Tackling Disinformation: EU Regulation of the Digital Space

Flavia Durach, Alina Bârgăoanu, Cătălina Nastasiu[1]

Abstract: This paper[2] provides an overview of current responses to fake news and digital disinformation inside and outside the EU, and assesses the advantages and disadvantages of each solution. Four approaches emerge: (1) self-regulation (i.e. actions undertaken on a voluntary basis by the digital platforms); (2) co-regulation (i.e. cooperation framework between EU-level and national-level authorities, the internet platform companies, media organizations, researchers, and other stakeholders); (3) direct regulation (i.e. legal measures & sanctions); and (4) audience-centred solutions (i.e. fact-checking and media literacy). We argue in favour of the co-regulation approach, while drawing attention to some current challenges in the response against disinformation. Furthermore, we need to go beyond the understanding of disinformation as an information/truth fraud, and draw additional measures to reflect the particular understanding of disinformation as a form of users' engagement fraud.

Keywords: online disinformation, fake news, regulation of disinformation

1. Shortcomings of public conversation on contemporary disinformation

In recent years, the issues surrounding the spread of disinformation in the online environment have been acknowledged and confirmed across the globe on several peak occasions, such as several electoral campaigns, Brexit, the independence referendum in Catalonia, and latest, the COVID-19 pandemic. Its consequences, as documented in the literature, include: negative effects on political attitudes[3],[4],[5], distrust

---

[3] M. Balmas, 'When fake news becomes real: Combined exposure to multiple news sources and political attitudes of inefficacy, alienation, and cynicism', *Communication Research*, vol. 41, no. 3, 2014, pp. 430-454.
[4] P.R. Brewer, D.G Young and M. Morreale, 'The impact of real news about "fake news": Intertextual processes and political satire', *International Journal of Public Opinion Research*, vol. 25, no 3, 2013, pp. 323-343.
[5] J. Littau and D.R.C. Stewart, "Truthiness" and second-level agenda setting: Satire news and its influence on perceptions of television news credibility. *Electronic News*, vol. 9, no. 2, 2015, pp. 122-136.

in media[6], and polarisation of opinion within online echochambers[7],[8].

As stated elsewhere[9], we advocate for understanding this new phenomenon from a broader perspective than the buzz word "fake news" would suggest. This latter term is seen as "inadequate, imprecise and misleading"[10], and the phenomenon requires a more inclusive and complex approach. For the purposes of this study, we adhere to the understanding of disinformation as "all forms of false, inaccurate, or misleading information" that was created to "intentionally cause public harm or for profit"[11].

There are some shortcomings of the public conversation about fake news/ disinformation in the EU (and elsewhere). These shortcomings influence the way disinformation is defined and understood, and act as barriers in designing countermeasures for fighting digital disinformation. Firstly, the focus is on ad hoc/ stand-alone disinformation instances (e.g. Russia's disinformation campaigns) or contexts (e.g. elections) at the expense of identifying big trends, especially related to the digital behaviour and the automated simulation of engagement. Secondly, too much responsibility is placed on journalism/mainstream media, and educating the public to recognize disinformation, whereas the locus of the current disinformation disorder is in functioning of the new digital ecosystem (which is platform, algorithm, big-data driven and, increasingly reliant on machine learning and Artificial Intelligence).

When defining disinformation, the current focus is on the actual content and its truth value, and consequentially, on specific countermeasures (i.e. fact-checking, debunking, coming up with counter-narratives), whereas digital disinformation relies on emotions and visual discourse, disseminated and, most importantly, amplified in the new digital ecosystem whose features we have previously underlined.

The Internet and social media allow disinformation campaigns to be created immediately and through automated accounts, fake profiles, bots or "army of trolls" shared over digital platforms, while having the advantages of low cost, rapid spread and high impact[12]. All of these actions and actors form an artificially inflated engagement (based on likes, comments, shares), that leads to the necessity to identify and combat the disinformation from a multi-layered perspective. Furthermore, the fact that manipulative and deceptive content manages to engage the users directly is highly successful strategy, as it creates a sense of ownership over the message (users have the capacity to "endorse", contribute to, alter, and share disinformation that confirms their worldviews). This practice allows disinformation to infiltrate the most intimate

---

[6] *Ibidem*.

[7] P. Törnberg, 'Echo chambers and viral misinformation: Modeling fake news as complex contagion', PLoS ONE, vol. 13, no. 9, 2018, pp. 1-21.

[8] S. Vosoughi, M.N. Mohsenvand and D. Roy, 'Rumor gauge: Predicting the veracity of rumors on Twitter', *ACM Transactions on Knowledge Discovery from Data*, vol. 11, no. 4, 2017, pp. 1-36.

[9] A. Bârgăoanu and L. Radu, 'Fake News or Disinformation 2.0? Some Insights Into Romanians' Digital Behaviour', *Romanian Journal of European Affairs*, no.18, 2018, p. 26.

[10] A. Alaphilippe et al., 'Automated tackling of disinformation - Major challenges ahead', *European Parliament. Science and Technology Options Assessment*, 2019, p. 5, available at https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624278/EPRS_STU(2019)624278_EN.pdf (accessed 10 February 2020).

[11] European Commission, 'Final report of the High Level Expert Group on Fake News and Online Disinformation', 12 March 2018, available at https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation (accessed 15 February 2020).

[12] A. Bendiek, and M. Schulze, *op. cit.*, p.3.

spaces of communication[13]. Given that viral content is inadvertently beneficial to digital platforms, their content curation algorithms are not prepared to deal with these particular challenges. Applying clear-cut rules and criteria for bringing down viral fake information would only tear up the whole fabric of social media, which is designed especially for promoting emotionally engaging content irrespective of its intention to deceive or not.

Through artificially stimulating engagement, disinformation can reach large audiences, and has the potential to virally multiply its effects long before giving the digital platforms or public authorities the chance to spot it and react. As such, we advocate for devising additional measures to reflect this particular understanding of disinformation as a form of "participatory propaganda"[14], or user's engagement fraud.

2. Challenges for regulatory bodies

As digital disinformation is constantly morphing, the challenges for regulatory bodies and policy-makers become greater. In our opinion, three key questions emerge in this regard: (1) Where to place the ultimate responsibility for the proliferation of digital disinformation (internet platform companies/governments/regular users/ other entities)? (2) How to decide what aspects should be targeted with priority? and (3) What are the correct approaches for regulating the complex ecosystem of digital communication?

Fighting disinformation requires a constant focus on monitoring, researching and evaluating the measures implemented by internet platform companies, international organizations or the nation states. Recent studies discuss the risks and opportunities of the European Union (EU) co-regulatory mechanism as compared to self-regulation[15], and their effects in potentially difficult contexts, such as the 2019 European Parliament elections[16].

Additionally, Poynter Institute[17] provides a complex report of how and where governments take action to legislate against digital disinformation and misinformation, whether by implementing media literacy campaigns, setting up task forces or expert groups, or enacting laws.

3. Method

In this exploratory qualitative study, we examine recent attempts to tackle digital disinformation, from the self-regulatory actions implemented by digital platforms, to

---

[13] G. Asmolov, 'The Effects of Participatory Propaganda: From Socialization to Internalization of Conflicts', *Journal of Design and Science*, (6), 2019, available at https://jods.mitpress.mit.edu/pub/jyzg7j6x (accessed 10 February 2020).
[14] *Ibidem*.
[15] P.J. Dittrich, 'Tackling the spread of disinformation. Why a co-regulatory approach is the right way forward for the EU'. Bertelsmann Stiftung Policy Paper, 12 December 2019, pp. 1-11.
[16] A. Bendiek and M. Schulze, 'Disinformation and elections to the European Parliament', *SWP Comment German Institute for International and Security Affairs*, no.16, 2019, pp. 1-8.
[17] D. Funke and D. Flamini, 'A guide to misinformation actions around the world', The Poynter Institute, 2018, available at https://www.poynter.org/ifcn/anti-misinformation-actions/ (accessed 15 February 2020).

EU-level actions, and from hard measures implemented individually by the member states, to soft measures, such as the creation of fact-checking platforms and promotion of media literacy. For the purposes of this exploratory study, we qualitatively assess relevant documents, reports and analyses, including: (1) official statements issued by internet platform companies, such as Facebook, Twitter or Google; (2) policies, reports, studies and communications made public by the European Commission and the European Parliament; (3) national laws implemented to counter disinformation; (4) policies or programs with respect to media education and fact-checking projects. Additionally, we turn to specific reports and studies to discuss the strengths and weaknesses of each type of response.

Four types of interventions emerge and will be discussed in the remaining sections of the article. One is self-regulation, reflecting actions undertaken on a voluntary basis by the digital platforms themselves. The second is the co-regulation approach, focusing on building a cooperation framework between EU-level and national-level authorities, the internet platform companies, media organizations, researchers, and other stakeholders. Thirdly, some EU and non-EU states set up direct regulation (hard legal measures) against disinformation, albeit how they define it may vary significantly across countries. Lastly, some audience-centred solutions have been proposed. Fact-checking and media literacy initiatives contribute to building the citizens' resilience to disinformation.

4. The self-regulation approach: digital platforms fighting disinformation

The self-regulation approach aims to counter digital disinformation based on measures that the platforms will "voluntarily implement"[18]. Self-regulation is seen as a mechanism that holds accountable internet platform companies for the content and behaviour in the online environment. Digital platforms like Facebook or Twitter, and companies like Google, which owns YouTube, announced a plan of actions they will take to "stop misinformation or false news"[19]. For instance, Facebook launched a tool[20] that will help users "understand and control" the posts they see. In addition to that, the social network created the "ad library" – designed to offer "advertising transparency", started a partnership with third-party network of fact-checkers, and publishes monthly reports on the number of accounts blocked for the "coordinated inauthentic behaviour". In the same vein, Twitter announced a ban on political ads, and developed a tool to "flag" false content by special moderators.

The self-regulatory approach faced some criticism, in terms of insufficient transparency, failure in providing publicly verifiable results, the voluntary nature of commitment, excessive reliance on automation for decision-making processes, impossibility of conducting independent verifications, poor monitoring of algorithm curation practices, and asymmetrical access to relevant data between the digital

---

[18] A. Alaphilippe et al., *op. cit.*, p.43.
[19] A. Mosseri,'Working to Stop Misinformation and False News', *Facebook Newsroom*, 7 April 2017, available at https://www.facebook.com/facebookmedia/blog/working-to-stop-misinformation-and-false-news (accessed 10 February 2020).
[20] R. Sethuraman, 'Why Am I Seeing This? We Have an Answer for You', *Facebook Newsroom*, 31 March 2019, available at https://about.fb.com/news/2019/03/why-am-i-seeing-this/ (accessed 15 February 2020).

platforms on the one side, and public authorities and researches, on the other[21]. One of the main weakness of the self-regulation approach resides in the conflicts of interest that can emerge, as digital platforms, and especially free-of-charge social networking sites depend on selling as much advertising as possible[22], as well as on attracting and maintaining the engagement of the audience for as long as possible.

Despite these shortcomings, self-regulation is considered to be an important step towards increased accountability of the digital platforms. The direct involvement of the digital platforms in countering disinformation is necessary, as actions undertaken by third-party fact checkers are considered to be "far from sufficient to tackle the problems of disinformation"[23], while human moderators aren't enough to face the enormous amount of content uploaded daily by users[24].

There is evidence that the digital platforms are becoming increasingly aware of issues such as transparency, personal data protection, developing tools to identify, flag and report false content. Future actions should be oriented towards developing instruments that combine both human and artificial intelligence to review the content published by billions of users worldwide and, more importantly, monitor user behaviour looking for signs of engagement fraud. Lastly, digital platforms need to acknowledge local contexts, as each country or region has its own vulnerabilities or sensible topics to be exploited in disinformation campaigns[25].

5. Co-regulation: The European Union approach

The EU strategy for countering digital disinformation starts from establishing a cooperation framework between expert groups and task forces, Member States, internet platform companies, media organizations, and researchers. A second, but equally important focus lays on promoting media literacy and empowering users to tackle disinformation on a daily basis[26]. The European Union's efforts rely on the co-regulation procedure, aiming to find "a compromise" which allows the implementation of a series of measures by the internet platform companies, monitored by an authority.[27]"

Starting with 2015, the European Commission established "East StratCom Task Force" – a task force addressed to Eastern Partnership countries, such as Ukraine, Georgia or Armenia – that was meant to identify and expose Russia's disinformation

---

[21] A. Alaphilippe et al., *op. cit.*, p. 44.

[22] A. Wood and A. Ravel, 'Fool Me Once: Regulating 'Fake News' and Other Online Advertising', *Southern California Law Review*, vol. 91, no. 6, 2018, p. 1245.

[23] I. Nenadic, 'Unpacking the "European approach" to tackling challenges of disinformation and political manipulation', *Internet Policy Review*, vol. 8, no. 4, 2019, p. 13.

[24] P.J. Dittrich, *op. cit.*, p.5.

[25] E. Humprecht, 'Why resilience to online disinformation varies between countries', *Democratic Audit*, 24 March 2020, available at https://www.democraticaudit.com/2020/03/24/why-resilience-to-online-disinformation-varies-between-countries/ (accessed 24 March 2020).

[26] European Commission, 'Tackling online disinformation', 13 September 2019, available at https://ec.europa.eu/digital-single-market/en/tackling-online-disinformation (accessed 15 February 2020).

[27] A. Alaphilippe et al., *op. cit.*, p. 44.

campaigns. Notably, its budget more than doubled to €5 million in 2019[28]. In 2016, the Joint Framework on countering hybrid threats[29] was adopted, followed by the Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats[30] in 2018. The same year, the European Commission announced the creation of the High Level Expert Group on Fake News and Online Disinformation, formed of representatives of news media, academia, and internet platform companies[31], with the purpose to address and explore digital disinformation, identify solutions to efficiently fight the phenomenon, offer regular reports on current state of affairs and recommend possible legal actions necessary to implement. The Final Report of the group offered guidelines on a number of interconnected and mutually reinforcing responses[32].

By building on previous actions, the 2018 EC Communication "Tackling online disinformation: a European Approach"[33] put forward several tools for countering disinformation, while emphasizing that "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"[34].

Later in 2018, as a follow-up of the Communication, the European Commission outlined "the first worldwide self-regulatory set of standards" – the Code of Practice on Disinformation, voluntarily signed by the digital platforms, advertisers and advertising industry. The Code's main purposes are to provide more transparency in online political advertising, address the issue of fake accounts, empower consumers to report the disinformation, and encourage more research. Recent evaluations of progress[35] point out that the Code has produced mixed results and has understandably failed to satisfy all parties and to mitigate the phenomenon. Key improvements should be made with respect to: persuading the digital platforms to open their APIs for policy-driven researchers (safe spaces) in order to expose the phenomenon, stopping the blaming game among stakeholders, increasing mutual trust between industry, governments,

---

[28] European Commission, 'Progress Report on Action Plan Against Disinformation', June 2019, available at https://ec.europa.eu/commission/sites/beta-political/files/factsheet_disinfo_elex_140619_final.pdf (accessed 15 February 2020).

[29] European Commission, 'Security: EU strengthens response to hybrid threats', 6 April 2019, available at https://ec.europa.eu/commission/presscorner/detail/en/IP_16_1227 (accessed 10 February 2020).

[30] European Commission, 'A Europe that protects: EU works to build resilience and better counter hybrid threats', 13 June 2018, available at https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4123 (accessed 15 February 2020).

[31] European Commission, 'Experts appointed to the High Level Group on Fake News and online disinformation', 12 January 2018, available at https://ec.europa.eu/digital-single-market/en/news/experts-appointed-high-level-group-fakenews-and-online-disinformation (accessed 15 February 2020).

[32] European Commission, 'Final report of the High Level Expert Group on Fake News and Online Disinformation', 12 March 2018, available at https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation (accessed 15 February 2020).

[33] European Commission, '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', 26 April 2018, COM(2018) 236 final, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236 (accessed 15 February 2020).

[34] *Ibidem*, p. 7.

[35] J. Pamment, 'EU Code of Practice on Disinformation: Briefing Note for the New European Commission', *Carnegie Endowment for International Peace*, March 2020, available at https://carnegieendowment.org/2020/03/03/eu-code-of-practice-on-disinformation-briefing-note-for-new-european-commission-pub-81187 (accessed 20 March 2020).

academia, and civil society, addressing the intra-European misinformation or disinformation campaigns, addressing the social media black market; funding trans-European policy-driven research projects; and creating a shared database of analytics to inform policymakers and the research on the community impact of influence operations and of countermeasures.

By the end of 2018, the Action plan against disinformation brought together the EU institutions, Member States, civil society and the private sector (especially the digital platforms) to implement actions for a coordinated response. The response "is based on four pillars: (i) improving the capabilities of Union institutions to detect, analyse and expose disinformation; (ii) strengthening coordinated and joint responses to disinformation; (iii) mobilising private sector to tackle disinformation; (iv) raising awareness and improving societal resilience.[36]" Proposed measures recognise the importance of data mining and analysis, of strengthening the national and EU Strategic Communication Task Forces, setting up a Rapid Alert System[37], and the close monitoring of the implementation of the Code of Practice. For safeguarding what at that point were the forthcoming European elections, the Action plan called on Member States to engage with media, online platforms, information technology providers and others, as a direct reflection of the notion of co-regulating within a collaborative mind set.

The most recent (at the moment of writing) report on progress of the Action plan against disinformation (June 2019)[38] provides an overview on the implementation of the Code of practice, reflecting measures such as actions against accounts that violate ad policies, safeguarding the integrity of services by deleting fake, scam, and spam accounts, increasing transparency of issue-based ads. Nevertheless, according to the same report, there is room for improvement in terms of identification of the actors involved in disinformation, and making additional datasets available to the research community, without conflicting with personal data protection rules. Additionally, more progress has been made with respect to promoting media literacy, raising awareness about disinformation, boosting the EU capacity to react to disinformation, and supporting quality journalism and independent fact-checking.

6. Direct regulation approach: more shortcomings than benefits?

State-driven hard, regulatory measures are debatable for reasons related

---

[36] European Commission, "JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS - Action Plan against Disinformation", 5 December 2018, JOIN(2018) 36 final, available at https://ec.europa.eu/commission/sites/beta-political/files/eu-communication-disinformation-euco-05122018_en.pdf (accessed 15 February 2020).

[37] European Union External Action, 'Rapid Alert System. Strengthening coordinated and joint responses to disinformation', March 2019, available at: https://eeas.europa.eu/sites/eeas/files/ras_factsheet_march_2019_0.pdf (accessed 10 February 2020).

[38] European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, 'JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGION- Report on the implementation of the Action Plan Against Disinformation', 14 June 2019, JOIN(2019) 12 final, available at https://eeas.europa.eu/sites/eeas/files/joint_report_on_disinformation.pdf (accessed 15 February 2020).

to possible accusations of censorship, limitations of the freedom of speech or even democracy itself, as well as for the difficulty to define what exactly is considered "fake news" or disinformation. Nevertheless, some EU Member States, such as Germany, France, and Hungary, and non-EU states, such as Singapore, Russia or Malaysia, have put in place laws that stipulate fines or imprisonment for publishing and disseminating content deemed as illegal. They empower state authorities to block websites, social media accounts or remove online unlawful content.

Within the European Union, Germany and France decided to take stricter measures to counter digital disinformation, demand more transparency of the digital platforms, apply monetary sanctions, or even block a foreign state-controlled broadcaster. *NetzDG*[39], the German Network Enforcement Law (2017), also known as "hate speech law" is addressed to issues like "defamation" or "incitement to crime or violence"[40]. The German law obliges digital platforms with at least two million registered users in Germany to remove illegal content within 24 hours and stipulates fines up to EUR 50 mln, if the content is not deleted. In 2018, a French legislative proposal on the publishing and dissemination of false information during an electoral campaign was enforced. According to the law, an electoral candidate or political party can appeal to a judge to take down false story or information, within 48 hours[41]. The same law empowers the French broadcasting regulator, the Audio-visual Council, to "block foreign state-controlled broadcasters that publish false information"[42].

A sticking recent example comes from Hungary, where the Parliament approved on March 30, 2020, new emergency powers in the context of the COVID-19 pandemic, allowing the ruling party to govern by decree indefinitely[43]. Among other measures, the new law targets the spread of misinformation by stipulating up to five years of imprisonment for those accused. The concerns related to this measure reflect the more general criticism of state-driven hard regulations, namely the fact they may open new avenues for abuse of power in deciding what is disinformation, and, consequently, suppression of free speech under authoritarian regimes.

In 2018, Malaysia introduced the *Anti Fake-News Act*, aimed to sanction illegal content by fines or imprisonment. The law was repealed later in October 2019 by the newly appointed government[44]. The legislation defined fake news as "any news, information, data and reports that are whole or partly false whether in the form of features, visuals or audio recordings or in any other form capable of suggesting words or ideas"[45]. Citizens or online network providers were liable to fines or a sentence to ten

[39] Network Enforcement Act (Netzdurchsetzunggesetz, NetzDG), *German Law Archive*, 1 September 2017, available at https://germanlawarchive.iuscomp.org/?p=1245 (accessed 10 March 2020).

[40] P.J. Dittrich, *op. cit.*, p. 6.

[41] A. Alaphilippe et al., *op. cit.*, p. 47.

[42] *Ibidem*.

[43] S. Stolton and V. Makszimov, 'Orbán to rule by decree with new powers to <<silence critics>>', *Euractiv*, 30 March 2020, available at https://www.euractiv.com/section/global-europe/news/orban-to-rule-by-decree-with-new-powers-to-silence-critics/ (accessed 16 April 2020).

[44] R. Latiff and N. Macfie, 'Malaysia parliament scraps law penalizing fake news', *Reuters*, 9 October 2019, available at https://www.reuters.com/article/us-malaysia-politics-fakenews/malaysia-parliament-scraps-law-penalizing-fake-news-idUSKBN1WO1H6 (accessed 15 February 2020).

[45] 'Malaysia Anti-Fake News Bill 2018', *CLJ Law*, available at https://www.cljlaw.com/files/bills/pdf/2018/MY_FS_BIL_2018_06.pdf (accessed 10 March 2020).

years of imprisonment.

By contrast, the Singapore *Protection from Online Falsehoods and Manipulation Act*[46] offers a more specific definition of falsehoods, as "false statements of fact" where the information is "prejudicial" to Singapore's "security, public safety, public tranquillity". The Singapore law applies to digital platforms, news websites and online publications, and empowers the government to decide whether the information is unlawful and to impose fines or imprisonment.

In 2018, the Egyptian government adopted several laws to fight the spread of false information. The law identifies as unlawful content "information deemed to threaten national security; disturb the public peace; or promote discrimination, violence, racism", and empowers authorities to block the access to a blog, website, or social media account.

In China, the criminal law stipulates up to seven years imprisonment for whoever fabricates "false information on dangerous situation, epidemic situation, disaster situation or alert situation"[47]. More recently, in 2019, Chinese government made it illegal to publish video and audio "deepfakes"[48].

As from March 2019, the Russian parliament passed a "Law on Fake News" that stipulates fines for users of digital platforms and blogs, media outlets, network publications that disseminate "knowingly inaccurate socially significant information", and empowers state authorities to immediately notify the editors of the "network publications" to delete the content, otherwise the access to the website will be blocked[49].

7. Audience-centred approaches: fact-checking and media literacy initiatives

Besides the aforementioned regulatory measures, another set of solutions is designed to empower the audience to discern between fake and genuine information, to develop critical thinking skills and fact checking reflexes, and to build resilience to disinformation. The strategies in this regard rely on fact-checking platforms and media literacy programs.

Fact-checking projects are oriented toward monitoring the factual accuracy of news, political statements or interviews and aim to debunk rumours, myths or any manipulated information, by offering counter-narratives to the untrue and manipulated information driven by emotions, not facts[50]. At EU-level, EUvsDisinfo is

---

[46] 'Protection from Online Falsehoods and Manipulation Act 2019 – Singapore', *Singapore Statutes Online*, available at https://sso.agc.gov.sg/Acts-Supp/18-2019/Published/20190625?DocDate=20190625#pr7- (accessed 10 March 2020).
[47] M. Repnikova, 'China's Lessons for Fighting Fake News', *Foreign Policy*, 6 September 2018, available at https://foreignpolicy.com/2018/09/06/chinas-lessons-for-fighting-fake-news/ (accessed 15 February 2020).
[48] Y. Yang, B. Gog and E. Gibbs, 'China seeks to root out fake news and deepfakes with new online content rules', *Reuters*, 29 November 2019, available at https://www.reuters.com/article/us-china-technology/china-seeks-to-root-out-fake-news-and-deepfakes-with-new-online-content-rules-idUSKBN1Y30VU (accessed 15 February 2020).
[49] A. Richter, 'Disinformation in the media under Russian law', *IRIS Extra, European Audiovisual Observatory, Strasbourg*, 2019, p. 13.
[50] K. Giereło-Klimaszewska, 'Political Fact-Checking in the Czech Republic on the Example of demagog.cz and manipulatori.cz Portals', *Mediatization Studies*, 2019, No. 3, p. 124.

the flagship initiative to create a database of messages in the international information space that are identified as providing a partial, distorted, or false depiction of reality, and is based on media reporting and analysis of the East StratCom Task Force. The fruitfulness of this approach is being tested, at the moment of writing, with respect to the disinformation waves about the COVID-19 pandemic. The Special Report of the EEAS available within the "News and Analysis" section of the EUvsDisinfo provides an overview of the results of fact-checking efforts on coronavirus disinformation[51]. Most notably, EU's approach to fact-checking allowed for the successful identification of the main disinformation narratives, and exposure of the incidence and morphology of pro-Kremlin disinformation targeting domestic and international audiences.

Across Europe, multiple projects have been established, such as the German fact-checking organization "*Correctiv*"[52], the Lithuanian platform "Debunk"[53], *Demagog* – in Czech Republic[54], or Faktabaari, in Finland[55].

Media and information literacy programs and policies were developed in the past decade, as critical thinking and the ability to recognize false stories are considered key skills "to engage more effectively with online information and social platforms.[56]" At the European Union level, an Expert Group on Media Literacy was established, and a Commission initiative to promote media literacy projects across EU, "Media Literacy Week", was implemented. Member States show a similar interest though individual initiatives.

8. Discussion

In this article, we provided an overview of current actions to counter disinformation. Until the moment of writing, responses to disinformation reflect an increasingly tighter collaboration between the digital platforms, the internet platform companies, EU institutions, national governments, journalists, researchers, and other relevant stakeholders. The approach fostered by the EU has a strong component of strategic communication (see the role of the East StratCom Task Force), and focuses on cooperation and dialogue, expert contributions (see the High Level Expert Group on Fake News and Online Disinformation and other research or policy studies), public consultations, and self-regulation on behalf of the digital platforms.

In countering disinformation, the EU relies on self-regulation and co-regulation "as private-public mechanisms for setting rules and standards"[57]. The approach holds the assumption that regulating the internet is done best by implementing voluntary-

---

[51] European External Action Service, 'SPECIAL REPORT: Disinformation on the coronavirus – short assessment of the information environment', EUvsDisinfo website, available at https://euvsdisinfo.eu/eeas-special-report-disinformation-on-the-coronavirus-short-assessment-of-the-information-environment/ (accessed 16 April 2020).
[52] Correctiv, 'About us. Investigations in the public interest', *Correctiv website*, available at https://correctiv.org/en/about-us/ (accessed 10 March 2020).
[53] Debunk, 'About Debunk', *Debunk website*, available at https://debunk.eu/about-debunk/ (accessed 10 March 2020).
[54] Demagog, 'O nàs', *Demagog website*, available at https://demagog.cz/stranka/o-nas (accessed 10 March 2020).
[55] FaktaBaari, 'Welcome to Faktabaari', *Faktabaari website*, available at https://faktabaari.fi/in-english/ (accessed 10 March 2020).
[56] A. Alaphilippe et al., *op. cit.*, p. 50.
[57] P.J. Dittrich, *op. cit.*, p. 3.

based measures. This approach requires collaboration and good will on behalf of all parties involved. This aspect is particularly striking with respect to the implementation of the Code of Practice, as its success heavily depends upon the agency of the digital platforms. After all, it is only sensible to allow platforms to self-regulate, since they have the insider know-how and needed instruments to counter the structural deficiencies that allow disinformation to flourish. It is a means of avoiding the awkward realization of how difficult it is to establish regulations for a domain lacking transparency and accountability. Internet platform companies like Facebook, Twitter, and Google are currently expressing more awareness of issues such as transparency, in particular, in political advertising, protecting personal data, developing tools to flag and report false content.

Self-regulation is not without limitations, though. Conflicts of interest may occur between the platforms' vital necessity to keep users engaged and monetize their engagement, and the public authorities' need to the safeguard the integrity and balance of democratic processes within the national public spheres while ensuring the freedom of expression. Other challenges for self-regulation include the enormous amount of content that has to be monitored, the limited efficiency of fact-checking, and the occasional failures of human moderation, and automatic processes of data curation within the digital space.

At the opposite end of the spectrum, direct regulations seem to be the preferred choice for many EU and non-EU states across the world. Many states adopted specific laws and penalties for dealing with fake or illegal content on the internet, while a commonly-agreed definition of disinformation, "fake news" has not been identified and will not be identified any time soon. State-imposed direct regulations face significant criticism, from concerns that these measures can threaten press freedom and the freedom of expression, to the risk of undermining democracy, fair political competition and impose a form of censorship. Furthermore, these regulations focus excessively and almost exclusively on content that is deemed as illegal, while ignoring that many variants of disinformation can successfully escape these definitions, that it is the digital behaviour of regular, well-intended users which contributes to the proliferation of disinformation, and that many misleading news, commentary, and interpretation of events can still circulate successfully "under the radar".

The quasi-inevitable inconsistency in the response against disinformation, between the soft measures the EU has adopted in recent years, and the hard, sanction-driven measures enforced by some individual Member States[58] can be partly overcome by moving more decisively to a co-regulatory framework of action at pan-European level. Co-regulation in countering digital disinformation would mean setting up the principles and objectives at the supranational level, followed by contributions from the industry (co-regulatory bodies from the industry), and lastly, the implementation of needed technical measures to satisfy both EU-regulations and the codes of conduct proposed by the co-regulatory bodies[59]. This solution, to be implemented under

---

[58] F. Giumelli, E. Cusumano and M. Besana, 'From Strategic Communication to Sanctions: The European Union's Approach to Hybrid Threats' in E. Cusumano and M. Corbe (eds), *A Civil-Military Response to Hybrid Threats*. Palgrave Macmillan, Cham, 2018, pp. 145-167.
[59] P.J. Dittrich, *op. cit.*, p. 8.

independent supervision, could represent a next step in alleviating "the supremacy of internet companies"[60], and ensure more efficiency in the fight against disinformation, while avoiding strict, hard measures that could backfire.

9. Conclusions

This paper provides an overview of the current approaches to digital disinformation, by identifying and discussing four main possibilities: self-regulation, co-regulation, direct regulation, and audience-centred solutions. In what actions undertaken at EU level are concerned, we advocate for moving towards a more decisive co-regulatory framework and a major overhaul of the digital platforms ad-based business model. This approach can correct some of the current asymmetries in power between social platforms and public authorities and policy-driven researchers, while ensuring the necessary flexibility for adapting regulations to the distinctive features of each platform as locus of disinformation, and to local social contexts as well.

Furthermore, we identified a limitation of the current responses to disinformation, which focus mainly on the identification and elimination of fake/false or misleading content. Digital disinformation can be understood both as a content-related fraud and as an engagement-related fraud. In its latter meaning, disinformation implies the artificial, big data and algorithm-driven amplification of engagement with the respective content, making it more viral, more compelling, and increasing legitimate for the audience. More measures need to be taken to address this specific challenge, by exposing ongoing practices such as targeted advertising, behavioural advertising, precision segmentation, psychographic profiling or extreme personalization of online content.

References:

- Alaphilippe, A. et al., 'Automated tackling of disinformation - Major challenges ahead', *European Parliament* (Science and Technology Options Assessment), March 2019, available at https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624278/EPRS_STU(2019)624278_EN.pdf (accessed 10 February 2020).

- Asmolov, G., 'The Effects of Participatory Propaganda: From Socialization to Internalization of Conflicts', *Journal of Design and Science*, vol. 6, 2019, available at https://jods.mitpress.mit.edu/pub/jyzg7j6x (accessed 10 February 2020).

- Balmas, M, 'When fake news becomes real: Combined exposure to multiple news sources and political attitudes of inefficacy, alienation, and cynicism', *Communication Research*, vol. 41, no. 3, 2014, pp. 430-454.

- Bârgăoanu, A. and Radu, L., 'Fake News or Disinformation 2.0? Some Insights Into Romanians' Digital Behaviour', *Romanian Journal of European Affairs*, no.18, 2018, pp. 24-38.

---

[60] A. Bendiek and M. Schulze, *op.cit.*, p. 7.

- Bendiek, A. and Schulze, M., 'Disinformation and elections to the European Parliament', *SWP Comment German Institute for International and Security Affairs*, no.16, 2019, pp. 1-8.

- Brewer, P.R., Young D.G and Morreale, M., 'The impact of real news about "fake news": Intertextual processes and political satire', *International Journal of Public Opinion Research*, vol. 25, no 3, 2013, pp. 323-343.

- European Commission, 'A Europe that protects: EU works to build resilience and better counter hybrid threats', *Press Release*, 13 June 2018, available at https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4123 (accessed 15 February 2020).

- European Commission, 'Experts appointed to the High Level Group on Fake News and online disinformation', 12 January 2018, available at https://ec.europa.eu/digital-single-market/en/news/experts-appointed-high-level-group-fakenews-and-online-disinformation (accessed 15 February 2020).

- European Commission, 'Progress Report on Action Plan Against Disinformation', June 2019, available at https://ec.europa.eu/commission/sites/beta-political/files/factsheet_disinfo_elex_140619_final.pdf (accessed 15 February 2020).

- European Commission, 'Security: EU strengthens response to hybrid threats', *Press Release*, 6 April 2019, available at https://ec.europa.eu/commission/presscorner/detail/en/IP_16_1227 (accessed 10 February 2020).

- European Commission, 'Final report of the High Level Expert Group on Fake News and Online Disinformation', 12 March 2018, available at https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation (accessed 15 February 2020).

- European Commission, 'JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS - Action Plan against Disinformation', 5 December 2018, JOIN(2018) 36 final, available at https://ec.europa.eu/commission/sites/beta-political/files/eu-communication-disinformation-euco-05122018_en.pdf (accessed 15 February 2020).

- European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, 'JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGION- Report on the implementation of the Action Plan Against Disinformation', 14 June 2019, JOIN(2019) 12 final, available at https://eeas.europa.eu/sites/eeas/files/joint_report_on_disinformation.pdf (accessed 15 February 2020).

- European Commission, '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', 26 April 2018,

COM(2018) 236 final, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236 (accessed 15 February 2020).

- European Commission, 'Tackling online disinformation', 13 September 2019, available at: https://ec.europa.eu/digital-single-market/en/tackling-online-disinformation (accessed 15 February 2020).

- European External Action Service, 'SPECIAL REPORT: Disinformation on the coronavirus – short assessment of the information environment', *EUvsDisinfo website*, available at https://euvsdisinfo.eu/eeas-special-report-disinformation-on-the-coronavirus-short-assessment-of-the-information-environment/ (accessed 16 April 2020).

- European Union External Action, 'Rapid Alert System. Strengthening coordinated and joint responses to disinformation', March 2019, available at https://eeas.europa.eu/sites/eeas/files/ras_factsheet_march_2019_0.pdf (accessed 10 February 2020).

- Dittrich, P.J., 'Tackling the spread of disinformation. Why a co-regulatory approach is the right way forward for the EU'. Bertelsmann Stiftung Policy Paper, 12 December 2019, pp.1-11, available at http://aei.pitt.edu/102500/ (accessed 10 February 2020).

- Funke, D. and Flamini, D., 'A guide to misinformation actions around the world', *The Poynter Institute*, 2018, available at https://www.poynter.org/ifcn/anti-misinformation-actions/ (accessed 15 February 2020).

- Giereło-Klimaszewska, K., 'Political Fact-Checking in the Czech Republic on the Example of demagog.cz and manipulatori.cz Portals', *Mediatization Studies*, no. 3, 2019, pp.115-135.

- Giumelli, F., Cusumano, E. and Besana, M., 'From Strategic Communication to Sanctions: The European Union's Approach to Hybrid Threats', in E. Cusumano and M. Corbe (eds), *A Civil-Military Response to Hybrid Threats*, Palgrave Macmillan, Cham, 2018, pp. 145-167.

- Humprecht, E., 'Why resilience to online disinformation varies between countries', *Democratic Audit*, 24 March 2020, available at https://www.democraticaudit.com/2020/03/24/why-resilience-to-online-disinformation-varies-between-countries/ (accessed 24 March 2020).

- Latiff, R. and Macfie, N., 'Malaysia parliament scraps law penalizing fake news', Reuters, 9 October 2019, available at https://www.reuters.com/article/us-malaysia-politics-fakenews/malaysia-parliament-scraps-law-penalizing-fake-news-idUSKBN1WO1H6 (accessed 15 February 2020).

- Littau, J. and Stewart, D.R.C., "Truthiness" and second-level agenda setting: Satire news and its influence on perceptions of television news credibility. *Electronic News*, vol. 9, no. 2, 2015, pp. 122-136.

- Mosseri, A., 'Working to Stop Misinformation and False News', *Facebook Newsroom*, 7 April 2017, available at https://www.facebook.com/facebookmedia/blog/working-to-stop-misinformation-and-false-news (accessed 10 February 2020).

- Nenadic, I., 'Unpacking the "European approach" to tackling challenges of disinformation and political manipulation', Internet Policy Review, vol. 8, no. 4, 2019, pp. 1-22.

- Pamment, J., 'EU Code of Practice on Disinformation: Briefing Note for the New European Commission', *Carnegie Endowment for International Peace*, March 2020, available at https://carnegieendowment.org/2020/03/03/eu-code-of-practice-on-disinformation-briefing-note-for-new-european-commission-pub-81187 (accessed 20 March 2020).

- Repnikova, M., 'China's Lessons for Fighting Fake News', *Foreign Policy*, 6 September 2018, available at https://foreignpolicy.com/2018/09/06/chinas-lessons-for-fighting-fake-news/ (accessed 15 February 2020).

- Richter, A., *Disinformation in the media under Russian law*, IRIS Extra, European Audiovisual Observatory, Strasbourg, June 2019, available at https://rm.coe.int/disinformation-in-the-media-under-russian-law/1680967369 (accessed 15 February 2020).

- Sethuraman, R., 'Why Am I Seeing This? We Have an Answer for You', *Facebook Newsroom*, 31 March 2019, available at https://about.fb.com/news/2019/03/why-am-i-seeing-this/ (accessed 15 February 2020).

- Stolton, S. and Makszimov, V, 'Orbán to rule by decree with new powers to <<silence critics>>', *Euractiv*, 30 March 2020, available at https://www.euractiv.com/section/global-europe/news/orban-to-rule-by-decree-with-new-powers-to-silence-critics/ (accessed 16 April 2020).

- Törnberg, P., 'Echo chambers and viral misinformation: Modeling fake news as complex contagion', PLoS ONE, 13(9), 2018, pp. 1–21, doi: 10.1371/journal.pone.0203958.

- Vosoughi, S., Mohsenvand, M.N. and Roy, D., 'Rumor gauge: Predicting the veracity of rumors on Twitter', *ACM Transactions on Knowledge Discovery from Data*, vol. 11, no. 4, 2017, pp. 1–36. doi: 10.1145/3070644.

- Wood, A. and Ravel, A., 'Fool Me Once: Regulating 'Fake News' and Other Online Advertising', *Southern California Law Review*, vol. 91, no.6, 2018, p. 1223-1278.

- Yang, Y., Gog, B. and Gibbs, E., 'China seeks to root out fake news and deepfakes with new online content rules', Reuters, 29 November 2019, available at https://www.reuters.com/article/us-china-technology/china-seeks-to-root-out-fake-news-and-deepfakes-with-new-online-content-rules-idUSKBN1Y30VU (accessed 15 February 2020).

Online sources:

- Correctiv, 'About us. Investigations in the public interest', *Correctiv website*, available at https://correctiv.org/en/about-us/ (accessed 10 March 2020).

- Debunk, 'About Debunk', *Debunk website*, available at https://debunk.eu/about-

debunk/ (accessed 10 March 2020).

- Demagog, 'O nàs', *Demagog website*, available at https://demagog.cz/stranka/o-nas (accessed 10 March 2020).

- FaktaBaari, 'Welcome to Faktabaari', *Faktabaari website*, available at https://faktabaari.fi/in-english/ (accessed 10 March 2020).

- 'Malaysia Anti-Fake News Bill 2018', *CLJ Law*, available at https://www.cljlaw.com/files/bills/pdf/2018/MY_FS_BIL_2018_06.pdf (accessed 10 March 2020).

- 'Network Enforcement Act (Netzdurchsetzunggesetz, NetzDG)', *German Law Archive*, 1 September 2017, available at https://germanlawarchive.iuscomp.org/?p=1245 (accessed 10 March 2020).

- 'Protection from Online Falsehoods and Manipulation Act 2019 – Singapore', *Singapore Statutes Online*, available at https://sso.agc.gov.sg/Acts-Supp/18-2019/Published/20190625?DocDate=20190625#pr7- (accessed 10 March 2020).