

Doc. 14844

19 March 2019

Social media: social threads or threats to human rights?

Report¹

Committee on Culture, Science, Education and Media

Rapporteur: Mr José CEPEDA, Spain, Socialists, Democrats and Greens Group

Summary

Social media are part of our daily lives. They play an important role in building social connections, provide a forum for free debate on political affairs and society, and can contribute to greater diversity of opinion and increased democratic participation. Their misuse, however, can trigger numerous harmful consequences, affecting individual rights and the functioning of democratic institutions. Information filtering, data mining, profiling and micro-targeting, aided by increasingly powerful artificial intelligence systems, risk threatening human dignity and opening the door to the hidden manipulation of individual behaviour or public opinion.

Public authorities and internet companies should combine forces to firmly defend freedom of expression and information, stop the spread of illegal content and ensure quality information. Greater transparency regarding algorithms, and adequate information about their functioning for users, will be needed. The Parliamentary Assembly should encourage the ratification of the Council of Europe's modernised Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, in order to strengthen data protection laws, while the major internet companies should rethink their economic models to give back to users control of their personal data.

1. Reference to committee: [Doc. 14184](#), Reference 4264 of 23 January 2017.



Contents	Page
A. Draft resolution	3
B. Explanatory memorandum by Mr José Cepeda, rapporteur	6
1. Rationale of the present report	6
1.1. Social media and their growing importance	6
1.2. The positive contribution of social media to the well-being of our societies	6
1.3. The dark side of social media and the scope of the present report	8
2. Freedom of expression	9
2.1. Boundaries of freedom of expression and the problem of illicit content	9
2.2. Power to control information disseminated through social media and arbitrary censorship	10
3. Freedom of information	11
3.1. The issue of information disorder	11
3.2. Biased access to preselected sources of information	12
3.3. Controlling the information and manipulation	13
4. The right to privacy	13
4.1. Information, user consent and privacy settings	14
4.2. Data profiling, automated decision making and manipulation	14
5. Ways forward	15
5.1. Upholding freedom of expression and freedom of information while avoiding abuses	15
5.2. Strengthening users' control over their data	17
6. Conclusions	21

A. Draft resolution²

1. The Parliamentary Assembly highly values the positive contribution of social media to the well-being and development of our societies. They are indispensable tools which help bring people closer together and facilitate the establishment and development of new contacts, thus playing an important role in building social capital. They provide a new public space, where political affairs and socially relevant themes are discussed, and where small parties, minorities or outsider groups frequently silenced in major legacy media can spread their ideas and views. They have the potential to expose users to more diverse sources of information and opinions, foster the plurality of voices which is needed in a democratic society and strengthen democratic participation.
2. Despite the huge beneficial potential of social media for individuals and for our societies, their misuse is also triggering numerous harmful consequences for our individual rights and well-being, for the functioning of democratic institutions and for the development of our societies, such as cyberbullying, cyberstalking, hate speech and incitation to violence and discrimination, online harassment, disinformation and manipulation of public opinion, and undue influence on political – including electoral – processes.
3. Social media are key actors in the regulation of the information flow on the internet and the way they operate has a significant impact on freedom of expression, including freedom of information, but also – in a more insidious way – on the right to privacy. These are not new concerns for the Assembly and, in the past, various reports have sought to identify measures to confine, if not eliminate, the risk of abuses which the internet generates in these sensitive areas. However, recent scandals have highlighted the need to further explore the responsibilities that social media should bear in this respect and the duty that public authorities have to ensure that such fundamental rights are fully respected.
4. The Assembly considers that social media companies should rethink and enhance their internal policies to uphold more firmly the rights to freedom of expression and of information, promoting the diversity of sources, topics and views and better quality information, while fighting effectively against the dissemination of unlawful material through their users' profiles and countering disinformation more effectively.
5. Moreover, the Assembly wonders whether it has become necessary to challenge the business model on which major social media companies have built their wealth, which is based on the massive acquisition of data from their users, as well as from their acquaintances, and on their – in practice almost unlimited – exploitation for commercial purposes. Data mining and profiling are phenomena which seem to have gone too far and beyond democratic control.
6. Proper use of big data can help to enhance policy design (for example on infrastructure development and urban planning) and the provision of key services (for example traffic management and health care); however, it is necessary to ensure data anonymisation and to guarantee that only reasonable inferences are drawn from users' data.
7. The Assembly believes that public authorities should guide efforts seeking to “secure the human dignity and protection of the human rights and fundamental freedoms of every individual and ... personal autonomy based on a person's right to control of his or her personal data and the processing of such data”, as stated in the Protocol (CETS No. 223) amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) (“the modernised Convention 108”). In line with the view expressed by the ministers when adopting the above-mentioned Protocol, the Assembly highlights the importance of a speedy ratification or accession by the maximum number of Parties in order to facilitate the formation of an all-encompassing legal regime of data protection under the modernised Convention 108.
8. The Assembly considers that strong collaboration of internet operators and public authorities is crucial to achieve results. In this respect, it welcomes the setting up of forms of partnership and co-operation between internet operators and various Council of Europe bodies, including the Assembly itself, and it encourages the partners concerned to further develop this co-operation and engage in ongoing constructive dialogue, in order to promote good practice and develop standards to uphold users' rights and a safe use of social media.

2. Draft resolution adopted unanimously by the committee on 4 March 2019.

9. The Assembly therefore recommends that the Council of Europe member States:

9.1. fully comply with relevant international obligations concerning the right to freedom of expression, in particular those arising from Article 10 of the European Convention on Human Rights (ETS No. 5), when developing the legal framework of this right, and deliver national regulations requiring that social media providers ensure diversity of views and opinions and do not silence controversial political ideas and content;

9.2. embed the teaching of information technology skills, including the use of social media, in the school curricula from the earliest age;

9.3. initiate without delay the process required under their national law to ratify the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data;

9.4. pending the above-mentioned ratification process, review as required the national legislation in force to ensure its full consistency with the principles enshrined in the modernised Convention 108, and in particular legitimacy of data processing, which must find its legal basis in the valid (and therefore also informed) consent of the users or in another legitimate reason laid down by law, as well as the principles of transparency and proportionality of data processing, data minimisation, privacy by design and privacy by default; the controllers, as defined in Article 2 of the modernised Convention 108, should be bound to take adequate measures to ensure the rights of the data subjects, as listed in its Article 9;

9.5. encourage and support collaborative fact-checking initiatives and other improvements of content moderation and curation systems which are intended to counter the dissemination of deceiving and misleading information, including through social media;

9.6. equip themselves with the means to sanction violations of their national legislation and of their international commitments that could occur on social media;

9.7. promote, within the Internet Governance Forum and the European Dialogue on Internet Governance, a reflection on the possibility for the internet community to develop, through a collaborative and, where appropriate, multi-stakeholder process, an external evaluation and auditing system aimed at determining that algorithms respect data protection principles and are not biased, and a “Seal of Good Practices” which could be awarded to internet operators whose algorithms are designed to reduce the risk of filter bubbles and echo chambers and to foster an ideologically cross-cutting exposure of users.

10. The Assembly invites the European Union to examine ways to encourage and support a Europe-wide project intended to provide internet users with a tool to create, manage and secure their own personal online data stores (“PODs”), and to consider how the national and European regulations should evolve to ensure that online services – especially the most popular ones – offer their users tools which respect data protection principles and are compatible with POD functionalities.

11. The Assembly calls on the social media companies to:

11.1. define in clear and unambiguous terms the standards regarding admissible or inadmissible content, which must comply with Article 10 of the European Convention on Human Rights and should be accompanied, if need be, by explanations and (fictional) examples of content banned from dissemination;

11.2. take an active part not only in identifying inaccurate or false content circulating through their venues but also in warning their users about such content, even when it does not qualify as illegal or harmful and is not taken down; the warning should be accompanied in the most serious cases by the blocking of the interactive functions, such as “like” or “share”;

11.3. make systematic use of a network analysis approach to identify fake accounts and bots and develop procedures and mechanisms to exclude bot-generated messages from their “trending” content or at least flag their accounts and the messages they repost;

11.4. encourage collaborative evaluation of the sources of information and items of news distributed, developing tools which could allow the online community to provide feedback on the accuracy and quality of content they consult, and put in place mechanisms of editorial oversight by professionals to detect and flag misleading or inaccurate content;

11.5. strongly engage in fact-checking initiatives which are intended to counter the dissemination of deceiving and misleading information through social media;

11.6. support and adhere to the Journalism Trust Initiative launched by Reporters Without Borders and its partners, the European Broadcasting Union, Agence France-Presse and the Global Editors Network;

11.7. design and implement algorithms which respect data protection principles and encourage plurality and diversity of views and opinions;

11.8. promote visibility of relevant issues with low emotional content against content of low relevance which is shared by emotional triggers;

11.9. even in the absence of binding national rules, abide by the principles enshrined in the modernised Convention 108 and ensure, through voluntary regulations and the development of good practice, the full respect of the rights of the data subjects, as listed in its Article 9; positive measures in this direction should be, among others, to:

11.9.1. improve the readability of the contractual terms and conditions which the users have to accept, for example by drawing up visual-based summaries of this information, in the form of tables with clear replies to key questions related to privacy concerns;

11.9.2. set privacy rules at the highest restriction level by default or, at least, provide the users with clear information and a user-friendly functionality to easily check privacy rules applicable to them and have the possibility to set these rules at the highest restriction level;

11.9.3. ensure that their users can oversee, evaluate and refuse profiling, including the possibility to check the “micro-categories” used to classify them and determine which ones must not apply to them; users must also be duly informed about the data the platform is using to filter and promote content based on their profile and be able to ask for any data to be deleted, unless the controller has conflicting legal obligations;

11.9.4. guarantee that the ownership of social media accounts of defunct people is transmitted to their relatives;

11.9.5. make sure that all functionalities offered to their users are progressively made compatible with the possibility for users to create, manage and secure their own personal online data stores.

B. Explanatory memorandum by Mr José Cepeda, rapporteur

1. Rationale of the present report

1.1. Social media and their growing importance

1. Online social networking sites (or social networks) and social media have been one of the fastest growing phenomena in the 21st century. For example, Facebook grew from less than 1 million users in 2004 to more than 2.23 billion monthly active users in June 2018 (with an increase of 100 million monthly active users from December 2017). If Facebook were a physical nation, it would be the most populated country on earth. YouTube follows closely, with 1.9 billion (namely an increase of some 300 million users in less than a year); Instagram (which is owned by Facebook) has reached one billion monthly active users. The success story of these giant sites is coupled with the growing popularity of mobile social networking apps. Just to mention the biggest two: WhatsApp and Messenger (both owned by Facebook) have 1.5 and 1.3 billion monthly active users respectively.³

2. Not only are more of us using social networks, we are also spending more and more time online. According to Eurobarometer,⁴ 65% of Europeans – and 93% of people aged between 15 and 25 – use internet either every day or almost every day. One of our most frequent activities online is participating in social networks: 42% of Europeans – and more than 80% of people aged between 15 and 25 – use online social networks daily. These proportions have risen continuously over the last few years and the expectation is that they will continue to increase. Moreover, our children are starting to use social media earlier and earlier in their young lives.

3. There is no doubt that the internet in general and social media in particular are influencing the way we look for and access information, communicate with each other, share knowledge and form and express our opinions. This is having a significant impact both on our individual lifestyles and on the way our societies develop.

1.2. The positive contribution of social media to the well-being of our societies

4. Social media have evolved from leisure-oriented venues into platforms where a significant part of social interaction takes place today. We use them to get in touch with friends, acquaintances and relatives, as well as to maintain relations with other people who have similar interests and with professional partners. Not only have social media turned into indispensable tools which help bring people closer together, but they also open up new connections and facilitate the establishment and development of new contacts, thereby increasing the number of our acquaintances.⁵ In other terms, they play an important role in building social capital.

5. Another trend in the evolution of social media drove them to become spaces for the distribution and consumption of information and news about political and civic events. Users not only share photographs of their holidays and talk about their hobbies; they also share information and views about their governments and policies they announce, about the draft laws their parliaments debate and about civic and societal issues.

6. Social media are no longer “just for fun” spaces or chatting rooms for soft topics; they have turned into an extension of the old public sphere, and they provide a new public space where political affairs and socially relevant themes are discussed. Moreover, social media have assumed (at least partially) the role played by local newspapers in the 19th century as tools through which citizens integrate into their local community and activate latent ties.⁶

7. These new public spheres have played a useful role in the political and civic terrain given that they have allowed minority groups to spread their voice and their message. As the Committee on Culture, Science, Education and Media has already stressed in its report on “Internet and politics: the impact of new information

3. Regularly updated statistics on the most popular social networking sites and apps are published by Dreamgrow: www.dreamgrow.com/top-15-most-popular-social-networking-sites/.

4. Standard Eurobarometer 88 – autumn 2017. The survey was conducted between 5 and 14 November 2017 in the 28 member States of the European Union, the five candidate countries (North Macedonia, Turkey, Montenegro, Serbia and Albania), and the Turkish Cypriot Community in the northern part of Cyprus.

5. Ellison N.B., Steinfield C. and Lampe C. (2007). “The benefits of Facebook ‘friends’: Social capital and college students’ use of online social network sites”, *Journal of Computer-Mediated Communication*, 12(4), pp. 1143-1168.

6. Joëlle Swart, Chris Peters and Marcel Broersma (2018). Sharing and Discussing News in Private Social Media Groups, *Digital Journalism*.

and communication technology on democracy” (Doc. 13386), internet and social media brought to an end the information oligopoly held by traditional media, institutions and the elites, and they deeply changed the paradigms of communication and knowledge dissemination. “Information is also built up thanks to input from Internet users from all backgrounds, regardless of politics, culture, socio-professional category or qualifications. Moreover, the Internet not only gives a larger part to individual views and opinions in public debate, but also encourages people to speak out on subjects in which the traditional media take little interest” (paragraph 11 of the explanatory memorandum).

8. Social media are a useful channel for small parties, minorities or outsider groups frequently silenced in major legacy media. Those actors can employ social media to circulate their ideas and views, and to channel and stimulate political participation. In Spain, for example, Facebook and Twitter have been two popular platforms for ecologists and animal rights defenders to promote campaigns, raise public awareness, mobilise their supporters and gain visibility for their actions.

9. This also means that social media have the potential to expose citizens and users to more diverse sources of information and opinions, including political and ideological views which citizens would not actively look for or become aware of in other environments.⁷ In this way, social media foster the plurality of voices which is needed in a democratic society. Another relevant beneficial consequence is in terms of participation: users who are exposed to a wider, more diverse range of news, opinions and views on events and societal issues also tend to show a higher degree of political participation and civic engagement, not only online but also offline.⁸

10. Although it should be noted that this conclusion is not confirmed by all researchers, I share the conviction of many experts whom we have heard that social media foster democratic participation: “Internet-based platforms have extended the ‘ladder of political participation’, widening the range of political activity. Basically the range of small things people can do has expanded enormously; political endorsements, status updates, sharing media content, ‘tweeting’ an opinion, contributing to discussion threads, signing electronic petitions, joining e-mail campaigns, uploading and watching political videos on YouTube, for example. ... These small political acts would make no difference at all if taken individually, but they can scale up to large mobilisations”.⁹ The Committee of Ministers of the Council of Europe upholds the same conviction in its Recommendations CM/Rec(2012)4 on the protection of human rights with regard to social networking services and CM/Rec(2007)16 on measures to promote the public service value of the Internet.

11. Social media can profit from these positive effects on political participation and encourage it through specific campaigns or activities. For example, in the American presidential elections in 2010 and 2014, Facebook incorporated the “I voted” feature. It allowed users to display a button on their virtual walls to share with their contacts that they had effectively participated in the election. Both campaigns saw a rise in the electoral participation rate.

12. However, “I voted” buttons may or may not be a positive feature, depending on whether they are transparent, unbiased, aimed at all users and displayed in the same manner for all users. To date, they have raised more questions than they have provided answers and are heavily criticised by many analysts. For example, in the United States elections, not every voter saw the same thing on their Facebook newsfeed and users were not informed about the experiment (i.e. an analysis of whether voter buttons can enhance voter turnout). In addition, the influence that Facebook (but also other social media) may have through this tool goes beyond the voter turnout; we can wonder: “Could Facebook potentially distort election results simply by increasing voter participation among only a certain group of voters – namely Facebook users?”¹⁰

7. Bakshy E., Messing S. and Adamic L.A. (2015). Exposure to ideologically diverse news and opinion on Facebook. *Science*, 348(6239), pp. 1130-1132.

8. Gil de Zúñiga H., Jung N. and Valenzuela S. (2012). Social media use for news and individuals' social capital, civic engagement and political participation. *Journal of Computer-Mediated Communication*, 17(3), pp. 319-336.

9. See paragraph 28 of the report “Internet and politics: the impact of new information and communication technology on democracy”, which refers to the views expressed by Professor Helen Margetts in her report to our committee (document AS/Cult/Inf (2013) 04, not published) following the committee meeting of May 2013, in London.

10. See the article by Hannes Grassegger: [Facebook says its “voter button” is good for turnout. But should the tech giant be nudging us at all?](#) (posted online on 15 April 2018).

1.3. The dark side of social media and the scope of the present report

13. While it is uncontested that social media (and the internet) have a huge beneficial potential for us as individuals and also for our societies, it is equally very clear that they are also triggering numerous harmful consequences for our individual rights and well-being, for the functioning of democratic institutions and for the development of our societies. There is a huge amount of research on the dangers which result from the misuse of internet and social media and from the malicious behaviour of ill-intentioned users.

14. The list is unfortunately long: cyberwarfare, cyberterrorism, cybercriminality and cyberfraud, cyberbullying, cyberstalking, hate speech and incitation to violence and discrimination, online harassment, child pornography, disinformation and manipulation of public opinion, undue influence on political – including electoral – processes, etc. In addition, deviant individual behaviour has self-destructive consequences: such as addiction (to online gaming or gambling) and dangerous – and even mortal – challenges which especially young people take up to gain some “likes” on their accounts. These risks and dangers are not always correctly perceived or understood.

15. It is not the purpose of the present report to cover such an extensive field of research. The focus of the report is on the right to freedom of expression, including freedom of information,¹¹ and on the right to privacy. To express myself with the wording of Committee of Ministers [Recommendation CM/Rec\(2018\)2](#) on the roles and responsibilities of internet intermediaries, social media – which are internet intermediaries – may “moderate and rank content, including through automated processing of personal data, and may thereby exert forms of control which influence users’ access to information online ..., or they may perform other functions that resemble those of publishers” (preamble, paragraph 5).

16. Social media, as key actors in the regulation of the information flow on the internet, have a significant impact on the rights to freedom of expression, freedom of information and privacy. These are not new concerns for the Parliamentary Assembly; in the past, various reports have sought to identify measures to confine, if not eliminate, the risk of abuses which the internet generates in these sensitive areas.¹² The main reason why I wish to consider again this topical question is because I believe it is important to further explore the responsibilities that social media should bear in this respect.

17. The issue at stake is whether we, as policy makers, should urge social media to enhance their self-regulation, so as to fight more effectively against the threats to these human rights, and whether, as legislators, we should enhance the legal framework, to impose a higher level of requirements and more stringent obligations on social media, in order to ensure effective protection of these rights. My analysis will build on the previous work of the Council of Europe¹³ and of the Assembly, as well as on the excellent contributions provided by the experts heard by the committee.¹⁴

11. According to Article 10 of the European Convention on Human Rights (ETS No. 5), the right to freedom of expression “shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers”. For the purposes of the present report, I will deal separately with freedom of expression and freedom of information, while acknowledging that they are closely intertwined, and even that they should be regarded as two sides of the same coin.

12. In addition to the report and adopted texts on “Internet and politics: the impact of new information and communication technology on democracy” (quoted above), see the report on “The protection of freedom of expression and information on the Internet and online media” by the Committee on Culture, Science, education and Media ([Doc. 12874](#) and [Addendum](#)), as well as [Resolution 1877 \(2012\)](#) and [Recommendation 1988 \(2012\)](#). The issue of freedom of expression and information online is also addressed in other reports, for example with a focus on the protection of media freedom or on the limits of freedom of expression and the issue of unlawful material disseminated via the internet.

13. See, among others, the following recommendations of the Committee of Ministers: [CM/Rec\(2018\)2](#) on the roles and responsibilities of internet intermediaries; [CM/Rec\(2014\)6](#) on a Guide to human rights for Internet users; [CM/Rec\(2012\)4](#) on the protection of human rights with regard to social networking services; [CM/Rec\(2012\)3](#) on the protection of human rights with regard to search engines.

14. I am particularly thankful to Professor Francisco Segado Boj, Director of the Research Group “Communication and Digital Society”, Universidad Internacional de la Rioja (UNIR), Spain, who is the author of the expert report I have used as a basis for my own report. I am also grateful to Ambassador Thomas Schneider, Chairperson of the Steering Committee on Media and Information Society (CDMSI) of the Council of Europe, and to the experts who attended the series of hearings on “Information society, democracy and human rights”, and in particular to: Mr Nello Cristianini, Professor of Artificial Intelligence, Intelligent Systems Laboratory, University of Bristol, United Kingdom; Professor Jean-Gabriel Ganascia, President of the CNRS Ethics Committee (COMETS), université Pierre et Marie Curie (UPMC); Mr Oliver Gray, representative of the European Advertising Standard Alliance (EASA); Mr Thomas Myrup Kristensen, Managing Director EU Affairs and Northern Europe, Facebook, Head of Office Brussels; Ms Victoria Nash, Deputy Director, Oxford Internet Institute, University of Oxford, United Kingdom; Mr Marco Pancini, Director of Public Policy of Google; Ms Sandra Wachter, Lawyer and research fellow in Data Ethics, AI, robotics and Internet Regulation/cyber-security, Oxford Internet Institute, University of Oxford, United Kingdom.

18. My idea is not that the entire burden must fall on social media (and other internet operators). Public authorities have clear responsibilities too in this domain and the aim is certainly not to discharge them from these responsibilities. The users themselves have responsibilities, that they should be helped to understand and shoulder properly.

19. However, social media companies are the actors which have got, and are getting, the highest benefits in economic terms; they have gained *de facto* enormous power as regulators of the information flow, without being sufficiently accountable as regards how this power is used. The roles and responsibilities of different actors should, I believe, be looked at again and corrected, so that public authorities, social media (and other internet operators) and internet users join efforts. We need to act together to uphold our rights online and ensure that social media can deliver all their benefits without endangering our individual and societal well-being.

2. Freedom of expression

20. Freedom of expression is a basic principle of democracy; it is, however, constantly under threat. Every time a new medium is developed, ideological, political and economic powers develop strategies and exert pressure to control the creation and distribution of content through this medium. This was the case with press, radio and television, and now also with internet and social media. Two interconnected key issues regarding freedom of expression and social media are the definition of its boundaries and the risk of arbitrary censorship.

2.1. Boundaries of freedom of expression and the problem of illicit content

21. Individuals and organisations must be entitled to express themselves and spread information and opinions through social media. There is a common understanding, however, that free speech is not absolute, but is in fact limited by other human rights and fundamental freedoms. Today, the most controversial issues drawing attention towards these boundaries are: instigation of criminal behaviour, such as terrorism propaganda, incitation to violence or discrimination, hate speech and information disorder.

22. While it is clear that society and individuals must be protected from the above, any action by public authorities or internet operators raises complex questions, must overcome technical and legal barriers and may affect civil liberties. In particular, although the unlawful nature of material shared on social media may seem obvious in most cases, it is not always straightforward to define what is illegal.

23. As an example, even in the United States, where restrictions to free speech are allowed by the First Amendment to the Constitution only in exceptional cases, a social networking site might be prosecuted if it is proved to host messages and material which might be responsible for advocating and supporting terrorist actions or terrorist organisations.¹⁵ None of us would consider this strange or problematic as such. Nevertheless, we are also well aware that the very concept of terrorism could be – and has been – used to reinforce censorship and retaliations against journalists or even individual users. In a democratic country, it must be ensured that, as is the case in the United States, legal actions against social media platforms and internet providers can only take place in very specific scenarios where messages clearly instigate terrorist actions, recruit for criminal organisations and promote indoctrination.¹⁶

24. The boundaries of freedom of expression are supposed to be set along the same lines online and offline. However, there are two distinct issues about the content moderation on the social media platforms that warrant highlighting: on the one hand, enforcement of the rules on illegal content is much more difficult online, due to the vast quantity of information disseminated online, but also to the anonymity of the authors; on the other hand, terms of service agreements may limit publication of legal content on social media. Therefore, a key question is what (public interest) responsibilities could be imposed on social media and how far content moderation by the social media platforms can be regulated. In this respect, I believe that when social media act exactly as the traditional media (Facebook newsfeed, for instance), they should be submitted to the same rules, to ensure a “common level playing field”. The revised European Union Audiovisual Media Services Directive (AVMSD)¹⁷ is a first step in this direction.

15. Tsesis A. (2017). Social Media Accountability for Terrorist Propaganda. *Fordham Law Review*, 86, p. 605.

16. Tsesis A. (2017). Terrorist speech on social media. *Vanderbilt Law Review*, 70, p. 651.

17. <https://ec.europa.eu/digital-single-market/en/revision-audiovisual-media-services-directive-avmsd>.

2.2. Power to control information disseminated through social media and arbitrary censorship

25. The issue of arbitrary State censorship lies beyond the scope of the present report and is regularly addressed by the committee through reports on media freedom and the safety of journalists. Nevertheless, one aspect is closely linked to the focus of this report, namely the fact that national authorities impose their decisions on internet intermediaries (including social media), which are sometimes obliged to be complicit in violations of freedom of expression. In the case of authoritarian (or even dictatorial) regimes, it is difficult (or sometimes even impossible) to circumvent the constraints that States may impose. In such circumstances, we can merely hope that the most powerful internet intermediaries find a way to discreetly offer resistance with a view to maintaining some spaces for freedom of expression and information even in those countries.

26. However, to deal with genuinely illicit content and to protect individual rights and the common good, national authorities and fact-checking initiatives need to be able to count on flawless collaboration on the part of internet intermediaries, particularly social media. As I stressed earlier, the new media context gives social media considerable power to control the information flow, which must be exercised with a responsibility commensurable with the extent of this power.

27. The social media companies have the power to control all the information which circulates publicly through these outlets, to highlight that information or hide it, or even silence certain issues or information. They not only set the rules regarding what can be posted and distributed, but also in cases such as Facebook they remain the owners of all the content created and uploaded to the platform by their users.

28. The upside of this situation is that social media can turn into allies of public authorities in order to detect, prosecute and stop illicit content. In this respect, our Assembly has already urged social media and other internet operators to act, for example in order to help fight phenomena like child pornography or hate speech. But there are also downsides.

29. One problem is that collaboration of this kind with governments can escape democratic control and result in serious violations of users' fundamental human rights, as was the case with the mass surveillance and large-scale intrusion practices disclosed by Edward Snowden in 2013.¹⁸ While governments themselves primarily bear responsibility in such cases, internet operators may be complicit in these abuses. This is not the focus of our enquiry, however.

30. The downside on which I would like to insist is that social media, by establishing and implementing their content moderation policies, can themselves become censors which unilaterally remove posts and information on their sites at their will, even though they are not illegal, which poses a threat to freedom of expression. Although Facebook and other social media claim not to have an editorial role and responsibility, there are numerous examples of statements and photographs being removed from individual users' pages. Their action of removing content may also affect traditional media. Since 2014, the BBC, for instance, has kept a list of its online articles that have been made invisible by the Google search engine, based on individuals' or companies' requests. This amounts to a censorship which lacks transparency, accountability and respect of public interest rights.¹⁹

31. In the implementation of self-regulation established with the valuable aim of preventing dissemination of illicit content, mistakes appear which seem abnormal. In various cases, social media companies have been accused of arbitrarily censoring content; as has happened with the feminist movement FEMEN, which was accused by Facebook of "promoting pornography" given the use of nudity in their protests.²⁰ Another anomalous case was the blocking of the iconic photograph of the "Napalm Girl" from the Vietnam War, as well as other examples of removal of art and photographs having an educational purpose.

32. These cases provoke questions about the social media regard for freedom of expression, and they raise concern about the lack of clarity of rules and regulations upon which the social media company base their decisions. They confirm the importance of examining the role of social media as news distributors and the editorial responsibility that this entails, bearing in mind the protection of the basic human right to freedom of expression and the consequences for the rule of law.

18. See the report by the Committee on Legal Affairs and Human Rights on "Mass Surveillance" (Doc. 13734).

19. See information published at: www.bbc.co.uk/blogs/internet/entries/2edfe22f-df3d-4a05-8a65-b2a601532b0d and www.wired.co.uk/article/bbc-right-to-be-forgotten.

20. Almeida Leite R. and Cardoso G. S. (2015). A arbitrariedade dos parâmetros de censura no facebook e a proibição da página do Femen. *Revista Ártemis*, 19.

3. Freedom of information

33. The possibility for everyone to access quality information – i.e. accurate, fact-based, relevant and balanced information – is a fundamental element of democratic societies. Legally speaking, we do not have a right to purely truthful and factual information. On the one hand, perfect information does not exist in practice: there is always a degree of approximation, and a given perspective of the narrator. On the other hand, there is no general obligation to deliver information which is 100% accurate, exhaustive, neutral and so on; satire and parody, for example, are not intended to be neutral and balanced and we know that newspapers and private broadcasters have and share political opinions. Moreover, the right to freedom of expression (as guaranteed by Article 10 of the European Convention on Human Rights) also covers information which – sometimes on purpose – is not accurate and views that could be shocking and hurt people and that could even be counterfactual. In other terms, disseminating content which is inaccurate and of low quality does not necessarily amount per se to an illegal (thus punishable) behaviour.

34. Certain actors have however more responsibilities than others. For example, people expect public authorities to deliver reliable information and national freedom of information acts secure (at least to a certain extent) access to such information detained by public administration. Similarly, media have a fundamental role in our democratic society and a responsibility in upholding the general interest by delivering quality information to the public; we expect a high level of accuracy and reliability of news broadcast by the media, and even more by public service media, offline and online.

35. Ideally, social media too should be a channel through which people access quality information, while avoiding manipulative and deceptive content which could drive social fractures. Even though social media do not create the informative content themselves, they have turned into a mainstream news provider for a significant proportion of the European and world population. In this sense, initiatives should be taken to guarantee that social media are a reliable channel for distributing and obtaining accurate, balanced and factual information.

36. Freedom of information is nothing but an illusion when the quality of the information available to readers is deteriorating and, despite the ever-growing number of sources (whose trustworthiness often goes unchecked), readers – unbeknownst to them – end up locked in bubbles where they can only find and access certain sources of information. The manipulation of opinions is a further problem here.

3.1. The issue of information disorder

37. Since the last United States presidential elections in particular, social media (mostly Facebook) have been accused of influencing the voters and the results through the information they allowed to be distributed. From all the issues regarding this topic, the one which gained the most attention was the so-called “fake news”. This concept can be wider defined as “fabricated information that mimics news media content in form but not in organisational process or intent”.²¹ This broad reference covers pieces of content related to news satire, news parody, fabrication, manipulation, advertising and political propaganda.²² Although the terminology of “fake news” is quite popular, I will speak here of “information disorder”, a concept which encompasses mis-information, dis-information and mal-information.²³ One side effect of online dis-information²⁴ and other types of online information disorder is a general feeling of distrust in journalism and the media sphere in general.²⁵

38. Moreover, social media has generalised a new kind of news consumption. In the traditional offline model, news was and is presented and received in a structured package, ordered in a hierarchical structure and delivered under a wide frame allowing users to interpret and give sense to the message.²⁶ Also, readers

21. Lazer D.M.J. *et al.*, (2018). The science of fake news. *Science*, 359(6380), pp. 1094-1096.

22. Tandoc Jr EC., Lim Z.W. and Ling R. (2018). Defining “Fake News” A typology of scholarly definitions. *Digital Journalism*, 6(2), pp. 137-153.

23. The Council of Europe report on “[Information Disorder: Toward an interdisciplinary framework for research and policy making](#)” describes the three different types as follows: Mis-information is when false information is shared, but no harm is meant; Dis-information is when false information is knowingly shared to cause harm; Mal-information is when genuine information is shared to cause harm, often by moving information designed to stay private into the public sphere.

24. On this specific issue see also the European Union report “[A multi-dimensional approach to online disinformation](#)”.

25. The report of our committee on “Public service media in the context of disinformation and propaganda” considers possible ways to deal with these problems also through an enhanced role of traditional media.

26. For example, when a user read a physical newspaper, he or she knew that pieces of news placed on the front page were the most important issues of the day, according to the editors’ criterion, and he could assume that pieces of news in the “political” section were more fact-based than those in the “editorial pages”, and that those in the “Lifestyle” section were to be taken less seriously than those in the “Science and Technology” pages.

knew that each medium delivered the news in particular frames and from different and particular perspectives.²⁷ This situation changed with the popularisation of news circulating through social media. In this new environment, content flows and reaches web users in an isolated way, with no context and with a weak link to the particular medium which publishes the news.

39. Thus, Facebook users are exposed to headlines, but lack any formal cue to interpret or detect bias or evaluate the quality of the medium which introduces the information summarised in those headlines. Standard and quality news providers such as the BBC or Euronews are placed along with links from satirical sites such as The Onion, or partisan media like Breitbart, Junge Freiheit, Libertad Digital or Fria Tider.

3.2. Biased access to preselected sources of information

40. Information and news reach audiences and social media users mostly through an automatised and personalised selection process, driven through carefully designed algorithms. Those algorithms are key parts of the technological development of social media and other internet-based platforms and environment, even though only 29% of people know that algorithms are responsible for the information which appears on their timelines and social media news feeds.²⁸

41. The algorithmic selection does not guarantee a balanced and neutral purveyance of information. In fact, algorithmic filtering can be biased by human and technological features which predetermine the nature, orientation or origin of filtered news.²⁹ In this sense, one of the greatest perils of Artificial Intelligence might be the proliferation of biased algorithms.³⁰

42. The idea behind the algorithmic filtering is a selection of news suited to the personal interests and preferences of each particular user. In some ways, it can be considered as a necessary service, because otherwise internet users would be obliged to seek the information they need from a sea of information of no interest to them. The likelihood of finding relevant information would depend on users' individual ability to correctly employ search tools that offer a wide choice of selection criteria, the time they could spend looking and their efforts to gradually hone their search. It is undoubtedly easier to rely on algorithms that run searches for us based on an individual "profile" they have established by analysing our data as it is fed into the system. However, is this risk-free?

43. We were reminded that interactions between an intelligent software agent (ISA) and human users are ubiquitous in everyday situations such as access to information, entertainment and purchases; and we have been warned that, in such interactions, the ISA mediates the user's access to the content, or controls some other aspect of the user experience, and is not designed to be neutral about outcomes of user choices. Research conducted by experts highlights that knowing users' biases and heuristics, it is possible to steer their behaviour away from a more rational outcome. The study also highlights that "while pursuing some short-term goal, an ISA might end up changing not only the user's immediate actions (e.g. whether to share a news article or watch a video) but also long-term attitudes and beliefs, simply by controlling the exposure of a user to certain types of content".³¹

44. As a result of the algorithmic selection, for example, each particular Facebook user news feed is unique. This is radically different to mass exposure to a same common media agenda and selection of topics, as happened with legacy media. This new trend in news consumption is leading to a lack of exposure to

27. In this sense, a reader expected that *The Times* or *Le Monde* introduced news in a more conservative interpretation than *The Guardian* or *Libération*. Meanwhile, tabloids like the *Daily Mail* or *Bild* offered a populist view of the current affairs and their information was expected to be less accurate and fact-based than those in "broadsheet" papers.

28. Newman N., Fletcher R., Kalogeropoulos A., Levy D.A.L. and Nielsen R.K. (2018). Digital News Report 2018. Reuters Institute for the study of journalism & Oxford University. <http://media.digitalnewsreport.org/wp-content/uploads/2018/06/digital-news-report-2018.pdf?x89475>. For example, Twitter was accused of silencing the Occupy movement protests by leaving it outside the "trending topics". The company explained that their algorithms selected as "trending topics" issues which provoked huge numbers of messages in short span periods. As the Occupy movement was a prolonged event which took place for months and did not reach high and brief intensity peaks of messages about that event, it never made it into the Twitter "trending topics".

29. Bozdag E. (2013). Bias in algorithmic filtering and personalization. *Ethics and information technology*, 15(3), pp. 209-227.

30. See (in Spanish): [Google advierte: el verdadero peligro de la IA no son los robots asesinos sino los algoritmos sesgados](#).

31. Burr C., Cristianini N. and Ladyman J. *An Analysis of the Interaction Between Intelligent Software Agents and Human Users*. In *Minds and Machines* (September 2018).

diverse sources of information. This phenomenon is known as “filter bubble” or “echo chamber”, a metaphor which tries to illustrate the situation where users only receive information which reinforces their prejudices and existing views. This factor contributes to radicalisation and growing partisanship in society.

3.3. Controlling the information and manipulation

45. The risk of manipulation of public opinion through the control of information sources is not new. Edward Bernays wrote in his seminal work, *Propaganda*:

“The conscious and intelligent manipulation of the organised habits and opinions of the masses is an important element in democratic society. Those who manipulate this unseen mechanism of society constitute an invisible government which is the true ruling power of our country.

We are governed, our minds molded, our tastes formed, our ideas suggested, largely by men we have never heard of. ...

Whatever attitude one chooses toward this condition, it remains a fact that in almost every act of our daily lives, whether in the sphere of politics or business, in our social conduct or our ethical thinking, we are dominated by the relatively small number of persons ... who understand the mental process and social pattern of the masses. It is they who pull the wires which control the public mind, who harness old social forces and contrive new ways to bind and guide the world.”³²

46. Bernays was speaking about American society in 1928. Today, with the internet, we are speaking about those few people who, through the internet and social media, are in a position to take control of all humanity. Nowadays, it is possible to achieve on a global scale what in the thirties could be done on the national scale through the monopoly of radio and of cinema newsreels.³³ In addition, mechanisms to prevent these abuses have been established at the national but not at the global level, namely because of jurisdictional problems.

4. The right to privacy

47. The right to privacy and to the protection of personal data is enshrined in Article 8 of the European Convention on Human Rights and key principles in this domain are stated by the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (STE No. 108). Personal data, as elements of “informational self-determination”, form an integral part of an individual; therefore, they cannot be sold or leased or given out. The individuals must be in control of their data and must have the possibility to decide on the processing of their data, including objecting to it at any time.

48. Sir Tim Berners-Lee (the inventor of the World Wide Web), at the opening of the Web Summit in Lisbon, on 5 November 2018, affirmed that the web is functioning in a dystopian way, referring to threats such as online abuse, discrimination, prejudice, bias, polarisation, fake news and political manipulation among others. Therefore, he called on governments, private companies and individuals to back a new “Contract for the Web” aimed at protecting people’s rights and freedoms on the internet.³⁴ This contract, which should be finalised and published in May 2019, will lay out core principles for using the internet ethically and transparently for all participants. I will highlight here two core [principles](#), one directed to governments and the other directed to the private companies: “Respect people’s fundamental right to privacy so everyone can use the internet freely, safely and without fear” and “Respect consumers’ privacy and personal data so people are in control of their lives online”.

49. The BBC is developing a concept of “Public Service Internet”. Its model is centred on four key themes; the first one on “Public-Controlled Data” implies the commitment to “treat data as a public good: put data back in the hands of the people, enhance privacy, and give the public autonomy and control over the data they create”.³⁵

32. Edward Bernays. *Propaganda* (1928), first paragraphs of Chapter 1.

33. Of course, we must keep in mind the difference between “media” and “social media”: the first are creators of news and can be manipulative through the creation of content; the second disseminate, curate and rank information and can be manipulative in the way they select or display content.

34. On this initiative, see for example the article published online by *The Guardian*: [Tim Berners-Lee launches campaign to save the web from abuse](#).

35. See: [Building A Public Service Internet](#).

50. The right to privacy is too often deeply affected by digital and social technologies. One of the issues in this regard is the exploitation of personal information. Digital technologies allow platforms and service providers to gather and analyse multiple information about their users. In some cases, these data are processed with legitimate purposes (such as evaluating the performance of content or improving some features of the platform). In other cases, however, the way these data are used raises concern.

51. Our committee report on “Internet and politics: the impact of new information and communication technology on democracy”,³⁶ for example, pointed to the issue of “semantic polling” – a technique for analysing large sets of data collected online, to draw conclusions about public opinion. Pollsters use methods for collecting and analysing data on Twitter and/or other networks about which the public have no information, which raises concerns about respect for privacy, in addition to the risk of distorting public opinion during electoral campaigns, for example (see paragraphs 60 and 61). The same report includes a twofold warning: on the one hand, “both personal data and the exercise of public freedoms on the web are subject to manipulation” and, on the other hand, “internet users have no way of knowing the details of how the processing algorithm works” (paragraph 68).³⁷ One of the main objectives of the modernisation process of Convention No. 108 was to address those issues at international level and to reinforce individuals’ rights.

52. I would add that, once sensitive data are collected, it is hard to offset the risk that they are made available to, and misused by, organisations or States with doubtful intentions. If the Cambridge Analytica case exemplifies possible misbehaviours by private organisations, I would also recall the recent decision (March 2018) of the Chinese Government to consider the data of its own citizens as the property of the Chinese State. As a result, many cloud providers (including Microsoft and Apple) have suspended their “cloud services” to Chinese citizens, obliging them to repatriate their data stored abroad in a server based in China, with all the consequences that this could provoke. The Chinese example could unfortunately be followed by other countries, even in Europe.

4.1. Information, user consent and privacy settings

53. Users are mostly unaware of the data a given service can collect from their activity. One of the most meaningful examples is what Facebook labels as “self-censorship posts”. This social media site registers and files everything the user posts and writes on its environment – every post, every comment – even though it is later deleted by the user and never published.

54. In this context, the information to the users and their meaningful consent (though there are cases when the latter is not required) are fundamental. When users join and access a social media site, they are accepting a series of terms and conditions of use, assimilated to a contract, but their implications are rarely understood. They are usually presented to users in an obscure and complex jargon, given that their primary aim is to avoid litigations rather than to clearly communicate the implications of using those platforms.³⁸

4.2. Data profiling, automated decision making and manipulation

55. The collection of vast amounts of personal information about users is connected to another worrying usage, which is called “micro-targeted advertising” or “data profiling”. By means of artificial intelligence, social media platforms label and categorise their users according to their behaviour, attitudes, etc. One problem is that those categories can identify beliefs or orientations that the user would rather not be made known to third parties. For example, it is known that Facebook allowed advertisers to address groups identified by its algorithm as “Jew haters”.³⁹ A study shows that automatic data classification can be used to identify homosexual users, even though no information is explicitly provided to the platform about the user’s sexual orientation.⁴⁰

36. [Doc. 13386](#).

37. Two other previous reports by our committee on “The protection of freedom of expression and information on the Internet and online media” ([Doc. 12874](#) and [Addendum](#)) and “The protection of privacy and personal data on the Internet and online media” ([Doc. 12695](#)) are also relevant in this respect.

38. Irene Pollach (2007), “What’s Wrong with Online Privacy Policies?”, *Communications of the ACM*, 50 (9), pp. 103-08.

39. Julia Angwin (2017), “Facebook’s Secret Censorship Rules Protect White Men from Hate Speech But Not Black Children”, ProPublica, www.propublica.org/article/facebook-hate-speech-censorship-internal-documents-algorithms; Angwin J., Varner M. and Tobin A. (2017). “Facebook enabled advertisers to reach ‘Jew haters’”, ProPublica, www.propublica.org/article/facebook-enabled-advertisers-to-reach-jew-haters.

40. Wang Y. and Kosinski M. (2018). Deep neural networks are more accurate than humans at detecting sexual orientation from facial images. *Journal of personality and social psychology*, 114(2), pp. 246-257.

56. The experts warned us that Big Data analytics and artificial intelligence are used to draw non-intuitive and unverifiable inferences and predictions about the behaviours, preferences and private lives of individuals, and this triggers new opportunities for discriminatory, biased and invasive decision-making. The suggestion in this respect was to consider the recognition of a new right to “reasonable inferences”.⁴¹ I find this proposal appealing, but I am not sure we need a new right, because, for me, Article 8 of the European Convention on Human Rights and the “modernised Convention 108”⁴² cover such inferences.

57. On 13 February 2019, the Committee of Ministers adopted a [Declaration on the manipulative capabilities of algorithmic processes](#). Noting that 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 warned the Council of Europe member States about the risks to democratic societies resulting from the possibility to employ advanced digital technologies, in particular micro-targeting techniques, to manipulate and control not only economic choices, but also social and political behaviours. The Declaration stresses, *inter alia*, the significant power that technological advancement confers to those – be they public entities or private actors – who may use algorithmic tools without adequate democratic oversight or control, and it underlines the responsibility of the private sector to act with fairness, transparency and accountability under the guidance of public institutions.

5. Ways forward

5.1. Upholding freedom of expression and freedom of information while avoiding abuses

58. Obviously, social media companies must comply with the legal requirements in each national setting and fight against the dissemination of unlawful material through their users' profiles. To enable them to do so effectively without resorting to forms of censorship, first the legislature must define objectionable content as clearly as possible. This means identifying the main characteristics of “terrorist propaganda”, “hate speech” or “defamation” and clearly indicating the responsibilities of social media companies faced with these trends (for example, the requirement to put in place detection mechanisms for unlawful content, which must subsequently be either temporarily blocked or reported to the authority responsible for ordering their removal).⁴³ It is the role of the legislature – and only the legislature – to set the boundaries of freedom of expression in full compliance with relevant international obligations, in particular those arising from Article 10 of the European Convention on Human Rights.

5.1.1. Improving social media content policies

59. Social media service providers should set no other limitations to the circulation of content, ideas and facts (i.e. accurate interpretation of historical events) than those defined by national regulations. Lawful (though controversial) political ideas and content should not be silenced or censored on social media spaces. Even where these providers establish their own set of rules for content, as a fundamental right, the right to freedom of expression is inalienable and user acceptance of standard contractual terms cannot absolve social media companies of their duty to respect this right. Furthermore, the standards set by social media service providers regarding admissible (or inadmissible) content must be defined in clear and unambiguous terms and be accompanied, if need be, by explanations and (fictional) examples of content banned from dissemination.

5.1.2. Enhancing information quality and counter disinformation

60. Social media companies must take an active part in identifying and warning their users about inaccurate or false content circulating through their venues. Automatic detection techniques – mainly based on linguistic cue approaches and network analysis approaches⁴⁴ – could help achieving this result.

41. See in this respect the paper by Sandra Wachter and Brent Mittelstadt (University of Oxford – Oxford Internet Institute) on [“A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI”](#).

42. Text resulting from Protocol (CETS No. 223) amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108).

43. The dividing line between “licit” and “illicit” content is not always easy to draw. This question is addressed in our committee’s ongoing report “Towards an Internet Ombudsman institution”.

44. Conroy N.J., Rubin V.L. and Chen Y. (2016). Automatic deception detection: Methods for finding fake news. *Proceedings of the Association for Information Science and Technology*, 52(1), 1-4.

61. For example, the network analysis approach makes it possible to identify bots (that is, accounts of users driven by a piece of software used to initially disseminate, repost and drive attention to the delivered fake pieces of news) by their behaviour. Therefore, social media sites could develop procedures and mechanisms to exclude bot-generated messages from their “trending” content or at least flag their accounts and the messages they repost. Another promising path currently being experimented on by some social media consists in blocking the possibility to “share” or “like” suspicious contents. However, technological and automated solutions might only provide a partial solution to this problem, as they would never prove the authenticity of a piece of news as a whole and focus mostly on distribution patterns.⁴⁵

62. Encouraging collaborative and social evaluation of the sources and pieces of news distributed could be an additional feature to be implemented. The online community could evaluate the accuracy and quality of the pieces of news they consult and on this basis a rating could be established, for example calculating an average score through votes of the users (as is the case with TripAdvisor reviews or Google Ratings). Web surfers could also have the possibility to flag misleading or inaccurate content; when several warnings are detected, the platform, after a careful verification by professionals, could include a label or a text indicating that there are doubts about the correctness of the content.

63. We need, however, to be aware that collective control mechanisms of this kind could be easily manipulated and biased, even beyond the good intentions of their creators.⁴⁶ Several users could take over a given piece of news if they agree and co-ordinate their efforts to misleadingly vote or disqualify it. That is, hundreds of supporters of a given political candidate could organise themselves to vote against pieces of news which picture politicians from a different tendency in a good light. However, there are solutions to avoid this situation. For instance, a high number of votes or notifications should be required to label the piece of news as “inaccurate”, as social evaluation systems are more trustworthy when they are based on high amounts of votes. This system could work better on Facebook, an environment where it is difficult to set up bots to manipulate the system (voting massively against one piece of news, for instance).

64. There are also initiatives that could be followed in the offline sphere. Mainstream and alternative media have launched section-specific websites and other projects in order to debunk fake news and fight misinformation through fact-checking initiatives which might be useful to counterbalance the circulation of deceiving and misleading information through social media, as stated in the European Commission Report on “A multi-dimensional approach to online disinformation”.

65. Social media sites could deliver and regulate “badges” or other graphical elements to identify content linked to quality news providers.⁴⁷ This recognition could be granted to media which meet given criteria, such as the following:

- a. most of their content is news about current events presenting civic and socially relevant information;
- b. most of their staff are professional journalists (e.g. with a university degree in communication sciences or an equivalent professional certification);
- c. a very high percentage of their news (e.g. 99%) are proven to be fact based and accurate.

66. The co-operation of social media with traditional media is a key tool to fight information disorder. In this respect, I praise and wish to support the Journalism Trust Initiative (JTI) launched by Reporters Without Borders (RSF) and its partners, the European Broadcasting Union (EBU), Agence France-Presse (AFP) and the Global Editors Network (GEN). The JTI is pursuing a self-regulatory and voluntary process aimed at creating a mechanism to reward media outlets which provide guarantees regarding transparency, verification and correction methods, editorial independence and compliance with ethical norms. At present, the algorithmic distribution of online content does not include an “integrity factor” and tends to amplify sensationalism, rumours, falsehoods and hate. To reverse this logic, the project is currently developing machine-readable criteria for media outlets, big and small, in the domains of identity and ownership, journalistic methods and ethics.⁴⁸

45. Huckle S. and White M. (2017). Fake news: a technological approach to proving the origins of content, using blockchains. *Big data*, 5(4), pp. 356-371.

46. The recent example of the inexistent London restaurant that became first in the ranking of TripAdvisor’s most rated and liked places proves that even the collaborative evaluation (in the absence of a transparent and accountable mechanism) could become a trap. See www.vice.com/en_uk/article/434gqw/i-made-my-shed-the-top-rated-restaurant-on-tripadvisor.

47. For example, a system of levels could be adopted, in order to establish “green sites” (which cover all predetermined criteria), “yellow sites” (which cover some of these criteria), “red sites” (which cover one criterion) and “black sites” (which cover no criterion or offer no information about this issue). The same colour code policy could apply to news quoted from these sites.

67. Last but not least, individual sharing of content is a crucial factor in the diffusion of fake news in social media: as long as one person believes and shares a fake news piece, that lie will continue its path into the public agenda. Thus, efforts should be made to improve media literacy and the development of critical thinking and attitudes towards media content. Digital media literacy attempts to develop competences related to finding, using and evaluating information on the internet.⁴⁹ It is vital to address competences which include understanding, detecting and preventing the spread of fake news and other kinds of misinformation. Our committee is preparing a specific report on this issue, to which I refer.⁵⁰

5.1.3. Ensuring diversity of sources, topics and views

68. Social media companies tend to argue that personalisation of the content offered to their users is a core feature of their business model, but research shows that personalisation of content is compatible with bringing a wider diversity of topics to the final users.⁵¹ Algorithms can be designed and implemented to encourage plurality and diversity of views, attitudes and opinions.⁵²

69. Ideally, companies should call on some outside evaluation and auditing in order to determine that their algorithms are not biased and foster plurality or diversity of facts, points of views and opinions. That said, those algorithms are not transparent enough to be evaluated or analysed; but this reality should not prevent the evaluation of the findings. Tests could be made in order to detect the kind of content which each algorithm filters and selects, and the kind of media content which appears on the user's news feed. Even though there are no mechanisms to make this recommendation mandatory, a "Seal of Good Practices" could be awarded to internet operators whose algorithms are designed to foster the selection of plural content, thus enabling ideologically cross-cutting exposure.

70. Another interesting idea builds on the possibility to widen the range of the "reaction buttons" (such as Facebook buttons allowing the expression of "Love", "Wow" or "Sad" reactions) and introduce an "Important" button, in order to encourage and gain visibility for relevant issues but with low emotional content.⁵³ This would enhance the reach of relevant content and make it stand above the irrelevant and meaningless content shared by emotional triggers.

5.2. Strengthening users' control over their data

71. I believe that the right to privacy implies that users must be able to regulate the access of third parties to their personal data, which are collected by social media platforms as a core part of their business plan. According to the preamble of the modernised Convention 108: "It is necessary to secure the human dignity and protection of human rights and fundamental freedoms of every individual and ... personal autonomy based on a person's right to control of his or her personal data and the processing of such data." This is not what happens today in practice. The Cambridge Analytica scandal is just the tip of an iceberg of doubtful practices, which we can no longer ignore.

5.2.1. Information, user consent and privacy settings

72. Users lack real knowledge about the information which social media companies collect on them and the purposes that data collection serves. The modernised Convention 108 and European Union legislation ask that the information provided to the users of these platforms be concise, transparent, intelligible and easily accessible.⁵⁴ The reality is however quite different.

48. See: [More than 100 media outlets and organizations are backing the Journalism Trust Initiative](#).

49. Cheever N.A. and Rokkum J. (2015). Internet Credibility and Digital Media Literacy. *The Wiley Handbook of Psychology, Technology, and Society*, pp. 56-73.

50. Media education in the new media environment (rapporteur: Ms Nino Gogvadze, Georgia, EC).

51. Möller J., Trilling D., Helberger N. and van Es B. (2018). Do not blame it on the algorithm: An empirical assessment of multiple recommender systems and their impact on content diversity. *Information, Communication & Society*, 21(7), pp. 959-977.

52. Bozdag E. and van den Hoven J. (2015). Breaking the filter bubble: democracy and design. *Ethics and Information Technology*, 17(4), pp. 249-265.

53. Pariser E. (2011). *The filter bubble: What the Internet is hiding from you*. Penguin UK.

54. Namely, according to the General Data Protection Regulation of the European Union (Article 30), users are entitled to the following information (among others): purposes of the data processing; description of the categories of data subjects and of the categories of personal data related to the processing; information on the categories of recipients to whom personal data have been, or will be, disclosed; information on whether transfers of personal data to third countries or international organisations have been, or will be, carried out.

According to Article 8 of the modernised Convention 108, the controller shall inform the data subject of:

73. An option to improve the readability of the contractual terms and conditions which the users have to accept could be the elaboration of visual-based summaries of the information listed on those legal documents, which has been proved to guarantee a better understanding of complex information.

74. In this respect, some scholars⁵⁵ propose that companies should adopt privacy policies presented in the form of “nutritional labels” and that the information could be summarised in a table, instead of a series of paragraphs. That “label” should give an answer to, at least, the following questions:

- Who can see what I post?
- What is going to be known about me?
- Which data are you going to collect about me?
- What are you going to do with my data?
- What are you going to do with my content?
- Who can contact or reach me?

75. Ideally, users should not only be able to get this information, but also to set rules and adapt the answers to those questions. It could also be asked that privacy settings are always set by default at the highest restriction level. Most users do not ever change these settings; therefore, social media companies set the lowest restriction level in order to collect the maximum amount of information possible. Changing and making the setting-up of those conditions mandatory on the most restrictive options would mean the highest protection for every user and not only those with digital skills or those who are more aware of data protection and privacy problems.

76. According to data protection laws and to the European Union General Data Protection Regulation (GDPR), internet operators (like any data controller) are obliged to have a valid legal base to collect user data, but many of them have applied a wide range of malpractices, in order to manipulate users and trick them into choosing the least restrictive options and privacy settings. For instance, some services choose counter-intuitive interfaces that, when collecting different categories of information, ask the users to choose between just two unlabelled buttons, with no text attached. One of the buttons was red and the other was green. Unexpectedly, the “red” option meant that the user accepted those conditions. I believe that special attention should be paid to this kind of malpractice, which should be detected and reprimanded or even punished.

77. In addition to this, unacceptable conditions or practices should be blacklisted and prohibited, in order to protect individuals from abusive behaviour from social media and internet companies. This should be the case, for example, with the selling of personal data by data brokers, which should not be allowed under any circumstances.

78. Another key principle of data protection (now also enshrined in Article 17 of the GDPR) is the right to erasure: data subjects have the right to obtain from the controller the erasure of personal data concerning them without undue delay, including in the case of withdrawal of the consent previously given.

79. This implies that the platform should also erase that information from its servers and no longer process it or include it in the users' profile and aggregated information. There should be no distinction between “visible information” and “invisible information”. That would also stop companies like Facebook from collecting users' activity in other webpages while the social networking site is open in a different browser tab.

80. I would like to stress that the modernised Convention 108 (unfortunately not in force yet) is a corpus of very clear principles and in particular legitimacy of data processing, which must find its legal basis in the valid, (thus informed) consent of the users or in another legitimate reason laid down by law, as well as the principles

“a. his or her identity and habitual residence or establishment;

b. the legal basis and the purposes of the intended processing;

c. the categories of personal data processed;

d. the recipients or categories of recipients of the personal data, if any; and

e. the means of exercising the rights set out in Article 9,

as well as any necessary additional information in order to ensure fair and transparent processing of the personal data.”

55. Fox A.K. and Royne M.B. (2018). Private information in a social world: assessing consumers' fear and understanding of social media privacy. *Journal of Marketing Theory and Practice*, 26(1-2), pp. 72-89.

of transparency and proportionality of data processing, data minimisation, privacy by design and privacy by default; the controllers, as defined in Article 2 of the modernised Convention 108 should be bound to take adequate measures to ensure the rights of the data subjects, as listed in its Article 9.1, according to which:

“Every individual shall have a right:

- a. not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration;*
- b. to obtain, on request, at reasonable intervals and without excessive delay or expense, confirmation of the processing of personal data relating to him or her, the communication in an intelligible form of the data processed, all available information on their origin, on the preservation period as well as any other information that the controller is required to provide in order to ensure the transparency of processing ...;*
- c. to obtain, on request, knowledge of the reasoning underlying data processing where the results of such processing are applied to him or her;*
- d. to object at any time, on grounds relating to his or her situation, to the processing of personal data concerning him or her unless the controller demonstrates legitimate grounds for the processing which override his or her interests or rights and fundamental freedoms;*
- e. to obtain, on request, free of charge and without excessive delay, rectification or erasure, as the case may be, of such data if these are being, or have been, processed contrary to the provisions of this Convention;*
- f. to have a remedy ... where his or her rights under this Convention have been violated;*
- g. to benefit, whatever his or her nationality or residence, from the assistance of a supervisory authority ... in exercising his or her rights under this Convention.”*

81. The Council of Europe member States should take the necessary steps to ratify the modernised Convention 108 as soon as possible, and in the meantime check and adapt their regulations to ensure their consistency with its principles and the effective protection of the rights of the data subjects that this convention proclaims. The Parties to Convention 108 which are not member States of the Council of Europe should also take the steps required for a rapid entry into force of the amending protocol.

5.2.2. *Oversee, correct and refuse data profiling*

82. Any profiling should respect Committee of Ministers [Recommendation CM/Rec\(2010\)13](#) on the protection of individuals with regard to automatic processing of personal data in the context of profiling.

83. On 28 January 2019, the Consultative Committee of the Convention 108 has published [Guidelines on Artificial Intelligence and Data Protection](#). These guidelines aim to assist policy makers, artificial intelligence (AI) developers, manufacturers and service providers in ensuring that AI applications do not undermine the right to data protection. The Convention 108 Committee underlines that the protection of human rights, including the right to protection of personal data, should be an essential prerequisite when developing or adopting AI applications, in particular when they are used in decision-making processes, and should be based on the principles of the modernised Convention 108. In addition, any innovation in the field of AI should pay close attention to avoiding and mitigating the potential risks of processing personal data and should allow meaningful control by data subjects over the data processing and its effects. These guidelines refer to important issues previously identified in the [Guidelines on the Protection of Individuals with regard to the Processing of Personal Data in a World of Big Data](#) and to the need to “secure the protection of personal autonomy based on a person’s right to control his or her personal data and the processing of such data”.

84. Therefore, users should have the right to oversee, evaluate and, ideally, refuse profiling. The opacity of the social media platform algorithms makes it difficult, but we can call for internet operators to implement good practice in this respect too and ask that public authorities force internet operators in the right direction if they are not willing to do it spontaneously. For example, governments could encourage social media companies to include a privacy feature where the users can check all the “micro-categories” they have been labelled into and determine, if they so wish, which categories must not apply to them.

85. Concerning micro-targeting advertising, a feature should be added in promoted publications (that is, paid or advertised) and organic reach publications (the ones seen by the user outside any promotional campaign). This feature, which could be named “Why am I seeing this”, should provide the user with all the information which has been used to offer him that post or piece of content. This feature should also let the

user ask for any information or data the platform is using to filter and promote content according to the data profile it possesses from the user, and for their deletion.⁵⁶ Of course, this feature should not be placed in a remote, hidden position in the “privacy settings” options, but it should be accessible, ideally like a button in every post, so that it can be easily checked by every user.

86. Furthermore this feature would contribute to an effective implementation of the right to object to the *processing*. Users are entitled to restrict the processing of their data to a given lapse of time; they should also have the right, in principle, to restrict the kind of information that is being processed about them. This also fits with the idea of “layered notices” which allow the users to set up the level of detail he or she prefers to be processed. Thus, processing could be restricted by the user by temporal co-ordinates but also by excluding different facets of his or her activity or personality.

5.2.3. Give back to users full control over their data

87. As mentioned above, the access to an online content or service is (almost) systematically subject to a so-called “consent”, which differs however from the one described in Article 5.2 of the modernised Convention 108, according to which “data processing can be carried out on the basis of the free, specific, informed and unambiguous consent of the data subject”. In the majority of cases, a simple tick in a box, with a link to a lengthy and legalistically drafted privacy policy, enables the data controller to disclose and even transfer user data to third parties. This practice should be stopped. The data subject has to remain in control of his/her data. The business model which builds on that implicit “consent” and has its main revenue from the selling of “targeted advertisement” based on these data should be subject to an open and inclusive public debate.

88. I would like to stress that the privacy issue is perceived as a crucial one by the World Wide Web community itself, or at least by part of it. For Sir Tim Berners-Lee, data openness and greater respect for privacy online are not in contradiction. In a note entitled “[One Small Step for the Web...](#)”, published on 28 September 2018, he has announced the launching of *Solid*, an open-source project which is intended to change the current model where users hand over their personal data to internet operators in exchange for the services they provide.

89. In this note, Tim Berners-Lee denounces that “the web has evolved into an engine of inequity and division; swayed by powerful forces who use it for their own agendas”. He adds that “Solid is how we evolve the web in order to restore balance – by giving every one of us complete control over data, personal or not, in a revolutionary way” and explains that this new platform “gives every user a choice about where data is stored, which specific people and groups can access select elements, and which apps you use. It allows you, your family and colleagues, to link and share data with anyone. It allows people to look at the same data with different apps at the same time”.

90. In other terms, *Solid* aims to allow users to create, manage and secure their own personal online data stores (“PODs”), i.e. a kind of “digital safe”, which can be located at home, at work or within a selected POD provider, and where users can store information such as photos, contacts, calendars, health data or others. They then can grant to other people, entities and apps permissions to read or write to parts of their Solid POD.

91. It should be noted that the concept of *Solid* is not entirely new; in France, a new service called [Cozy Cloud](#) has been available since the beginning of 2018. This service has the same ambition: to allow every person to benefit from more uses of his/her personal data while repossessing them.

92. A difficulty is however that the most popular online services – like Gmail or Facebook – do not seem to have on their agenda the development in the short term of their tools to ensure their compatibility with *Solid*. Maybe regulators should intervene to force such developments. The BBC announced a special app for child online protection, where all private data are locally stored on the device; this is an encouraging sign of a new trend in this direction, confirming that the advantages of personalised services could be conjugated with the right to privacy.

56. For example, if one given user is seeing an advertisement about “animal adoption”, he or she should be able to ask why the post is appearing in his or her newsfeed. The “why I am seeing this?” feature should then list the information upon which the filtering and promotion has been based and the “categories” – if any – the user appears in or the “categories” the advertiser looked for. If, for example, one of the reasons is that the user is listed as “vegan” (because he or she regularly posts vegetarian recipes), that reason should be clearly stated.

6. Conclusions

93. The Assembly and the Committee of Ministers have addressed many recommendations to national authorities and social media which target the issues of freedom of expression, freedom of information and privacy (also in relation to data gathering and data protection). However, this remains work in progress. We are in an environment which is continuously evolving at high speed; thus, in this domain, we need to continuously rethink, refine and complement our action.

94. I am convinced that the key to succeeding in our efforts to ensure effective protection for fundamental rights is to follow the path of co-operation between different actors and in particular here between public authorities and social media. In this respect, I welcome the fact that partners like Google and Facebook have agreed to engage in dialogue and contribute to this reflection.

95. By questioning the dominant business model of today's internet economy – a model based on the collection, analysis and use of our personal data – this report seeks to provoke thought. Do we wish to accept this model as the price we have to pay to use the services offered by internet companies? Or can we come up with another viable solution?

96. In so far as social media platforms have become major distributors of news and other journalistic content, such distribution cannot be exclusively driven by the aim of profit. Social media companies must endorse certain public interest responsibilities with regard to the editorial role that some platforms are already performing, but not in the most transparent manner, and to the massive exploitation of personal data.

97. Furthermore, the issue of the use of personal data is not just a question of protecting our right to privacy; it is also about being able to surreptitiously control us and skew the functioning of democracy, thereby rendering it meaningless.

98. This report makes no attempt to offer a miracle solution or definitive answer. My aim, with the assistance of the experts who have helped us, was to reflect on how, together, we can put the individual back at the heart of the debate on the role and responsibilities of social media. This is the reasoning behind the wide range of proposals I have offered on practical measures to take.