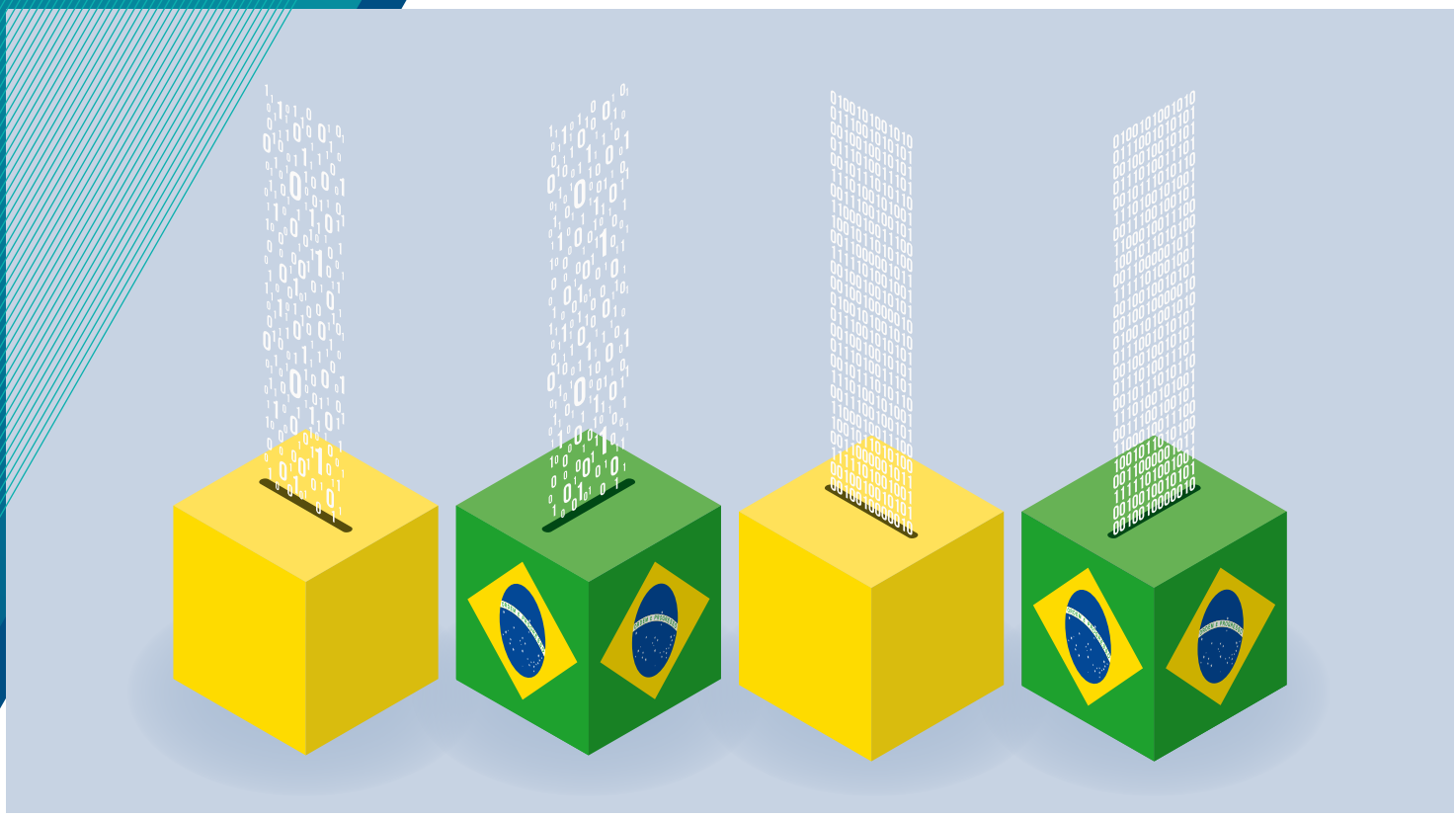
No 399 / July 2020
Facts & Findings

KONRAD ADENAUER STIFTUNG



Hacking the Electorate:
Thoughts on Misinformation and Personal Data Protection

Data-driven political campaigning is not new, but the tools and the possibilities are. And they become a real threat to democracy. Where are the conflicts? What are the solutions?

Eduardo Magrani

- 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
- 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.
- Current practices of unauthorized personal data processing are boosting misinformation and 'digital astroturfing strategies', capable of influencing citizens with great precision.
- Robust legal frameworks, such as the European general data protection regulations are applicable to political campaigning and can reduce the instrumental use of personal data for unfair political manipulation.

Table of Contents

History is old. Tools are modern.

It is vital in any democratic society that political parties and campaigners communicate effectively with voters.[1] In this sense, data-driven political campaigns are not a new phenomenon.[2] Political campaigns depend on information to guide several choices, such as places to hold rallies, which states or electoral bodies to concentrate efforts and resources on, and how to customize correspondence and advertising with supporters, swing voters, and non-supporters.[3]

With this purpose, 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.**[4]

Digital campaigning becomes a challenge for the rule of law.

In a study related to the 2016 elections in the USA[5], Harvard University researchers identified shifts in the production and consumption of political information. **With the arrival of participatory and social web[6], 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.** Even though large and traditional mass media organizations such as television, newspapers, and radio still play an important role, they are progressively migrating to online services, competing with all other content. As a consequence, **people in different countries are increasingly getting informed and learning about political candidates and other political related issues through social networks.** More importantly, these networks give them a sense of what others might think about issues and candidates, for better and for worse.[7]

In this context, 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 email addresses, phone numbers, and other personal data, such as the ones gathered through donations, at rallies, and through merchandise, allows political campaigners to obtain very sensitive information about specific target groups and voters.[8] **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.**[9]

Nevertheless, although new platforms and social media tools offer unprecedented opportunities to engage with a wide range of groups on issues of special importance to them in the democratic process, such innovations and effects have been so rapid that many voters do not know the scale or scope in which they are being targeted.[10]

Recipients do not know to what extent they are targeted.

Is there a problem?

Cambridge Analytica, the UK-based data analytics firm, has come onto the scene in 2016, following revelations that it might have played a role in different electoral processes, especially the USA election campaign of 2016. The company claimed to possess more than 5,000 data points on around 220 million Americans, consisting of psychological data from Facebook combined with a vast amount of consumer's information from data mining firms. **Essentially, 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.**[11]

A potential infringement can affect fundamental rights.

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. 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. On the other hand, all political parties and campaigners need to comply with the same data protection and electoral rules, regardless of the method or new technological developments.[12]

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.[13] 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.

Many countries, however, still lack adequate regulatory frameworks to guarantee data protection and privacy rights that are affected by this level of data processing and unfair manipulation, especially concerning sensitive personal data, such as political views or ethnicity.[14] Without a robust and effective safeguard for personal data processing, many abuses may come into play. **Current practices of unauthorized personal data processing are boosting misinformation and 'digital astroturfing strategies'**[15]**, capable of influencing citizens with even greater precision.** According to most recent research, these strategies are having an effective interference on political democratic processes in different countries.[16]

Misinformation strategies interfere with the political democratic processes.

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 democratic threats.[17] Citizens can only make genuinely informed choices about whom to vote for if they are certain that their decisions have not been influenced unfairly. That is why trust and confidence in the integrity of democratic processes should not be weakened.[18] [19]

The importance of data governance and compliance in elections

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[20]").[21] 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.[22]

Harmonizing general privacy and data protection regulations with electoral laws can guarantee rights.

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.[23]

Enhancing effectiveness and bridging the gaps

The possibility of bridging electoral regulation and the legal frameworks for campaign activities involving personal data depends on many factors. Foremost, the inclusion of provisions that refer to and contemplate data protection regulations in the orientations issued by the electoral courts and electoral laws, through harmonization of processes and effective application of personal data protection rules to political campaigning.

Furthermore, although data protection regulations can offer substantial safeguards in this context, it also has some "flexibilities" that must be addressed to avoid misleading orientations. In the European Union, for instance, the regulation allows Member States to introduce national laws to complement the GDPR, manifesting specific realities and idiosyncrasies through "derogations". Nevertheless, rather than protecting individuals' rights, in some cases these exceptions may lead to disproportionate restriction of freedom of expression, privacy breaches, and incitement of misinformation. **This lack of uniformity or misinterpretation of 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 negatively other regions.**[24]

The effectiveness of data protection regulation depends on external factors.

The effectiveness of data protection regulation depends on the capacity and institutional articulation of the different stakeholders involved. 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 prevent manipulation and misinformation practices.[25]

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.

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.

Data protection regulations can help to reduce the instrumental use of personal data.

On the one hand it is the role of public institutions through its resolutions and sanctions, to reinforce the compliance and 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.

---

1 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. See also 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.

2 See https://privacyinternational.org/case-study/763/case-study-profiling-and-elections-how-political-campaigns-know-our-deepest-secrets. See also: Baldwin-Philippi, J. (2019), "Data campaigning: between empirics and assumptions", Internet Policy Review, 2019.

3 Isaak, J. and Hanna M. (2018), "User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection", IEEE Computer. Volume: 51, Issue: 8, August 2018, https://ieeexplore.ieee.org/abstract/document/8436400, access November, 2019. See also 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.

4 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.

5 Benkler, Yochai et al. (2018), "Network propaganda: Manipulation, disinformation, and radicalization in American politics", Oxford University Press.

6 Referring to websites that emphasize user-generated content, based on the concept of WEB 2.0.

7 See https://privacyinternational.org/case-study/763/case-study-profiling-and-elections-how-political-campaigns-know-our-deepest-secrets, access January, 2020.

8 See https://privacyinternational.org/case-study/763/case-study-profiling-and-elections-how-political-campaigns-know-our-deepest-secrets, access January, 2020.

9 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.

10 European Parliament (2019), "Polarisation and the use of technology in political campaigns and communication", https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634414/EPRS_STU(2019)634414_EN.pdf, access January, 2020.

11 See https://privacyinternational.org/case-study/763/case-study-profiling-and-elections-how-political-campaigns-know-our-deepest-secrets, access January, 2020.

12 See https://privacyinternational.org/case-study/763/case-study-profiling-and-elections-how-political-campaigns-know-our-deepest-secrets, access January, 2020.

13 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.

14 See https://privacyinternational.org/case-study/763/case-study-profiling-and-elections-how-political-campaigns-know-our-deepest-secrets.

15 Related to fake online grassroots activity through the use, for example, of social bots and fake profiles. See Kovic, M., Rauchfleisch, A., Sele, M., & Caspar, C. (2018), "Digital astroturfing in politics: Definition, typology, and counter-measures. Studies in Communication Sciences".

16 European Parliament (2019), "Automated tackling of disinformation", https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624278/EPRS_STU(2019)624278_EN.pdf, access January, 2020.

17 As recent evidence shows, voters do not grasp the hidden existence of personal data uses, undermining the system of democracy through computational propaganda. 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.

18 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. See also 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.

19 Kaltheuner, F. (2018), "It's about human dignity and autonomy", Digital Society Blog.

20 The Brazilian general data protection law ("LGPD") was widely based on the EU's general data protection regulation ("GDPR"). Thus, there are many similarities between the two.

21 Besides the ongoing efforts of specific regulations against fake news and efforts coming from the private sector, for instance, with solutions "by design" such as implemented by WhatsApp and other companies. WhatsApp for instance limited the number of members of each group to 256, limited the number of massage following to 5 at a time, and implemented the need of authorization to be added in a specific WhatsApp group. See https://faq.whatsapp.com/en/30046788/?lang=en, access January, 2020, access January, 2020.

22 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 election's integrity and voters' autonomy, as well as trust in the use of their information. 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. See also 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.

23 Britto, F. et al. (2019), "Internet e eleições no Brasil: Diagnósticos e recomendações", InternetLab.

24 Pavel, V. (2019), "Dear European Commission: Don't let political parties use our data to manipulate the vote". Medium.

25 Britto, F. et al. (2019), "Internet e eleições no Brasil: Diagnósticos e recomendações", InternetLab.

Imprint

The Author

Ph. D. Eduardo Magrani is Fellow at the Konrad Adenauer Stiftung on the European and International Cooperation Program for Global Innovation Policy, Digitalization and Artificial Intelligence and Professor of Law and Technology and Intellectual Property at Getulio Vargas Foundation Law School, IBMEC and Pontifical Catholic University of Rio de Janeiro (PUC-Rio) in Brazil. He is also the President of the National Institute for Data Protection in Brazil. Lates publication: 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.

Konrad-Adenauer-Stiftung e. V.

Jason Chumtong
Policy Advisor Artificial Intelligence
T/p +49 30 / 26 996-3989
jason.chumtong@kas.de

Sebastian Weise
Innovation Policy
T/p +49 30 / 26 996-3732
sebastian.weise@kas.de

Department Economy and Innovation
Division Analysis and Consulting

Postal address: Konrad-Adenauer-Stiftung, 10907 Berlin

Publisher: Konrad-Adenauer-Stiftung e. V. 2020, Berlin
Design and typesetting: yellow too, Pasiek Horntrich GbR

ISBN 978-3-95721-716-5