Digital Democracy and Disinformation: The European Approach to Disinformation on Social Media in the Case of 2019 European Parliament Elections

Dawid Aristotelis Fusiek, Angeliki Elli Stougiannou, Theoharris William Efthymiou-Egleton

doi: 10.12681/jpentai.31215
Digital Democracy and Disinformation: The European Approach to Disinformation on Social Media in the Case of 2019 European Parliament Elections

Dawid Aristotelis Fusiek
Utrecht University, The Netherlands.

Angeliki Elli Stougiannou
Columbia University in the City of New York, U.S.A.

Theoharris-William Efthymiou-Egleton
London School of Economics and Political Science, U.K.

Abstract
This policy paper offers a brief overview of the hazards for digital democracy stemming from AI and digital tools and how the EU tackled online disinformation social media ahead of the 2019 European Parliament elections. The advent and introduction of social media into the political sphere has had a profound and substantial effect on Europe’s electoral processes affecting both voting behavior and the underlying factors that influence it. Whereas malicious actors often participating in disinformation have led to growing calls for reforms, this phenomenon has been most pronounced in the 2019 European parliament elections which saw an unprecedented reliance on digital media within the political process. Specifically, the European actors faced negative stemming from the scale of the vote and the algorithms and the attention-based business models used by the social media platforms. To meet these challenges, the EU not only employed legal and social means (e.g., the 2019 Action Plan Against Disinformation) but also created new initiatives focused on tackling disinformation (e.g., the Rapid Alert System). Notably, in an unprecedented manner, the EU also included the private sector in the process. As the paper argues, although its limitations, AI is an important tool for aiding the democratic process and tackling disinformation; however, a self-regulating approach favors the success of these endeavors.

Keywords: Social Media, Disinformation, European Union, Action Plan Against Disinformation, Rapid Alert System

1. Introduction
In the last decades, digital innovation and Artificial Intelligence (AI) are radically transforming democratic decision-making. Despite the initial positive reception by policymakers and academia of this shift, they soon realized that the intensification of both the use of social media and the spread of online information could potentially be an underlying threat to the future of democracy (Kreiss, 2015).
Due to the lack of objective standards and the increasing number of deceptive content, social media have proved to be capable of negatively affecting the process of election through the distribution of content that can sway, deceive, or even manipulate voters. Whereas this practice, referred to as either disinformation or “fake news” is not unprecedented, its utility as a tool to undermine democracy became apparent in the aftermath of the 2016 elections and Russia’s hybrid war against Ukraine (Jankowicz 2019). At the same time, the two events manifested other difficulties associated with disinformation, such as the difficulty to set consistent rules and keep up with the continuously changing disinformation tactics.

Not surprisingly, disinformation figured at the center of the European agenda ahead of the 2019 European Parliament elections (European Commission, 2018). Besides the global intensification of practices of disinformation, the size of the vote (28 countries participating simultaneously) made the Parliament’s election not only susceptible to disinformation campaigns but also difficult to shield from potential disinformation (Watson, 2019). Moreover, the plurality of languages, the political and historical setting (rise of populism and Euro sceptic parties), and the ignorance regarding the Union’s functions further contributed to the EU’s vulnerability (Lilkov, 2019). To meet these challenges, the EU employed a dynamic and multifaceted response that focused on data protection, transparency, cooperation with the private sector, promotion of diversity and credibility of information, rise of awareness, and the empowerment of the research community (Nenadic, 2019).

This policy paper offers a brief overview of the hazards for digital democracy stemming from AI and digital tools and how the EU tackled online disinformation on social media ahead of the 2019 European Parliament elections. Based on that, the research starts with an examination of the academic debate regarding disinformation and the role of social media in this phenomenon. Then, it focuses on how the European institutions approached the problem, the steps that were taken to protect European citizens, and the process of elections. Ultimately, the paper concludes with an estimation of the EU’s overall approach and general observations regarding the future of digital disinformation.

2. The Artificial Intelligence, Social Media and Democracy

Before analyzing the case study, it is important to define what exactly Artificial Intelligence is and how it presents itself in elections. The Brookings Institute defines AI as “machines that respond to stimulation consistent with traditional responses from humans, given the human capacity for contemplation, judgment, and intention” (West, 2018). Such digital systems are created to take decisions that typically require a specific level of human expertise (Shubhendu & Vajay, 2013). This
characteristic makes AI an optimal tool for election campaigns as its application into virtual platforms helps candidates and voters match with each other, or, if used malevolently, expose voters to fake news and disinformation to sway their vote to the opposing side (Asokan, 2019). This section thus will briefly look at the role of artificial intelligence as an enabler and deterrent of democratic elections.

Like most technological developments, AI maintains a range of benefits, limitations, and disadvantages. Its current use predominantly entails enhanced security, internet surveillance, social media marketing, and data analysis (Grottola, 2018). While all of these could be used for the “greater good” of society, to improve public safety, personalize social media experiences, and discover important trends, there is an undeniable possibility of malevolent usage (Efthymiou–Egleton et al., 2020). For instance, AI can easily facilitate a world of constant surveillance, minimal privacy, social ranking systems, and human rights violations (Grottola, 2018). Whichever ways governments choose to utilize these tools will determine whether the West continues to be a pillar of progressivism and democracy or will evolve into an Orwellian dystopia.

2.1. The Two Sides of the Artificial intelligence

The 2019 European Parliamentary Elections posed an excellent example of how AI can have negative and positive implications on the electoral process. Starting from the latter, as the platform YourVoteMatters.eu showed, AI can be a powerful tool to attract thousands of new voters. Specifically, the think-tank, Vote Watch Europe, constructed an algorithm paired with a questionnaire that simulated a decision-making process where the user was acting as a politician who voted on popular issues surrounding the elections (Swain, 2019). After the completion of the questionnaire, the AI algorithm would take the results and match the profile to a candidate with similar decisions in actuality (Ibid.). Then users were prompted to further research the candidates they matched with and discover more about their campaigns. This AI tool aids the common voter to self-educate and find a candidate that will create the world they want to see; it is evident that it is an enabler of the democratic process as it informs voters of candidates in an unbiased manner which permits them to vote intelligently (Minevich, 2020).

At the same time, AI technologies have been increasingly utilized negatively to deter the democratic process through the distribution and promotion of disinformation on social media. Over the last decade, the number of people using social media as a primary source of information has dramatically increased, especially among young users. Indicatively, in a 2018 Reuters study, in 37 states (located in Europe, the Americas, and the Asia Pacific) 54% of users identified social networks as a main source
of information, while this number is even higher in the young population reaching 69%. Capitalizing thus on mass audiences’ easy access to social media, especially Twitter, AI algorithms have been employed to misinform the public rapidly. Viral tweets spreading fake news, although easy to debunk with given time, can inflict great damage to elections and make them highly susceptible to short-term manipulation (Villasenor, 2020). These fake news campaigns usually entailed extreme views antagonizing the institutions of the EU, thus undermining the people's trust in their government and creating further problems for the European electoral process (Scott & Cerulus, 2019).

3. Online Disinformation Ahead of the 2019 European Parliament Elections

The issue of disinformation on social media has not been unprecedented for the EU. As a matter of fact, the first European initiatives to tackle this issue started in 2015 when the European Council recognized the threat in its conclusion on 20 March (European Council, 2015, 5). In the following years, the EU continued to build on its approach to countering disinformation through the adoption of legislation, such as the 2016 Joint Framework on countering hybrid threats, and the creation of corresponding institutions, such as the High-Level Expert Group on Fake News and Online Disinformation (European Commission, 2021). It is also important to notice that apart from the European instruments, each Member State has also developed similar initiatives on a national level. Excellent examples are the 2017 German Network Enforcement Act and the 2018 law regarding the fight against false information in France (Bayer, 2019). Given that, the EU already had operational foundations that enabled the development of a swift and successful response to disinformation on social media, always in line with its preventive approach to security.

Before the 2019 European elections, the EU faced two major issues: the algorithm and the attention-based business model which social media platforms use. Starting from the algorithm, it usually gives extra visibility to content-generating string, user-engagement, and numerous comments on social media platforms. As such, the algorithm amplifies provocative or divisive opinions and posts. The over-representation of such content on social media platforms creates not only the perception that these ideas are shared by the larger body of society but also facilitates the mainstreaming of radical opinions such as conspiracy theories and propaganda (Lilkov, 2019, 4).

Concerning the attention-based business model used by all free online media services, it relies on the promotion of specific content and advertisements to smaller groups of users based on their interests or individual characteristics (Joseph, 2018). Hence, this model contributes to a polarized and fragmented online information space that aids the dispensation of fake news and disinformation. An excellent
example of this problem is the case of Carles Puigdemont and the Catalan Separatist party which accounted for 21% of overall social media exposure due to their separatist claims and radical opinions (Simonet & Jamieson, 2019). Interestingly, these loopholes have been exploited by external players who use automated or paid users to contribute to the further distribution of disinformation and disruption of the democratic process.

Another threat that the EU confronted was the suppression of voter turn-out. This tactic, which relies on the distribution of wrong online information about voting procedures, was previously employed in the 2016 US presidential election where harmful online groups managed to successfully deter American voters from participating in the democratic process. Moreover, as the 2014 European Parliament elections indicated, the EU suffered from overall low voter turnout and citizen interest, as only 42.6% of eligible EU citizens voted. These trends made the EU vulnerable and susceptible to malign attacks capable of amplifying further already existing negative patterns and the overall perception of these elections as “second-order elections” (Bendiek & Schulze, 2019). These risks were especially present in Central and Eastern European countries that had the lowest turnout rate in the elections.

4. The European Response to Disinformation on Social Media

Given the plethora of threats and windows of opportunities, the EU adopted a multi-faceted response that incorporated legal (state legislation, self-regulation by the social network providers, and core regulation), technological (use of artificial intelligence), and social means (fact-checking, media literacy, and supporting quality journalism) (European Commission, 2020a). As noted in the previous section, the EU had already adopted corresponding legislation and created operational instruments that focused on the fight against disinformation. Considering the success of these practices, the EU followed a similar but more ambitious approach in 2018 (Efthymiou et al., 2020). Notably, one should also take into consideration challenges posed by the intergovernmental nature of the European undertaking. As the political analyst James Pamment (2020) points out, “many member states do not acknowledge the issue, do not publicly attribute particular malign activities to the offending adversaries, or are under political pressure to limit support to EU-level activities to counter disinformation.”

A year before the elections, the EU adopted a more focused approach to disinformation with the Code of Practice. What distinguishes the code from other similar endeavors is that it was the first time globally that industry giants, such as Facebook, Google, Twitter, Mozilla, and Microsoft, agreed
voluntarily to self-regulatory standards to fight disinformation (European Commission, 2018a). Following a definition of disinformation, the Code identifies five clusters of action to address the threat: a) scrutiny of ad placements (e.g., avoiding the monetization of disinformation-spreading websites); b) political advertising and issue-based advertising (e.g., more transparent distribution of political advertising); c) integrity of services (e.g., policies regarding the identity of the users); d) empowering consumers (e.g., investment in technological instruments prioritizing authentic information); e) empowering the research community (e.g., support of independent projects to track disinformation). Furthermore, the signatories made sure that the monitoring of development with the commitment of writing an annual public report of their work to counter disinformation, reviewable by a third party (Ibid.).

Later that year, the European Commission also published its Action Plan Against Disinformation (European Commission, 2018b). Specifically, the Communication aimed to assist the task of securing free and fair democratic processes considering the size of the vote. In line with the Code, following the recognition of the threat of disinformation, the Commission set the four pillars which are the bases of its response: a) improving the capabilities of Union institutions to detect and expose disinformation; b) strengthening coordinated and joint responses to disinformation; c) mobilizing private sector to tackle disinformation; d) raising awareness and improving societal resilience (p. 6-11).

Apart from the pillars, it also suggested maintaining the mandate of the East StratCom Task Force and revising the mandates of the Western Balkans and South Task Force (p.5) The Action Plan also introduced a new instrument, the Rapid Alert System that makes it possible to share data and give a coordinate response in Europe against disinformation campaigns. Specifically, the System is intended to link existing monitoring instruments inside and outside of the EU like the Emergency Response Coordination Centre and the EEAS Situation Room, along with the G7 Rapid Response Mechanism and the North Atlantic Treaty Organization. Due to its features, the Rapid Alert System was (and still is) one of the major weapons of the EU against the threat of disinformation not only on the regional but also on the international level.

**Conclusions**

This policy paper offers a brief overview of the hazards for digital democracy stemming from AI and digital tools and how the EU tackled online disinformation on social media ahead of the 2019 European Parliament elections. Indeed, Artificial Intelligence has both positive and negative aspects to its application, and many of both have been demonstrated in the recent EU election. Three of the most
destructive consequences of AI for democracy are the growing trend of disinformation on social campaigns, public office candidates, and foreign influence in elections. In the case of the European Union, the problem of malevolent AI usage was even greater as it had to endure all of the listed items and more. The EU saw an exponential increase in foreign hacking attempts, the mass spreading of fake news through social media, and election manipulation. The size of the vote, with 28 countries participating, made the Parliament’s election not only susceptible to disinformation campaigns but also difficult to “shield” the European voters from potential disinformation or voter suppression. Moreover, the algorithm and the attention-based business model that the social media platforms use facilitated the development of a polarized and fragmented online information space and amplified the visibility of divisive opinions.

To meet these challenges, the EU employed a dynamic and multifaceted response that focused on data protection, transparency, cooperation with the private sector, promotion of diversity and credibility of information, the rise of awareness, and the empowerment of the research community (Nenadic, 2019). Putting it simply, the EU incorporated legal (state legislation, self-regulation by the social network providers, and core regulation), technological (use of artificial intelligence), and social means (fact-checking, media literacy, and supporting quality journalism) (European Commission, 2020a). Specifically, in a united effort to protect the legitimacy and authority of the EU, there was a vast array of initiatives launched that now serve as defenders against the malevolent use of AI such as the Action Plan Against Disinformation, the Rapid Alert System, and the Code of Practice. Furthermore, the EU decided to strengthen pre-existing legislation and instruments like the maintenance of the mandate of the East StratCom Task Force.

Following the election, different civil society studies and journalistic investigations resulted that although present, disinformation on social media was lower than expected. However, it must be noted those numbers can and will likely change in the future. Applications of AI are increasingly being used in daily life and as a result of the digital age, they will continue to dominate in the future. Given that, the EU response offers a map for tackling the issue of disinformation across the web that AI has powered. Starting with Facebook's “War Room” in Dublin, Ireland where a team of political scientists and computer scientists started slowing down and filtering the spread of misinformation on the global platform. Furthermore, there was also an initiative in Brussels that was designed to track and halt hacking attacks that were coming from foreign nations and stop foreign nations from meddling in EU elections. Ultimately, the EU has not remained stagnant, but it has since then adopted two major

References


