian elections is a good example of a practice that would go against these duties. Specialized companies were then hired to send out such messages on a large scale to lists of numbers – under uncertain conditions¹²⁵. One could argue that the people in those lists did not have a reasonable expectation of receiving electoral propaganda or political news via WhatsApp, and the campaigners would have a hard time providing evidence of either specific consent or any other legal basis for such activities.

Similar to this issue is the collection and treatment of publicly available data. Such large-scale collection of data can be used for profiling¹²⁶ activities, whereby crossing distinct data sources and points allows one to make inferences and build a detailed profile of a subject. All the data thus collected and inferred is subject to data protection regulations, as it is “relating to an identified or identifiable natural person” (Art. 4, GDPR), or “information related to an identified or identifiable natural person” (Art. 5th, LGPD). This was the foundation of the abovementioned Cambridge Analytica case, whereby using data analytics techniques the company was able to categorize voters into distinct groups, even those who did not explicitly give consent to their data being collected¹²⁷. Based on what could be perceived as “publicly available” information – collected through users’ profiles and their friends’ profiles – CA effectively distorted the democratic process through psychometrics and big data.

Mentions of “publicly available” data, in the Brazilian LGPD, show up in three instances: Paragraphs 3rd, 4th and 7th of Article 7th. The first describes the processing of “publicly available personal data,” stating that it should observe the original purpose and public interest which based its publication, as well as good-faith. The second instance deals with “data manifestly made public by the subject,” creating an exception to consent in this case. The third, a late change to the law, allows processing of such data for new purposes. There is an apparent conflict between paragraphs 3 and 7, since the former limits further processing to the original context and the latter allows processing for new purposes. This is probably an issue that the new National Data Protection Authority (Autoridade Nacional de Proteção de Dados, ANPD) will have to deal with.

On this point, the GDPR is vastly more precise than the LGPD. Article 14 of the GDPR refers to “information to be provided where personal data have not been obtained from the data subject,” for instance, from publicly available data. The article contains a series of specifications of the duties of the controller regarding the processing of data. These are duties of information that include: the intended uses of the data, the period of processing, identity of controller, categories of data collected, purposes of processing, recipients and sources of the data, rights of the subject of rectification and of lodging a complaint with a supervisory authority, among others.

Based either on the LGPD or the GDPR, the possibilities of processing based on “publicly available personal data” must be carefully addressed by the authorities, taking into account what happened in specific situations, such as the massive distribution of WhatsApp messages in Brazil or the CA case. Even though there can be exemptions for consent concerning publicly available personal data, in many cases processing can be considered illegal by not taking fundamental compliance steps, such as informing the data subject about the processing and guaranteeing basic data protection principles and rights.

Due to the full applicability of personal data protection regulations, it is important that both the parties and candidates take all precautions in order to guarantee observance of all principles and rights. This usually begins with a full mapping of data flows in the campaign structure, a job closely related to a DPO’s responsibilities. Especially where sensitive data are being processed, which is commonly the case in political campaigns. Since the data they deal with usually includes political opinions of data subjects, the DPO’s role shall prove even more crucial. Different campaigns have different needs and formats, especially in wide and diverse contexts as the Brazilian and European political scenarios. A point-by-point account of all instances where data is collected, communicated, stored or processed in any way; of who has access to which kinds of data; of what is the legal basis for data processing, be it regular or sensitive; and the length and purpose of processing activities, is an invaluable first step.

One substantial difference between the two regulations is their treatment of the Data Protection Impact Assessment (DPIA). DPIAs are referred to in Article 35 of the GDPR and Articles 10, 32, and 38, among others, of the LGPD. The former establishes an obligation to conduct a DPIA whenever there is “high risk to the rights and freedoms of natural persons.” This assumes that at least a preliminary risk assessment for all processing activities should be conducted, in order to determine high risk and, consequently, the obligation to conduct a DPIA¹²⁸. The article is extensive and establishes not only duties for the controller, but also the involvement of the Data Protection Officer and duties of the Data Protection Authority, which is responsible for determining specific cases when a DPIA is obligatory.

The Brazilian law, on the other hand, deals with the subject of impact assessments more briefly, simply mentioning that the Brazilian Data Protection Authority (ANPD) may request them from controllers and determine their required content. Regarding this point, Article 38 of the LGPD states:

Art. 38. The national authority may order the controller to present a personal data protection impact assessment report, including of sensitive data, regarding their data processing operations, according to the specific regulation, observing industrial secrecy.

Sole paragraph. The report mentioned in this article’s caput shall contain, at least, a description of the types of data collected, the data collection and information security methods applied, and the controller’s analysis on adopted measures, safeguards and mitigating mechanisms.

Whereas Article 35, 7, of the GDPR thus states:

The assessment shall contain at least:

- a) *a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;*
- b) *an assessment of the necessity and proportionality of the processing operations in relation to the purposes;*
- c) *an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and*
- d) *the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.*

As with many topics, the Brazilian law chose to leave the specifics of the DPIA regulation to the ANPD. This will involve, for example, deciding which agents will be obligated to conduct DPIAs and in what circumstances. This is reinforced by at least two items of the law, namely Article 55-J, XIII and XVIII. The former states that the National Authority is competent to elaborate regulations and determine procedures for the DPIAs in cases where there is a high risk to the principles and rights guaranteed in the law. The latter states that it falls under the authority's purview to set special and simplified procedures for small companies and startups.

One further important distinction between the European and the Brazilian regulations is related to the automated processing of data. In the GDPR, the data subject has the right not to be included in automated decision-making processes, including profiling. This right meets three exceptions, namely:

Art. 22. Paragraph 2: 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 authorized 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.*

However, even if any of the exceptions apply, the European regulation guarantees the right of the subject to a human intervention in the automated process, in order to "express his or her point of view and to contest the decision" (Art. 22, 3). The Brazilian LGPD would have included a similar provision, had it been approved in its original form. The law was modified, though, by a Presidential Decree and, in its current form, Article 20 guarantees only the right to "revision" of automated decisions. That is, this revision does not need to be made by a human agent.

A final note is important on a specific recital regarding the processing of personal data on political opinions by parties during electoral activities. This processing, which, as explained above, would fall under the protections and restrictions set by the regula-

tions, is interpreted by recital 56 of the GDPR²⁹, which allows a looser processing based on public interest. Nevertheless, this possibility shall be carefully addressed, in order to keep the processing of political opinions by political parties in the spirit of the law.

Political opinions are classified by Article 9 of the GDPR as a special category of personal data, deserving stronger protection. Their processing is expressly prohibited (Art. 9, 1) and allowed only in exceptional cases (Art. 9, 2). The Brazilian law has no equivalent to recitals, and no express reference to the processing of political opinions except for their categorization as sensitive personal data, the equivalent to special category data in the GDPR. This apparent contradiction will be explored in the next section, where we discuss implementation in order to guarantee an effective democratic process in elections with regard to personal data protection.

Before we do that, nevertheless, it is important to highlight that, when it comes to comparing the quality of the European regulation versus the Brazilian regulation, there is no clear-cut answer. The Brazilian regulation is generally more flexible than the GDPR and this flexibility shows when we touch upon the number of legal bases for processing activities, the notification system after a breach has occurred, the amount of the administrative fines, among others. This may be perceived as positive factor on the one hand, because it gives the industry more room to adapt to the rules. On the other hand, however, this level of flexibility may give rise to ineffectiveness of the law, since the parameters set forth for controllers are too subjective and the provisions are not rigid enough to establish clear limits. Additionally, it puts even more responsibility on the data protection authorities' shoulders. In this matter, in Brazil, unlike the Data Protection Authorities (DPAs) in the EU, the National Authority is neither independent nor autonomous, as it is subordinate to the Presidency of the Republic. Also, its structure and body are yet being designed and formed. Considering the importance of the DPA in guaranteeing the effectiveness and providing specific regulation in complement of the law, all these elements bring uncertainty concerning the fulfillment and efficacy of the data protection scenario in Brazil.

Despite being similar to the LGDP, the GDPR is pointedly more straightforward and objective regarding the regulation of data protection. This is, again, a reason for both praise and criticism. On the one hand, rigidity creates an environment of legal certainty, guided through high parameters of protection of fundamental rights. That is, since there's a more controlled space for discretionary choices from the Supervisory Authorities, it is easier to have a harmonized application of the law throughout the European Union. On the other hand, by seeking to draw such parameters, the regulation may contain unfeasible provisions, such as the one dictated in Art. 33³⁰, that may take away some of its credibility by being too much of a burden and generating unnecessary costs to controllers.

Therefore, in light of the similarities and differences in approach of both regulations – that might inspire positive and negative comments – the question shall not be which regulation contains better provisions, since this can be subjective, but how to guarantee compliance and accountability in both scenarios. With that in mind, the next chapter is devoted to a practical analysis and indication of what steps should be taken for that purpose.

2. Compliance with data protection regulations on elections

-
- 114 BIONI, Bruno (2019), "Proteção de dados pessoais: A função e os limites do consentimento," *Forense*, p. 319.
- 115 ICO (2019), "Guidance on political campaigning: Draft framework code for consultation," <https://ico.org.uk/media/about-the-ico/consultations/2615563/guidance-on-political-campaigning-draft-framework-code-for-consultation.pdf>. Access December, 2019.
- 116 European Commission (2018), "Commission guidance on the application of Union data protection law in the electoral context: A contribution from the European Commission to the Leaders' meeting in Salzburg," https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-data-protection-law-electoral-guidance-638_en.pdf, access January, 2019.
- 117 HEWARD-MILLS, D (2019), "The DPO must be independent, but how?," <https://iapp.org/news/a/the-dpo-must-be-independent-but-how/>, access November, 2019.
- 118 More practical steps to the DPO's role will be described in the following section.
- 119 CNIL (2019), "Devenir délégué à la protection des données," <https://www.cnil.fr/fr/devenir-delegue-la-protection-des-donnees>, access November, 2019.
- 120 EDPB (2019), "Guidelines on Data Protection Impact Assessment (DPIA)," https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236, access November, 2019.
- 121 ICO (2019), "How do we apply legitimate interests in practice?," <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/>. See also <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/>, access November, 2019.
- 122 Britto, Cruz et al. (2019), "Internet e eleições no Brasil: Diagnósticos e recomendações," *InternetLab*, pp. 32–33.
- 123 Art. 5, l, b, of the GDPR.
- 124 ICO (2019), "Guidance on political campaigning: Draft framework code for consultation," <https://ico.org.uk/media/about-the-ico/consultations/2615563/guidance-on-political-campaigning-draft-framework-code-for-consultation.pdf>. Access December, 2019.
- 125 See "WhatsApp Admits Illegal Mass Messaging Used in Brazil's 2018 Elections," *The Rio Times*, <https://riotimesonline.com/brazil-news/brazil/whatsapp-admits-to-illegal-mass>, access November, 2019.
- 126 GDPR recital n. 71 defines profiling as "any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyze or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her."
- 127 REVELL, T. (2018), "How Facebook let a friend pass my data to Cambridge Analytica," <https://www.newscientist.com/article/2166435-how-facebook-let-a-friend-pass-my-data-to-cambridge-analytica/>, access November, 2019.
- 128 ICO (2019), "Guidance on political campaigning: Draft framework code for consultation," <https://ico.org.uk/media/about-the-ico/consultations/2615563/guidance-on-political-campaigning-draft-framework-code-for-consultation.pdf>, access December, 2019.
- 129 Recital 56: "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."
- 130 Art. 33: "In the case of a personal data breach, the controller shall without undue delay and, where feasible, no later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay."



3. Enhancing effectiveness and bridging the gaps

The importance of maintaining data hygiene and compliance in political campaigning is manifold. From the perspective of democratic institutions, as previously discussed, it is a condition for healthy electoral processes. In a time of ubiquitous connection, of instant and indiscriminate data sharing, ideas and beliefs can be shaped by online filters and the public sphere gets necessarily intertwined with new Information and Communication Technologies. Their failed functioning, be it by error or in consequence of a structurally flawed system, may put at risk people's ability to build consensus and find a middle-ground in a peaceful and balanced manner, as recently demonstrated by the meddling in electoral processes in various parts of the world.¹³¹

From the perspective of data controllers, and, in this specific case of political parties and politicians, following the rules precisely is not only a legal obligation, but shall prove to be a basic requirement in presenting oneself to society as an ethical subject deserving of attention, trust, and vote. This is even more true taking into account the recent cases where data processing techniques were applied to political campaigning, such as CA and WhatsApp's use in Brazilian elections, bringing the issue to the fore and heightening voters' attention to it. Not respecting people's privacy, right to data protection and informational self-determination should increasingly prove inexcusable in marketing and public image, especially as more and more people become aware of these issues.

Candidates and political parties should be careful with how they process data for their campaigns during electoral processes, looking for the best current practices, not only in their own interest, but also in the interest of data subjects and society as a whole.¹³² Due to the very nature of these processes, many of the personal data they will be dealing with, either directly collected or inferred through analytics and profiling techniques, will be sensitive – a special category of data that deserve special protection. Not only is it important to guarantee observance of rights and principles in the interest of the data subjects, observing the rule of law, but it is also crucial, especially in terms of political campaigning, where public image is a central component, to be able to demonstrate that privacy and data protection are being dealt with in the most ethical and lawful manner.

The increase in data breaches has reached a high point in 2019, with 5,183 data breaches and 7.9 billion records exposed in the first nine months of the year. This represents a 33.3% increase in comparison to 2018¹³³. If this is any indication of future trends, data security should be one of the main concerns in any personal data processing endeavor. Penalties for data breaches may reach tens of millions of dollars in fines, as well as asset suspension or exclusion. In order to prevent such losses, the controller must adopt the latest standards in security. For example, properly training all people involved in processing, as well as reducing the number of people who have access to personal data, are important steps. Multifactor authentication is also a basic requirement, as it has the potential to drastically reduce system vulnerabilities¹³⁴. Reducing the number of devices where the data are stored, and the transmission of data between devices, are other steps toward greater security which controllers can and should take, preferably through a Chief Information Security Officer (CISO), who should not be the same person as the DPO¹³⁵.

3. Enhancing effectiveness and bridging the gaps

The DPO has a leading role in making sure this whole system is functioning. It is the DPO's responsibility to track compliance with the data protection legislation. This means collecting information on wherever data is processed and making sure it follows all legal requirements; providing counsel to the controller based on their observations regarding how to improve compliance; training employees on security measures and good practices; and making a link between the organization, the authority, and data subjects. This last attribution means the DPO should be independent, which may prove difficult when they are hired internally.

Best practice is that the DPO should not answer to the controller, and instead should report directly to the highest level of decision-making in the management structure. In order to guarantee their independence, they should also have the necessary resources – staff, equipment, and finances – to perform their duties¹³⁶. Finally, they should not be put in a position of conflict of interest, such as working or having worked in data processing activities – in IT or HR departments, for example – which would force them to supervise themselves¹³⁷. These issues could be avoided by hiring an external DPO. Even then, it is important that the DPO has the necessary access and resources, as well as the technical expertise required.

All these are building blocks in a data processing and security strategy that starts with a straightforward assessment of the flow of data along an operation and the current risks involved. In order to ensure compliance with the GDPR and, consequently, with the LGPD – since both have very similar levels of data protection – political parties and candidates should be up-to-date on the best management practices and tools applied to data flows.

A controller should be able to have a birds-eye view of the personal data flows in their campaign, preferably through a compliance dashboard that should be used by all involved controllers and processors. This centralized data management system should also provide contact details and identify the Data Protection Officer in the campaign's structure, a complete mapping and governance of data being processed and transferred and their associated lawful purpose.

One must also remember their information duties according to the GDPR and LGPD, including informing: (i) identity and contact details of controller and DPO; (ii) identification or categories of recipients of the data; (iii) the purposes of processing, as well as the legal basis for doing so; (iv) the period for which processing will take place; (v) the rights of the data subject, especially of rectification and withdrawal of consent, when applicable; among others¹³⁸. Additionally, controllers should be able to process the Subject Access Requests in a timely manner. These requests are instances where data subjects may require access, rectification and, in some cases, erasure of their data.

The controller should also adopt means of maintaining “digital consent breadcrumbs,” that is, a register of the timeline of consent, or distinct consents, a subject has given or withdrawn for processing. Finally, permission and access control should be granular, meaning only the indispensable agents inside the campaign structure should have access to respective groups of data. All these aspects of the relationship between the processor and the data subject should be translated into easy-to-use interfaces, such as apps and forms, so that the subject comprehensively understands their rights and the controller is able to demonstrate compliance¹³⁹.

All this may sound like a lot of ground to cover, and it is. Fortunately, alongside capable professionals that might aid companies in building compliance, there are currently self-assessment tools regarding GDPR compliance, which should easily translate to LGPD requirements. The UK's Information Commissioner's Office (ICO), for example, has numerous specific resources, including compliance checklists for controllers, processors, information security, direct marketing, small and medium enterprises, and more¹⁴⁰. Another invaluable tool is their Privacy Notice Code, which covers in detail how one of the most frequent tools of communication between controller and data subject, the Privacy Notices found on websites and apps, should be structured to ensure compliance¹⁴¹.

A rundown of these tools demonstrates that the crucial point of an effective personal data compliance program is to know the processes involved in an operation: the what, the where, the when and how of personal data collection and processing. In political campaigning, this should be no different: a hands-on approach is necessary, involving marketing specialists, designers, legal experts, programmers, and volunteers into thinking how to best shield data subjects from any kind of violation to their right to privacy and data protection. As demonstrated in this study, highlighting specific legal guidelines and concrete situations, data protection regulations are fully applicable to political campaigns and have the ability to assist in reducing the instrumental use of personal data, while also avoiding the impact of misinformation and computational propaganda used for the purpose of political manipulation.

More pragmatically, political campaigns should take heed of at least the following recommendations, based on the principles and main guidance of general data protection regulations, always through the perspective of lawfulness, fairness, transparency, and accountability:¹⁴²

Identify the relevant actors: Which persons are Controllers and Processors and who is the DPO, if there is one.

- Art. 5°, LGPD; Art. 4, GDPR.
- **Example:** In a certain political campaign, the candidate has hired a marketing company to manage his public image. All decisions regarding the collection and processing of data are made by the marketing director. The director can be characterized as a data controller, since they are capable of deciding the purpose of processing. The candidate would also be a controller, since ultimately they are the decision-maker.

Identify how data is being collected and processed, i. e., what is the life cycle of data in the campaign's organizational flow.

- **Action:** Map all data collection and processing points; identify how much time it takes until a single point of data is eliminated; identify what devices/ services are used to store data; identify what third parties have access to the data.

Identify what data is collected and processed, and under what legal basis. Designate sensitive data¹⁴³ and pay special attention to their legal bases.

- Art. 5°, I, II; Art. 7°, Art. 11, LGPD; Art. 4, Art. 9, GDPR.
- **Action:** If there are data points where a legal basis cannot be specified, they should be eliminated, as they are a liability – this is basic “data hygiene.”

3. Enhancing effectiveness and bridging the gaps

Keep in mind that data minimization¹⁴⁴ is a good general rule (and a basic principle). If there is no need to collect a certain aspect of personal data, don't do it; if the purpose for collection has been achieved, delete the data.

- › Art. 15, Art. 16, LGDP; Art. 5, Art. 25, GDPR.
- › **Action:** If there is no need to collect a certain aspect of personal data, don't do it; if the purpose for collection has been achieved, delete the data.
- › **Example:** Candidate collects data from subjects in order to send digital copy of government plan. If consent is given strictly for distribution of said material: 1. candidate does not need to collect more than subject's name and e-mail address, so they should stick to these; 2. candidate should eliminate the data after sending the material, unless reasonable to expect otherwise, based on other legal bases, or via a new specific consent.

Have all legal bases documentation archived.

- › **Example:** Candidate collected and processed data in order to maintain a record of individual campaign donations, as per the Brazilian electoral law. The candidate should maintain a record of such operations with reference to the relevant laws and legal bases, in case of an audit.

Renew existing consent in compliance with the most up-to-date data protection regulations.

- › **Action:** In case of a new privacy policy text, or in regard to pre-GDPR/LGPD data subjects, obtain new consent or inform subjects of new policy and legal basis.
- › **Example:** Candidate already has a contact list collected through public events and webpage subscription form, prior to the GDPR/LGPD. They should send all recipients a request to confirm their willingness to receive political communications. Something along the lines of "We are updating our privacy and data protection practices according to the most recent data regulations. If you wish to continue receiving our content, please click the button below/renew your subscription at/[add some form of confirmation]."

Provide information: Remember the various information duties a controller has with respect to the data subject. The data subject should be able to discern what personal data is being collected, for what purpose, period of time, who is going to have access to it, what the process to request access to that data is, correct it, request its deletion, or transfer to another controller etc.

- › Art. 9^o, Art. 18, LGPD; Art. 13, Art. 14, GDPR.
- › **Action:** If consent is the legal basis, all relevant information should be provided in the act of consent. If there are other legal bases, the data subject should have easy access to such information via request or via public access [e. g., on a website]. If data is collected through other means than directly from the subject [e. g., publicly accessible data], the controller has a series of information duties [see relevant GDPR articles].

Maintain a record of processing activities, especially if legitimate interest is the legal basis (Art. 30, GDPR; Art. 37, LGDP). When applicable, have a DPIA¹⁴⁵ or LIA¹⁴⁶ at hand.

- › Art. 37, LGPD; Art. 30, GDPR.
- › **Action:** Keep a registry containing at least: 1. the purpose of processing; 2. description of data categories and subjects; 3. external data flows; 4. secu-

riety measures adopted; 5. identification and contact information of the controller; 6. deadlines for elimination of each data category¹⁴⁷.

- › **Example:** A small campaign on a local election has adopted an organizational flow in order to maintain a record of data processing activities. All information collected on data subjects is recorded on a spreadsheet with categories according to the source of the data. Subscription form data, for example, are categorized as consent-based, containing name and e-mail address, sent to a third-part newsletter service, kept on a restricted cloud server protected with two-factor authentication, and kept indefinitely, as agreed upon by data subjects when they gave their consent.

Inform data subjects of who their DPO is if there is one, and give them an easy communication channel for Subject Access Requests.

- › Art. 18, LGDP; Art. 12, GDPR.
- › **Example:** A campaign has, on their website, a contact form which connects directly with the DPO. It also includes specific fields for Subject Access Requests, which are prioritized.

Make sure the language and design of your platforms are suited for data subjects' optimal understanding.

- › **Action:** Adopt adequate typography [size, color, contrast, type etc.], language, visual cues, illustration, and any other means to obtain optimal understanding, considering the reader's specific capacities.
- › **Example:** A campaign has hired a team of legal experts, marketers, and web designers who will work together on creating a privacy policy document that contains not only the required legal language, but also simplified, explanatory content that non-jurists are able to understand.

Inform users of your privacy policy and any subsequent updates to it.

- › **Action:** Inform individuals of the processing that will be made of their data, including transfers to third-parties, specifying these third-parties or at least their categories, and the period for which the data will be kept.
- › **Action:** Be as specific as possible, as general permissions are not recognized under either regulation.
- › **Example:** A campaign knows it will be using Google Analytics on their website. They also built the website using a drag-and-drop website builder like Wix or Squarespace. All these platforms collect user data, and this should be mentioned to the data subjects.

Manage consent: Whenever consent is the legal basis, make sure it is given under appropriate conditions. This requires a multidisciplinary approach, from Law to IT and Design¹⁴⁸, to ensure consent is freely given, specific, informed, and unambiguous.

- › **Action:** Explicitly request permission to collect cookies and other identifying information [except if there is another reasonable legal basis for collection]¹⁴⁹.
- › **Example:** The candidate has a subscription form for a political newsletter on his campaign website, and his website collects cookies. It has a pre-marked box indicating consent to receiving the newsletter. This is not considered valid consent, and the box should not be pre-marked. Also, it has a "consent assumed from use of this website" cookie notice. This is equally not consid-

3. Enhancing effectiveness and bridging the gaps

ered valid consent¹⁵⁰. Best practice would be an informative disclaimer which allows the user to choose which kinds of cookies he allows, and explaining those which are necessary for the site to work; and which requires the user's active consent, that is, an action that reflects their consent.

Pay special attention to children's data and special category (sensitive) data, which have stricter regulations.

- › Art. 11, Art. 14, LGPD; Art. 8, Art. 9, GDPR.
- › **Action:** Consent should be specific and highlighted, and given by parents or legal representatives, in the case of children [there are age specification in the GDPR, see the relevant article]. The legal bases for processing of sensitive data are more restrictive [check relevant articles].

Observe portability: Make sure the data is in a format that allows portability. This is a right of the data subject under both LGPD and GDPR. Data subjects should be able to obtain their data "in a structured, commonly used, and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided" (Art. 20, GDPR).

- › Art. 18, LGPD; Art. 20, GDPR.

Define processor obligations: Any processors a controller hires or appoints should have a Data Processing Agreement¹⁵¹ defining their responsibilities, security standards and other legal requirements¹⁵².

- › Art. 28, GDPR.
- › **Action:** Have a Data Processing Agreement in place determining responsibilities and security standards.

Check if your service providers are compliant and manage data in a secure manner, and if the data is stored in a server located in a country which complies with the most up-to-date data protection regulations.

- › **Action:** Check whether the data handled by these third-parties is stored in countries with equivalent status in terms of data protection. The EU has a system in place to classify countries' legislations as equivalent or not.
- › **Action:** Have your legal team carefully read the terms of use of any third-party service you use to manage personal data and analyze its compliance with GDPR/LGPD.
- › **Example:** The campaign decides to collect data using Google Analytics, deliver ads using Facebook's native ad platform, send e-mails through Mailchimp and manage internal flows using an Indian tech solution. They have to be sure each of these is compliant with data protection laws, since they will have access, even if in passing, to the personal data collected and processed. In the case of the Indian tech solution, if data are stored on a server in India, the campaign should confirm if the EU has recognized India's compliance with the GDPR (as of Dec./2019, the country was seeking the status, but had not yet obtained it).

Manage breaches: There should be a process in place to identify and notify the authority and data subjects of breaches.

- › Art. 48, LGPD; Art. 33, GDPR.

- › **Action:** Security breaches must be notified to the National Authority without undue delay (in up to 72 hours, according to the GDPR). Notification to the data subjects is mandatory only in the LGPD, and in GDPR it is necessary only if there is substantial risk to the subjects' rights and freedoms.
- › **Example:** The campaign has a security team directed at finding bugs and flaws in the design and functions of all data processing activities. It has also trained all relevant personnel on how to react to a breach, including what information to report to the authority through what channels, and how to communicate with the public.

Manage security risks:

- › Art. 46, LGPD; Art. 32, GDPR.
- › **Actions:** Minimize transfer of data between devices; Encrypt, pseudonymize, or anonymize data whenever possible; Have an internal security policy in place; Train team members on security issues; Have a mandatory password security policy and multifactor authentication¹⁵³; Conduct a risk assessment of the infrastructure used to collect, process, and store data.
- › Compliance as a process: Data protection doesn't end when a controller writes a DPIA or provides data subjects with information on their privacy policies. It should be constantly monitored, reviewed, updated, and adapted to the data processing contexts and most recent technological advancements.

These are all actionable points directed at data controllers and their processing operations. However, a full data protection paradigm can only be achieved through the involvement of many actors. This means careful regulation and guidance by National Authorities – especially in Brazil's case, where the law left much to the discretion of the Data Protection Authority, which will decide on security standards, cases where a DPIA is necessary, and special regimes for small and medium organizations, among other subjects. It also means an active effort by the Judiciary to adapt their understanding to the principles and spirit of the law, interpreting hard cases and giving life to those principles with the protection of data subjects in mind.

This effort of giving substance to the regulations has already begun in Europe, and in the matter of political campaigning it is interesting to observe the legal debates that have arisen right after the GDPR entered into force related to the regulation's recital n. 56. The recital specified interpretation regarding processing personal data for electoral activities. In its words¹⁵⁴:

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.

The subsequent legislative efforts in some Member States, taking into account the recital, brought to the fore a discussion on the limits of processing in such cases. Spain and Romania introduced in their national legislations personal data processing bases for electoral campaigns founded on the public interest interpretation. In Romania, this meant an exemption of consent in personal data processing for elec-

toral ends, allowing, for example, the Romanian Post Office to close a deal with the country's Social Democratic Party to deliver political campaign material to targeted populations using the Office's data on elderly pensioners¹⁵⁵.

Similarly, in Spain, a national law allowed political parties to collect personal data from publicly available sources, such as social networks, and use them for profiling voters. The provision modifies Spanish electoral law to add Article 58 bis, which reads¹⁵⁶:

Article 58 bis. Usage of technological tools and personal data in electoral activities.

- 1. The collection of personal data related to people's political opinions carried out by political parties in their electoral activities shall be covered by public interest only when adequate guarantees are in place.*
- 2. Political parties, coalitions, and electoral groupings shall be able to utilize personal data obtained through web pages and other public access sources for electoral activities during the electoral period.*
- 3. The sending of electoral propaganda through electronic means or messaging systems and contracting of electoral propaganda in social networks or equivalent platforms shall not be considered a commercial communication activity.*
- 4. The aforementioned publicity activities shall clearly identify their electoral nature.*
- 5. The recipient shall have a simple and free of charge means of exercising their right to contest.*

In practice, the terms of the Spanish law could be interpreted as more lax in protecting personal data – in this case, the special data category of political opinions, which is the specific subject of the recital. Recital 56 should be interpreted as a specification of Article 9 of the GDPR, which, in item (2)(g), deals with processing “necessary for reasons of substantial public interest.” Thus, both the terms of the recital and, especially, of the article should be heeded when implementing such provision in national law.

Recital 56 requires that the compilation of such political opinion data be required for “the operation of the democratic system in a Member State” and be covered by “appropriate safeguards.” Article 9(2)(g) is stricter, mentioning the need for “substantial” public interest, as well as processing proportionate to the aims pursued, covered by “the essence of the right to data protection” and providing for “suitable and specific measures to safeguard the fundamental rights and the interests of the data subject¹⁵⁷.”

The fault in the Spanish law, as recognized by the country's Supreme Court in a case brought before it in March 2019, was that no “suitable and specific measures” nor “substantial public interest” were established¹⁵⁸.

In practice, the law ran the risk of allowing indiscriminate processing of sensitive data, in direct violation of the GDPR, and exposing citizens to practices similar to those carried out in the Cambridge Analytica scandal. On this point, in view of such controversies regarding the use of sensitive personal data in electoral campaigns, the European Data Protection Board (EDPB) published, in March 2019,

“Statement 2/2019 on the use of personal data in the course of political campaigns¹⁵⁹.”
The statement brings five concrete recommendations and clarifications to Member States:

- I. *that personal data revealing political opinions is a special category of data, and so its processing is prohibited and only allowed in narrowly-interpreted exceptions;*
- II. *data which have been made public by subjects are still under the EU data protection law and should be treated in a manner that respects obligations concerning transparency, purpose specification, and lawfulness;*
- III. *even when lawful, processing is still subject to all other obligations under the law, and political parties should be ready to provide information necessary for accountability and transparency;*
- IV. *solely automated decision-making, including profiling, where the decision legally or similarly significantly affects the subject, is restricted – the EDPB interprets affecting a person's vote as “legally affecting” the subject; and*
- V. *regarding targeting, the subject has the right to know who is sending the targeted content and why, and what rights they have in the face of such activity.*

Through these recommendations, the EDPB gives legislators in Member States clear guidance on the interpretation of Article 9.2.g) and Recital 56 regarding electoral processes. This is crucial, as an incomplete application of the guarantees and requirements demanded by the regulation may produce situations which go directly against the spirit of the law, as seen in the cases previously commented. In this sense, it is interesting to contrast the Spanish and Romanian cases with the approaches adopted by Italy and France. In Italy, personal data made publicly available on the Internet cannot be used for political communications, except if originally made public for that purpose, as determined by the country's Data Protection Authority in 2014. In France, a 2016 update of the French National Data Protection Commission's (CNIL) 2012 recommendations on political communication requires specific consent for the lawful aggregation and profiling of voters' personal data¹⁶⁰.

The controller should always keep in mind that the data protection laws are centered around the data subject and their rights, creating an enabling system for business practices and innovations around data, but within the limits of privacy and data protection, which are guarantees deeply rooted in personality rights and human dignity. Therefore, common practices in a pre-data protection regulation scenario, such as buying lists from data brokers and indiscriminately profiling subjects, including for electoral ends¹⁶¹, should be avoided under this new paradigm. Moreover, as previously stated, the protection of personal data has a direct impact on the quality of electoral processes, since these data are a necessary input for psychometrics and other techniques which, when applied to political campaigning, have a real effect on electoral outcomes.

In Europe and in Brazil, authorities are becoming aware of this risk, as demonstrated by the EDPB's actions to harmonize national legislations and a proper interpretation of Recital 56; and in Brazil, where the Superior Electoral Court recently included in its latest draft regulation for the coming municipal elections terms directed at curbing the spreading of misinformation, especially via social media and digital applications.

The harmonization of general data protection regulations with electoral resolutions, as well as compliance in the processing of information, should be seen as a priority, with the power to ensure effective mechanisms against misuse of personal data in electoral periods, helping to promote a fair electoral environment.

-
- 131 From the perspective of data subjects, new data protection regulations seem obviously beneficial, as they are aimed at increasing the autonomy of data subjects. However, being autonomous carries the responsibility of being self-sovereign over one's own identity. It enriches liberty, while also requiring a fundamental change in how people see their relation with data controllers, the services and products they offer, and, ultimately, how they understand that data economy and society should be.
- 132 Although general data protection regulations are already applicable in many countries, still many political deciders do not have a clear understanding of what is allowed in terms of data processing and the overall implications and importance of this matter. Therefore, awareness and capacity building aiming not only for citizens but also for political deciders, is also an important and ongoing effort that shall be strengthened to guarantee the right comprehension and enforcement of the applicable regulations.
- 133 See Risk Based Security (2019), Data Breach QuickView Report: 2019 Q3 trends.
- 134 AMIGORENA, F. (2019), "The Myths of Multifactor Authentication. DARKReading," <https://www.darkreading.com/endpoint/authentication/the-myths-of-multifactor-authentication/a/d-id/1336262>.
- 135 GDPR Informer (2017), "Data Security 101: Access Controls & Planning," <https://gdprinformer.com/gdpr-articles/data-security-101-access-controls-planning>.
- 136 HEWARD-MILLS, D. (2019), "The DPO must be independent, but how?," <https://iapp.org/news/a/the-dpo-must-be-independent-but-how/>, access November, 2019.
- 137 See GDPR-Info, <https://gdpr-info.eu/issues/data-protection-officer/>, access November, 2019.
- 138 See Art. 13 of the GDPR and Art. 9 and 18 of the LGPD.
- 139 FINUCANE, B. (2018), "A Post-GDPR Checklist for Political Parties," CPO Magazine, <https://www.cpomagazine.com/data-protection/a-post-gdpr-checklist-for-political-parties/>, access November, 2019.
- 140 Find a list of checklists here: <<https://ico.org.uk/for-organisations/data-protection-self-assessment/>>.
- 141 Find the code here: <<https://www.pdpjournals.com/docs/88625.pdf>>.
- 142 This list is mainly based on the previously cited resources, namely ICO's checklists and Finucane's checklist for political parties. It also reflects the terms of either the GDPR or LGPD and the author's analysis of both legal documents. Where other sources were consulted, they should be indicated in a footnote.
- 143 The GDPR's "special category data" are called "sensitive data" (dados sensíveis) in LGPD.
- 144 ICO, (2019), "Principle (c): Data minimization," <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/>, access November, 2019.
- 145 The ICO has provided a DPIA template here: <https://gdpr.eu/wp-content/uploads/2019/03/dpia-template-v1.pdf>.
- 146 The ICO recommends conducting a Legitimate Interest Assessment whenever relying on legitimate interest for data processing. This contributes to accountability and transparency, and insures the company in case of an audit. The LIA encompasses the three key aspects of the legitimate interest basis, that is, purpose, necessity, and the balance between those interests and the subject's interests, rights or freedoms. For more on the LIA, and a template LIA, see <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/>, access January, 2020.
- 147 BIONI, Bruno (2019), "A obrigação de registro das atividades de tratamento de dados," GEN Jurídico, <http://genjuridico.com.br/2019/08/27/registro-tratamento-de-dados/>, access December, 2019.
- 148 ICO (2019), "Privacy notices, transparency, and control: Data protection: a code of practice on communicating privacy information to individuals," <https://www.pdpjournals.com/docs/88625.pdf>, access November, 2019.
- 149 USTARAN, Eduardo (2019), "Getting cookie consent right," Infolaw, <https://www.infolaw.co.uk/newsletter/2019/11/getting-cookie-consent-right/>, access December, 2019.
- 150 CJEU (2019), "Judgment of the Court (Grand Chamber) of 1 October 2019, Case C-673/17," <http://curia.europa.eu/juris/liste.jsf?language=en&num=C-673/17>, access December, 2019.
- 151 See "What is a GDPR data processing agreement?," <https://gdpr.eu/what-is-data-processing-agreement/>, access November, 2019.

- 152 Find a Data Processing Agreement template here: <https://gdpr.eu/wp-content/uploads/2019/01/Data-Processing-Agreement-Template.pdf>.
- 153 GDPR.EU. Compliance checklist: <https://gdpr.eu/checklist/>, access November, 2019.
- 154 Recital 56. Available at: <https://gdpr-info.eu/recitals/no-56/>.
- 155 See <https://www.hotnews.ro/stiri-politic-23066729-exclusiv-contractul-prin-care-posta-livreaza-pliantele-psd-sunt-vizati-toti-pensionarii-inclusiv-cei-care-primesc-pensia-cont-card-posta-obligat-trimita-psd-informatii-din-baza-date-pensionarii.htm>, access November, 2019.
- 156 «Artículo cincuenta y ocho bis. Utilización de medios tecnológicos y datos personales en las actividades electorales. 1. La recopilación de datos personales relativos a las opiniones políticas de las personas que lleven a cabo los partidos políticos en el marco de sus actividades electorales se encontrará amparada en el interés público únicamente cuando se ofrezcan garantías adecuadas. 2. Los partidos políticos, coaliciones y agrupaciones electorales podrán utilizar datos personales obtenidos en páginas web y otras fuentes de acceso público para la realización de actividades políticas durante el periodo electoral. 3. El envío de propaganda electoral por medios electrónicos o sistemas de mensajería y la contratación de propaganda electoral en redes sociales o medios equivalentes no tendrán la consideración de actividad o comunicación comercial. 4. Las actividades divulgativas anteriormente referidas identificarán de modo destacado su naturaleza electoral. 5. Se facilitará al destinatario un modo sencillo y gratuito de ejercicio del derecho de oposición.»
- 157 GONZÁLEZ, E. G. (2019), "The good, the bad and the ugly: Spanish electoral system act: A tale with a happy ending. Secuoya," <https://secuoyagroup.com/2019/06/the-good-the-bad-and-the-ugly-spanish-electoral-system-act-a-tale-with-a-happy-ending/>, access December, 2019.
- 158 "De lo anterior se concluye que la ley no ha identificado la finalidad de la injerencia para cuya realización se habilita a los partidos políticos, ni ha delimitado los presupuestos ni las condiciones de esa injerencia, ni ha establecido las garantías adecuadas que para la debida protección del derecho fundamental a la protección de datos personales reclama nuestra doctrina, por lo que se refiere a la recopilación de datos personales relativos a las opiniones políticas por los partidos políticos en el marco de sus actividades electorales. [...] La declaración de inconstitucionalidad y nulidad se basa, como se ha dicho en el fundamento jurídico anterior, en que la Ley Orgánica 3/2018 no ha fijado por sí misma, como le impone el Art. 53.1 CE, las garantías adecuadas por lo que respecta específicamente a la recopilación de datos personales relativos a las opiniones políticas por los partidos políticos en el marco de sus actividades electorales. Ello constituye una injerencia en el derecho fundamental a la protección de datos personales de gravedad similar a la que causaría una intromisión directa en su contenido nuclear." Sentencia. Recurso de Inconstitucionalidad núm. 1405-2019. Available at: https://www.tribunal-constitucional.es/NotasDePrensaDocumentos/NP_2019_076/2019-1405STC.pdf, access November, 2019.
- 159 See EDPB Statement 2/2019 on the use of personal data in the course of political campaigns. Available at: https://edpb.europa.eu/our-work-tools/our-documents/ostalo/statement-22019-use-personal-data-course-political-campaigns_pt. Access November, 2019.
- 160 See EDPS Opinion 3/2018: EDPS Opinion on online manipulation and personal data. Available at: https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf, access December, 2019.
- 161 See "Voter Privacy: What You Need to Know About Your Digital Trail During the 2016 Election," EFF, <https://www.eff.org/deeplinks/2016/02/voter-privacy-what-you-need-know-about-your-digital-trail-during-2016-election>, access November, 2019.

Final Considerations

The culture of hyperconnectivity in which we live, despite generating countless and unquestionable benefits to citizens, also brings significant challenges to democratic spheres. In this context, it is important to pay special attention to the new way of campaigning in the new data world we live in, proposing appropriate and efficient regulations to ensure fair elections.

While the data-driven political campaign is not a new phenomenon, the tools used, the amount of accessible data and the potential ability to influence voters represent a new and challenging scenario for the rule of law.

In recent years, political parties around the world have invested heavily in online advertising, demonstrating the potential to reach more people in an efficient and targeted manner. However, recent experiences, as in the case involving Cambridge Analytica and the last elections in Brazil, demonstrate how strategies for voters' political manipulation through misinformation, algorithmic manipulation, behavioral micro-targeting, and social bots have been widely used in this scenario. In addition, these strategies are mostly based on unauthorized processing of personal data, as observed from the Cambridge Analytica case, the Brazilian election campaign in 2018, among others.

In the words of Colin Bennett and David Lyon:¹⁶²

Questions about the legitimate processing of personal data on the electorate is at the heart of the answer to each of these larger questions. The conduct of voter analytics and the micro-targeting of political messages, including the delivery of so-called “fake news” has a direct relationship to programmatic advertising, and to the impersonal algorithms that target individual citizens, often without their knowledge and consent. Familiar privacy questions are now injected into this heated international debate about democratic practices and regulators, such as data protection authorities (DPAs), now find themselves at the center of a global conversation about the future of democracy. Thus, “privacy and data protection have rarely in the past been ‘Big P’ political questions. They are now”

Therefore, considering the importance that personal data processing represents in this context, part of the possible abuses and risks arising from misuse can be mitigated by the application of robust legal frameworks for personal information governance, such as the GDPR in Europe and the recently sanctioned Brazilian Data Protection Law (LGPD), which will come into effect soon.


As demonstrated along this study, highlighting specific legal guidelines and concrete situations, both data protection regulations are fully applicable to political campaigns and have the ability to assist in reducing the instrumental use of personal data, while also avoiding the impact of misinformation and computational propaganda used for

the purpose of political manipulation. Therefore, a data protection approach can sum up strategically with other efforts, for example, coming from the private sector, helping reduce misinformation in electoral campaigns by sanctioning the illegal processing of personalized data, serving as an effective and useful legal instrument in the present context.

On the one hand it is the role of public institutions through its resolutions and sanctions to reinforce compliance with and the effectiveness of the LGPD and GDPR guidelines. On the other hand, it is the duty of political parties to comply with legal requirements, having full responsibility, transparency, and good faith in the processing of voters' personal data.

Unauthorized processing of personal data, along with misinformation techniques and unfair use of bots, profiles, deep fakes, and others, undermines voters' confidence and the integrity of political processes and should be viewed by institutions as threats to democracy.

162 Bennett, C. J. & Lyon, D. (2019). Data-driven elections: implications and challenges for democratic societies. *Internet Policy Review*, 8(4).



Although data-driven political campaigns are not a new phenomenon in themselves, the tools used, the amount of data available and the potential ability to influence voters represent a new and challenging scenario for the rule of law around the world. This study explains how this challenge can be handled and what opportunities legal standards can play in the protection of personal data, using the European and Brazilian legal framework as an example.