

Normativity in the EU's Approach towards Disinformation

Anna Kobernjuk
Agnes Kasper

Tallinn Law School
Tallinn University of Technology
Akadeemia tee 3
Tallinn 12618, Estonia
Email: anna.kobernjuk@taltech.ee
Email: agnes.kasper@taltech.ee

Abstract: With the rapid growth of disinformation, two major steps were taken to battle the phenomenon in the online environment—first on the global level, and second on the European Union level. The first step is the Joint Declaration on Freedom of Expression and “Fake News”, Disinformation and Propaganda, which provides a general overview of possible actions to be taken to fight disinformation, and how “things should be”. The steps are connected to following human rights standards, promoting the diversity of media, and paying special attention to intermediaries and media outlets. The second one is the Code of Practice on Disinformation, which is a self-regulatory document that can be voluntarily signed by major social media platforms and advertising bodies, and its main focus is making political advertising coherent and clear, preventing the creation of fake accounts, providing users with tools to report disinformation, and promote further research. Nevertheless, based on the reports and criticism from stakeholders, the Code of Practice has not reached a common ground regarding definitions, it has provided no mechanism to access the development, and has had several other drawbacks which need additional attention and discussion. The article is devoted to identifying gaps in the Code of Practice on Disinformation based on the reports and criticism provided by the stakeholders and elaborating on possible practices to regulate the legal issues raised by disinformation on the European Union level. We use doctrinal and comparative methods in the work.

The doctrinal method targets the cluster that was identified in order to analyze the Code of Practice, identifies weak spots and inconsistencies, and offers solutions from different areas of law. The comparative method was selected since in several areas of law, such as human rights and consumer protection law, the previously identified approaches will be addressed to find the best outcomes. This combination of methods allows an in-depth understanding of legal documents and identifying successful solutions, which can influence further development based on efficient examples.

Keywords: *Code of Practice on Disinformation, definition, disinformation, fake news, human rights, Joint Declaration, liability, regulation*

1. Introduction

Disinformation cannot be considered a new phenomenon, although its presence has become critically evident in the past few years. With the rapid development of the internet, access to the news and similar platforms where such news can be broadcasted to a wider audience, it has become easier to see behind fake news, yet it is also more challenging from a normative perspective. Everyone can now post their own thoughts and ideas, comment on the news and articles, subjecting other users to millions of daily posts that in some cases lack quality and responsibility.

The Joint Declaration on Freedom of Expression and “Fake News”, Disinformation and Propaganda (2017), which was the result of cooperation between the United Nations Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe, the Organization of American States, and the African Commission on Human and Peoples’ Rights, and was brought to life in 2017, may be considered one of the first responses to the issue of disinformation on a global scale. The document itself may be viewed as a collection of guidelines and applicable standards and actions that shall be taken into consideration when applying different methods for regulating disinformation (Joint Declaration, 2017).

Due to the nature and complexity of issues regarding disinformation, there has been a need for drastic changes, and a new step was introduced to increase awareness about the seriousness of this phenomenon, this time on

the European Union level. The Commission called together a High-Level Expert Group on Fake News and Online Disinformation, which advised the European Commission to approve a many-sided path for spotting and disproving online disinformation (Vaque, 2018, p. 413). The Commission was expected to take into consideration “a self-regulatory approach based on a clearly defined multi-stakeholder engagement process, framed within a binding roadmap for implementation, and focused on a set of specific actions” (Vaque, 2018, p. 413). Such an approach should be based on the requirements to provide clarity of online news, support media and information literacy, come up with tools that will allow users to report and fight back false information posts, and promote further research (Vaque, 2018, p. 413). On the basis on these steps, a self-regulatory approach known as the Code of Practice on Disinformation was brought to life in 2018.

The aim of this study is to identify gaps in the approaches towards the Code of Practice on Disinformation based on the reports and criticism from social media platforms and stakeholders and, on the basis of the said information, the possible practices for regulating the legal issues related to disinformation on the European Union level shall be presented. Solutions will be derived from the proposal for an EU Regulation, human rights, the definition, and from the perspective of liability. Out of the provided list, the most balanced and least intrusive solution can be chosen for further elaboration and implementation on the European Union level. Doctrinal and comparative methods have been used in the study. The doctrinal method was applied in order to analyze the Code of Practice and use it as the main point of focus. The comparative method was also used, since several areas of law, such as the human rights and consumer protection law, will be addressed to find the best outcomes.

The current article consists of several parts. The authors will present information for a better understanding of the issue and definitions for fake news and disinformation, and the consequences it may have in the relations of states, and introduce independent actions that have been taken previously by some European Union countries. Then, the focus will be shifted specifically to the European Union, tracing the steps that have already been taken to fight fake news on the EU level with an analysis assessing the efficiency of such actions. Furthermore, the authors are prepared to provide readers with solutions from different areas of law. The article concludes with a brief conclusion and a list of references.

2. Fake news and disinformation

This chapter is devoted to providing explanations on the reasons why 'disinformation' has been chosen instead of the widely used term 'fake news'. Firstly, a brief explanation is provided regarding what is fake news and the categories that it covers, followed by presenting a definition of disinformation. Fake news is considered to be a class of disinformation (Gelfert, 2018, p. 103). Specifically, fake news is used as a term that reflects modern disputes in relation to new emerging technologies (Kalsnes, 2018). In simpler terms, fake news is a more recent word added to the terminology, which is nowadays used to label all news posts in an online environment. Fake news consists of several groups under one title and may include, among other things, "complete fabrications, misleading content, satire or parody, foreign interference in domestic politics, and bad journalism" (Francis, 2018, p. 102).

Bad journalism may be produced by an inexperienced person who has no intention to lie to the wider public, just facts were not checked accordingly or time limitations affected the publication, while intentionally posted misleading content by another user could be punishable for causing panic. Furthermore, moving on to other categories, satire is used to present incorrect incidents for entertainment purposes (Shu *et al.*, 2017, p. 23). Such performances consist of correct information, adding up extra layers, adjusting the layout, and making the news appear more comical for the general public. Another category is the fabricated news which are created in a similar manner as legitimate news but there has been no attempt to confirm the data and there is no understanding provided behind the sources (Pepp *et al.*, 2019, p. 76). Fabricated news may use the same language, sentence structure, titles that mimic actual media, but they may contain no or only bits of accurate information. Propaganda is the news stories which are created by political entities to influence public opinion (Edson *et al.*, 2018, p. 146). The categories also vary in the way they rely on actual facts and the desire to deceive. Satire has very minimal intent to deceive the public; on the contrary, it is used to discuss political well-being or other critical issues, while propaganda and fabrication, on the other hand, are aimed to trick a wider public (Edson *et al.*, pp. 147–148). There are different objectives which are at stake, but mostly those are either political or financial, although simple trolling cannot be excluded either. Fake news is a widely used term that is adopted to label any information in the online environment, even if this is an online post where the data is correct but the

user cannot agree with the provided details and considers them to be fake without a factual basis.

Disinformation is the data the main purpose of which is to deceive and impact the public's opinion (Nunez, 2020, pp. 785–786). The High-Level Expert Group on Fake News and Online Disinformation came to a conclusion that the term 'disinformation' shall be used instead of 'fake news' based on two points: (1) the term is not restricted only to news but also covers the distribution of false data via any possible means, from videos to fake accounts; and (2) fake news are being constantly used by politicians if something is against the opinions expressed by them (Pollicino & Bietti, 2019, p. 48). Fake news is associated solely with news, while disinformation covers a wider scope of information. Disinformation was mentioned both in the Joint Declaration and Code of Practice, and since this term is considered to be precise and not as misleading as fake news, disinformation shall be used as the appropriate one.

2.1 Cases of disinformation and its consequences to the countries

There is a huge amount of examples available to illustrate the destructive force of disinformation, and several of these will be presented in this subchapter. One of the first and most discussed examples is the 2016 United States elections. It is speculated that the previous President of the United States was able to win the elections due to Russian interference (Yilma, 2017, p. 102). This became possible with the dissemination of false information on other candidates on major social media platforms (Yilma, 2017, p. 102). Not only were bots spreading fabricated information, but also fake websites were created that were not flagged by platforms as they seemed like legitimate news sites from where articles were reposted with false facts and presented on social media platforms (Murray, 2016). This affected one of the human rights, more precisely the right to free elections, since the opinion regarding other candidates was influenced by the posts in the media. The voters were not able to enjoy the right, as they had no possibility to determine whether the information online was truthful or not but had to make choices based on it. Seeing the imperfections and wrongdoings of one candidate, people tend to pick the least controversial one without double-checking the details presented in the news stories.

One of the elements of the nature of cyber threats may be related to the possibility to influence people's opinion via the internet without the

individuals' knowledge, in other words known as information warfare (Swiatkowska, 2017, p. 88). The development of the internet has made it possible to rapidly share information and easily influence people to change their opinions with only a few sentences. An example of information warfare could be seen in the Polish–Ukrainian relations. This case involves the Ukraine–European Union Association Agreement, which was blocked by the former President of Ukraine in 2013, and due to those actions riots spread over the entire country (Swiatkowska, 2017, p. 89). Poland offered support to Ukraine, however, certain circles did not take it lightly, and information campaigns flourished online to break the friendly relations between the two countries using both historical events and news regarding Poland's desire to take over Ukraine (Swiatkowska, 2017, pp. 89–90). This was an elaborated intervention, which combined several methods, such as disinformation, provocation, and similar actions in order to spread false information to a wider audience (Info Ops Polska Foundation, 2020). In both countries, certain groups were rolling out incorrect information to create a negative image of the neighboring country, creating messages using historical and sensitive events to weaken the relations between the countries, using a specific model for cyberspace which was described as a process consisting of many different connected parts that disseminated information to weaken selected areas of cyberspace and twist the information, and many other actions were taken by specific groups to negatively affect the countries' relations (Info Ops Polska Foundation, 2020). Such planned large-scale campaigns do not go unnoticed. Manipulative messages, portraying other countries as enemies, using facts without a solid basis—all this threatens the well-being of countries not only physically but also in the cybersphere, since it is being filled up with reposted articles that are transformed by every other repost and either turned into a user's personal opinion, or additional facts add up and the original source is being lost, but the damage is already done.

2.2 Regulatory approaches to disinformation in EU Member States: France, Germany, and Hungary

After providing information regarding the possible consequences of disinformation posts in the previous chapters, it is vital to understand how the states are dealing with disinformation without any regulation or directive available, using only a self-regulatory Code of Practice. Three countries with different approaches may be used here as examples. The following chapter will focus on the explanation regarding legal approaches taken by the European Union countries.

The first country to take into consideration is France. Even though France has implemented various legal documents to fight against disinformation, they have proved to be inefficient enough (Boring, 2019). There is the 1881 Law on Freedom of Press, which forbids the disturbance of public peace through dishonestly issuing, spreading, or copying disinformation, and the Electoral Code in action, which forbids the spreading of disinformation that may affect election results (Boring, 2019). However, this has been considered incompetent enough to battle disinformation, especially during the times of elections, so the amended version provides a set of rules for major online platforms to follow for the duration of three months before the general elections, where there is a requirement for transparency regarding the authors of such posts and the amount of money spent (Boring, 2019).

There is an additional specification that during this three-month period, a judge may order to stop the spreading of deceptive information online and, additionally, any person can forward to the judge a case involving disinformation and expect a response within 48 hours (Boring, 2019). Moreover, the legislation also requires major online platforms to apply certain measures which would allow users to tag false information and prevent it from spreading to not affect the public order, or the outcome of the elections and even television broadcasting services which are under the control of foreign governments can be deferred for providing disinformation on purpose (Boring, 2019). As can be seen from the above, France's main goal is to stop disinformation mainly from affecting democracy and elections.

The second example is Germany. Since in the internet era, all information is available to users online via portals, social media platforms, and similar, it is considered to be a good start to make such platforms liable for the content posted by a person who uses such a commodity. Germany has implemented a law precisely for such purposes. The Network Enforcement Act imposes great fines on social media platforms which have more than two million users for not removing unlawful posts (Nunez, 2020, p. 796). However, the law was not considered an ideal solution, as even the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression indicated that social media platforms may remove content from the platforms not because it is unlawful, but rather out of fear of being fined (Nunez, 2020, p. 796). Nevertheless, this law was introduced by Germany to limit the spread of false news since users see great potential in social networks to do so without the danger of being caught (Andorfer, 2018, p. 1426). Even though this law is under criticism for limiting and having a crucial impact on the freedom of expression, it is stated by defenders of

the law that this is not a new step, rather it simply forces social media platforms to follow the already existing rules regarding hate speech and incitement in Germany (Andorfer, 2018, p. 1426). In simpler terms, this law is connected to defamation, in which the said words could affect a person's reputation (Gesley, 2019). Another angle, which is the media law, states that the information and communication services which provide journalistic content should ensure that the basis and trustworthiness of a news source are confirmed by the provider before it is communicated to the wider public (Gesley, 2019). The third point is that service providers are not liable for the content posted by users, however, once they have become aware of the illegal manner of the content or have been notified regarding this, the content is taken down (Gesley, 2019). So, according to the above explanation, Germany has not introduced a new law, rather the existing ones were grouped under the same Act to make online space cleaner and safer, not only before and during elections, but at any time. However, even though here the legal grounds are understandable, the chance of being censured by social media platforms is quite high. It is indeed easier for a platform to take down dubious content rather than actually determine if it breaks the law, which is far from an ideal solution against disinformation.

The final example considered here, Hungary, responded specifically to disinformation flowing around the virus, and passed the bill which allows the government to punish those who intentionally disseminate false information that may affect the government's steps in fighting the pandemics with prison sentences (Carson & Fallon, 2021, p. 34). However, this was not accepted without criticism. Opponents expressed fear that the bill will allow punishing anyone who will express disapproval of the government (Carson & Fallon, 2021, p. 34). This is the third approach, connected to health measures, while the other two were concerned with either elections or hate speech and defamation. Such dissimilar approaches demonstrate how differently countries react to disinformation, and how vital it is to have a common path for the entire European Union.

3. Steps to battle disinformation globally and by the EU

After looking into the definition and classification and initiatives adopted by the states to battle disinformation, the following chapters will be understood and examined as steps taken globally and by the European Union to

address the phenomenon of disinformation. The first document is the Joint Declaration, followed by the Code of Practice. The latter document will be assessed through criticism, and reports from social media platforms will be presented to provide understanding regarding the implementation of the document into the daily operations of platforms.

3.1 The first global steps to battle disinformation: Joint Declaration on Freedom of Expression and “Fake News”, Disinformation and Propaganda

The Joint Declaration is considered to be the first and global response to disinformation, which is why certain background information is needed to gain full understanding of the first actions taken to battle the phenomenon. The Declaration specifies the standards of human rights that shall be taken into consideration while taking any action to fight against disinformation (as cited in Goldberg, 2018, p. 424). The Joint Declaration on Freedom of Expression and “Fake News”, Disinformation and Propaganda specifies that the definition of disinformation should not be focused on using falseness criteria (Francis, 2018, p. 105). Falseness criteria can be quite indefinite and prone to change after certain facts become available (Francis, 2018, p. 105).

The Joint Declaration (2017, pp. 2–3) sets quite high protection on freedom of expression, specifying in the General Principles section that states may impose restrictions only if this is prescribed by law, in pursuit to achieve a legitimate interest, which shall be acknowledged under international law, and such steps are obligatory and balanced to protect the mentioned interests. Additionally, protection is provided for intermediaries and the individuals who were merely reposting or promoting the content of which they are not the authors (Joint Declaration, 2017, pp. 2–3). The intermediaries can only be held liable if they were aware of the content, intervened, or refused to take it down (Joint Declaration, 2017, p. 2). Severe measures, such as blocking of entire websites, IP addresses, and similar steps, are completely forbidden unless it is provided by law and is required to protect other human rights or legitimate public interest (Joint Declaration, 2017, p. 3). Any severe restrictive measures should be used in the last instance, only if other, less intrusive possibilities have been exhausted.

Moving forward, the intermediaries should adopt clear policies regarding restricting third-party content (Joint Declaration, 2017, p. 4). Those policies should be understandable and accessible by users, so it would be possible to actually acknowledge on which grounds the posted content may be taken

down. However, this would not be done without any notice to users; on the contrary, users shall be notified in an unambiguous way why a post was taken down and the users will be allowed to oppose such measures (Joint Declaration, 2017, p. 4). The final part is a proposal for all relevant stakeholders to support self-regulation and continue to demonstrate how disinformation and propaganda affect different rights (Joint Declaration, 2017, p. 5).

The Joint Declaration can be considered a solid ground for moving further. While the topics are touched upon in a quite general manner, it grasps the most topical ones and leaves stakeholders to consider the self-regulatory tools based on them. The Declaration mentions the need to look at the subject from a human rights perspective, brings attention to disinformation and propaganda, does not support harsh methods, and encourages further development.

3.2 The second step to battle disinformation on the European Union level: Code of Practice on Disinformation

In 2018, the European Commission brought to life the Code of Practice on Disinformation, which is a self-regulatory document to be signed freely by digital platforms, advertisers, and the advertising industry (Durach *et al.*, 2020, p. 10). This was the most logical and synchronized attempt to tackle disinformation, which includes working with major content platforms and the advertising industry (Pielemeier, 2020, p. 931). The industry agreed out of free will to follow self-regulatory standards to address disinformation, which had never before been the case.

In the Preamble to the document, there is a specification of what is considered to be disinformation. The Commission together with the High-Level Expert Group defined this phenomenon as unarguably wrong or deceiving information which was created to receive monetary gain or with the direct purpose to mislead the public, with the possibility to cause public harm (European Commission, 2018, p. 1). The Code provides that there is a great amount of false information spreading in the online environment, and to promote further principles of democracy, a balance must be struck and a possibility reached to spread legitimate content (European Commission, 2018, p. 1). Since each signatory party plays a different role, there is a possibility to accept only certain commitments, and the document does not need to be implemented fully (European Commission, 2018, pp. 2).

The main goals to achieve by the Code of Practice were related to making advertising clear and free of disinformation; stopping accounts which actively post false content; making posting of political ads more coherent for users; empowering consumers with tools provided for reporting disinformation and data for researches for further development (Plasilova *et al.*, 2020, pp. 28–29). In order to promote posting ads without disinformation, the parties of the Code shall develop methods which may include actions like using brand safety tools and cooperation with verification companies (Plasilova *et al.*, 2020, pp. 28–29). Political advertising shall be unambiguous and may include the identity of a person who paid for such ad and the amount spent; however, the balance shall be achieved between the need for transparency and other human rights (Plasilova *et al.*, 2020, p. 30). Additionally, information shall be provided regarding policies connected to the unallowable use of bots and such data shall be promoted and openly provided for users and the signatory party shall be educated further regarding what disinformation is and what consequences it may bring (Plasilova *et al.*, 2020, pp. 30–31).

3.2.1 Pros and cons of the Code

However, even with the list of established goals, there are major flaws in the Code of Practice. One of the points expressed by the critics is that self-regulatory tools are not sufficient enough to face disinformation issues (Fink & Gillich, 2020, p. 274). Member States will implement measures differently in their own countries, which may lead to a lack of harmonization at further stages (Fink & Gillich, 2020, p. 274). The Code of Practice is a voluntary document, and parties and platforms may not take into consideration the provided guidance and follow their own principles and rules.

The Sounding Board, which was involved in the creation of the Code of Practice, provided their own critical view on the Code of Practice, mentioning the lack of coherent and substantial commitments and no enforcement tools (as cited in Nenadić, 2019, p. 10). It was stated by the Board that due to the voluntary status of the document, there are no transparency obligations and cannot be any enforcement mechanisms implemented to share information and track progress (Dittrich, 2019, p. 4). Without this, the Code of Practice would not provide any visible results.

Furthermore, from the provided reports by social media platforms, there are issues with all the established goals. Regarding the placement of ads on the platform, then even though the platforms reported the existence of brand safety tools, there are still weak spots in the identification of sources of

disinformation and creating indicators for honest media sources, some of the established goals are not strictly related to the spread of disinformation, and due to that the objectives become vague and mixed (European Commission, 2019, p. 5). Touching upon the topic of political advertising, political ads were not in all cases correctly labelled, which means that the archives and the amount spent on political ads is not up-to-date and cannot be trusted (European Commission, 2019, p. 7). Not only that, but the possibility to look through the archives is quite limited and some information regarding advertising is not fully accessible, which makes such tools useless (as cited in Nenadić, 2019, p. 11). The points connected to consumers and the research community are being developed at a slower pace and require severe attention in the future (European Commission, 2019). Additionally, it was established that the reports lack harmonization and do not allow to actually check the progress and understand if a situation was changed due to the Code of Practice, which is a vital point for non-signatory parties, but no factual details or templates were proposed by the signatory parties in order to adjust reports and reach the full potential (Plasilova *et al.*, 2020, p. 33). If other non-signatory parties will not be able to compare the situation before and after the implementation of the Code of Practice, the document will not be signed by other platforms. It is vital to bring the Code of Practice to stakeholders, since major platforms are the ones who shape public opinion and filter out other ideas (de Cock Buning, 2018, p. 32). If the platforms follow the Code of Practice, the dissemination of disinformation will be put to a stop and any misleading posts for monetary value will be banned, but this still requires addressing the lack of coherent, clear, and non-discriminatory points in the Code of Practice (de Cock Buning, 2018, p. 32).

On the other hand, it was concluded by the stakeholders that the Code of Practice is required due to disinformation still being a major problem (Plasilova *et al.*, 2020, p. 3). The Code itself allowed starting a dialogue regarding disinformation, brought attention to the seriousness of the topic, and provided stakeholders and signatory parties with guidance (Plasilova *et al.*, 2020, p. 3). The Code of Practice makes the parties to be creative, monitor with tools the spread of disinformation, and take certain actions to bring truthful information to the surface.

3.2.2 The efficiency of the Code and reports of major platforms

After a twelve-month period, the signed parties submitted reports regarding the implementation of the practices from the Code (European Commission, 2019, p. 1). Major social media platforms, such as Facebook and Twitter, were

taken into consideration. Several points from the reports will be specified in order to show how well the platforms adjusted their policies and what steps were taken to promote cleaner online environments.

The first point concerns ad placements. Facebook (2019, p. 2) implemented Advertising Policies, according to which advertisements would be reviewed and posted on the Facebook platform only if they are in compliance with the policies. During the analysis, every aspect of the advertisement, such as images, text, and similar points, is checked and the ads may not be granted the status of approval if the page is not functional, if there are discrepancies between product or service and the page, and if the page simply does not obey advertising policies (Facebook, 2019, p. 2). Twitter (2019, pp. 2–3) implemented a certification process, which consists of different points, for example, for organizations or candidates to submit verification documents in order to provide proof of identity and location. This way, an intervention from foreign states and actors shall be avoided (Twitter, 2019, pp. 2–3). Twitter also implemented an Advertising Policy with a list of information specifying what will be considered inappropriate content; additionally, certain checks and reviews will be done for advertising accounts before the ads will be visible to a wider public (European Commission, 2019, p. 3). The policies contain more or less similar information regarding the content that will not be posted on the platforms.

The second point was related to political and issue-based advertising. On Facebook now, political ads shall be labelled with a specified disclaimer “Paid for by” (European Commission, 2019, p. 5). Several points are checked before the approval—“page or organization’s name; website; email address; phone number; and address” (Facebook, 2019, p. 3). Not only that, but Facebook also has an Ad Library, containing all the ads saved with information regarding how much was spent on the ad and which population (age and gender) was reached (European Commission, 2019, p. 6). Twitter (2019, pp. 10–11) expanded the Political Campaigning Ads Policy, which allows users to see details such as by whom the ad was purchased, and by which candidate or party. The above cases suggest that such major platforms now require political ads to be tagged as a sponsored content and have a disclaimer specifying who is paying for this ad and who is targeted (European Commission, 2019, p. 7).

A further point is the integrity of services, which should not be manipulated or used for abusive conduct (European Commission, 2019, p. 8). Facebook (2019, pp. 6–7) has a range of policies implemented for creating a safer

environment. Twitter (2019, p. 14) is specifically focusing on spam and similar actions which may prevent public conversation to happen. Not only have they created the Election Integrity Policy to stop the exploitation of services for harming elections, but they have also established a reporting feature for users, so that it would be easier to report misleading tweets connected to voting or tweets which have spam (Twitter, 2019, p. 14).

Giving more power to consumers is another point to take into consideration. Facebook provided information to users, and not only that but also a tool “Why am I seeing this post?” and a possibility for users to modify their own news feed (European Commission, 2019, p. 9). Twitter (2019) also helps users find appropriate information by providing direct links to mental health resources and forms to fill to receive help when users search for information connected to self-harm and suicide, trustworthy resources appear when users search for vaccine- or disease-related questions, and many more hashtags with direct and credible information regarding certain events. Additionally, all specified platforms provide specific tools for researchers and the fact-checking community to access platform data (European Commission, 2019, p. 12).

One of the breakthroughs for the Facebook platform was the establishment of the Facebook Oversight Board. Due to an excessive amount of users and posts being reported against Community Standards, there is a need to have decisions regarding such behavior coming out as efficiently as possible (Douek, 2019). One of the goals of the Board is to provide users a possibility to submit a request for a review of the deleted posts or of the ones submitted to Facebook for review (Klonick, 2020, p. 2463). The decisions are publicly available and are stored in the database (Klonick, 2020, p. 2474). The Board consists of people of different backgrounds, which will allow decisions regarding the content to be addressed attentively and on a human level, each member bringing their own experience to the final decision. This is a bonus due to the fact that artificial intelligence may mistakenly take down content that was not false, whereas a human would be able to understand if the data is misleading or just satirical. The decisions will be binding for Facebook and shall follow the goal to promote free expression. Since the decisions are also publicly available, Facebook tends to be clear regarding the steps taken and allows users to feel welcomed on the platform. One of the recent case examples is connected to overruling Facebook's decision regarding posts with data about the existence of COVID-19 cure and France's health strategy (Oversight Board, 2021). It was specified by the Board that the “misinformation and imminent harm rule” in Community Standards

is unclear and not in compliance with human rights and a new guide shall be created specifically for health misinformation (Oversight Board, 2021). The post itself did not urge readers to buy medicine and apply it without prescription, so there was a possibility for Facebook to pick a less intrusive method, such as provide additional information, but the company failed to use it (Oversight Board, 2021).

However, after all the steps taken by the platforms based on the Code of Practice, the desired result was not achieved. It was stated by the Commission and High Representative of the Union for Foreign Affairs and Security that measures taken by platforms were far from being effective (Carrapico & Farrand, 2021). An activist group, Avaaz, mentioned that there is still a great number of groups and pages on Facebook which post information against European Union and which are being followed by an excessive number of people (Shackelford *et al.*, 2020, p. 1788). From the provided reports from social media platforms, there is still a need for further development in identifying the actors behind the disinformation and sharing information with the research community (Durach *et al.*, 2020, p. 11).

Furthermore, the Code of Practice highlights the need for a balance between diminishing the amount of disinformation to allow freedom of expression to flourish and open internet, but there is a lack of measures to achieve such balance (Saurwein & Spencer-Smith, 2020, p. 835). Also, the Code of Practice and the Electronic Commerce Directive seem to collide, since the Code of Practice provided platforms with a requirement to moderate content, but if intermediaries are under the obligation to moderate data, they will be aware of the unlawful nature of the content and will not be under the protection of the Electronic Commerce Directive (Saurwein & Spencer-Smith, 2020, p. 836). Such clash with other European Union documents reduces the efficiency of the Code, however, it was mentioned that the Digital Service Act may rectify the issue by providing protection to intermediaries for proactive monitoring (Saurwein & Spencer-Smith, 2020, p. 836). The Digital Service Act is a new combination of rules for a safer online environment that will cover the entire European Union and will allow amending the Electronic Commerce Directive (Elvinger Hoss Prussen, 2021). This will be further addressed in the solution given in the chapter on liability perspective.

Thus, as can be seen, there are good points, such as labelling posts and marking them as false, but, at the same time, there are points which still need further attention. Social media platforms tend to delete health-related information which protects the users, but with the rapid creation of bots

and similar pages, the issue of disinformation is still present. The Code of Practice refreshed the users' understanding regarding the seriousness of disinformation issues, but it still requires further development to fully reduce the number of misleading and fake posts. The results are quite mixed, and even though the Commission stated that the outcomes of the Code of Practice are not high, it still puts pressure on the platforms to deal with disinformation. There are goals set up by the Code of Practice, but no steps or understandable paths are proposed on how to reach them.

To sum up and point out areas for further development and improvement, the terminology issue is the first one to pay attention to (Plasilova *et al.*, 2020, p. 34). With a clear definition and clarification regarding the vital points, it would be easier to understand and stick to the commitments provided in the Code of Practice. The second point is to implement a certain mechanism if the signatory parties do not comply with points provided in the Code of Practice (Plasilova *et al.*, 2020, p. 34). Currently, the progress of the parties can be checked in the reports, however, there are no penalties if some actions are not taken into consideration, are missed, or misused. This shall be improved, so the already existing parties and newly signed ones will take the Code seriously. The last point is the approach of the Code called "à la carte", where signatory parties can pick some commitments and follow them, but not sign up for others (Plasilova *et al.*, 2020, p. 34). Either this should be changed and the Code of Practice should be allowed to be accepted fully, or the accepted points shall be drafted in a more general manner to fill the required information for a successful implementation of the document.

3.2.3 Disinformation during a pandemic outbreak

During the global COVID-19 pandemic, a massive amount of false and misleading information appeared on the surface (European Commission, 2020a, p. 1). Social media platforms provided a response to such major issues as well based on the European Commission Communication on COVID-19 disinformation. Facebook took several steps to tackle disinformation related to the pandemic and to provide users with correct information, which would not be harmful in any way. Facebook (2020, p. 2) partnered with the health authorities, which include the WHO, UNICEF, and the European Centre for Disease Control organizations, to be able to provide users of the platform with up-to-date information regarding the disease by redirecting anyone who was searching for COVID-19 related news. Just the way disinformation has been battled before, the COVID-19 related news is revised in the Community Standards, in which incorrect and harmful content, such as speculations

about the reality of the disease, vaccination, and 5G connection to COVID-19 is being removed. Once the content is removed, the user is provided with the data regarding why this was done; the posts that do not lead to harm in reality but which were marked as false by fact-checkers will appear less frequently and come with a warning label, so that the number of people who will see it was not large or the users would be able to understand based on the label that the information may not be trusted; further empowerment of fact-checkers; providing funding to researchers; launching campaigns to educate users; inserting labels on state-controlled news; specific attention was provided to advertisements and banning the ones that are for selling masks, sanitizers, and similar goods. (Facebook, 2020, p. 12) Facebook took great steps to actually make the platform comfortable and useful during the pandemic period.

Twitter made similar changes to their platforms. Some differences from Facebook were that Twitter has an Events Page, which provides tweets from various trustworthy sources in local languages; different hashtags, and campaigns to wear masks and wash hands (Twitter, 2020). But looking through the provided report, the actions were more or less the same by both platforms, which is a good step further and shows the commitment of major platforms to fight against the phenomenon of disinformation during difficult times and to protect users, who under pressure may make uninformed decisions based on misleading content.

4. Possible solutions from several areas of law

Having gone over the issues surrounding the definition and approaches proposed globally and by the European Union, this chapter introduces solutions to fight against disinformation in a more coherent manner. Previous criticism shall be taken into consideration as well. The results will be introduced from the perspective of a Regulation, human rights, liability and definition.

4.1 Solution from the perspective of a Regulation

One of the main points of criticism is the voluntary approach of the Code of Practice. It was mentioned above that a regulatory path may be taken into consideration if the Code of Practice will prove to be insufficient enough. The first subchapter will go over the attempts to create a common Regulation.

The first attempts to actually regulate disinformation were made a long time ago, specifically with the International Convention Concerning the Use of Broadcasting in the Cause of Peace of 1936 (Fink & Gillich, 2020, p. 266). This convention was implemented to prevent the spread of political propaganda; the parties to stop the spreading of any incorrect information and checking such data before broadcasting (as cited in Baade, 2019, p. 1365). However, such a convention can be hardly applicable today for the reason of some disinformation cases not falling under international and incorrectness criteria, which play a vital role in Article 3 of the Convention (Baade, 2019, p. 1369). Not that many states ratified the Convention, and a preferable solution would be reached with an up-to-date document, which would take into consideration new technologies and modern issues.

Drafting such legal documents requires a legal basis in the European Union treaties. The Treaty on the Functioning of the European Union (TFEU) provides in Articles 2 to 6 a list of competencies of the European Union; however, there are no specifications regarding the possibility to regulate free speech. The only possible way out is the harmonization clause in Article 114 of the TFEU (Fink & Gillich, 2020, p. 275). However, this Article discusses the internal market and free movement of products. There are two ways in which disinformation can be associated with such Articles: disinformation posts as goods or false advertising threats.

First, there is a need to understand the definition of goods. Even though the EU treaties do not provide any definition, it was defined by the Court of Justice of the European Union as products evaluated for money and forming a part in commercial transactions (Cuyvers, 2017, p. 327). When disinformation posts are created, one of the goals which their authors follow is to receive monetary gain. The more clicks a post gets, the more money the authors receive. As the definition of the Court of Justice of the European Union suggests, payment for goods is a crucial part. If disinformation will be indeed understood as goods and will be regulated from this point of view, it will allow the European Union to penalize harmful products.

Additionally, disinformation can be looked at from the aspect of false advertising as well. According to Directive 2006/114/EC (2006), misleading advertising can be considered as any possible advertising which may deliberately make persons believe in something that is not true and, as a result, influence their economic behavior or harm a competitor. Fake articles, miracle products can all be misleading advertising for goods that can negatively affect readers and consumers, even injure some or be the cause of death. In order to regulate disinformation, proof has to be provided, since because of the rapid spread of disinformation, the marketplace will no longer be active and will simply collapse (Waldman, 2018, p. 863).

Having said that, the approach based on the regulation is being criticized for being the start of censorship and limitation on other human rights, such as freedom of expression (Durach *et al.*, 2020, p. 12). Although, based on recent examples related to the virus, understanding of the phenomena of disinformation needs to be re-evaluated. When human life is at stake, intervention in the form of regulation seems like the most valuable option. Even though major social media platforms delete fake accounts, strike them down, provide truthful information by adding filters, labels and tags, the people behind such campaigns will not be penalized. The pandemic situation specifically provided examples regarding how people received emails or came across advertising posts about hand sanitizers and face masks, which would only steal money from such customers and send them no or useless products (Read, 2020). This is false advertising combined with harmful goods which can be a point of departure for further classifications of disinformation.

If misleading posts are connected to goods and a regulatory approach will be taken into consideration for disinformation, this will at the same time protect consumer rights and affect all the states in the European Union. The European Union states would not be under pressure to regulate posts with disinformation personally, with some states taking a soft approach, while others being silent in general. A Regulation would apply rules across all the states, making the solution affordable and without patchwork.

4.2 Solutions from a human rights perspective

Several human rights—specifically, freedom of expression, prohibition of abuse of rights, the right to know, and the right to truth—may offer a solution from their perspective. Below, an explanation will be given to all the mentioned rights and whether any of the rights provides an alternative to regulate disinformation.

The first is the right to know. The right to know is mentioned on several occasions in different contexts. The so-called mentioning of the right to know is present in the Directive on Freedom of Access to Environmental Information. According to the Directive, Member States should ensure that “public authorities make information on the environment available to any person at his request, and without his having to prove a legal interest, or explain why he wants the information” (Wheeler, 1994, p. 1). However, this right is connected purely to environmental issues. Not only is this right tackled in the above Directive, but also in Article 33 of the European Registration, Evaluation, Authorization, and Restriction of Chemicals Regulation, wherein it is specified that “a supplier has to inform a professional recipient automatically and any customer on request whether a product contains a critical substance” (Rolke *et al.*, 2019, p. 172). Furthermore, the Restriction of Hazardous Substances Directive not only requires specifying what substances there are in the electrical and electronic merchandise but also bans the marketing of a device (Rolke *et al.*, 2019, p. 172). So, as the examples seem to indicate, such a right is being used mostly in connection with environmental issues or dangerous goods.

From another perspective, the right to truth is connected to the states' obligations to make available the information regarding gross violations of human rights (Baranowska & Gliszczyńska-Grabias, 2018, p. 97). A mention of that can be found in Article 32 of the Additional Protocol of the Geneva Convention (Baranowska & Gliszczyńska-Grabias, 2018, pp. 97–98). To be more precise, Article 32 of the Additional Protocol of the Geneva Convention (1977) states that a family should know the fate of own members. In the study conducted and published by the High Commissioner of Human Rights regarding the right to truth, there are two aspects in this right—individual and collective (Baranowska & Gliszczyńska-Grabias, 2018, p. 98). The individual aspect is connected to being aware of human rights violations and what happened to the victim, while the collective aspect is connected to the right of a society to be aware of horrible crimes and the steps that lead to them (Baranowska & Gliszczyńska-Grabias, 2018, p. 98). This right is related to historical events and cannot be applied to the phenomenon of disinformation.

It was stated that the right to truth has a certain connection with Article 13 of the European Convention on Human Rights, which is known as the right to an effective remedy. This Article states that not only shall an effective remedy be guaranteed, but in case of severe violations also the public authorities are required to go through a full investigation process and reveal the truth behind

violations (Antkowiak, 2002, p. 982). Additionally, both Article 2, which is the right to life, and 3, which is prohibition of torture, from the mentioned Convention may imply that if investigation was conducted poorly and truth was not revealed behind killings and torture, there was a violation of human rights (Antkowiak, 2002, p. 982). Also, the right to truth has an influence on Article 3 of Protocol 1 of the same Convention, which is connected to free elections (Mastroianni, 2019, p. 45). To exercise such a right, people shall be well informed regarding the candidates, but such a right is under threat if information circulating around elections is fake. However, there are no direct mentions of the word 'truth' in the specified Articles.

Another possibility is to look at the issue from the perspective of freedom of expression. If we take into consideration Article 10 of the European Convention on Human Rights, specifically the word 'truth' or any similar wording is not present there. In 2006, Article 10 was given a broader meaning which also entails the right to have access to information (Mazur, 2018, p. 185). There are four points that determine what qualifies as the right to access information: a person's right to receive and communicate data, fulfilling of public interest test, providing the received information to the wider public, and making such data ready and accessible (Mazur, 2018, pp. 185–186). Through access to information, freedom of expression constitutes a vital part of the development of democracy by allowing “‘freedom of political debate’ and ‘pluralism, tolerance, and broadmindedness’” (*Handyside v. The United Kingdom* [1976] cited in Francis, 2018, p. 104). However, an accurate political perspective would not be possible if the information is not up-to-date. Nevertheless, the Article has specific limitations, upon which the rights can be limited. Being prescribed by law is linked to the need of actual law, so that the conduct of citizens can be shaped accordingly (Francis, 2018, p. 105). This point cannot be achieved while there is no clear definition of disinformation. An attempt to regulate disinformation under the other points reveals that public interest or the rights of individuals are not broad enough to capture disinformation; and as to the last point, the government is under an obligation to provide cases that such expression is planned to encourage violence (Francis, 2018, p. 106).

If not the freedom of expression, then Article 17 may provide a solution, since this Article is considered to be general. Disinformation affects freedom of expression, violates free elections, however, it still does not seem to be as disastrous as required by the above-mentioned Article (Francis, 2018, p. 107). Considering a previous decision under Article 17, it is clearly evident that the Article is applicable only if

the aim of the offending actions must be to spread violence or hatred, to resort to illegal or undemocratic methods, to encourage the use of violence, to undermine the nation's democratic and pluralist political system, or to pursue objectives that are racist or likely to destroy the rights and freedoms of others. (*Lehideux and Isorni vs. France* [1998] cited in Keane, 2007, p. 648)

However, the applicability of this Article shall be under strict observation (*Lehideux and Isorni vs. France* [1998] cited in Keane, 2007, p. 649). As specified in the *Lehideux* case, the Court does not use Article 17, but rather requires the interference to be in accordance with Article 10, paragraph 2 (Keane, 2007, p. 656).

Taking into consideration Article 19 of the International Covenant on Civil and Political Rights, which can be considered one of the core treaties in the United Nations Human Rights institution and which allows international and high standard protection of free expression, it also has a responsibility to fulfil a three-step test in order to limit freedom of expression (Aswad, 2020, pp. 1013–1014). Being provided by law requires precision, but in the case of disinformation, the terminology is unclear (Aswad, 2020, pp. 1014–1015). The second point is to prove that the limitation chosen is the least intrusive in achieving public interest goals and if it is possible to achieve the same goal without the restriction, which requires certain checks on government actions, and which other solutions were implemented before completely restricting free speech and what were the outcomes (Aswad, 2020, p. 1016). The final point is whether this is a legitimate intervention (Aswad, 2020, p. 1017). Even though actions shall be weighted against the three-point test, it shall be taken into consideration that freedom of expression is a cornerstone to many rights, and leaving issues of disinformation without a solution is also not an appropriate path (Anansaringkarn & Neo, 2021, p. 5). In case of disinformation, many of the mentioned rights are being violated, among them Article 17 of the International Covenant on Civil and Political Rights, since it is connected to the right to privacy, which can be violated if personal data of users is available and disinformation posts are being sent directly to users (Pamment, 2020, p. 6). In case of disinformation, as can be seen above, this is not just a violation of expressing oneself and receiving information, it is also putting all other rights in danger of being breached.

Still, filtering out disinformation by limitations to freedom of expression can prove quite a troublesome path. However, if we were to develop the right to know further, not only leave it at the level of the environment and goods but

also consider the need to receive appropriate information in order to maintain other human rights, then disinformation can be given new limitations. Fake information, for example, may reduce the right to peacefully protest, since both sides of the conflict may specify incorrect information regarding how many people came, compromising such events (Civicus, 2017). If readers receive incorrect numbers, locations, and what the protest is connected to, then the whole idea behind such gatherings will be lost and violates the principles of democracy. Additionally, disinformation can be as harmful as the chemicals which are shared with customers according to the Regulation mentioned at the beginning of the chapter. Advertised fake products for curing diseases can be harmful and fatal to people, which is why waiting for truthful information to prevail shall not be an appropriate point of view. The right to know information is required and needs to be promoted further.

4.3 Solutions from the perspective of liability: changes in the liability and role of internet intermediaries

Internet intermediaries do not impose liability regarding the content that is published by users. In case there is a notice of certain unlawful content on the website, the reaction will occur only at that moment and the content will be taken down. Nevertheless, if stricter liability is imposed on the intermediaries, it means that those platforms are now the ones who decide which information is correct and which is not (Sugow, 2019, p. 37). Not yet having a clear definition, this will put the intermediaries under pressure and will lead them to take down all the potential content that even remotely resembles disinformation. This will lead to censorship of users, who may then leave the platform.

However, the main question is whether it would be even possible to impose liability on the intermediaries when they are protected by law. In the US, Section 230 of the CDA protects intermediaries from liability, yet, in the case of *FTC v. LeadClick Media*, the section did not provide any immunity to LeadClick Media (Vojak, 2017, p. 156). LeadClick Media “operated an affiliate-marketing network to provide advertising in internet commerce by connecting [its merchant clients] to third-party publishers-affiliates who advertised the merchant’s products” (*Federal Trade Commission v. LeadClick Media* [2016] cited in Vojak, 2017, p. 156). The third-party publishers would create fake sites where genuine reporters talked about weight loss products and how healthy and good they are, plus comments from other people who used those products and reported their results, but

all this information was fabricated (Vojak, 2017, p. 156). The Court did not provide immunity to LeadClick Media under Section 230 of the CDA and considered the intent, content, and effect that the speech had (Vojak, 2017, p. 157). It was understood by the Court that there was an intent to bewilder, the content was clearly deceitful, and the goal was to deceive users (Vojak, 2017, p. 157).

While the above case took place in the United States, it is vital to understand the situation in the European Union. There are states which have imposed liability on internet intermediaries. One of the illustrative examples is Germany with the Network Enforcement Act, which allows enforcement of penalties on social media outlets for not withdrawing illegal content (Shattock, 2020). Considering the European Union generally, there is the Electronic Commerce Directive that protects internet intermediaries under the categories of mere conduit, cache and hosting, but still draws attention to such companies for illegal content posted online (Shattock, 2020). However, disinformation cannot be considered illegal content as such; it does not allow regulating posts under the mentioned Directive, leaving them in the grey zone (Shattock, 2020).

A sufficient development in this area is represented by the Digital Service Act. The Act suggests a horizontal framework to regulate, put responsibility and clearance requirements on the online environment (Communication COM/2020/790 final). Platforms will be faced with greater responsibility regarding moderating the content, advertising and algorithm processes and major online platforms will not only evaluate risks connected with “illegal content and products”, but also risks connected to “fundamental rights, public health and security” (Communication COM/2020/790 final). Among other things, the Act provides opportunities to create a cleaner and safer online environment by not only empowering users, but also requires that the platforms adjust measures via which it would be possible to flag unlawful content; identify users who are dealing and marketing unlawful goods; provide users with a possibility to challenge moderation decisions; put a stop to exploitation of the system; provide researchers with required data regarding the functionality of the platform; and several other obligations which are quite similar to what platforms were doing based on the reports above (European Commission, 2021). Regarding the liability, internet service providers can still be excluded, but several additional points were added, specifically requirements for internet service providers to solve complaints in line with rules in the Digital Service Act and create complaint handling procedures (Meneghetti & Anderson, 2021). It is also encouraged to

create codes of conduct which shall be identified by the new legal document (Proposal COM/2020/825 final). Disinformation still poses great risks to the society and democracy, such self-regulatory and co-regulatory approaches are required to further limit the dissemination of illegal content (Proposal COM/2020/825 final).

In terms of new documents, online platforms are now facing responsibilities connected to the content stored on websites. If the online platforms do not follow the rules, a penalty will be imposed on them, which can be considered as an additional motivation to follow the guidelines. Currently, such an outcome may be considered one of the suitable options, since not only will online platforms be actively monitoring content and imposing mechanisms to clear out misleading posts, it will be also beneficial for users and the online environment.

4.4 A solution for finding an acceptable definition

To regulate something by law, the phenomenon has to be described precisely and without any vagueness. It can be quite difficult to define disinformation. As seen from the definitions provided above, the vital point of any understanding behind disinformation is intent. There may be a list created with certain points that the Courts can go through to establish intent, such as monetary gain from the post, however, the situations are not always so clear and the steps taken require cooperation to come to a logical consensus. Secondly, there may be issues with defining to whom those posts are applicable. Identifying harmful impacts and which groups the news are targeted at may prove complicated.

To come up with a precise definition, the boundaries should be quite limited and the definition should not be touching upon other possible speeches that fall under freedom of expression. The points that can be taken into consideration is whether the speech is seeking monetary gain, how much false information does it contain, how many people have seen the news and to how many it should have been shown if there are similar posts like this, how truthful the speech is in presenting itself, the intent of the publisher, and which was its effect (Vojak, 2017, p. 153). Monetary gain will allow grouping posts containing disinformation which have received money specifically from clicks and the amount of attention received, which refers to the chapter regarding the categorization of such news as goods. The amount of false and correct information, however, has been pointed out as an inappropriate point of measure. It is vital not to focus on the falseness criterion, since this

may change when new information becomes available (Haiden & Althuis, 2018, p. 5). The intent of the publisher will allow determining if a post was made just for fun or with a malicious aim to cause chaos.

As far as the Act implemented by Germans is concerned, it was specified that illegal content shall be removed from the platforms, but as there is no clear understanding or definition regarding what illegal content means, social media platforms are required to refer to the Criminal Code (Gesley, 2019). However, social media platforms, due to high fines, may ban any content which even slightly resembles illegal information. This can be considered the main issue of such legal documents. Every point needs special clarification. While the Code of Practice on Disinformation contains a mention of the definition of disinformation by the High-Level Expert Group, it was still mentioned that a mutual agreement between Member States will be reached regarding what is considered to be disinformation in order for actions not to contradict each other (Plasilova *et al.*, 2020, p. 32). The above points, in a way, may provide guidance for further codes of conduct.

Moreover, the European Democracy Action Plan, presented by the European Commission, introduces further steps provided to fight disinformation (European Commission, 2020b). Specifically, developing tools to fight foreign propaganda, aligning the Code of Practice with the upcoming Digital Service Act and further adjusting the Code of Practice and implementing the monitoring system (European Commission, 2020b). The Action Plan (2020) contains a vital requirement for distinguishing phenomena that are separate from disinformation to ensure a correct drafting of policies. Misinformation, disinformation, information influence and foreign interference were provided with a definition and having distinct policy responses was mentioned as an important point (Communication COM/2020/790 final). Not only shall a common definition be achieved, but also the need to have a clear and responsible digital system (Communication COM/2020/790 final). So, according to the points to define disinformation listed above, it is possible to come to a mutual agreement and specify the vital points in detail for future legal documents.

5. Conclusion

The phenomenon of disinformation is a complex issue. Disinformation consists of fake news, combining categories such as parody, bad journalism, misleading news, and fabrications. Disinformation may affect the relations between countries and violate certain human rights, which is why states in the European Union try to regulate such a phenomenon locally—Germany by penalizing social media platforms, France by paying closer attention to disinformation specifically during elections, and Hungary by regulating disinformation in relation to health actions.

Nevertheless, several steps have been taken by the European Union, but this can be considered only as a beginning. During the coronavirus pandemic, disinformation has been met with filtering and taking additional steps to fight back, however, there is still a long way to go. The main points of criticism from the reports have to do with the fact that signatory parties can voluntarily apply some points and leave others unnoticed; without monitoring mechanisms it is quite tedious to determine if the Code of Practice has resulted in any major changes; and without a mutually agreed definition, the limitations may apply unequally.

The authors proposed several solutions in the final chapter of the article. The solutions derive from different areas of law and can be combined for efficiency, including a proposal for a Regulation; the possibility to consider disinformation as goods and false advertising; to tighten the liability of social media platforms; to further develop the right to truth in order to avoid harmful posts and goods; to devise a definition based on monetary gain; identify the percentage of falseness, the number of people who checked a post and the amount that was required; intent; similarity to other publications and public reaction. Such solutions will be able to minimize the influence of disinformation and make the internet environment a cleaner and friendlier place.

Anna Kobernjuk is a master's programme student of law at Tallinn Law School, Tallinn University of Technology. She holds her first diploma in a technical field, specifically electronics and bionics, and a second diploma in European Union and international law. Anna has participated in the All-European International Humanitarian and Refugee Law Moot Court Competition. Her research focuses on human rights.

Dr. **Agnes Kasper** is a senior lecturer of Law and Technology at Tallinn Law School, Tallinn University of Technology. She holds diplomas in international business, law and management, and has also received formal training in the technical aspects of cybersecurity and digital evidence. Dr Kasper has served at embassies, human rights organizations and she was leading the legal department in an IT consultancy and development company. She has also acted in advisory capacity in consultations with governments on issues relating to cybersecurity, as well as been an external expert for the European Commission. Her current research focuses on the regulatory aspects of cybersecurity.

References

- Anansaringkarn, P. & Neo, R.** (2021), 'How can state regulations over the online sphere continue to respect the freedom of expression? A case study of contemporary 'fake news' regulations in Thailand,' *Information & Communications Technology Law*.
<https://doi.org/10.1080/13600834.2020.1857789>
- Andorfer, A.** (2018), 'Spreading like wildfire: solutions for abating the fake news problem on social media via technology controls and government regulation,' *Hastings Law Journal*, vol. 69, no. 5, pp. 1409–1432.
- Antkowiak, T. M.** (2002), 'Truth as right and remedy in international human rights experience,' *Michigan Journal of International Law*, vol. 23, no. 4, pp. 977–1014.
- Aswad, E.** (2020), 'In a world of "fake news," what's social media platform to do?' *Utah Law Review*, vol. 2020, no. 4, pp. 1009–1028.
- Baade, B.** (2019), 'Fake news and international law,' *The European Journal of International Law*, vol. 29, no. 4, pp. 1357–1376.
<https://doi.org/10.1093/ejil/chy071>
- Baranowska, G. & Gliszczynska-Grabias, A.** (2018), 'Right to truth and memory laws: general rules and practical implications,' *Polish Political Science Yearbook*, vol. 47, no. 1, pp. 97–109. <https://doi.org/10.15804/ppsy2018107>
- Boring, N.** (2019), 'Initiatives to counter fake news: France.' *Library of Congress Law*. Retrieved from <https://www.loc.gov/law/help/fake-news/france.php> [accessed 10 Feb 2021]
- Carrapico, H. & Farrand, B.** (2021), 'When trust fades, Facebook is no longer a friend: shifting privatisation dynamics in the context of cybersecurity as a result of disinformation, populism and political uncertainty,' *Journal of Common Market Studies*. <https://doi.org/10.1111/jcms.13175>

- Carson, A. & Fallon, L.** (2021), 'Fighting fake news: a study of online misinformation regulation in the Asia Pacific,' Report, La Trobe University.
<https://doi.org/10.26181/60640ea43558f>
- Civicus (2017), "'Fake news' violates citizens' right to be informed.' Retrieved from <https://www.civicus.org/index.php/fr/medias-ressources/112-news/2757-fake-news-violates-citizens-right-to-be-informed> [accessed 10 Feb 2021]
- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions On the European Democracy Action Plan, COM/2020/790 final, 3.12.2020.
- Cuyvers, A.** (2017), 'Free movement of goods in the EU,' in E. Ugirashebuja, J. E. Ruhangisa, T. Ottervanger & A. Cuyvers (eds.) *East African Community Law Book: Institutional, Substantive and Comparative EU Aspects*, Leiden Boston: Brill Nijhoff, pp. 326–344. https://doi.org/10.1163/9789004322073_021
- de Cock Buning, M.** (2018), 'A multi-dimensional approach to disinformation: Report of the independent High Level Group on fake news and online disinformation.' Retrieved from http://diana-n.iue.it:8080/bitstream/handle/1814/70297/DeCock_B_2018?sequence=1&isAllowed=y [accessed 21 Apr 2021]
- Directive 2006/114/EC of the European Parliament and of the Council of 12 December 2006 concerning misleading and comparative advertising (codified version) (Text with EEA relevance), *OJ L* 376, 27.12.2006.
- Dittrich, P. J.** (2019), 'Tackling the spread of disinformation. Why a co-regulatory approach is the right way forward for the EU,' *Bertelsmann Stiftung Policy Paper*, 12 December.
- Douek, E.** (2019), 'Facebook's Oversight Board: move fast with stable infrastructure and humility,' *North Carolina Journal of Law & Technology*, vol. 21, no. 1, pp. 1–78.
- Durach, F.; Bargaonu, A. & Nastasiu, C.** (2020), 'Tackling disinformation: EU Regulation of the Digital Space,' *Romanian Journal of European Affairs*, vol. 20, no. 1, pp. 5–20.
- Edson, C. T. Jr.; Zheng, W. L. & Ling, R.** (2018), 'Defining "fake news",' *Digital Journalism*, vol. 6, no. 2, pp. 137–153. <https://doi.org/10.1080/21670811.2017.1360143>
- Elvinger Hoss Prussen (2021), 'European Union: focus on European Commission's proposal for a Digital Services Act,' *Mondaq*, 2 March. Retrieved from <https://www.mondaq.com/media/1041478/focus-on-european-commission39s-proposal-for-a-digital-services-act> [accessed 13 Apr 2021]
- European Commission (2018), *EU Code of Practice on Disinformation*, Brussels. Retrieved from https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=54454 [accessed 10 Feb 2021]

- European Commission (2019), *Code of Practice on Disinformation. First Annual Reports – October 2019*, Brussels. Retrieved from https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62698 [accessed 10 Feb 2021]
- European Commission (2020a), *Coronavirus: EU strengthens action to tackle disinformation* [Press release], 10 June. Retrieved from https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_20_1006/IP_20_1006_EN.pdf [accessed 10 Feb 2021]
- European Commission (2020b), *European Democracy Action Plan: making EU democracies stronger* [Press release], 3 December. Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2250 [accessed 24 Apr 2021]
- European Commission (2021), *Europe fit for the Digital Age: new online rules for platforms*. Retrieved from https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment/europe-fit-digital-age-new-online-rules-platforms_en [accessed 20 Feb 2021]
- Facebook, Inc. (2019), *Facebook report on the implementation of the Code of Practice for Disinformation*, European Commission. Retrieved from https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62681 [accessed 10 Feb 2021]
- Facebook, Inc. (2020), *Facebook response to the European Commission Communication on Covid-19 Disinformation*, European Commission. Retrieved from https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=69158 [accessed 10 Feb 2021]
- Fink, U. & Gillich, I.** (2020), 'Fake news as a challenge for journalistic standards in modern democracy,' *University of Louisville Law Review*, vol. 5, no. 2, pp. 263–282.
- Francis, C.** (2018), 'Trial of truth: law and fake news,' *Edinburgh Student Law Review*, vol. 3, no. 3, pp. 100–113.
- Gelfert, A.** (2018), 'Fake news: a definition,' *Informal Logic*, vol. 38, no. 1, pp. 84–117. <https://doi.org/10.22329/il.v38i1.5068>
- Gesley, J.** (2019), 'Initiatives to counter fake news: Germany.' Retrieved from <https://www.loc.gov/law/help/fake-news/germany.php> [accessed 3 Apr 2021]
- Goldberg, D.** (2018), 'Responding to fake news: is there an alternative to law and regulation,' *Southwestern Law Review*, vol. 47, no. 2, pp. 417–448.
- Haiden, L. & Althuis, J.** (2018), 'The definition challenges of fake news,' King's Centre for Strategic Communications, Department of War Studies, King's College London.
- Info Ops Polska Foundation (2020), 'A short review of the infosphere-based information and psychological operations targeting relations between Poland and Ukraine.' Retrieved from <https://informnapalm.org/en/psychological->

- operations-targeting-relations-between-poland-and-ukraine/ [accessed 3 Apr 2021]
- Joint Declaration (2017), Joint Declaration on Freedom of Expression and “Fake News”, Disinformation and Propaganda, OSCE, FOM.GAL/3/17, 3.3.2017. Retrieved from <https://www.osce.org/files/f/documents/6/8/302796.pdf> [accessed 10 Feb 2021]
- Kalsnes, B.** (2018), ‘Fake news,’ *Oxford Encyclopedia of Communication*. <https://doi.org/10.1093/acrefore/9780190228613.013.809>
- Keane, D.** (2007), ‘Attacking hate speech under Article 17 of the European Convention on Human Rights,’ *Netherlands Quarterly of Human Rights*, vol. 25, no. 4, pp. 641–664. <https://doi.org/10.1177/016934410702500404>
- Klonick, K.** (2020), ‘The Facebook Oversight Board: creating an independent institution to adjudicate online free expression,’ *Yale Law Journal*, vol. 129, no. 8, pp. 2418–2499.
- Mastroianni, R.** (2019), ‘Fake news, free speech and democracy: (bad) lesson from Italy,’ *Southwestern Journal of International Law*, vol. 25, no. 1, pp. 42–74.
- Mazur, J.** (2018), ‘Right to access information as collective-based approach to the GDPR’s right to explanation in European law,’ *Erasmus Law Review*, vol. 11, no. 3, pp. 178–189. <https://doi.org/10.5553/ELR.000116>
- Meneghetti, A. & Anderson, C.** (2021), ‘What implications does the EU’s proposed Digital Services Act have for the UK?’ *RadcliffesLeBrasseur LLP*, 1 March. Retrieved from <https://www.rlb-law.com/briefings/corporate/what-implications-does-the-eus-proposed-digital-services-package-have-for-the-uk/> [accessed 11 Apr 2021]
- Murray, A.** (2016), ‘US election: Fake news becomes the news,’ *BBC*, 7 November. Retrieved from <https://www.bbc.com/news/world-us-canada-37896753> [accessed 3 Apr 2021]
- Nenadić, I.** (2019), ‘Unpacking the “European approach” to tackling challenges of disinformation and political manipulation,’ *Internet Policy Review*, vol. 8, no. 4, pp. 1–22. <https://doi.org/10.14763/2019.4.1436>
- Nunez, F.** (2020), ‘Disinformation legislation and freedom of expression,’ *UC Irvine Law Review*, vol. 10, no. 2, pp. 783–[viii].
- Oversight Board (2021), ‘Oversight Board overturns Facebook decision: Case 2020-006-FB-FBR.’ Retrieved from <https://oversightboard.com/news/325131635492891-oversight-board-overtturns-facebook-decision-case-2020-006-fb-fbr/> [accessed 10 Apr 2021]
- Pamment, J.** (2020), ‘The EU’s role in fighting disinformation: taking back the initiative,’ Carnegie Endowment for International Peace. Retrieved from https://carnegieendowment.org/files/Pamment_-_Future_Threats.pdf [accessed 23 Apr 2021]

- Pepp, J.; Michaelson, E. & Sterken, R.** (2019), 'What's new about fake news,' *Journal of Ethics and Social Philosophy*, vol. 16, no. 2, pp. 67–94.
<https://doi.org/10.26556/jesp.v16i2.629>
- Pielemeier, J.** (2020), 'Disentangling disinformation: what makes regulating disinformation so difficult?' *Utah Law Review*, vol. 2020, no. 4, pp. 917–940.
- Plasilova, I.; Hill, J.; Carlberg, M.; Goubet, M. & Procee, R.** (2020), *Study for the "Assessment of the Implementation of the Code of Practice on Disinformation"*, Luxembourg: Publications Office of the European Union. Retrieved from https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=66649 [accessed 10 Feb 2021]
- Pollicino, O. & Bietti, E.** (2019), 'Truth and deception across the Atlantic: a roadmap of disinformation in the US and Europe,' *Italian Journal of Public Law*, vol. 11, no. 1, pp. 43–85.
- Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM/2020/825 final, 15.12.2020.
- Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8.6.1977.
- Read, S.** (2020), 'Fraud: Banks reveal the 10 coronavirus scams to be wary of,' *BBC*, 29 July. Retrieved from <https://www.bbc.com/news/business-53573408> [accessed 10 Feb 2021]
- Rolke, A.; Rath, H. & Backmann, J.** (2019), 'Digital tools and the right to know,' *International Chemical Regulatory and Law Review*, vol. 2019, no. 4, pp. 171–178. <https://doi.org/10.21552/icrl/2019/4/8>
- Saurwein, F. & Spencer-Smith, C.** (2020), 'Combating disinformation on social media: multilevel governance and distributed accountability in Europe,' *Digital Journalism*, vol. 8, no. 6, pp. 820–841. <https://doi.org/10.1080/21670811.2020.1765401>
- Shackelford, S. J.; Raymond, A.; Stemler, A. & Loyle, C.** (2020), 'Defending democracy: taking stock of the global fight against digital repression, disinformation, and election insecurity,' *Washington and Lee Law Review*, vol. 77, no. 4, pp. 1747–1810. <https://doi.org/10.2139/ssrn.3548670>
- Shattock, E.** (2020), 'Is it time for Europe to reassess internet intermediary liability in light of coronavirus misinformation?' *European Law Blog*, 20 April. Retrieved from <https://europeanlawblog.eu/2020/04/20/is-it-time-for-europe-to-reassess-internet-intermediary-liability-in-light-of-coronavirus-misinformation/> [accessed 10 Apr 2021]
- Shu, K.; Sliva, A.; Wang, S.; Tang, J. & Liu, H.** (2017), 'Fake news detection on social media: a data mining perspective,' *SIGKDD Explorations Newsletter*, vol. 19, no. 1, pp. 22–36. <https://doi.org/10.1145/3137597.3137600>

- Sugow, A.** (2019), 'The right to be wrong: examining the (Im) possibilities of regulating fake news while preserving the freedom of expression in Kenya,' *Strathmore Law Review*, vol. 4, pp. 19–46.
- Swiatkowska, J.** (2017), 'Cybersecurity statecraft in Europe: a case study of Poland,' *Georgetown Journal of International Affairs*, vol. 18, no. 3, pp. 83–94. <https://doi.org/10.1353/gia.2017.0040>
- Twitter, Inc. (2019), *Twitter Progress Report: Code of Practice against Disinformation*, European Commission. Retrieved from https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62682 [accessed 10 Feb 2021]
- Twitter, Inc. (2020), *Twitter Report: Staying safe and informed on Twitter during COVID-19*, European Commission. Retrieved from https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=69160 [accessed 10 Feb 2021]
- Vaque, L.** (2018), 'Fake news in the food sector: consumer distrust and unfair competition,' *European Food and Feed Law Review (EFFL)*, vol. 13, no. 5, pp. 411–420.
- Vojak, B.** (2017), 'Fake news: the commoditization of internet speech,' *California Western International Law Journal*, vol. 4, no. 1, pp. 123–158.
- Waldman, A.** (2018), 'The marketplace of fake news,' *University of Pennsylvania Journal of Constitutional Law*, vol. 20, no. 4, pp. 845–870.
- Wheeler, M.** (1994), 'The right to know in the European Union,' *Review of European, Comparative & International Environmental Law*, vol. 3, no. 1, pp. 1–6. <https://doi.org/10.1111/j.1467-9388.1994.tb00146.x>
- Yilma, K.** (2017), 'Fake news and its discontent in Ethiopia,' *Mekelle University Law Journal*, vol. 5, no. 1, pp. 98–114.