DEMOCRACY
REPORTING
INTERNATIONAL

REPORT

A EUROPE FIT FOR THE DIGITAL AGE

A CIVIL SOCIETY DISCUSSION ON THE REGULATION OF ONLINE PLATFORMS IN THE EU

A EUROPE FIT FOR THE DIGITAL AGE

A CIVIL SOCIETY DISCUSSION ON THE REGULATION OF ONLINE PLATFORMS IN THE EU

CONTENTS

ACKNOWLEDGEMENTS 5

1. WHERE DOES THE EU STAND ON THE REGULATION OF TECH PLATFORMS ? 6

2. POLICY RECOMMENDATIONS 6

2.1 Principles to guide EU Regulation 6
2.2 Topic-specific recommendations 8
2.2.1 Transparency and accountability 8
2.2.2 Illegal content 9
2.2.3 Disinformation 9
2.2.4 Online political finance 11

ANNEX 1: THE DIGITAL SERVICES ACT AND THE EUROPEAN DEMOCRACY ACTION PLAN 13

Plans so far 13
Actors 13

A CIVIL SOCIETY DISCUSSION ON THE REGULATION OF ONLINE PLATFORMS IN THE EU

ACKNOWLEDGEMENTS

This report provides an overview of civil society discussions in a two-day online roundtable event (31 March – 1 April 2020) dealing with the regulatory plans of the European Commission on tech companies to address challenges posed by online platforms to public/democratic discourse. Regulatory responses to disinformation, illegal and harmful content, online political finance, and transparency and accountability, along with other overarching issues that should be part of the EU regulatory plans were discussed. The discussions were led by:

- Stiftung Neue Verantwortung (SNV)
- AlgorithmWatch
- The Portuguese University ISCTE-IUL MediaLab
- Democracy Reporting International (DRI)

We are grateful to these organisations and the other organisations who shared their views and comments on this paper. These include Access Now, Avaaz, Civil Liberties Union for Europe, Civitates, Election Observation and Democracy Support, EU DisinfoLab, European Digital Rights, European Partnership for Democracy, German Marshall Fund, Institute for Strategic Dialogue, Open Society European Policy Institute, Panoptykon, and Tactical Tech.[1]

We also thank Prabhat Agarwal (Directorate-General for Communications Networks, Content and Technology), Marie-Hélène Boulanger (Directorate-General for Justice and Consumers), Felix Kartte (European External Action Service), Meg Chang and Ania Helseth from Facebook for briefing the participants on their plans and ideas, as well as Benoît Loutrel, from the Institut national de la statistique et des études économiques (INSEE), who spoke in his personal capacity. This report is part of a project funded by the German Foreign Ministry.

[1] The organisations were selected for their expertise and work on the challenges that the EU regulation aims at addressing. This paper does not necessarily reflect the opinion of each participant and it is not a reflection of their institutional positions. We have tried as much as possible to refer to their publications and resources in the discussions presented below.

1. WHERE DOES THE EU STAND ON THE REGULATION OF TECH PLATFORMS ?

The purposes and types of digital services providers have changed drastically since the adoption of the 2000 e-Commerce Directive. Over the past 20 years, the use of digital technologies has changed how we travel, commute, plan holidays, discuss politics and consume information. Beyond that, the increase in the number of users has resulted not only in the exponential increase of content generated on these platforms, including harmful and illegal content, but also has generated a whole new dimension for how content is amplified: now, content spreads much faster and algorithms are not calibrated to balance the risks different types of content can pose to users.

Member states have adopted their own regulations to address these rising challenges, risking regulatory fragmentation across the EU against a Single Market cohesive approach. With the e-Commerce Directive outdated for dealing with these challenges, the European approach has been mostly to self-regulate through codes of conduct and codes of practice. Building on that experience, the European Commission's communication Shaping Europe's Digital Future[2] outlines two parallel tracks. Firstly, the Digital Services Act (DSA) aims at harmonising standards to ensure smooth digital operations across the common market, possibly including common rules on illegal content. Secondly, the European Democracy Action Plan (EDAP) will focus on democratic resilience.

The EU's regulatory objectives are articulated in the new Commission President's political guidelines, My Agenda for Europe, and the follow-up communication on Shaping Europe's Digital Future. While originally indicating that draft proposals for regulations are to be expected by the end of 2020, the covid-19 crisis has pushed the timeline to the first quarter of 2021, with public consultations being held before that. The DSA and EDAP will likely run in parallel and are designed to be mutually reinforcing.

Draft proposals for regulations are expected in the last quarter of 2020, and public consultations on the DSA were launched by the European Commission on 2 June, to last until 8 September 2020. The aim of this document, therefore, is to provide feedback and input on topics and areas that should be part of the EU set of tools to approach these challenges, be they in the form of regulatory, mechanisms, financial incentives or through coordination of existing initiatives.

[2] "Shaping Europe's Digital Future", Communication by the European Commission, Brussels, February 2020, https://ec.europa.eu/info/sites/info/files/communication-shaping-europesdigital-future-feb2020_en_3.pdf

2. POLICY RECOMMENDATIONS

Action Plans, such as the proposed EDAP, are made up of concrete proposals for **Better Regulation**, **Better Funding** and **Better Knowledge.**[3] These proposals can be regarded as non-binding contributions to the design of future and the revision of existing EU legislation, instruments and initiatives. An Act, on the other hand, may be comprised of **binding legal instruments** (regulations, directives and decisions), **non-binding instruments** (resolutions, opinions, communications) or **other instruments** (EU institutions' internal regulations, EU action programmes, etc.).

At the online roundtable we discussed four policy areas to be covered under the EU legal instruments: disinformation, online political finance, illegal and harmful content, and transparency and accountability. We considered the whole spectrum of policy instruments above to present principles and recommendations that the EU should follow.

2.1 PRINCIPLES TO GUIDE EU REGULATION

A number of issues are relevant for EU policy-making and regulation across the board.

1. **Statement to recognise relevance of online public sphere:**

The EU has issued numerous acts of regulation, policies and codes of conduct on issues related to governing the internet and the digital sphere. Somewhat missing is an overall statement on the relevance of the online public sphere that could be replicated across various legal acts and documents. The e-Commerce directive only mentions democracy in passing (recital 63), but by now it has become clear that the online public sphere, which is dominated by commercial companies, has become an essential part of the overall public sphere of our democracies. Beyond that, information shared widely online has the potential to trigger offline events. Across the world we have examples of online false information and hate speech triggering offline violence, violation of rights and injustices.

In view of this, it is desirable to anchor a general statement of the EU's approach across EU documents including in legal acts like the DSA and the EDAP. It should highlight that the EU does not see the online democratic space as a purely commercial marketplace. We propose this language to be included:

"A big part of public debate has moved to the online sphere. It is essential for a functioning democracy, the protection of human rights — in particular by ensuring freedom of speech,

[3] "What is an Action Plan?", European Commission, October 2019, https://ec.europa.eu/futurium/en/action-plans/what-action-plan

diversity of opinion and media pluralism — and a public order based on the rule of law, the key values of Article 2 EU Treaty. The EU strives to provide a regulatory framework that respects these values and that gives society significant control over the functioning of online debates."

Such a statement is not innovative; similar sentiments are expressed in other EU documents. It would echo for example the language of the Audio-Visual Media Service Directive (recital 5), which states that *"Audiovisual media services are as much cultural services as they are economic services. Their growing importance for societies, democracy — in particular by ensuring freedom of information, diversity of opinion and media pluralism — education and culture justifies the application of specific rules to these services."*

2. Equality of member states:

Another principle that should be better anchored in regulation is the principle of equality of EU member states regardless of their size. The large companies tend to give significantly more attention to bigger member states, which represent bigger markets. EU regulation should ensure that companies of a certain size are accountable in each EU member states in comparable ways. For example, the elections to the European Parliament in 2019 led to the Code of Practice on Disinformation, which made Google, Twitter and Facebook enhance ad transparency across EU member states, providing tools such as the Ad Library/Ad Transparency Centre/Transparency Reports. However, these tools were of differing quality in each member state and they were weaker across the EU than those the platforms had provided for elections in the US. Overall, they did not provide easy-to-access and comprehensive data and metrics,[4] standardised across countries and platforms, to enable comparative research for greater accountability. On the side of reporting on transparency, the assessment of the EU Code of Practice[5] noted that the reports from tech companies lacked uniformity, making it difficult to assess whether members states had been treated equally when it came to the monitoring efforts ahead of the 2019 European Parliamentary Elections. At a minimum, the standards should be the same across all member states, and with metrics that allow for comparability. These cases are examples of why relying on industry self-regulation may not be enough to achieve the desired goals.

3. The question of liability for content:

the e-Commerce Directive exempts intermediaries from liability for the content they manage if they fulfil certain conditions, with some exceptions (like illegal content). When services play a neutral, merely technical and passive role towards the content they host, they are covered by the liability exemption.[6] Article 12 states that *"…the service provider is not liable for the information transmitted, on condition that the provider (a) does not initiate the transmission; (b) does not select the receiver of the transmission; and (c) does not select or modify the information contained in the transmission."*

This clause is no longer adequate to addresses current realities, as it focuses mainly on the *message*[7] or, in the language of the e-Commerce Directive "information". This is most clearly articulated in recital 43: "A service provider can benefit from the exemptions for 'mere conduit' and for 'caching' when he is in no way involved with the information transmitted; this requires among other things that he does not modify the information that he transmits; this requirement does not cover manipulations of a technical nature which take place in the course of the transmission as they do not alter the integrity of the information contained in the transmission." If an intermediary does not control the information it passes on or stores (the *message*), it is not considered to be actively involved. However, in the realm of social media, the focus of many intermediaries – Facebook being the prime example – is related to the *messaging*, i.e. the distribution of messages/information on platforms. These companies essentially **select** what viewers see (be it by ranking posts, by recommending related content or by displaying search results). In this realm they are highly active operators, curating the pieces of content that a viewer sees, even if not changing their content. The business model is based on curation, mostly to identify content – often sensational rather than authoritative – to keep viewers as long as possible on the platform so as to increase the time they can be exposed to paid advertising.[8]

As the curation role is essential to what the viewers see, it is not appropriate to consider such services as passive. At the same time, they cannot be viewed as media services either, as they do not create content. In the case of Facebook, CEO Mark Zuckerberg has taken the following position: "Right now there are two frameworks that I think people have for existing industries. There's like newspapers and existing media, and then there's the telco-type model, which is 'the data just flows through you'. But you're not going to hold a telco responsible

[4] "Facebook and Google: This is What an Effective Ad Archive API Looks Like", Mozilla, March 2019, https://blog.mozilla.org/blog/2019/03/27/facebook-and-google-this-is-what-an-effective-ad-archive-api-looks-like/

[5] Plasilova *et al.*, "Study for the assessment of the implementation of the Code of Practice on Disinformation", commissioned by the European Commission, May 2020, https://ec.europa.eu/digital-single-market/en/news/study-assessment-implementation-code-practice-disinformation

[6] *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')*, https://ec.europa.eu/digital-single-market/en/e-commerce-directive

[7] See DRI's 3 M model (message, messaging/distribution, messenger): https://democracy-reporting.org/bp100-online-threats-to-democratic-debate/

[8] For this reason, it also seems misplaced to focus mostly on questions of freedom of expression, as the e-Commerce directive does when mentioning human rights. The curating of messages that viewers see does not involve deletion of messages. It involves ranking them. While de facto a very low ranking may have the same effect as deletion, it is not the same.

if someone says something harmful on a phone line. I actually think where we should be is somewhere in between."[9]

This seems to be the right approach. Social media companies cannot be compared to a telecommunications operator (which does not choose which calls a customer receives with priority), but it is not a full-fledged media company either.

This leaves two possibilities:

- Either companies with this kind of business model reset their approach and offer content purely on a chronological basis (as a messaging service or a phone company would do), in which case the limitation of liability would still make sense, or

- A new category needs to be created in which such companies are not liable for content (as with media) but they are liable for curating content (messaging) and for ensuring the authenticity of users (messenger) – in whichever form. What such a liability might entail in detail would need further discussion.

4. Monitoring obligation:

Article 15 of the ECD exempts intermediaries from general obligations to monitor information they transmit, but states that member states may establish obligations for providers to inform the competent public authorities of alleged illegal activities undertaken, at their request. This prohibition refers solely to monitoring of a general nature.[10] Using voluntary mechanisms present in the e-Commerce Directive , the EU Commission agreed with Facebook, Microsoft, Twitter, Google and Mozilla two voluntary codes on content monitoring: the Code of Conduct on Countering Illegal Hate Speech Online in May 2016, and the Code of Practice on Disinformation in October 2018. While companies should not be responsible for performing general monitoring, they should have a more defined responsibility in detecting actors abusing such platforms to spread problematic content widely, or specific responsibilities during key moments such as elections or states of emergency. Specific transparency and reporting obligations could ensure that they take actions combating violations of their terms of service equally across member states.

5. The role of a regulator:

Fragmentation of regulations between countries is to be avoided; here the problem is not one of lack of authorities or actors. Rather, monitoring, enforcement and cooperation of authorities at the national level should not only be assessed, but constantly monitored to ensure that the principles of transparency and equality of member states are respected. The Code of Practice on Disinformation showed that self-regulation without independent information-gathering powers is not sufficient. Oversight can serve as an external accountability mechanism, to ensure these principles are respected, or go beyond, defining audit processes and a regulatory power that sanction such companies if they fail to comply with the requirements established under the DSA. The European Parliament's Committee on the Internal Market and Consumer Protection (IMCO) recommended that a central regulatory authority, working closely with the national enforcement bodies, should be established with the responsibility to ensure oversight and compliance with the DSA, with powers to tackle cross-border issues as well as investigation and enforcement powers[11].

2.2 TOPIC-SPECIFIC RECOMMENDATIONS

2.2.1 Transparency and accountability

The EU has nudged tech companies to become more transparent through codes of practice and conduct which outline what information should be publicly available across all platforms, as well as which general transparency standards should be adopted. Voluntary monitoring proved a good first step in the general frameworks agreed with the EU[12] but was insufficient to fight hate speech/illegal content and disinformation and there is room to go further in this area.

The EU should regulate industry-wide transparency requirements. They could be monitored at EU-level to ensure all member states are treated equally, and to ascertain differences between social media abuse in different countries. Such obligations could be defined according to the market share of companies or similar metrics to avoid imposing excessive costs to smaller companies or market entrants.

Transparency requirements should have two elements: **benchmarks** to follow, and **verification mechanisms**.

[9] Fadilpašić, "Facebook 'should face less scrutiny than media organisations'", February 2020, https://www.itproportal.com/news/facebook-should-face-less-scrutiny-than-media-organisations/

[10] Kuczerawy, "To Monitor or Not to Monitor? The Uncertain Future of Article 15 of the E-Commerce Directive", July 2019, https://www.law.kuleuven.be/citip/blog/to-monitor-or-not-to-monitor-the-uncertain-future-of-article-15-of-the-e-commerce-directive/

[11] European Parliament's Committee on the Internal Market and Consumer Protection, "DRAFT REPORT with recommendations to the Commission on Digital Services Act: Improving the functioning of the Single Market (2020/2018(INL))", April 2020, https://www.europarl.europa.eu/doceo/document/IMCO-PR-648474_EN.pdf

[12] See the study for the assessment of the implementation of the Code of Practice on Disinformation (08.05.2020): https://ec.europa.eu/digital-single-market/en/news/study-assessment-implementation-code-practice-disinformation

Regarding **benchmarks**, the lessons learned from codes of practice and conduct should inform the definition of specific indicators to measure and perfect transparency standards. These should include data about the type of content that is restricted, blocked, or removed, as well as continuous information on how much content has been taken down, on what ground and within what timeframe, the number of appeals, their resolutions, etc. Such efforts should be reported on for the whole EU but also broken down by EU member state for comparability.

Verification mechanisms would include compliance requirements on regular reporting, as well as how the data is presented by the companies, and the involvement of third parties.[13] Such third-party verification would require that companies provide data access to third parties to strengthen external accountability. The European Data Protection Supervisor's preliminary opinion on data protection and scientific research[14] states that EU codes of conduct for scientific research could be used to push for access to data accounting for data-protection standards while addressing the needs of researchers. In addition to third-party verification, support/funding of data journalism would help to develop a specialised public that could scrutinise companies' reporting.

Third-party verification could be formalised as a system of formal auditing to verify compliance with the General Data Protection Regulation (GDPR) for member state regulators and the accuracy of companies' compliance reporting. Auditing processes could shed light on internal processes and decisions, which would better inform about what type of transparency would be desirable in these different fields.

2.2.2 Illegal content

Defining illegal content and mechanisms of enforcement is mostly a responsibility of EU member states. An EU-wide regulation would need to consider that some EU member states are not currently respecting the rule of law and democratic norms. An EU system could thus be abused to restrict freedom of speech under the guise of implementing EU laws. However, the EU can plan a role in defining a framework to govern such content to standardise rules across the Single Market.

Some issues currently covered in codes of conduct or mentioned in communications should be elevated to the level of binding regulation. The Commission's 2017 Communication on Illegal Content notes "…online platforms and law enforcement or other competent authorities should appoint effective **points of contact** in the EU, and where appropriate define effective digital interfaces to facilitate their interaction." This should be strengthened and become binding. "Effective" point of contact should mean: sufficient human resources, proficiency in the relevant language(s), a physical presence in that member state, and in-depth knowledge of the national market and context to facilitate discussions and issues arising between tech companies, member states and their publics.

To strengthen content governance, the EU can help establish a broader **notice and take down mechanism**. This should be a clear, transparent framework outlining the process and steps companies must take once notified of hosting allegedly illegal content on their platform. Such a system (a) should ensure transparency, so that users are aware of their content being subject to platform action and on what grounds, and that users are informed of any decisions made regarding their content; (b) should ensure that there is due process, recourse on content take-downs/action is possible in a fast and responsive, agile manner to reflect the speed of online ecosystem. Blocking and suspending content is preferable to deletion, as it ensures due process is meaningful, and can be reversed if the action is judged to be mistaken.

An **online dispute settlement system** should be considered for this, in line with the recommendations of the Committee on the Internal Market and Consumer Protection.[15] It should also consider the inclusion of expert civil society organisations that understand issues like hate speech, disinformation, and inauthentic and coordinated behaviour. Any regulation/system must build on the freedom of expression and transparency. A system could include an intermediary between users and platforms to ensure obligations in processing complaints are met, and/or a mechanism for users to track complaints, or decision records. Data and information about the complaint processing (e.g. decisions and actions taken concerning a complaint) could be recorded and published in anonymised ways.

2.2.3 Disinformation

Disaggregation of concepts around disinformation

In our discussion, there was no consensus on the merit of a changed definition of disinformation or of the wisdom of enshrining a definition in hard regulation. Nevertheless, some experts feel that the current definition[16] of the EU

[13] See "computational transparency/access" on https://www.isdglobal.org/isd-publications/extracts-from-isds-submitted-response-to-the-uk-government-online-harms-white-paper/

[14] European Data Protection Supervisor, "A Preliminary Opinion on data protection and scientific research", January 2020, https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf

[15] European Parliament's Committee on the Internal Market and Consumer Protection, "DRAFT REPORT with recommendations to the Commission on Digital Services Act: Improving the functioning of the Single Market (2020/2018(INL))", April 2020, https://www.europarl.europa.eu/doceo/document/IMCO-PR-648474_EN.pdf

[16] Stated in the Communication on tackling on-line disinformation, COM(2018) 236. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018DC0236&from=EN

unnecessarily stresses **intent to deceive the public**, considering that false information can be harmful even without intent of deception. For example, a good faith advice on false cures to covid-19 may end up being more harmful than other forms of intentional disinformation. Furthermore, a refined definition of disinformation should disaggregate better the three aspects of message, the messenger and messaging/distribution of messages.[17]

Specifically, analysis should establish that the *message* is misleading and can produce harm. Following this, it should be determined whether the *messaging* is of concern – has it gone viral or does it have the potential to do so? The *messenger*, or agent of disinformation is also relevant. Do they have a history of spreading disinformation? Is their authenticity in doubt? Is the same source of information using several accounts to promote the content?

Disinformation and elections

Disinformation also has a timing component. The mechanisms established under the code dealing with disinformation was subject to the context of the European Parliamentary elections, and therefore lacked tools to address the systemic role disinformation campaigns have in changing people's perceptions over time, and not only in the weeks prior to voting. False information influences users of different age groups on different platforms on which it is shared, affecting not only voter behaviour, but political beliefs and world views.[18]

While the focus should be expanded in dealing with the problem, the code and previous recommendations[19] of the commission offer a good starting point to deal with the issue during elections. The recognition of political parties and actors as actors of disinformation could lead to a legally binding code of conduct on disinformation and ways of disciplining party members at the European level, with non-binding guidelines for member states.[20] Lead candidates and party communication departments should have rules of engagement that clarify responsibilities for posting on social media. In addition, verification requirements for official party pages giving responsibility over content should be developed, for example where unverified pages cannot use the visual identity of a party.

Best practices such as the "correct the record" policy,[21] which requires platforms to inform users and push effective corrections to every person who saw information that independent fact checkers have determined to be disinformation, can be obligatory measures, if not always, at least around key moments such as elections. This policy has been adopted regarding misinformation related to covid-19 and has the potential to reach people who have interacted with false information.

Another example of a detailed anti-disinformation policy would be to require news articles to indicate clearly at the top in cases where they are not recent (as The Guardian now does as a matter of policy), in order to avoid misrepresentation of old news as current.

Shedding light on disinformation, making disinformation campaigns more expensive and increasing long-term resilience

Funding independent research on disinformation is key to providing external assessment of online platforms and political parties' commitments against disinformation. The current EU funding mechanism focuses more on the message (strengthening media literacy and supporting journalism and factchecking initiatives) and less on the origin and distribution of the content (research and investigations on how disinformation campaigns work). A more flexible funding mechanism[22] for investigations of disinformation campaigns, including open source investigations, could help create a solid ecosystem of civil society organisations and consequently raise awareness of disinformation campaigns to the public and institutions.

The identification of dynamics of disinformation, both by tech companies themselves and independent researchers, can help trace and identify service providers supporting the disinformation ecosystem and shed light on how this content is spread on different platforms. The ranking criteria of platforms when defining the "trustworthiness of sources", for example, should be made public and be legitimised by independent ranking systems, fact checkers, researchers and civil society organisations. Enforcing bans of fake accounts and unlabelled bots that are used as conduits for disinformation could be considered. Many platforms' guidelines and policies already include such bans, but they underperform on actively searching for fake accounts. They should do more, closing the loopholes that allow such accounts to multiply and reducing the incentives provided by

[17] See DRI's 3 M model (message, messaging/distribution, messenger): https://democracy-reporting.org/bp100-online-threats-to-democratic-debate/

[18] Democracy Reporting Interntional, "Briefing Paper 100: Online Threats to Democratic Debate: A Framework for a Discussion on Challenges and Responses", June 2019, https://democracyreporting.org/wp-content/uploads/2019/06/BP_Threats-to-digitaldemocracy.pdf

[19] European Commission Recommendation, "C(2018) 5949 final on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns in the context of elections to the European Parliament", Brussels, September 2018, https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-cybersecurity-elections-recommendation-5949_en.pdf

[20] Including the adoption of internal codes of conduct to disincentivize and penalize party members who actively participate in generating false or misleading information, and guidelines for the use of data for campaigning purposes.

[21] Avaaz, "White Paper: Correcting the Record", April 2020,https://secure.avaaz.org/campaign/en/correct_the_record_study/

[22] Beyond the support of projects, financial support should be extended to the physical and cybersecurity of organisations researching on disinformation to protect investigators, journalists and organisations working against disinformation from threats and harassment.

their own services that favour the existence of bots. Bots should be prominently and effectively labelled, and all content distributed by bots must include the label and retain the label when the content or message is shared, forwarded, or passed along in any other manner, so that it is immediately clear to any user that they are not interacting with a human being.

Strategies to make disinformation more expensive and difficult to manufacture and to successfully deploy include requiring platforms to: pro-actively identify and suppress manipulative practices such as selling likes, clicks and followers; establish processes to identify and easily display to researchers whether there is activity on coordinated sharing of links (how many times and by which pages a link is being shared); provide access to data for researchers on content that is taken down because it violated community standards; and oblige platforms to visibly include the date of publication of the domain on page previews, among others.

By strengthening projects that shed light on the dynamics of disinformation, civil society and investigative journalists can support tech companies to identify and monitor new trends in the disinformation field, helping to increase resilience against future attempts to interfere in the public debate.

2.2.4 Online political finance

Paid online political communication does not have clear guidelines and limits, presenting risks for open or pluralistic political debates, such as the ultra-segmentation of audiences to target political messages and the potential of distortion of the debate with the interference of big money in political discussions, without sufficient scrutiny and transparency about who is sponsoring messages and how much is spent on them.[23]
The EU could play a role in at least three aspects: definition of the issue, enforcement of cross-country transparency standards, and enforcement of data-protection requirements around election campaigns online.

There is no agreed definition between different tech companies about what does and what does not constitute political advertising, or over what other aspects of political/campaign financing (e.g. paid influencers) could be restricted, for example to only allow registered entities to pay for advertising of a political nature. The existing definitions of the main tech companies focus heavily on election ads, but many fail to acknowledge the role that advertising dealing with other issues of national importance may have outside of the electoral cycle (therefore influencing democratic debate).

Google defines Election Ads[24] as ads that feature a political party, a current elected officeholder, or candidate for the EU Parliament or within an EU member state, or that poses a referendum question up for vote, a referendum campaign group, or a call to vote related to a national referendum or a state or provincial referendum on sovereignty. Twitter prohibits the promotion of political content,[25] defining it as content that references a candidate, political party, elected or appointed government official, election, referendum, ballot measure, legislation, regulation, directive, or judicial outcome. It does not, however, mention whether it allows paid content dealing with social issues that could be used to polarise public opinion without necessarily referencing these concepts. Facebook has a broader concept, defining them as Ads About Social Issues, Elections or Politics[26] and acknowledging that social issues go beyond the traditional electoral angle, covering sensitive topics that are debated and may influence public opinion in other moments.

This multitude of definitions creates different standards when dealing with this type of content, and subjects them to the decisions of private companies. The development of a baseline definition should include different stakeholders (regulators, civil society activists, platform representatives) at the EU level, accounting for the different nuances that this issue may have in different member states, and serve as a base for more specific regulations that electoral bodies of member states may require. A common definition would also be helpful to set comparable transparency standards across different companies. Currently, ad libraries/ad transparency centres provide different levels of information that makes it difficult to compare the phenomena across countries and platforms.

EU regulation should include obligations on what information ad libraries should include.[27] Meaningful transparency includes ensuring an application programming interface (API)[28] regime for advertisement, fostering measures to give a comprehensive and comparable source of information to external observers.[29]

[23] A comprehensive contextualization of issues and regulatory suggestions on online political advertising by Stiftung Neue Verantwortung can be found here: https://www.stiftung-nv.de/en/publication/rules-fair-digital-campaigning.

[24] Google Support: Advertising Policies Help, accessed on June 2020, https://support.google.com/adspolicy/answer/6014595?hl=en#

[25] Business Twitter: Political content, accessed on June 2020, https://business.twitter.com/en/help/ads-policies/prohibited-content-policies/political-content.html

[26] Facebook for Business: Advertisements on social issues, elections, or politics, accessed on June 2020, https://www.facebook.com/business/help/1838453822893854

[27] A comprehensive discussion on the content of ad libraries can be found on Panoptykon's analysis on political ads used in different Polish elections: https://panoptykon.org/political-ads-report

[28] An application programming interface is a set of programming code that enables data transmission between one software product and another. It also contains the terms of this data exchange. For more, see: https://www.altexsoft.com/blog/engineering/what-is-api-definition-types-specifications-documentation/

[29] Ideas such as the Online Political Advertising Library (OPAL) should be encouraged, to provide not only a comparable perspective on advertising across platforms, but to empower civil society organizations to assess whether such

Regarding privacy and targeted advertising, the EU could provide greater clarification of how the GDPR applies to political advertising. This includes mandatory, expanded, easy-to-understand ad disclosures in user feeds and ad archives, platform transparency reporting on ad content policies, ad targeting policies, ad delivery policies and mandatory financial disclosures for EU-wide political campaigns. Effective oversight of such measures could be supported by strengthening data-protection authorities' capacities at the national level to implement the GDPR in their jurisdiction.

libraries are comprehensive, or if they fail to provide complete information of ads targeting users.

ANNEX 1: THE DIGITAL SERVICES ACT AND THE EUROPEAN DEMOCRACY ACTION PLAN

PLANS SO FAR

The DSA aims for a deepening of the Internal Market for Digital Services, by increasing and harmonising the responsibilities of online platforms and by bolstering the oversight over platforms' content policies. Aside from aiming to ensure uniform, fair and contestable markets for new entrants, this regulation package also intends to avoid confronting social media and other relevant companies with a fragmented legal environment, especially as some member states (most notably France and Germany) have adopted national legislation on illegal content and hate speech. In. In her agenda for Europe, President of the European Commission Ursula van der Leyen envisions the Union benefiting from opportunities offered by the digital technologies within "safe and ethical boundaries", high privacy, security, safety and ethical standards.[30] The DSA is part of this, as it "will up upgrade our liability and safety rules for digital platforms, services and products, and complete our Digital Single Market."[31]

In contrast to the Single Market logic of the DSA, the EDAP is framed within the context of defending European democracies, specifically from the manipulation of public opinion and disinformation campaigns aimed at undermining democratic institutions. It will focus on the need to protect the EU against foreign interference, and the large scale spread of disinformation and hate speech on digital platforms, especially around elections. The EDAP also calls for greater transparency of information, highlights the importance of trust in the media in the EU, and makes reference to another action plan specifically for the media and audio-visual sector.[32]

The two initiatives have different goals, but they need to be complementary. For example, the DSA will define an overall liability regime for tech firms, and this will impact the responsibility of companies under the topics regulated by the EDAP.

ACTORS

This dual-track approach extends into the highest level of the European Commission's hierarchy. Margarethe Vestager, one of two executive Vice-Presidents, will oversee a "Europe fit for

the Digital Age". The DSA will fall under her remit and that of internal market commissioner Thierry Breton, who reports to her. The Directorate-General for Communications Networks, Content and Technology (DG CONNECT) will have the leading role.

	Digital Services Act	European Democracy Action Plan
Leads	**Commissioner Margrethe Vestager** **(Vice-President)** A Europe fit for the Digital Age -Steering the DSA -Upgrading liability and safety rules for digital platforms, services and products -Ensuring working conditions of platform workers are properly addressed -Also addressing the European strategy on data (artificial intelligence (AI), ethical implications) **Commissioner Thierry Breton** -Leading on the Single Market for digital services, clarify obligations of online platforms, and give smaller businesses legal clarity and a level playing field -Also addressing European digital sovereignty (data, AI, 5G, space tech) -Reports to Vestager	**Commissioner Věra Jourová** **(Vice-President)** Values and Transparency -Steering the EDAP -Addressing external intervention in EU elections -Also driving transparency in paid political advertising, political campaign finance; supporting on countering disinformation, press and media freedom, Code of Practice **Commissioner Didier Reynders** -Leading on consumer empowerment and citizens' rights -Also ensures the full implementation and global promotion of the GDPR
Commission Services	**Directorate-General for Communications Networks, Content and Technology (DG CONNECT)** **Digital Single Market unit** Prabhat Agarwal **Media policy unit** Paolo Cesarini **Audio-visual Services** Anny Helmund	**Directorate-General for Justice and Consumers (DG JUST)** **Citizenship and Movement Unit** Marie-Hélène Boulanger
Other players		**Commissioner Josep Borrell** **(Foreign Policy High Representative,** **European External Action Service (EEAS))** Strategic Communications Division -Addresses disinformation, foreign interference and democracy support from abroad Democracy and Election Observation Unit -Observes online election manipulation

[30] Ursula von der Leyen, „A Union that Strives for More: My Agenda for Europe", European Commission, Brussels, 2019, https://ec.europa.eu/commission/sites/beta-political/files/politicalguidelines-next-commission_en.pdf

[31] Page 13, Ursula von der Leyen, „A Union that Strives for More: My Agenda for Europe", European Commission, Brussels, 2019, https://ec.europa.eu/commission/sites/beta-political/files/politicalguidelines-next-commission_en.pdf

[32] See page 11, "Shaping Europe's Digital Future", Communication by the European Commission, Brussels, Feburary 2020, https://ec.europa.eu/info/sites/info/files/communication-shaping-europesdigital-future-feb2020_en_3.pdf

The EDAP will be managed by the other Vice President, Věra Jourová, responsible for Values and Transparency. In turn, she will be supported by Commissioner Didier Reynders who heads DG Justice and Consumers (DG JUST), who will lead on the Democracy Action Plan.

The Foreign Policy High Representative Josep Borrell will also be consulted, especially on the EDAP, given the work on disinformation done by the European External Action Service (EEAS). Its Strategic Communications Division addresses disinformation from abroad and its Democracy and Election Observation Division addresses the issue as well, in particular as part of EU Election Observation Missions that now also analyse social media debates before elections and thus add to the growing body of evidence on disinformation and online discourse.

Democracy Reporting International is an independent, non-partisan and not-for-profit organisation which operates on the conviction that democratic, participatory governance is a human right and that governments need to be accountable to their citizens.

Through careful assessment of the institutional aspects of the democratic process such as elections, the role of parliaments and constitutional arrangements *Democracy Reporting International* seeks to provide citizens, legislators, the media, and the international community with specialist analysis. *Democracy Reporting International* also offers policy advice and recommendations on how improvements can be made in line with international standards and engages political actors to advocate for these reforms.

Democracy Reporting International

Prinzessinnenstraße 30
10969 Berlin / Germany
T / +49 30 27 87 73 00
F / +49 30 27 87 73 00-10
info@democracy-reporting.org
www.democracy-reporting.org

Democracy Reporting International