DISINFORMATION AND ELECTORAL CAMPAIGNS

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Disinformation and electoral campaigns

Yves-Marie Doublet

Directorate General of Democracy
Democratic Governance
Division of Electoral Assistance

Council of Europe

French edition:
Désinformation et campagnes électorales
ISBN 978-92-871-8910-3

The opinions expressed in this work are the responsibility of the author and do not necessarily reflect the official policy of the Council of Europe.

Cover and layout: Documents and Publications Production Department (SPDP), Council of Europe

Cover photo : © Depositphotos

Council of Europe Publishing
F-67075 Strasbourg Cedex
http://book.coe.int

ISBN 978-92-871-8911-0

Printed at the Council of Europe

Contents

Introduction

1. The Cambridge Dictionary defines fake news as "false stories that appear to be news, spread on the internet or using other media, usually created to influence political views or as a joke".

2. Since the summer of 2016, fake news has denoted the deliberate viral spreading of false news on the internet and social media.[1] It includes fabricated content, manipulated content, imposter content, misleading content, false context or connection, satire and parody. It has therefore taken a variety of meanings. *The Guardian* was the first newspaper to mention the small city of Veles in Macedonia where it originated. Veles was the place where political websites used clickbait – which is used to encourage visitors to click on a link to a particular web page – to make money from Trumpmania during the American electoral campaign in 2016. More than 100 sites posting fake news were run by teenagers in this town. An investigation led by the American website Buzzfeed on 3 November 2016, some days before the US presidential election, explains the success of the phenomenon: "The best way to generate buzz is to share political publishing on Facebook with sensationalist and often wrong content, which may please Trump supporters".[2]

3. This way of working leads to the distinction between misinformation, disinformation and propaganda, precisely described by the American researcher Renee DiResta, Head of Policy at Data for Democracy.[3] Misinformation refers to incorrect or wrong information delivered by journalists without any malicious intention. Disinformation is a deliberate attempt to make people believe things which are not accurate. Disinformation involves fabricated information blended with facts and practices that go well beyond anything resembling news, to include automated accounts used for networks of fake followers, manipulated videos or targeted advertising.[4] This technique is spread by one group to target another group and mislead readers.

4. In this hierarchy of different ways of communication, propaganda denotes information with a specific agenda which is spread by a government, co-operatives or

1. "Fake News–Definition und Rechtslage", Wissenschaftlicher Dienste, Deutscher Bundestag, 2017.
2. "L'histoire vraie des *fake news*", *L'Opinion*, 1315, 7 August 2018.
3. "How do we know what's true anymore?", YouTube, 13 April 2018.
4. "A multi-dimensional approach to disinformation", Report of the Independent High Level Expert Group on Fake News and Online disinformation, European Commission, 12 March 2018.

people. In November 2017, the British Prime Minister stated that planting fake news was a way to "weaponise information".[5] All these different channels are often lumped together under the banner of fake news, but means and intentions differ from one type of information to another. From a social point of view, fake news contributes to forming communities of people who have access to the same opinions, and share the same ideology and the same conspiracy theories.[6]

5. Fake news may take several forms: it may consist of statements, the expression of opinion without any evidence, or hate speech against social groups or minorities. Even if the initiative behind such manipulation of public opinion is private in origin, some governments attempt to control social media to shape public opinion and to counter opposition and criticism.

6. Over the past few years, this practice, which hampers citizens from making informed decisions, has become more widespread. The impact of this phenomenon is especially significant because its diffusion is extremely quick and the identification of the authors of such campaigns and digital material is very difficult.

7. Several factors explain the development of fake news.

The impact of social media – In 2016, active Facebook users amounted to 2 billion per month and Twitter had 400 million users. There are about 1.8 billion monthly users of YouTube. In its Digital News Report 2018, the Reuters Institute for the Study of Journalism considers Facebook to be by far the most important network for finding, reading, watching and sharing news, even if its usage fell from 42% in 2016 to 36% in 2018. In the US, 62% of adults obtain news from social media.[7] For every age group under 45, online news is more important than TV news.

The methods and their speed – Facebook has created a targeting paradigm enabling political parties during electoral campaigns to access more than 162 million US users and to target them individually by age, gender, congressional district and interests.[8] It has been stressed that digital media uses an algorithm process to target both customers and voters. Bot accounts are used to influence political discourse. They tweet and retweet with likes and followers to reach a large audience, but these likes and followers are often artificial. Moreover, a recent study by the Massachusetts Institute of Technology showed that false news spreads quicker than real news. According to this study, false news stories are 70% more likely to be retweeted than true stories, and it takes true stories about six times as long to reach 1 500 people as it does for false stories to reach the same number of people.[9]

The costs – This has become cheaper and is based on a short-term strategy which does not care to build a reputation for quality. To finance propaganda on social networks, you just need 40 000 euros; 5 000 euros is enough to buy a hate speech initiative

5 Buchan L. "Theresa May warns Russia over election meddling and vows to protect the UK", *The Independent*, 13 November 2017.

6. Zizek S.,"Fake News, Wohin das Auge reicht", *Neue Zürcher Zeitung*, 6 August 2018.

7. Allcott H. and Gentzkow M., "Social Media and Fake News in the 2016 Election", *Journal of Economic Perspectives*, Volume 31, Number 2, 2017, pp. 211-236.

8. Chester J., "The role of digital marketing in political campaigns", Internet Policy Review, Center for Digital Democracy, Washington DC, 31 December 2017.

9. http://news.mit.edu/2018/study-twitter-false-news-travels-faster-true-stories-0308.

and with 2 600 euros you can buy 300 000 followers on Twitter.[10] False and harmful information is produced for profit. In this manner, a marriage was forged between digital companies and media businesses for several years, and political campaigns have combined voters' profiles with commercial information from data brokers. This development has favoured the growth of data-driven political marketing and may have significant effects on society, fair elections and democracy.

8. This trend raises a number of questions. Is fake news so different from false information that was used in the past, for instance during the Cold War by both superpowers? Do social media change practices which are traditionally enforced during electoral campaigns? Has fake news had a real impact on the outcome of elections? Should we view these practices as inevitable side effects of a technological shift, also because they are difficult to regulate? Should the response to this phenomenon rely on a self-regulatory approach or does it require strict rules – especially if a self-regulatory approach reveals itself to be ineffective, in particular when these practices are carried out outside the territory where elections take place? Does such a regulatory approach comply with the principle of freedom of expression? What kinds of legal tools have been introduced in different member states of the Council of Europe or in other countries to counter fake news? What lessons can be drawn from these experiences? How is the protection of the privacy of citizens guaranteed? Should legal action be taken at international level, given the numerous cases of destabilisation of election campaigns recently recorded in various countries? Besides a possible regulatory framework, how can public awareness be enhanced about the authenticity of information and the need for fact-checking, in addition to encouraging more discerning editorial judgment in media outlets?

9. This report attempts to answer these questions and offer proposals for shaping a legal framework at the level of the Council of Europe.

10. www.assemblee-nationale.fr/15/pdf/rapports/r0990.pdf.

1. General overview of the situation

10. The fake news issue may be considered from both technical and political perspectives.

1.1. Technical data

11. To provide an awareness of the importance of technical issues in this context, we should remind ourselves of the various techniques that can be used in social media.

12. Studies show that more people are discovering news through algorithms (search, social and other aggregates)[11] than through editors and those algorithms are exposing most users to a greater range of online sources. Algorithms are not neutral. They have been conceived with maximum accuracy precisely to choose, sort, classify, rank, filter, target and order the available information or breaking news. They are a way of organising information on a large scale by enhancing certain aspects of it. Computational algorithms have recourse to machine learning to produce an output. Machine learning algorithms are used as generalisers, providing them with data from which they will be able to learn. The algorithm makes its own decisions regarding the operations to be performed to accomplish the task in question. This technique makes it possible to carry out much more complex tasks than a conventional algorithm. Andrew Ng, of Stanford University, defines machine learning as follows: "the science of getting computers to act without being explicitly programmed". This encompasses the design, analysis, development and implementation of methods enabling a machine to operate via a systematic process, and to accomplish difficult tasks.

A real business model relying on monetised data collection and supervision of individual online behaviour has been developed.[12] Samantha Bradshaw, from the Oxford Internet Institute, told the Digital, Culture, Media and Sport Committee of the

11. Newman N., "Executive Summary and Key Findings", *Reuters Institute Digital News Report 2017*.
12. *How can humans keep the upper hand? The ethical matters raised by algorithms and artificial intelligence*, Commission nationale informatique et libertés, December 2017: available at www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_ai_gb_web.pdf.

House of Commons about the power of Facebook to manipulate people's emotions by showing different types of stories to them: "If you showed them more negative stories, they would feel more negatively. If you showed them positive stories, they would feel more positive".[13] It is worth reminding ourselves that the Oxford Dictionary's Word of the Year 2016 was "post-truth", an adjective defined as relating to or denoting circumstances in which objective facts are less influential in shaping public opinion than appeals to emotion and personal belief. The use of data analytics, based on the psychological profile of the audience, was for instance at the heart of the work of Cambridge Analytica, born in 2012 out of the already established SCL consultancy group, whose work involved "presenting a fact that is underpinned by an emotion".

13. The former CEO of Cambridge Analytica testified before the above-mentioned committee:

> In order to match the right type of message to voters, Cambridge Analytica needed information about voters, such as what merchandise they bought, what media they read, what cars they drove. *The Guardian*, following investigations lasting about a year, wrote: "[Cambridge Analytica] … paid researchers at Cambridge University to gather detailed psychological profiles about the US electorate using a massive pool of mainly unwitting US Facebook users built with an online survey.[14]

To target voters and to direct the messages campaigners want to disseminate, tools tailored to specific groups are called "micro-targeting" tools. The term "dark ads" has also been used to describe micro-targeting.

14. Experts use the "political echo chamber" as a metaphor for online "clicks" that result in the political "bubble" people can get themselves into while using online services. The following is an example of how algorithmic feeds encourage bias.

> If you read liberal news sources – or even just have predominantly liberal friends – Facebook will show you more liberal-leaning news. The same thing happens for conservatives and even the most fringe members of the political spectrum. In short, this algorithmically enforced confirmation bias means the more you read information you agree with, the more Facebook will show you even more information you agree with. ... The more you hear the same perspectives from the same sources, the more it reinforces your ideas without ever challenging them.[15]

15. But data and algorithms "are opaque in the sense that if one is a recipient of the output of the algorithm, he does not have any concrete sense of how or why particular classification has been arrived at from inputs. Additionally, the inputs themselves may be entirely unknown or known only partially".[16] Stirista, a digital marketing firm, offers lookalike modelling to identify people who are potential supporters and voters. The company claims it has matched 155 million voters to their "email addresses, online cookies and social handles" as well as "culture, religion, interests, political positions and hundreds of data points to create rich, detailed voters' profiles".[17] If someone's political conviction is not always shaped by algorithms, algorithms may be used to

13. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/363.pdf.
14. Ibid.
15. https://lifehacker.com/how-sites-like-google-and-facebook-put-you-in-political-1787659102.
16. Burrell J., "How the machine 'thinks': Understanding opacity in machine learning algorithms", *Big Data and Society*, January 2016, pp. 1-12.
17. Chester J., op. cit.

determine the profile of voters. It became part of a business model because it is a way to earn money.

16. The opacity of algorithms raises two questions: is the outcome a result of the will of the designer of the platform? And is this outcome observable by a user? Some undesirable impacts of algorithms have been set up deliberately but are unknown to users. In such cases, opacity is described as an intentional strategy of secrecy and the manipulation of consumers or voters. It is up to programmers, public authorities, NGOs and journalists to audit these algorithms with their hidden targets. In other cases, these impacts may not have been conceived by the operators and either these impacts have been identified by the users or not.[18]

17. A "bot" is another sophisticated leverage mechanism for influencing voters. It is an automated software program that mimics human behaviour on social media by posting, liking and talking to real people.[19] As one German expert put it: "Social bots are fake accounts on social media who pretend to be real persons".[20] A person who controls just one bot may therefore exert influence on a million people. For example, bots may polarise public opinion through hate speech. In the same hearing before the Bundestag Committee on the Digital Agenda, the expert ranked bots among the techniques associated with "low-quality, high-frequency manipulation". They are different from certain fake news stories associated with "high-quality, slow-frequency manipulation".[21] According to estimates by cloud services provider Imperva Incapsula, bots made up 51.2% of all web traffic in 2016. If many of them have commercial purposes, malicious bots are unidentifiable and can be used for hacking, spamming or stealing content.[22]

18. Under British electoral law, campaigners can purchase bots and pay people to spread their campaign messages, which is misleading if voters cannot see that this has happened.[23]

19. A "troll" is a real person who spends time on the internet and social media, posting divisive or irrelevant messages and comments to annoy or anger other people.[24]

20. Hashtags, which are short codes inserted into messages to make them researchable, are reported during election campaigns. Popular hashtags contain "trending topics", which give access to conversations. Hashtags are manipulated by bots. Hashtags that are reproduced reflect the opinion of very few persons who have a great number of accounts. It gives the impression that they represent many people. Simple short codes lead people to believe that an opinion expresses a largely widespread view.[25]

---

18. Cardon D., "Le pouvoir des algorithmes", *Pouvoirs*, *La Datacratie*, 164, 2018.
19. *Digital campaigning: Increasing transparency for voters*, The Electoral Commission, June 2018.
20. Hegelich S., *Ausschuss Digitale Agenda Fragenkatalog*, Deutscher Bundestag Auschussdrucksache 18 (24) 125.
21. "Fake News, Social Bots, Hacks und Co-Manipulationsversuch demokratischer Willensbildungsprozesse im Netz", Wortprotokoll der 81 Sitzung, 25 January 2017, Deutscher Bundestag.
22. Freedom on the Net 2017: "Manipulating social media to undermine democracy".
23. *Digital campaigning: Increasing transparency for voters*, op.cit.
24. Ibid.
25. "L'histoire vraie des *fake news*", op.cit.

21. In 2011, spending by campaigners on digital advertising amounted to 0.3% of total advertising expenditure in the UK. In 2017, this spending rose to 42.8% of total advertising expenditure.[26]

1.2. Political data

22. Social media has been praised for making democratic information available and for promoting online conversation. It makes political information more accessible and helps voters to make more informed choices. In its judgment of 10 March 2009, in the case of *Times Newspaper Ltd v. the United Kingdom*, the European Court of Human Rights stated that:

> In light of its accessibility and its capacity to store and communicate vast amounts of information, the Internet plays an important role in enhancing the public's access to news and facilitating the dissemination of information generally.[27]

But social media may be misused and may affect political beliefs.

23. In order to identify the influence of networks of fake accounts and bots on votes, research has been conducted on US election campaigns, the referendum on the EU in 2016 in the United Kingdom, the French presidential election, the British and German general elections in 2017 and the Czech presidential election in 2018.

24. During the 2008 and 2012 US presidential elections, Barack Obama's campaign teams had scores of datasets at their disposal on virtually all voters. It is generally admitted that fake news may have contributed to the election of Donald Trump in the 2016 US presidential election. Social media represented 13.8% of the sources of election news during the 2016 US elections. Fake news was both shared and heavily tilted in favour of Donald Trump. A database collected by a study contains 115 pro-Trump fake stories that were shared on Facebook a total of 30 million times and 41 pro-Clinton fake stories shared a total of 7.6 million times.[28] Among these fake stories, one stated that that the Pope supported Donald Trump's candidacy. More generally, Facebook advertisements were decisive in Trump's victory. Trump's presidential campaign spent most of its digital advertising budget on Facebook. He sent 5.9 million messages to targeted voters, whereas Hillary Clinton sent just 66 000 messages.[29] Where there was little to separate the two candidates in a few swing states, it can be considered that this targeting had a decisive impact on the outcome of the US presidential election.

25. According to the above-mentioned interim report of the Digital, Culture, Media and Sport Committee of the House of Commons on Disinformation and Fake News, published on 29 July 2018: "During the Presidential Election, the Russians ran over 3 000 adverts on Facebook and Instagram to promote 120 Facebook pages in a campaign that reached 126 million Americans".[30] In the April 2018 hearings before the US Congress, Facebook CEO Mark Zuckerberg explained that Russian accounts

26. *Digital campaigning: Increasing transparency for voters*, op.cit.
27. Paragraph 27 of the judgment.
28. Allcott H. and Gentzkow M., op. cit, pp. 211-236.
29. "L'histoire vraie des *fake news*", op.cit.
30. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/36302.htm.

primarily used advertisements to influence views on issues rather than promoting specific candidates or political messages.

26. Concerning the 2016 referendum on membership of the EU in the United Kingdom, a joint research project by the University of Swansea and the University of California at Berkeley identified 156 252 Russian accounts tweeting about Brexit and found that they posted over 45 000 Brexit messages in the last 48 hours of the campaign.[31] According to a report from 89up, the communications agency, Russia Today (RT) and Sputnik published 261 media articles on the EU referendum, with an anti-EU sentiment, between 1 January and 23 June 2016. The report also showed that RT and Sputnik had more reach on Twitter for anti-EU content than either the Vote Leave or Leave campaigns.[32]

27. In the case of the French presidential election of 2017, a study revealed anomalous account usage patterns, which suggested the possible existence of a black market for reusable political disinformation bots.[33] On the basis of 17 million posts collected, it appeared that the users who engaged with Macron leaks were mostly foreigners with a pre-existing interest in alt-right topics and alternative news media rather than French users with diverse political views.

28. Regarding the British general election in 2017, a report from Oxford University's Internet Institute's project on computational propaganda considered that "junk news", defined as "misleading, deceptive or incorrect information purporting to be real news about politics, economics and culture", made up 11.4% of content shared.[34]

29. If we observe the impact of fake news on the general elections in Germany in 2017, we note that foreign fake news played a limited role. Most of the fake news was disseminated by the extreme right. Priority was not systematically given to social media; traditional media was also used. The attention of fake news was mainly focused on two themes: refugees and criminality. The limited role of social media in the channels of information in Germany, in comparison with the United States, may explain the modest impact of fake news. The biggest fake news item dealt with a pitched battle where 1000 immigrants were supposed to have been fighting in a small town in Baden-Württemberg. It was shared by 500 000 people.[35]

30. Evidence provided by numerous trending articles from Facebook pages also highlights the role of foreign influence and disinformation in the last Czech presidential election in 2018.[36]

---

31. "Putin's Brexit? The influence of Kremlin media and bots during the 2016 UK EU referendum", 89up, February 2018.
32. "Russian Twitter accounts promoted Brexit ahead of EU referendum", Reuters, 15 November 2017.
33. Ferrara E., "Disinformation and social bot, operations in the run-up to the 2017 French Presidential Election", *First Monday,* 22(8) 2017.
34. www.niemanlab.org/2017/06/brits-and-europeans-seem-to-be-better-than-americans-at-not-sharing-fake-news/.
35. Sängerlaub A., Meier M. and Dieter-Rühl W., "Fakten statt Fakes", Stiftung Neue Verantwortung, March 2018.
36. www.europeanvalues.net/wp-content/uploads/2018/02/The-role-of-the-Kremlin%E2%80%99s-influence-and-disinformation-in-the-Czech-presidential-elections.pdf.

31. Some observers consider that this expression of disinformation deserves to be put into perspective. Such practice has always existed because it is part and parcel of political debate. Chancellor Otto von Bismarck said that people never lie as much as after a hunt, during a war or before an election. There are clear historical examples of political lies from almost every era. Examples may refer to 5th-century Romania, 17th-century France and 19th-century Germany, as well as throughout the world in the 20th century.[37]

1.3. The intensification of the process

32. Even if the impact of disinformation varies from country to country, the rapid spread of the phenomenon, its technical sophistication in terms of speed, scale and extraterritoriality, its harmless perception by society and its relatively limited funding requirements all constitute big changes and threats not only for the electoral process but also for our democracies in general. The Gartner consulting and research group considers that by 2020 artificial intelligence as a tool of disinformation will outstrip the artificial intelligence used to detect it.[38]

33. A lot of water has flowed under the bridge since the adoption of a European Parliament resolution on EU strategic communication to counteract propaganda against it by third parties in 2016.[39]

34. More and more countries are concerned. In its report for 2017, Freedom on the Net documented a comprehensive study of internet freedom in 65 countries covering 87% of the world's internet users. It noted the prevalence of political bots in 20 countries, the practice of fake news around elections in 16 countries and the use of hijacked accounts in 10 countries. In these 20 countries, characteristic patterns of online activity suggested co-ordinated use of bots to influence political discourse.[40]

35. It seems clear that the above-mentioned cases of influence of social media on electoral campaigns in western democracies are not isolated. Evidence of formally organised social media manipulation campaigns in 48 countries (up from 28 countries last year) has been provided by the Computational Propaganda Research Project of the University of Oxford.[41] In each country there is at least one political party or government agency using social media to manipulate public opinion domestically. Small countries with less-educated voters may be more vulnerable to junk news and disinformation than large countries with more-educated voters and quality journalism.

37. http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/fake-news/written/85595.html. Also Huyghe F-B., "Désinformation : armes du faux, lutte et chaos dans la société de l'information", *Sécurité globale*, No. 6, 2016, p. 64.
38. Gartner, "Gartner Reveals Top Predictions for IT Organizations and Users in 2018 and Beyond", press release, 3 October 2017.
39. 23 November 2016 (2016/2030(INI)): paragraph 52: "[The European Parliament] underlines that particular attention should be paid to new technologies – including digital broadcasting, mobile communications, online media and social networks, including those of a regional character – which facilitate the dissemination of information about…".
40. Freedom on the Net 2017, "Manipulating social media to undermine democracy, 2018", Freedom House.
41. http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/07/ct2018.pdf.

36. Digital disinformation operations affect more voters than traditional techniques. We can expect an increase in such practices in comparison to traditional techniques, and digital methods allow larger audiences to be reached. Followers of politicians contribute to this trend. In the pre-digital age political activists with similar views would have spent much more time attempting to reach voters: going door to door to gather information and convincing people to vote.

37. Techniques devised by data brokers to understand the psychological profile of voters, as we have seen, are much more invasive than in the past, thanks to algorithms and search engines.

38. It would seem that algorithms are reinforcing individuals' tendencies to embrace only those objects, people, opinions and cultures that conform to their interests. One conclusion of the report of the French Data Protection Authority in December 2017 on the ethical matters raised by algorithms and artificial intelligence was that personalisation of information could lead to an extreme fragmentation of the public space and the disappearance of a minimum core of information shared by people. It leads to an atomisation of the political community.

39. It also raises the question of the right to privacy. In countries such as the US, given the First Amendment that guarantees freedom of speech, use of political data is not protected. In this regard, European countries have developed general privacy rules, unlike in the US, which could be used to step up anti-disinformation efforts.

40. Digital techniques change at a very quick pace and continue to evolve. The damage from current fake news pales in comparison to the harm that could come from "deepfakes". These refer to the artificial-intelligence-powered imitation of speech and images to create alternative realities, making someone appear to be saying or doing things they never said or did. In their simplest form, deepfakes are achieved by giving a computer instructions and feeding it images and audio of a person to teach it to imitate that person's voice.[42]

41. Between 12 and 14 hours are needed to deny a rumour that continues to circulate on Twitter.[43] The impact of junk news on the eve of a polling day may therefore be devastating.

42. Relativism in our societies is increasing. It means that truth and falsity, right and wrong, standards of reasoning, and procedures of justification are considered as products of differing conventions and frameworks of assessment. Their authority is confined to the context giving rise to them.[44] This point has been outlined by the philosopher Slavoj Zizek to explain the development of the phenomenon of fake news relating to postmodern deconstruction, because people may not be able to distinguish any difference between real news and false news.[45] When President Trump was interviewed by the journalist Lesley Stahl – it was the first television interview with Trump after his 2016 election victory – he said he bashed the press to "demean"

42. https:// whatis.techtarget.com/ definition/deepfake.
43. Rapport n° 677 (2017-2018) de M[me] Catherine Morin-Desailly, La commission de la culture, de l'éducation et de la communication du Sénat français,18 July 2018 (in French).
44. https://plato.stanford.edu/entries/relativism/.
45. Zizek S., op. cit.

and "discredit" reporters, so that no one would believe negative stories about him.[46] This deliberate strategy, against a background of distrust of journalists, creates a climate which plays to the fears and prejudices of people in order to influence their behaviour and contributes to destabilising voters who lose their points of reference.

43. The increasing use of digital tools in political campaigning has a serious financial impact, which must be taken in account. All member states of the Council of Europe have introduced regulations on political finance in compliance with Recommendation Rec(2003)4 on common rules against corruption in the funding of political parties and electoral campaigns. These rules deal with spending limits, transparency of resources, monitoring and sanctions. This legal framework has been implemented step by step thanks to the impetus of GRECO (the Group of States against Corruption).

In most Council of Europe member states, current legal rules on campaign funding do not require the inclusion of digital material, and if foreign donations to political parties or candidates are banned, no rules explicitly prohibit overseas spending.

In the UK, during the referendum campaign on EU membership, Vote Leave (as the designated lead "Leave" group), where digital campaigning was largely used, attracted criticism for the use of funding for these digital tools. The permitted expenditure limit was £7 million during the referendum campaign. Arron Banks, who is regarded as being close to Russian interest groups, is believed to have donated £8.4 million to the Leave campaign, the largest political donation in British politics. The source of this money remains unclear. Donations from clandestine sources[47] made to influence an electoral campaign, and digital electoral campaigns conducted from abroad to influence voters, weaken the rules on political finance based on transparency, and can even render them ineffective.

1.4. Possible responses

44. The legal status of an internet service provider has to be precise in terms of EU law. For detail regarding the responsibilities of a service provider, we need to refer to Article 14 of Directive 2000/31.[48] It must be interpreted as meaning that the rule laid down applies to an internet service provider where that provider has not played an active role in such a manner that it has knowledge of, or control over, the data stored. If it has not played such a role, that service provider cannot be held liable for

46. www.cnbc.com/2018/05/22/trump-told-lesley-stahl-he-bashes-press-to-discredit-negative-stories.html.
47. Paragraph 191 of the Interim Report: https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/363.pdf.
48. "1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:
    a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or
    b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.
    2. Paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider."

the data which it has stored at the request of an advertiser, unless, having obtained knowledge of the unlawful nature of those data or of that advertiser's activities, it failed to act expeditiously to remove or to disable access to the data concerned.[49] A host provider like Facebook therefore only has to remove an unlawful message if it has knowledge of it. In a communication of 28 September 2017 on tackling illegal online content towards an enhanced responsibility regarding online platforms, the European Union outlined a European approach, combining the need for fast and effective removals of illegal content and prevention and prosecution of crimes with safeguarding the right to free speech online.[50] On 1 March 2018, the European Commission issued a recommendation on measures to effectively tackle illegal online content, which we will refer to in paragraph 97.[51]

45. In the context of countering the practice of dissemination of false information, two options are possible: one is based on self-regulation, the other on statutory regulation.

1.4.1. Self-regulation

46. Practitioners plead for self-regulation: Facebook and Twitter have announced internal initiatives to provide the public with more action and information to identify which organisations or individuals pay for political advertisements and who the intended targets are.

47. In January 2018, the European Commission set up a High Level Expert Group (HLEG) to advise on policy initiatives to counter fake news and disinformation spread online. The main deliverable of the HLEG was a report designed to review best practices in the light of fundamental principles, and suitable responses stemming from such principles.[52] To give an impression of its content, this report has been described in the following terms: "a good dose of ethics, a shred of accountability".[53]

48. The multidimensional approach recommended by the HLEG is based on a number of interconnected and mutually reinforcing responses. These responses rest on five pillars, designed to:

1. enhance transparency of online news, involving an adequate and privacy-compliant sharing of data about the systems that enable circulation online;
2. promote media and information literacy to counter disinformation and help users navigate the digital media environment;

---

49. Judgment of the European Court of Justice (Grand Chamber) of 23 March 2010, *Google France SARL and Google Inc. v. Louis Vuitton Malletier SA* (C-236/08), *Google France SARL v. Viaticum SA and Luteciel SARL* (C-237/08), and *Google France SARL v. Centre national de recherche en relations humaines (CNRRH) SARL and Others* (C-238/08).
50. https://ec.europa.eu/digital-single-market/en/news/communication-tackling-illegal-content-online-towards-enhanced-responsibility-online-platforms.
51. https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-measures-effectively-tackle-illegal-content-online.
52. https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation.
53. Bensamoun A., "Stratégie européenne sur l'intelligence artificielle : toujours à la mode éthique", *Recueil Dalloz,* 2018, No. 19, p. 1022.

3. develop tools for empowering users and journalists to tackle disinformation and foster positive engagement with fast-evolving information technologies;
4. safeguard the diversity and sustainability of the European news media ecosystem; and
5. promote continued research on the impact of disinformation in Europe to evaluate the measures taken by different actors and constantly adjust the necessary responses.

49. With a view to the forthcoming EU elections in May 2019, the European Union has expressed its concern about the possible risk of the spread of disinformation before polling day. On 26 April 2018, it proposed an EU-wide Code of Practice on Disinformation. The Commission was to assess its implementation in broad consultation with stakeholders and on the basis of key performance indicators based on its objectives. Should the results prove unsatisfactory, the Commission might consider further measures, including regulatory measures. The Commission would support the creation of an independent European network of fact-checkers to establish common working methods, exchange best practices, achieve the broadest possible coverage across the EU and participate in joint fact-checking and related activities. It would foster online accountability and harness new technologies to tackle disinformation over the longer term. It draws attention to the need to reinforce the resilience of societies to disinformation. It was due to report on progress made by December 2018.

50. Regarding these initiatives, two proposals deserve attention: the activities of online platforms and fact-checking.

51. Concerning the activities of online platforms, the HLEG reminds us that advertising networks operated by the platforms themselves or by other parties play an important role within their strategy, which pursues three aims:

- that advertising networks refuse to place advertisements on websites identified as purveyors of disinformation; this directly reduces the income for disinformation providers;
- that advertising providers exclude advertisements from disinformation sources and clearly describe political advertisements as sponsored content to create transparency; and
- that advertising networks distribute revenues to sites and partners only after confirming that they operate within relevant terms and conditions.

52. In 2018, Facebook invested in advertisements globally proclaiming that "fake accounts are not our friends". But the above-mentioned report of the House of Commons Committee takes the view that the serious failings in the company's operations that resulted in data manipulation, leading to misinformation and disinformation, have occurred again.[54] Before the Committees for Legal Affairs and Culture of the French Senate, one manager of Google France insisted that Google took many initiatives against disinformation online, such as the removing of advertising used to disseminate fake news, the implementation of a "follow the money" principle in the fight against disinformation, and changes to the references of algorithms related

54. Paragraph 133: https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/363.pdf.

to events.[55] Both Facebook and Twitter have promised to set up archives for political advertising accessible to the public.[56] For the US mid-term elections in autumn 2018, Facebook, Google and Twitter stated that they would check if campaigners were based in the US and that they would publish databases of the political adverts that they had been paid to run.[57] Facebook removed 32 accounts and pages on its platform regarding the 2018 mid-term elections to the US Congress.[58] It created networks of false accounts and events. It used networks to identify and neutralise "bad actors". Some 652 pages created in Iran and disseminating pro-Iranian messages were also blocked.[59]

53. The fact-checking of narratives using fact-checking internet entities (such as Snopes.com) should be strengthened. For instance, the director of Pagella Politica,[60] an Italian independent fact-checking organisation, emphasises the efforts of its operation: "Once we find a news article that is obviously false, we write a fact-checking piece that is published in a specific section of our website and we provide its link to Facebook".[61] The international fact-checking network IFCN's Code of Principles has to be quoted too. The German Research Centre for Artificial Intelligence (Deutsche Forschungszentrum für künstliche Intelligenz GmbH-DFKI), for instance, has developed an application to identify fake pictures used to deliver false information that were originally published in quite different contexts.[62]

But we must remember that every day hundreds of millions of pieces of information are circulating on the web. Fact-checkers can only manage to deal with a fraction of these pieces of information. The processing capacity of fact-checkers clearly does not meet the evident need, even if fact-checkers do not just work for an operator like Facebook but offer their fact-checking to the online platforms. There is obviously a strong imbalance between those who supervise algorithms and data, and the data subjects. There is also an imbalance between the human resources that drive disinformation and the number of people who detect it. For instance, an East StratCom Task Force was set up in September 2015 under the European External Action Service.[63] It relies on volunteers to collect disinformation stories, but is notoriously understaffed. A March 2018 report of the Atlantic Council recommended that the EU require all member states to provide a seconded national expert to boost this task force.[64]

54. We must conclude that self-regulation is not a complete solution.

---

55. Rapport n° 677 (2017-2018), M[me] Catherine Morin-Desailly, op. cit.
56. Chester J., op. cit.
57. "Digital campaigning: Increasing transparency for voters", op.cit.
58. "Facebook deckt neue gefälschte Konten auf", *Neue Zürcher Zeitung,* 2 August 2018.
59. "Fake News: la tech américaine orchestre sa réplique", *Les Échos*, 23 August 2018.
60. https://pagellapolitica.it.
61. www.theatlantic.com/international/archive/2018/02/europe-fake-news/551972/.
62. DFKI Newsletter 40, 2017.
63. https://euvsdisinfo.eu/news.
64. www.atlanticcouncil.org/publications/reports/democratic-defense-against-disinformation.

1.4.2. Statutory regulations

55. Statutory regulations are unable, from a legal perspective, to undermine the freedom to provide services and the freedom of expression.

1.4.2.1. Freedom to provide services

56. In terms of the rules of the EU, restrictions in the general interest may be brought to ensure freedom to provide services to protect consumers.[65]

1.4.2.2. Freedom of expression

57. Some countries have adopted bills that enable governments to prosecute people suspected of spreading "false" information on the internet. This was the case in Malaysia in April 2018 and in Belarus in June 2018.[66] But the background to the concept of freedom of expression makes the option of censorship unrealistic in Europe. Such proposals would quickly be dealt with by references to an "Information Ministry" or a "Truth Ministry".[67] This argument was put forward during a parliamentary debate against a members' bill from the Partido Popular in the Spanish Lower House on 17 July 2018. The chamber rejected the bill, which was aimed at improving the monitoring capacities of the intelligence services for disinformation.

58. In Europe, freedom of expression is enshrined in Article 10 of the European Convention on Human Rights[68] and in Article 11 of the Charter of Fundamental Rights of the European Union.[69] In the case of *Handyside v. the United Kingdom* of 7 December 1976, the European Court of Human Rights considered that freedom of expression is applicable not only to "information" or "ideas" that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the state or any sector of the population. This falls within the values of pluralism, tolerance and broadmindedness without which there is no "democratic society". This means, among other things, that every "formality", "condition", "restriction" or "penalty" imposed in this sphere must be proportionate to the legitimate aim pursued. In another judgment,[70] the Court in Strasbourg considered

65. *Commission v. France*, 22 October 1998, C-184/96.
66. "Lukaschenkos Schlag gegen den Journalismus", *Neue Zürcher Zeitung*, 10 August 2018.
67. Reuter M., "Stellungsnahme Auschuss Digitale Agenda", Deutscher Bundestag, Netzpolitik.org.
68. "Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.
The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."
69. "Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers."
70. *Salov v. Ukraine*, 6 September 2005, 655118/01.

that in electoral campaigns, the dissemination of news must take place even if this news may be considered as false. Article 10 of the Convention as such does not prohibit discussion or dissemination of information received, even if it is strongly suspected that this information might not be truthful. To suggest otherwise would deprive persons of the right to express their views and opinions about statements made in the mass media and would thus place an unreasonable restriction on the freedom of expression set forth in Article 10 of the Convention.

59. The Court takes care not to support any measures that may lead to abuse, for example concerning blocking orders; blocking access to host and third-party websites in addition to websites concerned by proceedings renders much information inaccessible, thus restricting the rights of internet users. This interference had not been foreseeable and had not afforded the applicant in one case the degree of protection he was entitled to from the rule of law in a democratic society.[71] Blocking a user's access to YouTube without a legal basis infringes the right to receive and impart information.[72]

60. Member states of the Council of Europe have a positive obligation to ensure the effectiveness of freedom of expression: they are required to create a favourable environment for participation in public debate by all persons concerned, enabling them to express their opinions and ideas without fear. The state must not just refrain from any interference in the individual's freedom of expression but is also under a "positive obligation" to protect his or her right to freedom of expression against attack, including by private individuals.[73]

61. The existence of facts can be demonstrated, whereas the truth of value judgments is not reliant on proof. A requirement to prove the truth of a value judgment is impossible to fulfil and infringes freedom of opinion itself, which is a fundamental part of the right secured by Article 10.[74]

62. Besides the jurisprudence of the Court, reference has to be made to the standards adopted by the Council of Europe: Recommendation CM/Rec(2016)5 of the Committee of Ministers to member States on Internet freedom (13 April 2016), which calls on member states to create an enabling environment for internet freedom, including, *inter alia*, the provision of media and digital literacy programmes. It needs to be recalled that "hate speech" was defined by the Committee of Ministers in 1997. The Council of Europe adopted the Convention on Cybercrime in Budapest on 23 November 2001 and it may be assumed that a cyberattack could be construed as a form of disinformation. Until recently, cyber threats were considered to have either physical or economic consequences, but disinformation may now be considered to have the potential to damage the democratic process.

63. For a comprehensive overview of international standards in this field, the 2017 Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda issued by the special rapporteurs of the United Nations, the Organization

71. *Ahmet Yildirim v. Turkey*, 18 December 2012, 3111/10.
72. *Cengiz and Others v. Turkey*, 1 December 2015, 48226/10 and 14027/11.
73. *Dink v. Turkey*, 14 September 2010, 2668/07, 6102/08, 30079/08, 7072/09 and 7124/09.
74. *Jerusalem v. Austria*, 27 May 2001, 26958/95.

for Security and Co-operation in Europe, the Organization of American States and the African Commission on Human and Peoples' Rights[75] expresses the concern of international organisations about online disinformation. It highlights the positive obligation of states to create an enabling environment for freedom of expression and identifies broad standards of public policy to achieve this goal.[76]

64. There is therefore a strong need and a significant demand for regulations which would go beyond a simple self-regulatory regime. But to draw up proposals for a regulatory framework addressing disinformation, it is first necessary to make an inventory of current rules on these matters with a sample of member states and other countries.

1.4.2.3. Examples of legal frameworks

France

65. Rules governing personal data protection limit the extent to which software that targets individuals can develop in practice, since consent is a prerequisite for such data collection. The French legal system makes a distinction between regular and occasional political contact initiated with political parties and candidates. For regular contact, people must be informed about the processing of data (the nature of the data, purpose of the processing and the conditions under which they may express their opposition to this processing). For occasional contact the consent of the person is required for the processing.[77] These rules are similar to EU standards.

66. Fake news is already regulated by an article of the Act of 29 July 1881 which originally applied to the press. It refers to news which could be considered as having the potential to disrupt public order.[78] Three conditions are required: that the news that is published, duplicated or disseminated is false; that the publication has the potential to disturb public order; and that the author has acted in bad faith. Facts must be precise and detailed. Legal proceedings may be initiated by the prosecutor. If the public order is not disturbed, there is no legal ground for any legal action. In practice there are very few examples of cases being brought to court. The dissemination of false news is punishable by a fine of 45 000 euros. These rules were extended to online information in 2004.

---

75. They are designated by the UN, the OSCE, the OAS and the ACHPR to promote international co-operation and articulate standards relating to freedom of expression, media freedom and media.
76. Point 3 of the Joint Declaration: "a. States have a positive obligation to promote a free, independent and diverse communications environment, including media diversity, which is a key means of addressing disinformation and propaganda.
    b. States should establish a clear regulatory framework for broadcasters which is overseen by a body which is protected against political and commercial interference or pressure and which promotes a free, independent and diverse broadcasting sector."
77. www.cnil.fr/fr/communication-politique-quelles-sont-les-regles-pour-lutilisation-des-donnees-issues-des-reseaux.
78. Auvret, P., "Fausses nouvelles", *Jurisclasseur Communication,* Fascicule 3210.

67. Article 411-10 of the Criminal Code deals with the fundamental interests of the nation.

> Supplying the French civilian or military authorities with false information liable to mislead them and damage the fundamental interests of the nation, in order to serve the interests of a foreign undertaking or organisation or an undertaking or organisation under foreign control, is punishable by seven years' imprisonment and a fine of 100 000 euros.

68. Dissemination of false news to influence votes or to lead voters to abstain is punishable by one year of imprisonment and a fine of 15 000 euros (Article L.97 of the Electoral Code).

69. Dissemination of false news may affect the legality of the vote and render the election null and void. This happened on one occasion when it was announced that a candidate had withdrawn his candidacy in favour of another candidate. The Council of State as electoral judge considered that this could have affected the fairness of the outcome resulting in the cancellation of the election.[79]

70. In 2018, after suspected fake news came to light concerning Emmanuel Macron during the presidential electoral campaign of 2017, a members' bill was introduced aimed at preventing fake news during electoral campaigns when the act comes from the territory of a member state of the EU. The bill was criticised by the press and lawyers. After a first reading by the National Assembly, the Senate rejected it, considering that it was unable to solve the question raised by disinformation, that it was contrary to freedom of expression during electoral campaigns, and fearing the process could be abused for political purposes. However, the bill is again on the agenda of the National Assembly, which will have the final say.

71. The bill law aims to identify and stop deliberate allegations of a false or misleading fact on an online platform in the three-month period before an election.

72. Platforms are subject to an obligation of transparency. They must give clear, correct and transparent information about their own identity or about that of any third party that sponsors content. They must also make public the amount received in exchange for sponsoring the content.

73. A prosecutor, any person with legal interest in bringing the case before a judge on the basis of urgency, parties or candidates may complain about an item of information of an allegedly false or implausible nature that is deliberately, artificially and widely disseminated online. This notion of artificial and widespread dissemination will be a clue to false information. A judge is obliged to rule on a case of this nature within 48 hours and has the right to block the publication and to force the platform to stop its campaign.

74. Technical intermediaries, who are persons offering access to communication services, will be subject to a reinforced co-operation requirement. They will thus need to promptly remove any illicit content brought to their attention and implement an easily accessible and visible mechanism for persons to notify them about any fake news.

---

79. Conseil d'État, France, 14 April 1999, 196924. Jurisdata 1999-050242.

75. The Conseil supérieur de l'audiovisuel (CSA), the French Regulatory Broadcasting Authority, has the right to refuse to sign a convention with a foreign country if the latter's activities could seriously upset the life of the nation by disseminating fake news or violating media pluralism.

Germany

76. Freedom of expression is provided for in Article 5, paragraph 1, of the Fundamental Law, covering freedom of expression and freedom of dissemination.[80] Proceedings launched by the Turkish Head of State against a German journalist who attacked Recep Tayyip Erdoğan were rejected. The prosecutor considered that the act could not be regarded as an offence.[81]

77. According to German criminal law, a distinction must be made between statements regarding specific individuals and general statements. Dissemination of general false news without any reference to any determined persons or groups of persons is not liable to criminal sanction. Insults and defamation may be liable to sanction if specific persons are denigrated. In a judgment of 22 June 2018, the Constitutional Court did not admit a complaint directed against a criminal conviction for inciting hatred and violence against segments of the population by way of a denial of crimes committed under Nazi rule, and, specifically, the denial of murders committed at the Auschwitz-Birkenau extermination camp. Disseminating factual claims that are demonstrably untrue and deliberately false do not contribute to the opinion-forming process. Thus, it is not covered by the freedom of expression.[82] Insults are sanctioned with a fine or imprisonment for two years. The same sanctions apply to deliberate insults against individuals. Claims about the removing of news are not explicitly regulated but fixed by the judiciary.

78. Any person who offers a platform for news, comments, blogs and internet forums – in compliance with EU law (paragraph 44) – is considered a "host provider" according to paragraph 10 of the *Telemediengesetz* (Telemedia Act) and is not entitled to actively monitor the content of messages regarding requirements of law and criminal law. When they do have knowledge of such messages or content, they must remove them immediately.

79. Since 1 October 2017, the *Netzwerkdurchsetzungsgesetz*[83] (Network Enforcement Act – NetzDG) has been in force. Dubbed the "Facebook Act", the NetzDG is clearly directed at social sharing platforms that enable individual communication, and aims to fight hate speech and the sharing of criminal content (anti-constitutional, terrorism-related or concerned with child pornography, for example, and defamatory).[84] Providers of social networks that receive more than 100 complaints per calendar year

80. BVerfGE 54, 208 57, Heinrich Böll, 3 June 1980.
81. Brauer J., "Ermittlungsverfahren gegen Jan Böhmermann wegen Beleidigung von Organen und Vertretern ausländischen Staaten usw. Vermerk zur rechtlichen Bewertung", Generalstaatsanwalt, Koblenz, 13 October 2016.
82. 1 BvR 673/18, "Bundesverfassungsgericht stärkt Meinungsfreiheit", *Frankfurter Allgemeine Zeitung*, 4 August 2018.
83. www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf?__blob=publicationFile&v=2.
84. www.technologylawdispatch.com/2017/10/social-mobile-analytics-cloud-smac/germanys-new-hate-speech-act-in-force-what-social-network-providers-need-to-do-now.

about unlawful content are obliged to produce half-yearly German-language reports on the handling of complaints about unlawful content on their platforms and are obliged to publish these reports in the *Federal Gazette* and on their own website no later than one month after the half-year concerned has ended. The reports published on their own website must be easily recognisable, directly accessible and permanently available.

80. The report must contain the following:

- general observations outlining the efforts undertaken by the provider of the social network to eliminate criminally punishable activity on the platform;
- a description of the mechanisms for submitting complaints about unlawful content and the criteria applied when deciding whether to delete or block unlawful content;
- the number of incoming complaints about unlawful content in the reporting period, broken down according to whether the complaints were submitted by complainant bodies or by users, and according to the reason for the complaint;
- the organisation, personnel resources and specialist and linguistic expertise in the units responsible for processing complaints, as well as the training and support of the persons responsible for processing complaints;
- membership of industry associations with an indication as to whether these industry associations have a complaints service;
- the number of complaints for which an external body was consulted in preparation for making the decision;
- the number of complaints in the reporting period that resulted in the deletion or blocking of the content at issue, broken down according to whether the complaints were submitted by complainant bodies or by users.

81. Under the NetzDG, platforms that are not based in Germany "shall immediately name a person authorised to receive service in the Federal Republic of Germany and shall draw attention to this fact on their platform in an easily recognisable and directly accessible manner". The content must be deleted or blocked within 24 hours if it is manifestly unlawful. Other unlawful content must be deleted or blocked "immediately", meaning within seven days from when the content was "evaluated". This obligation does not apply to complaints lodged through means other than the complaint-management procedure. Very likely, geo-blocking would not suffice.

82. Regulatory offences may incur fines of up to 5 million euros for individuals and up to 50 million euros for the platform provider itself. The regulatory offence may be sanctioned even if it is not committed in the Federal Republic of Germany.

83. Some lawyers deem the act incompatible with the principle of freedom of expression. Even the *Wissenschaftlicher Dienst* of the Bundestag (the Research Service of the German Assembly which supports members' political work in parliament and constituencies by supplying specialist information, analyses and expert opinions), expressed its concern about the compliance of this act with the Fundamental Law on several points: the very short periods within which the compatibility of messages with freedom of expression have to be evaluated; the legitimacy of the objective of the act (to fight against poisoning the mood of the country, the *Vergiftung der*

Stimmung im Land); the ambiguous provisions of the act about the requirement or not of detailed facts; the proportionality of the fines regarding freedom of expression; and the compliance of the act with the law relating to privacy. The jurisprudence of the German Constitutional Court, of the Court of Justice of the European Union and of the European Court of Human Rights would be needed to clarify these points.

United Kingdom

84. The British Electoral Commission has called for increasing transparency for voters with regard to the practice of digital electoral campaigns. It has provided recommendations on the responsibility of digital campaigns, spending on digital campaigns, the transparency of payments for digital campaigns and enforcement of these rules.[85]

United States

85. The Honest Ads Act presented in October 2017 before the US Congress introduced disclosure and disclaimer rules to online political advertising. Technology companies need to keep copies of election advertisements and make them available to the public. The advertisements also need to contain disclaimers similar to those included in TV or print political advertisements, informing voters about who paid for the advertisement, how much and whom they targeted. The date and time of when the first advertisement was first displayed also needs to be provided.[86] Twitter pledged to support the bipartisan bill introduced by Senator Amy Klobuchar (D-MN), Senator Mark Warner (D-VA) and former Senator John McCain (R-AZ).

86. It is clear that many countries are aware of the dangers of the manipulation of public opinion during electoral campaigns and there are comprehensive efforts being made to implement new regulations to counter disinformation. However, there remain many obstacles to drafting effective rules that are compatible with constitutional and international standards, which will only make the whole exercise more difficult.[87]

87. The following recommendations could provide the necessary input for a debate on possible international standards inside the Council of Europe. These standards are a mix of self-regulation and official regulation because this issue is an ensemble of the strengthening of privacy, transparency, deterrence, responsiveness of monitoring, ethics, education and good practices employed by the platforms.

85. "Digital campaigning: Increasing transparency for voters", op. cit.
86. www.warner.senate.gov/public/index.cfm/the-honest-ads-act.
87. This is the reason why the French State Council gave its legal opinion on the draft private members' bill on fake news.

2. Recommendations

88. To take on these legal and technical challenges, the Council of Europe could consider addressing the following issues.

2.1. Definition of terms

89. The terms "disinformation" or "false information" should be used instead of "fake news".

90. The HLEG takes the view that the term "fake news" is "inadequate to capture the complex problem of disinformation, which involves content that is not actually or completely 'fake' but fabricated information blended with facts and practices that go beyond anything resembling 'news'".[88] The same working group believes that the term "fake news" is not only inadequate but also misleading because it has been appropriated by some politicians and their supporters, who use the term to dismiss coverage that they find disagreeable. It has therefore become a weapon with which powerful actors can interfere with the circulation of information and attack and undermine independent news media.

91. In French Law, the scope of "false information" is broader than "fake news" because it does not refer to any previous dissemination of the information, where it may have been linked to precise and detailed facts. But to prevent public authorities from getting involved in the legal issues around the protection of freedom of information, it is to be established that there is malicious intent in the dissemination of such false information.

92. In this context, we need to be mindful of the jurisprudence of the European Court of Human Rights:

> The existence of facts can be demonstrated, whereas the truth of value judgments is not susceptible of proof; a requirement to prove the truth of a value judgment is impossible to fulfil and infringes freedom of opinion itself, which is a fundamental part of the right secured by Article 10 [of the European Convention on Human Rights].[89]

88. "A multi-dimensional approach to disinformation, Report of the independent High level Group on fake news and online disinformation", European Commission, 2018, p.10.
89. *Morice v. France*, 23 April 2015, 293969/10.

2.2. Transparency

93. The issue of transparency should focus on the operators and the funding of their activities.

94. Requirements of transparency already apply in the field of communication. Article 6 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce in the internal market ("Directive on electronic commerce"), provides that member states shall ensure that commercial communications which are part of, or constitute, an information society service comply at least with the following conditions:

a. the commercial communication shall be clearly identifiable as such;

b. the natural or legal person on whose behalf the commercial communication is made shall be clearly identifiable.

95. The regulation on electronic identification and trust services for electronic transactions in the internal market (910/2014) of 23 July 2014 can be also mentioned. It provides a predictable regulatory environment for online cross-border use, recognition and enforcement of electronic identification, authentication and trust services that could be relied upon to foster the development and the voluntary use of systems for the secure identification of suppliers of information based on the highest security and privacy standards, including the possible use of verified pseudonyms.

96. Article 5 of Directive 2016/1148 of 6 July 2016, concerning measures for a high common level of security of network and information systems across the European Union, lays down ways to identify operators of essential services.

97. A recommendation from the European Commission of 1 March 2018 on measures to effectively tackle illegal online content[90] enhances transparency and the accuracy of notice-and-action mechanisms:

> (16) Hosting service providers should be encouraged to publish clear, easily understandable and sufficiently detailed explanations of their policy in respect of the removal or disabling of access to the content that they store, including content considered to be illegal content.
>
> (17) Hosting service providers should be encouraged to publish at regular intervals, preferably at least annually, reports on their activities relating to the removal and the disabling of content considered to be illegal content. Those reports should include, in particular, information on the amount and type of content removed, on the number of notices and counter-notices received and the time needed for taking action.

So, there is a general trend for enhancing transparency for service providers in the EU.

98. American and French draft legislation and the British Electoral Commission assert the need to identify who is behind these online platforms. To fulfil this need, the British Electoral Commission suggests that digital material used for electoral campaigns must include an imprint. This requirement would be useful in enforcing

90. https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-measures-effectively-tackle-illegal-content-online.

spending limits on political parties, candidates and third parties because sources of political advertising are widespread and difficult to identify. To make transparency more acute, the British Electoral Commission recommends that "campaigners should be required to provide invoices from their suppliers which contain more meaningful information about the details of their campaigns".

99. Do the regulations go a step further with labelled social media platforms? Reporters sans frontières, which is one of the leading NGOs in the defence and promotion of freedom of information, wants to set up a repository with a European ISO on the transparency of the media, ethics and independence. If such a system makes the sources clear, it could be counterproductive. "Whitelists" of articles or news sources, based either on user or an independent institution's ratings, often become a proxy for government-approved news. It would give the impression that only social media that carry such a label are reliable. In their communication on disinformation of 26 April 2018,[91] EU institutions recommended the setting up of indicators of trustworthiness of content sources, based on objective criteria and endorsed by news media associations. But who would be entitled to deliver this label and what would happen if a platform with the label disseminated false news?

100. The US Honest Ads Act argues that transparency of funding for political advertisements is essential to enforce other campaign finance laws, including the prohibition on campaign spending by foreign nationals. It extends the current requirements for public access to broadcasting, cable and satellite records of political advertisement sales to digital platforms. It enhances transparency and accountability for paid political advertisements by requiring digital platforms with 50 million or more unique monthly visitors, during a majority of the months in the preceding 12 months, to maintain a complete record of requests from advertisers whose aggregate requests to purchase qualified political advertisements on that platform within the preceding 12 months exceed 500 US dollars.

101. For the same purposes, the British Electoral Commission invites campaigners to report how much they have spent on producing and sending targeted messages to voters using digital channels.

2.3. Duration of electoral campaigns

102. Restrictions on advertising, limited to the period of electoral campaigns, would not infringe the freedom to provide services and the freedom of expression with regard to the standards of the European Union, especially given the general public interest at stake.

103. In order to cover digital campaign activity, the electoral period must be precisely determined by law and must not be too short. There are countries where this period is very short (Azerbaijan, Greece, Lithuania, North Macedonia). In this context, parties and candidates are not required to record income and expenditure incurred before this period even if they are related to an election campaign. So, the value of short campaign periods must be questioned and the periods extended to avoid the risk

91. European Commission Brussels. 26.04.2018 COM (2018) 236 final.

of unfair competition and interference by significant digital campaigns before the start of the official electoral campaign.

104. For instance, six months before a general election in France, any advertising of achievements or of the management of the public body that is conducted in a constituency where an election is to take place, is prohibited (Article L.52-1 of the Electoral Code). Such a rule could be transposed with a shorter time limitation to regulate or ban any dissemination of disinformation on a large and artificial scale.

2.4. Spending on digital electoral campaigns

105. Spending on digital campaigns should be considered part of electoral expenditure if there is no other provision on these matters, and should be included in the ceilings of party, candidate and, if relevant, third-party expenditure, if need be.

106. Should spending on digital campaigns from a foreign country be banned? Would that run contrary to the right of freedom of expression?

107. In different member states of the Council of Europe, there are MPs who represent voters overseas. These are citizens of member states who live abroad but who vote in their home-country and European elections. European citizens may vote for local elections in the European country where they live. But as voters of any kind, they may be concerned by disinformation.

108. Is a ban on foreign electoral expenditure different from a ban on foreign donations, which is a rule in some Council of Europe member states (France, Germany under certain conditions, Latvia, Moldova, Romania, Turkey and Ukraine, for instance)? Why should foreign donations be banned and foreign electoral expenses be allowed? What would the impact of a ban on foreign donations be if at the same time foreign electoral campaign expenditure was permitted? Foreign electoral digital expenditure could be regarded as in-kind donations from third parties. Moreover, a ceiling on electoral expenditure does not apply everywhere. So, if this matter is not regulated, it could be a way to permit unequal opportunities between political parties and candidates and to circumvent a ceiling on electoral expenditure where it applies.

109. Freedom of expression has not been put forward for consideration when the legislator in different member states has decided to prohibit donations from foreign companies. As foreign companies do not vote, a ban on any campaign spending stemming from a foreign company could comply with the principle of freedom of expression.

110. Concerning the right of an NGO to broadcast political advertisements on radio and television, the European Court of Human Rights has been required to balance the applicant NGO's right to impart information and ideas of general interest that the public is entitled to receive with the authorities' desire to protect the democratic debate and process from distortion by powerful financial groups with advantageous access to influential media. The Court has recognised that such groups could obtain competitive advantages in the area of paid advertising and thereby curtail a free

and pluralist debate, of which the state remains the ultimate guarantor.[92] As a result, the risk of an imbalance between political forces in competition has to be taken into account to maintain a free and pluralist debate. The same risk that the Court has in the past had to assess for traditional broadcast means now needs to be applied to social media, which is far more widespread today than in years gone by. Some candidates and political parties may benefit from powerful and anonymous online platforms whereas others may not receive any help at all from social platforms. Unregulated interference by social media in electoral campaigns therefore carries the danger of creating unfair electoral campaigns.

2.5. The processing of personal data according to the European General Data Protection Regulation (GDPR) and the protection of citizens

111. The USA and the European Union have different approaches to privacy. The First Amendment in the USA allows the use of political data as a protected form of speech.

112. Across the European Union, the GDPR has been applied since 25 May 2018, and all member states had to incorporate it into their own national legislation by 6 May 2018. It states that the protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8, paragraph 1, of the Charter of Fundamental Rights of the European Union and Article 16, paragraph 1, of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data.

113. According to the GDPR, the processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. The GDPR respects all fundamental rights and observes the freedoms and principles recognised in the charter as enshrined in the treaties of the European Union, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.

114. The GDPR does not apply to issues of protection of fundamental rights and freedoms or the free flow of personal data related to activities which fall outside the scope of EU law, such as activities concerning national security. It may be considered that electoral matters fall under the sovereignty of each member state and are covered by the subsidiarity principle. But political parties may compile personal data on the population's political opinions. The processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are established.

92. *Animal Defenders International v. the United Kingdom*, 22 April 2013, 48876/08. Yves-Marie Doublet, "L'interdiction des campagnes politiques publicitaires à la télévision et à la radio n'est pas contraire à l'article 10 de la CEDH", *Revue trimestrielle des droits de l'homme*, 2014, 98, p. 483.

115. In March 2018, the European Council stated that: "social networks and digital platforms need to guarantee transparent practices and full protection of citizens' privacy and personal data."[93] Despite the scope of the GDPR, inspiration for a legal framework against disinformation could be sought by the Council of Europe in a number of its provisions, because to a certain extent the purpose of the GDPR and the purposes of a possible legal framework provided by the Council of Europe are the same. Definitions, the requirement of consent of individual persons and the transparency of processing means could be of some interest to the Council of Europe, in order to guarantee the integrity of electoral campaigns and elections.

116. With respect to the 2019 elections for the European Parliament, the European Union is seeking the power to impose fines on European political parties which misuse a voter's personal data to influence elections. The sanctions could amount to 5% of the annual budget of a political party funded from the general budget of the European Union and from donations and contributions. This draft was reported by the *Financial Times* on 26 August 2018. It assumes the approval of EU governments and the EU Parliament and needs to amend Regulation 1141/2014 of 22 October 2014 on the statute and funding of European political parties and political foundations, which has been in force since 1 January 2017.[94] Article 27, paragraph 4 (a) on sanctions provides that in cases of non-quantifiable infringements, the percentage of the annual budget of the European political party or European political foundation concerned is 5%. The scope of this rule is limited to European political parties. It is meant to ensure the trustworthiness of the content of messages.

2.5.1. Definitions

117. The definition of personal data and processing provided by the GDPR may be useful when considering the permitted exploitation of data to define voter profiles.

118. The definition of personal data is wider in the GDPR than in previous EU legislation, and includes online identifiers, such as an IP address. "Personal data" means any information relating to an identified or identifiable natural person ("data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. "Processing" means, for the purposes of the GDPR, any operation or set of operations that are performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Individuals have the right not to be subject to decisions based on automated processing without any human intervention, if such a decision can cause them harm.

93. www.consilium.europa.eu/en/press/press-releases/2018/03/23/european-council-conclusions-22-march-2018/.
94. Koch T., "Das neue Recht der europäischen politischen Parteien", PRUF, MIP 2018, 24. Jahrgang, S.71.

119. Algorithms should be regulated by these rules only if they rely on personal data; if this is not the case, it is a blind spot from a legal point of view.[95] This tricky question should therefore be tackled.

2.5.2. Transparency of processing

120. Pursuant to the GDPR, any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data should be easily accessible and easy to understand, and that clear and plain language must be used.

2.5.3. Requirement of the consent of the individual person

121. In order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis, as laid down by law, either in the GDPR or in other EU or member state law as referred to in the GDPR. This would include the necessity for compliance with any legal obligation to which the controller is subject or a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract. There can be no assumption that consent is given. Consent must be able to be withdrawn at any time, as easily as it was given.

122. If this data protection regulation is not the sole response to the problem, it is a key element in empowering individuals and making digital operators more accountable.

2.6. Fundamental principles for algorithms and artificial intelligence

123. Article 1 of the GDPR provides that the protection of natural persons in relation to the processing of personal data is a fundamental right. For that reason, the French Data Protection Authority (CNIL) considers that artificial intelligence should respect two fundamental principles: fairness[96] and continued attention and vigilance. Fairness applies to platforms and consists of "ensuring, in good faith, the search engine optimisation (SEO) or ranking service, without seeking to alter or manipulate it for purposes that are not in the users' interest". Fairness lays down an obligation with regard to controllers.

Because the development of algorithms brings with it a decrease in individual vigilance, the principle of continued attention and vigilance should be enshrined for algorithms in the legal framework on disinformation.[97]

95. Villani C. et al., *Donner un sens à l'intelligence artificielle, Pour une stratégie nationale et européenne*, La Documentation française, Paris, 2018, p.148.
96. Conseil d'État, "Le Numérique et les droits fondamentaux", 2014, pp. 273 and 278-281.
97. www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_ai_gb_web.pdf, p.50.

2.7. Summary procedure in case of urgency

124. Judicial action in accelerated court procedures in urgent cases, as is proposed in the current French draft members' bill, may be a deterrent but it raises three issues.

- The European Court of Human Rights considers that words and language may be more exaggerated during electoral campaigns than usual. During electoral campaigns, verbal excesses are permitted.[98] As a result, the question of the applicability of this interference may arise.
- On the one hand, in France as in Germany, a judge does not have much time to rule on whether disinformation is a threat to public order and whether it could destabilise an electoral campaign (48 hours and 24 hours after receiving the complaint). On the other hand, given the speed of dissemination of false news, a quick judicial decision would enable a candidate who is subject to attacks and junk news to reply.
- If this option were selected by the Council of Europe, attention should be paid to the proportionality of the sanction. An internet service provider may be ordered to block its customers' access to a copyright-infringing website. Such an injunction and its enforcement must, however, ensure a fair balance between the fundamental rights concerned. The measures adopted by the internet service provider must be strictly targeted, in the sense that they must serve to bring an end to a third party's infringement of copyright or of a related right but without thereby affecting internet users who are using the provider's services in order to lawfully access information. Failing that, the provider's interference in the freedom of information of those users would be unjustified in light of the objective pursued.[99]

2.8. Co-operation with different stakeholders

125. As underlined by the HLEG, an effort should be made to improve information literacy and to heighten awareness of the media and the education system of the dangers of various digital mechanisms of disinformation. It calls for action to support media and literacy programmes for people of all ages.

126. Stakeholders are platforms, fact-checkers, journalists, media and research organisations. Fact-checking is today a piecemeal activity in the member states. Initiatives should be taken by member states to develop fact-checking platforms.

127. The HLEG suggests encouraging user control over the selection to be displayed according to quality signals. It pleads for an empowerment of journalists through professional automatic content verification tools, training and media innovation projects.

128. The defence of freedom of expression, free press and pluralism and support for quality journalism is the foundation of the HLEG's programme of action. Trust in news varies by country. For example, 62% of people in Finland say they have trust in news

98. European Court of Human Rights, *Brasilier v. France*, 11 April 2006, Application No. 71343/01.
99. CJEU, UPC Telekabel, 27 March 2014, C-314/12.

organisations and journalists while in Greece this figure is just 23%. Only seven out of 21 Council of Europe member states surveyed by Reuters in a 2017 report have a rate of over 50% when it comes to trust in news organisations: Finland, Portugal, Poland, the Netherlands, Spain, Germany and Denmark.[100] News organisations and journalists suffer a loss of confidence too in this situation. Attention should also be paid to the form of state aid to media organisations.

129. These steps should be completed by an implementation framework. As we have seen, the HLEG has invited the European Commission to promote a general European-wide code of practice reflecting the roles and responsibilities of different stakeholders. Transparency, especially financial transparency, accountability, privacy, compliant access, ensuring a distinction between political advertising and other content and the co-operation between platforms are the main points which are raised.

130. This is a consensual approach where online platforms have a key role. But the US experience shows that digital markets cannot only be in the hands of the operators. A more prominent role should be entrusted to public authorities.

131. Four further points deserve attention.[101]

- There is a need for representatives of civil society to audit operators. Actions driven in the USA by Upturn,[102] Propublica[103] and the Electronic Frontier Foundation[104] may be referred to in this context.
- The promotion of ethics in the training of engineers, technicians and managers of online platforms.
- The introduction of a class action not only to end any infringements, but to remedy any loss that may be sustained in a personal capacity.
- The creation of a committee dedicated to ethics in digital technologies which could disseminate guides to good practice, devise codes of conduct and give advice to governments.

2.9. Compliance with European law

132. The proposed legal framework would be in line with the liability exemptions for service providers spelled out by Article 14 of Directive 2000/31 EC. But the service providers would also be subject to other requirements: transparency in accordance with the above-mentioned tools applying to online platforms and with the guidelines provided by the European Commission recommendation on measures to effectively tackle illegal content online, even if the scope of this recommendation is different from the present issue under discussion. It would also be in accordance with the right to the protection of personal data granted by the GDPR.

100. https://reutersinstitute.politics.ox.ac.uk.
101. Villani C., op. cit.
102. upturn.org.
103. www.propublica.org.
104. www.eff.org.

The direction of this approach may be considered to follow in the wake of previous European Union initiatives, without calling into question the principle of liability exemption laid down in Article 14 of Directive 2000/31/EC.

2.10. Enforcement

133. If governments or non-government stakeholders are reluctant to implement such rules on transparency or judicial monitoring, these rules will remain empty rhetoric. In a fast-moving digital world, each party should adopt the necessary measures to establish jurisdiction over any offence of dissemination of false and misleading information. But how can the responsibility to detect, investigate and prosecute this offence be imposed on a state where the offence was committed if that state reserves the right not to apply its obligations in practice?

2.11. Summary of the proposals

134. Three types of provisions are proposed.

- Digital law regulations – In compliance with European and constitutional standards, these regulations would be focused on service providers. In accordance with the principle of liability exemption and the diverse provisions of the European Union on transparency, these legal provisions would require from service providers transparency about their activities and the protection of personal data. An accelerated legal procedure would be set up to deal with urgent matters.
- Electoral law regulations – Longer electoral campaigns, transparency of financial resources of providers and a ban on electoral expenditure on digital activities by a foreign legal or physical person could provide the basis for an efficient legal framework.
- Good practice – Other measures would concentrate on fact-checking, co-operation with all stakeholders, ethics, the development of literacy programmes and the self-regulation of service providers, all supporting quality journalism.

3. Programme of action

135. A programme of action concerning disinformation and electoral campaigns could be the right framework to meet the challenges of this complex issue.

Convinced that free and fair elections are a priority of the Council of Europe for strengthening democratic governance and participation of Europe's citizens;

Conscious that re-establishing trust in the basic institutions of our democracies is a permanent fight and efforts must be systematic to combat attempts to devalue truth which erode democracy;

Concerned by the risk that social media may be used as a global system and as a business model undermining the political process of electoral campaigns and convinced that questions raised by algorithms and artificial intelligence to a large extent during electoral campaigns are significantly influencing the political process;

Having regard to the breakneck speed at which technological progress is taking place and the fact that digital disinformation operations affect more voters than traditional techniques;

Recognising the limited transparency of digital campaigning through the use of advertising, algorithms, bots and the limits of oversight and the lack of public policies in that field;

Taking into account the new European General Data Protection Regulation, which aims to respect personal data and obtain user consent and which imposes upon social media platforms stricter rules than in the past, and considering that because of a lack of regulation member states of the European Union and of the Council of Europe have no effective legal means to protect themselves against digital mechanisms of manipulation during an electoral campaign, a paradox in which the European voter is less protected than the European consumer;

Considering that there are non-governmental and governmental solutions for tackling these issues, some relying on self-regulation, others on incentives and coercive measures;

Welcoming recent actions and further developments of the European Union to combat disinformation in view of the forthcoming European Parliament elections.

Member states of the Council of Europe should, within a given time frame, adopt an overall strategy on social media and electoral campaigns, which would be a combination of statutory measures and self-regulation. They should:

- agree to focus their efforts on ensuring free and impartial information during electoral campaigns and on regulating disinformation practices, and in their references to such practices should not refer to "fake news", which is not an appropriate and adequate concept for a legal framework;
- draw up an inventory of different existing types of self-regulation and statutory regulation on digital campaigns that currently apply to member states;
- define the length of electoral campaigns to avoid the risk of significant digital campaigns before electoral campaigns;
- require imprints of digital material to reveal who is behind online platforms;
- obtain disclosure for spending on digital electoral campaign activity by online platforms;
- ban funding of digital electoral expenditure by a foreign physical or legal person;
- be inspired by the GDPR by requiring the consent of citizens for the use of their personal data for electoral digital campaigns, except if these citizens have regular contact with a political party or a candidate in connection with its purposes and if those personal data are not disclosed without the consent of the citizen in question;
- impose obligations of fairness and continued attention and vigilance with respect to online platforms and algorithms;
- enable a court, in the case of the widespread dissemination of false information, to block an online platform disseminating false news on a large scale, on an urgent basis, through the use of accelerated court procedures;
- encourage fact-checking initiatives through a network across the Council of Europe, with the objective of promoting the growth of broad-based operations;
- educate and empower users to better access and use online information, and inform users when content is generated or spread by a bot or algorithms;
- foster education on the subject of ethics for all those involved in digital technologies that have an impact on elections;
- strengthen ethics with business online platforms;
- promote good practice by online platforms by signing agreements with them, based on policy recommendations jointly defined by relevant public authorities and online platforms;
- continue to promote high-quality media organisations and journalism;
- create an ethics commission in every member state and assign them to lead discussions on ethical, political and social matters raised by the development of technologies, especially in electoral digital campaigns;
- provide effective, proportionate and dissuasive penalties applicable to infringements of the relevant regulations on digital electoral campaigns;
- create a co-operation group between member states to support and facilitate strategic co-operation and the exchange of information.

Conclusion

136. Electoral law is part of the sovereignty of states. It is influenced by their historical background and bound by the organisation of their institutions. It is a field where, except for general principles on free and fair elections to ensure in practice the free expression of the opinion of the electorate in the choice of their representatives, there are no common regulations. But the impact of invasive digital techniques within the framework of globalisation creates a new context, which requires international instruments to protect European democracies that are facing common threats.

137. The Council of Europe is the most appropriate and the most legitimate body in Europe to initiate a discussion in this field and to go further than the European Commission and the joint declaration of the UN and the OSCE, of 2017.

138. A European legal instrument promoted by the Council of Europe could provide a common direction for a comprehensive framework. A Council of Europe instrument could ensure a level playing field for every member state. A range of different tools are available.

139. We have suggested a preliminary proposal for a programme of action. A programme of action against corruption was adopted by a multidisciplinary group in 1995 and was the starting point for multiple legal instruments of the Council of Europe on these matters: criminal and civil law conventions, recommendations, resolutions and reports. But even if devising a programme of action is a time-consuming process, the options of various available measures have to be considered, together with the arguments for and against each of these potential solutions.

140. In certain cases, recommendations or resolutions preceded conventions of the Council of Europe. This was the case for private corruption or cybercrime. Recommendations would set out general standards and encourage member states to initiate legislation. It would be the most reasonable and the quickest approach to tackling this issue. But this option has the disadvantage of allowing room for interpretation by member states, whereas to be efficient regulations in this field must be uniform and standardised.

141. Guidelines are appropriate when there is already an established legal framework either with an international tool or with legislation in member states. They allow for policy advice on implementation and the fleshing out of existing regulations.

142. A convention has the merit of being a binding instrument. A certain number of ratifications could be determined to allow this convention to come into force without waiting for its ratification by each member state. Two other arguments support this option. Most conventions of the Council of Europe include a monitoring mechanism for ensuring compliance and make provision for non-member states to become parties to the convention. The drawing up of this convention would start from scratch because only a few member states have adopted targeted rules on these matters, which may make its drafting easier, given the lack of existing mechanisms. However, negotiation of a convention requires time.

143. Given the consensus reached on the threats of disinformation to the electoral process, the Council of Europe needs to decide on the most appropriate legal form for a response to this issue. Whatever form is chosen, it will contribute to enhancing democracy in Europe and will support the Council of Europe in its duty to ensure free and fair elections, which have become a fundamental part of European identity and its constitutional values.

Sales agents for publications of the Council of Europe
Agents de vente des publications du Conseil de l'Europe

BELGIUM/BELGIQUE
La Librairie Européenne -
The European Bookshop
Rue de l'Orme, 1
BE-1040 BRUXELLES
Tel.: + 32 (0)2 231 04 35
Fax: + 32 (0)2 735 08 60
E-mail: info@libeurop.eu
http://www.libeurop.be

Jean De Lannoy/DL Services
c/o Michot Warehouses
Bergense steenweg 77
Chaussée de Mons
BE-1600 SINT PIETERS LEEUW
Fax: + 32 (0)2 706 52 27
E-mail: jean.de.lannoy@dl-servi.com
http://www.jean-de-lannoy.be

CANADA
Renouf Publishing Co. Ltd.
22-1010 Polytek Street
CDN-OTTAWA, ONT K1J 9J1
Tel.: + 1 613 745 2665
Fax: + 1 613 745 7660
Toll-Free Tel.: (866) 767-6766
E-mail: order.dept@renoufbooks.com
http://www.renoufbooks.com

CROATIA/CROATIE
Robert's Plus d.o.o.
Marasovićeva 67
HR-21000 SPLIT
Tel.: + 385 21 315 800, 801, 802, 803
Fax: + 385 21 315 804
E-mail: robertsplus@robertsplus.hr

CZECH REPUBLIC/
RÉPUBLIQUE TCHÈQUE
Suweco CZ, s.r.o.
Klecakova 347
CZ-180 21 PRAHA 9
Tel.: + 420 2 424 59 204
Fax: + 420 2 848 21 646
E-mail: import@suweco.cz
http://www.suweco.cz

DENMARK/DANEMARK
GAD
Vimmelskaftet 32
DK-1161 KØBENHAVN K
Tel.: + 45 77 66 60 00
Fax: + 45 77 66 60 01
E-mail: reception@gad.dk
http://www.gad.dk

FINLAND/FINLANDE
Akateeminen Kirjakauppa
PO Box 128
Keskuskatu 1
FI-00100 HELSINKI
Tel.: + 358 (0)9 121 4430
Fax: + 358 (0)9 121 4242
E-mail: akatilaus@akateeminen.com
http://www.akateeminen.com

FRANCE
Please contact directly /
Merci de contacter directement
Council of Europe Publishing
Éditions du Conseil de l'Europe
F-67075 STRASBOURG Cedex
Tel.: + 33 (0)3 88 41 25 81
Fax: + 33 (0)3 88 41 39 10
E-mail: publishing@coe.int
http://book.coe.int

Librairie Kléber
1, rue des Francs-Bourgeois
F-67000 STRASBOURG
Tel.: + 33 (0)3 88 15 78 88
Fax: + 33 (0)3 88 15 78 80
E-mail: librairie-kleber@coe.int
http://www.librairie-kleber.com

NORWAY/NORVÈGE
Akademika
Postboks 84 Blindern
NO-0314 OSLO
Tel.: + 47 2 218 8100
Fax: + 47 2 218 8103
E-mail: support@akademika.no
http://www.akademika.no

POLAND/POLOGNE
Ars Polona JSC
25 Obroncow Street
PL-03-933 WARSZAWA
Tel.: + 48 (0)22 509 86 00
Fax: + 48 (0)22 509 86 10
E-mail: arspolona@arspolona.com.pl
http://www.arspolona.com.pl

PORTUGAL
Marka Lda
Rua dos Correeiros 61-3
PT-1100-162 LISBOA
Tel: 351 21 3224040
Fax: 351 21 3224044
E mail: apoio.clientes@marka.pt
www.marka.pt

RUSSIAN FEDERATION/
FÉDÉRATION DE RUSSIE
Ves Mir
17b, Butlerova ul. - Office 338
RU-117342 MOSCOW
Tel.: + 7 495 739 0971
Fax: + 7 495 739 0971
E-mail: orders@vesmirbooks.ru
http://www.vesmirbooks.ru

SWITZERLAND/SUISSE
Planetis Sàrl
16, chemin des Pins
CH-1273 ARZIER
Tel.: + 41 22 366 51 77
Fax: + 41 22 366 51 78
E-mail: info@planetis.ch

TAIWAN
Tycoon Information Inc.
5th Floor, No. 500, Chang-Chun Road
Taipei, Taiwan
Tel.: 886-2-8712 8886
Fax: 886-2-8712 4747, 8712 4777
E-mail: info@tycoon-info.com.tw
orders@tycoon-info.com.tw

UNITED KINGDOM/ROYAUME-UNI
The Stationery Office Ltd
PO Box 29
GB-NORWICH NR3 1GN
Tel.: + 44 (0)870 600 5522
Fax: + 44 (0)870 600 5533
E-mail: book.enquiries@tso.co.uk
http://www.tsoshop.co.uk

UNITED STATES and CANADA/
ÉTATS-UNIS et CANADA
Manhattan Publishing Co
670 White Plains Road
USA-10583 SCARSDALE, NY
Tel: + 1 914 472 4650
Fax: + 1 914 472 4316
E-mail: coe@manhattanpublishing.com
http://www.manhattanpublishing.com

Council of Europe Publishing/Éditions du Conseil de l'Europe
F-67075 STRASBOURG Cedex
Tel.: + 33 (0)3 88 41 25 81 – Fax: + 33 (0)3 88 41 39 10 – E-mail: publishing@coe.int – Website: http://book.coe.int

Since summer 2016, "fake news" has denoted the deliberate, viral spreading of false information on the internet and social media with the intention, for example, of discrediting a political party, tarnishing someone's reputation or casting doubt on scientific truth. This practice, which hinders citizens in making informed decisions, has become very widespread. Its impact is especially significant not only because of how quickly fake news spreads, but also because identifying the authors of such campaigns and digital material is very difficult.

This report attempts to provide responses to issues raised by this phenomenon, in particular during electoral campaigns, and offer proposals to shape a legal framework at European level.

PREMS 006719

ENG

www.coe.int

The Council of Europe is the continent's leading human rights organisation. It comprises 47 member states, including all members of the European Union. All Council of Europe member states have signed up to the European Convention on Human Rights, a treaty designed to protect human rights, democracy and the rule of law. The European Court of Human Rights oversees the implementation of the Convention in the member states.

http://book.coe.int
ISBN 978-92-871-8911-0
€9/US$18

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE