The impact of social media on elections: Disinformation and micro-targeting advertising in the 2019 EU Elections

Marret, Christophe

Veröffentlichungsversion / Published Version
Arbeitspapier / working paper

NUPRI Working Paper

WP 04 | julho 2020

The impact of social media on elections

Disinformation and micro-targeting advertising in the 2019 EU Elections

Christophe Marret

Núcleo de Pesquisa em Relações Internacionais

Universidade de São Paulo, Brasil

NUPRI-USP

About the author:
Christophe Marret holds an MBA from EMLyon, France. He is a Master's student at the Institute of International Relations (IRI) of the University of São Paulo (USP), Brazil.

Editor: Daniel Oppermann

Núcleo de Pesquisa em Relações Internacionais
Universidade de São Paulo
Rua do Anfiteatro 181
Colméia Favo 7
Cidade Universitária
05508-060
São Paulo, SP
Brasil

https://www.nupri.com.br
https://nupri.prp.usp.br

Abstract

In 2018, the Facebook/Cambridge Analytica case raised serious concerns on the impact of data protection infringements on electoral processes, both in the 2016 US presidential elections, and in the 2017 UK general elections. The EU seems to have rapidly reacted after this case to adapt its own legislation to this new threat to democracy, especially with the application of the data protection regulation GDPR. This article focuses on two worrying effects of the digital platforms in the electoral context: the viral proliferation of fake news (disinformation), and the unlawful use of citizens' personal data to target specific groups of strategic voters (micro-targeting and profiling). This article concludes that the EU chose the co-regulation approach which seems to be the best way, if better supervised (detecting and swamping fake news with other sources of information): the legislative and coercive approach seems to be counterproductive as it could reinforce the auto-persuasion power of fake news. This paper then focuses on the specific application of the European GDPR in the electoral context and concludes that it was partially successful during the last elections for the European Parliament in May 2019. Finally, this article highlights the bureaucratic approach of the European strategy, evaluates the difficulties to applicate it in a new digital economy, and concludes that it is important to continue developing other types of non-legislative measures to combat the disinformation phenomenon, such as fact-checking education at school, and a better collaboration between public authorities, digital industry, and society.

Keywords: GDPR, European Union, elections, fake news, profiling

Introduction

The Facebook/Cambridge Analytica case concerning the alleged unlawful processing of personal user data acquired from Facebook by the company Cambridge Analytica raised serious concerns on the impact of data protection infringements on the 2016 US presidential elections and the 2017 UK general elections. For the first time, European political leaders and citizens realized that social networks could also be harmful to the democratic process of elections (Potemkina 2019). The institutions of the European Union seem to have rapidly reacted after this case to adapt their own legislation to this new threat to democracy (GDPR, ePrivacy Directive and Regulation project, amendments of key regulations on political parties financing, and framework of actors' responsibilities, being among the most important decisions taken).

This article focuses on two potentially dangerous effects of the digital platforms in the electoral context: the viral proliferation of fake news (disinformation), and the unlawful use of citizens' personal data to target specific groups of strategic voters (micro-targeting and profiling). In both cases, these can manipulate the electoral choice of masses of voters and ultimately interfere with the sincerity of the electoral results (Alemanno 2018).

Based on a limited academic literature and official reports review (Alemanno 2018; Bode and Vraga 2015; Clayton et al. 2019; European Commission 2018b; European Parliament and the Council 2019; Haciyakupoglu et al. 2018; Lewandowsky et al. 2012; Mena 2019; Nyhan and Reifler 2010; Pennycook et al. 2020) this article argues that there are three normative solutions to combat disinformation: the co-regulation, the legislative and the coercive approaches. The European Union chose the co-regulation approach which seems to be the best way, if better supervised (detecting and swamping fake news with other sources of information). On the other hand, the legislative and coercive approaches seem to be counterproductive as they could reinforce the auto-persuasion power of fake news.

This paper then focuses on the application of the 2018 European General Data Protection Regulation (GDPR) in the electoral context and studies how this ambitious regulation can in practice (through the example of Facebook during the last elections for the European Parliament in May 2019) help to reduce the risk of electoral manipulation through micro-targeting and profiling. This paper investigates whether the GDPR was successful on this particular point during the last elections for the European Parliament in May 2019.

Finally, this paper searches to highlight the bureaucratic approach of the European strategy and evaluates the degree of difficulty to enforce it in a new digital economy (for future elections): the advent of the "pluralist model of speech regulation" where the latter is only effective with the goodwill of publicly identified actors. In particular, it is necessary to focus on the new threat of the "satellite" digital campaigns organized by undefined actors and therefore, apparently impossible to be regulated with the current EU model.

For this reason, it seems important to continue developing other types of measures to combat the disinformation phenomenon, such as fact-checking education at school, and a better collaboration between public authorities, digital industry, and society.

Besides this introduction, section one discusses the different approaches to combat fake news on the social networks, section two presents the specific response of the EU to the challenge of the political microtargeting strategies used on those social networks, and section three balances the limits of the EU bureaucratic approach in our digital environment.

Anti-Fake-News Approaches

"Fake news" has a variety of definitions: each of them carries a political message and a vision of how disinformation should be regulated (or not). According to Alemanno (2018), there is not a unique definition. The European Commission, however, defines "fake news" as "verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and in any event to cause public harm". It clarifies that this definition excludes "reporting errors, satire and parody, or clearly identified partisan news and commentary". It distinguishes between verifiably false news and misleading information (European Commission 2018b).

An official report by Facebook defines "fake news" as "a catch-all phrase to refer to everything from news articles that are factually incorrect to opinion pieces, parodies and sarcasm, hoaxes, rumors, memes, online abuse, and factual misstatements by public figures that are reported in otherwise accurate news pieces." After using the term "catch-all" to minimize the scope of the disinformation concept, the same report warns that "the overuse and misuse of the term "fake news" can be problematic because, without common definitions, it is impossible to un-

derstand or fully address these issues" (Weedon, Nuland, and Stamos 2017).

The British public audiovisual group BBC uses the definition "false information deliberately circulated by hoax news sites to misinform, usually for political or commercial purposes" and distinguishes it from false news (UK Parliament and BBC 2017), while the British private media group The Guardian suggests the definition of "fictions deliberately fabricated and presented as non-fiction with intent to mislead recipients into treating fiction as fact or into doubting verifiable fact" (UK Parliament and The Guardian 2017).

Allcott and Gentzkow define "fake news" as "news articles that are intentionally and verifiably false, and could mislead readers" (Allcott and Gentzkow 2017).

Disinformation is far from being a new phenomenon: "before the advent of the Internet, it was seen as propaganda in which the mass media had been a vehicle that was exploited by both state and non-state actors to push messages that distort the opinions and emotions of people largely for the promotion of certain political agenda or ideology". Here are some famous and tragic examples; (i) during the Mark Antony smear campaign circa 44 BC: "Octavian's propaganda campaign against Antony deployed Twitter-worthy slogans etched onto coins to smear Antony's reputation"; (ii) during the 1899-1902 Boer War: "propaganda perpetuated 'the Boer' stereotype during this conflict in South Africa, it was popularised by the British Army to sway British public opinion to support an unpopular war"; (iii) during the 1939-1945 World War II: "Edward Herzstein, in his book The War that Hitler Won (1978), described the Nazi propaganda campaign as 'the most infamous propaganda campaign in history', the Nazis demonised and persecuted Jews so effectively that atrocities were committed with popular support and Holocaust denialism continues in the 21st century" (Herzstein 1978; Posetti and Matthews 2018).

But the novelty lies in its major amplification thanks to the power of internet high speed networking: "(i) internet platforms, which publish content with significantly lower cost, wider reach and rapid circulation; (ii) social media, which enables more people and groups of various persuasions to interact even as they consume, produce and re-circulate content; and (iii) artificial intelligence (AI) agents that automate the work of human propagators" (Haciyakupoglu et al. 2018). We could add here the impacts of (iv) the possible anonymization of the authors and sources of financial funding of certain messages; (v) and the creation of personalized posts ("dark ads") linked to the predicted behavior of each user by the algorithms and based on its collected personal data ("profiling" method) (Rainie, Anderson, and Albright 2017).

Ways to combat disinformation

Alemanno (2018) identifies and evaluates three solutions to combat disinformation on the current social networks platforms, what he calls "a Taxonomy of Anti-fake News Approaches": (i) the State intervention, (ii) the exhaustive accountability of the platforms for all the editorial contents of what is published by third parts on their networks, and (iii) the "swamping" of fake news with various news from other sources and points of views about the same issue on the user's page. According to the author, the first two solutions were counterproductive and resulted in reinforcing the capacity of self-conviction of fake news they claimed to minimize. The third solution, for being a kind of "supervised co-regulation" (a mix of the first two solutions) could be the most efficient way to downgrade the power of fake news (Alemanno 2018).

State intervention

According to this approach, Alemanno (2018) observes that the public authorities are expected to police the social media platforms (and more generally speaking, the media environment). The main risk with this approach lies in the creation of "Ministries of Truth", whose mission would be to "model" the citizens' point of view.

For instance, the European Union has created an official network named "Disinformation Review" (https://euvsdisinfo.eu), and made up of "400-plus experts, journalists, officials, NGOs and Think Tanks in over 30 countries, reporting disinformation articles to EU officials, and then to the public. This network was initially devoted to debunk fake news and Russian propaganda, as part of the East StratCom Team (EEAS: part of the administration of the European Union, focused on proactive communication of EU policies and activities in the Eastern neighborhood and beyond). As an experiment, Alberto Alemanno (2018) submitted a request to the EEAS to know the criteria it uses to identify fake news, and how it communicates about it: the EEAS did not outline any clear criteria. The concern is that "the criteria appear to be vague and subjective and the review violates due process in relation to enlisted sources of information" (Alemanno 2018).

As history counts, there is a great risk of informational slippage with this approach: this is even more true when authoritarian rule comes to power.

Exhaustive accountability of the platforms for all the editorial contents of what is published by third parts on their networks: three national examples

According to the current most prescriptive model, this approach "consists of imposing penalties to entities that engage, not just in content-creation but even mere circulation of 'illegal content'" (Alemanno 2018): this could be done through laws, regulations, or directives.

A good example of this approach is the "German Network Enforcement Act" (effective since January 2018). Under this controversial legislation, social media platforms must remove any "obviously illegal" content (such as hate speech and defamation) within 24 hours of its publication, and must publish detailed reports of this activity: failing that duty, they face harsh fines (from 5 million to 50 million). The UN's Special Rapporteur on Freedom of Expression has expressed his warning about the potential consequences of (self-)censorship of this law (Alemanno 2018).

Alemanno states as well the Italian case where an anti fake-news draft law was introduced in 2017: as for the German approach, the Italian law "would criminalise the posting or sharing of 'false, exaggerated, or tendentious news', imposing fines of up to 5000 on those responsible" (Alemanno 2018), and even prison sentences for incitement to crime or violence. In practice, citizens would be incentivized to report what they consider fake news (posted or shared by any organization or any citizen) on a governmental online portal with as much details as possible. These details would then allow the Italian State Police in charge of cybercrime to fact-check the information and to pursue its authors if "laws were broken" (Alemanno 2018). In a country like Italy where fascist history still lies in everybody's mind, the notion of "denouncement of citizens against other citizens to the government" is not a neutral approach.

The French government, under the impulsion of the President Emmanuel Macron (who suffered online disinformation during his 2017 campaign), also tried to legislate on the issue: the law adopted by the Parliament in late 2018 focuses on the electoral context: the new provisions allow a candidate or party to apply to interim justice to stop (within 48 hours) the dissemination of "false information" during the three months preceding a national ballot. The main digital platforms - Facebook, Twitter and Google - are also obliged to reinforce the fight against the risks of manipulation of information: they have the obligation to provide information on paid political advertisements they publish on their site. They must publish the amount paid for electoral messages, and make available to voters an online register with information on the identity of the promoters of these electoral advertisements (France 24 2018). Again, the threat of the creation of "Ministries of Truth" is close.

The last interesting example: on 29 March 2020, the Brazilian president Jair Bolsonaro posted on both Facebook and Instagram (part of the same corporate group) a video claiming that the drug hydroxychloroquine was working well as a treatment against the Covid-19 virus, in all parts of the world. On the next day, Facebook decided to delete this video from both social networks, as a violation of its policy which provides for the removal of publications "that make false claims about cures, treatments, availability of essential services or about the location or severity of the pandemic outbreak" (Marques 2020). Without prejudging the veracity of the president's statements, one can wonder about the risks of interference in the policy of a country, on the part of a private company (Facebook) which can potentially follow a particular agenda based on the research of its own private interests, and using an internal policy with vague criteria as a pretext.

Under this coercive approach, the legislator and ultimately the court can "either decide what constitutes fake news, or outsource this responsibility immediately to social media" (Alemanno 2018). There is here another limit of this approach, the "pay-as-you-go business model" of the social media platforms: Facebook and Google are remunerated only when a user "clicks" on the political advertisement, so that those platforms are very reluctant about playing the role of arbiters of truth (Alemanno 2018). However, in 2019, Twitter renounced paid electoral advertisements (whilst Facebook reaffirmed them as part of its business model).

Legal measures to target fake news may result in unexpected scenarios: "(i) removing fake news may give rise to the so-called 'Streisand effect', whereby deleting content increases audience attention on it [...], (ii) with the prospect of hefty fines looming over them, social media companies are likely to err on the side of caution by aggressively removing posts, driving healthy discourse underground" (Haciyakupoglu et al. 2018). The first scenario would result in an enhancement of the self-conviction power of fake news amongst the people who believe in them, whilst the second scenario would choke the debate and finally would downgrade the other point of views, through a kind of "self-censorship" of the platforms. In both cases, the cure would be worse than the disease.

Moreover, both approaches contain one other major flaw: "when fake news stories do get denounced

as potentially false, or the interim judge is ready to take action, it is already too late and the story has gone viral" (Alemanno 2018): 24 or 48 hours represent an eternity in the light of the digital information dissemination. As evidence suggests, categorizing a piece of news as fake (and thereby give it greater publicity) gives the latter a boost and spreads its reach even further (Alemanno 2018): again, the "Streisand effect".

The "swamping" of fake news with various news from other sources and points of views about the same issue on the user's page

This latest approach seems counterintuitive, and remains largely overlooked in today's public debate about disinformation regulation. "Instead of killing the story, you surround that story with related articles so as to provide more context and alternative views to the reader. In other words, the social platform hosting the disputed news alters the environment in which that story is presented and consumed" (Alemanno 2018). Facebook has been experimenting since 2017 this functionality on a voluntary basis with its new product "Related Articles": the ambition of the private digital company is to provide an "easier access to additional perspectives and information, including articles by third-party fact checkers" (Su 2017). This "swamping" approach is still on a voluntary basis, but "it could be mandated by law across virtually all social networks" (Alemanno 2018). The idea is to kill the "bubble filters" effect which encloses the user in a flow of information with similar points of views.

However, this method still leaves open the deeper problem of algorithmic accountability (even when done through artificial intelligence): by whom and how will be evaluated news considered as fake? But academic research suggests that this "design-centered" approach could make a real difference in reader's perceptions (Bode and Vraga 2015).

As an alternative way of identifying disinformation, the article of Paul Mena (2019) about "the effect of warning labels on likelihood of sharing false news on Facebook" is very significant. The "flagging" of fake news is done by the proper community of Facebook users. "We find that the flagging of false news may indeed have an effect on reducing false news sharing intentions by diminishing the credibility of misleading information. Furthermore, we find that users may be prone to believing that others are more likely to share false news than themselves, confirming the third-person effect. This study shows that flagging of false news on social media platforms like Facebook may indeed help the current efforts to combat sharing of deceiving information on social media" (Mena 2019). However, it is important to be careful with those results as, less than a decade ago, research showed that corrections of fake news by flagging may actually reinforce false beliefs (Lewandowsky et al. 2012). Studies found this "backfire effect" when exploring the political misperceptions (Nyhan and Reifler 2010). In this way, research has shown that the effects of misinformation may continue to influence attitudes even after false claims have been discredited (Lewandowsky et al. 2012) by flagging. In fact, warning labels may thus help people to distinguish between true and false news stories by stimulating (Lewandowsky et al. 2012), and not affirming what is true or false.

In this context, research has found that warning labels decrease people's willingness to share fake news headlines, although repetition of fake news posts was found to increase the perceived accuracy of false stories even when the stories were labeled as disputed by fact-checkers. Moreover, it was shown that warning labels may lead to a modest reduction in perceived accuracy of false news stories, but also result in unlabeled false stories being seen as accurate (or "implied truth" effect) (Pennycook et al. 2020). Clayton (2019), however, has shown that warning labels are relatively successful in reducing belief in false news and found no evidence of an "implied truth" effect.

The EU approach for the 2019 elections: supervised co-regulation with the "Code of Practice on Disinformation" and legislative threats

In order to prepare the elections of the European Parliament of May 2019, the European Commission published in October 2018 the "EU Code of Practice on Disinformation" (European Commission 2018c). This code is a good example of the European Union approach on the issue of disinformation, based on a "partnership" with the major digital media companies (Facebook, Google, Twitter, Microsoft, Mozilla, et al.). The code is part of a wider action plan against disinformation to "build up capabilities and strengthen cooperation between Member States and EU institutions to proactively address disinformation" (European Commission 2018c). The signatories undertook to some major commitments about: (i) scrutiny of advertisement placements to "reduce revenues of the purveyors of disinformation", (ii) transparency of the origin of the political advertisements (distinct from other editorial content, and, most importantly, with the identification of the actual sponsor and the amounts spent), (iii) integrity of information (to accelerate efforts to close fake and bot accounts), (iv) empowering consumers ("to

invest in technologies to help people make informed decisions", "to prioritize relevant, authentic and authoritative information where appropriate in search, feeds, or other automatically ranked distribution channels", and "to make it easier for people to find diverse perspectives about topics of public interest"), (v) empowering the research community ("to support good faith independent efforts to track disinformation and understand its impact, including the independent network of fact-checkers facilitated by the European Commission", "not to prohibit or discourage good faith research into Disinformation and political advertising on their platforms") (European Commission 2018c).

The code provides key indicators of performance (KPIs), and the signatories commit to deliver an annual account of their work to counter Disinformation in the form of a "publicly available report reviewable by a third party" (European Commission 2018c).

Furthermore, "the signature of the Code of Practice will be followed by an assessment period of 12 months, during which the Signatories will meet regularly to analyze its progress, implementation and functioning" (European Commission 2018c).

Online platforms and trade associations representing the advertising sector have submitted a baseline report in January 2019, setting out the inventory of the measures taken to comply with their commitments under the Code. Between January and May 2019, the EU Commission carried out a targeted monitoring of the implementation of the commitments by Facebook, Google and Twitter with particular pertinence to the integrity of the European Parliament elections in May 2019. In particular, the Commission asked the three platforms (signatories to the Code of Practice) to report on a monthly basis on their actions undertaken to improve the scrutiny of ad placements, ensure transparency of political and issue-based advertising and to tackle fake accounts and malicious use of bots. The Commission published on its website the reports received for the five months together with its own assessment (European Commission and High Representative of the Union for Foreign Affairs and Security Policy 2019).

Analyzing the last reports of May 2019, the European Commission concluded that the major platforms made significant progress on (i) the transparency of political advertising, (ii) the integrity of their services, and (iii) the scrutiny of ad placements. However, the Commission urged the platforms to improve their cooperation with fact checkers in all Member States and to empower users to better detect disinformation. Platforms should also make additional datasets available to the research community (in particular, the Commission claimed an official access to the algorithms for academic purposes). Of all the major platforms, Facebook was the one which needed to progress most (European Commission and High Representative of the Union for Foreign Affairs and Security Policy 2019).

However, in August 2018, Facebook launched a new public report, Ad Library Report, which "lets people see how many political and issues ads were run in a given country – as well as aggregated advertiser spend and top searched keywords in the Ad Library (Facebook 2018).

One additional initiative of Facebook needs to be highlighted: the so-called "EU war room" in Dublin. Facebook built a team of 40 specialists working in an operation center to counter digital threats that would undermine the European Parliament elections (Scott 2019). The team counted with coders, digital engineers and specialists in all of the EU's 24 official languages, and it was split along national boundaries: the digital monitoring was not limited to disinformation but also to illegal content, including hate speech (Hinds 2019).

Partial conclusion and discussion

In an open letter to the European press (Gabriel and King 2019) in February 2019, Mariya Gabriel (European Commissioner for the Economy and the Digital Society) and Sir Julian King (European Commissioner for the Union of Security) reminded that if the results prove to be insufficient, they could propose other measures, including regulatory ones. But many observers doubted the determination of the European Commission, in particular because of the strong lobbying work done by those major platforms in Brussels. According to the data protection NGO Corporate Europe Observatory (2018), "while 2,25 million euros get Facebook rank 19 on the list of corporation's biggest EU lobby budget, it ranks 4th among the corporations with the most lobby meetings at the Commission" in 2017. In March 2019, the UK national newspaper The Guardian, based on the leak of internal Facebook documents, revealed a "secretive global lobbying operation targeting hundreds of legislators and regulators in an attempt to procure influence across the world". The document includes details of how Facebook "lobbied politicians across Europe in a strategic operation to head off 'overly restrictive' GDPR legislation. They include extraordinary claims that the Irish prime minister said his country could exercise significant influence as president of the EU, promoting Facebook's interests even though technically it was supposed to remain neutral" (Cadwalladr and Campbell 2019).

Ahead of the EU elections, the NGO Avaaz con-

ducted a Europe-wide investigation on disinformation on Facebook. The period of the investigation was three months (from February to May 2019) and it concerned six European countries (France, Germany, Italy, Poland, Spain, and the United Kingdom). The investigation of Avaaz was the first of its kind and it was published on May 22, 2019, just one day before the first countries voted. Avaaz reported almost "700 suspect pages and groups to Facebook, which were followed by over 35 million people and generated over 76 million 'interactions' (comments, likes, shares) over the period of three months. Facebook had taken down 132 of the pages and groups reported, together the pages taken down reached 762 million estimated views." Interestingly, the pages removed had more than twice the number of followers compared to the main European far right parties combined (Avaaz 2019).

Between November 2018 and March 2019, SafeGuard Cyber (a private company which develops platforms to detect threats in digital channels) analyzed almost 3,5 million posts on Twitter, Facebook, Instagram, and YouTube to evaluate Russian misinformation campaigns. The report focused on the period of 1-10 March 2019 and on "bad actors" (bots, trolls, and hybrids which are humans using software). To determine misinformation contents, they used a tool that aggregates the data from 155 fact-checking sites (such as "Politifact", "EU vs Disinfo") in 53 different languages and a database containing over 500.000 known troll and bot accounts. The main findings were the following: (i) misinformation agents worked within clear narrative categories; (ii) the message was suited for a European audience (iii) the tendency was to amplify already existing content, rather than creating new content, underlining already existing societal and political tensions (for instance, the most used categories of narrative by Russian misinformation were Brexit in the UK, the "yellow vest" movement and the low popularity of President Macron in France, irregularities about EU funds, and supporting Euroscepticism), (iv) content was often related to hashtags that could have been picked by bots automatically and shared rapidly (like 2,3 posts per second). Real users could also be used to amplify through hashtags; (v) as the narrative exploited existing tensions, some states with lower Eurodeputies representation were bombarded by bad actors' messages. One example are the Netherlands (with about 3% of Eurodeputies allocation in the European Parliament) which received 10% of Russian bad actors, due to the tension around the rise of the Dutch Party for Freedom; (vi) analysing Twitter accounts, they found that 12% of the accounts following Jean-Claude Juncker's official Twitter profile were probably "bad actors". Otavio Freire, the co-founder of SafeGuard Cyber, affirmed to The Guardian that "Our report reinforces the need for a new approach to security, as today's bad actors are not at all hindered by the cybersecurity tactics of yesterday" (Boffey 2019). In conclusion, the report had shown the existence of Russian interference during the European Parliament elections. This was the major fear of the European Union (SafeGuard Cyber 2019).

According to the Commission itself, the European anti fake-news strategy seems to have been relatively successful during the last campaign for the European Parliament of May 2019 (European Commission and High Representative of the Union for Foreign Affairs and Security Policy 2019): so far, no significant case of massive-scale disinformation has been publicly opened. To the contrary, the partnership of the European Commission with the main social media platforms resulted in a better transparency of the political advertising sources both for the users and the regulator. "This has been recognized by independent actors and media as well. A study by the Oxford Internet Institute found that less than 4% of news sources shared on Twitter ahead of the European elections were disinformation content, while mainstream professional news outlets received 34% of shares. According to FactCheckEU, there was less disinformation than expected in the run up to the European elections and it did not dominate the conversation as it did around the past elections in Brazil, the United Kingdom, France or the United States" (European Commission and High Representative of the Union for Foreign Affairs and Security Policy 2019). This innovative approach is based on a partnership, i.e. a supervised co-regulation of the platforms, which run the risk of consistent fines at the European and national scales. This partnership is a shared responsibility of all relevant actors: EU institutions, Member States, private sector/online platforms, fact-checkers, civil society, and researchers: a sort of "ecosystem" to fight political fake news messages. However, the European Commission stated that a lot of progress still needed to be done by the platforms to ensure the sincerity of the electoral results (innovation never stops) and urged the platforms to give academic researchers access to one of their best kept industrial secrets: the algorithm.

The reactive response of the EU to the microtargeting approach

"Microtargeting is a term used in more and more situations: it is brought up anytime a sampling process is based on detailed segmentation of the target audience, mostly in online commercials, but the term was firstly used during American election campaign lobbying. One compelling definition comes from Tom Agan, who defines microtargeting as a way to successfully create personalized messages or offers, correctly estimated of their impact (in regards to sub-grouping) and delivery directly to individuals" (Barbu 2014).

As the European Commission noted in 2018 in its "Commission guidance on the application of Union data protection law in the electoral context", "engagement with the electorate is the basis of the democratic process" (European Commission 2018d). In the history of democracies, parties and candidates have always tried to tailor electoral communication to groups of audiences, considering the specific interests of each of them.

However, as the European Commission notices, "the development of micro-targeting of voters based on the unlawful processing of personal data as witnessed in the case of the Cambridge Analytica revelations is of a different nature. It illustrates the challenges posed by modern technologies, but also it demonstrates the particular importance of data protection in the electoral context. It has become a key issue not only for individuals but also for the functioning of our democracies because it constitutes a serious threat to a fair, democratic electoral process and has the potential to undermine open debate, fairness and transparency which are essential in a democracy. The Commission considers that it is of utmost importance to address this issue to restore public trust in the fairness of the electoral process" (European Commission 2018d).

This innovative approach of the electoral marketing is deeply linked with the problem of disinformation as discussed in the first chapter of this article: drawing the same parallel, the issue of targeting electoral audience was not born with the Internet advent, but novelty lies in its major amplification thanks to the power of internet high speed networking (Haciyakupoglu et al. 2018).

Another challenge is the way the candidate/party manages to constitute its own database of voters' personal data: in the Cambridge Analytica case, the actors clearly used an illicit way to get those data. In particular, the data processor did not get a formal consent of the users for this specific processing and electoral finality (European Commission 2018d).

Here, we should highlight the concept of "profiling": a tool frequently used by the data processors to maximize the impact of their digital microtargeting campaigns. As the European Commission defines it in the same guidance, "profiling is a form of automated data processing used to analyze or predict aspects concerning for instance personal preferences, interests, economic situation, etc. Profiling can be used to micro-target individuals, namely to analyze personal data (such as a search history on [the] internet) to identify the particular interests of a specific audience or individual in order to influence their actions. Micro-targeting may be used to offer a personalized message to an individual or audience using an online service e.g. social media" (European Commission 2018d; European Parliament 2016). The combination of personalized micro-targeting fake news messages based on a profiling process of illicitly acquired personal data can be very harmful to the electoral process and to the sincerity of the electoral results, because it encloses the voter in a flow of erroneous information with few opportunities to get a counter point of view.

As Roberto J. González notices, "according to psychologist Michal Kosinski (personal communication) both sides in the 2016 US presidential election used personality profiling software, and similar tools were also used in Barack Obama's successful 2012 campaign. Furthermore, 'off-the-shelf' products and apps such as IBM Watson, Crystal and Apply Magic Sauce can hypothetically be used to create personality profiles based upon social media information and 'digital footprints'. What is more, computer scientists and psychologists are devising other ways to analyze personalities, including social media profile photos and 'emotional analytics' software that interprets facial expressions with the use of webcams" (González 2017). But Condliffe also relativizes the scope of the profiling as "that there is no concrete evidence to support [or] to suggest that 'psychographics' can be used to significantly influence people's political behavior" (Condliffe 2017).

As the European Commission notices in its 2018 guidance, "micro-targeting" is not an illicit tool (when not using illicit personal data), but the democratic process needs to protect itself from its impact when it produces sufficiently significant effect on individuals: for instance, when personalized messages have "the possible effect to stop individuals from voting, or to make them to vote in a specific way" (European Commission 2018a).

These approaches can impact the decision and psychology of voters, but also result in the rise of "strategic" (Alvarez and Nagler 2000) and "tactic" (Dommett and Temple 2018) votes. In the last UK

general elections in 2017, Katharine Dommett and Luke Temple (2018) highlighted the role of a site name "Swap my Vote" which "uses social media to help pair voters who want to swap, each casting each other's preferred vote where it could count for more" (http://www.swapmyvote.uk).

However, despite all these threats, the results of the last elections of the European Parliament in May 2019 (the first European-scale ones after the entry in force of the GDPR on May 25, 2018), seem not to have been impacted significantly by political micro-targeted advertisements. It is still too early to conclude whether the newly adopted European legislation (mainly the GDPR of 2018) and its supervised co-regulation approach based on partnerships with the major platforms (through the "EU Code of Practice on Disinformation" of September 2018, discussed in the first chapter of this article), had a real and significant impact on this result. But compared to the 2016 US Presidential Elections tainted by the Cambridge Analytica affair, the European Commission noticed that "the preliminary analysis shows that it contributed to expose disinformation attempts and to preserve the integrity of the elections, while protecting freedom of expression. The highest turnout in the past twenty years (50.97%) reflects the interest of the citizens for the Union and its importance for their lives" (European Commission and High Representative of the Union for Foreign Affairs and Security Policy 2019). The European Commission suggested here that the intensive use of social media, for as harmful to democracy they can be, are also a source of democratic vigor for the political parties.

But as the disinformation issue has to be combated, the sensitive personal data of social media users have to be protected to ensure the integrity and sincerity of the elections. And after the Cambridge Analytica affair, the European Union institutions responded very reactively.

Chronology of the EU legislative response

According to Potemkina (2019), the chronology can be described as following: (i) on 19th of March, 2018, the New York Times and The Observer published articles about the leak affair; Facebook admitted (a long time after) that sensitive (or not, Facebook denying this term) personal data of 87 million users had been transmitted to Cambridge Analytica through an application, including 2,7 million Europeans (official figures from Facebook, still contested by Cambridge Analytica). Cambridge Analytica processed these personal data with other sources and "profiling" methods to deduce the political profile of each user. Cambridge Analytica helped the Republican Party to send micro-targeted advertisements to "strategic" American citizens to influence their votes (until now, the impact of this affair on the result of the elections is unclear, according to the academic literature). This affair represented a strong awareness both for EU institutions and civil society; (ii) right after this publication, the European Commission publicly protested and asked for a public audition of the Facebook and Cambridge Analytica board members including Mark Zuckerberg, and for an investigation, using the pretext of the 2,7 million European users who had been impacted; (iii) the EU Commission has been in close contact with the US Federal Trade Commission since March 2018, immediately after identifying the data leak; (iv) Mark Zuckerberg apologized in front of the US Congress on April 11, 2018, and in front of the EU Parliament on May 23, 2018, Facebook accepted to collaborate for a better supervision during the European elections of May 2019; (v) on April 26, 2018, the European Commission published the official communication "Tackling online disinformation: a European Approach", which is the guideline of the EU politics on the issue until now; (vi) on May 25, 2018, the GDPR entered into force (this new regulation had been signed on April 14, 2016); (vii) on June 25, 2018, the European Parliament adopted a resolution to force Facebook to comply immediately with the EU regulation, principally on personal data (GDPR) and communication (e-Privacy Directive), and asked the ENISA (European Union Agency for Cybersecurity) to conduct an audit on the situation; (viii) on September 12, 2018, in his annual "State of the Union Speech" in front of the European Parliament, the President of the EU Commission Jean-Claude Juncker urged the European institutions to take actions for "fair elections" and announced his intention to undertake a number of measures to counter manipulation during the election campaign (Juncker 2018); (ix) in September 2018, under pressure of the European Commission, Google, Facebook, Twitter, Mozilla, and various other private actors signed the "EU Code of Practice on Disinformation" as discussed in the first chapter (European Commission 2018b); (x) to achieve its goals, the European Commission proposed a "security package" to the European Council in Salzburg on September 19 and 20, 2018: the "Commission guidance on the application of Union data protection law in the electoral context" (which is a guidance of the application of the GDPR in the electoral context), and a list of legislative measures to adapt/amend the European laws to this new electoral context (European Commission 2018a): for instance, the European Commission proposed to

amend the 2014 law regulation on funding of European political parties and foundations to allow financial sanctions in case of infringement to the new legislation about disinformation and personal data protection.

The EU legislative data protection framework in the context of elections

According to the EU "Commission guidance on the application of Union data protection law in the electoral context" (European Commission 2018a), the data protection regime in place for the previous 20 years in the EU "suffered in particular from the fragmented application of the rules between the Member States, the absence of any formalized mechanisms for cooperation between national data protection authorities, and the limited enforcement powers of those authorities". The GDPR intends to resolve these issues through (i) the harmonization of key concepts such as consent; (ii) the empowerment of the users with the right to receive information about the processing of their data; (iii) the clarification of the conditions under which personal data can be further shared to third parties; (iv) the introduction of rules on personal data breaches; (v) the establishment of a cooperation mechanism between the different national Data Protection Authorities (DPA) in cross-border cases, the enforcement of their powers; (vi) the creation of the European Data Protection Board (EDPB), which groups all national data protection authorities, as well as the European Data Protection Supervisor, and plays a key role in the application of the GDPR by issuing common guidelines, recommendations and best practices.

In case of infringement of EU data protection rules, DPAs have the powers to investigate (by, for instance, ordering to provide information, carrying out inspections at the premises of controllers and processors) and to correct behavior (by, for instance, issuing warnings and reprimands, or impose a temporary or definitive suspension of the processing). They also have the power to impose fines up to EUR 20 million or, in the case of a company, up to 4% of its worldwide turnover. "In the electoral context, it is probable that the gravity of the infringement and the number of persons affected will be high. This might lead to the imposition of high-level fines, in particular considering the importance of the issue of citizens' trust for the democratic process" (European Commission 2018d).

The "Directive on privacy and electronic communications", or "e-Privacy Directive" (European Parliament and the Council 2002) completes the Union data protection framework, and is relevant in the electoral context as its scope includes rules on the electronic sending of unsolicited communications, including for the purposes of direct marketing. The e-Privacy Directive also lays down rules on the storing of information and on the access to information already stored, such as cookies that may be used to track a user's online behavior, in terminal equipment, like a smartphone or a computer. The Commission's proposal for a Regulation on privacy and electronic communications, the "e-Privacy Regulation", currently under negotiation, is based on the same principles as the e-Privacy Directive. The new regulation will widen its scope beyond traditional telecommunication operators to include internet-based electronic communication services" (European Commission 2018d). The next sub-chapters will present how the European Commission interprets the GDPR and the e-Privacy Directive in the specific context of the elections.

Key obligations and rights of the various actors

According to the EU "Commission guidance on the application of Union data protection law in the electoral context" (European Commission 2018a), the GDPR applies to all actors active in the electoral context such as European and national political parties, European and national political foundations, platforms, data analytics companies and public authorities responsible for the electoral process. They must process personal data (for example names and addresses) (i) lawfully, (ii) fairly, (iii) in a transparent manner, (iv) and for specified purposes only.

The notion of personal data is a comprehensive one: in the electoral context, it will often include "special categories of personal data ("sensitive data"), such as political opinions, trade union membership, ethnic origin, sex life, etc. . . " (European Commission 2018a). Those sensitive data will benefit from a more protective regime.

"Moreover, data analytics can infer "sensitive data" (such as political opinions but also religious beliefs or sexual orientations) from sets of non-sensitive data. The processing of those inferred data also falls within the scope of the GDPR and should therefore comply with all data protection rules" (European Commission 2018a).

Data controllers and processors

The European Commission defines the data controller as "the organization deciding (alone or with others), why and how the personal data is processed: the data processor processes personal data on behalf and under the instructions of the controller" (European Commission 2018a) (it may be the same organization as the data controller, or an

outsourced one). The ultimate liability lies with the data controller, in charge of taking measures appropriate to the risks and who should be able to demonstrate its compliance with the GDPR (European Commission 2018a).
In the electoral context, on the one side, a number of actors can be considered as data controllers: political parties and foundations, individual candidates, national electoral authorities... On the other side, platforms and data analytics companies can be (joint) controllers or processors for a given processing depending on the degree of control they have over the concerned processing.
Companies based outside the EU also have to comply to the GDPR when their processing activities relate both to the offering of goods and services to individuals resident in the EU, and to the monitoring of their behavior in the EU: this is the case of companies outside the EU, contracted by European companies to process the personal data of European electors. If the data processor is not a European organization, it needs to have a representative inside the EU, officially registered by a national DPA (European Commission 2018d).

Special conditions for "sensitive data"
Actors involved in elections (whether data controllers or data processors), can only process personal data (including those obtained from public sources -like social media-) in accordance with the GDPR principle of lawfulness, and, specifically in the electoral context, based on a limited amount of relevant grounds: (i) the consent of the individual; (ii) or the performance of a task carried out in the public interest (with some limitations regarding this second point). In addition, storing information (or gaining access to information already stored) in the terminal equipment (computer, smartphone, through cookies for instance), must be in compliance with the e-Privacy Directive requirements: which means that the user must give his/her consent again.
Public authorities involved in the electoral context have the right to process personal data (lists of electors for instance, containing name, surname, electoral number, physical address, et al.), in order to comply with legal obligations (the organization of the election for instance). Political parties and foundations may do so, only if authorized by the law of a Member State, and only for the purpose of advertising in the electoral context.
The processing of "sensitive data" (like the electoral profile of the individuals) is strictly prohibited by the GDPR (with the exception of the political parties' own members).
The European Commission states that "the purpose of the data processing should be specified at the time of collection" (this is the "purpose limitation" principle), and "can only be further processed for a compatible purpose" (European Commission 2018a). "In particular, when data brokers or social media platforms collect data for commercial purposes, that data cannot be further processed in the electoral context" (European Commission 2018a). Political parties and foundations are responsible to ensure that the data they receive from a third-party have been obtained "lawfully". In this case, the company should clearly ask for the user's consent again (European Commission 2018a).

Transparency
As the European Commission recalls, "the Cambridge Analytica case has shown the importance of fighting opacity and properly informing the individuals concerned" (European Commission 2018a) about what they are contracting, as most of the time they do not know who processes their personal data and for which purposes. According to the GDPR, the data controller has to inform the individuals every time it intends to collect personal data, and at each stage of the processing, with the following information: "(i) the identity of the controller; (ii) the purposes of processing; (iii) the recipients of personal data; (iv) the source of the data when not collected directly from the person; (v) the existence of automated decision-making; (vi) and any further information necessary to ensure fair and transparent processing" (European Commission 2018a). This information has to be provided in a "concise, transparent, intelligible, and easily accessible form, using clear and plain language" (European Commission 2018a). The European Commission recalls that "the incomplete information on the purposes for which the data were collected was a key shortcoming in the Cambridge Analytica case" (European Commission 2018a).
It is here important to question the technical feasibility of providing information to the individuals at "each stage of the processing" of personal data.

Profiling, automated decision-making, and micro-targeting
The European Commission defines profiling as "a form of automated data processing used to analyse or predict aspects concerning, for instance, personal preferences, interests, economic situation, etc. Profiling can be used to micro-target individuals, namely to analyse personal data (such as a search history on internet) to identify the particular inter-

ests of a specific audience or individual in order to influence their actions" (European Commission 2018a). In the commercial context, this can be made through personalized advertisements that appear on our web browser or applications (through the use of cookies saved in the internet browser of the user). As the European Commission recalls, in the electoral context, "the Cambridge Analytica case has shown the particular challenges raised by micro-targeting methods on social media. Organizations can be mining the data collected through social media users to create voters' profiles. This might allow these organizations to identify voters who can be more easily influenced and therefore allow them to exert an impact on the outcome of the elections" (European Commission 2018a).
In this context, the GDPR obliges all data controllers, for instance political parties or data analysts working for them, to inform the individuals on their consequences when they use such techniques. It also provides that "individuals have the right not to be subject to decisions based solely on the automated processing of their personal data" (European Commission 2018a).

Security, accuracy, and impact assessment
The GDPR created a framework of supervision of the data controllers: it requires these latter to notify any personal data breach in their system to their national DPA within 72 hours at the latest. It also states that "when the personal data breach is likely to result in a high risk to the rights and freedoms of individuals, the controller must also inform the individuals affected by that data breach without undue delay" (European Commission 2018a).
The GDPR also states that organisations and actors involved in the electoral process are fully responsible for the accuracy of personal data when these latter are collected and compiled from various sources: "inaccurate data must be immediately erased or rectified and, where necessary, updated" (European Commission 2018a).
Finally, the GDPR requires the data controller to carry out a "data protection impact assessment" before using any data process which "is likely to result in a high risk to the rights and freedom of individuals" (European Commission 2018a): this is the case when a data controller uses the "profiling" methods or when it processes sensitive data on a large scale.

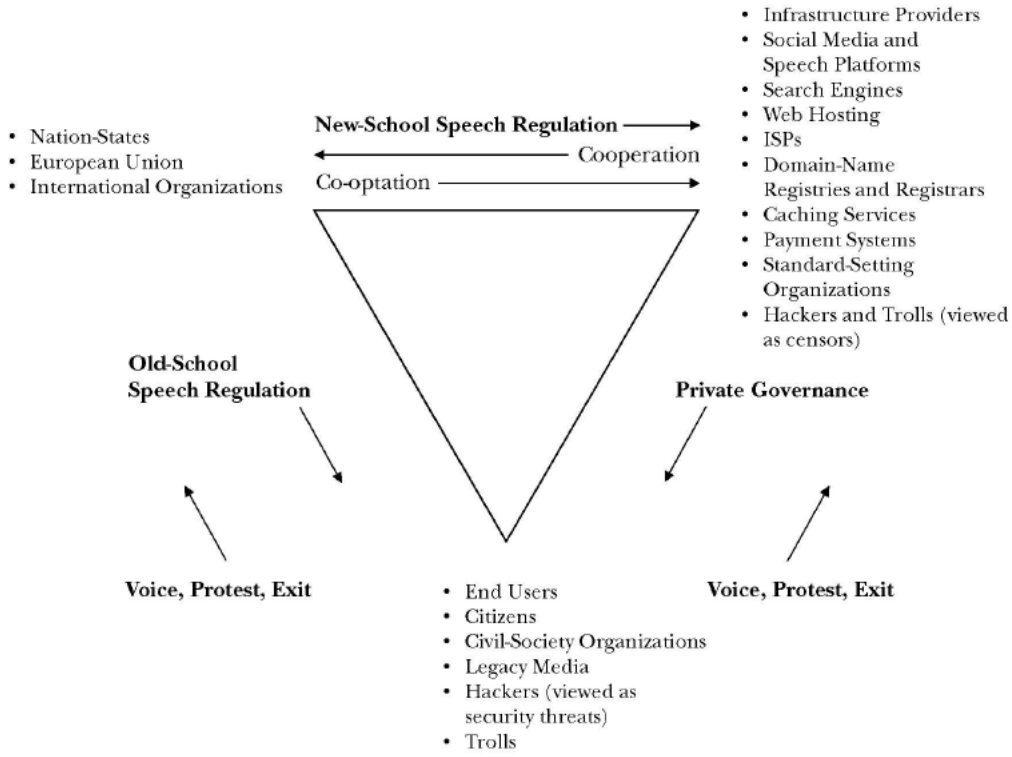
Rights of individuals
To protect the voters, the General Data Protection Regulation "gives individuals additional and stronger rights which are particularly relevant in the electoral context: (i) the right to access their personal data; (ii) the right to request the deletion of their personal data if the processing is based on consent and that consent is withdrawn, if the data is no longer needed or if the processing is unlawful; (iii) the right to have incorrect, inaccurate or incomplete personal data corrected" (European Commission 2018a). The GDPR also concedes (iv) "the right to object to processing" (European Commission 2018a) even if the organisation argues that this process is based on the "legitimate interest" or the "public interest" grounds; (v) "the right not to be subject to decisions based solely on automated processing of the personal data" (European Commission 2018a), that means, when the organisation uses the "profiling" methods; and (vi) "the right to lodge a complaint to a supervisory authority and the right to a judicial remedy" (European Commission 2018a).
All these obligations and rights, derived from the GDPR and e-Privacy Directive, intend to protect the individuals' personal data, and particularly their sensitive ones. It is still too early to completely evaluate the efficiency of these legislative measures, but no very significant case (of the same impact as the Cambridge Analytica case) occurred during the last elections for the European Parliament in May 2019. The European Commission, in its final report of June 2019, congratulates itself for the implementation of these measures and the overall respect of them by the main actors of the political process and communication. The Commission notices that progresses and efforts still need to be made to achieve a better sincerity of the results of the elections. This "pack" of legislative measures seem to achieve, at least partially, the goal that had been assigned: to protect the individuals' personal data in the electoral context, in order to preserve the sincerity and integrity of the election results. In this sense, it seems possible to conclude that the European approach (in comparison with the US approach for instance), constitutes a model (with still some defects and breaches, like every model).
The third and last chapter of this article will discuss the limits of this European model, based on a "bureaucratic" approach, and which seems to be efficient only when the actors are well and publicly defined. But, in the era of artificial intelligence (AI), big data, robots, bots, trolls, which can publish posts to thousands of individuals in seconds, without being well identified by public authorities, how can this model pretend to ensure the protection of individuals' personal data and integrity of the elections in the close future/present time? How can a "bureaucratic" approach still be adequate in a digital

environment dominated by velocity and trackless transfers of information?

The limits of the EU bureaucratic approach in a digital environment

In his article "Free speech is a triangle", Jack M. Balkin (2018) concludes that "the vision of free expression that characterized much of the twentieth century is inadequate to protect free expression today". For the author, the last century featured a dualist model of speech regulation with only two well identified basic kinds of players: territorial governments on the one hand, and private speakers on the other hand. Our new XXIst century is pluralist, with multiple players. "It is easiest to think as a triangle. On one corner are nation-states and the European Union. On the second corner are privately owned internet-infrastructure companies, including social media companies, search engines, broadband providers, and electronic payment systems. On the third corner are many different kinds of speakers, legacy media, civil-society organizations, hackers, and trolls" (Balkin 2018). Figure 1 illustrates this "pluralist model of speech regulation" theory developed by Balkin.

Fig 1. The pluralist model of speech regulation



Source: Balkin 2018, p. 2014

For the author, the "practical ability to speak in the digital world "emerges from the struggle for power between these various forces, with 'old-school', 'new-school', and private regulation directed at speakers, and both nation-states and civil-society organizations pressuring infrastructure owners to regulate speech" (Balkin 2018).

This configuration creates three problems: "first, nation-states try to pressure digital companies through new-school speech regulation, creating problems of collateral censorship and digital prior restraint. Second, social media companies create complex systems of private governance and private bureaucracy that govern end users arbitrarily and without due process and transparency. Third, end users are vulnerable to digital surveillance and manipulation" (Balkin 2018).

The XXth century model of free speech regulation is no longer adapted to the new digital environment: yet, despite all the positive impacts of the EU approach on the electoral context within a digital environment, it seems that this approach is only adapted for a dualist model in transition (toward a triangle model), where the actors are still very well identified (to be supervised, and fined if necessary), and, finally, of good willingness (see the concept of co-regulation that we already discussed in this article). But this European approach does not seem able to regulate the action of robots, trolls, hackers, and others coming from outside the European Union. One thing is to make the data controllers judicially responsible for every piece of information which is published, processed, and for any breach in their enormous databases of personal data (through a quite heavy bureaucratic process which, until now, seems to have been relatively successful); another one is to make sure that, even with this process, the final choices of the individuals will not be altered at the moment of voting because they were exposed to huge volume of disinformation just before closing the electoral process. And nowadays, the conjunction of AI, big data, robots, bots, trolls, and others are able to pass through the regulation, even more, when they come from outside the European Union.

The current threat of campaigns organized by authorities outside the EU: extraterritorial legal application and robots

As Haciyakupoglu states, "to date, most proposed legislation against fake news does not directly address the issue of extraterritorial application. However, some proposed bills do have extraterritorial implications. Germany's Network Enforcement Act mandated the establishment of a local point of contact for transnational technology companies to cooperate with local law enforcement authorities on takedown requests. The proposed Honest Ads Act, although framed generally in terms of protecting US domestic order, targets the role of foreign nationals and seeks to prevent contributions, expenditures, and disbursements for electioneering communications... in the form of online advertising" (Haciyakupoglu et al. 2018). But once again, this would be only efficient in case of defined actors coming from outside the EU. In the case of the Russian interference during the last elections, it has been obviously impossible to clearly identify the responsible organizations behind.

For instance, and as Nikolas K. Gvosdev argues, "considerable evidence exists demonstrating that entities affiliated with and acting at the direction of the Russian Federation have sought to influence the direction and outcome of a series of major elections in Western democracies. These incidents include notably the referendum over whether the United Kingdom should exit the European Union and episodes during the 2016 and 2017 U.S. and French presidential elections" (Gvosdev 2019). How can the European approach limit this "foreign" interference when no organization is clearly identified as the responsible behind this spread of fake news?

New dynamics brought about by technological advancements is a concern for governments which want to use their laws to fight fake news. Ministers of Justice in three German states, for example, have proposed anti-botnet legislation to reduce the impact of automated social media accounts in disseminating fake news. Haciyakupoglu states another case, "Jenna Abrams, a popular Twitter account that attracted up to 70,000 followers through its support for US President Donald J. Trump and advocacy of far-right views, for example, is believed to have been run by the Russian propaganda machine to discredit the Democrats. The role of automated accounts in influencing elections was raised during the US Senate hearings as well" (Haciyakupoglu et al. 2018).

The GDPR does not specifically address this issue and makes again the social media platforms solely responsible (they would have to delete fake and robot accounts). But, in fact, the only possible retaliation measure would have been to condemn the social media which published such fake news, sent in high volume and velocity by robots. As discussed, "when fake news stories do get denounced as potentially fake, or the interim judge is ready to take action, it is already too late and the story has gone viral" (Alemanno 2018).

Finally, one can consider that the European Commission itself acknowledged that it was a lost battle (with the protection tools as of today), investing

massive amounts of financial resources in education, communication, counter-information (through the website https://euvsdisinfo.eu for instance), and forming the EU East StratCom Taskforce in 2015 to counter Russia's disinformation campaigns (Haciyakupoglu et al. 2018).

The new threat of "satellite campaigns" organized by undefined actors within the EU

Katharine Dommett and Luke Temple, investigating the 2017 general elections in the UK (to decide which government would implement the voted Brexit), focused on a new development in the online electoral campaigns: the increased visibility of digital infrastructure offered by non-party organizations to encourage voting and campaigning. For instance, the authors note that "innovations such as Momentum's "My Nearest Marginal" app [1], fundraising sites such as "CrowdPac", and campaigning hubs like the "Progressive Alliance" or "Campaign Together" were seen to empower and connect individuals to contribute to electoral campaigns via non-traditional routes" (Dommett and Temple 2018). All these organizations are located in the UK, all are close to the Labour Party; however, none of them has contractual or juridical links with the Party. "It suggests that, in addition to Whiteley and Seyd's categories of the central party campaign, centrally coordinated local campaigns, and purely locally directed campaigns, we can also identify campaigns originating beyond party structures and control: those termed here 'satellite' campaign" (Dommett and Temple 2018).

One of the benefits of satellite campaigns is the potential for innovation: as organizations less restricted by legal requirements and responsibilities (they are not considered as political parties or foundations in the scope of the GDPR for instance), these bodies have the space to innovate and trial new tools that traditional parties may be wary of promoting: the example of the UK site "Swap my vote", already discussed here, is significant.

The main issue of the rise of this "citizen-initiated campaigning", in the electoral context, is that they are not considered as official political parties, but, in fact, they do act like political parties.

The GDPR seems to be efficient in a digital environment where every actor plays without a mask, and with a certain transparency. When it deals with robots, botnets, hackers, or even "citizen-initiated" campaigns, i.e. when it is impossible (or very complicated, or very time consuming) to identify the responsible organization behind the campaign, the European approach as of 2019 seems to be useless.

Conclusion

Disinformation and illicit profiling strategies become a national security issue when they undermine the foundations of the nation state. In this regard, fake news could serve as a tool for disinformation campaigns at a massive-scale: the intentional dissemination of false information for influencing opinions or policies of the receiving audience. It is currently too early to assess definitively the impacts of the European legislative initiatives against fake news and illicit profiling strategies. As Haciyakupoglu states, "any attempt to legislate against fake news would inevitably meet with difficulties given: (i) issues on the definition of fake news, (ii) global dimension of the cyberspace vis-a-vis the territorial boundaries of legislation, (iii) challenges in identifying the actual perpetrator of fake news, and (iv) sophistication of disinformation campaigns" (Haciyakupoglu et al. 2018). It seems urgent to "reconcile" online regulations with offline regimes (example of pornography which is prohibited in some countries, but publicly accessible on the internet, and the controversial use of VPN) (Haciyakupoglu et al. 2018).

The European Union has launched a "pack" of legislative measures and co-regulation system with the social media platforms to combat the disinformation and illicit profiling phenomenons in electoral context, which seems to be, until now, the most "avant-gardist" and efficient approach, in the current state of the art and according to the literature. However, progress and efforts still need to be made by all actors to follow the race for innovation launched by the protagonists of disinformation. In spite of all possible efforts, it seems that the technology always will have a head start over legislation.

This is why, in spite of these necessary (but not sufficient) legislative measures, it seems urgent to continue developing other types of measures, on the short, and long terms. On the immediate term, it is important to continue developing (i) fact-checking efforts, (ii) counter fake news websites and communication, (iii) fake news flagging directly on the social media platforms (potentially with the help of algorithms, artificial intelligence and machine learning). On the long term, it seems important to develop measures to: (i) promote the ability of (social) media decryption in the education of chil-

[1] My Nearest Marginal is an application used in the 2017 UK elections by the Momentum movement (a British political organisation described as a grassroots movement supportive of the Labour Party) to direct activists flooding into strategic "swing" constituencies (Rees 2017).

dren at school (it will be helpful for adults too), (ii) support new social practices against fake news such as the individual responsibility before sharing messages (checking and authenticating the sources and author, reading the information extensively), and (iii) to clearly define the responsibilities of the technology companies (Haciyakupoglu et al. 2018). It is important to consider the creation of a new ecosystem to fight fake news in the electoral context: (i) a State able to define new rules of conduct for the electoral campaigns, which protects the data of its citizens by law, and which imposes a minimum of transparency rules to the social media platforms, (ii) technology companies aware of their social and democratic responsibilities, which autoregulate themselves (under the State supervision), and which collaborate with the civil society sharing useful research data, and (iii) a civil society (users -individuals and organizations-, scientific research) which fully assumes its role as a controller of both the State and the private technology companies. Considering all those elements, the approach of the European Commission to protect the sincerity of the election results for the European Parliament in May 2019 seems to have brought some interesting progress in the vast debate of personal data protection through: (i) a reactive answer to the Cambridge Analytica affair, (ii) a regional collaboration of all the national DPAs, (iii) an incentive to the NGOs and journalists consortiums to develop fact-checking platforms, and (iv) an innovative partnership based on co-regulation with the main social media platforms. In addition, it is important to highlight the growing necessity of a more transparent governance at the head of the social media companies, especially in their policy of posts validation criteria, and, to be more exhaustive, in the construction of their algorithms.

References

Alemanno, Alberto (2018). "How to Counter Fake News? A Taxonomy of Anti-fake News Approaches". In: *European Journal of Risk Regulation* 9.1, pp. 1–5.

Allcott, Hunt and Matthew Gentzkow (2017). "Social Media and Fake News in the 2016 Election". In: *Journal of Economic Perspectives* 31.2, pp. 211–236.

Alvarez, R. Michael and Jonathan Nagler (2000). "A New Approach for Modelling Strategic Voting in Multiparty Elections". In: *British Journal of Political Science* 30.1, pp. 57–75.

Avaaz (2019). *Far Right Networks of Deception*. Avaaz Report, 22 May 2019. URL: https://secure.avaaz.org/campaign/en/disinfo_network_report/ (visited on 10/10/2019).

Balkin, Jack M. (2018). "Free Speech is a Triangle". In: *Columbia Law Review* 118.7, pp. 2011–2056.

Barbu, Oana (2014). "Advertising, Microtargeting and Social Media". In: *Procedia - Social and Behavioral Sciences* 163, pp. 44–49.

Bode, Leticia and Emily K. Vraga (2015). "In Related News, That Was Wrong: The Correction of Misinformation Through Related Stories Functionality in Social Media". In: *Journal of Communication* 65.4, pp. 619–638.

Boffey, Daniel (May 8, 2019). *241m Europeans 'may have received Russian linked disinformation'*. The Guardian, London. URL: https://www.theguardian.com/world/2019/may/08/241m-europeans-may-have-received-russian-linked-disinformation (visited on 10/10/2019).

Cadwalladr, Carole and Duncan Campbell (Mar. 2, 2019). *Revealed: Facebook's global lobbying against data privacy laws*. The Guardian, London. URL: https://www.theguardian.com/technology/2019/mar/02/facebook-global-lobbying-campaign-against-data-privacy-laws-investment (visited on 10/10/2019).

Clayton, Katherine et al. (2019). "Real Solutions for Fake News? Measuring the Effectiveness of General Warnings and Fact-Check Tags in Reducing Belief in False Stories on Social Media". In: *Political Behavior* (11 February). URL: https://link.springer.com/article/10.1007/s11109-019-09533-0 (visited on 03/30/2020).

Condliffe, Jamie (Feb. 27, 2017). *The Right-Wing Propaganda Machine May Not Be as Smart as You Think*. MIT Technology Review. URL: https://www.technologyreview.com/2017/02/27/153532/the-right-wing-propaganda-machine-may-not-be-as-smart-as-you-think/ (visited on 06/23/2020).

Corporate Europe Observatory (May 21, 2018). *Post-scandal Facebook: will the EU stop treating the tech giant as a trusted partner?* URL: https://corporateeurope.org/en/power-lobbies/2018/05/post-scandal-facebook-will-eu-stop-treating-tech-giant-trusted-partner (visited on 10/10/2019).

Dommett, Katharine and Luke Temple (2018). "Digital Campaigning: The Rise of Facebook and Satellite Campaigns". In: *Parliamentary Affairs* 71.suppl_1, pp. 189–202.

European Commission (Sept. 12, 2018a). *Commission guidance on the application of Union data*

protection law in the electoral context. Guidance Document, COM (2018) 638 final. URL: https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-data-protection-law-electoral-guidance-638_en.pdf (visited on 06/23/2020).

European Commission (Apr. 26, 2018b). *Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee, and the Committee of the Regions Tackling Online Disinformation: A European Approach*. COM (2018) 236 final. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236 (visited on 06/23/2020).

– (Sept. 2018c). *EU Code of Practice on Disinformation*. URL: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=54454 (visited on 06/23/2020).

– (Sept. 12, 2018d). *Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU, Euratom) No 1141/2014 as regards a verification procedure related to infringements of rules on the protection of personal data in the context of elections to the European Parliament*. COM (2018) 636 final/2 2018/0336 (COD). URL: https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-protection-data-elections-regulation-636_en.pdf (visited on 06/23/2020).

European Commission and High Representative of the Union for Foreign Affairs and Security Policy (June 14, 2019). *Report on the implementation of the Action Plan Against Disinformation*. URL: https://eeas.europa.eu/sites/eeas/files/joint_report_on_disinformation.pdf (visited on 06/23/2020).

European Parliament (Apr. 27, 2016). *Regulation 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)*. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R0679-20160504 (visited on 06/23/2020).

European Parliament and the Council (July 12, 2002). *Directive 2002/58/EC*. EUR-Lex. URL: http://data.europa.eu/eli/dir/2002/58/2009-12-19 (visited on 06/23/2020).

– (Mar. 25, 2019). *Regulation (EU, Euratom) 2019/493 of the European Parliament and of the Council - of 25 March 2019 - amending Regulation (EU, Euratom) No 1141/2014 as regards a verification procedure related to infringements of rules on the protection of personal data in the context of elections to the European Parliament*. PE/14/2019/REV/1. URL: http://data.europa.eu/eli/reg/2019/493/oj (visited on 06/23/2020).

Facebook (Aug. 1, 2018). *Facebook Ad Library*. URL: https://www.facebook.com/ads/library/ (visited on 04/03/2020).

France 24 (Nov. 21, 2018). *Ce que contient la loi française contre les "fake news"*. URL: https://www.france24.com/fr/20181121-loi-contre-fake-news-definitivement-adoptee-macron-election (visited on 04/05/2020).

Gabriel, Mariya and Julian King (Feb. 28, 2019). *Désinformation: Facebook, Twitter et Google doivent mieux faire*. Les Echos. URL: https://www.lesechos.fr/idees-debats/cercle/desinformation-facebook-twitter-et-google-doivent-mieux-faire-994700 (visited on 10/10/2019).

González, Roberto J. (2017). "Hacking the citizenry?: Personality profiling, 'big data' and the election of Donald Trump". In: *Anthropology Today* 33.3, pp. 9–12.

Gvosdev, Nikolas K. (2019). "Is Russia Sabotaging Democracy in the West?" In: *Orbis* 63.3, pp. 321–333. (Visited on 03/30/2020).

Haciyakupoglu, Gulizar et al. (2018). *Countering Fake News: A Survey of Recent Global Initiatives*. S. Rajaratnam School of International Studies, Policy Report, March. URL: http://hdl.handle.net/11540/8063 (visited on 06/24/2020).

Herzstein, Robert (1978). *The war that Hitler won: the most infamous propaganda campaign in history*. New York: Putnam.

Hinds, Shari (2019). "The European Union approach to disinformation and misinformation. The case of the 2019 European Parliament elections". M.A. Thesis. University of Strasbourg. URL: https://doi.org/20.500.11825/1103 (visited on 06/24/2020).

Juncker, Jean-Claude (Sept. 12, 2018). *State of the Union 2018. The Hour of European Sovereignty*. European Commission. URL: https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-speech_en.pdf (visited on 06/23/2020).

Lewandowsky, Stephan et al. (2012). "Misinformation and Its Correction". In: *Psychological Science in the Public Interest* 13.3, pp. 106–131.

Marques, José (Apr. 1, 2020). *Facebook apagou post de Bolsonaro por 'alegação falsa' de cura para coronavírus*. Folha de São Paulo, São Paulo. URL: https://www1.folha.uol.com.br/poder/2020/04/facebook-apagou-post-de-bolsonaro-

por-alegacao-falsa-de-cura-para-coronavirus.shtml (visited on 04/04/2020).

Mena, Paul (2019). "Cleaning Up Social Media: The Effect of Warning Labels on Likelihood of Sharing False News on Facebook". In: *Policy & Internet* 12.2, pp. 165–183.

Nyhan, Brendan and Jason Reifler (Mar. 30, 2010). "When Corrections Fail: The Persistence of Political Misperceptions". In: *Political Behavior* 32, pp. 303–330.

Pennycook, Gordon et al. (2020). "The Implied Truth Effect: Attaching Warnings to a Subset of Fake News Headlines Increases Perceived Accuracy of Headlines Without Warnings". In: *Management Science*. URL: https://doi.org/10.1287/mnsc.2019.3478 (visited on 06/24/2020).

Posetti, Julie and Alice Matthews (2018). *A Short Guide to History of Fake News and Disinformation*. International Center for Journalists. URL: https://www.icfj.org/news/short-guide-history-fake-news-and-disinformation-new-icfj-learning-module (visited on 06/23/2020).

Potemkina, Olga (2019). "Regulation of Social Networks in the Upcoming Elections to the European Parliament". In: *Contemporary Europe* 2.88, pp. 50–61.

Rainie, Lee, Janna Anderson, and Anderson Albright (Mar. 29, 2017). *The Future of Free Speech, Trolls, Anonymity, and Fake News Online*. Pew Research Center. URL: https://www.pewresearch.org/internet/2017/03/29/the-future-of-free-speech-trolls-anonymity-and-fake-news-online/ (visited on 06/29/2020).

Rees, Emma (June 12, 2017). *What made the difference for Labour? Ordinary people knocking on doors*. The Guardian, London. URL: https://www.theguardian.com/commentisfree/2017/jun/12/labour-knocking-on-doors-jeremy-corbyn-momentum (visited on 05/04/2020).

SafeGuard Cyber (2019). *Contactless Actions against the Enemy*. URL: https://www.safeguardcyber.com/blog/the-bots-never-left-how-russia-is-using-social-media-to-influence-european-parliamentary-elections (visited on 10/10/2019).

Scott, Mark (May 5, 2019). *Inside Facebook's European election war room*. Politico. URL: https://www.politico.eu/article/facebook-european-election-war-room-dublin-political-advertising-misinformation-mark-zuckerberg/ (visited on 10/10/2019).

Su, Sara (Apr. 25, 2017). *New Test With Related Articles*. Facebook Newsroom. URL: https://about.fb.com/news/2017/04/news-feed-fyi-new-test-with-related-articles/ (visited on 06/24/2020).

UK Parliament and BBC (Mar. 2017). *Written evidence submitted by the BBC*. FNW0114. URL: data.parliament.uk/WrittenEvidence/CommitteeEvidence.svc/EvidenceDocument/Culture,%20Media%20and%20Sport/Fake%20News/written/48758.html (visited on 10/10/2019).

UK Parliament and The Guardian (Mar. 2017). *Written evidence submitted by Guardian News & Media*. FNW0096. URL: data.parliament.uk/WrittenEvidence/CommitteeEvidence.svc/EvidenceDocument/Culture,%20Media%20and%20Sport/Fake%20News/written/48259.html (visited on 10/10/2019).

Weedon, Jen, William Nuland, and Alex Stamos (Apr. 27, 2017). *Information Operations and Facebook*. Facebook. URL: https://www.semanticscholar.org/paper/Information-operations-and-Facebook-Weedon-Nuland/f633771f0f586aaa89120a9003e2b24dddaf4d89 (visited on 06/24/2020).