SOLUTIONS FOR REGULATING TARGETED POLITICAL ADVERTISING ON ONLINE PLATFORMS

November 2, 2021

CIVIL LIBERTIES UNION FOR EUROPE

Publisher

Civil Liberties Union for Europe e.V
Ringbahnstraße 16-18-20
12099 Berlin, Germany
www.liberties.eu

Authors

Jascha Galaski
Eva Simon

Table of contents

Introduction

Online targeting provides political actors, such as government officials, political parties, paid influencers or local activists, new opportunities to influence people over political issues. Political advertisers can target people based on the personal data they provide online or target people based on online behavioral data collected and made available by online platforms. Political advertisers can use these data to segment groups of people susceptible to being convinced by a given message and send those people highly personalized appeals to support a particular candidate or policy proposal.

Targeting techniques benefit political actors, for example by allowing them to reach disengaged citizens and those who ignore traditional mass media, which may increase political participation and knowledge about specific issues. But targeting can also be used to mislead, manipulate, discriminate against or demobilize voters. Political parties can use targeting techniques to say different things to different people. This allows candidates to engage in duplicitous campaigning (promising different things to different people) and can lead to feeding citizens only with information and arguments that reinforce their own existing beliefs. Instead of enriching political debate, it creates echo chambers and increases polarization.

Since the Cambridge Analytica scandal was revealed in 2018,[1] European lawmakers have been actively looking for ways to prevent malign actors from compromising fair elections.[2] Political advertising, whether offline or online, is currently regulated by national electoral laws and by online platforms' terms of service. Facebook and Google impose certain legal and transparency requirements on advertisers. Other online platforms, such as Twitter,[3] Pinterest,[4] LinkedIn[5] and TikTok[6] even went as far as banning all political advertising – although it is worth noting that political advertisements were never an important source of revenue for these companies. However, issue-based advertisements on these platforms persist, and the key question – where do we draw the line between political and non-political content – remains. What is worrying is that the laws governing elections are partially set by private companies that aren't democratically accountable to voters.

1 Cadwalladr, C and Graham-Harrison, E. *"Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach"* The Guardian, March 17, 2018

2 European Commission. "*Report on the 2019 elections to the European Parliament*" June 19, 2020

3 Twitter. https://business.twitter.com/en/help/ads-policies/ads-content-policies/political-content.html

4 Pinterest. https://policy.pinterest.com/en/advertising-guidelines#sub-section-political-campaigning

5 LinkedIn https://www.linkedin.com/legal/ads-policy#D

6 Chandlee, B. "*Understanding our policies around paid ads*" TikTok, , October 3, 2019.

The ability of political parties to deliver political messages to the public is protected by the right to freedom of expression. At the same time, users also have a right to share their own opinions and have access to the opinions of other users and politicians. On the other hand, online political targeting practices may undermine citizens' fundamental rights, including the protection of personal data, privacy, and the right to a fair election, affecting the lives of millions of people.

The European Commission has already underlined in the European Democracy Action Plan the need to ensure greater transparency in political advertising and plans to present a proposal in the third quarter of 2021 to mitigate the damaging impact of targeted political advertising. The ongoing legislative procedure of the Digital Services Act (DSA) will also regulate political advertising to a certain extent. We believe that besides existing General Data Protection Regulation (GDPR) rules, new regulations should limit the existing practice of targeted political advertising through enforceable transparency rules, limitation on targeting, and creating proper enforcement.

This paper analyzes what measures European and national lawmakers, and European and national authorities, should take to regulate targeted political advertising. This paper focuses on political advertising on online platforms.[7] We intentionally avoid covering commercial advertising. We want to analyze targeting from the fundamental rights perspective, namely, freedom of expression, personal data protection, and the impact on fair elections. These fundamental rights are closely connected to targeted political speeches, let them be advertising or others. We want to make sure that political actors can continue delivering their messages on online platforms while protecting free elections and the privacy of individuals. We limit ourselves to examining advertising on online platforms.

There are solutions that are fundamental rights-friendly and still allow political parties to deliver their messages to the general public. In addition, transparency requirements, the need for strong enforcement, and the applicable GDPR rules offer solutions horizontally to online targeting.

We call targeting methods targeting in general, let that be micro- or nanotargeting. We believe that general rules, especially data protection rules, should be applied and further specified to protect the fundamental rights of the users and healthy public debate where participants can freely express themselves, which in turn allows the users to make informed decisions about politics.

7 You can read about our findings for online advertising in the AdTech industry here: Simon, E. June 4, 2019. https://www.liberties.eu/en/stories/stop-spying-on-us-fix-ad-tech-campaign/275 Reich, O. "*New Privacy Complaints Filed In Against Invasive Online Advertising*" Civil Liberties Union for Europe. December 10, 2020.

Key Findings

Liberties advocates the following solutions concerning targeted political messages:

1. Greater transparency from online platforms. Online platforms should be subject to strict transparency obligations. In particular, there should be:

- Mandatory disclaimers on all political and issue-based advertisements. The disclaimers should include detailed information on why, how, and by whom advertisement recipients are targeted. Most importantly, recipients should be informed that the message is a paid political advertisement.

- Mandatory advertisement archives with detailed information on all political and issue-based advertisements. It should contain, among other things, the advertisement's content, the targeting criteria used to reach out to online platform users, the amount spent, the time it started and the time it stopped and the performance of the advertisement. The archive must be publicly available, easy to navigate, and designed to facilitate research and analysis.

- A mechanism where online platforms must answer users' (data subject) requests about their targeting methods, the data processed, and the rights set out in Article 15 of the GDPR. Online platforms should have 15 days to answer such requests.

- public access to information related to direct and indirect payments or any other remuneration received to display advertisement.

These are the first steps that would allow independent researchers, relevant authorities, national electoral commissions, other public authorities, and regulatory bodies to monitor political advertising and better understand its impact on democracy and fundamental rights.

2. More financial transparency from political advertisers. Besides online platforms, political advertisers should also be subject to stricter transparency requirements. They should publish a report at least once a year that provides insights into their online advertising activity, including information on the performance of their advertisements, the targeting criteria used, the money spent, and the intended purpose. These transparency measures are critical in countries like Hungary, where the government excluded online political advertisement from political advertising rules and from campaign spending. Journalists and citizens can only rely on Google's and Facebook's transparency databases.

3. Enforce the GDPR. The European Commission and national Data Protection Authorities (DPAs) must properly enforce the GDPR. The GDPR has the potential to safeguard EU residents' rights and prevent the misuse of their personal data for targeting purposes. It can eliminate dark patterns that online platforms use to trick users into sharing their data, such as "I agree" buttons that users click to get rid of annoying pop-ups or banners. Consent of the data subject is needed prior to processing personal data for targeted advertising. Even

though the GDPR provides solid ground for valid consent requirements, the lack of enforcement creates a reference in new pieces of legislation, such as the Digital Services Act (DSA) and the relevant upcoming proposal for targeted political advertising. Proper enforcement of the GDPR and further rules would correct the current power imbalance between online platforms and users.

4. Strengthen data protection rules through DSA and ePrivacy Regulation. The Commission and national DPAs should elaborate guidance to clarify how the GDPR should be applied to political advertising. It is obvious by now that more detailed data protection rules are needed to establish a robust and universal application of privacy-friendly advertising methods. The draft ePrivacy regulation or the draft Digital Services Act offers the possibility for European legislators to fine-tune GDPR rules in this field. In addition, the Commission should urge the Member States to provide DPAs with the funds necessary for the tasks they are expected to undertake and explore ways of supporting DPAs directly, for example by providing them with expertise and services.

5. Conduct Data Protection Impact Assessments and Human Rights Impact Assessments. In fulfilling their transparency obligations, political parties, interest groups, and platforms should be required to conduct and publish Data Protection Impact Assessments and Human Rights Impact Assessment relating to online political campaigns hosted on relevant platforms. National DPAs, Digital Services Coordinators (DSCs), and the electorate bodies should have the authority to order binding remedial action. This includes issuing fines to online platforms and political parties or interest groups and referral of the DPAs' and DSCs' findings to national electoral commissions. Joint liability of platforms and political parties could force them to follow the rules.

6. Empower users. There is a severe power imbalance between online platforms and users. Users should have more control over their news feed and their personal data online. They should be allowed to decide whether they want to receive targeted political advertisements or not. For this to happen, and in accordance with EU data protection rules, online platforms should receive users' explicit consent via an opt-in. To limit pop-up fatigue, there should be rules that limit how often online platforms can ask users to opt-in.

7. Limit targeting methods to the minimum. Regulators should limit the targeting methods that online platforms make available to political advertisers. Targeted political advertisements based on observed (e.g. what sort of content users like and share) and inferred data (assumptions that algorithms make about users' preferences based on their online activity) should be fully prohibited. The only form of personalized targeting allowed should be based on relevant broad demographic data provided by users and are proven to be necessary to promote greater democratic engagement by citizens, such as data shared voluntarily about broad location data, age, and language preferences or for using opt-in mechanisms. Here too it is only legitimate if the data subject consents to use these data sets for targeting. This limitation on the

choice of targeting criteria would reduce the possibility that political actors tailor different promises to different homogenous groups of people and manipulate the electorate. Instead, we believe that non-surveillance methods such as contextual advertising offer the best way forward.

8. Strong enforcement of new rules. Regulation of targeted political advertising is essential to healthy democratic debate and fair elections across the EU. As we have seen concerning the GDPR, the key is how rules are enforced. We learned the lesson that self-regulation and voluntarily applied transparency rules are not enough. We believe that regulatory oversight is a must. Data Protection Authorities, Digital Services Coordinators, electoral authorities, and independent auditors are critical in creating meaningful mechanisms. We need a European-level, cross-sector authority for proper oversight. One solution is the European Digital Services Coordinators Board, similar to the European Data Protection Board.

9. Cautiously define political advertising and advertisers. To regulate political advertising, we need a definition. To avoid over-regulation and limitation of public discourse, we advocate for a narrow definition. However, we firmly believe that the solution limiting targeted political advertising is to minimize the data set and require the consent of the users. In this way, the targeting method would not depend on the classification of the advertisement but rather the data minimization and the consent approach that could effectively limit the practice of targeting. We also believe that defining certain primary and secondary advertisers, who would then face heightened scrutiny and possibly volume or spending caps, is also an approach worth considering.

Why are targeted political advertisements a threat to democracy and fundamental rights?

Targeted political messaging practices pose several threats to democracy. Foremost among these is polarization. In a well-functioning democracy, citizens are confronted with points of view that differ from their own. As a result, they get the chance to participate in a balanced debate and consider different perspectives. However, targeted advertising exposes citizens repeatedly to opinions similar to their own, thus reinforcing their own beliefs. Sealing people in such ideological echo chambers limits their right to information and leads to polarization. This in turn makes it difficult for the democratic process to deliver compromises that can make citizens across the political spectrum feel heard. Instead, it makes 'winner-take-all' politics more likely, which can alienate large numbers of voters.

Targeting campaigns also allow the same actor to provide different categories of voters with plainly contradictory messages while concealing this duplicity. Instead of presenting a consistent agenda to the general public, political actors can send tailored messages to homogenous groups promising to focus on the issue that is the most salient for them. These

groups would then have a biased perception of the political actor's priorities.

Malign actors can further exploit these bubbles for disinformation campaigns and to suppress voters.[8] For example, during the 2016 US elections, black Americans, who generally favor Democrats over Republicans, were spammed with messages attacking Hillary Clinton in order to discourage them from voting.

Finally, targeting can be used to discriminate against and exclude certain groups from receiving information, which can increase marginalization and social exclusion. For example, advertisements about employment, housing, or elections can be hidden from certain people, based on age, gender, location, or more sensitive data, like ethnicity, political and sexual orientation, or browsing behavior. This was demonstrated in a study by investigative journalists who published housing advertisements and, using Facebook's targeting tools, excluded certain groups, such as Black Americans, Jews, mothers of high school kids, or people interested in wheelchair ramps.[9]

Transparency by default and going beyond

Increased transparency is part of the solution to countering the damaging impacts of political targeting and must be one of the basic principles of any regulation. Individuals exposed to political advertisements should know exactly why, how, and by whom they are being targeted. When individuals are made aware of why they are receiving specific messages, they are more likely to evaluate them critically. However, while empowering users is one tool, it is far from enough. Offering transparency for users means placing a burden on them to navigate a broken system, and many people don't have the time or inclination to do this. We should not expect people to report systemic problems of the online ecosystem.

On the other hand, more transparency will help authorities and lawmakers to understand better the impact of political targeting and take appropriate measures. Regulators will be able to identify patterns, such as large amounts of funding from particular sources, links between organizations and political parties or concerted efforts to mislead public opinion. This information will allow regulators to adapt electoral rules, for example by expanding campaign finance rules to include spending on social media. It will also give regulators more insights to understand whether there is a need for further rules to protect public debate. More transparency will also facilitate the work of journalists and researchers to signal attempts by political advertisers to mislead, manipulate or demobilize voters. This additional scrutiny by journalists and researchers is crucial, as

8 ubramanian, S. "*Inside the Macedonian Fake-News Complex*" Wired, February 2, 2017.

9 Angwin, J. et al "Facebook (Still) Letting Housing Advertisers Exclude Users by Race" ProPublica, November 21, 2017.

regulators may be subject to political pressure and limited resources.

In response to regulators' concerns, digital platforms have recently started to offer some transparency mechanisms. Google and Facebook, for example, have labeled political advertisements and issue-based advertisements, respectively. When Facebook users click on an advertisement related to a social issue (e.g. elections or immigration), they have access to some limited information, including the sponsor's identity. A "why am I seeing this?" button reveals basic information on the targeting criteria, and users have the option to click to see fewer advertisements about certain issues in the future. These are important mechanisms, as they allow users to get a better understanding of and some control over their news feed. However, they are still rudimentary. The information accessible to users is extremely limited and can give a false sense of understanding. For example, the "why am I seeing this?" feature from Facebook only reveals one parameter to users, while advertisers usually choose multiple criteria. Researchers have also found that Facebook's explanations are often misleading.[10] During the 2019 European elections, pregnant women in Poland were targeted with messages on prenatal screenings and perinatal care; if they clicked on "why am I seeing this?" they would only be informed that they were targeted because of their interest in "medicine", the most common attribute, and not because of their interest in "pregnancy".

Further important transparency tools are advertisement archives. Both Google and Facebook have created online repositories. Google's archive contains political advertisements, whereas Facebook's archive contains advertisements related to social issues. However, these archives have serious shortcomings. First, they are extremely hard to navigate and lack important information, such as the exact targeting criteria or advertisement performance. Second, studies[11] have shown that some political advertisements are missing in the archives while some commercial advertisements are erroneously included. This makes it harder for researchers and journalists to get a proper understanding, impeding public scrutiny and accountability.

A proper advertisement archive should provide a comprehensive overview of all political and issue-based advertisements. It should contain 1) the content (i.e. the text, image and/or video content), 2) detail the targeting criteria used to reach out to online platform users, 3) the amount spent and the performance of the advertisement. The archive must be 4) publicly available, 5) easy to navigate and instead of restricting and putting constraints, it should 6) facilitate research and analysis. Liberties endorses the recommendations by the Mozilla Foundation and a group of independent

10 Iwańska, K.. et al. "*Who (really) targets you?*". Panoptykon Foundation https://panoptykon.org/political-ads-report

11 European Partnership for Democracy. "*Universal Advertising Transparency by Default*" , September 2020. European Partnership for Democracy. "*Virtual Insanity? Transparency in digital advertising*" March 2020 .

researchers on the required features of an effective advertisement archive API (Application Programming Interface),[12] as well as the detailed model advertisement archive developed by the organization Who Targets Me.[13]

Aside from introducing and enforcing transparency requirements, platforms and advertisers should be obliged to carry out Data Protection Impact Assessments and Human Rights Impact Assessments.[14] Analyzing the impact of political campaigns and disclosing related data would serve as further safeguards to better protect fundamental rights and democratic values.

In the draft DSA, transparency requirements are set out for very large online platforms. Recital (63) and Article 36 will require very large online platforms to ensure public access to advertisement repositories, while the Commission is obliged to encourage the development of codes of conduct. We are of the opinion that a code of conduct is far from enough to regulate and provide oversight of such activities. The DSA offers a great opportunity to limit targeted political advertising to a minimum, while also introducing detailed provisions and effective oversight tools to enforce transparency and eliminate unlawful targeting methods. The draft DSA Article 24 (advertising) and Article 29 (recommender systems) require only limited data disclosures and focus only on targeting attributes, but not on platforms and the algorithm they use. Regulators should focus on the algorithm because the surveillance advertising models are hidden in the algorithm, and it conflicts with with the fundamental rights of the users and the democratic values of the European Union. Another solution is to have these rules in a separate act, such as the rules based on the European Democracy Action Plan.

The problem with defining online political advertising

There is currently no common definition of political advertising at EU level. Online platforms have created their own definitions and rules. Twitter and TikTok have banned political advertisements. Google[15] has different election advertisement policies depending on the region.[16] In the EU, political advertisers (e.g. political parties) must first be verified by

12 Mozilla. "*Facebook and Google: This is What an Effective Ad Archive API Looks Like*" March 28, 2019

13 Who Targets Me. https://whotargets.me/en/ad-transparency-standards-a-technical-proposal/ December 18, 2020.

14 See EDPB Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202008_onthetargetingofsocialmediausers_en.pdf, Adopted on 4 April 2017.

15 Google Advertising Policies.

16 Google Advertising Policies.

Google and the targeting criteria they can use are limited to geographic location, age, gender and contextual targeting options. Facebook uses a definition of issue-based advertisements. This means that Facebook effectively designates advertisements as 'political' depending not on whether they are directly connected to a particular political campaign but rather based on whether they concern topics that are politically sensitive.[17] These issue-based advertisements are subject to increased transparency obligations. For example, political advertisers in the EU who want to launch an advertisement on 'civil and social rights' on Facebook are required, among other things, to use 'Paid for by' disclaimers. However, these definitions are often inconsistent with the requirements set out in the laws of EU Member States where they exist.[18] Also, it sheds light on the problem that unaccountable companies motivated by profit rather than the desire to support democracy effectively make the rules about what people can say to whom during elections.

Defining 'political advertising' is a complex issue that raises many questions.[19] On the one hand, defining 'political advertising' too broadly may seriously limit the right to freedom of expression and freedom of information by imposing rules on content that is not political advertising. On the other hand, an overly narrow definition would leave too much scope for political advertisers to bypass legal limitations. Whether political advertising is defined broadly or narrowly, the definition is still likely to create some legal uncertainty. There is, however, one major advantage in agreeing on a common definition of political advertising: it facilitates oversight and enforcement.

Another possibility is instead of providing an all-encompassing, content-based definition, regulators, online platforms, civil society actors and other stakeholders could also agree on defining certain actors as primary political advertisers (e.g. political parties, political foundations, interest groups) and secondary advertisers (those who advertise on their behalf).[20] These actors would face heightened scrutinies, such as reporting obligations or possibly volume or spending caps. However, some actors, like civil society or influencers, who can also pay to deliver political messages and potentially influence citizens' voting behavior, would not be covered in this definition.

17 Facebook

18 European Regulators Group for Audiovisual Media Services. "*Report of the activities carried out to assist the European Commission in the intermediate monitoring of the Code of practice on disinformation*", June 2019.

19 Jaursch, J. "*Defining Online Political Advertising*" Stiftung Neue Verantwortung, November 24, 2020.

20 See Footnote 19.

It is unlawful under the GDPR to target people with political messages by default

The GDPR only allows the use of limited targeting methods and requires the user's consent for being targeted. We believe that the limitation on targeted advertisement could have been introduced by applying the GDPR properly. The lack of enforcement creates an environment where further guidance, clarifications, and limitations are needed both for political parties and platforms to apply data protection rules.

Here we argue that even the GDPR serves as solid ground for limiting targeted political advertisements. In the GDPR, there are two legal bases to process personal data of online platform users in the targeting processes:[21] either with the consent of the user, or for the purposes of a legitimate interest.[22]

Liberties is of the opinion that legitimate interest (GDPR Art 6 (1) (f)) does not constitute a legal basis for targeting the users of online platforms with political messages because online platforms' economic or political interests should not be considered as legitimate interests. Therefore, anyone who targets users should have the users' prior consent (GDPR Article 6 (1) (a)).[23]

Online platforms whose business model is based on data harvesting must meet the requirements of the GDPR and require user consent to use their personal data for targeting purposes. This means that anyone who wishes to get tailored messages based on provided data should opt-in for this 'service' voluntarily, based on an informed decision. This rule is currently circumvented by online platforms,

21 Data subject's consent (Article 6(1)(a) GDPR) or legitimate interests (Article 6(1)(f) GDPR).

22 For detailed analysis see Guidelines 8/2020 on the targeting of social media users Version 1.0, adopted on 2 September 2020. However, we call attention to the significant difference between targeting political and non-political messages. While we can have a well-established argument that sanitary products are only targeted for a certain age group, we cannot argue the same for political advertisements.

23 The Judgment in Fashion ID, 29 July 2019, C-40/17, para. 95 - ECLI:EU:C:2019:629, CJEU reiterated that in order for a processing to rely on the legitimate interest, three cumulative conditions should be met, namely (i) the pursuit of a legitimate interest by the data controller or by the third party or parties to whom the data are disclosed; (ii) the need to process personal data for the purposes of the legitimate interests pursued; and (iii) the condition that the fundamental rights and freedoms of the data subject whose data require protection do not take precedence. The CJEU also specified that in a situation of joint controllership "it is necessary that each of those controllers should pursue a legitimate interest […] through those processing operations in order for those operations to be justified in respect of each of them". https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202008_onthetargetingofsocialmediausers_en.pdf para 44. Liberties believes that in political campaigns, these cumulative conditions can never be met.

which benefit from consent fatigue to continue tracking users.[24]

But even targeting those who choose to opt-in would only offer platforms and advertisers limited avenues for targeting messages. There are three main categories of data sets that could be used for targeting:[25]

- *Provided data:* Targeting individuals on the basis of provided data (i.e. data provided by data subjects voluntarily), such as age or location.

- *Observed data:* Targeting individuals on the basis of observed data, such as the data subjects' social media activity (e.g. what content they like or share), data from the device on which the social media app is used (e.g. mobile phone operating system or GPS coordinates) or data collected by third parties (e.g. data subjects' activity on other websites).

- *Inferred (derived) data:* Targeting individuals on the basis of inferred (or derived) data. That is, based on algorithm-derived data about their possible interests (e.g. an online platform may deduce that a person is likely to be interested in a specific product or service based on the person's browsing behavior).

In our understanding, the GDPR protects users from being targeted by observed or inferred data sets. The reason is that people can not consent to certain types of data processing when they don't have proper information about it. Consent is valid if "freely given, specific, informed" and there is an "unambiguous indication of the data subject's [...] agreement."[26] However, no one can give informed consent to dark patterns that trick users into sharing their data and non-transparent data processing. Only genuine transparency that informs users in each and every occurrence of data collection and targeting would validate their consent. This means that the use of observed data and derived data are not allowed for targeting, even in opt-in cases, because these categories are not transparent, and the user has no oversight and therefore run contrary to the GDPR.

If people wish to be subject to targeting, they can still opt-in for that purpose. This consent should be separated from accepting a platform's privacy policy or general terms of service. According to the European Data Protection Board's (EDPB) guidelines on consent, "If consent is bundled up as a non-negotiable part of the terms and conditions, it is presumed not to have been freely given".[27] Obtaining consent does not diminish the obligations of platforms or targeters to adhere to the data processing principles set out in Article 5 of the GDPR, such as fairness, necessity, or proportionality.

24 Ruiz, D. M. *"e-Privacy and the doorstep salesmen"* The European Consumer Organisation (BEUC), October 17, 2017

25 See footnote 15.

26 Article 4 (11) of the GDPR

27 European Data Protection Board (EDPB) "*Guidelines 05/2020 on consent under Regulation 2016/679"*, May 4, 2020.

Withdrawal by a user of their consent or any other objection from the user could also be processed through the platforms.[28]

But even for provided data sets, targeting should not be permitted for minors[29] or on the basis of sensitive data,[30] which allows for targeting vulnerable groups. In order to avoid fatiguing recipients who refuse to consent, platforms should respect terminal equipment settings that signal an objection to the processing of personal data.

In order to strengthen enforcement of the GDPR, the Commission and national DPAs should elaborate guidance to clarify how the rules of the GDPR should be applied to targeted political advertising. DPAs have the authority to order binding remedial action. This includes issuing fines to online platforms and political parties or interest groups and referral of the DPA's findings to national electoral commissions.

Profiling and automation under the GDPR

We learned from investigations into Cambridge Analytica that personality or psychological profiling can seriously distort political debate and even election results. The creation of voter profiles is always based on data harvested by online platforms. And this occurs through an automated decision-making process. Under Article 22 of the GDPR, everyone has the right not to be subject to these automated decision-making processes unless it is based on i) a contractual relationship; ii) authorized by law; or iii) it is based on the users' explicit consent. Points i) and ii) are not applicable in the case of social media services, even though they tend to argue to the contrary. This is because acceptance by a user of non-negotiable terms of service is not considered a contractual relationship.[31] Therefore, data processing in relation to the automated decision-making process can only rely on users' explicit consent under Article 4 (11) of the GDPR. The right of the users to contest an automated decision entitles them *not to consent* to any kind of automated decision-making method without human intervention. Users must be able to understand decisions made about them as well as understand how automated decision making affects them, and they must also understand how to contest a decision if necessary, according to Article 21 (1) of the GDPR. Human intervention is also essential for transparent decision making and transparent appeal mechanisms to correct the imbalance between online platforms and users. Therefore, Article 22 of the GDPR can also be a reference for mandating greater transparency for using targeting methods.

28 See the European Data Protection Supervisor's (EDPS) "*quick guide to necessity and proportionality*" January 28, 2020.

29 Recital 38 of the GDPR

30 Recital 51 of the GDPR

31 Article 6 (1) b) of the GDPR

Strong enforcement needed

The GDPR has taught us that enforcement requires more attention. Counting on online platforms to self-regulate and apply transparency rules voluntarily is not sufficient, and it is also the easiest way for platforms to circumvent regulation. We believe that regulatory oversight is a must. We suggest establishing an EU-level Digital Services Coordinator Board (DSCB) similar to the European Data Protection Board (EDPB) to oversee political advertisements online. The European-level authority should cooperate with the EDPB, with nation DPAs, electoral authorities, and independent auditors. These bodies are critical in creating meaningful enforcement mechanisms.

One of the main reasons why GDPR enforcement has been so slow is that national DPAs are chronically understaffed and underfunded.[32] Many national DPAs do not have the financial and technical capacity to tackle cases against big online companies effectively. Therefore, they should be properly equipped with resources,[33] staff, technical knowledge, and IT specialists, and they must use these to take action. In this regard, we urge the European Commission to start infringement procedures against the Member States that do not provide DPAs with enough resources. Furthermore, authorities potentially responsible for enforcing targeted political advertising rules, such as national media regulators, electoral commissions, and the Digital Services Coordinator (DSC) foreseen in the upcoming DSA will also require resources, autonomy and enforcement powers to ensure that they have the capacity to oversee online political campaigns, investigate electoral expenditures, address complaints, issue penalties and enforce the DSA rules. This is particularly important considering that these bodies will have to acquire new knowledge and take over new tasks. It is also crucial to ensure that these agencies are independent of government and business and can work coordinated under a lead authority.

There is a need to establish a relevant authority for developing opinions and guidelines, coordinating efforts of national regulators, and ensuring that there is a coherent approach across the EU with the involvement of national electorate authorities where such entities exist. However, these authorities have limited capacities and power. Therefore, we advocate enforcing rules related to targeted political advertisement through a DSCB, similar to the EDPB. The GDPR has also shown us that enforcement can be quite unevenly applied throughout the EU, allowing platforms to forum shop. For that reason, it is important to create a European body that would help national DSCs apply DSA and GDPR rules and other relevant political ad transparency rules evenly and issue guidance to help proper application of relevant rules to protect personal data, democratic values and expose campaign spendings. With this

32 Massé, E., Two Years Under the EU GDPR, An Implementation Progress Report, Access Now, May 2020.

33 Open letter https://edri.org/wp-content/uploads/2020/05/GDPR-Open-Letter-m.pdf, May 25, 2020.

solution, they would be able to speak in one voice and enforce EU-level rules.[34]

Conclusion

The upcoming DSA and the proposal for the Regulation on transparency for targeted political advertising give the EU the opportunity to update outdated rules and mitigate the damaging impact of targeted political advertising.

Properly enforcing the GDPR would correct the current power imbalance between online platforms and users, as the former will have to receive users' explicit consent via an opt-in option to subject them to targeted advertisements (based on provided data). The European Commission must help national DPAs develop guidelines on how to apply the GDPR to political advertising and press Member States to provide more resources to DPAs. Besides the DPAs, we advocate for the establishment of an EU level Digital Services Coordinator Board to help enforce rules evenly across the EU.

Regulators should ban any form of targeting based on people's online activity (observed data) and personality assumed by algorithms (inferred data) and reduce the targeting possibility solely to a very limited data set, and only if the data are provided by the data subjects themselves (after obtaining their consent). This would not only protect users' personal data but also make it more likely that political parties present themselves in a consistent way to different audiences, giving a better, more honest basis for political debate.

However, we also need new rules for proper regulation. Imposing stricter transparency obligations on online platforms is a first step that would allow independent researchers, journalists, public authorities, regulators and the general public to get a better understanding of the risks of targeted political advertising to democracy and fundamental rights. This will make it easier to adapt existing rules and raise the alarm when political actors try to distort the political debate and mislead and manipulate the electorate.

Successful alternative models that respect users' fundamental rights exist. Contextual advertising in particular not only protects users' personal data, access to information and the right to a fair election, as well as political actors' right to political speech, but it also allows the advertising industry to pursue its commercial activities.[35]

34 Jaursch, J. "*The DSA Draft: Ambitious Rules, Weak Enforcement Mechanisms*" Stiftung Neue Verantwortung, May 25, 2021.

35 Ryan, J. "*(Six Months of Data): lessons for growing publisher revenue by removing 3rd party tracking*" Brave, July 24, 2020.

The Civil Liberties Union for Europe (Liberties) is a non-governmental organisation promoting and protecting the civil liberties of everyone in the European Union. We are headquartered in Berlin and have a presence in Brussels. Liberties is built on a network of national civil liberties NGOs from across the EU. Unless otherwise indicated, the opinions expressed by Liberties do not necessarily constitute the views of our member organisations.

Website:
liberties.eu

Contact info:
info@liberties.eu

The Civil Liberties Union for Europe e. V.
Ringbahnstr. 16-20
12099 Berlin
Germany

Subscribe to our newsletter
https://www.liberties.eu/en/subscribe

Reference link to study
Please, when referring to this study, use the following web address:
https://www.liberties.eu/f/MM-Oxv

Follow us