COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 9 November 2018

CDDG(2018)11
Item 8 of the agenda

EUROPEAN COMMITTEE ON DEMOCRACY AND GOVERNANCE (CDDG)

REPORT ON "IMPACT OF NEW INFORMATION TECHNOLOGIES ON ELECTORAL PROCESSES"

Information document prepared by Yves-Marie Doublet, Deputy Director at Assemblée Nationale (France)

For information and discussion

Secretariat Memorandum
prepared by the
Directorate General of Democracy
Democratic Governance Department

Introduction

To protect the integrity of the democratic process by identifying and implementing effective responses to multiple threats that interfere with the electoral processes and influcence voter behavior, notably the use of technologies and social media is an area of concern for the Council of Europe and its member states.

This contribution was prepared as a follow-up to the report by the Secretary-General of the Council of Europe on the State of Democracy, Human Rights and the Rule of Law (2018) "Role of institutions. Threats to institutions" which notes that "countering computational propaganda should be understood as an important challenge for the member states" and recommends that the Council of Europe maintains and reinforces its capacity to respond early and effectively to the challenges posed by technology.

The matter of interference with electoral processes via numeric networks becomes equally important and urgent. The Division of electoral assistance has already received several requests to assist in training and strengthening the capacity of actors involved in electoral processes in view of effective countering such interferences.

Therefore, this report has a double purpose of helping the Division of electoral assistance to prepare training and capacity-building tools and to inspire the CDDG in its work on e-democracy.

Action required

The CDDG members are invited to take note of the information presented in this document and to hold a first debate as to the possible operational follow-up thereto.

IMPACT OF NEW INFORMATION TECHNOLOGIES ON ELECTORAL PROCESSES

Yves-Marie Doublet, Deputy Director at Assemblée Nationale (France)

Introduction 4
1. General Overview of the situation 6
1.1. Technical data 6
1.2. Political data 8
1.3. The intensification of the process 10
1.4. Possible responses 13
1.4.1. Self-regulation 14
1.4.2. Statutory regulations 16
1.4.2.1. Freedom to provide services 16
1.4.2.2. Freedom of expression 16
1.4.2.3. Examples of legal frameworks 18
France 18
Germany 20
United Kingdom 22
United States 22
2. Recommendations 23
2.1. Definition of terms 23
2.2. Transparency 24
2.3. Duration of electoral campaigns 25
2.4. Spending on digital electoral campaigns 26
2.5.Protection of citizens in relation to the processing of personal data regulated by the European General Data Protection Regulation (GDPR) 27
2.5.1. Definitions 28
2.5.2. Transparency of processing 29
2.5.3. Requirement of the consent of the individual person 29
2.6. Fundamental Principles for algorithms and artificial intelligence 30
2.7. Summary procedure in case of urgency 30
2.8. Cooperation with different stakeholders 31
2.9. Compliance with European Law. 32
2.10. Enforcement 32
2.11. Summary of the proposals 32
3. Programme of Action 33
Conclusion 35

Introduction

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

2. Since the summer of 2016, Fake News denotes the deliberate viral spreading of false news on the Internet and social media[1]. It is related to 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 webpage - 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 the 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 bad 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 Government, cooperatives or people. In November 2017, the British Prime Minister stated that planting Fake News was a way to "*weaponize information*". All these different channels are often rolled up under the name 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 form communities of people who have access to the same opinions, share the same ideology and the same conspiracy theories[5].

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.

[1] Fake News Definition und Rechtslage, Wissenschaftlicher Dienst, Deutscher Bundestag. 2017
[2] L'histoire vraie des Fake News, L'Opinion, 1315, 7 août 2018
[3] How do we know what's true any one? You Tube, Apr. 13 2018
[4] A multi-dimensional approach to disinformation, Report of the Independent High-level Group on Fake News and Online disinformation, European Commission, 2018
[5] Fake News, Wohin das Auge reicht, Slavoj Zizek, Neue Zürcher Zeitung, 6 August 2018

6. Over the past 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, Reuters Institute for the Study of Journalism considers that Facebook is by far the most important network for finding, reading, watching and sharing news, even if its usage has fallen from 42% in 2016 to 36 % in 2018. Only in the US, 62% of adults get news on social media[6]. 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[7]. It has been stressed that digital media uses an algorithm process to target both customers and voters. Bots accounts are used to influence political discourse. They tweet and retweet with artificial 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 1500 people as it does for false stories to reach the same number of people[8].

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 are enough to buy a hate speech initiative and with 2 600 Euros you can buy 300 000 followers on Twitter[9]. False and harmful information is produced for profit. In this manner, a marriage was forged between digital companies and media businesses for several years, 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? Does 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, especially 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 kind of legal tools have been introduced until now in different Member States of the Council of Europe (CoE) or in other countries to counter Fake News? What lessons can be drawn from these experiences?

[6] Social Media and Fake News in the 2016 Election, Hunt Allcott and Matthew Genztkow, Journal of Economic Perspectives, Volume 31, Number 2 Spring 2017, p.211-236

[7] Jeff Chester, The role of Digital marketing in political campaigns, Center for digital democracy Washington DC, 31 Dec 2017

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

[9] http://www.assemblee-nationale.fr/15/pdf/rapports/r0990.pdf

How is the protection for the privacy of citizens guaranteed? Should legal action be taken on an international level, given the numerous cases of destabilization of election campaigns recently recorded in various countries? Besides a possible regulatory framework, how can public awareness be promoted regarding the authenticity of information and the need for fact-checking, in addition to encouraging a more discerning editorial judgment in media outlets?

9. This report attempts to answer these questions and to make proposals to shape a legal framework at the level of the CoE.

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)[10] than editors and that 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 organizing information on a big scale by enhancing certain aspects of it. Computational algorithms have recourse to machine learning to produce an output. Machine learning algorithms are used as generalizers, 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[11]. Samantha Bradshaw, from the Oxford Internet Institute, told the Digital, Culture, Media and Sport Committee of the 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*"[12]. We have to remind 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

[10] Nic Newmann, Executive Summary and Key Findings, Reuters Institute Digital News Report 2017
[11] How can humans keep the upper hand? The ethical matters raised by algorithms and artificial intelligence, Commission nationale Informatique et libertés, décembre 2017
https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_ai_gb_web.pdf
[12] https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/363.pdf

at the heart of the work of Cambridge Analytica, born in 2012 out of the already established SCL consultancy group *"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*"[13]. To target the voters and to direct the messages the campaigners want to reach, tools tailored to specific groups are called "*micro-targeting"*. 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' which result in a 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"*[14]*.*

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*"[15]. 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*"[16]. If someone's political conviction is not always shaped by algorithms, algorithms may be used to 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 due to the will of the designer of the platform? 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, NGO's 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[17].

[13] Idem

[14] https://lifehacker.com/how-sites-like-google-and-facebook-put-you-in-political-1787659102

[15] Jenna Burrell, How the machine thinks': Understanding opacity in machine learning algorithms, Big Data and Society, January 2016, 1-12

[16] Jeff Chester, The role of Digital marketing in political campaigns, Center for digital democracy Washington DC, 31 Dec 2017

[17] Dominique Cardon, Le pouvoir des algorithmes, Pouvoirs, La Datacratie 164, 2018

17. A "bot" is another sophisticated leverage mechanism to influence voters. It is an automated software program that mimics human behavior on social media by posting, liking and talking to real people[18]. As a German expert says: " *Social bots are Fake-accounts in Social media who pretend to be real persons"*[19]. A person who controls just one bot may therefore exert influence on a million people. For example, bots may polarize public opinion through hate speech. In the same hearing before the Committee on Digital Agenda of the Bundestag, 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*"[20] . 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, stealing content[21].

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[22].

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[23].

20. Hashtags which are short codes inserted into messages to make them researchable are reported during election campaigns. Popular hastags contain "*trending topics*", which give access to conversations. Hashtags are manipulated by bots. Hashtags which are reproduced, reflect the opinion of very few persons who have a great number of accounts. It gives the impression that they represent a large number of persons. Simple short codes lead people to believe that an opinion expresses a largely widespread view[24].

21. In 2011, spending by campaigners on digital advertising amounted to 0,3% of total advertising spend in the UK. In 2017, this spending rose to 42, 8% of total advertising spend[25].

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. United Kingdom, the European Court of Human Rights (ECHR) 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*"[26]. But social media may be misused and may affect political beliefs.

[18] Digital campaigning, Increasing transparency for voters, The Electoral Commission, June 2018
[19] Prof. Dr. Simon Hegelich, Hochschule für Politik München, Ausschuss Digitale Agenda, Deutscher Bundestag Auschussdrucksache 18 (24) 125
[20] Fake News, Social Bots, Hacks und Co. Manipulationsversuch demokratischer Willensbildungsprozesse im Netz, Wortprotokoll der 81 Sitzung, 25. Januar 2017, Deutscher Bundestag
[21] Freedom on the Net 2017. Manipulating Social Media to undermine Democracy
[22] Digital campaigning, Increasing transparency for voters, The Electoral Commission, June 2018
[23] Idem
[24] L'histoire vraie des Fake News, L'Opinion, 1326, 23 août 2018
[25] Digital campaigning, Increasing transparency for voters, The Electoral Commission, June 2018
[26] § 27 of the judgment

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 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 success of the election of Donald Trump at the 2016 US Presidential election. Social media represented 13, 8% of the sources of 2016 Election news. Fake News was both shared and heavily tilted in favour of Donald Trump. A data base 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[27]. Among these fake stories, one stated that that the Pope supported candidate Donald Trump. More generally, Facebook advertisements were decisive in Trump's victory. The Trump 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[28]. When there was not much in it in a few swing states, it can be considered that it 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* »[29]. In the April 2018 hearings before the US Congress, Facebook CEO Mark Zuckerberg explained that Russian accounts primarily used advertisements to influence views on issues rather than promoting specific candidates or political messages[30].

26. Concerning the Referendum of 2016 on the EU in the United Kingdom, a joint research project by the Universities 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. Their report also showed that RT and Sputnik had more reach on Twitter for anti-EU content than either Vote Leave or Leave [32].

27. In the case of the French presidential election 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.

[27] Social Media and Fake News in the 2016 Election, Hunt Allcott and Matthew Genztkow, Journal of Economic Perspectives, Volume 31, Number 2 Spring 2017, p.211-236
[28] L'histoire vraie des fake news, L'Opinion, 1321, 16 Août 2018
[29] https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/36302.htm
[30] http://www.europarl.europa.eu/thinktank/en/document.htmlreference=EPRS_ATA(2018)620230
[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] Emilio Ferrara, Disinformation and Social Bot, Operations in the Run up to the 2017 French Presidential Election, First Monday 22(8) 2017

28. Regarding the British General election 2017, a report from Oxford University's Internet Institute's Project on computional 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 but classical 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 1 000 immigrants were supposed to be fighting in a small town of Baden-Württemberg. It was shared by 500 000 people[35].

30. From evidence provided by numerous trending articles from Facebook pages, the role of foreign influence and disinformation in the last Czech presidential election in 2018 has been underlined[36].

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 a country to country, the quick spreading of the phenomenon, its technical sophistication in terms of speed, scale and extraterritoriality, its harmless perception by society and its relatively limited funding requirements, 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 within 2020 artificial intelligence as tool of disinformation will outstrip artificial intelligence carried out to detect it[38].

[34] http://www.niemanlab.org/2017/06/brits-and-europeans-seem-to-be-better-than-americans-at-not-sharing-fake-news/

[35] A. Sängerlaub, M. Meier and W. Dieter-Rühl, Fakten statt Fakes, Stiftung für neue Verantwortung, März 2018

[36] http://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

[37] http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/fake-news/written/85595.html . Also F-B Huyghe : Désinformation : armes du faux, lutte et chaos dans la société de l'information. Sécurité globale n°6, 2016, p.64

[38] Gartner, Gartener reveals Top predictions for IT Organisations and Users in 2018 and Beyond, pressrelease 3 October 2017

33. A lot of water has flowed under the bridge since the adoption of a resolution of the European Parliament 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, 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 coordinated 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 organized social media manipulation campaigns in 48 countries (up from 28 countries last year) has been brought 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 big countries with a more educated population and quality journalism.

36. Digital disinformation operations affect more voters than classical techniques. We can expect an increase of such practices in comparison with classical techniques, and they 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 to reach voters: going door to door to gather information and to convince 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 set 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 which guarantees freedom of speech, use of political data is not protected. In this regard, European countries have developed general privacy rules in comparison with the US, which could be used to step-up anti-disinformation efforts.

[39] 23 November 2016 (2016/2030(INI)) : § 52 :"*The European Parliament) underlines that particular attention should be paid to new technologies-including digital broadcasting, mobile communications, online media and social network, including those of regional character-which facilitate the dissemination of information about….*"
[40] Freedom on the Net 2017, Manipulating Social Media to undermine Democracy
[41] http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/07/ct2018.pdf

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*". It refers 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 rumor 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 increases. 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 make any difference between real news and false news[45]. When President Donald Trump was interviewed by the journalist Lesley Stahl - it was the first television interview with Donald Trump after his 2016 election as president - he said he bashes the press to "*demean*" and "*discredit*" reporters, so that no one will 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 destabilize voters who lose their points of reference.

43. The increasing use of digital tools in political campaigning has a serious financial impact which has to be taken in account.

All Member States of the CoE have introduced regulations on political finance in compliance with Recommendation 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 the GRECO.

In most of the 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.

[42] https://www.ft.com/content/8e63b372-8f19-11e8-b639-7680cedcc421

[43] Rapport n° 677 (2017-2018) de Mme Catherine Morin-Desailly, fait au nom de la commission de la culture, de l'éducation et de la communication du Sénat, déposé le 18 juillet 2018

[44] https://plato.stanford.edu/entries/relativism/

[45] Fake News, Wohin das Auge reicht, Slavoj Zizek, Neue Zürcher Zeitung, 6 August 2018

[46] https://www.cnbc.com/2018/05/22/trump-told-lesley-stahl-he-bashes-press-to-discredit-negative-stories.html

In the UK, during the Referendum campaign on the EU Vote Leave (as the designated lead 'Leave' group), where digital campaigning was largely used, concern has been expressed on the funding of these digital tools. The permitted expenditure limit was £7 million during the Referendum campaign on the EU. 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] that are made to influence an electoral campaign, together with digital electoral campaigns conducted from abroad to influence voters, make the rules on political finance based on transparency much more fragile 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 have 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 the data which it has stored at the request of an advertiser, unless, having obtained knowledge of the unlawful nature of that 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 Commission issued a Recommendation on measures to effectively tackle illegal content online, which we will refer to in point 97[51].

[47] § 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 knowlefge or awareness, acts expeditiously to remove or to disable access to the information.
2. Paragraph 1 shall not apply when the recipent of the service is acting under the authority or the control of the provider. »

[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

45. In the context of countering the practice of the spreading of false information, two options are possible: the 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 what organizations or individuals paid for political advertisements and who the intended targets are.

47. In January 2018, the European Commission set up a high-level group of experts (”HLEG") to advise on policy initiatives to counter Fake News and disinformation which is 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 multi-dimensional 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 their circulation online;
2. promote media and information literacy to counter disinformation and help users navigate the digital media environment;
3. develop tools for empowering users and journalists to tackle disinformation and foster a 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 upcoming EU elections in May 2019, the European Union expressed its concern regarding possible risks of disinformation before the 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 present further actions, including action of a regulatory nature. 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 in tackling 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.

[52] https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation

[53] A. Bensamoun, Stratégie européenne sur l’intelligence artificielle : toujours à la mode éthique, Recueil Dalloz 2018, p.1022

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

51. Concerning activities of online platforms, the HLEG reminds us that it pursues three aims:

- advertising networks not placing advertisements on websites identified as purveyors of disinformation, this directly reduces the income from disinformation providers;
- advertising providers not accepting advertisements from disinformation sources and clearly describing political advertisements as sponsored content to create transparency; and
- advertising networks not distributing revenues to sites and partners until they have been able to confirm that they operate within relevant terms and conditions.

52. Over the past month, Facebook has been investing in advertisements globally, proclaiming the fact that "*Fake accounts are not our friends*." But the above-mentioned report of the Committee of the House of Commons takes the view that the serious failings in the company's operations that resulted in data manipulation, resulting in misinformation and disinformation, have occurred again[54]. Before the Committees for Legal Affairs and Culture of the French Senate, one manager of Google France let it be known that Google took many initiatives against disinformation online such as the removing of advertising which was used to disseminate Fake News, the implementation of the principle « *follow the money* » in the fight against disinformation, and changes of the references of algorithms related 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 this autumn, Facebook, Google and Twitter have stated that they will check if campaigners are based in the US and that they will publish databases of the political adverts that they have been paid to run[57]. Facebook removed 32 accounts and pages on its platform regarding the next mid-term elections at the US Congress[58]. It created networks of false counts and events. It used networks to identify and neutralize "*bad actors*". 652 pages created in Iran and disseminating pro-Iranian messages have been blocked[59].

53. Fact-checking the narrative through action of fact-checking Internet entities (such as Snopes. Com) should be strenghtened. For instance, the director of Pagella Politica[60], an Italian independent fact-checking organization emphasizes the efforts of its structure: "Once *we find a news article that is obviously false, we write a fact-checking piece that is published in a specific section or our website and we provide its link to Facebook*"[61]. The international Fact-checking network IFCN Code of Principles has to be quoted too. The German Research Center for Intelligence (Deutsche Forschungszentrum für künstliche Intelligenz GmbH-DFKI) develops for instance an application to identify fake pictures which are used to deliver false information and which have been originally published in a quite different context[62].

[54] § 133https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/363.pdf
[55] Rapport n° 677 (2017-2018) de Mme Catherine Morin-Desailly, fait au nom de la commission de la culture, de l'éducation et de la communication du Sénat, déposé le 18 juillet 2018
[56] Jeff Chester, The role of Digital marketing in political campaigns, Center for digital democracy Washington DC, 31 Dec 2017
[57] Digital campaigning, Increasing transparency for voters, The Electoral Commission, p.12, June 2018
[58] Facebook deckt neue gefälschte Konten auf, 2 August 2018, Neue Zürcher Zeitung
[59] « Fake News » : la tech américaine orchestre sa réplique, 23 août 2018, Les Echos
[60] https://pagellapolitica.it
[61] https://www.theatlantic.com/international/archive/2018/02/europe-fake-news/551972/
[62] DFKI Newsletter 40, 2017

But we must remember that every day, hundreds of million of pieces of information are circulating on the web. Fact-checkers would 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 don't 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 who 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 it is notoriously understaffed. A March 2018 report of the Atlantic Council recommended that the EU requires all Member States to provide a seconded national expert to boost this task force[64].

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

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, which will enable the government to prosecute people suspected of spreading "*false*" information on the Internet. That was the case of Malaysia last April and Belarus last June[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 of the Partido Popular at the Spanish Lower House the 17 July 2018. It rejected this Bill, which aimed at developing the monitoring capacities of the intelligence services relating to disinformation[68].

[63] https://euvsdisinfo.eu/news

[64] http://www.europarl.europa.eu/thinktank/en/document.htmlreference=EPRS_ATA(2018)620230

[65] Commission v. France, 22 october 1998, C-184/96

[66] Lukaschenkos Schlag gegen den Journalismus, 10 August 2018, Neue Zürcher Zeitung

[67] Markus Reuter, Stellungsnahme Auschuss Digitale Agenda, Deutscher Bundestag, Netzpolitik.OrG

[68] https://www.antena3.com/noticias/espana/congreso-debate-este-martes-como-reforzar-lucha-noticias-falsas-fake-news

58. In Europe, Freedom of expression is enshrined by article 10 of the European Convention of Human Rights[69]and by article 11 of the Charter of Fundamental Rights in Europe[70]. In the case of Handyside v. the United Kingdom of 7 December 1976, the ECHR 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, amongst other things, that every" *formality",* "*condition*", "*restriction*" or "*penalty*" imposed in this sphere must be proportionate to the legitimate aim pursued. In another judgement[71], the Court of Strasbourg considered that in electoral campaigns, the dissemination of news has to 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 ECHR 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 seen foreseeable and had not afforded the applicant the degree of protection he was entitled by the rule of law in a democratic society[72]. Blocking a user's access to YouTube without a legal basis infringes the right to receive and impart information[73].

60. Member States of the CoE 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[74].

---

[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. 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. "*

[70]*"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 "*

[71] Salov v. Ukraine 6 September 2005, 655118/01

[72] Ahmet Yildirim v. Turkey, 18 December 2012,3111/10

[73] Cengiz and Others v. Turkey, 1 december 2015, 48226/10 and 14027/11

[74] Dink v. Turkey, 14 September 2010, 2668/07, 6102/08, 30079/08, 7072/09 and 7124/09

61. The existence of facts can be demonstrated, whereas the truth of value judgments is not susceptible of proof. The 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[75].

62. Besides the jurisprudence of the ECHR, reference has to be made to the standards adopted by the CoE: Recommendation CM/Rec (2016) of the Committee of Ministers to Member States on Internet Freedom (13 April 2015), calling 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 a convention on Cybercrime in Budapest the 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 of damaging the democratic process.

63. For a comprehensive overview of international standards in this field, the 2017 Joint Declaration on « *Fake News* », Disinformation and Propaganda adopted by the Special Rapporteurs[76] expresses the concern of international organizations on online disinformation. It higlights 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[77].

64. There is therefore a strong need and a significant demand for regulations which would go beyond a simple self-regulation 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 in 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 which 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 contacts initiated with political parties and candidates. For regular contacts, people have to be informed on the processing of data (nature of data, purpose of the processing, conditions under which they may express their opposition to this processing). For occasional contacts the consent of the person for the processing is required[78]. These rules are similar to EU standards.

---

[75] Jerusalem v. Austria, 27 Mai 2001, 26958/95

[76] They are designated by the UN, the OSCE, the OAS and the ACPHR to promote international cooperation and articulate standards relating to freedom of expression, media freedom and media

[77] 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. »

[78] https://www.cnil.fr/fr/communication-politique-quelles-sont-les-regles-pour-lutilisation-des-donnees-issues-des-reseaux

66. Fake News is already regulated by an article of 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[79]. Three conditions are required: news which is published, duplicated or disseminated is false, the publication has the potential of disturbing the public order and 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 cases of cases being brought to court. Dissemination of false news is punished with a fine of €45 000. These rules were extended to online information in 2004.

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*".

68. Dissemination of false news to influence the vote or to let voters to abstain is punished by one year of imprisonment and a fine of € 15 000 (Article L.97 of Electoral Code).

69. Dissemination of false news may affect the legality of the vote and render the election null and void. It happened when it was announced that a candidate whithdrew his candidacy in favour of another candidate. The Council of State as electoral judge considered this was able to affect the fairness of the outcome. It entailed cancellation of the election[80].

70. In 2018, after suspected Fake News came to light concerning Emmanuel Macron during the Presidential electoral campaign 2017, a Members' bill aimed at preventing Fake News during electoral campaigns when the act comes from the territory of a Member State of the EU. This draft was criticized by the press and lawyers. After a first reading by the National Assembly, the Senate rejected it. It considered that it was unable to solve the question raised by disinformation and that it was contrary to freedom of expression during electoral campaigns and feared that the process could be abused for political purposes. However, the draft is again on the agenda of the National Assembly, which is to have the "*final say*".

71. The draft 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 on their own identity and quality or of that of the third party for which it sponsors the 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 allegedly false or implausible deliberately, artificially and massively disseminated information online. This notion of artificial and widespread dissemination will be a clue for 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 this campaign.

[79] Jurisclasseur Communication. Fascicule 3210. Patrick Auvret. Fausses nouvelles

[80] CE, 14 April 1999, 196924. Jurisdata 1999-050242

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

75. The Conseil supérieur de l'Audiovisuel (CSA), the French Regulatory Broadcast 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 the dissemination of fake news or violated pluralism of streams of opinion.

Germany

76. Freedom of expression is provided for in Article 5, §1 of the Fundamental Law, covering freedom of expression and freedom of dissemination[81]. Proceedings launched by the Turkish Head of State against a German journalist who attacked Recep Tayip Erdogan was rejected. The Prosecutor considered that the act could not be regarded as an offence[82].

77. According to Criminal Law, a distinction has to 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 denial of crimes committed under Nazi rule, and specifically, the denial of the 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[83]. Insults are sanctioned with a fine or an imprisonment to two years. The same sanctions apply to deliberate insults against individuals. Claims for removing of news are not explicitly regulated but fixed by the judiciary.

78. The person who offers a platform for news, comments, blogs and Internet fora - in compliance with EU law - (§ 44) is considered as a Host provider according to § 10 of the "*Telemediengesetz*" and is not entitled to monitor actively the contents of the messages regarding requirements of Law and Criminal Law. But when they have knowledge of such messages or content, it must remove them immediately.

[81] BVerfGE 54, 208 57, Heinrich Böll, 03.06.1980

[82] Brauer, Generalstaatsanwalt, Koblenz, Ermittlungsverfahren gegen Jan Böhmermann wegen Beleidigung von Organen und Vertretern ausländischen Staaten usw. Vermerk zur rechtlichen Bewertung 13.10.2016

[83] 1 BvR 673/ 18. Bundesverfassungsgericht stärkt Meinungsfreiheit, Frankfurter Allgemeine Zeitung, 4 August 2018

79. Since 1 October 2017, the *Netzwerkdurchsetzungsgesetz*[84] (Network Enforcement Act - NetzDG) is in force. Named the « *Facebook Act* », the NetzDG clearly is directed to social sharing platforms that are designed to enable individual communication, as the NetzDG aims to fight hate speech and the sharing of criminal content (anti-constitutional, terrorist, child pornography, etc. – but also defamatory)[85]. Providers of social networks which receive more than 100 complaints per calendar year 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 has to contain the following:

1. General observations outlining the efforts undertaken by the provider of the social network to eliminate criminally punishable activity on the platform;

2. Description of the mechanisms for submitting complaints about unlawful content and the criteria applied in deciding whether to delete or block unlawful content;

3. 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;

4. Organisation, personnel resources, specialist and linguistic expertise in the units responsible for processing complaints, as well as training and support of the persons responsible for processing complaints;

5. Membership of industry associations with an indication as to whether these industry associations have a complaints service;

6. Number of complaints for which an external body was consulted in preparation for making the decision;

7. 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. Platforms that are not established 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 has to be deleted or blocked *"immediately*", meaning within a seven-day time limit during which the content is "*evaluated*". This obligation does not apply to complaints lodged through means other than the complaint-management procedure. Very likely, geo-blocking would not suffice.

[84]https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf?__blob=publicationFile&v=2

[85] https://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

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

83. A number of lawyers deems the law 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 (fight against intoxication of the mood of the country, « *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; the compliance of the Act with the law relating to privacy. Jurisprudence of the German Constitutional court, of the Court of Justice of the European Union and of the ECHR would need to clarify these points.

United Kingdom

84. The British Electoral Commission called on increasing transparency for voters with regard to the practice of digital electoral campaigns. It made recommendations about the responsibility of digital campaigns, spending on digital campaigns, transparency on payments for digital campaigns and enforcement of these rules[86].

United States

85. The Honest Ads Act presented in October 2017 before the US Congress introduces disclosure and disclaimer rules to online political advertising. Technology companies would have to keep copies of election advertisements and make them available to the public. The advertisements would also have to contain disclaimers similar to those included in TV or print political advertisements, informing voters who paid for the advertisement, how much, and whom they targeted. The date and time when the first advertisement was first displayed also needs to be provided [87]. Twitter pledged to support the bipartisan bill was by Sen. Amy Klobuchar (D-MN), Sen. Mark Warner (D-VA), and former Sen. 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 is a comprehensive effort being made to implement new regulations to counter disinformation. However, there are many obstacles to draft effective rules that are compatible with constitutional and international standards which will make the exercise difficult[88].

[86] Digital campaigning, Increasing transparency for voters, The Electoral Commission, June 2018
[87] https://www.warner.senate.gov/public/index.cfm/the-honest-ads-act
[88] It is the reason why the French State Council gave its legal opinion on the draft private Members' bill on Fake news http://www.conseil-etat.fr/Decisions-Avis-Publications/Avis/Selection-des-avis-faisant-l-objet-d-une-communication-particuliere/Lutte-contre-les-fausses-informations :

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

2. Recommendations

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

2.1. Definition of terms

89. "The words" *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""*[89]. The same working group estimates 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 allow public authorities not to get 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 ECHR: "*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 ECHR*"[90].

[89] A multi-dimensional approach to disinformation, Report of the Independent High level Group on Fake News and Online disinformation, European Commission, 2018, p.10

[90] 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 the 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 Union, lays down ways of identification of operators of essential services.

97. A Recommendation of the European Commission of 1 March 2018 on measures to effectively tackle illegal online content[91], 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.

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

98. American and French draft legislation and the British Electoral Commission have the same views on the need to identify who is behind these online platforms. To fulfill 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 spending limits of 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 transparency of 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 becomes 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[92], institutions of the EU 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 disseminates 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 50 000 000 or more unique monthly visitors, during a majority of the months during 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.

101. For the same purposes, the British Electoral Commission invites campaigners to report how much they have spent to produce and send 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 on 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.

[92] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/uri=CELEX:52018DC0236&from=en

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, Former Yugoslav Republic of Macedonia). In this context, parties and candidates are not required to record income and expenditures incurred before this period even if they are related to an election campaign. So short campaign periods have to be drawn into question and must be extended to avoid the risk 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 as part of electoral expenditure if there is no other provision on these matters and should be included in the ceilings of expenditures of the parties, candidates and of relevant third parties, if need be.

106. Should spending on digital campaigns from a foreign country be banned? Would it come up against the right of freedom of expression?

107. In different Member States of the CoE, there are members of Parliament who represent voters overseas (France, Portugal and Romania, for instance). These are voters of Member States who live abroad but who vote in their motherland where they are registered as voters and in the EU. 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 widespread rule in the CoE (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 expenditures are admitted? Foreign electoral digital expenditures could be regarded as in-kind donations from third parties. Moreover, a ceiling on electoral expenditures 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 decided to prohibit donations from foreign companies. As foreign companies do not vote, a ban of 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 make political advertisements on radio and television, the ECHR took the view it required to balance, on the one hand, the applicant NGO's right to impart information and ideas of general interest which the public is entitled to receive, with, on the other, the authorities' desire to protect the democratic debate and process from distortion by powerful financial groups with advantageous access to influential media. The Court 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[93]. 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. This risk which was stressed by the Court of Strasbourg at that time with classical Broadcast may occur with social media, which were not so widespread as today. Candidates and political parties may benefit from powerful and anonymous online platforms, in comparison to other candidates and political parties without any help from social platforms. Unregulated interference of social media in electoral campaigns therefore carries the danger of supporting unfair electoral campaigns.

2.5. Protection of citizens in relation to the processing of personal data regulated by the European General Data Protection Regulation (GDPR)

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

112. In the European Union, the GDPR[94] applies across the European Union as from 25 May 2018, and all Member States had to incorporate it into their own national law by 6 May 2018. It states that **t**he protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(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 that Regulation, 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. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, 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.

[93] Animal Defenders v. UK, 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

[94] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/uri=CELEX:32016R0679&from=EN

114. This Regulation 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 Union law, such as activities concerning national security. It may be considered that electoral matters fall under the sovereignity 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.

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* [95]." Despite the scope of this Regulation, inspiration for a legal framework against disinformation could be sought by the CoE in various of its provisions, because to a certain extent, the purpose of the Regulation and the purposes of a possible legal framework provided by the CoE are the same. Definitions, the requirement of consent of individual persons and the transparency of processing means, could be of some interest for the CoE to guarantee the integrity of electoral campaigns and elections.

116. In view of 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 which is funded by the General budget of the European Union, by donations and contributions. This draft was reported by the Financial Times on 26 August 2018[96]. It assumes the approval of EU Governements 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 in force since 1 January 2017[97]. Article 27, 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 regarding the permitted exploitation of data to define voter profiles.

[95] http://www.consilium.europa.eu/en/press/press-releases/2018/03/23/european-council-conclusions-22-march-2018/

[96] https://www.ft.com/content/0f079dd6-a6f8-11e8-8ecf-a7ae1beff35

[97] Apl. Pr. Dr. Thorsten Koch, Das neue Recht der europäischen politischen Parteien, PRUF, MIP 2018,24. Jahrgang, S.71

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 purposes of the Regulation, any operation or set of operations which is 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.

119. Algorithms should be regulated by these rules only if they rely on personal data. But if this is not the case, it is a blind spot from a legal point of view[98]. This tricky question should therefore be tackled.

2.5.2. Transparency of processing

120. Pursuant to the Regulation, 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 is or will be processed. The principle of transparency requires that any information and communication relating to the processing of that 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 Regulation or in other Union or Member State law as referred to in this Regulation. 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.

[98] Cedric Villani, Donner un sens à l'intelligence artificielle, Pour une stratégie nationale et européenne, 2018, p.148

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[99] 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 is bringing 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[100].

2.7. Summary procedure in case of urgency

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

-The ECHR considers that the words may be more exaggerated during electoral campaigns than usual. During electoral campaigns, verbal excesses are admitted[101]. As a result, the question of the applicability of this interference may arise.

- On the one hand, in France as in Germany, the judge would not have much time to appreciate if disinformation is a threat for the public order and is able to destabilize the 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 will enable a candidate who is subject to attacks and junk news to reply.

-If this option was selected by the CoE, 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[102].

[99] Conseil d'Etat, Le Numérique et les droits fondamentaux, 2014, p.273 and 278-281
[100] https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_ai_gb_web.pdf, p.50
[101] ECHR, Brasilier v. France, 11 April 2006, 71343/01
[102] CJEU, UPC Telekabel, 27 March 2014, C-314/12

2.8. Cooperation with different stakeholders

125. As it is underlined by the HLEG, an effort should be made to heighten awareness of the media, information literacy and the educational system to the dangers of various digital mechanisms of disinformation. It calls on actions to support media and literacy programmes for citizens of all ages.

126**.** Stakeholders are platforms, fact-checkers, journalists, media and research organizations.

Fact-checking is today a piecemeal activity in the Member States. Initiatives should be taken by Member States to develop platforms of fact-checking.

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, media innovation projects.

128. Defence of freedom of expression, free press and pluralism, support of quality journalism are key points of the programme of action of the HLEG. Regarding this point, trust in news depends upon the country concerned. This trust in news organisations and journalists amounts to 62% in Finland and to 23% in Greece. Only 7 Member States of the CoE have a rate over 50 % among the 21 Member States analysed by Reuters in its late report 2017[103]: Finland, Portugal, Poland, the Netherlands, Spain, Germany and Denmark. 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 organizations.

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, distinction of political advertising from other contents and the cooperation 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[104]:

- the need for representatives of civil society to audit operators. Actions driven in the USA by Team Up turn[105], Propublica[106], Electronic Frontier Foundation[107] may be referred to in this context;

- the promotion of ethics in the training of engineers, technicians, 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. It could disseminate guides to good practice, elaborate codes of conduct and give advice to Government.

[103]https://reutersinstitute.politics.ox.ac.uk
[104] Cedric Villani, Idem
[105] https://www.teamupturn.org/
[106] https://www.propublica.org/
[107] https://www.eff.org/

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 the 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; with the guidelines provided for by the Recommendation of the European Commission 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.

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

2.10. Enforcement

133. But if government 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 measures as may be necessary to establish jurisdiction over any offence of dissemination of false and misleading information. But how can the detection, investigation and prosecution of this offence be imposed on a state where the offence was committed, if it 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 are focused on service providers. In accordance with the principle of liability exemption and diverse provisions of the European Union on transparency, these legal provisions require from service providers transparency on their activities and protection of personal data. An accelerated legal procedure would be set up in case of urgent matters.

Electoral Law regulations: longer electoral campaigns, transparency of financial resources of providers and a ban on electoral expenditure for digital activities by a foreign legal or physical person, could provide the basis of an efficient legal framework.

Good practice: other measures will concentrate on fact-checking, cooperation with all stakeholders, ethics, development of literacy programmes, and self-regulation of service providers, 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 is 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 erodes 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 classical techniques;

Recognizing 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 (GDPR), which aims at respecting personal data, obtaining user consent and which imposes social media platforms to 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. It is a paradox that the European voter is less protected than the European consumer;

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

Welcoming recent actions and further developments of the European Union in combating disinformationthe in view of the election of the European Parliament;

Within a given timeframe, Member States of the Council of Europe should 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 to ensure free and impartial information during electoral campaigns, 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;

- Make an inventory of different existing types of self-regulation and statutory regulation regarding digital campaigns which apply among Member States;

- Define the length of electoral campaigns to avoid the risk of significant digital campaigns before the electoral campaigns;

- Require imprints of digital material to know who is behind online platforms;

- Obtain disclosure of spending made 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 that personal data is not disclosed without the consent of the citizen in question;

- Set up 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 initiatives of fact-checking through a network across the Council of Europe, with the objective of promoting the growth of broadly based operations;

- Educate and empower users to better access and use of online information, and informing users when content is generated or spread by a bot or algorithms;

- Foster education of all players involved in digital technologies having an impact on elections in the subject of ethics;

- 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;

- Support for quality media organizations and journalism;

- Create an Ethics Commission in every Member State and assigning 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 cooperation group between Member States to support and facilitate strategic cooperation and the exchange of information.

Conclusion

136. Electoral Law is part of the sovereignty of states. It is related to their historical background, the organization 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 electors in the choice of their representatives, there are no common regulations. But the impact of invasive digital techniques within the framework of globalization creates a new context, which requires international instruments to protect European democracies which face common threats.

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

138. A European legal instrument promoted by the CoE could provide a common direction for a comprehensive framework. A Council of Europe instrument could ensure a level playing field for every Member State. 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. It was the starting point of multiple legal instruments of the CoE on these matters: criminal and civil law conventions, recommendations, resolutions and reports. But even if 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 CoE. It 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 tackle this issue. But this option has the disadvantage to leave room for interpretation to Member States, whereas to be efficient, regulations in this field must be uniform and standardized.

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

142. A convention has the merit of 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 CoE include a monitoring mechanism for ensuring compliance and make provision for non-Member States to become Parties. The elaboration of this convention would start from scratch, because just a few Member States have adopted targeted rules on these matters, which may make its drafting easier if there are not yet existing mechanisms. But negotiation of a convention requires time.

143. Given the consensus reached on the threats of disinformation on the electoral process, the Council of Europe needs to decide on what is 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 the European identity and its constitutional values.