Parliamentary Assembly
Assemblée parlementaire
https://pace.coe.int

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Doc. 15028
08 January 2020

Democracy hacked? How to respond?

Report[1]
Committee on Political Affairs and Democracy
Rapporteur: Mr Frithjof SCHMIDT, Germany, Socialists, Democrats and Greens Group

Summary

The report analyses the impact of disinformation on democracy, especially through the internet and social media. It points to the need to improve the internet's content and architecture, build up the resilience of Europe's democratic systems and societies, counter disinformation, invest in quality journalism and preserve freedom of expression and media and political pluralism, especially in the context of elections.

To address disinformation challenges, the Council of Europe member States are called on to implement a number of strategies from a European and global perspective, in particular with regard to data-driven electoral campaigning on social media and the use of personal data in elections, the promotion of digital literacy skills, fact-checking initiatives, and transparency in political online advertising, as well as researcher's access to data, security agency co-operation, self-regulation frameworks for media companies and appropriate judicial reforms. The Committee on Political Affairs and Democracy supports the Venice Commission's efforts to prepare a list of principles for the use of digital technologies in the context of elections.

1. Reference to committee: Bureau decision, Reference 4353 of 22 January 2018.

Contents **Page**

A. Draft resolution[2]

1. The Parliamentary Assembly is concerned about the scale of information pollution in a digitally connected and increasingly polarised world, the spread of disinformation campaigns aimed at shaping public opinion, trends of foreign electoral interference and manipulation, as well as abusive behaviours and hate amplification on the internet and social media, which all represent a challenge for democracy and in particular for the electoral processes throughout Council of Europe member States.

2. As regards cyberattacks, the Assembly recalls the concerns raised in Resolution 2217 (2018) and Recommendation 2130 (2018) "Legal challenges related to hybrid war and human rights obligations", in particular with regard to numerous cases of mass disinformation campaigns intended to undermine security, public order and peaceful democratic processes, and to the need to develop tools to protect democracy from "information weapons".

3. As the internet and social media seep into more aspects of the political landscape, the Assembly points to the need to improve the internet's content and architecture, build up the resilience of Europe's democratic systems and societies, counter disinformation, invest in quality journalism and preserve freedom of expression and media and political pluralism, especially in the context of elections.

4. The Assembly takes the view that data-driven electoral campaigning on social media, based on segmentation and profiling of users, especially dark adverts on platforms targeting potential voters, is a growing phenomenon which must be better regulated, in order to ensure transparency and data protection, and build public trust. The Assembly in particular:

4.1. praises the work that has been done by the Council of Europe on personal data protection and electoral rights, in particular the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS N°108) and its relevance with regard to electoral rights, and welcomes and other soft law instruments addressing different aspects of privacy and personal data protection in the context of information society, including in social networks;

4.2. welcomes the adoption of the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223) modernising the convention and addressing emerging challenges resulting from the use of new information and communication technologies, and supports the call of the United Nations Special Rapporteur on the Right to Privacy, Mr Joseph A. Cannataci, to all United Nations member States to accede to Convention 108, where their legislation and practice comply with the provisions of the Convention;

4.3. supports the future work of the Committee of Convention 108 on the use of personal data in elections and their possible misuse in a political context.

5. To address disinformation challenges in the context of democratic elections, governments of Council of Europe member States need to:

5.1. recognise the transnational nature of the problem and enhance co-operation with internet intermediaries and social media operators, whose commercial interests tend to collide with human rights and political rights, for instance the principle of electoral equity, in line with the Committee of Ministers' Recommendation CM/Rec (2018)2 on the roles and responsibilities of internet intermediaries;

5.2. enable voters to receive trustworthy information and become more informed and engaged, with a view to preserving the exercise of their right to truly free and fair elections;

5.3. break up the monopoly of tech companies controlling, to a great extent, citizen's access to information and data.

6. To tackle these challenges, the Assembly calls on Council of Europe member States to implement a number of strategies from a European and global perspective and to create a model that includes co-responsibility and multiple regulatory and conflict-resolution approaches, in particular by:

6.1. promoting media education and digital literacy skills to strengthen the legal and democratic culture of citizens, in line with Resolution 2314 (2019) on Media education in the new media environment, enhance public awareness of how data are generated and processed, empower voters toward a critical evaluation of electoral communication and increase society's resilience to disinformation;

2. Draft resolution adopted by the committee on 9 December 2019.

6.2. encouraging and supporting collaborative fact-checking initiatives and other improvements of content moderation and curation systems which are intended to counter the dissemination of deceptive and misleading information, including through social media, in line with Resolution 2281 (2019) "Social media: social threads or threats to human rights?";

6.3. securing adequate funding to independent public service media, so that they can allocate enough resources to innovation in content, form and technology to foster their role as major players in countering disinformation and propaganda and as a cutting-edge stakeholder in protecting communication and media ecosystems in Europe, in line with Resolution 2255 (2019) "Public service media in the context of disinformation and propaganda";

6.4. strengthening transparency in political online advertising, information distribution and algorithms and business models of platform operators, in particular by:

6.4.1. guaranteeing, where political parties and candidates have the right to purchase advertising space for election purposes, equal treatment in terms of conditions and rates charged;

6.4.2. developing specific regulatory frameworks for internet content at election times and include provisions on transparency in relation to sponsored content on social media, so that the public is aware of the source that funds electoral advertising or any other information or opinion, in line with Resolution 2254 (2019) "Media freedom as a condition for democratic elections", and prevent illegal foreign involvement;

6.5. addressing the implications of micro-targeting political ads with a view to promoting a political landscape which is more accountable and less prone to manipulation;

6.6. supporting researcher's access to data, including datasets with deleted accounts and content, with a view to examining the influence of strategic disinformation on democratic decision making and on electoral processes, and possibly propose the setting up of a European network of researchers in this area;

6.7. considering national and international regulation to share best practices and increase security agency co-operation, for instance by creating a specific mechanism for monitoring, crisis management and post-crisis analysis and sharing resources that already exist in various countries, in line with Recommendation 2144 (2019) "Internet governance and human rights";

6.8. calling on professionals and organisations in the media sector to develop self-regulation frameworks that contain professional and ethical standards relating to their coverage of election campaigns, including enhanced news accuracy and reliability and respect for human dignity and the principle of non-discrimination, in line with Resolution 2254 (2019);

6.9. initiating judicial reforms and set-up specialised divisions for judges and prosecutors focusing on disinformation and hate speech.

7. Furthermore, the Assembly welcomes the European Union's action to counter disinformation, address the threats of external intervention in European elections and ensure greater transparency on paid political advertising and clearer rules on the financing of European political parties, as part of the forthcoming European Democracy Action Plan for 2019-2024. It calls on the European Union to ensure synergy with the Council of Europe's action in those areas and promote further co-operation with all 47 member States of the Council of Europe.

8. Finally, the Assembly supports the work of the European Commission for Democracy Through Law (Venice Commission) in its efforts to prepare a list of principles for the use of digital technologies in the context of elections and resolves to closely follow this matter.

B. Explanatory memorandum by Mr Frithjof Schmidt, rapporteur

1. Introduction

1. I was appointed rapporteur on 12 March 2018, following a current affairs debate at the Standing Committee meeting in Copenhagen, upon the initiative of our colleague Mr Emanuelis Zingeris (Lithuania, EPP/CD), in November 2017 entitled *Democracy hacked? How to respond?*,[3] which was then referred to the Committee on Political Affairs and Democracy for report. The change of public structures by means of modern technologies and social networks in the functioning of European democratic systems and the impact of information disorder – i.e. misinformation, disinformation and malinformation – on electoral processes are clearly a matter of interest to our committee.

2. At the outset, I would like to raise the following questions: does the introduction of digital public structures threaten our public debates and current model of representative democracies? How can we increase society's resilience to disinformation? Is there not a risk that the way social media operates, by accentuating what researchers call "cocooning", i.e. the tendency of connected groups of individuals to keep to themselves and only follow "news", whether true or false, that confirms their points of view, as well as the business logic of platform operators and the lack of transparency in information distribution will cut these groups of web users off from confronting views they do not share? In other words, if democracy involves acceptance of debate among people who hold different views, does this trend not render this aspect of democracy obsolete?

3. The relationship between democracy and a new technological environment is a complex one. On the one hand, the internet and social media have become a central platform of political interaction. In some democracies, the use of technology tools has facilitated democratic participation and political activism. On the other hand, internet and social media can endanger the voters' free will or the principle of equal opportunities for all candidates as well as voters' rights to privacy.

4. As a matter of fact, the increase of content production[4] and the centralisation of online distribution channels such as Twitter, Google and Facebook have had several unintended consequences: the proliferation of private and public disinformation tactics, and most importantly, the arrival of non-regulated private actors in the democratic arena that literally "owns" the information infrastructure and gateways to information. Virtual tools can be used as a threat for the integrity of the elections in several ways, such as suppressing voter turnout, tampering with election results, stealing voter information, conducting cyberespionage or doxing of candidates for the purposes of manipulation and shaping the opinions of voters.

5. In relation to defence, cyberattacks are becoming increasingly significant in what is now called "hybrid warfare", a new type of warfare combining conventional and non-conventional methods. This also involves a redefinition of conventional military strategy concepts of attack and defence. In this context, there is a great risk of civil society being targeted directly and its rights being jeopardised. The importance of this issue is without doubt; however it falls outside the scope of my report. I therefore refer to Resolution 2217 (2018) and Recommendation 2130 (2018) "Legal challenges related to hybrid war and human rights obligations", adopted by the Assembly on 26 April 2018, and to the reply by the Committee of Ministers of 13 December 2018.

6. My intention is to focus on issues related to disinformation, internet infrastructure and transparency and their impact on the democratic process and on elections. I shall discuss how European countries respond to the issue of disinformation, especially in the context of elections, and present the work done by the Council of Europe and the European Union as well as social media companies' self-regulation efforts.

7. On 25 June 2018, the committee held a first exchange of views on security in elections with the participation of Ms Simona Granata-Menghini, Deputy Secretary of the European Commission for Democracy through Law of the Council of Europe (Venice Commission), and on information disorder with the participation of Mr Patrick Penninckx, Head of the Information Society Department of the Council of Europe Directorate General of Human Rights and Rule of Law.

---

3. https://pace.coe.int/documents/10643/4007015/AS-PER-2017-PV-03-EN.pdf/a862c5d8-2417-453a-9d9d-9cd0b7d6d0c8.

4. According to 2018 Global Digital report 2018, more than 4 billion people around the world use the internet each month and more than 3 billion use social media. The average internet user spends around 6 hours each day using internet-powered devices and services.

8. On 11 September 2018, the committee held another hearing with Ms Divina Frau-Meigs, Professor, sociologist and media researcher at the University Sorbonne Nouvelle, Paris, and Mr Ben Scott, member of the management board of the think tank Stiftung Neue Verantwortung and policy adviser for innovation at the State Department during the Obama administration.

9. On 15 May 2019, I paid a visit to Stockholm to discuss this matter with the Swedish authorities[5] who have been confronted with attempts to interfere in their elections and have a comprehensive vision of possible responses to share with other Council of Europe member States.

10. Finally, on 14 November 2019 in Berlin, the committee organised a joint hearing with the Committee on Legal Affairs and Human Rights, with the participation of Mr Georg Thiel, President of the German Federal Statistical Office and Federal Returning Officer; Ms Astrid Schumacher, Head of Branch "IT Security Consulting and Security of Classified Material" at the German Federal Office for Information Security; Mr Johan Farkas, from Malmö University; and Ms Ulrike Klinger from the Institute for Media and Communication Studies, at Freie Universität in Berlin. During the meeting, I was also provided with valuable information from our colleague Mr Emanuelis Zingeris, who is preparing an opinion to this report.

11. I believe it is time for all Council of Europe member States to assume greater responsibility and to work to combat disinformation, preserve the integrity of elections, protect democracy and strengthen the principle of accountability on the part of social media themselves.

2. The extent of the problem

12. According to Freedom House, manipulation and disinformation tactics played an important role in elections in at least 18 countries in 2017, damaging citizens' ability to choose their leaders based on factual news and authentic debate and giving rise to what has been named "digital authoritarianism". At the same time, governments around the world are tightening control over citizens' data and using claims of "fake news" to suppress dissent, eroding trust in the internet as well as the foundations of democracy.[6]

13. In January 2018, Swedish security chief Anders Thornberg, in the context of the Swedish general elections, pointed to several examples of fake news articles that sought to create division and undermine trust, including one that claimed that Muslims had vandalised a church. The latter was spread, using bots,[7] which were from outside Sweden. He pointed out the national security implications when a foreign actor uses such disinformation campaigns.[8] In January 2019, Facebook took down two large-scale disinformation operations linked to Russian State actors and operating across Eastern and Central Europe.[9] In February 2019, the German authorities arrested a 20-year-old student who confessed to having illegally accessed information on more than 1 000 public figures, including high-ranking politicians[10]. More recently, in November 2019, Facebook announced that it had removed 5.4 billion fake accounts throughout the year.[11]

14. Built as an open and democratic space, the internet is a global village allowing information to spread easily at low cost. Therefore, it is difficult to identify trustworthy information or find those responsible for illegal behaviour online. Online propaganda, disinformation and hate-speech have increased in the digital sphere. In this context, guaranteeing the freedom of voting and fair elections, while preserving freedom of expression, represents a major challenge. If citizens are unable to distinguish between false and true data and are unaware of the conditions under which they exercise their rights and freedoms, the purity of their will might be compromised, as well as the democratic legitimacy of the elections themselves.[12]

---

5. I held meetings with representatives of the Committees on the Constitution and of Defence of the Swedish Parliament, of the Ministry of Foreign Affairs and Culture, researchers on media, information literacy and democratic dialogue, NGOs and civil society actors, the Swedish Civil Contingency Authority as well as the Election Authority.
6. Freedom House, Freedom on the Net 2018, the rise of digital authoritarianism (latest).
7. Social media accounts controlled by computer scripts that try to disguise themselves as human users.
8. BBC News, Swedish security chief warning on fake news, 4 January 2018.
9. https://www.politico.eu/article/facebook-takes-down-two-russian-disinformation-networks-in-eastern-europe/.
10. https://www.politico.eu/article/europe-most-hackable-election-voter-security-catalonia-european-parliament-disinformation/.
11. https://edition.cnn.com/2019/11/13/tech/facebook-fake-accounts/index.html.
12. Venice Commission "Study on the role of social media and the internet in democratic development'', CDL-LA (2018)001; 21/11/2018, 9.

15. Experts claim that misinformation, sometimes backed by governments, has already influenced several major events in Europe. For example, some claim that disinformation may have influenced the Dutch vote on the EU-Ukraine Association Agreement, the result of the Brexit vote, the debates around the independence of Catalonia, and immigration issues in Italy.

16. According to the Final Report of the UK House of Commons' Digital, Cultural, Media and Sport Committee of 14 February 2019, following an 18-month investigation into disinformation, "democracy is at risk from the malicious and relentless targeting of citizens with disinformation and personalised 'dark adverts' from unidentifiable sources, delivered through the major social media platforms".[13]

17. Furthermore, according to a Venice Commission study, the use of artificial intelligence (AI) during election campaigns raises ethical and democratic questions as there is evidence and further possibility to use them to manipulate citizens and influence the electoral results.[14] Ms Deborah Bergamini (Italy, EPP/CD) is currently preparing a report for our committee which focuses on the need for democratic governance of artificial intelligence.

18. Behind the rampant disinformation on the internet, I believe there are some key issues which fall within the committee mandate. I also wish to refer to previous resolutions and recommendations based on relevant reports prepared by the Committee on Culture, Science, Education and Media,[15] including a most recent Resolution 2314 (2019) "Media education in the new media environment", which was adopted on 29 November 2019. Regarding the manipulation of democratic opinion-forming processes, especially during elections, the committee should focus on means of increasing transparency, the resources to be allocated to training and research and those assigned to ways of checking information. It is also important to identify governments' responsibilities in terms of protecting citizens through judicial reforms and specialised public prosecutors and how the protection should be implemented at international level through the strengthening of existing conventions and through establishing new international conventions.

19. As for data protection and IT security, I will focus on the protection of a society which I believe must remain open, with safeguards to ensure that the privacy and freedom of all citizens are respected, and that violations are sanctioned under international law.

20. There is a wealth of literature concerning the hacking of democracy, particularly in parliaments. For example, the United Kingdom House of Commons Digital Committee and committees from the French National Assembly and Senate prepared reports on combating the manipulation of information. There are also crucial minutes of major hearings such as those of Mr Mark Zuckerberg, Chief Executive Officer of Facebook, before the United State Senate and House of Representatives, the German authorities and the European Parliament, and of Mr Christopher Wylie, whistle-blower in the Cambridge Analytica affair, before the House of Commons Digital Committee.[16]

3. Manipulation of democratic opinion-forming processes and privacy issues during elections

21. There is much talk nowadays about "fake news", which denotes the deliberate viral spreading of false news on the internet and social media. It is related to fabricated content, manipulated content, imposter content, misleading content, false context or connection, satire or parody.

---

13. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/179102.htm.
14. Venice Commission "Joint Report on Digital Technologies and Elections», CDL-AD(2019)016; 24/06/2019, 10.
15. Resolution 2256 (2019) "Internet governance and human rights"; Resolution 2254 (2019) "Media freedom as a condition for democratic elections"; Recommendation 2033 (2014) and Resolution 1970 (2014) "Internet and politics: the impact of new information and communication technology on democracy"; Resolution 2213 (2018) "The status of journalists in Europe"; Resolution 2212 (2018) "The protection of editorial integrity"; Resolution 2255 (2019) "Public service media in the context of disinformation and propaganda"; Resolution 2143 (2017) "Online media and journalism: challenges and accountability"; Recommendation 2075 (2015) and Resolution 2066 (2015) "Media responsibility and ethics in a changing media environment"; Recommendation 2111 (2017) and Resolution 2179 (2017) "Political influence over independent media and journalists"; Recommendation 2106 (2017) and Resolution 2171 (2017) "Parliamentary scrutiny over corruption: parliamentary cooperation with the investigative media"; Recommendation 2097 (2017) and Resolution 2141 (2017) "Attacks against journalists and media freedom in Europe"; Recommendation 2062 (2015) and Resolution 2035 (2015) "Protection of the safety of journalists and of media freedom in Europe"; Resolution 1877 (2012) and Recommendation 1998 (2012) "The protection of freedom of expression and information on the Internet and online media".
16. https://www.parliament.uk/business/committees/committees-a-z/commons-select/digital-culture-media-and-sport-committee/news/fake-news-evidence-wylie-correspondence-17-19/.

22. In November 2017, the British Prime Minister stated that planting fake news was a way to "weaponise information".[17] From a social point of view, disinformation contributes to forming communities of people who have access to the same opinions, share the same ideology and the same conspiracy stories.

23. Disinformation may take several forms: it may consist of statements or the expression of opinions without any evidence. Even if the initiative behind such manipulation of public opinion is private in origin, some governments may attempt to control social media to shape public opinion and to counter opposition and criticism.

24. New information technologies make democratic processes more accessible to all citizens. From the right of access to information to the formation of centralised registries of voters, the internet makes it easier for everyone to exert their political rights. Furthermore, the internet and new information technologies allow for greater transparency and accountability, as well as for broader and more efficient forms of political participation, and extend the reach of the public sphere, thereby strengthening deliberative democracy However using social media as a news source may result in the phenomenon called "news finds me": people who are not actively seeking information but believe their network will somehow inform them. This perception can lead to lower political knowledge.

25. Social media, understood as "Internet platforms that allow for bidirectional interaction through user-generated content,"[18] can have positive effects on democracy. Today, they constitute a relevant platform of political debate and, as such, they are important sources of political information for and an indispensable part of modern political campaigning[19]. At the same time social media companies are profit-oriented and the problems they can cause for democracy are at best collateral damage.

26. During the 2008 and 2012 US presidential elections, Mr Barack Obama's campaign teams had scores of datasets at their disposal on virtually all voters. There is some indication that strategic disinformation may have had an influence in the election campaign of Donald Trump in the 2016 US presidential elections. The release of the Mueller report in March 2019 shows in great detail that the public discourse associated with the elections was influenced by a number of actors tracked back to Russian sources.[20] During the 2017 French presidential election attempts by Russian actors to influence the electoral process were also detected.[21]

27. Five stages of election meddling have been identified: (1) using disinformation to amplify suspicions and divisions; (2) stealing sensitive and leakable data; (3) leaking the stolen data via supposed 'hacktivists'; (4) whitewashing the leaked data through the professional media; and (5) secret colluding (between a candidate and a foreign State) in order to synchronise election efforts.[22]

28. For a better illustration I recall the Cambridge Analytica case, which involved Facebook users' data being collected and then used during the 2016 US presidential election without their consent. This represents a clear example of affecting opinion-forming process of voters. This micro-targeting operation relied on illegal access to data and machine learning to influence people's emotions. Different voters received different messages based on predictions about their susceptibility to different arguments.[23]

29. Most commonly used AI techniques to influence opinion-formation process of voters are as follows:

– social platforms collect and process information via algorithms, therefore selecting information to be shown according to the preferences of the targeted users. Algorithms evolve quickly so it is difficult to understand the way data is processed and the complex resulting implications. That could be used either for or against a certain party or candidate;

– the information used to produce political ads also includes information collected by political parties. However, targeted advertising does not always allow for the identification of its political nature, nor its sources. Advertising could be placed even by anonymous providers, including ones who are based outside the country where elections are taking place. Monitoring the funding of the campaign therefore becomes an issue;[24]

---

17. https://www.theguardian.com/politics/2017/nov/13/theresa-may-accuses-russia-of-interfering-in-elections-and-fake-news.
18. Definition by International IDEA 2014.
19. For a detailed analysis, I refer to the report by the Committee on Culture, Science, Education and Media on Social media: social threads or threats to human rights? (rapporteur: Mr José Cepeda, Spain, SOC), Doc 14844.
20. https://apps.npr.org/documents/document.html?id=5955997-Muellerreport.
21. Center for strategic and international studies, Successfully countering Russian electoral interference, June 2018.
22. Mika Aaltola, Democracy's Eleventh Hour: Safeguarding Democratic Elections against Cyber-Enabled Autocratic Meddling, Briefing Paper 226 (Helsinki: Finnish Institute of International Affairs, November 2017).
23. The Conversation, How artificial intelligence conquered democracy, 8 August 2017.

– massive dissemination of false or damaging information is also done through fake profiles, many of which are automated. Anonymous profiles, bots and false accounts can be easily created by web centres offering campaign promotion services. By mimicking people's online behaviour, such centres scale up the massive dissemination of information and generate trends of opinion in an artificial way;

– cloning an existing social profile with fake ones that mimic the originals for attributing false information to parties or candidates can be a powerful manipulation technique. Creating a new character who interacts with other profiles by building a reputation and trust is also a common technique. By getting closer to a specific category of voters, the bot can act as an influencer for users.

30. The use of micro-targeted political ads, which are tailored and targeted towards citizens based on their data profiles regarding personal behaviour, preferences, 'likes' on social media, age and gender, have also been criticised by experts. According to many critics, by banning or limiting micro-targeted political ads, our political landscape would both become more accountable and less susceptible to political manipulation.

31. Furthermore, the monitoring of people's online activity without their consent and for the purpose of exploiting their behavioural paths contradicts not only the very principle of free and fair elections but also their right to privacy. I believe we need new international legal instruments to deal with the new public media and communication structure.

32. According to the 2018 EU Special Eurobarometer on democracy and elections, 73% of respondents said they are concerned or very concerned about disinformation or misinformation.[25] Political opponents have an interest in hacking each other and cybersecurity companies profit from their services and counter services in election times. Companies like Twitter and Facebook also acknowledge that fake accounts are a threat to the integrity of elections.[26]

33. A study by the Oxford Internet Institute found that less than 4% of news sources shared on Twitter ahead of the 2019 European Parliament elections was disinformation content, while mainstream professional news outlets received 34% of shares. According to FactCheckEU, there was less disinformation than expected in the run up to the European elections and it did not dominate the conversation as it did around the past elections in Brazil, the UK, France or the United States.[27]

34. However, according to a 2019 European Commission report on the implementation of the Action Plan Against Disinformation,[28] Russian groups or actors carried out a widespread disinformation campaign aiming to suppress turnout and influence voter preferences and using hot-button topics to sow public anger. These covered a broad range of topics, ranging from challenging the EU's democratic legitimacy to exploiting divisive public debates on issues such as migration and sovereignty.

35. In 2019, Facebook announced that advertisers will be required to provide verifiable public contact details before they can run political campaigns on social platforms. The restrictions require advertisers on "political" topics (defined differently in each nation), to prove that they live in the country they are targeting, and to store all their adverts in a public database for seven years, along with information about targeting, spend and reach. The rules require advertisers to disclose who "paid for" the advert, a requirement that has earned Facebook criticism in the past, since the company allowed users to write anything they wanted in the box and did not verify the names. Facebook will continue to allow users to write what they want as the source of the funding but will require they provide at least a phone number or email address through which interested parties can contact the advertiser. Users who advertise in a personal capacity will be free not to enter that information, but their name will be published instead, as verified by the site.[29] Twitter also announced a ban on all political ads and YouTube stated it would delete illegal content in a stricter manner. While these positive steps should be welcomed, in my view it is important to reflect further on international regulation which would apply to all social media companies.

---

24. A report is being prepared on Transparency and regulation of donations to political parties and electoral campaigns from foreign donors (rapporteur: Mr Konstantin Kuhle, Germany, ALDE).
25. https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/SPECIAL/surveyKy/2198.
26. Politico, Europe's most hackable election – The EU faces hackers, trolls and foreign agents as it gears up for a vote in May, 16 January 2019.
27. Oxford Internet Institute, Junk News during the EU Parliamentary Elections, May 2019.
28. https://eeas.europa.eu/sites/eeas/files/joint_report_on_disinformation.pdf.
29. Facebook, Protecting elections in the EU, 28 March 2019.

4. Relevant work by the Council of Europe

36. The work of the Council of Europe on personal data protection and electoral rights has been remarkable. Not only has it adopted the first internationally binding legal instrument, i.e. the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS N°108) but it has produced soft law instruments addressing different aspects of privacy and personal data protection in the context of information society, including in social networks. Our Assembly should support the future work of the Committee of Convention 108 on the use of personal data in elections and their possible misuse in a political context.

37. Under the European Convention on Human Rights, as interpreted by the European Court of Human Rights, member States have an obligation to secure the rights and freedoms for everyone within their jurisdiction, both offline and online. The crucial issue is to determine whether the obligations of the State in assuring equal publicity of political parties and candidates are to be applied to internet intermediaries and if so, in what manner.

38. In this regard, the Committee of Ministers' Recommendation CM/Rec (2018)1 on media pluralism and transparency of media ownership and Recommendation CM/Rec (2018)2 on the roles and responsibilities of internet intermediaries, point to the potentially disturbing impact that online platform's control over the flow, availability, findability and accessibility of information can have on media pluralism. The Committee of Ministers called on member States to act as the ultimate guarantor of media pluralism by ensuring pluralism in the entirety of the multimedia ecosystem.

39. Internet intermediaries, including social media, play a crucial role in providing services of public value and facilitating public discourse and democratic debate. Council of Europe standards set out the intermediaries' responsibilities with respect to ensuring human rights and fundamental freedoms on their platforms, which includes the right to free elections. In this regard, internet intermediaries should be subject to effective oversight and regular due diligence assessments of their compliance with their responsibilities.[30]

40. In 2002, the Venice Commission adopted the Code of Good Practice in Electoral Matters which ensures electoral equity and equality of opportunity. This applies, in particular, to radio and television air-time, public funds and other forms of backing and entails a neutral attitude by State authorities, in particular with regard to election campaigns, media coverage, especially by publicly owned media, and public funding of parties and campaigns. However, the Code also states that "legal provision should be made to ensure that there is a minimum access to privately owned audio-visual media, with regard to the election campaign and to advertising, for all participants in elections" and that "the principle of equality of opportunity can, in certain cases, lead to a limitation of political party spending, especially on advertising."[31]

41. Furthermore, important work is being done by the Venice Commission, which, on 24 June 2019, adopted a joint report, with the Directorate of information society and action against crime, on Digital technologies and elections, which proves relevant to my analysis.[32] The Venice Commission also decided to prepare a list of principles for the use of digital technologies in a human rights compliant manner, in relation to elections. Our Assembly should encourage, support and follow this work, perhaps also via a separate report.

42. In 2011, our Assembly adopted Resolution 1843 (2011) and Recommendation 1984 (2011) on "The protection of privacy and personal data on the Internet and online media". The resolution emphasised that the protection of the right to data protection is a necessary element of human life and of the humane functioning of a democratic society, and that its violation affects a person's dignity, liberty and security.

43. In 2012, the Committee of Ministers adopted two relevant Recommendations on the protection of human rights with regard to search engines and social networking services. In the first text[33], the Committee of Ministers recognised the challenge caused by the fact that an individual's search history contains a footprint which may reveal the person's beliefs, interests, relations or intentions, and could reveal, *inter alia*, one's political opinions or religious or other beliefs. The Recommendation called for action to enforce data protection principles, in particular purpose limitation, data minimisation and limited data storage, while data subjects must be made aware of the processing and provided with all relevant information.

---

30. Venice Commission, "Joint Report on Digital Technologies and Elections", CDL-AD(2019)016; 24/06/2019, 5, 18; CDL-LA (2018)002, 9.
31. See also the report being prepared for our committee by Mr Hendrik Daems (Belgium, ALDE) on Setting minimum standards for electoral systems in order to offer the basis for free and fair elections (Doc. 15027).
32. CDL-AD(2019)016.
33. Recommendation CM/Rec(2012)3.

44. On social networks, the Committee of Ministers recommended that member States take actions to provide an environment for users of social networks that allows them to further exercise their rights and freedoms, to raise users' awareness of the possible challenges to their human rights and of the negative impact on other people's rights when using these services, as well as to enhance transparency about data processing, and forbids the illegitimate processing of personal data.[34]

45. Concerned with the interference of the right to private life by rapid technological developments, in 2013 the Committee of Ministers adopted a *Declaration on risks to fundamental rights stemming from digital tracking and other surveillance technologies*.[35]

46. In 2017, the Council of Europe report on Information disorder: Toward an interdisciplinary framework for research and policy making,[36] which was also presented to our committee, suggests ways to determine the type of response suited to the threat. As the concept of "fake news" is too imprecise, the report makes a distinction between: misinformation – when false information is shared, but no harm is meant; disinformation – when false information is knowingly shared to cause harm; malinformation – when genuine information is shared to cause harm, often by moving information designed to stay private into the public sphere. The report points out that our societies need:

– in the short term, to address the most pressing issues, for instance around election security;

– in the long term, to increase society's resilience to disinformation;

– a structure capable of checking and constantly adapting responses.

47. The report also stresses that new educational reforms must be implemented for young people to be able to deal with the flow of information on the internet as our education systems were designed in the 19th century, long before the digital era.

48. On 19 and 20 April 2018, the 15th Conference of Electoral Management Bodies on Security in Elections, organised by the Venice Commission and the section for elections of the Ministry of local government and modernisation of Norway, showed clearly that the right to free suffrage was facing digital challenges in two respects: voters' freedom to form an opinion and their freedom to express their will. It was also stressed that while criminal penalties should apply to cyberattacks, the effectiveness of judicial responses to date was relatively limited.[37]

49. On 13 February 2019, the Committee of Ministers adopted an important Declaration on the manipulative capabilities of algorithmic processes.[38] The Committee of Ministers called on its 47 member States to tackle the risk that individuals may not be able to form their opinions and take decisions independently of automated systems, and that they may even be subjected to manipulation due to the use of advanced digital technologies, in particular micro-targeting techniques. Machine learning tools have the growing capacity not only to predict choices but also to influence emotions and thoughts, sometimes subliminally. The Committee of Ministers encouraged member States to assume their responsibility to address this growing threat in particular by taking appropriate and proportionate legislative measures against illegitimate interferences, and empowering users by promoting critical digital literacy skills.

50. The Committee of Ministers went as far as stressing the need to assess the regulatory frameworks related to political communication and electoral processes to safeguard the fairness of elections and to ensure that voters are protected against unfair practices and manipulation. It also stressed the significant power that technological advancement confers to those who may use algorithmic tools without adequate democratic oversight or control and underlined the responsibility of the private sector to act with fairness, transparency and accountability under the guidance of independent public institutions.

51. Furthermore, on 26 and 27 February 2019, the Helsinki conference on *Governing the Game Changer – Impacts of artificial intelligence development on human rights, democracy and the rule of law*, organised by the Council of Europe and the Finnish Presidency of the Committee of Ministers, stressed in particular that:

– effective supervisory mechanisms and democratic oversight structures regarding the design, development and deployment of AI must be in place;

---

34. Recommendation CM/Rec(2012)4.
35. https://rm.coe.int/168068460d.
36. Council of Europe report on Information Disorder.
37. Website of the 15th European Conference of Electoral Management Bodies.
38. CM Declaration on the manipulative capabilities of algorithmic processes.

– the functioning democratic processes require an independently informed public, and the encouragement of open and inclusive debates. Public awareness of the potential risks and benefits of AI must be enhanced, and necessary new competencies and skills developed. Due public trust in the information environment and AI applications must be fostered.[39]

52. The World Forum for Democracy, which took place in Strasbourg on 6-8 November 2019, was entitled *Is democracy in danger in the information age?* and focused on the extent to which the information available helps or hinders citizens in taking part in democratic processes. Building resilience to disinformation, Artificial intelligence and information, Fact checking, and Voting under influence were among the themes that are most relevant to my report.

53. I wish to recall an important distinction between "information" and "awareness" which was made by one of the Forum panellists, Mr Enrico Letta, former Prime Minister of Italy. Mr Letta stressed that nothing is as important as giving young people the compass to understand the information they receive abundantly and freely on the internet and social media. Without a compass however, it is impossible to understand a world in which the problem is not lack of information but rather the opposite. In fact, one of the fundamental problems lies in avoiding being buried under an overwhelming quantity of information or being manipulated by it. The real divide which we must fight is the one between those who are 'aware' and those who are passive receivers of information (or disinformation) and therefore easy to manipulate.

5. European Union action and the industry's self-regulatory Code on Disinformation: is this enough?

54. The European Union has been actively tackling disinformation since 2015, when the East StratCom Task Force was set up in the European External Action Service (EEAS) to effectively communicate the EU's policies towards its eastern neighbourhood,[40] with the European Council stressing "the need to challenge Russia's disinformation campaigns".[41]

55. In October 2018, representatives of online platforms, leading social networks, advertisers and advertising industry agreed on a self-regulatory Code aimed at achieving the objectives set out by the 26 April 2018 European Commission's Communication *Tackling online disinformation: a European approach.*[42] They set a wide range of commitments, from transparency in political advertising to the closure of fake accounts and demonetisation of purveyors of disinformation. That was the first time that industry agreed, on a voluntary basis, to self-regulatory standards to fight disinformation.[43] In brief, the Code provides for:

– political ads to be clearly labelled as such and to be shown only under the users' authorisation (targeted on the basis of location);

– an election commission to conduct an independent forward-looking assessment on the role played by Facebook in elections;

– bringing down fake accounts;

– the previous approval of particular content and sources.

56. Google, Facebook, Twitter, Mozilla and the trade associations representing the advertising sector submitted their first reports on the measures taken to comply with the Code, which the Commission published on 29 January 2019. While the Commission welcomed the progress made, it also called on signatories to intensify their efforts in the run up to the 2019 European elections.

57. The monitoring of the Code of Practice is part of the Action Plan against Disinformation to build up capabilities and strengthen co-operation between EU member States and EU institutions to proactively address the threats posed by disinformation. In addition, a Rapid Alert System was set up among the EU institutions and member States to facilitate the sharing of insights related to disinformation campaigns and co-ordinate responses. The system is based on open-source information and also draws upon insights from academia, fact-checkers, online platforms and international partners.

---

39. Conclusions from the Conference.
40. https://eeas.europa.eu/headquarters/headquarters-homepage/2116/-questions-and-answers-about-the-east-stratcom-task-force_en.
41. European Council meeting (19 and 20 March 2015) – Conclusions https://www.eesc.europa.eu/resources/docs/european-council-conclusions-19-20-march-2015-en.pdf.
42. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018DC0236&from=EN.
43. https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation.

58. In January 2019, the European Council also concluded that disinformation should be addressed in the broader context of foreign interference, hybrid threats and strategic communication. This includes the reinforcement of the three strategic communication task forces of the EEAS, which were set up in order to promote fact-based narratives about the EU in the Eastern neighbourhood, the Southern neighbourhood and the Western Balkans.[44]

59. The Code of Practice represents a voluntary approach to disinformation. Whether it will be successful or not is hard to say yet. However, I applaud the action taken by the European Commission to tackle the problem of disinformation and I wish to underline the importance of European and international conventions to work on strengthening the principle of transparency and accountability.

60. Early in 2019, Facebook vowed to protect the integrity of the European Parliament elections by launching new measures to combat strategic disinformation and foreign interference and ensure that the platform was not used to stop the election from being conducted fairly. However, social media companies should be required to act in line with European and international human rights standards.

61. To help prevent foreign interference and make political advertising more transparent, advertisers will be required to confirm their identity and include additional information about who is responsible for their ads.[45] The company said it would expand its fact-checking programme to cover content in 16 languages and set to open new operations centres, focused on "election integrity" and to draw on co-operation from lawmakers, academics and election commissions, among others.[46]

62. Facebook's founder himself acknowledged that "deciding whether an ad is political isn't always straightforward. Our systems would be more effective if regulation created common standards for verifying political actors. Online political advertising laws primarily focus on candidates and elections, rather than divisive political issues where we've seen more attempted interference. Some laws only apply during elections, although information campaigns are nonstop. And there are also important questions about how political campaigns use data and targeting. We believe legislation should be updated to reflect the reality of the threats and set standards for the whole industry".[47]

63. However, as stressed during the November 2019 committee hearing, there is no way to independently verify Facebook's claims, which fake accounts were removed, which countries were targeted, what was their content and how many accounts showed signs of large-scale orchestration. Researchers and journalists must have better access to data on fake accounts and disinformation without social media companies strictly controlling them. Policy makers cannot regulate what they don't understand, nor can they implement them and sanction non-compliance without independent checks and controls.

64. Despite this contribution by the private sector, many regulatory problems remain unresolved and can only be tackled through international conventions as well as legislation at national and international level. Best practices and a better security agency co-operation should become normative in the defence of democratic elections.[48]

65. Interestingly, European Commission President, Ms Ursula von der Leyen, in the Political Guidelines for the next European Commission 2019-2024, promised to put forward a "European Democracy Action Plan to address the threats of external intervention in our European elections". This will "include legislative proposals to ensure greater transparency on paid political advertising and clearer rules on the financing of European political parties".[49]

---

44. https://www.consilium.europa.eu/en/meetings/fac/2019/01/21/?utm_source=dsms-auto&utm_medium=email&utm_campaign=Foreign+Affairs+Council%2c+21%2f01%2f2019.

45. To improve the authenticity of the stories that appear in voters' news feeds, Facebook would remove content that violates community standards; reduce the distribution of stories that do not directly violate the community standards but are deemed to "undermine the authenticity of the platform"; and give people more context on the information they see.

46. In Germany, for instance, Facebook partnered with German news agency DPA as part of a large-scale effort to fight fake news through fact-checking. It planned to train more than 100 000 German students in media literacy. In addition to human intervention, refining machine learning methods to identify untrustworthy messages on the platform will be a key component in Facebook's battle against misinformation.

https://www.euronews.com/2019/01/28/facebook-vows-to-fight-fake-news-foreign-interference-in-eu-electionshttps://www.euronews.com/2019/03/18/facebook-teams-up-with-german-news-agency-dpa-to-fight-fake-news-ahead-of-eu-elections.

47. https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html?noredirect=on&utm_term=.385878d0e864.

48. https://www.theglobeandmail.com/opinion/article-the-new-rules-for-the-internet-and-why-you-shouldnt-delete-facebook/.

66. On 10 October 2019, the European Parliament adopted a resolution calling for an upgrade of the EU East StratCom Task Force to a permanent structure with higher financing. They also called on internet and social media companies to co-operate in countering disinformation, without undermining freedom of speech, and called on the EU to create a legal framework to counter hybrid threats and to address the question of foreign funding of European political parties and foundations. Interestingly, the MEPs also took the view that further consideration could be given as to whether a special committee on foreign electoral interference and disinformation should be established within the European Parliament.[50]

6. Regulation and education: the cases of Germany, France and Sweden

67. The 2018 European Commission Final report of the High Level Expert Group on Fake News and Online Disinformation, drawing upon the input of experts from around the world, contains an inclusive, collaborative approach to addressing misinformation. However, it explicitly recommends against regulating.[51]

68. Social media companies themselves have called on policy makers in Europe, the United States and elsewhere to find an international consensus on how to "police the digital world" to avoid a fragmentation of the internet, which is divided along national borders,[52] including in dealing with disinformation in the context of free and fair elections.

69. One should also bear in mind that authoritarian regimes can easily use regulation to censor the opposition. China, for instance, has some of the strictest laws in the world when it comes to misinformation and criminalises creating or spreading rumours that generally "undermine economic and social order". In June 2018, Belarus lawmakers passed controversial amendments to Belarus' media laws that allow the government to prosecute people who spread false information online.[53] The Committee to Protect Journalists argued that this move could worsen the selective prosecution of journalists, in a country which has no press freedom, according to Freedom House.[54] Also Vietnam and Thailand misuse protection from disinformation for the sake of mass surveillance.

70. Several Council of Europe member States have attempted to tackle disinformation and its effect on our democracies, with related difficulties concerning the infringement of freedom of speech and the lack of a definition of what constitutes "fake news", as thoroughly analysed in the Council of Europe report on Information disorder.

71. Just to name a few, while France and Germany have chosen the way of regulation, Belgium, Denmark, the Netherlands, Sweden and the UK have published reports or launched media literacy campaigns or handbooks, aimed at countering disinformation or foreign interference.[55]

72. On the related subject of hate speech, the Network Enforcement Act (NetzDG)[56] was passed in Germany on June 2017 to combat hate and extremist content online and requires social media companies to block or remove content that violates restrictions on hate and defamatory speech in the German Criminal Code. Where falsehoods are used to further hate speech, it can be removed through this legislation. Companies that repeatedly fail to comply with the NetzDG may be fined up to fifty million euros. What makes content "manifestly" illegal is – in the first instance – left up to human or algorithmic judgment. As a result, the NetzDG incentivises intermediaries to remove demeaning content that could potentially violate the Criminal Code.[57] It should be noted that the UN Special Rapporteur on freedom of opinion as well as media freedom activists criticised the law as being unconstitutional and endangering freedom of expression.[58]

---

49. 'A Union that strives for more: My agenda for Europe': https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf.
50. http://www.europarl.europa.eu/doceo/document/B-9-2019-0108_EN.html.
51. https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation.
52. https://www.politico.eu/article/facebook-mark-zuckerberg-regulation-tech-europe-privacy-data-protection-washington-nick-clegg/.
53. https://www.rferl.org/a/belarus-assembly-passes-controversial-fake-news-media-legislation/29291033.html.
54. https://cpj.org/2018/06/belarus-moves-to-prosecute-fake-news-control-the-i.php.
55. The Poynter Institute for Media studies has issued a "Guide to anti-misinformation action around the world" and keeps it updated on an ongoing basis: https://www.poynter.org/ifcn/anti-misinformation-actions/.
56. *Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken*, also known as the Facebook Act.
57. https://law.yale.edu/mfia/case-disclosed/germanys-netzdg-and-threat-online-free-speech.
58. https://www.ohchr.org/Documents/Issues/Opinion/Legislation/OL-DEU-1-2017.pdf.

73. Particularly problematic is the requirement to delete false information within 24 hours, which is similar to the French law. This represents a major challenge not only to platform operators but also to the German legal system. Without a reform of judicial structures this regulation is hard to implement and may pose a threat to the freedom of expression.

74. In December 2018, the French Parliament passed a law cracking down on manipulation of information, allowing courts to rule whether reports published during election periods were credible or should be taken down. The law allows election candidates to sue in order to remove contested news reports during election periods, as well as forcing social platforms, such as Facebook and Twitter, to disclose the source of funding for sponsored content.[59] The law has been criticised by civil society activists and a group of 50 senators from the opposition who appealed to the Constitutional Court arguing that the law falls short of the principle of proportional justice. The Constitutional Court then validated the constitutionality of the law.[60]

75. The Swedish authorities, whom I met on 15 May 2019, are particularly active in protecting freedom of speech, democracy and individual rights, in the context of disinformation, and highlight the role of Swedish society in confronting this threat, the support by media organisations of independent fact-checking, and the government's desire for primary school children to be taught how to spot false information.

76. A number of lessons can also be drawn from the 2018 Swedish election. Further to foreign attempts to interfere, the Swedish Civil Contingencies Agency commissioned an election report from the Institute of Strategic Dialogue and the London School of Economics called "Smearing Sweden",[61] which described how sources attributed to Russian actors supported and amplified the far-right in the United States, Europe and Sweden. The report also noted Twitter accounts which had earlier supported Mr Trump and Ms Le Pen and were now supporting the Swedish far-right fringe party AfS.[62]

77. All of the interlocutors I met in Stockholm confirmed their attachment to freedom of expression, the protection of anonymity and data protection. The laws on discrimination or hatred and defamation in Sweden are deemed to be enough. They fear that tightening an open society carries the risk of further radicalisation. However, they believe that the judiciary should be better equipped to respond adequately to new threats and an ever-changing internet environment.

78. The Ministry of Culture set up a new Media and Democracy Unit, two areas that were previously separate. The critical handling of information and source/fact-checking are an integral part of the curriculum in schools. Beyond schools, raising awareness among society at large is also a priority. The Swedish Civil Contingencies Agency updated its public emergency preparedness brochure to include a section about false information. It warns about potential foreign disinformation campaigns and includes a list of things citizens can do to fact-check information online. The government tries to understand where people, the young, get their information from and what effect, for instance, online games have on political education and behaviour. The government also works with multipliers, including trade unions, municipalities, sports clubs, etc.

79. Building off both the Swedish Civil Contingencies Agency and the parliamentary Defence Commission, an independent authority – not controlled by the government – could be set up soon aimed at countering disinformation and foreign influence campaigns. This would ensure that factual public information can be quickly and effectively communicated even under disruptive conditions, as well as identify, analyse and confront influencing operations.

80. According to *Reporters sans Frontières* rather than top-down, prescriptive laws, we should be thinking about changing the environment in which readers act, and empowering them, for instance by displaying related, fact-checked articles next to disputed stories; apps allowing users to check for veracity; and certification systems.[63]

---

59. https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000037847559&dateTexte=&categorieLien=id
60. https://www.conseil-constitutionnel.fr/decision/2018/2018773DC.htm.
61. https://www.isdglobal.org/wp-content/uploads/2018/11/Smearing-Sweden.pdf.
62. The report also noted an attempt to establish "election fraud" on Twitter well in advance of the election. Different election fraud hashtags peaked, according to the report, on September 10, the day after the election, with 13,558 posts. This was fuelled by the fact that the website of the Election Authority went down during election night. It did not affect counting, nor the reporting of the ongoing counting to media, but did affect the presentation of the result on the Election Authority´s own website. However, during the period the website was down, Sweden Democrats' percentage of the vote also went down. This led to another wave of narratives of "stealing the election from SD." The Election Authority admitted that a DDOS attack (distributed denial-of-service) took down the website. https://disinfoportal.org/lessons-from-the-2018-swedish-elections/.
63. https://www.theguardian.com/media/2018/apr/24/global-crackdown-on-fake-news-raises-censorship-concerns

7. Conclusions

81. As the internet seeps into more aspects of our political lives, there is a need for improvements in both its content and architecture, and to protect the electoral process and the very essence of democracy from its "hackers". Disinformation, foreign interference, abusive behaviour, hate amplification, trolling, identity theft, are just some of the symptoms of "democracy hacking".

82. Many pioneers of the tech industry also expressed a longing for internet structures that would entice users to be better humans, an internet that is moral.[64] As a matter of fact, in what has been defined as a "post-truth world", emotions can affect the electoral process more than facts, which can be exploited by propagandists and disinformation agents.[65]

83. The conclusions of the conference of the Electoral Management Bodies, co-organised by the Venice Commission in April 2018 as well as the more recent report on Digital technologies and elections mentioned above, are relevant to my report and I would like to borrow some of their recommendations.

84. Social media represents a powerful tool of communication but the legal framework regulating media coverage of elections was not designed for social media and needs to be addressed. Information disorder during electoral campaigns compromises the level playing field amongst political contestants. Countering them, however, should not be at the expense of freedom of expression.

85. In addition, data-driven electoral campaigning on social media, based on segmentation and profiling of users, especially dark adverts on platforms targeting potential voters, is a growing phenomenon which must be better regulated, in order to ensure transparency and data protection, and build public trust. There is nothing wrong in trying to convince swing voters, but they should be made aware that they are being brought political information.

86. To address disinformation challenges, we must recognise that the internet and social media have reshaped the democratic landscape: there is a new powerful player in the equation, with its own interests and commercial purpose that tend to collide with both personal rights (i.e. privacy, protection of personal data and freedom of expression) and political rights and principles (i.e. electoral equity).

87. Co-operation with internet intermediaries and service providers is necessary and should be enhanced. Social media operators should be better regulated and interact with institutions and agencies in charge of electoral processes in order to encourage and empower users to act in a responsible manner; specific information campaigns should be conducted to educate the public about the risks of irresponsible information exchanges. International co-operation is crucial in this respect.

88. While self-regulation in line with existing international standards, notably the Committee of Ministers Recommendation CM/Rec(2018)2 on the roles and responsibilities of internet intermediaries, is welcome and encouraged, further reflection and standard setting on the part of the Council of Europe should be considered.[66]

89. Voters need to be enabled to classify trustworthy information and knowledge. The promise of an open, free internet serves the purpose of the voters to become more informed and engaged. The effort needed is to break up the monopoly of tech companies controlling, to a great extent, citizen's access to information. Europe must also aim at increasing the diversity of information providers and ensure a genuine and fair competition among them.

90. It is easy to blame AI technology for the world's wrongs (and sometimes for lost elections) but the underlying technology itself is not inherently harmful. If used appropriately, AI can help people discover the political positions of each candidate. Crucially, personalised political ads must serve their voters and help them be more informed, rather than undermine their interests. The algorithmic tools that are nowadays used to mislead, misinform and confuse the voters could equally be repurposed to support democracy.[67]

91. To face these challenges, governments could implement a number of strategies from a European and global perspective and create a model that includes co-responsibility and multiple regulatory and conflict-resolution approaches. Such model could focus on a number of strategies, which I have detailed in the draft

64. David D. Clarck, Designing an Internet, MIT Press, October 2018.
65. Warsaw Institute, In the Age of Post-Truth: Best Practices in Fighting Disinformation, April 2017.
66. https://www.coe.int/en/web/electoral-management-bodies-conference/conclusions-emb2018.
67. Vyacheslav Polonski, Artificial intelligence can save democracy, unless it destroys it first, Oxford Internet Institute – Blog, August 2017, https://www.oii.ox.ac.uk/blog/artificial-intelligence-can-save-democracy-unless-it-destroys-it-first/ Medium.

resolution, including strengthening digital literacy skills and transparency in political online advertising, supporting fact-checking initiatives, public service media and researcher's access to data, sharing best practices and increasing security agency co-operation as well as encouraging self-regulation frameworks and initiating judicial reforms.

92. I believe that more efforts should be made in implementing Council of Europe legal standards also in the context of political activities through social media. Citizens need to be empowered to identify unreliable information and manipulation and to recognise where to draw the line between forms of permissible persuasion and unacceptable manipulation during electoral campaigns. Our Assembly could also further consider the possibility to recommend binding conventions on co-operation against disinformation and influence in foreign decision-making processes.

93. I welcome the EU's action to counter disinformation, address the threats of external intervention in European elections, and ensure greater transparency on paid political advertising and clearer rules on the financing of European political parties, as part of the forthcoming European Democracy Action Plan for 2019-2024. However, our Assembly should also call on the EU to ensure synergy with the Council of Europe's action in those areas and promote further co-operation with all 47 member States of the Council of Europe.

94. Finally, we should support the work of the Venice Commission in its efforts to prepare a list of principles for the use of digital technologies in the context of elections and continue following this matter.