INFORMING THE “DISINFORMATION” DEBATE

JOINT REPORT BY

ACCESS NOW
CIVIL LIBERTIES UNION FOR EUROPE
EUROPEAN DIGITAL RIGHTS

18 October 2018

Table of contents

Executive Summary

Access Now, Civil Liberties Union for Europe (Liberties) European Digital Rights (EDRi) (hereinafter "we" or "the undersigned organisations") have evaluated the Report of the High Level Expert Group on Fake News and Online Disinformation[1] (hereinafter "HLEG Report") and related policy documents dealing with online "disinformation" and/or "fake news" from different EU bodies and institutions. This document represents our combined contribution, to provide constructive feedback for the European Commission's elaboration of an Action Plan on this topic.

Good policy development

Our analysis, building on our experience in policy development in relation to a wide range of problematic content, is that credible benchmarks are an essential element of good policy development.

Good benchmarking requires a clear understanding of the nature, size and evolution of the problem being addressed. Our analysis confirms the need for targeted research, in order to be able to develop strategy but also, crucially, to adapt strategy in a continually changing online environment.

Concerns regarding proposed solutions

Our analysis then moves on to look at solutions that have been proposed or implemented as responses to disinformation. This includes:

- *Fact-checking*

The HLEG Report proposed an "independent European Network of fact-checkers". Such initiatives are not a novel invention. Our analysis concludes that the task is far more complex than it seems. In particular, it is difficult to guarantee independence or accidental or deliberate bias. Significantly more work is therefore needed to ensure the credibility and validity of such networks, particularly over time.

- *Artificial intelligence and emerging technologies*

Technology often seems to be both the cause of and solution to all problems. Ultimately, any such technology will be privately implemented and therefore will have questions regarding accountability. Shortcomings like inaccuracy, bias, lack of accountability and transparency have implications on - not least – freedom of expression, personal data protection, privacy, the rights to non-discrimination and equality, access to information, to participation in cultural life, to meaningful access to remedy, and more.

- *EU vs Disinfo*

For reasons that are not particularly obvious, the European External Action Service East Stratcom Task Force has an "EU versus Disinformation" campaign. It is focused on pro-Kremlin disinformation on outlets that are accused of being "linked to the Kremlin or pro-Kremlin". There is no indication that this approach has any positive impact, but it has led to difficulties for legitimate websites.[2]

- *Limiting anonymity*

The suggestion has been made in various contexts that limiting or abandoning anonymity online would be a positive contribution to fighting disinformation. Our analysis suggests that this would be a significant infringement of fundamental freedoms. Furthermore, this cost is not likely to lead to the hoped-for benefits.

More meaningful solutions

Controlling online manipulation as a business model

Our analysis points out that the main economic purpose of key social media companies is to collect enough data to be able to manipulate the economic and political choices of individuals. More data is collected by keeping the internet user's attention and therefore it seems logical to assume that more sensationalist stories are more amenable to this business model. We therefore argue for strong enforcement of the General Data Protection Regulation (GDPR) and the rapid adoption of the ePrivacy Regulation in order to counterbalance this effect.

Preventing the misuse of personal data in elections

We welcome recent steps by the European Commission to ensure that electoral processes are not manipulated through the misuse of personal data. This problem is closely related to disinformation, as it is the same social media companies that are expected to "self-regulate" their curation of news feeds and search results that profit from tracking-based targeted election advertising.

Media and information literacy

Here, we agree with the recommendation of the HLEG Report on media literacy, including that "media literacy cannot […] be limited to young people but needs to encompass adults as well as teachers and media professionals". The Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda" issued jointly by the United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information (the "special mandate holders") correctly points out, "[s]tates should take measures to promote media and digital literacy, including by covering these topics as part of the regular school curriculum and by engaging with civil society and other stakeholders to raise awareness about these issues."

Introduction

This document is intended as a positive contribution to EU- and national-level discussions around the problem of disinformation – sometimes inappropriately referred to as "fake news".

The signatory organisations all work to defend fundamental rights and believe that answers to this phenomenon must be and can be protective of core values of the European Union.

The protection of fundamental rights is one of the primary goals of the European Union. As explained in the Charter of Fundamental Rights of the European Union, it is necessary to strengthen the protection of fundamental rights in light of changes in society, social progress and scientific and technological developments.

Among fundamental rights, freedom of expression is one of the core values of democracies. It is not only about protecting information or ideas that are "favourably received or regarded as inoffensive", but also about protecting those that "offend, shock or disturb the State or any sector of the population" (European Court of Human Rights, case 5493/72). "Solutions" that are proposed that put regulation of freedom of expression into the hands of profit-motivated corporations seriously threaten this core principle.

The undersigned organisations point to the definitions used in the Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda" issued jointly by the United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information (the "special mandate holders") (hereinafter Joint Declaration).[3] We advise against the use of the term "fake news". We first refer to the terms disinformation and propaganda according to Joint Declaration and we will further elaborate on the necessary elements of the definition of disinformation to accurately address the problem at hand:

- disinformation: statements which are known or reasonably should be known to be false. It misleads population, and as a side effect it interferes with the public's right to know and the right of individuals to seek, receive, and impart information.
- propaganda: statements which demonstrate a reckless disregard for verifiable information.

We also add:

- misinformation: is false information, but the person who is disseminating it believes it to be true.

We understand the subject matter of this joint report primarily, but not only, as analysing, responding to and building on the recommendations of the Commission and the Report of the High Level Expert Group on Fake News and Online Disinformation[4] (hereinafter "HLEG Report") to address the issue of the intentional dissemination of information that is designed to have an impact on democracy, journalism and civic space.

The special mandate holders expressed concerns in their Joint Declaration that "disinformation and propaganda are often designed and implemented so as to mislead a population, as well as to interfere with the public's right to know and the right of individuals to seek and receive, as well as to impart, information and ideas of all kinds". There are situations, however, when disinformation and propaganda does not achieve that designed impact, but at scale, they can still negatively influence the democratic discourse and the digital sphere. Any policy recommendation or action must be based on evidence related to that negative impact.

We should not live in a world where conversations about important topics cannot happen online due to over-strict, vague, or unpredictable terms of service, that are enforced by unaccountable online companies against specific speech due to governmental or public relations pressure. If we were all prompted to think or write in the same way, we would no longer live in a society where there is freedom of thought, expression and opinion. Member States and the EU may only impose restrictions on people's fundamental rights, such as freedom of expression and opinion, our rights to privacy and data protection, if it is provided for by law; if the essence of our rights and freedoms is respected; if the restriction is necessary and proportionate; and if it serves a genuine objective of general interest or - with certain limitations - is needed to protect the rights and freedoms of others.

While our report mostly focuses on online media, we believe that the role of partisan television, radio channels and print newspapers in contributing to the problems at hand should also be reflected upon, as well as the specificities of distorted advertisement markets in both online and offline media.

Section 1: Elements of good policy development

Chapter 1.1 Evidence-based policy

Definition

The first step to developing policy is to be clear about the definition of the issue at hand.

The HLEG created a definition of *disinformation*: It includes all forms of false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit. It does not cover issues arising from the creation and dissemination online of illegal content. Nor does it cover other forms of deliberate but not misleading distortions of facts, such a satire and parody.

The definition is not clear for five reasons:

1. The definition for disinformation starts with "all forms" of content. There is a difference between intent and effect, the fact that something is intended maliciously does not mean that the effect merits restrictive measures. "All" is also too broad, as there is always some sort of information that should not fall under the definition. It's better to avoid the broad terms such as "all forms".

2. The definition sets "false", "inaccurate" and "misleading" as alternative criteria, because of using the word "or". To set these requirements as conjunctive criteria would create a clearer definition. Many people would argue that many, if not all, of the ostensibly inaccurate reports from the UK press quoted (promoted by the European Commission, albeit without malicious intent) on the blog of the EC Mission to the UK would fall under this definition, even though the European Commission does not overtly accuse the outlets in question (including the Guardian, Financial Times, The Times and others) as being purveyors of "disinformation".[5]

3. The definition attempts to cover both online and offline content; the exclusion of illegal content, however, is only applicable to online content. The exclusion of illegal content is supported by the undersigned organisations, but all illegal content should be excluded, both online and offline.

4. The definition of disinformation requires that the content intentionally causes public harm or is designed for profit. Profit is a very risky element of the definition on its own. Again, taking measures to restrict an activity that is not illegal, on the basis of intention rather than impact is clearly unwise.

5. Satire and parody are not disinformation and should be excluded. The undersigned organisations support this idea. However, one should note that parody and satire often deliberately, maliciously and misleadingly distort facts. The fact that it was felt necessary to introduce these exceptions indicates the weakness of the definition.

The undersigned organisations suggest that the definition be rewritten according to the above-mentioned criteria:

> *Disinformation includes ~~all forms of~~ false, inaccurate, ~~or~~* ***and*** *misleading information designed, presented and promoted to intentionally in ways that cause* ***demonstrable and significant*** *public harm ~~or for profit~~. It does not cover issues arising from the creation and dissemination ~~online~~ of illegal content.*

Create Benchmarks

In order to find and implement appropriate and proportionate solutions to any problem, it is crucial to assess the issue accurately. This enables the creation of benchmarks, against which the proportionality, success or failure of policy initiatives can be assessed.

This is a greater challenge with regard to "disinformation" than it is with regard to other content regulation issues. It is a greater challenge because the content in question can exist without causing harm, can be consumed without causing harm, is difficult to define and appears in different forms in different media. The challenge of benchmarking is shown most clearly by the fact that the HLEG Report explicitly says that research "has shown that citizens often associate the term 'fake news' with partisan political debate and poor journalism broadly, rather than more pernicious and precisely defined forms of disinformation." This statement alone casts huge doubt on the reliability of the statistics generated by the Eurobarometer report on "fake news" presented by the European Commission. That report appears not to have taken this risk into account to any appreciable extent and makes benchmarking on the basis of those data much more difficult, if not impossible. Such mistakes should be diligently avoided.

For policy development, benchmarking needs to define, for example:

- the scale of the problem being addressed;
- the mechanisms for identifying counterproductive effects and;
- the levels and impacts that would trigger the abandonment of measures that have been implemented.

It is absolutely crucial to refrain from assumptions that simple deletion or flagging of political advertising/misinformation is, of itself, a positive metric, as the European Commission has repeatedly done in relation to online regulation problems, such as "hate speech".[6]

The undersigned organisations believe that benchmarking is needed to define the scale at which public or private action would be considered necessary and proportionate. The benchmarking criteria must be in line with existing human rights standards. It is important to define the impacts that are expected of the action that is proposed or required.

Conduct Research

The undersigned organisations urge the European Commission to commission independent and thorough research on online disinformation. As ARTICLE 19 pointed out, "new research shows that online misinformation might have a broad reach but would in fact have only little impact on the public. This might not mean that all the agitation is entirely in vain, but before we can develop a genuine response to the spread of misinformation we need to understand what impact it's having."[7]

Research is necessary to ensure a proper policy-making process that is based on evidence, rather than being based on hot trends, popular phrases and political slogans. We need more information about how disinformation affects the media and the online landscape, individual users and society as a whole. For example, what is the influence or impact of personal-data driven clickbait and attention-grabbing platforms in driving this phenomenon?

We need research to understand the effect of online and offline disinformation. Without knowing what the real impact disinformation has and its drivers, policy-makers will not have the tools to develop and implement effective and proportionate responses to the problems that need to be tackled.

Section 2: Limitations of existing "solutions"

Chapter 2.1 Fact-checking is a questionable solution for disinformation

It is generally agreed that reliable information is necessary for a functioning democracy. However, it is less certain who has the authority to assess what constitutes an incontrovertible fact or "truth", or whether someone should have that authority at all.

Fact-checking initiatives have been a noticeable part of news reporting in certain countries for some years. For example, in traditional news media, in 2003, US based Factcheck.org extended its scope to cover politics. Similarly, in 2005 in the United Kingdom, the Channel 4 News *Fact Check Blog* was established for the same purpose. In addition, collaborative efforts by multiple stakeholders have resulted in the organisation of projects such as The Credibility Coalition and The Trust Project.

The Commission's call for the creation of an independent European Network of fact-checkers raises questions, as assuring the independence and criteria for correctly carrying out the task of "fact-checking" is not as easy or simple as it sounds. There are risks of conflicts of interest, both direct and indirect, abuse of power, bias and other significant costs involved in institutionalised "fact checking," for which there is no demonstrable benefit.

Furthermore, regardless of the outcome, the verdicts of independent fact-checkers often still come under scrutiny, be it for ideological reasons, reliability of data, or inherent bias. With regard to the last point, fact-checking according to a particular viewpoint is, of course, permissible, as a part of the freedom to impart information. Nonetheless, it is clear that fact-checking may not be sufficient to combat skepticism towards the media.

Proposals for private companies, especially online platforms, to participate in fact-checking are worrisome. They are also not arbiters of truth, it is neither in their interest nor design (i.e. their business model) to prioritise "truth" or "facts". The role these companies could play in elaborating community standards regarding fact checking should be transparent and meaningfully contestable at independent bodies. We need to consider also that it is important to remain cognisant of the fact that some internet giants also sell election influence as a service, which raises fundamental questions regarding conflicts of interest and their role as part of the problem rather than part of the solution.

We urge the Commission that, before creating any fact-checking mechanism or body, it should assess existing international best practices, networks,[8] models and standards to focus on seeding trusted, non-compromised fact-checkers in the media.

One criterion of assessing the credibility and validity of such networks should be evidence that the set standards are enforced and they do not accept organisations to their network (or keep them in this role) that do not meet their requirements.

The undersigned organisations therefore recommend refraining from simplistic "fact-checking" solutions and considering their impacts and potential (un)intended consequences.

Chapter 2.2 Artificial Intelligence and emerging technologies

Private and public sector initiatives in relation to emerging technologies appear mostly based on the belief that, through Artificial Intelligence (AI), society will be able to better address a broad spectrum of issues, ranging from hate speech and extremist content, to copyright violations, and the spread of disinformation online.[9] There is however still a great deal of uncertainty and lack of evidence about the actual impact of these technologies both on addressing the alleged problems and their possible impact on human rights.[10]

As the HLEG Report states, "disinformation is a multifaceted problem, which does not have one single root cause and thus does not have one single solution". Machine learning systems alone are therefore inadequate to solve the problem of disinformation, and a blind faith in a technical solution risks seriously infringing on human rights and failing to achieve public policy goals.

We disagree with the HLEG Report's assertion about the legitimacy of the application of tools such as "behavioural data collection, analytics, advertising exchanges, tools for cluster detection and tracking social media sentiment" as a general rule. This overlooks the fact that much of this technology would be implemented by economic actors that are, to put it mildly, not without fault in the promotion of sensationalist news as a means of competing in the market for individuals' attention. We also stress the fundamental rights infringements generated by such technologies for privacy and freedom of expression.

Shortcomings like inaccuracy, bias, lack of accountability and transparency have implications for, at least, freedom of expression, personal data protection, privacy, the rights to non-discrimination and equality, access to information, to participation in cultural life, to meaningful access to remedy, and more. In order to avoid these harms and shortcomings, human rights law and standards must be respected in the development and use of technology if it is to be deployed to combat the proliferation of disinformation, as is elucidated in the Toronto Declaration.[11]

The undersigned organisations warn that the development and deployment of any emerging technology must respect fundamental rights and be human-centric. Private and public sectors must uphold their obligations and responsibilities under human rights law. Governments must fully respect their positive obligations with regard to private-sector application of any such technologies.

Chapter 2.3 EU vs Disinfo (East Stratcom)

The EU vs Disinfo[12] project appears to have been set up without any particular plan in mind. There is little obvious benefit in collecting examples of disinformation without having a clear audience in mind and a clear outcome to be achieved. The "about" page on the EU vs Disinfo website does not provide any such insights, surprisingly.

Without wishing to question the choice, we note that the site is only about Russian disinformation, but no effort is made to explain why this is the case and why other cases of potential (or actual) interference are not included. To see the broader human cost of misleading news (and, therefore, argue against this narrow approach), it is worth reflecting on the limited good research in this field. The PIPA/Knowledge Networks poll on "Misperceptions, the Media and the Iraq War" raises broader questions about the human cost of disinformation that would need to be considered if "false, inaccurate, misleading information designed, presented or promoted to intentionally cause public harm or for profit" is to be addressed in a meaningful way.[13]

Similarly, while the HLEG Report correctly says that, in theory, parody should not be impacted by measures against disinformation, three Dutch publications (Geenstijl, TPO and De Gerlander) needed to go to court in order to be delisted from the EU vs Disinfo website,[14] leading to a majority vote of the second chamber of the Dutch parliament calling for the EU vs Disinfo website to be shut down.[15]

The methodology used by the EU vs Disinfo website is also very chaotic. In some cases, stories are reported as being "disinformation" on the simple basis that evidence was not provided for a story that falls within some form of pattern identified by the site and sometimes the disinformation identified falls entirely outside the scope of the European Commission's definition of disinformation.

The undersigned organisations recommend to reconsider the EU vs Disinfo project, thoroughly analyse its impact and cost, to address inconsistencies and undesired consequences, such as listing erroneous publications.

Chapter 2.4 Limiting Anonymity

As UN Special Rapporteur on Freedom of Expression David Kaye has found in his report on encryption, anonymity, and the human rights framework that "[e]ncryption and anonymity, separately or together, create a zone of privacy to protect opinion and belief." He also found that "encryption and anonymity provide individuals and groups with a zone of privacy online to hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attacks."[16]

Despite the importance of anonymity for the exercise of fundamental rights online, various national[17] and EU-level[18] organisations have presented it as part of the disinformation problem.

The right to privacy and freedom of expression include the right to anonymity, since the loss of anonymity and pseudonymity in online spaces has a chilling effect on freedom of expression and undermines privacy. Encryption and anonymity are protected because of the critical role they can play in securing those rights. The right to anonymous and pseudonymous expression is a historically protected right in international and domestic laws and norms. The harms and dangers of limiting anonymity have been extensively detailed in analysis of Facebook's "real name" policy.[19]

Laws and policies allowing anonymity and pseudonymity online are not only essential components of fundamental rights but also enable innovation and economic growth for web content and service providers. [20] Allowing pseudonyms increases the quantity and quality of user posts online.[21]

Undermining or putting online anonymity at risk, in the hope of countering disinformation will restrict freedom of expression, while not reducing inflammatory or offensive speech, nor increasing diversity of opinions.[22] Furthermore, it is not demonstrated how these would contribute to the fight against disinformation.

The European Commission's Communication on "Tackling online disinformation: a European approach" sets "a more transparent, trustworthy and accountable online ecosystem" as a goal, and it explains that "[t]he 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."[23] As we explain in Section 3 of this report on meaningful solutions, we couldn't agree more with this issue. The Communication, however, proposes policies to foster what is referred to as "online accountability" that would put the responsibility for the creation of such ecosystem on users. "Suppliers of information" could easily be individuals who should be protected by anonymity and not be subject to "voluntary" online identification system. Similarly, "more responsible behaviour online" could lead to self-censorship.

The undersigned organisations strongly believe that measures to foster online accountability must not undermine privacy and freedom of expression and must respect the right to anonymity and pseudonymity. Any such measures must not result in mandatory identification policies and must not conflate the issues of user anonymity and the attribution of cyber attacks.

Section 3: Meaningful solutions

Chapter 3.1 Addressing the online manipulation business model

As the European Data Protection Supervisor (EDPS) stated, fostering online accountability has "focused on transparency measures, exposing the source of information while neglecting the accountability of players in the ecosystem who profit from harmful behaviour."[24] When discussing harmful behaviour that promotes disinformation, it is of paramount importance to separate the issues of the role of online platforms and economic interests behind the spreading of dis/misinformation from state-led "hybrid threats" such as cyber attacks and disinformation campaigns. When it comes to the economic aspect associated with online platforms, the EDPS rightly points out that "fake news is a symptom of concentrated, unaccountable digital markets, constant tracking and reckless handling of personal data".

Certain contemporary political campaigns have been successful in spite of an easily demonstrable lack of respect for basic facts. This phenomenon has been aided in part by the use of social media, specifically platforms that profit on the collection and analysis of user data. Such data processing operations are based on naturally promoting spreadable media and disregarding the veracity of the content – the more sensational the "news", the more attention is grabbed, the more profiling data is generated and it is such profiling data that generates profits for the platform.

Companies such as Facebook employ micro-targeting/surveillance advertising by using user data as the basis for decisions about the advertisements that users see in their news feeds, based on what will likely appeal to them and they will subsequently engage with and click on. This type of data manipulation reinforces the need for the ePrivacy regulation to enter into force as soon as possible as a means of changing the balance of incentives for companies away from a model that relies on sensationalism and shock. This needs to change to ensure that the right to privacy in the electronic communications sector is prioritised ahead of current unsustainable approaches. The New York Times investigated one of the widely known disinformation stories of the 2015 US Presidential Election and found it to be motivated by advertising revenue, that was successfully generated by Google.[25]

It is not appropriate to encourage platforms to adopt mechanisms of removal or verification (such as flagging and 'disputed tags'), if the fundamental business model of the platform itself facilitates or propagates the problem.

The undersigned organisations recommend firmly observing data protection and privacy legislation to reconfigure the priorities of online companies would serve as a major tool in the fight against disinformation.

Chapter 3.2: Preventing the misuse of personal data in elections

The undersigned organisations welcome the acknowledgement of the Commission[26] that unlawful use of personal data can result in serious impediments to the democratic process and elections, as shown by recent events. The Cambridge Analytica[27] and Facebook[28] scandals show that opaque processing operations of citizens' data have been used to micro-target citizens with political advertising, and potentially even targeted disinformation.

Even though these cases of abuse of personal data are drastic examples for the disasters that surveillance-based business models can cause, it is important that the response to these problems does not consist of ill-tailored solutions that aggravate the situation for citizens' fundamental rights. Through the GDPR, the EU offers some guarantees for the processing of personal data in the course of electoral activities. It is now time to enforce these rules and to ensure that any entity that engages in unlawful targeting of citizens is duly sanctioned.

The Commission explicitly acknowledges the role of the GDPR and the ePrivacy Directive in the context of elections and disinformation,[29] and has accordingly issued guidelines on the application of the GDPR in electoral processes. Additionally, it has presented a set of initiatives with the aim of securing free and fair European elections. Apart from the *ad-hoc* approach of the self-regulatory Code of Practice on Disinformation agreed by a handful of companies such as Google, Facebook and Mozilla, these measures overall provide a good complement to the EU's existing data protection regime.

These measures will be complemented further by a legislative amendment to tighten the rules on European political party funding with regard to the abuse of personal data. Sanctions would amount to 5% of the annual budget of the European political party.

If illegal collection and access to citizens' data is stopped, micro-targeted disinformation campaigns would lose much of their alleged effectiveness and threat potential. As is already clear, weak data protection rules and enforcement not only impact user privacy and choice, but also leads to constant monitoring, profiling and 'nudging' towards political and economic decisions.

In the context of elections, the undersigned organisations recommend that transparency and limitation of behavioural advertising for political purposes, as well as the capacity to impose sanctions for using illegally acquired data in electoral processes should be strengthened in national legal frameworks.

Chapter 3.3: Media and information literacy

Media and information literacy is very important for people to better understand the news industry, other relevant actors and how online disinformation works. It is also a tool that strengthens critical attitudes towards different sources of news. Media and information literacy is a useful tool to address the problem of online disinformation. It has a significant role in teaching people to critically analyse certain information.

As the Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda correctly points out, "[s]tates should take measures to promote media and digital literacy, including by covering these topics as part of the regular school curriculum and by engaging with civil society and other stakeholders to raise awareness about these issues."

The HLEG Report stresses the importance of media and information literacy, because it enables people to identify disinformation. The undersigned organisations agree with the view that "[t]here is a need to think more strategically about how media literacy is implemented across Europe". Effective media and information literacy programs have to part of national public education curricula.

The HLEG Report clearly states that "media literacy cannot […] be limited to young people but needs to encompass adults as well as teachers and media professionals" in order to help them keep pace with digital technologies. The undersigned organisations support this idea. We underline the importance of the independent public service media, which should be involved in media literacy projects along with civil society.

The undersigned organisations support the idea of better media education, but it has to be handled appropriately. It will not solve the problem of distrust in the news media, nor will it stop populist politicians from branding as "fake news" any story or news outlet that they disagree with. However, it seems to have more consensus as a reasonable solution to the problems identified.

Conclusion

The spreading of online disinformation and propaganda in Europe, and in particular in social media, has been in the forefront of policy debates for a few years, due to the political pressure to take measures, particularly following the 2016 US elections and the Brexit campaign.

We recognise that the spreading of online disinformation can interfere with the right to freedom of expression, the right of individuals to seek and receive, as well as to impart information and ideas of all kinds, regardless of frontiers; it can harm individual reputations and privacy, personal data protection, or incite to violence, discrimination or hostility against identifiable groups or individuals in society.

While addressing this issue, however, the EU and Member States must refrain from undue interference and censorship. Member States are also under a positive obligation to foster an enabling environment for fundamental rights, such as freedom of expression, which includes promoting, protecting and supporting diverse media both online and offline.

Therefore, we urge the European Commission and all other state and non-state actors engaged in this debate to consider solutions that are based on evidence both in terms of the problem definition and the efficiency of measures to be put in place, and that meet their respective obligation and responsibilities under international human rights law. The undersigned organisations urge the Commission to start evaluating the European media landscape, and media ownership related to the notion of online disinformation before any further measures are taken. A EU-level open database, which is accessible to the general public in a reusable and open format would support transparency and help the work against online disinformation.

We believe that all measures to tackle the spreading of disinformation online:

- must be in line with international human rights obligations to respect and promote the right to freedom of expression, opinion and information, the right to privacy and personal data protection, the right to non-discrimination, and other relevant rights;

- must be subject to continuous assessment and independent research;

- must be based on evidence and adequate benchmarking criteria;

- must not create institutionalised fact-checking mechanisms that might reinforce or lead to conflicts of interest, abuse of power or bias;

- must not lead to the manipulation of the electorate or to silencing minority voices;

- must address the business model of online manipulation through appropriate data protection, privacy and competition laws;

- must not undermine anonymity online;

- must not be blindly reliant on automated means, artificial intelligence or similar emerging technologies without ensuring that the design, development and deployment of such technologies are individual centric and respect human rights;

- must ensure that media literacy programs are implemented at national level, be part of the national education curriculum, also targeted at the adult (especially elderly) population, and examines the roles and responsibilities in Public Service Broadcasting; and

- must evaluate existing initiatives such as the East STRATCOM Task Force.

The undersigned organisations look forward to any upcoming opportunities to further discussing our recommendations to ensure a pluralistic, democratic, and fundamental rights respecting digital ecosystem. In particular, we hope that the EU follows these recommendations prior and after the adoption of its forthcoming EU Action Plan.

Notes

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

2 https://euvsdisinfo.eu/removal-of-three-cases-further-to-complaints-by-dutch-media/

3 https://www.ohchr.org/Documents/Issues/Expression/JointDeclaration3March2017.doc (Microsoft Word document)

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

5 https://blogs.ec.europa.eu/ECintheUK/euromyths-a-z-index/

6 See, for example, https://ec.europa.eu/information_society/newsroom/image/document/2016-50/factsheet-code-conduct-8_40573.pdf

7 https://www.article19.org/resources/free-speech-concerns-amid-fake-news-fad/

8 https://ifcncodeofprinciples.poynter.org/

9 There is no widely accepted definition of Artificial Intelligence (AI). Here AI refers to the theory and development of computer systems that can act without explicit human instruction and can self-modify as necessary. AI is used broadly to refer to a wide range of technological approaches that encompass everything from knowledge-based systems throuh so-called machine learning to the development of autonomous, connected objects to the futuristic concept of "the Singularity."

10 Raso, Hilligoss, Krishnamurthy, Bavitz, Kim, Artificial Intelligence & Human Rights: Opportunities & Risks, Berkman Klein Center for Internet & Society at Harvard University, 25 September 2018, https://cyber.harvard.edu/sites/default/files/2018-09/2018-09_AIHumanRightsSmall.pdf

11 https://www.accessnow.org/cms/assets/uploads/2018/08/The-Toronto-Declaration_ENG_08-2018.pdf

12 Website: https://euvsdisinfo.eu/

13 https://web.stanford.edu/class/comm1a/readings/kull-misperceptions.pdf

14 https://euvsdisinfo.eu/removal-of-three-cases-further-to-complaints-by-dutch-media/

15 https://www.volkskrant.nl/nieuws-achtergrond/kamer-lijnrecht-tegenover-kabinet-ollongren-moet-zich-hard-maken-voor-opheffen-europese-nepnieuws-waakhond~b0d3eed1/

16 https://www.ohchr.org/EN/HRbodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc (Word document)

17 https://www.politico.eu/article/social-media-anonymous-online-uk-digital-minister-considering-measures-restrict/

18 https://www.socialistsanddemocrats.eu/newsroom/commission-must-do-more-tackle-spread-fake-news

19 See, for example, https://qz.com/267375/facebooks-real-name-policy-isnt-just-discriminatory-its-dangerous/

20 Examples such as Twitter, Reddit, and Weibo demonstrate that some of the most popular sites and services on the internet today have allowed users to conceal their identities. For instance, researchers found a dramatic drop in the number of monthly Weibo posts beginning in March 2012, when the government mandated a real-name policy and restricted rumors of a government coup, forcing the platform to shut down comments for three days. https://www.telegraph.co.uk/news/worldnews/asia/china/10608245/China-kills-off-discussion-on-Weibo-after-internet-crackdown.html

21 Disqus is a company that offers a commenting platform for millions of blogs and websites, and is seen by one billion monthly visitors in more than 40 languages. Based on its research, commenters using pseudonyms, or fictitious names, post 6.5 times more than anonymous commenters, and 4.7 times more than commenters using Facebook to login. According to the company, "the most important contributors online are those using pseudonyms," which are "nearly essential because they allow people to be expressive, and appropriately so." See Disqus. Research: Pseudonyms, at http://disqus.com/research/pseudonyms

22 TechCrunch. Surprisingly Good Evidence That Real Name Policies Fail To Improve Comments. Accessed 28 May 2014, http://techcrunch.com/2012/07/29/surprisingly-goodevidence-that-real-name-policies-fail-to-improve-comments

23 Communication on "Tackling online disinformation: a European approach" (26 April 2018), https://ec.europa.eu/digital-single-market/en/news/communication-tackling-online-disinformation-european-approach.

24 https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=uriserv:OJ.C_.2018.233.01.0008.01.ENG

25 https://www.nytimes.com/2017/01/18/us/fake-news-hillary-clinton-cameron-harris.html

26 http://europa.eu/rapid/press-release_IP-18-5681_en.htm

27 https://www.theguardian.com/news/series/cambridge-analytica-files

28 https://www.nytimes.com/2018/08/16/technology/facebook-microtargeting-advertising.html

29 https://www.euractiv.com/section/digital/interview/gabriel-facebook-users-need-to-know-what-happened-with-their-data/

Website:
accessnow.org
edri.org
liberties.eu

Contact info:
Access Now: info@accessnow.org
EDRi: brussels@edri.org
Liberties: info@liberties.eu

Access Now
12 Rue Belliard
1040 Bruxelles
Belgium

Civil Liberties Union for Europe e. V.
Prinzenstr. 103.
10969 Berlin
Germany

EDRi
12 Rue Belliard
1040 Bruxelles
Belgium