EU fundamental rights and democracy implications of data-driven political campaigns

Maja Brkan*

Abstract
This paper examines the impact of data-driven political campaigns on fundamental rights and democracy in the European Union. It demonstrates that such campaigns risk curtailing a number of rights and freedoms enshrined in the EU Charter of Fundamental Rights. They can affect voters’ right to respect for private life and protection of personal data (Articles 7 and 8 Charter) through the collection of massive amounts of personal data that serve as the base for profiling of voters. Moreover, they can restrain freedom of information of voters (Article 11 Charter) by providing them only partial information about campaigns of political parties. Furthermore, political manipulation stemming from targeted political advertising may affect the freedom of elections (Article 39(2) Charter), even though it might be a step too far to assert that the use of data-driven political campaigns undoubtedly leads to elections that are not ‘free’. Finally, the author cautions that it might be challenging to rely on the foundational legal category of democracy from Article 2 TEU, given that this provision needs to be given a concrete expression through another Treaty provision. Rather, in case of manipulative data-driven political campaigns, democracy as a value can be affected.

Keywords
Data-driven political campaigns, Charter of Fundamental Rights of the EU, freedom of expression and information, freedom of elections, democracy

1. Introduction
Data-driven political campaigns that rely on the collection and processing of voters’ data are rapidly gaining popularity among political parties for several reasons. Firstly, this type of
campaigning seems to be more efficient as it gives the political parties the possibility to diversify
the messages and to appeal to personal preferences of voters; it also allows to more easily identify
swing voters. Therefore, it gives political parties the opportunity to approach their political
campaigns in a more strategic manner and to focus on particular selected voters or geographical
areas. Secondly, reduced costs of data analytics, coupled with increased computing power, make
these types of campaigns more feasible, which offers political parties additional incentives to rely
on data processing for political purposes. Finally, data-driven political campaigns lend themselves
well to the use on social media. This widens the possibility to reach voters who follow political
campaigns predominantly on social media and engage with traditional media less frequently (TV,
newspaper), particularly young voters.

One of the core traits of data-driven political campaigns is that they rely on targeted political
messages. These messages are specifically tailored to voters, based on their profile inferred from
the data available about them. However, political advertising based on data does not necessarily
need to be targeted. As Dommett convincingly argues, data can inform political communication in
four different ways. It can incite political parties to send either (i) general or (ii) specific messages
to all voters, (iii) general messages to specific voters or (iv) specialised messages to specific
voters. Data-driven political campaigns are therefore not to be readily equated with political
micro-targeting.

Yet, as this article will demonstrate, it is precisely the political micro-targeting that can arguably
pose the greatest risks for fundamental rights. In addition, given the appeal of micro-targeting,
numerous political campaigns have so far made use of data to personalize their political ads in
order to appeal to voters. This is shown by the increasingly broad use of such campaigns, starting
already with the US presidential campaign in 2012, UK elections in 2015, to the most notorious

1. See in this sense ‘Digital Microtargeting. Political Party Innovation Primer 1’, International Institute for Democracy and
Electoral Assistance (2018), https://www.idea.int/sites/default/files/publications/digital-microtargeting.pdf, p. 7, 13, 16.
2. Compare, in this sense D. Nickerson and T. Rogers, ‘Political Campaigns and Big Data’, HKS Working Paper No.
RWP13-045 (2014), https://ssrn.com/abstract=2354474, p. 4.
3. D. Nickerson and T. Rogers, ‘Political Campaigns and Big Data’, HKS Working Paper No. RWP13-045 (2014), p. 3-4.
4. For example J. Ohme, F. Marquart and L. M. Kristensen, ‘School lessons, social media and political events in a get-out-
the-vote campaign: successful drivers of political engagement among youth?’, Journal of Youth Studies (2019), https://
doi.org/10.1080/13676261.2019.1645311, point out, referring to other academic work, that ‘young citizens increasingly
receive political information through social media’ and that ‘receiving political information via social media mobilizes
political engagement of young citizens in various ways’.
5. Data-driven political campaigns and political microtargeting used in these campaigns has been subject to the extensive
academic research in the past years. Some of the core works include: I. S. Rubinstein, ‘Voter Privacy in the Age of Big
Data’, Wisconsin Law Review (2014), p. 861-936; D. Nickerson and T. Rogers, ‘Political Campaigns and Big Data’,
HKS Working Paper No. RWP13-045 (2014), p. 1-34; T. Dobber et al., ‘Two crates of beer and 40 pizzas: the adoption
of innovative political behavioural targeting techniques’, 6 Internet Policy Review (2017), https://doi.org/10.14763/
2017.4.777, p. 1-25; F. J. Zuiderveen Borgesius et al., ‘Online Political Microtargeting: Promises and Threats for
Democracy’, 14 Utrecht Law Review (2018), p. 82–96; K. Dommett, ‘Data-driven political campaigns in practice: under-
standing and regulating diverse data-driven campaigns’, 8 Internet Policy Review (2019), p. 1-18; C. J. Bennett and
D. Lyon, ‘Data-driven elections: implications and challenges for democratic societies’, 8 Internet Policy Review (2019),
https://doi.org/10.14763/2019.4.1433, p. 1-16.
6. K. Dommet, 8 Internet Policy Review (2019), p. 11.
7. I. S. Rubinstein, Wisconsin Law Review (2014), p. 864-865.
8. F. J. Zuiderveen Borgesius et al., 14 Utrecht Law Review (2018), p. 84.
uses during the US presidential elections\(^9\) and the Brexit referendum in 2016,\(^10\) as well as to other uses in Europe,\(^11\) India,\(^12\) Brasil,\(^13\) Canada\(^14\) and Africa.\(^15\)

This article examines the impact of data-driven political campaigns on EU fundamental rights and European democracy. It first explores the risks that these types of campaigns pose for selected rights and freedoms guaranteed by the EU Charter of Fundamental Rights (Charter): the freedom of information of voters, their data protection and privacy as well as their right to free elections. It also reflects on the impact on the value of democracy that is protected by Article 2 TEU (part 2). Furthermore, the article discusses various regulatory responses to these risks of data-driven political campaigns (part 3). In the next section, the article critically assesses one of the most controversial regulatory approaches in this regard, namely the prohibition of political profiling, from a fundamental rights perspective (part 4). Finally, the concluding part argues that further research is needed into the actual effects of data-driven political campaigns and that specific regulatory actions are needed on the EU level (part 5).

2. Fundamental rights risks of data-driven political campaigns

A. Risks for freedom of information

Data-driven political campaigns can pose numerous risks for freedom of information enshrined in Article 11 of the Charter. Since messages to different voters are personalised, political parties and social media could considerably limit freedom of information of potential voters, who would make their voting choices lacking impartial information on political candidates.\(^16\) This can be particularly aggravated if targeted political messages are shared through private communication channels (messengers, chat apps, chat groups) or if the major social media outlets favour a particular interest or agenda.

---

9. K. Manheim and L. Kaplan, ‘Artificial Intelligence: Risks to Privacy and Democracy’, 21 Yale Journal of Law & Technology (2019), p. 137-145.
10. C. Cadwalladr, ‘The great British Brexit robbery: how our democracy was hijacked’, The Guardian (2017), https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy.
11. For The Netherlands, see for example T. Dobber et al., 6 Internet Policy Review (2017), p. 1-25; for Germany, see for example A. Essif, ‘CDU, SPD and Greens use big data to target Bundestag voters’, DW (2017), https://www.dw.com/en/cdu-spd-and-greens-use-big-data-to-target-bundestag-voters/a-40244410. In Spain, the national legislation initially allowed for the use of personal data obtained from websites and other public sources for political activities during election periods, but this provision was struck down by the Spanish Constitutional Court in 2019; see the judgment of the Spanish Tribunal Constitucional 76/2019 of 22 May 2019, ECLI:ES:TC:2019:76, https://hj.tribunalconstitucional.es/HJ/es/Resolucion/Show/25942.
12. A. Varna, ‘Big Data Analytics and Transformation of Election Campaign in India’, Proceedings of the 2nd International Conference on Information Systems & Management Science (ISMS) (2019), http://dx.doi.org/10.2139/ssrn.3511428, p. 1-3.
13. R. Evangelista and F. Bruno, ‘WhatsApp and political instability in Brazil: Targeted messages and political radicalization’, 8 Internet Policy Review (2019), https://doi.org/10.10147.\(2019.4.1434, p. 1-23.
14. C. Bennett, ‘Data-Driven Elections in Canada: What We Might Expect in the 2019 Federal Election Campaign?’, Journal of Parliamentary and Political Law (2019), https://ssrn.com/abstract=3516999, p. 277-290.
15. See for example G. Wright, ‘Kenya: Data and Digital Election Campaigning’, Tactical Tech (2018), https://ourdataourselves.tacticaltech.org/posts/overview-kenya/.
16. Compare F. J. Zuiderveen Borgesius et al., 14 Utrecht Law Review (2018), p. 87, who points out that a political party ‘may highlight a different issue for each voter’, which ‘could lead to a biased perception regarding the priorities of that party’. See also S. Eskens, N. Helberger and J. Moeller, ‘Challenged by News Personalization: Five Perspectives on the Right to Receive Information’, Journal of Media Law (2017), https://doi.org/10.1080/17577632.2017.1387353, p. 22.
political candidate. It is true that traditional media (TV, radio, newspapers) could equally choose political messages depending on their preference for a political candidate. However, such messages would still be displayed in an equal manner to the entire electorate who can freely choose whether to consume information from this or another media source. Differently, targeting can enable the exclusion of certain groups from political discussion on certain topics, especially on those that might incite them to vote for another candidate.

The restrictions outlined above could potentially lead to an interference with Article 11 of the Charter, which protects freedom of information. The CJEU has, in its case law, not yet clarified whether the abovementioned limitations caused by data-driven political campaigns could fall within the scope of application of this provision. Hitherto, its case law had a different focus, for example on cases regarding balancing between copyright and freedom of expression/information (SABAM, Scarlet Extended, Spiegel Online, Funke Medien, GS Media) or between this right and exclusive broadcasting rights (Sky Österreich), freedom of expression and information in the context of labelling of products (Philip Morris, Neptune Distribution) or advertising of products (Damgaard). Differently, the ECtHR case law could give some indication in this regard. For example, this court accepted the prevention ‘of distortion of the electoral process, including fair competition between the candidates’ as a legitimate aim in Erdoğan Gökçe v. Turkey. Similarly, in Orlovskaya Iskra v. Russia, it accepted, as a legitimate aim, ‘the voters’ right to impartial, truthful and balanced information via mass media outlets and the formation of their informed choices in an election’. This could indicate that acts encroaching upon these values could amount to interferences with voters’ fundamental rights, in particular their right to information.

Furthermore, it needs to be noted that Article 11 of the Charter would only apply to data-driven political campaigns used during elections of members of the European Parliament and not to such campaigns in the framework of national elections in EU Member States. According to the well-established line of case law of the CJEU, starting with Akerberg Fransson, Union law is binding on the Member States only ‘when they act in the scope of Union law’. This would evidently not be the case for national elections, where national constitutions and the ECHR would apply.

---

17. F. J. Zuiderveen Borgesius et al., 14 Utrecht Law Review (2018), p. 88, 92, 95.
18. Case C-360/10 SABAM, EU:C:2012:85.
19. Case C-70/10 Scarlet Extended, EU:C:2011:771.
20. Case C-516/17 Spiegel Online, EU:C:2019:625.
21. Case C-469/17 Funke Medien NRW, EU:C:2019:623.
22. Case C-160/15 GS Media, EU:C:2016:644.
23. Case C-283/11 Sky Österreich, EU:C:2013:28.
24. Case C-547/14 Philip Morris Brands and Others, EU:C:2016:325.
25. Case C-157/14 Neptune Distribution, EU:C:2015:823.
26. Case C-421/07 Damgaard, EU:C:2009:222.
27. ECtHR, Erdoğan Gökçe v. Turkey, Judgment of 14 October 2014, Application No. 31736/04, para. 40.
28. ECtHR, Orlovskaya Iskra v. Russia, Judgment of 21 February 2017, Application No. 42911/08.
29. Case C-617/10 Akerberg Fransson, EU:C:2013:105, para. 20.
30. Tentatively, an argument could be made that the application of EU secondary legislation such as the General Data Protection Regulation, could bring national elections also within the scope of the Charter. While this could be true for the scope of application of the fundamental rights to privacy and data protection (Articles 7 and 8), it is unlikely that the application of this piece of legislation would trigger also the application of Article 11 of the Charter. As I argue elsewhere, Article 11 is not comprehensively ‘concretized with the EU secondary legislation’, and that could potentially limit the application of this provision in the Member State context; see M. Brkan, ‘Freedom of Expression and Brkan 777
Moreover, a close reading of Article 11 of the Charter raises the controversial question whether it can actually bind private actors, such as political parties and social media spreading targeted political messages. Article 11 of the Charter precludes only interferences ‘by public authority’, which seems to expressly exclude interferences by private parties. We have examined this question at length elsewhere, arguing that there are four possible ways to overcome this lacuna in legal protection: (i) rejecting horizontal direct effect of this provision and relying on secondary legislation; (ii) recognising horizontal direct effect of this provision; (iii) imposing a positive obligation on Member States to protect this fundamental right; and (iv) recognising quasi-public powers of the abovementioned private parties in order to turn a horizontal relationship into a vertical one.

Even though the CJEU did not yet have the opportunity to directly examine this question in the context of political campaigns, it is worth noting that it indirectly already recognised in *UPC Telekabel Wien*32 and *Mc Fadden*33 that private parties need to respect freedom of information of internet users in the context of the protection of copyright.34

Nevertheless, expressly recognising a general obligation of private parties to observe Article 11 of the Charter would directly contradict its wording and would lead to a *contra legem* interpretation of this provision. Therefore, the most appropriate way to solve this conundrum would be for the EU legislator to adopt secondary legislation to regulate targeted political advertising, taking into account a fair balance between all of the fundamental rights involved, notably freedom of information of voters, freedom of expression of political parties and freedom of elections overall. We explore different regulatory options in section 3 of this article.

**B. Risks for data protection and privacy**

Given the large-scale use of voters’ personal data, data-driven political campaigns also pose significant risks for data protection and privacy. Indeed, data protection has been at the forefront of discussions, regulatory actions and enforcement regarding this type of campaigns.35 Moreover, this issue has been subject to significant academic research.36 While data protection instruments are currently crucial for prevention of abusive practices, also because very few other legal instruments are available, suffice it to point out that data protection is insufficient to address the core challenges of data-driven political campaigns. This is because the ultimate threat of these type of campaigns is not a threat for private interests of data subjects, but rather a threat for public interests, such as freedom of elections and democracy.

31. See in detail M. Brkan, ‘Freedom of Expression and Artificial Intelligence: On Personalization, Disinformation and (Lack Of) Horizontal Effect of the Charter’, *Maastricht Faculty of Law Working Papers* (2019), https://ssrn.com/abstract=3354180, p. 9-10.
32. Case C-314/12 UPC Telekabel Wien, EU:C:2014:192.
33. Case C-484/14 Mc Fadden, EU:C:2016:689.
34. Case C-314/12 UPC Telekabel Wien, para. 56; Case C-484/14 Mc Fadden, para. 93.
35. See more in detail below section 3.A of this article.
36. See for example I. S. Rubinstein, *Wisconsin Law Review* (2014), p. 861-936; C. J. Bennett, ‘Voter databases, micro-targeting, and data protection law: can political parties campaign in Europe as they do in North America?’, 6 *International Data Privacy Law* (2016), https://doi.org/10.1093/idpl/ipw021, p. 261–275; A. Poulou, ‘Political Profiling: From the US to the EU, Data Protection Regulation from a Transatlantic Perspective’ (2018), https://ssrn.com/abstract=3160549.
C. Risks for freedom of elections

1. Freedom of elections as a core tenet of European elections

Data-driven political campaigns can potentially affect the fundamental right to freedom of elections, as protected by the Charter. In the Charter, the freedom of European elections is mandated by Article 39(2), according to which the ‘[m]embers of the European Parliament shall be elected by direct universal suffrage in a free and secret ballot.’ As specified in the Explanations to the Charter and as confirmed in the case Delvigne, this provision embodies the core ‘principles of the electoral system in a democratic State’. Further, recent cases such as Junqueras Vies and Puigdemont reiterate that this provision of the Charter embodies the abovementioned principles of direct universal suffrage in a free and secret ballot.

The current case law of the CJEU does not yet clarify whether data-driven political campaigns fall within the material scope of application of this fundamental right. Rather, it focuses for example on deprivation of the right to vote after a criminal conviction (Delvigne), immunity of an elected Member of European Parliament (Junqueras Vies), correct determination of official results of European elections (Puigdemont), conditioning the eligibility to vote with a residence requirement (Eman and Sevinger, Spain v UK) or appointment of an MEP following the withdrawal of candidates. Nevertheless, given the potentially manipulative impact of data-driven political campaigns on voters it can be reasonably assumed that they could be included into the scope of application of this fundamental right.

The wording of Article 39(2) of the Charter corresponds verbatim to Article 14(3) TEU. In contrast to freedom of information, the fact that the same provision appears also in the TEU shifts the focus of the discussion from the theoretical question whether provisions of the Charter should produce horizontal direct effect to the more practical question whether Article 14(3) TEU actually fulfils the conditions for direct effect. This question is particularly relevant from the perspective of ever more powerful private actors, such as social media and data brokers, which play a crucial role in data-driven political campaigns and can potentially encroach upon this fundamental right.

While Article 14(3) TEU indeed seems unconditional, it is questionable whether it is sufficiently precise as it does not impose any clear obligations on private parties. However, since EU secondary legislation equally requires freedom of European elections, this question becomes less pressing.
The ECHR protects freedom of elections in Article 3 of Protocol No. 1, which obliges States parties to that convention ‘to hold free elections [...] under conditions which will ensure the free expression of the opinion of the people in the choice of the legislature.’ While freedom of elections is one of the core elements of democracy, it is also conditioned upon freedom of expression, which enables opinions to circulate freely prior and during election times.\(^{49}\) This inextricable link between freedom of elections, freedom of expression and democracy was expressly recognized by the ECtHR in cases such as \(\text{Özgür Gündem v Turkey}\)\(^{50}\) and \(\text{Bowman v UK}\).\(^{51}\) Furthermore, differently than EU law, the ECtHR imposes a positive obligation on states to protect infringements of freedom of expression, even if they stem from actions of private individuals.\(^{52}\) This is again important in the framework of data-driven political campaigns because the EU Member States could still be held responsible under the ECHR if private parties obstructed freedom of expression related to elections.

2. Can data-driven political campaigns interfere with freedom of elections?

However, threats to free elections posed by data-driven political campaigns do not necessarily mean that free elections as a fundamental right protected by the Charter and the ECHR is unjustifiably restricted. From a legal perspective, without discussing free elections as a more political value, it is not entirely clear whether the use of data for electoral campaigns would necessarily endanger this fundamental right. As mentioned above, data-driven political campaigns could obstruct other fundamental rights, such as freedom of information of voters, but it remains unclear whether, in case of manipulative nature of such campaigns, the elections would indeed cease to be free. An unjustifiable interference with freedom of expression or information of voters does not seem to automatically lead to the violation of the fundamental right to free elections. Moreover, the abundant ECtHR case law on the right to free elections\(^{53}\) as well as the CJEU judgments regarding the right to vote under EU law\(^{54}\) do not seem to give a conclusive answer to this question. Nevertheless, some general pointers, applied by analogy, can be inferred from this case law.

The ECtHR clarified on numerous occasions that the core tenet of free elections is not the lack of states’ interference with elections, but rather their positive obligation to ensure democratic

\(^{49}\) Joint Report of the Venice Commission and of the Directorate of Information Society and Action Against Crime of the Directorate General of Human Rights and Rule of Law (DGI) on Digital Technologies and Elections, 16 CDL-AD (2019), point 50.

\(^{50}\) In \(\text{Özgür Gündem v Turkey}\), the ECtHR for example recognised ‘the key importance of freedom of expression as one of the preconditions for a functioning democracy’; see ECtHR, \(\text{Özgür Gündem v Turkey}\), Judgment of 16 March 2000, Application No. 23144/93, para. 43.

\(^{51}\) In \(\text{Bowman v UK}\), the ECtHR recognised that ‘free elections and freedom of expression, particularly freedom of political debate, together form the bedrock of any democratic system’. ECtHR, \(\text{Bowman v United Kingdom}\), Judgment of 19 February 1998, Application No. 141/1996/760/961, para. 42.

\(^{52}\) ECtHR, \(\text{Dink v Turkey}\), Judgment of 14 September 2010, Application No. 2668/07, 6102/08, 30079/08, 7072/09 et 7124/09, para. 106; ECtHR, \(\text{Özgür Gündem v Turkey}\), para. 43.

\(^{53}\) See for example ECtHR, \(\text{Matthews v United Kingdom}\), Judgment of 18 February 1999, Application No. 24833/94; ECtHR, \(\text{Sitaropoulos and Giakoumopoulos v Greece}\), Judgment of 15 March 2012, Application No. 42202/07; ECtHR, \(\text{Mathieu-Mohin and Clerfayt v Belgium}\), Judgment of 2 March 1987, Application No. 9267/81; ECtHR, \(\text{Labita v Italy}\), Judgment of 6 April 2000, Application No. 26772/95; ECtHR, \(\text{Cumhuriyet Halk Partisi v Turkey}\), Judgment of 26 April 2016, Application No. 19920/13.

\(^{54}\) Case C-145/04 Spain v United Kingdom; Case C-300/04 Eman and Sevinger; Case C-650/13 Delvigne.
More precisely, the benchmark for the elections to be ‘free’ is that they ensure ‘free expression of the opinion of the people in the choice of the legislature’.56 The ‘thwarting’ of such peoples’ opinion would deprive the elections from their capacity of being free57 and this seems to apply both to the period before the actual elections as well as for the period after, for example through procedural breaches during the phase of counting of votes that lead to ‘gross distortion of the voters’ intent’.58 Similarly, the CJEU clarified in Puigdemont59 that ‘the composition of [European] Parliament must faithfully and completely reflect the free expression of the choices made by the citizens of the European Union . . . as to the people by whom they wish to be represented in a given legislature’.60

However, it is unclear whether the use of voters’ data could indeed have such an effect. It seems that, in order for the abovementioned standard to be met, a negative and manipulative impact on election results would need to be empirically proven or would at least need to have a tangible effect on the outcome of elections. Nevertheless, determining such an effect might be challenging as it is difficult to determine what would be the outcome of election results without the (manipulative) data-driven campaign. A way to construct this standard in the framework of data-driven political campaigns is to require that the manipulative effect of such campaigns is sufficiently serious, in which would establish a presumption that there was a ‘thwarting’ effect on elections. Yet, the seriousness of such an effect might be equally challenging to be established.

An alternative would be to loosen the abovementioned criteria by recognising that merely a potential manipulative effect could deprive the elections to be free.61 This thesis seems to be more in line with the issues related to data-driven political campaigns where the exact empirical impact on the outcome of elections might be difficult to prove. However, the disadvantage of this criterion might be that the criterion of potential effect is too vague and could encompass also practices that in reality do not have any negative impact on elections. To the contrary, States parties to the ECHR could even argue that data-driven political campaigns allow them to show to the voters more relevant election materials.62 This question will therefore need to be further clarified in the case law.

D. Risks for democracy

EU law equally protects the value of democracy in Article 2 TEU. While democracy as a value is certainly at stake in case of data-driven political campaigns, invoking this provision in the context of such campaigns might be somewhat far-reaching. Reliance on this provision would namely raise

55. ECHHR, Mathieu-Mohin and Clerfayt v. Belgium, para. 50; ECHHR, Sitaropoulos and Giakoumopoulos v. Greece, para. 67; ECHHR, Communist Party of Russia and Others v. Russia, Judgment of 19 June 2012, Application No. 29400/05, para. 123. Golubok, referring to the ECHHR case law, talks in this regard about the elections that are ‘free from the influence of strangers and authorities’ representatives respectively’; see S. Golubok, ‘Right to Free Elections: Emerging Guarantees or Two Layers of Protection?’, 27 Netherlands Quarterly of Human Rights (2009), p. 373.
56. ECHHR, Mathieu-Mohin and Clerfayt v. Belgium, para. 53 and 57.
57. See in this sense ECHHR, Mathieu-Mohin and Clerfayt v. Belgium, para. 52 and 57.
58. For the period after the elections, see ECHHR, Davydov and Others v. Russia, Judgment of 30 May 2017, Application No. 75947/11, para. 287.
59. Case C-646/19 P(R) Puigdemont i Casamajó and Comín i Oliveres v Parliament, para. 59.
60. Case C-646/19 P(R) Puigdemont i Casamajó and Comín i Oliveres v Parliament, para. 59.
61. I am grateful to Natali Helberger for attracting my attention to this point.
62. F. J. Zuiderveen Borgesius et al., 14 Utrecht Law Review (2018), p. 85.
a question whether political parties and social media that obstruct freedom of elections contravene Article 2 TEU. It is submitted that this is not the case, since the mechanism for determining breaches of this provision requires a ‘serious’ and ‘persistent’ breach only on the part of a Member State and not individual private actors. Furthermore, Article 2 TEU also does not seem to be precise enough to be able to create obligations for private parties. Yet, even in case of alleged breaches of this provision by a Member State, the CJEU has hitherto always required reliance on another, more concrete provision of EU primary law. In case of democracy, such more concrete provisions could be those ensuring the freedom of elections of the European Parliament, analysed above. However, encroaching upon the latter provisions might not necessarily mean that Article 2 TEU would be contravened as well. Therefore, from a purely legal perspective it might be difficult to claim that Article 2 TEU can be infringed through data-driven political campaigns.

However, democracy as a value can clearly be undermined through the misuse of data in political campaigns, even though no formal breach of Article 2 is established. After all, free elections that enable an open discussion of political issues are the core component of any democratically established system. The idea of liberal, deliberative democracy rests upon the premise that democracy can function only if all actors are able to discuss and deliberate on political issues. In this regard, one can draw upon the Habermas’ theory of public sphere and its inextricable link to democracy. If deliberation is the core tenet of the value of democracy, this value might be threatened if some (targeted) messages, displayed only to a handful of voters, do not form part of this debate. From this, Habermasian perspective, democratic decisions are legitimate only if ‘all citizens are free to deliberate and reason with each other about policy’. Data-driven political campaigns can therefore have a major impact on the value of democracy.

3. Regulatory responses to the risks of data-driven political campaigns

A. The data protection response

Currently, the predominant response to the abovementioned risks is channeled through the existing data protection rules. The reason for this is not only the circumstance that this type of political campaigns can lead to large scale data breaches, but also that data protection is one of the few legal regimes that can deter the risks of such practices, having effective enforcement mechanisms and high fines. A further advantage of this regime is that it would also apply to data processed in the context of Member State elections and not only EU elections. It is therefore not surprising that

---

63. See Article 7 TEU, particularly paragraphs 1 and 2.
64. See per analogy, for the rule of law, Case C-619/18 Commission v Poland (Independence of Supreme court), EU:C:2019:531, para. 47; Case C-585/18 A.K. (Independence of disciplinary chamber of Supreme court), EU:C:2019:982, para. 167; Case C-216/18 PPU LM, EU:C:2018:586, para. 50.
65. Compare C. Brettschneider, ‘The Value Theory of Democracy’, 5 Politics, Philosophy, and Economics (2006), p. 259-278, https://ssrn.com/abstract=1746002.
66. For an analysis of the theory, see for example L. Goode, Jurgen Habermas: Democracy and the Public Sphere (Pluto Press, 2005).
67. Zuiderveen et al., 14 Utrecht Law Review (2018), p. 89.
68. C. Brettschneider, 5 Politics, Philosophy, and Economics (2006), p. 265.
numerous data protection authorities already imposed fines on Facebook in the aftermath of the Cambridge Analytica scandal, for example in Italy,\textsuperscript{69} in the UK\textsuperscript{70} and the USA.\textsuperscript{71}

In addition, on the EU level, the rules regulating funding of European political parties were amended in a way to prohibit these parties to impact the outcome of European elections by ‘taking advantage of an infringement’ of European data protection rules.\textsuperscript{72} Again, the observance of data protection rules is at the centre stage of mitigating the risks for European elections. Along these lines, the European Data Protection Supervisor recently issued a reprimand towards the European Parliament for using personal data of voters during the 2019 European elections.\textsuperscript{73}

However, reliance on data protection rules in the framework of elections seems to be unsatisfactory.\textsuperscript{74} Indeed, even campaigns where data is used in compliance with data protection legislation (for example, data collected with explicit consent of voters) may nevertheless manipulate the voters and have a detrimental impact on their fundamental rights and democracy. Therefore, data protection does not seem to be the most appropriate instrument to comprehensively mitigate the entirety of risks posed by this type of campaigns.

\textbf{B. The transparency response}

It has been argued that specific ‘labelling’ of targeted political ads, indicating not only that they contain sponsored content, but also that they are based on profiling of potential voters,\textsuperscript{75} would potentially be an important measure to mitigate the risks of political micro-targeting. This has already been a subject of debate in certain EU Member States.\textsuperscript{76} Along these lines, the European Commission calls for greater transparency of paid online political advertising more generally,

\textsuperscript{69} Ordinanza ingiunzione nei confronti di Facebook Ireland Ltd e Facebook Italy s.r.l. of 14 June 2019, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9121486.

\textsuperscript{70} Decision of the Information Commissioner’s Office of 24 October 2018, https://ico.org.uk/media/action-weve-taken/rnps/2260051/r-facebook-mpn-20181024.pdf.

\textsuperscript{71} See FTC press release, ‘FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook’, 24 July 2019, https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-privacy-restrictions. In addition, in December 2019 the FTC issued a decision against Cambridge Analytica for deceiving consumers; see FTC press release, ‘FTC Issues Opinion and Order Against Cambridge Analytica For Deceiving Consumers About the Collection of Facebook Data, Compliance with EU-U.S. Privacy Shield’, FTC (2019), https://www.ftc.gov/news-events/press-releases/2019/12/ftc-issues-opinion-order-against-cambridge-analytica-deceiving.

\textsuperscript{72} Article 10a(1) of Regulation (EU, Euratom) No 1141/2014 of the European Parliament and of the Council of 22 October 2014 on the statute and funding of European political parties and European political foundations, [2014] OJ L 317/1, in the version amended by Regulation 2019/493.

\textsuperscript{73} See ‘EDPS closes investigation into European Parliament’s 2019 election activities’, European Data Protection Supervisor 2020, https://edps.europa.eu/press-publications/press-news/press-releases/2020/edps-closes-investigation-european-parliaments_en.

\textsuperscript{74} Dobber, O Fathaigh and Zuiderveen Borgesius argue that the application of GDPR in the context of political micro-targeting is ‘necessary, but not sufficient’; see T. Dobber, R. O Fathaigh and F.J. Zuiderveen Borgesius, ‘The regulation of online political micro-targeting in Europe’, 8 Internet Policy Review (2019), p. 1.

\textsuperscript{75} Zuiderveen et al., 14 Utrecht Law Review (2018), p. 94-95.

\textsuperscript{76} Bodó, Helberger and de Vreese draw attention to the circumstance that the obligation to disclose political advertising are still missing in many countries and that the first regulatory approaches are emerging in The Netherlands, UK and Ireland; see B. Bodó, N. Helberger and C. H. de Vreese, ‘Political micro-targeting: A Manchurian candidate or just a dark horse? Towards the next generation of political micro-targeting research’, 6 Internet Policy Review (2017), p. 7-8.
regardless of whether it is combined with micro-targeting or not.\textsuperscript{77} According to the Commission, it should be disclosed who is behind such political advertising and, in cases of micro-targeting, which criteria are used for targeting.\textsuperscript{78} While it is true that labelling of sponsored content would enable European citizens to more easily recognize political advertising,\textsuperscript{79} this measure could potentially be insufficient in case of political micro-targeting.

The approach of the Commission seems to rest on a premise that the citizens would be potentially less manipulated through (targeted) political advertising if they were more aware that they are facing sponsored content. While increased transparency is certainly primordial for political advertising generally speaking, this approach could potentially prove insufficient in cases of political micro-targeting. On the one hand, it is possible that a certain proportion of voters might not fully discern the mechanisms behind political micro-targeting. On the other hand, it remains unclear how, where and in what detail the targeting criteria should be disclosed. Informing a citizen that she ‘received this sponsored content based on available data about her’ would be obviously quite different from cautioning her that ‘this sponsored content was specifically tailored according to her conscientious personality type’. The more detail is disclosed to the voter, the better (after all, the rights to information and access are enshrined already in Articles 13-15 GDPR), but it still seems unlikely that the voter would readily, just on the basis of this information, gain insight into how her political profile is constructed. It is even less likely that such labelling would immunize the voter against potential manipulation that targeting could bring along.

C. The self-regulatory response

Social media platforms and other intermediaries play a similar role as traditional media in imparting political information, but they have by and large not yet adopted ethical obligations that are similar to those of more traditional media.\textsuperscript{80} In particular, the lack of uniform regulation of these platforms, which nowadays act as crucial gatekeepers of information, can lead to the application of rather diverging self-regulatory rules on political campaigning. The self-regulation of targeted political advertising is a typical example of such divergence. While Twitter banned all political advertising in 2019,\textsuperscript{81} Google limited the way political ads are targeted by allowing only targeting based on general categories, including age, gender, and postal code.\textsuperscript{82} Differently, Facebook decided not to ban or limit any type of political advertising, whether targeted or not.\textsuperscript{83} In

\textsuperscript{77} Commission Recommendation of 12 September 2018 on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns in the context of elections to the European Parliament, C(2018) 5949, 8.

\textsuperscript{78} Ibid. 8.

\textsuperscript{79} Ibid. 3.

\textsuperscript{80} Joint Report of the Venice Commission and of the Directorate of Information Society and Action Against Crime of the Directorate General of Human Rights and Rule of Law (DGI) on Digital Technologies and Elections, 16 CDL-AD (2019), point 124.

\textsuperscript{81} M. Kelly, ‘Twitter will ban all political advertising starting in November’, The Verge (2019), https://www.theverge.com/2019/10/30/20940587/twitter-political-ad-ban-election-2020-jack-dorsey-facebook.

\textsuperscript{82} S. Spencer, ‘An update on our political ads policy’, Google (2019), https://blog.google/technology/ads/update-our-political-ads-policy.

\textsuperscript{83} See for example K. Swisher, ‘Google Changed Its Political Ad Policy. Will Facebook Be Next?’, New York Times (2019), https://www.nytimes.com/2019/11/22/opinion/google-political-ads.html; AP, ‘Facebook refuses to restrict untruthful political ads and micro-targeting’, The Guardian (2020), https://www.theguardian.com/technology/2020/jan/09/facebook-political-ads-micro-targeting-us-election.
consequence, the one major social media provider that allows for this practice would not only become a major battleground for paid political advertisements, this divergence could also have an impact on which segments of population would consequently be micro-targeted. It is highly questionable whether an important question such as regulation of targeted political advertising should be left to the self-regulatory practices of the social media.

D. The response requesting prohibition of political profiling

It is relatively straightforward to see that the use of micro-targeting and profiling, in particular psychographic profiling, deeply touches upon the personal freedom of voters, going way beyond the question of lawful processing of their personal data. The possibility of manipulation of voters, triggering their deepest fears and convictions through targeted messages, is an aspect that voters can hardly prevent by giving explicit consent to such profiling. It is perhaps with this rationale in mind that the European Parliament called for a ban on ‘profiling for political and electoral purposes and profiling based on online behaviour that may reveal political preferences’.\textsuperscript{84} The European Parliament opines that both profiling based on political opinions as well as profiling based on other data (socio-economic or demographic) should be prohibited.\textsuperscript{85}

Despite the fact that this proposition has not yet received a political epilogue in a form of legislation, there are strong arguments in favour of such prohibition of political profiling. As elaborated above, data-driven political campaigns can, through manipulation of voters’ opinions, pose significant risks to fundamental rights and democracy. Despite such a ban, political parties would still be able to pass their non-targeted political messages to the public in an unfettered way, for example through a TV debate. The impact of micro-targeting on voters might be more challenging if the message is tailored to a smaller group of voters targeted through private communication channels rather than shared publicly online. Banning political profiling would therefore not mean that general political advertising would be banned on social media altogether,\textsuperscript{86} but that it could no longer rely on users’ data to profile them and to show them highly individualized advertisements.\textsuperscript{87}

However, it is also questionable whether enforcing such a ban in practice would be efficient, as it might be \textit{prima facie} difficult to distinguish between general advertisements and targeted advertisements. In case of a ban, political parties might not only seek to keep their methods of data processing secret,\textsuperscript{88} but also try to depict targeted political ads as non-targeted ones. For example, if it is well known that a small segment of population in a particular region fears increased migration and a far-right political party opposing migration subsequently reinforces its campaign in that region on social media, would this qualify as ‘targeted’ political advertising?

\textsuperscript{84} European Parliament resolution of 25 October 2018 on the use of Facebook users’ data by Cambridge Analytica and the impact on data protection (2018/2855(RSP)), point 9.
\textsuperscript{85} Ibid.
\textsuperscript{86} The measure would therefore be different from Twitter’s ban of political advertisement, see for example M. Kelly, ‘Twitter will ban all political advertising starting in November’, \textit{The Verge} (2019), https://www.theverge.com/2019/10/30/20940587/twitter-political-ad-ban-election-2020-jack-dorsey-facebook.
\textsuperscript{87} This is also the position of Ellen L. Weintraub, chair of the US Federal Election Commission; see E. L. Weintraub, ‘Don’t abolish political ads on social media. Stop microtargeting.’, \textit{The Washington Post} (2019), https://www.washingtonpost.com/opinions/2019/11/01/dont-abolish-political-ads-social-media-stop-microtargeting/.
\textsuperscript{88} Bennett points out more generally that processing of data by political parties is ‘typically shrouded in a good deal of secrecy’; see C. J. Bennett, ‘Voter databases, micro-targeting, and data protection law: can political parties campaign in Europe as they do in North America?’ 6 \textit{International Data Privacy Law} (2016), p. 267.
Banning targeted political ads might pose a challenge for classifying them as ‘targeted’. While on the one hand, the definition of ‘targeting’ should not be as narrow as to allow political parties to easily escape a potential prohibition, it should also not be as broad as to encroach upon general political advertising altogether. This issue could potentially be solved through sufficiently detailed definitions in EU secondary legislation of what ‘targeted’ means, perhaps also through enumeration of criteria on which targeting cannot be based (for example, psychological characteristics, health data or race). In application of these criteria, the existence of ‘targeting’ would then need to be assessed on a case by case basis.

### 4. Compatibility of prohibition of political profiling with European fundamental rights

Even though it seems that banning political profiling could prima facie be an appropriate measure to tackle the risks of such profiling, it needs to be verified whether such a ban would be in compliance with the Charter, notably with freedom of expression of political parties.

#### A. Existing judicial approaches to political advertising

Currently, there is no case law of the CJEU or ECtHR that directly clarifies whether a ban on political profiling would be compatible with the Charter and/or the ECHR. While the CJEU did not yet have the opportunity to engage with political advertising, the case law of ECtHR in this regard remains inconclusive. On the one hand, the existing ECtHR case law on freedom of expression (Article 10 ECHR) of political parties does not concern online political advertising, but rather advertising on TV and radio. On the other hand, this case law is also quite divergent from the perspective of the outcome.

More precisely, in *TV Vest v Norway* and *Verein gegen Tierfabriken v Switzerland* the ban of political advertising indeed violated the freedom of expression. In these two cases, which concerned respectively an advertisement by a smaller political party and an advertisement relating to animal protection, the ECtHR placed particular emphasis on the prohibition’s aim to protect smaller political actors and on the circumstance that the animal protection advertisement was in public interest ‘as it related to consumer health and to animal and environmental protection’.

Differently, in a later case from 2013, *Animal Defenders International v UK*, the ECtHR found no violation of freedom of expression in case of prohibition of political advertising on TV and radio. In this case, the Strasbourg court reasoned differently by placing more accent on the circumstance that there is a lack of consensus among the states of the Council of Europe, which gives them a wider margin of discretion in these matters. Moreover, the Court pointed out that the

---

89. ECtHR, *TV Vest As & Rogaland Pensjonistparti v Norway*, Judgement of 11 December 2008, Application No. 21132/05 (prohibition of only TV political advertising); ECtHR, *Verein gegen Tierfabriken Schweiz (VgT) v Switzerland* (no. 2), Judgment of 30 June 2009, Application No. 32772/02 (TV and radio); ECtHR, *Animal Defenders International v United Kingdom*, Judgment of 22 April 2013, Application No. 48876/08 (TV and radio).

90. In ECtHR, *TV Vest As & Rogaland Pensjonistparti v Norway*, para. 73, the ECtHR pointed out that the ban was in principle intended to protect parties such as the party in question, which was not a major political party, and which was at a disadvantage in comparison with major political parties ‘which had obtained edited broadcasting coverage’.

91. ECtHR, *Verein gegen Tierfabriken Schweiz (VgT) v Switzerland*, para. 92.

92. ECtHR, *Animal Defenders International v UK*, para. 123.
applicant, an NGO that campaigned against the use of animals in leisure and commerce, could have had recourse to alternative media routes, including internet and social media.\textsuperscript{93}

Therefore, the current case law on political advertisements does not give enough guidance regarding a potential ban of online targeting in political advertisements. The ECtHR, however, recognizes that internet and social media ‘remain powerful communication tools’.\textsuperscript{94} Even though this Court in \textit{Animal Defenders} considered that the applicant can use this communication tool ‘in achieving its own objectives’,\textsuperscript{95} it is currently unclear whether the ECtHR or the CJEU would allow for targeted political advertising if it examined potential justificatory grounds for limitation of political parties’ freedom of expression. This question is explored below.

\textbf{B. Potential justificatory grounds for limitation of political parties’ freedom of expression}

The limitation of freedom of expression of political parties caused by the ban of political advertising could potentially be justified with various objectives of general interest, provided that they meet the requirement of proportionality.\textsuperscript{96} For example, in \textit{Neptune Distribution}, the CJEU recognized such an objective of general interest as a justificatory ground for limitation of freedom of expression of a business; in this particular case, the concrete objective was the need to ensure to the consumers accurate and transparent information and the related protection of human health.\textsuperscript{97} Per analogy, different objectives of general interest could be applied regarding data-driven political campaigns, notably transparency of political campaigns, prevention of manipulation of voters and balancing with competing fundamental rights of voters. All these justificatory grounds consequently also protect democracy.

\textbf{1. Prevention of manipulation of voters}

One of the core justificatory grounds for limitation of freedom of expression of political parties is prevention of manipulation of voters, Data-driven political campaigns have a potential for manipulation, since they restrain information to certain voters and choose which political information to display to others.\textsuperscript{98} The manipulative potential is particularly sensitive in case of psychographic profiling, where voters are mostly not aware that the targeted advertisements deliberately appeal to their most intimate sensitivities and fears.\textsuperscript{99} Micro-targeting can be based on sensitive data about voters and inferences stemming from this data, which enables to find a ‘weak spot’ of each particular voter or a group of voters. Moreover, research shows that bias in search results can lead to shifting of voting preferences,\textsuperscript{100} which can be partially mitigated by alerting users about the

\textsuperscript{93}ECtHR, \textit{Animal Defenders International v UK}, para. 124.
\textsuperscript{94}ECtHR, \textit{Animal Defenders International v UK}, para. 124.
\textsuperscript{95}Ibid.
\textsuperscript{96}According to Article 52(1) of the Charter, confirmed by the settled case law of the CJEU, limitations of fundamental rights may be justified if they ‘genuinely meet objectives of general interest recognised by the Union’ and if they are proportionate. In case law, see for example Joined Cases C-293/12 and C-594/12 \textit{Digital Rights Ireland}, EU:C:2014:238, para. 38, 41-44; for proportionality see para. 45-69.
\textsuperscript{97}Case C-157/14 \textit{Neptune Distribution}, para. 74.
\textsuperscript{98}F. J. Zuiderveen Borgesius et al., 14 \textit{Utrecht Law Review} (2018), p. 87.
\textsuperscript{99}Broader on threats of political micro-targeting see F. J. Zuiderveen Borgesius et al., 14 \textit{Utrecht Law Review} (2018), p. 87-89. See also K. Manheim and L. Kaplan, 21 \textit{Yale Journal of Law & Technology} (2019), p. 137-144.
\textsuperscript{100}R. Epstein and R. E. Robertson, ‘The search engine manipulation effect (SEME) and its possible impact on the outcomes of elections’, 112 \textit{Proceedings of the National Academy of Sciences} (2015), E4512-E4521.
existence of ranking bias. The risk of manipulation is particularly problematic if targeted messages are coupled with disinformation. Disinformation might be more difficult to be detected as untruthful if it is displayed only to a limited amount of voters, since these voters might not necessarily be faced with competing truthful information.

2. Transparency of political campaigns

Ensuring transparency of political campaigns can be a further important justificatory ground. In highly diversified data-driven political campaigns, it is more difficult to monitor both transparency of campaigning and transparency of campaign spending. If the spending rules do not prescribe specific reporting regarding campaign spending on social media, political parties could categorize digital advertising as market research or simply as advertising more generally. Due to challenges relating to transparency of campaigning, it is also potentially more difficult to enforce silence periods preceding the elections. Lack of clear transparency rules as to the origin of political messages potentially also facilitates meddling of third countries into elections of other states; through the use of voters’ data, different interest groups and third countries can directly target voters with political messages supporting their preferred political option in the country where elections are taking place.

3. Balancing with fundamental rights of voters

Freedom of expression of political parties can be equally justified through balancing with competing fundamental rights of voters, in particular those discussed above: voters’ freedom of information, privacy and data protection as well as freedom of elections. Such balancing is not new in the case law of the CJEU. In cases such as Spiegel Online and Funke Medien on balancing between copyright and freedom of expression, this court expressly stressed that it is particularly important to take into account ‘the nature of the “speech” or information’, notably ‘in political discourse and discourse concerning matters of the public interest’. In terms of data-driven political campaigns, this phrase could be understood in a sense that voters must be able to have access to unfettered political information, while allowing the political parties to freely express this information. However, that does not mean that political parties should be free to express their

101. R. Epstein et al., ‘Suppressing the Search Engine Manipulation Effect (SEME)’ Proc. ACM Hum.-Comput. Interact. (2017), Article 42, 1.
102. On the connection between disinformation and microtargeting, see J. Bayer, ‘Disinformation and Propaganda – Impact on the Functioning of the Rule of Law in the EU and its Member States’, HEC Paris Research Paper No. LAW-2019-1341 (2019), https://ssrn.com/abstract=3409279, p. 32-33, who point out that disinformation can be spread through platforms through different means, including microtargeting.
103. D. Tambini, Council of Europe Study on the use of internet in electoral campaigns, 11 DGI (2017), p. 17.
104. Ibid.
105. Ibid, p. 8.
106. Methodologically speaking, instead of balancing between different fundamental rights, the fundamental right that serves as a justification for restriction of another fundamental right can also be seen as an objective in general interest. Such an approach was taken by the CJEU in Case C-283/11 Sky Österreich, ECLI:EU:C:2013:28, para. 53, where the Court pointed out that the ‘safeguarding of the freedoms protected under Article 11 of the Charter undoubtedly constitutes a legitimate aim in the general interest’.
107. Case C-516/17 Spiegel Online.
108. Case C-469/17 Funke Medien NRW.
109. Case C-516/17 Spiegel Online, para. 58; Case C-469/17 Funke Medien NRW, para. 74.
views in a way to limit voters’ fundamental rights, when alternative ways exist that limit those fundamental rights in a less restrictive way.

5. Conclusion

The analysis in this article allows to draw two sets of conclusions. First, it stems from the analysis above that data-driven political campaigns can have a detrimental impact on fundamental rights, notably on freedom of information of voters (Article 11 Charter) as well as on their rights to privacy and data protection (Articles 7 and 8 Charter). Moreover, under certain circumstances, the freedom of elections (Article 39(2) Charter) and the value of democracy can be equally affected. Nevertheless, further research is needed into the actual harmful effects of data-driven political campaigns. In particular, experimental and empirical research determining the impact of these campaigns on voters’ voting behaviour is crucial. This research is however not without challenges. Voting behaviour is a rather complex phenomenon, which is not only affected by political campaigns, but also by numerous other factors, such as the social environment of the voter, her values and beliefs, psychological or other factors. It might therefore be challenging to determine the exact impact of data-driven campaigns on voters. Still, it would be highly beneficial to know more about which segments of population these types of campaigns can particularly impact and whether they only affect swing voters or also other voters with clearer political convictions. This information is important to know also in order to determine whether future legislation on data-driven campaigns needs to follow a more strict or a less strict approach.

Secondly, and related to the above, a more specific EU regulation of data-driven political campaigns is needed on the EU level. For reasons put forward in this article, it is important that this regulation goes beyond the field of data protection. Obviously, the regulatory choices between an outright ban, labelling, regulating the advertising criteria, self-regulation or leaving the choice to voters to opt in or out of targeted political advertising will depend on the role that we want to give to the European legislator in this matter. On the one hand, one could argue that an overzealous effort to prevent voters’ manipulation through a ban of political micro-targeting would be a too patronising approach, especially given that manipulation could occur also with other means of political communication and given that voters bear their own responsibility for their political choices. On the other hand, it can be argued that the psychological subtleties of targeting, the detail in which voters can be profiled and the extent to which political messages can be personalized put this type of advertising in a different category from general (non-targeted) political advertising.

Moreover, the data-driven political advertising should also, from a regulatory perspective, be clearly distinguished from commercial advertising. While the latter might have effect primarily on private interests of consumers, political advertising may have a much wider and more far-reaching impact on public interests, that is, on the outcome of elections and consequently

110. See in this sense F. J. Zuiderveen Borgesius et al., 14 Utrecht Law Review (2018), p. 94.
111. In the EU, the Directive on unfair commercial practices determines when (commercial) advertising can be seen as misleading commercial practice. See in particular Article 6(2)(a) of Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council, [2005] OJ L 149/22.
democracy, which warrants specific regulation. Finally, it seems important that the addressees of any regulation of data-driven political campaigns are not limited merely to political parties, but include also other actors in the advertisement ‘production’ and ‘distribution’ chain, including social media and data science companies. That approach, enshrined in the EU secondary legislation, would ultimately help to overcome the difficulties related to horizontal application of EU fundamental rights regime among private parties.

**ORCID iD**

Maja Brkan [https://orcid.org/0000-0001-7149-2805](https://orcid.org/0000-0001-7149-2805)