

Artificial Intelligence and Democracy:

The Impact of Disinformation, Social Bots and Political Targeting

Maja Brkan*

Free elections and democracy in Europe and globally can be detrimentally affected by a malicious use of new technologies, in particular artificial intelligence (AI). AI can be used as a tool to produce and spread disinformation or facilitate psychographic micro-targeting of voters in the run-up to elections. At the same time, AI can effectively counter such uses of technology. This article discusses the ways in which freedom of elections and democracy can be impacted through the deployment of AI.

I. Introduction

European and global democracies are under a severe threat due to extensive spread of disinformation through social and traditional media. The use of automated accounts and bots, psychographic micro-targeting, and deepfakes to proliferate fake news during elections are making the problem even more alarming. In addition, freedom of elections in the EU and the European democracy can be detrimentally affected by the use of artificial intelligence (AI) in other ways. For example, automated social bots can be (mis)used to promote political candidates and convince the voters to vote for this candidate even if they do not spread disinformation, in particular if coupled with micro-targeting.

The increasing use of artificially intelligent tools can seriously threaten public values of democracy, rule of law, freedom of elections and prevention of manipulation of voters. Nevertheless, it is also crucial to balance these values against freedom of expression, media freedom and media pluralism. EU institutions, governments, media outlets and civil society are deploying regulatory mechanisms to ensure the balance between these public values. For example, numerous policy documents have been adopted on the level of the EU to counter disinformation¹ and in response to political advertising.² This article aims to discuss the ways in which the use of AI can impact democracy and freedom of elections. More specifically, it discusses the potentially detrimental impact of the use of social bots, psychographic micro-targeting, disinformation and voting advice applications.

II. The Use of Artificial Intelligence to Impact Democracy

1. Social Bots

Social bots are automated or semi-automated social media accounts, primarily controlled by algorithms and programmed in a way to have the ability to interact with human social media users.³ They can automatically generate and spread content, without re-

DOI: 10.21552/delphi/2019/2/4

* Associate Professor of EU Law, Faculty of Law, Maastricht University, The Netherlands. For correspondence: <maja.brkan@maastrichtuniversity.nl>

- 1 For EU efforts to counter disinformation, see for example Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Tackling online disinformation: a European approach, COM(2018) 236 final; Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: Action Plan against Disinformation, JOIN(2018) 36 final; Commission Recommendation of 12.9.2018 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 final
- 2 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)), points 7-8
- 3 Kai-Cheng Yang et al, 'Arming the public with artificial intelligence to counter social bots' (2019) Human Behavior and Emerging Technologies 48.; Naja Bentzen, 'Computational propaganda techniques' (2018) European Parliamentary Research Service <[http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_ATA\(2018\)628284](http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_ATA(2018)628284)> accessed 5 April 2019; Philip N Howard, Samuel Woolley and Ryan Calo, 'Algorithms, Bots, and Political Communication in the US 2016 Election: The Challenge of Automated Political Communication for Election Law and Administration' (2018) 15 Journal of Information Technology & Politics 2, 81-93

vealing their non-human identity.⁴ One of the most important features of bots is that they can achieve scalability,⁵ which enables them to massively spread information and hence to (artificially) enhance the importance of a particular idea or popularity of a political candidate. Social bots used for political propaganda are sometimes termed also 'political bots',⁶ which strive to generate 'likes' and attract followers on social media.⁷ These bots can also identify keywords in public posts or conversations and then populate the content with their own posts (if they act as spam bots) or conversations (if they act as chat bots).⁸

Consequently, social bots can impact public political opinion by promoting or discrediting political candidates. Simultaneous use of numerous bots at the same time may also convey the impression that the information is coming from highly diverse sources, and is hence more reliable. Nevertheless, social bots can spread truthful information as well as disinformation alike, depending on the (potentially manipulative) goal for which they are being used. Finally, social bots can be efficient in mobilising citizens for the so-called 'astroturf' campaigns.⁹ Astroturf campaigns give the impression to be grassroots campaigns run by non-profit organisations or citizens, whereas in reality their driving force are busi-

nesses or politicians who do not reveal their identity.¹⁰

The use of social bots in election campaigns raised a considerable degree of controversy primarily during the 2016 US presidential elections.¹¹ However, elections and referenda in Europe do not seem to be immune on the impact of bots either. For example, (dis)information was spread with the help of bots in Germany during debates on the UN migration pact¹² and during the 2017 German elections,¹³ in Sweden during the 2018 elections¹⁴ and in France during the 2017 presidential elections.¹⁵ Moreover, the Brexit referendum campaign is a salient example of the use of social bots,¹⁶ where the latter were allegedly even used to massively sign a petition for a second Brexit referendum.¹⁷ Bots were reportedly spreading information also in the run up to the Catalan independence referendum,¹⁸ within the framework of a debate on immigration in Italy¹⁹ and in the run-up to the European elections.²⁰

From a technical perspective, the creation of social bots on social networks is becoming increasingly easier. On Twitter, for example, the creation of social bots is greatly facilitated through the open application programming interface (API)²¹ and it has been found that bots represent up to a quarter of all Twit-

4 See in this sense Kai-Cheng Yang et al (n 3) 48

5 *ibid*

6 See for example Robert Gorwa, Douglas Guilbeault, 'Unpacking the Social Media Bot: A Typology to Guide Research and Policy' (2018) *Policy & Internet* 8; Philip N Howard, Samuel Woolley and Ryan Calo (n 3) 85-87; Alessandro Bessi, Emilio Ferrara, 'Social Bots Distort the 2016 US Presidential Election Online Discussion' (2016) 21 *First Monday* 11, 1-14

7 Christian Grimme, Mike Preuss, Lena Adam, Heike Trautmann, 'Social Bots: Human-Like by Means of Human Control?' (2017) <<https://arxiv.org/abs/1706.07624>> accessed 9 April 2019

8 *ibid*

9 Philip N Howard, Samuel Woolley, Ryan Calo (n 3) 86

10 More on this notion from the perspective of international legal processes, see Melissa J Durkee, 'Astroturf Activism' (2017) 69 *Stanford Law Review*, 201-268

11 Samuel C Woolley, Douglas R. Guilbeault, 'Computational Propaganda in the United States of America: Manufacturing Consensus Online' (2017) Samuel Woolley, Philip N Howard (eds), *Computational Propaganda Research Project: Working Paper No 2017.5*, 1-28

12 'Germany mulls crackdown on social media bots', DW, 16 December 2018 <<https://p.dw.com/p/3ADar>> accessed 5 April 2019

13 Brachten et al estimate that the impact of social bots on German elections was minimal; see Florian Brachten et al, 'Strategies and Influence of Social Bots in a 2017 German State Election – A Case Study on Twitter' (Australasian Conference on Information

Systems, Hobart, 2017) <<https://arxiv.org/abs/1710.07562>> accessed 5 April 2019

14 For an analysis, see Johan Fernquist, Lisa Kaati, Nazar Akrami, Katie Cohen, Ralph Schroeder, 'Bots and the Swedish Election: A Study of Automated Accounts on Twitter' FOI Memo 6466, FSS Marknadsarbete Digitala lägesbilder valet 2018, September 2018 <<https://www.foi.se/rapportsammanfattning?reportNo=FOI%20MEMO%206466>> accessed 5 April 2019

15 Emilio Ferrara, 'Disinformation and social bot operations in the run up to the 2017 French presidential election' (2017) 22 *First Monday* 8

16 Marco T Bastos, Dan Mercea, 'The Brexit Botnet and User-Generated Hyperpartisan News' (2017) 37 *Social Science Computer Review* 1, 38-54

17 BBC 'EU Referendum Petition Hijacked by Bots' (BBC, 27 June 2016) <<https://www.bbc.com/news/technology-36640459>> accessed 5 April 2019

18 Mark Scott, Diego Torres, 'Catalan referendum stokes fears of Russian influence' *Politico* (29 September 2017) <<https://www.politico.eu/article/russia-catalonia-referendum-fake-news-misinformation>> accessed 5 April 2019

19 David Alandete and Daniel Verdú, 'How Russian Networks Worked to Boost the Far Right in Italy' *EL PAÍS in English* (1 March 2018)

20 Emmi Bevensee, Alexander Reid Ross and Sabrina Nardin, 'We built an Algorithm to Track Bots During the European Elections – What We Found Should Scare You' *Independent* (22 May 2019)

21 Robert Gorwa, Douglas Guilbeault, 'Unpacking the Social Media Bot: A Typology to Guide Research and Policy' (2018) *Policy & Internet*, 7

ter accounts.²² Facebook is equally populated with a considerable amount of fake accounts²³ and bots on its Messenger service.²⁴ Increasingly, the creation of bots does not require specific in-depth programming skills as it is facilitated by online services such as Somiibo.

2. Psychographic Micro-Targeting

Democracy and freedom of elections can be significantly impacted also through micro-targeting of voters with political advertisements,²⁵ particularly if coupled with the spread of disinformation. In the social media environment, profiling for the purposes of advertising is usually based on the combination of objective criteria, such as gender, age, marital status or place of residence, and subjective criteria, such as personal interests and personal history. While micro-targeting has traditionally been used for commercial advertising, nowadays it is increasingly deployed for political advertising during election campaigns.

In particular, during the 2016 US presidential elections, micro-targeting using psychographic criteria – also termed psychographic profiling – was widely used to convince the voters to cast their vote for the Republican candidate.²⁶ In other words, political advertisements that targeted individual voters on social media, appealed on their personality type. The profiles were created by the data science company Cambridge Analytica mainly on the basis of a personality quiz launched on Facebook that enabled to classi-

fy the users as having an open, conscientious, extravert, agreeable and neurotic personality type.²⁷ In addition, this data was coupled with a massive amount of other Facebook data about users, which were, in turn, micro-targeted with tailored political advertisements.²⁸ This data operation allegedly helped Donald Trump win US elections in 2016.²⁹ A similar data science manipulation apparently also contributed to the win of the 'leave' vote during the Brexit referendum.³⁰

3. AI as a Tool to Create and Spread Disinformation

During the past years, democratic political systems in Europe and globally have been significantly endangered by spreading of disinformation (fake news), particularly during the run-up to elections. The use of AI can significantly exacerbate these threats in three regards.

First, as already analysed above, the spread of disinformation through automated accounts and bots, coupled with psychographic micro-targeting, does not only reach an incomparably greater number of voters, but also appeals to their sensitivities, fears and psychological characteristics.

Secondly, while automated journalism may greatly facilitate reporting, it is also highly important that the content generated by automated means is regularly verified and that accountability for such journalism is ultimately attributed to a human.³¹ However, unless there is a malicious intent behind such

22 See, with reference to other literature cited therein, Tobias R Keller, Ulrike Klinger, 'Social Bots in Election Campaigns: Theoretical, Empirical, and Methodological Implications' (2018) 36 Political Communication 1, 176

23 Jack Nicas, 'Does Facebook Really Know How Many Fake Accounts It Has?' *New York Times* (30 January 2019)

24 Khari Johnson, 'Facebook Messenger passes 300,000 Bots' *VentureBeat* (1 May 2018) <<https://venturebeat.com/2018/05/01/facebook-messenger-passes-300000-bots/>> accessed 9 April 2019

25 Rubinstein calls this 'political direct marketing'; see Ira S Rubinstein, 'Voter Privacy in the Age of Big Data' (2014) *Wis L Rev* 861, 882

26 For an analysis of the use of micro-targeting of voters during the 2016 US presidential elections, see for example Karl Manheim and Lyric Kaplan, 'Artificial Intelligence: Risks to Privacy and Democracy' 21 *Yale J L & Tech* 106, 137-145. However, micro-targeting of voters based on data collection was used in US already well before these elections; see Chris Evans, 'It's the Autonomy, Stupid: Political Data-Mining and Voter Privacy in the Information Age' (2012) 13 *Minn J L Sci & Tech* 867, 884, 886

27 Karl Manheim and Lyric Kaplan, 'Artificial Intelligence: Risks to Privacy and Democracy' 21 *Yale J L & Tech* 106, 139

28 *ibid* 139-140

29 *ibid* 140

30 See for example Jamie Stanley, 'Meet Cambridge Analytica: The Big Data Communications Company Responsible for Trump & Brexit' (NOTA UK, 2 February 2017) <<https://nota-uk.org/2017/02/02/meet-cambridge-analytica-the-big-data-communications-company-responsible-for-trump-brexit/>> accessed 31 May 2019; for a proposal of Cambridge Analytica in this regard, see Cambridge Analytica and SCL Group, 'Leave.EU: Psychographic Targeting for Britain' (2015) <<https://www.parliament.uk/documents/commons-committees/culture-media-and-sport/BK-Background-paper-CA-proposals-to-LeaveEU.pdf>> accessed 31 May 2019

31 It is currently disputed who should bear the accountability for automated journalism; see for example Matteo Monti, 'Automated Journalism and Freedom of Information: Ethical and Juridical Problems Related to AI in the Press Field' (2018) *Opinio Juris in Comparatione* 1, 8-9

automated content, false information would be at best created incidentally and have limited capacity to harm freedom of elections. Nevertheless, the potential of automated journalism to create large-scale disinformation should not be neglected³² and should be included in the policy debates on disinformation.

Third, an even more significant threat to democracy could be posed by the creation of political deepfakes.³³ Deepfake technology enables creation of video or audio material that appears to be real, but is actually fake. It can take a form of interposing parts of the video with other content (such as swapping the face) or manipulating the video so that it seems that the person on the video is saying something she is actually not.

There is currently a disagreement as to whether deepfakes effectively represent a threat to democracy: some see it as a potentially severe source for political manipulation,³⁴ whereas others consider it to be a 'false alarm' whose threat 'hasn't materialised'.³⁵ Nonetheless, the mere potential for political manipulation is a sufficient source for concern and for an early regulatory response. Numerous examples have been put forward to depict these threats that can be, in the framework of elections, broadly categorised in two categories: videos aimed to harm political opponents and those seeking to enhance the candidates' political popularity. The first category could include videos depicting politicians involved in corruption or another controversial or criminal activity and uttering statements with inappropriate or offensive

content.³⁶ The second category could include fake videos of politicians attending high-level international meetings they never attended, shaking hands with prominent world leaders or offering support to vulnerable societal groups, such as homeless, sick or otherwise affected. The recent doctoring of videos of Nancy Pelosi demonstrates that deepfakes could represent a serious threat for democracy and freedom of elections.³⁷

However deepfakes are used, they have the capacity to lead to manipulation of elections where timing is of essential importance; if such a video is released shortly before elections, it can severely damage a candidate's political reputation or even sway election results.³⁸ This potentially harmful effects can be exacerbated by difficulties to effectively detect and debunk these quasi-realistic videos that give the audience an appearance of truth.

4. Algorithmic Voting Advice Applications

The aim of the voting advice applications is to help users take a decision which political party corresponds best to their political opinions. This is particularly important in a multi-party system with numerous smaller or mid-size political parties whose political agendas do not differ considerably, yet aspire for their voice to be heard. Voting advice applications have become widespread in the run-up to numerous elections, both on the national as well as on the Eu-

32 Compare Matteo Monti, 'Automated Journalism and Freedom of Information: Ethical and Juridical Problems Related to AI in the Press Field' (2018) *Opinio Juris in Comparatione* 1, 13

33 For an in-depth analysis of deepfakes see for example Robert Chesney and Danielle Keats Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2018) 107 *California Law Review* (2019, Forthcoming); U of Texas Law, Public Law Research Paper No. 692; U of Maryland Legal Studies Research Paper No. 2018-21, <<https://ssrn.com/abstract=3213954>> accessed 22 May 2019, 1-58

34 See in this sense for example Rachel Metz, 'The fight to stay ahead of deepfake videos before the 2020 US election' (*CNN Business*, 26 April 2019) <<https://www.cnn.com/2019/04/26/tech/ai-deepfake-detection-2020/index.html>>

35 Russell Brandom, 'Deepfake Propaganda is Not a Real Problem' (*The Verge*, 5 March 2019) <<https://www.theverge.com/2019/3/5/18251736/deepfake-propaganda-misinformation-troll-video-hoax>> accessed 21 May 2019, 7

36 For examples, see Holly Kathleen Hall, 'Deepfake Videos: When Seeing Isn't Believing' (2018) 27 *Cath. U. J. L. & Tech.* 51, 52; Robert Chesney and Danielle Keats Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2018) 107 *California Law Review* (2019, Forthcoming); U of

Texas Law, Public Law Research Paper No 692; U of Maryland Legal Studies Research Paper No 2018-21, <<https://ssrn.com/abstract=3213954>> accessed 22 May 2019, 20-21; Kelly Truesdale, 'Can You Believe Your Eyes? Deepfakes and the Rise of AI-Generated Media' (2018) *Georgetown Law Technology Review* <<https://georgetownlawtechreview.org/can-you-believe-your-eyes-deepfakes-and-the-rise-of-ai-generated-media/GLTR-03-2018/>> accessed 22 May 2019

37 CBS News 'Doctored Nancy Pelosi video highlights threat of "deepfake" tech' (*CBS News* 25, May 2019; updated 26 May 2019) <<https://www.cbsnews.com/news/doctored-nancy-pelosi-video-highlights-threat-of-deepfake-tech-2019-05-25/>> accessed 31 May 2019

38 Robert Chesney and Danielle Keats Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2018) 107 *California Law Review*, 107 *California Law Review* (2019, Forthcoming); U of Texas Law, Public Law Research Paper No 692; U of Maryland Legal Studies Research Paper No 2018-21, <<https://ssrn.com/abstract=3213954>> accessed 22 May 2019, 22; Kelly Truesdale, 'Can You Believe Your Eyes? Deepfakes and the Rise of AI-Generated Media' (2018) *Georgetown Law Technology Review* <<https://georgetownlawtechreview.org/can-you-believe-your-eyes-deepfakes-and-the-rise-of-ai-generated-media/GLTR-03-2018/>> accessed 22 May 2019

ropean level. For example, in the run-up to the 2019 European elections, different voting advice applications were offered to the European citizens, not only on the national level, but also through a Europe-wide recommender systems such as euandi2019³⁹ or EUvox⁴⁰.

In the Netherlands, for example, voting recommender systems are widely used to help voters choose their preferred party; different websites are available that offer a specific EU version of the recommender system for European elections, such as StemWijzer⁴¹, mijnstem⁴², Kieskompas⁴³, or the MVO Kieswijzer⁴⁴. According to statistical data, around 10% of the Dutch population used the StemWijzer recommender system before the 2019 European elections; for the national elections, this number was much higher.⁴⁵ In Slovenia, similar voter recommender systems were used before the 2019 European elections, such as the one from the newspapers Večer⁴⁶ or Delo⁴⁷. In Poland, a similar recommender system was used for previous elections, named 'Latarnik wyborczy' (meaning Election lighthouse).⁴⁸

The most pressing question with regard to the voting advice applications is whether the recommender algorithms do not suffer from an engrained bias that would lead to favouring of a particular political party. Such potential presence of bias would depend also on whether the organisation that sets up such an application is an independent body or a body potentially affiliated with a certain political party. Unfortunately, on many of the abovementioned applications, this information is not available. Moreover, as

with many other algorithmic decisions, transparency regarding how exactly the matching between the users' answers and those provided for by political parties is not available. Further work therefore needs to be done to enhance the transparency of these recommender systems, to avoid potential bias.⁴⁹

Moreover, the voting advice applications collect sensitive data about peoples' political preferences and political opinions. Even though many of the applications seemingly function on an anonymous basis, which would render the General Data Protection Regulation (GDPR) inapplicable,⁵⁰ they sometimes nevertheless collect personal data that allows for identification of users. For example, the Dutch voting advice application Kieskompas requires data about the year of birth, province, postal code and even (optionally) e-mail address of users, which is clearly information that enables the identification of the user.⁵¹ The possibility to identify users would lead to the application of the GDPR and the requirement of processing such data on one of the legitimate grounds for processing from Article 9(2) GDPR, with the most common ground being explicit consent (Article 9(2)(a)). However, the websites offering voting advice applications that collect personal data in principle do not require the users to give their explicit consent.

However, the impact that the voting advice applications have on voters' electoral choices seems to be limited. Research suggests that the voters were mostly impacted in their electoral choice when the suggested party already coincides with the party they were already considering to vote, but little impact has

39 See <<https://euandi2019.eu>> accessed 23 May 2019

40 See <www.euvot.eu> accessed 23 May 2019

41 The version for European elections in 2019 was available on <<https://eu.stemwijzer.nl/#intro>> accessed 23 May 2019

42 For European elections in 2019, see <<https://europa.mijnstem.nl/survey/45cbee7d488120/start>> accessed 23 May 2019

43 For European elections in 2019, see <<https://eu.kieskompas.nl>> accessed 23 May 2019

44 See <<https://mvokieswijzer.nl/>> accessed 23 May 2019

45 According to the statistical data, around 1,7 million Dutch voters used StemWijzer for the 2019 European elections, which accounts for about 10% of the entire population in the Netherlands; for the national elections in 2017, this figure was much higher, 6,8 million; see 'Bijna 1,7 miljoen gebruikers voor StemWijzer' (ProDemos, 23 May 2019) <<https://prodemos.nl/nieuws/bijna-17-miljoen-gebruikers-voor-stemwijzer/>> accessed 23 May 2019

46 See <<https://www.vecer.com/evropske-volitve#kvizEU>> accessed 23 May 2019

47 See <<https://www.delo.si/novice/volitve/interaktivni-vprasalniki-koga-naj-volim.html>> accessed 23 May 2019

48 Krzysztof Dyczkowski, Anna Stachowiak, 'A Recommender System with Uncertainty on the Example of Political Elections' in Salvatore Greco et al (eds), *Advances in Computational Intelligence, Proceedings of the 14th International Conference on Information Processing and Management of Uncertainty in Knowledge-Based Systems* (Springer 2012) 441, 442

49 On the question of bias, compare Clifton van der Linden and Jack Vowles, '(De)coding elections: the implications of Voting Advice Applications' (2017) 27 *Journal of Elections, Public Opinion and Parties* 2, 3-4

50 See Recital 26 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1

51 See <<https://eu.kieskompas.nl>> accessed 23 May 2019

been noticed when the system suggested the user to vote for a party she did not previously consider.⁵² This demonstrates that voting advice applications might not have a detrimental effect on democracy and freedom of elections.

III. Conclusion

The use of artificial intelligence can threaten and protect democracy at the same time. As demonstrated above, numerous application of technologies deploying AI can be detrimental to democracy. Due to this broad array of impacts, it seems appropriate to concur with Polonski who somewhat controversially, albeit truthfully, opined that the AI 'silently took over democracy'.⁵³ In response to this 'takeover', the EU has already taken numerous legal and policy measures to protect democratic processes, especially through protection of voters' data. The European Parliament for example called for more transparency

with regard to political advertising⁵⁴ and the rules regarding funding of European political parties have been amended with the aim to prevent misuse of data to impact the outcome of elections on the EU level.⁵⁵ It seems that the rules on data protection are therefore no longer serving only the protection of private individuals, but also safeguarding public values, including democracy. Finally, it is perhaps important to note that AI itself can also play a significant role in protecting democracy and democratic values, such as freedom of expression and fairness of elections. The detection of controversial uses of AI technologies is sometimes possible only with the AI itself. Typical examples are automated detection of deep-fakes which cannot be recognisable with a naked eye or the establishment of existence of bots on social media. It is important to recognise that any technology is in and of itself neutral and that democracy and other public values are impacted through the human use of this technology and its purpose, as determined by humans.

52 See for example R Michael Alvarez, Ines Levin, Peter Mair, Alexander Trechsel, 'Party Preferences in the Digital Age: The Impact of Voting Advice Applications' (2014) 20 Party Politics 227, 234; Matthew Wall, André Krouwel and Thomas Vitiello, 'Do Voters Follow the Recommendations of Voter Advice Application Websites? A Study of the Effects of Kieskompas.nl on its users' Vote Choices in the 2010 Dutch Legislative Elections' (2014) 20 Party Politics 416, 426. Compare Jan Kleinnijenhuis, Jasper van de Pol, Anita MJ van Hoof and André PM Krouwel, 'Genuine Effects of Vote Advice Applications on Party Choice: Filtering out Factors that Affect Both the Advice Obtained and the Vote' (2019) 25 Party Politics 291, 299-300

53 Vyacheslav Polonski, 'How Artificial Intelligence Silently Took Over Democracy' (*World Economic Forum*, 9 August 2017) <<https://www.weforum.org/agenda/2017/08/artificial-intelligence-can-save-democracy-unless-it-destroys-it-first/>> accessed 17 May 2019

54 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)), points 5, 8

55 See 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