EUROPEAN
COMMISSION

Brussels, 26.4.2018
COM(2018) 236 final

# COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

## Tackling online disinformation: a European Approach

## 1. INTRODUCTION

The exposure of citizens to large scale disinformation, including misleading or outright false information, is a major challenge for Europe.

Our open democratic societies depend on public debates that allow well-informed citizens to express their will through free and fair political processes. Media have traditionally played a key role in holding public authorities to account and in providing the information that enables citizens to form their own views on societal issues and actively and effectively participate in democratic society. In Europe, traditional media is subject to a wide range of rules on impartiality, pluralism, cultural diversity, harmful content, advertising and sponsored content. Democracy in the European Union rests on the existence of free and independent media.[1]

Today, the Internet has not only vastly increased the volume and variety of news available to citizens but has also profoundly changed the ways citizens access and engage with news. Younger users, in particular, now turn to online media as their main source of information. The easy availability of diverse quality information has the potential to make democratic processes more participatory and inclusive.

Yet, new technologies can be used, notably through social media, to disseminate disinformation on a scale and with speed and precision of targeting that is unprecedented, creating personalised information spheres and becoming powerful echo chambers for disinformation campaigns.

Disinformation erodes trust in institutions and in digital and traditional media, and harms our democracies by hampering the ability of citizens to take informed decisions. Disinformation also often supports radical and extremist ideas and activities. It impairs freedom of expression, a fundamental right enshrined in the Charter of Fundamental Rights of the European Union (Charter).[2] Freedom of expression encompasses respect for media freedom and pluralism, as well as the right of citizens to hold opinions and to receive and impart information and ideas "without interference by public authorities and regardless of frontiers".

The primary obligation of state actors in relation to freedom of expression and media freedom is to refrain from interference and censorship and to ensure a favourable environment for inclusive and pluralistic public debate. Legal content, albeit allegedly harmful content, is generally protected by freedom of expression and needs to be addressed differently than illegal content, where removal of the content itself may be justified. As the European Court of Human Rights has concluded, this is particularly important in relation to elections.[3]

Mass online disinformation campaigns are being widely used by a range of domestic and foreign actors to sow distrust and create societal tensions, with serious potential

[1] http://ec.europa.eu/information_society/newsroom/image/document/2016-50/2016-fundamental-colloquium-conclusions_40602.pdf

[2] Article 11, Charter. Article 6(1) of the Treaty of the European Union confers binding force on the Charter and states that it "shall have the same legal value as the Treaties."

[3] See e.g. Case of Bowman v. The United Kingdom (141/1996/760/961) http://hudoc.echr.coe.int/eng?i=001-58134.

consequences for our security. Furthermore, disinformation campaigns by third countries can be part of hybrid threats to internal security, including election processes, in particular in combination with cyberattacks. For example, Russian military doctrine explicitly recognises information warfare as one of its domains.[4]

The spread of disinformation also affects policy-making processes by skewing public opinion. Domestic and foreign actors can use disinformation to manipulate policy, societal debates and behaviour in areas such as climate change, migration, public security, health[5], and finance. Disinformation can also diminish trust in science and empirical evidence.

In 2014, the World Economic Forum identified the rapid spread of misinformation online as one of the top 10 trends in modern societies.[6]

In 2016, social media news aggregators and search engines were, taken together, the main ways to read news online for 57% of users in the EU.[7] As regards young people, a third of 18–24s say social media are their main source of news.[8]

80% of Europeans have come across information they believe was false or misleading several times a month or more. 85% of respondents perceive this as a problem in their country.[9]

The online platforms that distribute content, particularly social media, video-sharing services and search engines, play a key role in the spread and amplification of online disinformation. These platforms have so far failed to act proportionately, falling short of the challenge posed by disinformation and the manipulative use of platforms' infrastructures. Some have taken limited initiatives to redress the spread of online disinformation, but only in a small number of countries and leaving out many users. Furthermore, there are serious doubts whether platforms are sufficiently protecting their users against unauthorised use of their personal data by third parties, as exemplified by the recent Facebook / Cambridge Analytica revelations, currently investigated by data protection authorities, about personal data mined from millions of EU social media users and exploited in electoral contexts.

The rise of disinformation and the gravity of the threat have sparked growing awareness and concerns in civil society, both in EU Member States and internationally. In March 2015, the European Council invited the High Representative to develop an action plan to address Russia's on-going disinformation campaigns,[10] which resulted in establishing East Stratcom Task Force, effective as planned since September 2015. In a June 2017 Resolution, the European Parliament called upon the Commission "to analyse in depth

[4] https://www.rusemb.org.uk/press/2029

[5] In the area of vaccine hesitancy, the Commission is proposing a Council Recommendation including specific measures to monitor and tackle disinformation in this area. See COM (2018)245/2

[6] http://reports.weforum.org/outlook-14/top-ten-trends-category-page/10-the-rapid-spread-of-misinformation-online/.

[7] https://ec.europa.eu/digital-single-market/en/news/eurobarometer-internet-users-preferences-accessing-content-online.

[8] *Digital News Report 2017*, Reuters Institute, https://reutersinstitute.politics.ox.ac.uk/risj-review/2017-digital-news-report-now-available.

[9] http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/flash/surveyky/ 2183.

[10] http://www.consilium.europa.eu/en/press/press-releases/2015/03/20/conclusions-european-council/

the current situation and legal framework with regard to fake news and to verify the possibility of legislative intervention to limit the dissemination and spreading of fake content."[11] In March 2018, the European Council stated "social networks and digital platforms need to guarantee transparent practices and full protection of citizens' privacy and personal data."[12] The *Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda,* adopted in 2017 by Special Rapporteurs appointed by international organisations,[13] provides a focused treatment of the application of international human rights standards to this phenomenon.

Several Member States are currently exploring possible measures to protect the integrity of electoral processes from online disinformation and to ensure the transparency of online political advertising.[14]

It is clear, however, that while the protection of the electoral process lies primarily within the competence of Member States, the cross-border dimension of online disinformation makes a European approach necessary in order to ensure effective and coordinated action and to protect the EU, its citizens, its policies and its Institutions.

This Communication has been developed taking into account the extensive consultations with citizens and stakeholders. The Commission set up in late 2017 a High-Level Expert Group to advise on this matter. The Group delivered its report on 12 March 2018.[15] The Commission also launched a broad public consultation process, comprising online questionnaires that received 2,986 replies,[16] structured dialogues with relevant stakeholders,[17] and a Eurobarometer opinion poll covering all 28 Member States.[18]

This Communication sets out the views of the Commission on the challenges associated with disinformation online. It outlines the key overarching principles and objectives which should guide actions to raise public awareness about disinformation and tackle the phenomenon effectively, as well as the specific measures which the Commission intends to take in this regard.

## 2. SCOPE AND CAUSES OF ONLINE DISINFORMATION

### 2.1. Scope

Disinformation is understood as verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and

[11] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2017-0272+0+DOC+PDF+V0//EN.

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

[13] *Joint Declaration on Freedom of Expression and "Fake News," Disinformation and Propaganda*, http://www.osce.org/fom/302796?download=true.

[14] Some Member States have adopted – or are planning to adopt - measures regarding political advertising. These include inter alia the recent French draft law on false information and non-binding guidelines proposed by the Italian regulator.

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

[16] https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-fake-news-and-online-disinformation.

[17] https://ec.europa.eu/epsc/events/high-level-hearing-preserving-democracy-digital-age_en and https://ec.europa.eu/digital-single-market/en/fake-news.

[18] http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/flash/surveyky/2183.

may cause public harm. Public harm comprises threats to democratic political and policy-making processes as well as public goods such as the protection of EU citizens' health, the environment or security. Disinformation does not include reporting errors, satire and parody, or clearly identified partisan news and commentary. This Communication is without prejudice to the applicable legal rules at Union or national level relating to the issues discussed, including disinformation containing illegal content.[19] This Communication is without prejudice to ongoing approaches and actions in relation to illegal content, including as regards terrorist content online and child sexual abuse material.

83% of Europeans consider fake news to present a problem for democracy in general, either "definitely" (45%) or "to some extent" (38%).[20]

Intentional disinformation aimed at influencing elections and immigration policies were the two top categories considered likely to cause harm to society, according to respondents to a public consultation conducted by the Commission. These were closely followed by disinformation in the fields of health, environment, and security policies.[21]

### 2.2. The context and main causes of disinformation

The proliferation of disinformation has interrelated economic, technological, political, and ideological causes.

First, the spread of disinformation is a symptom of wider phenomena that affect societies facing rapid change. Economic insecurity, rising extremism, and cultural shifts generate anxiety and provide a breeding ground for disinformation campaigns to foster societal tensions, polarisation, and distrust. Organisations and agencies of influence (be they undertakings, states, or non-governmental organisations with a stake in political and policy debates, including sources external to the EU) can use disinformation to manipulate policy and societal debates. The impact of disinformation differs from one society to another, depending on education levels, democratic culture, trust in institutions, the inclusiveness of electoral systems, the role of money in political processes, and social and economic inequalities.

In the long term, tackling disinformation will only be effective if accompanied by clear political will to strengthen collective resilience in support of our democratic bearings and European values.

Second, the spread of disinformation takes place in the context of a media sector undergoing profound transformation. The rise of platforms active in the media sector has deeply affected journalists and professional news media outlets, which are still generally seeking to adapt their business models and find new ways to monetise content. Moreover, some platforms have taken on functions traditionally associated with media outlets, entering the news business as content aggregators and distributors without necessarily taking on the editorial frameworks and capabilities of such outlets. Their economic incentives lead them to capture a large users' base by exploiting network

[19] Commission Recommendation of 1 March 2018 on measures to effectively tackle illegal content online (C(2018) 1177 final), https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-measures-effectively-tackle-illegal-content-online.

[20] https://ec.europa.eu/digital-single-market/en/news/first-findings-eurobarometer-fake-news-and-online-disinformation.

[21] https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-fake-news-and-online-disinformation.

effects and to maximize the time users spend on their services by privileging quantity of information over quality, regardless of the impact.

Between 2010 and 2014, news publishers' total print revenues decreased by €13.45 billion and digital revenues rose by €3.98 billion: a net revenue loss of €9.47 billion (-13%).[22] In addition, news publishers report that the current decline of the industry has already led to closing down or reducing their editorial teams.[23]

Third, social networking technologies are manipulated to spread disinformation through a series of sequential steps: (i) creation; (ii) amplification through social and other online media; and (iii) dissemination by users.

**(i) Creation of disinformation**

Disinformation is a powerful and inexpensive – and often economically profitable – tool of influence. To date, most known cases have involved written articles, sometimes complemented by authentic pictures or audiovisual content taken out of context. But new, affordable, and easy-to-use technology is now available to create false pictures and audiovisual content (so called "deep fakes"), offering more potent means for manipulating public opinion.

**(ii) Amplification through social and other online media**

A variety of drivers provide a fertile ground for the spread of disinformation online. The mechanics of the proliferation of disinformation are:

– Algorithm-based: The criteria algorithms use to prioritise the display of information are driven by the platforms' business model and the way in which this privileges personalised and sensational content, which is normally most likely to attract attention and to be shared among users. By facilitating the sharing of personalised content among like-minded users, algorithms indirectly heighten polarisation and strengthen the effects of disinformation.

– Advertising-driven: Today's digital advertising model is often click-based, which rewards sensational and viral content. This model relies on advertising networks operated by agencies that ensure real-time placement of ads based on algorithmic decision-making. This facilitates the placement of advertisements on websites that publish sensationalist content appealing to users' emotions, including disinformation.

– Technology-enabled: Online technologies such as automated services (referred to as "bots") artificially amplify the spread of disinformation. These mechanics can be facilitated by simulated profiles (fake accounts) which have no authentic user behind them, sometimes orchestrated on a massive scale (referred to as "troll factories").

**(iii) Dissemination by users**

[22] http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=17211.
[23] https://ec.europa.eu/digital-single-market/en/news/public-consultation-role-publishers-copyright-value-chain-and-panorama-exception.

Users themselves are also playing a role in disseminating disinformation, which tends to travel more quickly on social media due to the propensity of users to share content without any prior verification. The ever-increasing volume and speed of content flowing online increases the risk of indiscriminate sharing of disinformation.

Although the most popular news websites have a higher average monthly reach, false news spread more virally. For example, in France, one false news outlet generated an average of over 11 million interactions per month—five times greater than more established news brands.[24]

Respondents to the public consultation considered that disinformation spreads more easily via online media because it appeals to readers' emotions (88%), can influence the public debate (84%), and is designed to generate revenues (65%).[25]

## 3. A EUROPEAN APPROACH TO TACKLE ONLINE DISINFORMATION

Given the complexity of the matter and the fast pace of developments in the digital environment, the Commission considers that any policy response should be comprehensive, continuously assess the phenomenon of disinformation, and adjust policy objectives in light of its evolution.

There should be no expectation that a single solution could address all challenges related to disinformation. At the same time, inaction is not an option.

In the Commission's view, the following overarching principles and objectives should guide action to tackle disinformation:

- First, to improve transparency regarding the origin of information and the way it is produced, sponsored, disseminated and targeted in order to enable citizens to assess the content they access online and to reveal possible attempts to manipulate opinion.
- Second, to promote diversity of information, in order to enable citizens to make informed decisions based on critical thinking, through support to high quality journalism, media literacy, and the rebalancing of the relation between information creators and distributors.
- Third, to foster credibility of information by providing an indication of its trustworthiness, notably with the help of trusted flaggers, and by improving traceability of information and authentication of influential information providers.
- Fourth, to fashion inclusive solutions. Effective long-term solutions require awareness-raising, more media literacy, broad stakeholder involvement and the cooperation of public authorities, online platforms, advertisers, trusted flaggers, journalists and media groups.

[24] *Measuring the reach of "fake news" and online disinformation in Europe,* Reuters Institute https://reutersinstitute.politics.ox.ac.uk/our-research/measuring-reach-fake-news-and-online-disinformation-europe.

[25] https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-fake-news-and-online-disinformation.

Building on all gathered input, the Commission intends to take the following actions. They complement the General Data Protection Regulation, which will apply across the EU as from 25 May 2018, and which will strengthen protection of the personal data of users of online platforms.[26] The General Data Protection Regulation clarifies the notion of consent and includes the key concept of transparency of processing. It also clarifies and harmonises the conditions under which personal data can be further shared ("further processed").

### 3.1. A more transparent, trustworthy and accountable online ecosystem

The mechanisms that enable the creation, amplification and dissemination of disinformation rely upon a lack of transparency and traceability in the existing platform ecosystem and on the impact of algorithms and online advertising models. Therefore, it is necessary to promote adequate changes in platforms' conduct, a more accountable information ecosystem, enhanced fact-checking capabilities and collective knowledge on disinformation, and the use of new technologies to improve the way information is produced and disseminated online.

#### *3.1.1. Online platforms to act swiftly and effectively to protect users from disinformation*

There are growing expectations that online platforms should not only comply with legal obligations under EU and national law, but also act with appropriate responsibility in views of their central role so as to ensure a safe online environment, to protect users from disinformation, and to offer users exposure to different political views.

Overall, platforms have not provided sufficient transparency on political advertising and sponsored content. They also have not made sufficient information available on the use of strategic dissemination techniques, such as paid human influencers and/or robots to market messages. This has been a major driver of initiatives in some Member States and third countries adopting measures on transparency around political advertising online.

The Commission calls upon platforms to decisively step up their efforts to tackle online disinformation. It considers that self-regulation can contribute to these efforts, provided it is effectively implemented and monitored.

To this end, the Commission will support the development of an ambitious Code of Practice, building on the Key Principles proposed by the High Level Expert Group[27] and committing online platforms and the advertising industry to achieve the following objectives:

- Significantly improve the scrutiny of advertisement placements, notably in order to reduce revenues for purveyors of disinformation, and restrict targeting options for political advertising;

- Ensure transparency about sponsored content, in particular political and issue-based advertising; this should be complemented by repositories where comprehensive

[26] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

[27] https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation, p. 32 of the HLEG report.

information about sponsored content is provided, such as the actual sponsor identity, amounts spent and targeting criteria used. Similar mechanisms should be put in place so that users understand why they have been targeted by a given advertisement;

- Intensify and demonstrate the effectiveness of efforts to close fake accounts;

- Facilitate users' assessment of content through indicators of the trustworthiness of content sources, based on objective criteria and endorsed by news media associations, in line with journalistic principles and processes, transparency regarding media ownership and verified identity;

- Dilute the visibility of disinformation by improving the findability of trustworthy content;

- Establish clear marking systems and rules for bots and ensure their activities cannot be confused with human interactions;

- Empower users with tools enabling a customized and interactive online experience so as to facilitate content discovery and access to different news sources representing alternative viewpoints; provide them with easily-accessible tools to report disinformation;

- Ensure that online services include, by design, safeguards against disinformation; this should, for example, include detailed information on the behaviour of algorithms that prioritise the display of content as well as development of testing methodologies;

- Provide trusted fact-checking organisations and academia with access to platform data (notably via application programming interfaces), while respecting user privacy, trade secrets, and intellectual property; this will enable them to better understand the functioning of related algorithms and better analyse and monitor disinformation dynamics and their impact on society.

Actions pursuing these objectives should strictly respect freedom of expression and include safeguards that prevent their misuse, for example, the censoring of critical, satirical, dissenting, or shocking speech.[28] They should also strictly respect the Commission's commitment to an open, safe and reliable Internet.

*The Commission will convene **a multistakeholder forum on disinformation**, to provide a framework for an efficient cooperation among relevant stakeholders, including online platforms, the advertising industry and major advertisers, media and civil society representatives, and to secure a commitment to coordinate and scale up efforts to tackle disinformation. This forum is separate from the EU Internet Forum on terrorist content online. The forum's first output should be an **EU–wide Code of Practice on Disinformation** to be published by July 2018, with a view to producing measurable effects by October 2018. The Commission will assess its implementation, in broad consultation with stakeholders and on the basis of key performance indicators based on*

[28] As the European Court of Human Rights has observed, freedom of expression applies not only to information and ideas that are favourably received or inoffensive, but also to those "offend, shock or disturb." *Handyside v. United Kingdom*, App. No. 5493/72 (7 December 1976), § 49.

*the above objectives. Should the results prove unsatisfactory, the Commission may propose further actions, including actions of a regulatory nature.*

*In parallel, the Commission will launch a* ***study to examine the applicability of EU rules and possible gaps in relation to the identification of online sponsored content****. In this context, it will also assess the effectiveness of possible identification tools for online sponsored content.*

#### *3.1.2. Strengthening fact checking, collective knowledge, and monitoring capacity on disinformation*

Fact-checkers have emerged as an integral element in the media value chain, verifying and assessing the credibility of content based on facts and evidence. They also analyse the sources and processes of information creation and dissemination. Fact-checkers' credibility depends upon their independence and their compliance with strict ethical and transparency rules.

A dense network of strong and independent fact-checkers is an essential requirement for a healthy digital ecosystem. Fact-checkers need to operate on the basis of high standards, such as the International Fact-Checking Network *Code of Principles.*[29]

In addition, many aspects of disinformation remain insufficiently analysed and access to online platforms' data is still limited. An effective response requires a solid body of facts and evidence on the spread of disinformation and its impact. Additional data gathering and analysis by fact-checkers and academic researchers should include the following activities:

- Continuously monitoring the scale, techniques and tools, and the precise nature and potential impact of disinformation;
- Identifying and mapping disinformation mechanisms that contribute to digital amplification;
- Contributing to the development of fair, objective, and reliable indicators for source transparency; and
- Sharing knowledge with news media, platforms and public authorities to enhance public awareness about disinformation.

Providing better access to online platforms' data and a secure space to analyse and exchange information are key requirements.

*As a first step, the Commission will support the* ***creation of an independent European network of fact-checkers*** *to establish common working methods, exchange best practices, achieve the broadest possible coverage across the EU, and participate in joint fact-checking and related activities. The network will be invited to participate in the multistakeholder forum on disinformation. The Commission will make available to the network online tools (e.g. a secured shared space) to enable their collaboration.*

[29] The International Fact-Checking Network (IFCN) Code of Principles is for organizations that regularly publish nonpartisan reports on the accuracy of statements by public figures and major institutions and other widely circulated claims of interest to society, https://www.poynter.org/international-fact-checking-network-fact-checkers-code-principles.

*As a second step, the Commission will launch a **secure European online platform on disinformation** to support the independent European network of fact-checkers and relevant academic researchers. The platform should offer cross-border data collection and analysis tools, as well as access to EU-wide open data, such as reliable independent statistical information. This will enable the network to act as trusted flaggers. It will also facilitate deeper understanding of online disinformation and formulation of evidence-based strategies for further limiting its spread. To this end, the Commission will consider the use of the Connecting Europe Facility and build on the experience gained in implementing the "Safer Internet" programme.*

#### *3.1.3. Fostering online accountability*

Identification of the source of disinformation by ensuring its traceability throughout its dissemination is essential to accountability, as well as to increase trust in identifiable suppliers of information and encourage more responsible behaviour online. For instance, a user could choose to only engage with others on online platforms that have identified themselves.

To this end, the Regulation on electronic identification[30] provides a predictable regulatory environment for the online cross-border use, recognition and enforcement of electronic identification, authentication and trust services that could be relied upon to foster the development and the voluntary use of systems for the secure identification of suppliers of information based on the highest security and privacy standards, including the possible use of verified pseudonyms.

To facilitate the investigation of malicious online behaviour, as indicated in the Joint Communication on Cybersecurity presented in September 2017, the Commission will continue to promote the uptake of Internet Protocol version 6 (IPv6), which allows the allocation of a single user per Internet Protocol address. It will also pursue its efforts to improve the functioning of and the availability and accuracy of information in the Domain Name and IP WHOIS[31] systems in line with the efforts of the Internet Corporation for Assigned Names and Numbers (ICANN) and in full compliance with data protection rules.

*The Commission will encourage the eIDAS Cooperation Network to promote, in cooperation with platforms, voluntary online systems allowing the identification of suppliers of information based on trustworthy electronic identification and authentication means, including verified pseudonyms, as provided under the Regulation on electronic identification.*

Taken altogether, these would also contribute to limiting cyberattacks, which are often combined with disinformation campaigns in the context of hybrid threats.

#### *3.1.4. Harnessing new technologies*

Emerging technologies will further change the way information is produced and disseminated, but they also have the potential to play a central role in tackling disinformation over the longer term. For instance:

[30] Regulation 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[31] https://whois.icann.org/en

– Artificial intelligence, subject to appropriate human oversight, will be crucial for verifying, identifying and tagging disinformation;

– Technologies for media to enable customizable and interactive online experiences can help citizens discover content and identify disinformation;

– Innovative technologies, such as blockchain, can help preserve the integrity of content, validate the reliability of information and/or its sources, enable transparency and traceability, and promote trust in news displayed on the Internet. This could be combined with the use of trustworthy electronic identification, authentication and verified pseudonyms; and

– Cognitive algorithms that handle contextually-relevant information, including the accuracy and the quality of data sources, will improve the relevance and reliability of search results.

The Commission is active in the field of emerging technologies, in particular through its Next Generation Internet initiative.[32]

*The Commission will make **full use of the Horizon 2020 work programme to mobilise these technologies**. Beyond, the Commission will also **explore the possibility for additional support** to help deploy tools to combat disinformation, accelerating time-to-market of high-impact innovation activities, and encouraging the partnering of researchers and businesses.*

### 3.2. Secure and resilient election processes

The security of election processes, the basis for our democracy, requires particular attention. Disinformation now forms part of a wider array of tools used to manipulate electoral processes, such as hacking or defacing websites or gaining access to and leaking personal information about politicians. Cyber-enabled operations may be used to compromise the integrity of public information and prevent the identification of disinformation sources. This is critical during election campaigns, where compressed schedules may prevent timely detection of disinformation and response.

In recent years online manipulation and disinformation tactics were detected during elections in at least 18 countries, and *"disinformation tactics contributed to a seventh consecutive year of overall decline in internet freedom"*.[33]

With a view to the 2019 European Parliament elections, the Commission has encouraged[34] the competent national authorities to identify best practices for the identification, mitigation and management of risks to the electoral process from cyberattacks and disinformation. In the Cooperation Group established under the Directive on the security of Network and Information Systems (NIS Directive), Member States have started to map existing European initiatives on cybersecurity of network and information systems used for electoral processes, with the aim of developing voluntary guidance.

[32] https://ec.europa.eu/digital-single-market/en/next-generation-internet-initiative.
[33] *Freedom on the net 2017 report*, Freedom house, https://freedomhouse.org/report/freedom-net/freedom-net-2017.
[34] Commission recommendation of 14.2.2018 on enhancing the European nature and efficient conduct of the 2019 elections to the European Parliament, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL%3A2018%3A045%3ATOC.

*The Colloquium on Fundamental Rights 26-27 November 2018 will focus on "Democracy". Key ingredients for inclusive and healthy democratic societies will be discussed, including opportunities and challenges brought about by digitalisation for an informed and pluralistic democratic debate and discuss the negative impact of propaganda.*

*The Commission will initiate a continuous dialogue to support Member States in the management of risks to the democratic electoral process from cyber-attacks and disinformation, particularly in view of such processes in Member States and the European elections of 2019. This will include:*

*- appropriate follow-up to a first exchange with Member States at the conference on electoral best practices held on 25-26 April 2018;*

*- all the necessary support, together with the European Union Agency for Network and Information Security, to the work that the NIS Cooperation Group is carrying out on the cybersecurity of elections. By the end of 2018, the Group should deliver a compendium of practical recommendations and measures that can be implemented by Member States to secure election life-cycles.*

*- a high-level conference with Member States on cyber-enabled threats to elections in late 2018 under the auspices of the Security Union Task Force.*

### 3.3. Fostering education and media literacy

The life-long development of critical and digital competences, in particular for young people, is crucial to reinforce the resilience of our societies to disinformation.

The Digital Education Action Plan, adopted by the Commission in January 2018,[35] highlights the risks disinformation poses for educators and students and the urgent need to develop digital skills and competences of all learners, in both formal and non-formal education. The Digital Competence Framework for Citizens, developed by the Commission, sets out the wide mix of skills needed by all learners, from information and data literacy, to digital content creation, to online safety and well-being.[36]

A majority of respondents to the public consultation considered that educating and empowering users to better access and use online information and informing users when content is generated or spread by a bot are measures online platforms can take that would have a strong impact on preventing the spread of disinformation.[37]

Because of the cross-border dimension of disinformation, the EU has a role in supporting the dissemination of good practice across the Member States to increase citizens' resilience, and the Commission can further strengthen its actions addressing young people and adults:

[35] https://ec.europa.eu/education/sites/education/files/digital-education-action-plan.pdf.
[36] https://ec.europa.eu/jrc/en/digcomp/digital-competence-framework.
[37] https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-fake-news-and-online-disinformation.

- The Commission steers the Media Literacy Expert Group and supports pilot project such as 'Media Literacy for All'.[38]

- The Audiovisual Media Services Directive recognises the importance of media literacy,[39] and its revision aims at strengthening the monitoring of actions undertaken by the authorities of Member States on media literacy.[40]

- The Commission supports a number of initiatives, including through the Erasmus+ programme, on Internet safety, digital well-being and, digital skills that aim at fostering a critical awareness of citizens – in particular, young people – of the digital environment, which in turn helps strengthen digital media literacy.

- Member States, social partners and education organisations share experience and good practice on digital education through the EU's Working Group on Digital Skills and Competences.[41]

- The Commission encourages Member States to mobilise resources and include in their educational policies digital citizenship, media literacy, the development of critical-thinking skills for the online environment, and awareness-raising activities on disinformation and online amplification techniques. Support for teachers, including training and sharing of good practice is vital in this respect.

*Furthermore, the Commission will:*

- *Encourage independent fact-checkers and civil society organisations to provide educational material to schools and educators.*

- *Include in the #SaferInternet4EU[42] Campaign targeted initiatives on disinformation online.*

- *Organise a European Week of Media Literacy with the aim of raising awareness and support cross-border cooperation amongst relevant organisations.*

- *Report on media literacy in the context of application of the Audiovisual Media Services Directive.*

- *Work with the Organisation for Economic Co-operation and Development, in the framework of the Programme for International Student Assessment process, to explore the possibility of adding media literacy to the criteria used by the organisation in its comparative reports.*

[38] https://ec.europa.eu/digital-single-market/en/news/2016-call-proposals-pilot-project-media-literacy-all
[39] The Audiovisual Media Services Directive states that "the development of media literacy in all sections of society should be promoted and its progress followed closely" (Recital 47).
[40] In its general approach, the Council has included an obligation for Member States to promote and take measures for the development of media literacy skills. This requirement is currently being discussed by the co-legislators as part of the revision of the Audiovisual Media Services Directive.
[41] https://ec.europa.eu/education/policy/strategic-framework/expert-groups/digital-skills-competences_en
[42] https://www.betterinternetforkids.eu/web/portal/saferinternet4eu.

– *Further encourage the work of the Digital Skills and Jobs Coalition,*[43] *to support digital skills, including for participation in society.*

– *Continue implementation of the Digital Education Action Plan*[44] *and continue to support initiatives, such as the Digital Opportunity traineeship,*[45] *which aim at strengthening digital skills and the awareness of European citizens – in particular, the younger generation – and promoting common values and inclusion.*

### 3.4. Support for quality journalism as an essential element of a democratic society

Quality news media – including public media – and journalism play an important role in providing citizens high quality and diverse information. By ensuring a pluralistic and diverse media environment, they can uncover, counterbalance, and dilute disinformation.

In an evolving digital environment, there is a need to invest in high quality journalism, reinforce trust in the key societal and democratic role of quality journalism both offline and online, and encourage quality news media to explore innovative forms of journalism.

According to the Eurobarometer survey, citizens perceive traditional media as the most trusted sources of news: radio (70%), television (66%) and print newspapers and news magazines (63%). The least trusted sources of news are video hosting websites (27%) and online social networks (26%). Younger respondents are more likely to trust news and information they access online.[46]

There is also a need to rebalance the relation between media and online platforms. This will be facilitated by a swift approval of the EU copyright reform, which will improve the position of publishers and ensure a fairer distribution of revenues between right holders and platforms, helping in particular news media outlets and journalists to monetise their content.

Journalists and media professionals should also further embrace the opportunities offered by new technologies and develop the necessary digital skills to enable them to use data and social media analytics, with a view to enhancing fact-finding and verification.

Finally, public support to media and public service media are very important to the provision of high quality information and the protection of journalism in the public interest. Member State support measures in view of achieving objectives of common EU interest, such as media freedom and pluralism, have been declared compatible with EU State aid rules, as demonstrated by Commission Decisions on media aid.[47]

[43] https://ec.europa.eu/digital-single-market/en/digital-skills-jobs-coalition.
[44] https://ec.europa.eu/digital-single-market/en/news/specific-actions-digital-education-action-plan.
[45] https://ec.europa.eu/digital-single-market/en/digital-opportunity-traineeships-boosting-digital-skills-job.
[46] http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/flash/surveyky/2183.
[47] The Commission notably has approved aid for news agencies (e.g. SA.30481, State Aid in favour of Agence France-Press (AFP), France, http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=3_SA_30481), general press aid schemes (e.g. SA.36366, Production and innovation aid to written media, Denmark, http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=3_SA_36366) and schemes

*Member States are encouraged to consider horizontal aid schemes to address market failures hampering the sustainability of quality journalism, as well as support measures for specific activities, such as training for journalists, service and product innovation.*

*Existing rules*[48] *clarify the conditions under which public support may be granted by Member States. To enhance the transparency and predictability of State aid enforcement in this area, the Commission will make an online repository publicly available, with reference to the applicable State aid rules and relevant precedent cases. Moreover, regularly updated information on aid granted by Member States will be accessible on the transparency register.* [49]

*The Commission will* ***launch a call in 2018 for the production and dissemination of quality news content on EU affairs*** *through data-driven news media.*

*Building on ongoing projects, the Commission will explore increased funding opportunities to support* ***initiatives promoting media freedom and pluralism, quality news media and journalism,*** *including skills, training for journalists, new technologies for newsrooms, and collaborative data-driven platforms.*

*The Fundamental Rights Agency* ***toolkit for media professionals on coverage from a fundamental rights angle*** *will provide recommendations, tips and tools to journalists on how to deal with ethical dilemmas, including disinformation, from a fundamental rights angle.*

### 3.5. Countering internal and external disinformation threats through strategic communication

Communication and awareness-raising by public authorities is an integral part of the response to disinformation. In addition to detection and data analysis, strategic communication requires suitable outreach activities to counter false narratives. The measures set out in Section 3.1 will make detection and analysis of online disinformation more accurate and timely, and will facilitate strategic communication about Europe and EU policies.

This is particularly important since the EU is often a target of disinformation campaigns designed to undermine its Institutions, policies, actions and values. The sources of such activities can be domestic or external, the actors private or public – and they carry out their activities both on EU territory and in third countries. As noted, in 2015 the East Stratcom Task Force was set up within the European External Action Service to address

targeting publications with limited advertising revenue (e.g. SA.47973 French Press Aid 2015 Decree France, http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=3_SA_47973).

[48] Regarding public service broadcasting, specific detailed guidelines are in place (Communication from the Commission on the application of State aid rules to public service broadcasting, OJ C 257 of 27 October 2009, p.1). Depending on the type of support envisaged, the guidelines for R&D&I aid (Communication from the Commission — Framework for State aid for research and development and innovation, OJ C 198 of 27 June 2014, p. 1) and the General Block Exemption Regulation (Commission Regulation (EU) No 651/2014 of 17 June 2014 declaring certain categories of aid compatible with the internal market in application of Articles 107 and 108 of the Treaty, OJ L 187 of 26 June 2014, p. 1, as amended by Commission Regulation (EU) 2017/1084 of 14 June 2017, OJ L 156 of 20.6.2017, p. 1) may also be relevant.

[49] State aid transparency public search page: https://webgate.ec.europa.eu/competition/transparency/public/search/home?lang=en.

Russia's on-going disinformation campaigns, in recognition of one important dimension of this challenge. Similarly, the EU Hybrid Fusion Cell was established in 2016 within the EU Intelligence and Situation Centre to monitor and address hybrid threats by foreign actors, including disinformation, aimed at influencing political decisions inside the EU and in its neighbourhood. These institutions, together with the recently established European Centre of Excellence for Countering Hybrid Threats, form the basis of a strengthened European response,[50] and are important elements in the cooperation between EU and the North Atlantic Treaty Organisation to improve European resilience, coordination and preparedness against hybrid interference.

*The Commission, in cooperation with the European External Action Service will strengthen its strategic communication capability by first reinforcing the internal coordination of its communication activities aiming at tackling disinformation.*

*The Commission, in cooperation with the European External Action Service, will extend this collaboration, its knowledge and its activities to other EU institutions and, through an appropriate mechanism, to Member States. The network will use the data gathered by the secure online platform on disinformation referred to in Section 3.1.2 in order to design outreach activities aimed at countering false narratives about Europe and tackling disinformation, within and outside the EU.*

*The Commission and the European External Action Service will explore further options to develop strategic communications responses and other mechanisms, together with Member States, to build resilience as well as counter systematic disinformation campaigns and hybrid interference by foreign governments towards citizens and entities in the EU.*

*The Commission, in cooperation with European External Action Service, will report in June on the progress on bolstering capabilities to address hybrid threats, including cybersecurity, strategic communication and counter intelligence areas.*

## 4. CONCLUSION

A well-functioning, free, and pluralistic information ecosystem, based on high professional standards, is indispensable to a healthy democratic debate. The Commission is attentive to the threats posed by disinformation for our open and democratic societies. This Communication presents a comprehensive approach that aims at responding to those serious threats by promoting digital ecosystems based on transparency and privileging high-quality information, empowering citizens against disinformation, and protecting our democracies and policy-making processes. The Commission calls on all relevant players to significantly step up their efforts to address the problem adequately. It considers that the actions outlined above, if implemented effectively, will materially contribute to countering disinformation online. However, the Commission will continue its work is this area.

By December 2018, the Commission will report on progress made. The report will also examine the need for further action to ensure the continuous monitoring and evaluation of the outlined actions.

[50] *Joint Framework on countering hybrid threats: a European Union response*, Joint Communication to the European Parliament and Council of 6 April 2016, JOIN(2016) 18 final, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=en.