Polish Political Science Yearbook, **vol. 50 (2021), pp. 61–80**
DOI: https://doi.org/10.15804/ppsy202153 PL ISSN 0208-7375
www.czasopisma.marszalek.com.pl/10-15804/ppsy

Krzysztof Wasilewski
Koszalin University of Technology (Poland)
ORCID: 0000-0002-5378-2822
e-mail: krzys.wasilewski@gmail.com

Fake News and the Europeanization of Cyberspace

Abstract: As both the European Union and its member states acknowledge that the proliferation of fake news threatens their political stability and – consequently – the general idea of European integration – they have undertaken many steps to confront that problem. Them, the article examines how EU institutions, together with the member states, have tackled the spread of disinformation within the common policy of cybersecurity. The novelty of this study is that it does so concerning the ongoing process of Europeanization of cyberspace, combining the field of information technology with European studies.

Keywords: *European Union, fake news, cybersecurity, Europeanization, public sphere*

Introduction

It is hard to disagree with the European Commission when it states that "as fake news proliferates, disinformation threatens democracy and efficient governance" (Knowledge for Policy, 2019). Smartphones and other low-cost electronic devices, which are becoming more and more easily accessible to individuals, have not only replaced state-orchestrated propaganda machines from the Cold War era but have become political weapons in their own right – unparalleled with any other disinformation tool in the past (Wooley & Howard, 2019, pp. 3-18). Consequently, instead of performing the role of a marketplace of ideas, social media sites often serve as platforms of information warfare (Zhang & Ghorbani, 2020). Such a situation threatens the very foundations of every democratic system. Liberal democracy relies on the idea of a public sphere where people can freely communicate with each other, present their opinions, and work out compromise solutions (Habermas, 1984). It becomes impossible if lies replace true statements. In other words, any – even a minor – perturbation in communication has negative consequences for the entire political system. Disinformation is such a perturbation in communication. In this sense, it resembles a virus that spreads

from one element of social life to another, infecting them all step by step. Just as a case of flu first manifests itself in the form of a seemingly harmless cough but ultimately may lead to lethal pneumonia, so does the spread of so-called fake news first infect communication, only to gain strength and attack the vital organs of the entire system.

This comparison with flu is not accidental, considering the volume of false information on the coronavirus pandemic that have spread throughout the Internet in 2020. Not only has it fueled mass protests in many cities across the world, but it also undermined actions taken by democratic governments. Unsurprisingly, many studies indicate that disinformation campaigns might have significantly impacted the outcomes of the 2016 presidential election in the United States and the 2016 Brexit referendum, which eventually led to the United Kingdom leaving the European Union (EU) in 2020 (Rose, 2017). As such, fake news affects both national and supranational levels of communication, along with politics and governance.

Since 2016 the EU has undertaken many initiatives against the proliferation of false information. In fact, as Annina Claesson (2019, p. 13) of the Center for Strategic and International Studies observes, "Europe has been a testing ground for tactics to counter disinformation in democracies. (…) Now, the European Union is aiming to complement national efforts by scaling up its own response through EU-level policies". Considering the negative impact that the proliferation of fake news seems to have on the political stability of the European Union and its member states (Tackling COVID-19 disinformation…) – as well as "traditional" problems impacting European media – there is no exaggeration in stating that these efforts will decide the future of European integration.

Then, the following article examines how EU institutions, together with member states, have tackled the spread of disinformation. The innovative nature of this study is, first and foremost, that it examines this issue concerning the ongoing process of the Europeanization of cyberspace, combining the field of information technology with European studies. Thus, the paper asks the following research question:

> Q1: If and in what aspects of the EU response to the proliferation of online disinformation can the process of Europeanization be observed?

Institutional Analysis and Europeanization

With its sophisticated net of institutions and bodies, the European Union appears to be the perfect subject for institutional analyses. Although it may seem that the inner structure of this international organization has changed very little throughout the years, its "underlying nature and functions have been subject to a fundamental process of amendment that continues still" (Watts, 2008, p. 75). Unsurprisingly, the EU attracts the attention of scholars representing various disciplines and paradigms. The systematic rise of research papers in European studies has been observed since the first half of the 1990s, when the Maastricht

Treaty – the Treaty on European Union – was introduced and implemented by member states, laying the foundations for the contemporary structure of the European Union. At the same time, institutionalism regained its high position in political science, which resulted in scholars' growing interest in formal and informal institutions and their functions at national and supranational levels (Peters, 2009). Consequently, most of the available publications on the EU concern two broadly defined topics: 1) the competences of consecutive EU institutions and bodies; and 2) the evolution of the sovereignty of member states. The fact that these two topics are prevalent in the reviewed literature is hardly surprising, taking into account that the "transfer potential of the European Union lies in its multi-level character and the scope that exists for moving policy up or down between the supra-national, national and sub-national levels of governance" (Bulmer & Padgett, 2004, p. 103). Despite the noticeable body of studies located within the paradigm of the so-called new institutionalism (Goetz & Hix, 2000), EU-related topics have been researched mainly from the perspective of historical institutionalism (Pierson & Skocpol, 2002).

Among the advantages of this perspective, one is of particular importance to contemporary European studies: it provides scholars with methods and techniques to measure and evaluate the process of Europeanization. Incorporating this idea into European studies helped establish common ground between intergovernmentalists and functionalists. It has also attracted interest in previously neglected topics, e.g., how domestic political systems are impacted by EU institutions (Graziano & Vink, 2013). With its definition being systematically developed since the early 1990s, at present, Europeanization can be understood as a:

> Process of (a) construction (b) diffusion and (c) institutionalization of formal and informal rules, procedures, policy paradigms, styles, "ways of doing things", and shared beliefs and norms which are first defined and consolidated in the making of EU decisions and then incorporated in the logic of domestic discourse, identities, political structures and public policies (Radaelli, 2003, p. 30).

There can be distinguished two main approaches to Europeanization, namely: top-down and bottom-up. The former analyzes how the EU impacts national politics and institutions (Ladrech, 1994); the latter focuses on the reverse process, that is, how national-level politics affect EU-level politics (Flockhart, 2010). However, it must be remembered that the process of Europeanization may take other forms than the two mentioned. One of the leading researchers in the field, Janusz Ruszkowski (2019), indicates as many as five "trajectories" through which Europeanization can manifest itself. Other studies also point out that top-down and bottom-up are not the only approaches to the process (Ruszkowski, 2003; Lipowicz, 2008; Pacześniak, 2014; Cianciara, 2015). Although it is difficult, if not impossible, to separate trends and processes within Europeanization, the vast majority of studies seem to focus on the top-down approach to Europeanization. According to Graziano and Vink (2002), such a situation derives, first and foremost, from the fact that Europeanization "is more concerned

with domestic political change rather than EU political development. Therefore, Europeanization has been used as an analytical approach to understand domestic changes, being more relevant for country specialists and comparative politics scholars". Nevertheless, the number of studies analyzing changes within domestic-level politics during the consecutive phases of European integration (negotiations at the EU level, implementing EU regulations, etc.) is systematically growing and producing interesting findings (Exadaktylos & Radaelli, 2009; Radaelli, 2006; Giulianni, 2001).

The following study of "fake news" in European cybersecurity combines both approaches to the process of Europeanization. Since the very idea of cyberspace[1] – as a phenomenon more resembling a public sphere than a tangible, material construction (Dahlberg, 1998) – makes it impossible to delineate its national and supranational levels, adapting either a top-down or a bottom-up approach would reveal an over-simplified picture of the problem. In other words, decisions concerning cyberspace, whether made at the national or European level, affect one another simultaneously and should not be examined separately. Many studies support this thesis (Marszałek-Kawa et al., 2020; Ruohonen, 2019; Carrapico, 2017; Jokela, 2010). Therefore, an analysis of the Europeanization of cyberspace in the case of "fake news" (or any other issue) must include all the institutions and levels of politics involved and avoid giving any of them precedence over another. Consequently, institutions are understood here in a broad sense, including established and hierarchical bodies, such as the European Commission or European Parliament, and high-tech companies, media systems, broadcasting companies, and others.

Research Question and Methods

The cyber policy requires simultaneous coordination at every level of politics and poses severe challenges to each element of the system. All the actors must reach common definitions, establish new institutions and bodies, and, consequently, cede part of their powers. The EU's current efforts to combat the proliferation of so-called "fake news" provides a good case study to examine if and how Europeanization penetrates cyberspace. Thus, this study asks the following research question:

> Q1: If and in what aspects of the EU response to the proliferation of online disinformation can the process of Europeanization be observed?

> H1: With so-called "fake news" posing a serious challenge to the political stability of both the European Union and its member states, combating online false information demands close cooperation between institutions responsible for cybersecurity

[1] The term „cyberspace" was coined by writer William Gibson who first introduced it in his book *Neuromancer* in 1984.

at national and supranational levels. Policies developed and carried out against "fake news" can demonstrate the process of the Europeanization of cyberspace. However, the contemporary prerogatives of the EU and exclusive responsibilities of member states for their media policies make it extremely difficult to work out a pan-European mechanism to combat online misinformation.

The research question will be answered within the perspective of historical institutionalism. As Orfeo Fioretos (2011, pp. 370-371) points out, historical institutionalism is a "theoretical tradition that gives particular attention to a discrete set of substantive themes that are analyzed with a distinct combination of analytical concepts and methods". The timing and sequence of political events are important in historical institutionalism, as decisions are taken in a given context that may change significantly over time. Therefore, this study presents consecutive stages of the EU's response to the spread of false information. Based on close textual analysis of official documents (reports, communications, leaflets, etc.) and the examination of institutions' structure, it investigates the measures undertaken by EU institutions against disinformation campaigns. First, however, the study defines the phenomenon of "fake news" and various (political, social, communicative, etc.) repercussions that affect the functioning of the European Union and its member states.

"Fake news", the Public Sphere, and Democracy

The term "fake news" has been widely used in journalistic and political debates worldwide, Europe notwithstanding. However, despite its omnipresence, it lacks a single popularly acknowledged definition. It thus comes as no surprise that in his foreword to the "Handbook for Journalism and Training", published by UNESCO, Guy Berger concedes that it would be better to avoid assuming that "'fake news' has a straightforward or commonly-understood meaning". This conviction derives from the fact that such words as "news" and "information" may themselves be understood differently, depending on numerous factors, such as a media system or even one's political affiliation. Faced with this dilemma, Berger then concludes that "'news' means verifiable information in the public interest, while information that does not meet this standard does not deserve the label of news. In this sense, then, 'fake news' is an oxymoron that lends itself to undermining the credibility of information which does not indeed meet the threshold of verifiability and public interest – i.e., "real news" (Berger, 2018, p. 7).

But what exactly does "fake news" mean? In their article on the typology of this term, Edson C. Tandor Jr. et al. provide a list of definitions of "fake news" – used in both academic and public discourse. One of the most popular understandings of "fake news" in the latter implies that the term refers to "viral posts based on fictitious accounts made to look like news reports" (Tandor et al., 2017, p. 2). However, according to one scholarly definition, referred to by the authors, "fake news" should be regarded as "news articles that are intentionally and verifiably false, and could mislead readers" (Tandor et al., 2017, p. 2). Most media

scholars agree that the contemporary understanding of "fake news" should focus on news fabrication and manipulation, along with propaganda (Brennen, 2017). That group includes media content that is published either for financial or ideological reasons. In the first event, the main function of "fake news" is to generate profit. "Clickbait", as this practice is called, relies on constructing engaging yet entirely or partially untrue stories that will attract as many readers as possible and, as a consequence, make money from advertising (Bakir & McStay, 2017). In the second event, "fake news" is spread to win adherents for one political agenda or discredit another. Although the commercial use of hoax stories should not be disregarded, the political dimension of "fake news" poses the greatest danger to democracy (Kshetri & Voas, 2017). That is why some scholars associate "fake news" with "information disorder" and its related challenges, such as echo chambers (Wardle & Derakhshan, 2017). The high interaction of fake websites and the growing number of visitors make them a severe threat to communication and politics at every level of governance (Marszałek-Kawa, 2019; Fletcher et al., 2018).

Healthy democracies rely on the free exchange of opinions and ideas. Jürgen Habermas, who first introduced the concept of the public sphere, maintains that without it, it would be impossible to secure popular sovereignty, formal law, constitutionally guaranteed rights, and civil liberties (Kellner, 2004). If, as Habermas desires, the public sphere is reproduced through communicative action in which participants use rational arguments to reach an agreement, then disinformation poisons the very foundation of such a public sphere (Habermas, 1996, p. 360). In the aftermath of the 2018 Brazilian presidential election, which was won by the far-right candidate Jair Bolsonaro, the columnist Zack Beauchamp (2019) noted that "authoritarian factions inside democratic states – far-right politicians and parties that are at best indifferent to democratic norms – benefit from the nature of modern social media platforms". This journalistic observation is supported by recent findings that point toward a strong and global interdependence between the spread of online disinformation and the growing popularity of social media (Ipsos, 2019). For example, according to one research study, most Americans admitted to searching for news concerning the 2016 US presidential election on social media. Moreover, for 14 percent of them, social media was the "most important source of election news" (Allcott & Gentzkow, 2017). In addition to this, the research found "115 pro-[Donald] Trump fake stories that were shared on Facebook a total of 30 million times, and 41 pro-[Hilary] Clinton fake stories shared a total of 7.6 million times" (Allcott & Gentzkow, 2017, p. 212). Unsurprisingly, as of June 2019, half of Americans believed "fake news" to be a greater threat to the country than terrorism (Mitchell et al., 2019).

However, there appears to be yet another challenge to the public sphere and democracy apart from the unrestrained flow of "fake news" in cyberspace. After all, false information is as old as the news industry itself. Two scholars, Johan Farkas and Jannick Schou, have taken this one step further by claiming that "fake news" is used to criticize or discredit political opponents and build an entirely new political community. In order to prove their

thesis, they reach for Ernesto Laclau's concept of a "floating signifier" and describe "fake news" as a part of a "much larger hegemonic struggle to define the shape, purpose and modalities of contemporary politics. It becomes a key moment in a political power struggle between hegemonic projects" (Farkas & Schou, 2018, p. 300). In Farkas and Schou's opinion, "fake news" as a floating signifier is used in three main contemporary political discourses, namely: 1) a critique of digital capitalism; 2) a critique of right-wing politics and media; 3) and a critique of liberal and mainstream media. Each of these discourses holds its own set of values, which is often hostile to democratic rules. Consequently, the authors conclude, "fake news" has become "the center of contemporary political struggles, used as a discursive weapon within competing discourses seeking to delegitimize political opponents" (Schou, 2018, p. 308). Politicians have learned that the easiest way to delegitimize any critical voices is to call them "fake news". Therefore, political debate can no longer produce substantive arguments necessary for any efficient deliberative democracy (Chambers, 2020).

Such a "discursive weapon" presents a threat to every democratic public sphere, let alone such a complex formation as the public sphere constituted by the European Union. A union of 27 member states (with the United Kingdom that officially left the EU on February 1, 2020), the EU is often considered as a "union of deep diversity", defined as a "plurality of ways of belonging [which are] acknowledged and accepted" (Fossum, 2004). It can be achieved and legitimized only through deliberative democracy, which needs a public sphere where participants may freely discuss and exchange ideas. In other words, cardinal concepts for the EU's integrity, such as European identity and European values, are developed within the public sphere, being produced by "various discourses and may also be perceived as persuasive and convincing grand narratives" (Ivic, 2017, p. 90). Fragile as it already is, the EU public sphere additionally suffers from the spread of online disinformation.

Some scholars have observed that the "Internet could be an ideal place for a European and enlightened public space, in principle. But instead, it risks becoming an anti-enlightenment echo chamber where fact and fiction merge into some kind of post-factual universe" (Weizsacker & Wilkens, 2017). There is little doubt that while undermining the European public sphere, disinformation can also undermine the entire EU. Brexit is an excellent example of how infecting one national public sphere with false information may lead to the country's hasty reverse of its international commitments and create a counter-hegemonic discourse that questions the very process of European integration. Commenting on Brexit, publicist Alex Barker (2019) pointed out that it had "transformed the narrative adopted by anti-EU politicians in the EU". In other words, used as a "discursive weapon", online disinformation has allowed the emergence of a discourse aiming to "fundamentally transform the EU's political orientation from liberal democracy to a union of states with authoritarian tendencies that build new and old borders" (Ondarza & Schenuit, 2018). Therefore, "fake news" should be regarded as a severe threat not only to the EU's cybersecurity but to the EU itself.

"Fake News" and the European States

EU member states have made many initiatives to tackle online disinformation. The following case studies were chosen to illustrate various approaches to online disinformation within the European Union. One of the first attempts in Europe was made in Germany, where, in October 2017, a Network Enforcement Act (NetzDG) was passed by the parliament (Tworek & Leersen, 2019). As the act is known, the "hate speech law" allows one to remove illegal content from social networks, such as Facebook and Twitter. Among 22 categories of illegal content are "incitement to hatred", "distribution of child pornography", "defamation", "insult", and "forgery of data intended to provide proof". The act requires social platforms to establish a mechanism for their users to submit complaints about illegal content. Once such a platform receives over 100 such complaints, it is obliged to publish semi-annual special reports. Although the introduction of NetzDG triggered a lengthy debate over online censorship and the freedom of communication, it was approved by a majority of Germans (He, 2020). Within the first year of the act being in force, Twitter received almost 265,000 complaints, YouTube 244,000, while Facebook received only 1,704. However, "most of the takedowns resulting from NetzDG complaints removals appear to have occurred under the companies' community guidelines (or "terms of service"), rather than the German speech laws which NetzDG is intended to enforce" (Tworek & Leersen, 2019). A similar law was approved in France in November 2018, namely a Bill Against the Manipulation of Information, which targets the online dissemination of fake news, especially by social media platforms, such as Facebook. They are required to publish the name of the author and the amount paid for any sponsored content. In addition to this, the law allows judges to halt the circulation of fake news if it meets three criteria: it is manifested, disseminated deliberately on a massive scale, and aims to compromise the outcome of an election or disturb the peace. Moreover, in May 2020, the French parliament passed the Act to Fight Against Hate on the Internet. However, soon after, the French Constitutional Council decided it disproportionately infringed on freedom of speech and did not come into effect.

Whereas Germany and France have established permanent legal mechanisms to combat the spread of online misinformation, some European countries have opted for ad-hoc solutions. For example, in January 2018, two months before a parliamentary election, the Italian Interior Ministry enacted an Operating Protocol for the Fight Against the Diffusion of Fake News through the Web on the Occasion of the Election Campaign for the 2018 Political Elections. According to this document, the postal police were given authority to fact-check news published online and, if necessary, to report the alleged crime to the judicial authorities. The introduction of this protocol drew criticism from opposition parties and human-rights activists, who argued that the document conferred "excessively broad discretion on the government to prosecute statements that are critical of public and political figures" (Verza, 2018). The same arguments were used against the 2018 amendment of the Data Protection Law in Spain. With an upcoming general election in April 2019, the Spanish government announced

that it would introduce special protocols to "eliminate content that violates the constitutional right to freely communicate or receive truthful information through any means of communication". To ensure fair and free elections, in 2017, the Czech Republic established the Centre Against Terrorism and Hybrid Threats, whose main goal was to tackle Russian propaganda. In many countries, especially those with strong political polarization and distrust, governmental attempts to pass "anti-fake news" laws have provoked criticism from human rights groups and opposition parties. It is why a group of EU members has refrained from taking any concrete steps against online disinformation. In such cases, government-led efforts are often limited to sponsoring information and education campaigns. However, other governments have taken advantage of the problem of fake news to test the possibility of imposing regulation and control over social media platforms and the Internet in general. In Poland, the current right-wing government has made complaints against Facebook, Twitter, and other social platforms, which, in their opinion, have censored conservative posts. Although the Polish authorities have fallen short of their plan to "re-polonize" the media (that is, buy out a private print and audiovisual media outlets) and establish a control system over the content of social media platforms, Poland serves as an example of the threats associated with the issue of online misinformation.

The EU's Legal Approach to "Fake News"

Since "fake news" threatens both the European public sphere and the European Union itself, combating this negative phenomenon demands a determined response in the three main spheres of the EU's activity, namely: legislation, politics, and security. The EU's legal system and decision-making procedures are a highly complex matter, struggling to find the right balance between the sovereign right of each member state and EU competences. Apart from the treaties which constitute the Union's main primary legislation, its secondary legislation can be divided into three types, namely: regulations; directives; along with decisions, recommendations, and opinions (The EU legal system…). Regulations apply automatically and uniformly to all member states while directives require EU countries to achieve a certain result yet leave them free to choose how to reach that goal. Regarding media (including regulations concerning the Internet), however, the EU allows each member state to regulate its own media system, providing it adheres to democratic rules and pluralism. In her analysis, media scholar Alison Harcourt (2005, p. 12) points out that the EU "simultaneously practiced a 'softer' approach to furthering its [media] policy agenda through the suggestion of best practices, models and solutions to the problem of regulating media markets". Consequently, all attempts by the EU to introduce any general media laws have so far been unsuccessful, as this remains within the remit of the 1992 European Commission statement that "transparency as such is not at present seen as a need which would justify specific action on the part of the Community, as long as there are no obstacles to exchanges of information between national authorities" (Commission, 1992, p. 81).

Nevertheless, in 2011, a group of EU-appointed experts issued a report entitled *A free and pluralistic media to sustain European democracy* in which they stated that "the European Union must intervene when there is a restriction of fundamental rights or media pluralism" (Vike-Freiberga et al., 2016, p. 19). Two years later, the European Parliament adopted a resolution calling on member states and the European Commission to "ensure better monitoring and enforcement of media freedom and pluralism across the EU", as well as to "include rules on the transparency of media ownership, media concentration and conflicts of interest" (Directorate-General for Internal Policy, 2016, p. 28). This evolution to a more active role for EU institutions derives from the fact that the number of member states facing a risk to pluralism in the political and market domain is gradually increasing. In 2014, the European Council managed to work out a compromise on basic tenets regarding media freedom and pluralism. It also underlined the dependence between EU media regulations and the strengthening of the single market. Despite the actions taken by the EU (within its contemporary competences – see: CMPF, 2013), media organizations in member states "are pressured from both political and the economic powers" (A comparative analysis, p. 61). Moreover, available reports on media pluralism and freedom in Europe underline the "worsening of the working and economic conditions in the media sector" in almost every member state. Among other main factors that prevent European media organizations from performing their democratic functions are political interference, self-censorship, and a rising concentration in the media sector. Although in the 2020 World Press Freedom Index media from eleven EU members ranked in the top 20, others recorded falls, most notably Poland, Greece, Hungary, and Bulgaria. In all these countries, the media has experienced pressure from governmental authorities and institutions.

The EU prefers the option of "self-regulation", defined as "a type of voluntary initiative which enables economic operators, social partners, non-governmental organizations or associations to adopt common guidelines amongst themselves and for themselves" (Ilves et al., 2016). The praxis of the "self-regulation" policy has brought some success in the EU's legislative struggle with "fake news". Faced with the risk of false information influencing the 2019 European parliamentary election, in the second half of 2018, the European Commission announced that it would start to work on its own pan-European "fake news bill", should tech giants refuse to accept the proposed code of conduct voluntarily. The code consists of five main elements in the moderation of "fake news" online, namely: disrupting advertising revenues from companies that spread disinformation; tackling fake accounts and online bots; making political advertising more transparent; allowing users to report instances of disinformation more easily; providing better frameworks to monitor the spread of disinformation (Stolton, 2018). The publishing of the code was met with some heavy criticism. For example, the Multistakeholder Forum on Disinformation Online, which groups representatives of online platforms, advertisers, academics, media, and civil society organizations, issued a statement criticizing the code for being too general in scope, as well as for its lack of a common approach (The Sounding Board's, 2018). Nevertheless, in

response to the European Commission's announcement, in October 2018, tech companies such as Facebook, Google, Twitter, and Mozilla submitted their plans to meet the code's requirements. For example, Twitter prioritized actions against malicious actors, whereas Facebook strengthened its cooperation with fact-checkers and the research community across the EU. By the end of January 2019, the first report was published by the companies. In its review of the report, the European Commission stated that "there [had] been some progress, notably in removing fake accounts and limiting the visibility of sites that promote disinformation. However, additional action is needed to ensure full transparency of political ads" (Code of Practice, 2019). Under the *Code of Practice*, Google, Facebook, and Twitter published monthly reports from January through May 2019, detailing actions that they had undertaken to combat "fake news". While the European Commission positively assessed the reports, it maintained that the big tech companies should introduce more comprehensive solutions in their social media platforms.

The EU perceives its media legislation through the prism of the Single Market. In 2015, the European Commission adopted the Digital Single Market Strategy designed to "open up digital opportunities for people and business and enhance Europe's position as a world leader in the digital economy". The EU considers the Digital Single Market as an extension of the fundamental single market policy, which allows the free movement of persons, goods, services, and capital between the member states. Until the Commission presided by Juncker ended its term on November 30, 2019, it had produced 30 legislative proposals concerning the Digital Single Market Strategy, 28 of which had been agreed upon by the co-legislature. One of them is the *Action Plan against Disinformation*, published on December 5, 2018. In its introduction, the document states that "freedom of expression is a core value of the European Union enshrined in the European Union Charter of Fundamental Rights and in the constitutions of Member States" (Action Plan, 2018, p. 1). It also introduces an EU-acknowledged definition of "fake news" – or disinformation – as "verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm" (Action Plan, 2018, p. 1). Much like most of the previously published similar documents, the plan focuses on political and security issues, which will be analyzed in the following sections of this paper. Regarding legislation, it calls on strengthening cooperation between the EU and its member states, especially "as regards information-sharing, common learning, awareness-raising, pro-active messaging and research" (Action Plan, 2018, p. 8). Moreover, apart from the EU member states, the plan issues recommendations to "large online platforms" like Facebook and Twitter. According to the document, they should "immediately ensure scrutiny of ad placement and transparency of political advertising, based on effective due diligence checks of the identity of the sponsors; close down fake accounts active on their services; and identify automated bots and label them accordingly" (Action Plan, 2018, p. 9).

In addition to the initiatives within the Single Digital Market Strategy, in April 2019, the EU adopted the so-called Cybersecurity Act – Regulation (EU) 2019/881 of the Eu-

ropean Parliament and the Council on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) No. 526/2013. That seemingly tangible departure from the policy of "self-regulation" and recommendations in the field of media policy resulted from the conviction that "cybersecurity is not only an issue related to technology but one where human behavior is equally important. Therefore, 'cyber-hygiene', namely, simple, routine measures that, were implemented and carried out regularly by citizens, organizations and businesses, minimize their exposure to risks from cyber threats, should be strongly promoted" (Cybersecurity Act, 2019, p. 16). However, the act neither regulates media systems of the member states nor does it directly address the problem of "fake news". Here, the EU perceives cybersecurity not as a part of media systems but as an element of the digital single market, which should be controlled at the pan-European level. As such, the adoption of the Cybersecurity Act brings together all the previous actions taken by the EU regarding cybersecurity. In 2013, the EU introduced the Cybersecurity Strategy of the European Union. Three years later, it adopted its first legal act in cybersecurity – Directive (EU) 2016/1148 – which established the first mechanisms to enhance strategic and operational cooperation between member states and introduced obligations concerning security measures and incident notifications. Both documents are analyzed in this paper's following section.

The 2019 European parliamentary election and the risk of its results being influenced by "fake news" made the EU aware of the threats of spreading false information. Together with the European Parliament and other institutions, the European Commission has taken measures to keep European cyberspace – and the European public sphere in general – free of "fake news". However, no new laws concerning the problem have been introduced so far. Instead, the EU has preferred to issue recommendations and opinions and rely on "self-regulation" by tech companies. The introduced *Code of Practice* and *Action Plan against Disinformation* are two examples of this strategy. This unwillingness for decisive action derives from the fact that the problem of "fake news" lies within each member state's media system, each of which has been developed independently of the EU's regulations. Apart from the risk of antagonizing individual member states, any new such law would also have to face accusations of censorship. As a result, the introduction of laws concerning "fake news" has remained a sovereign decision of each member state.

EU's Cybersecurity and "Fake News"

Cybersecurity has been one of the EU's priorities for the last two decades. In 2001, the European Commission took its first step in this field, adopting the Network and Information Security Agenda. Another step was taken three years later to establish the European Union Agency for Network and Information Security (ENISA). However, it was not until 2013 that the Cybersecurity Strategy of the European Union was implemented to "prioritize and integrate [EU's] policies and actions internally and externally; well aware that the EU could

not address cybersecurity challenges alone given the global and open nature of the Internet" (Christou, 2016, p. xi). This intensification of producing works concerning cybersecurity at the EU level can doubtlessly be linked to the advancement of the digital single market. Covering such spheres of cyberspace activity as digital marketing, e-commerce, and telecommunications, the digital single market is especially prone to cybersecurity perils. Since it is estimated that the setting up of the digital single market may increase European GDP by some €415 bn, the EU considers the market's proper protection one of its top priorities.

The EU, following its member states, understands cybersecurity in almost exclusively technical terms – thus the integration of the EU's cybersecurity policy with the development of the digital single market. On the other hand, "fake news" as a political and media-related issue seems to have been left out of the European cybersecurity agenda, which can be explained by the EU's lack of prerogatives in this field. One example of such a stance is the NIS Directive adopted in 2016, namely Directive (EU) 2016/1148 of the European Parliament and the Council concerning measures for a high common level of security of network and information systems across the Union. The document raises many issues, such as online marketplaces, online search engines, or cloud computing services, calling for their integration within the digital single market: "Standardization of security requirements is a market-driven process. To ensure a convergent application of security standards, Member States should encourage compliance or conformity with specified standards so as to ensure a high level of security of network and information systems at Union level" (NIS Directive, 2016, p. 10). In addition to this, each member state is obliged by the Directive to adopt a national strategy on the security of network and information systems. Since the document does not establish the problem of "fake news" as an element of the European cybersecurity agenda per se, it leaves each member state the freedom to decide on its own whether to include this issue in its national strategy.

The Cybersecurity Act, which came into force on June 27, 2019, reinforces the Directive's outlook on cybersecurity. In its introductory section, the document states that "network and information systems are capable of supporting all aspects of our lives and drive the Union's economic growth. They are the cornerstone for achieving the digital single market" (The Cybersecurity Act, 2019). This understanding of cybersecurity as, first and foremost, the protection of technology infrastructure also transpires across the act's remaining sections, which concern the problem of "vulnerabilities in ICT products, ICT services and ICT processes" (The Cybersecurity Act, 2019). Moreover, the document defines a "cyber threat" as "any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons" (The Cybersecurity Act, 2019). Despite the visible marginalization of the disinformation threat to European cyberspace, the act is an important step in establishing the EU's common cybersecurity policy. According to Dominioni (2019) of the Italian Institute for International Political Studies, the act "is strengthening the Union's cybersecurity competency with innovative and frontrunner tools". In his opinion, the "EU did not copy-paste

other cyber-policies, nor did it opt to withdraw from competition in cyberspace. Rather it built upon shared member states' interests and mediated compromises for a unified cyber position which will (hopefully) protect and improve EU citizens' security in-of-and-around cyberspace" (Dominioni, 2019).

Although the NIS Directive and the Cybersecurity Act largely ignore the problem of "fake news", false information is still considered a threat to European cybersecurity. For example, in September 2017, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy published a joint communication to the European Parliament entitled *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*. Since then, the document has set the direction of the development of cyberpolicy. The communication reads that the "use of cyberspace as a domain of warfare, either solely or as a part of a hybrid approach, is now widely acknowledged. Disinformation campaigns, fake news and cyber operations targeted at critical infrastructure are increasingly common and demand a response" (Communication, 2017, p. 2). Much like other such documents, this one also places the problem of "fake news" within the issue of "cyber hygiene and awareness". The member states are asked to conduct awareness campaigns, remembering that "awareness-raising in relation to online disinformation campaigns and fake news on social media specifically aimed at undermining democratic processes and European values is equally important" (Communication, 2017, p. 12).

In the last several years, ENISA has undertaken several steps to combat false information. In 2013, the EU reviewed ENISA's accomplishments, which resulted in the EU Regulation No. 526/2013 transforming the agency into the European Union Agency for Network and Information Security and broadening its duties. The agency has been additionally strengthened by the Cybersecurity Act, which granted ENISA a permanent mandate and established the first EU-wide cybersecurity certification framework (Wessel, 2015). Apart from protecting the flow of electronic communications, as well as network and information security, ENISA is now supposed to "assist the relevant Union institutions, bodies, offices and agencies and the Member States in public education campaigns to end users, aiming at promoting safer individual online behavior and raising awareness of potential threats in cyberspace, including cybercrimes such as phishing attacks, botnets, financial and banking fraud, as well as promoting basic authentication and data protection advice" (EU Regulation No. 526, 2013, p. 44). Although "fake news" is not explicitly listed as one of the threats to the EU's cybersecurity, the spread of false information remains within the scope of ENISA, especially through its education campaigns and assistance to member states.

In response to earlier proposals of the EU Commission to tackle online disinformation, in April 2018, ENISA published an opinion paper. According to the paper, although the agency does not consider "fake news" as a problem for European cybersecurity as such, it admits that disinformation is a "potential disruptor of democratic processes globally" (Strengthening Network, 2019, p. 3). What is more, it "may be characterized as a weapon, where posting on social media, emails, spam and other online activities can cause damage to others, as

well as to society at large" (Strengthening Network, 2019, p. 3). In response to these threats, ENISA called on online platforms to improve their mechanisms of evaluating information. It also underlined the positive role of Artificial Intelligence (AI) in combating "fake news". According to the Agency, "AI algorithms should be deployed to assist in the detection of online disinformation campaigns and misuse of online platforms such as scraping, spam, etc. The outputs of these algorithms should be verified by humans before any action is taken" (Strengthening Network, 2019, p. 7). Later in 2018, ENISA organized a special event entitled "Bonding EU Cyber Threat Intelligence". Among the issues that were raised during the event was the problem of "fake news".

The problem of "fake news" moved to the top of the list of the EU's priorities in the months preceding the 2019 European parliamentary elections, which some experts thought was the most important in the EU's history (Dempsey, 2019). However, judging from the statements of EU officials, instead of perceiving "fake news" as a threat to European cybersecurity as such, they considered the spread of disinformation as – first and foremost – an impediment to the member states' political and media systems. Nevertheless, in February 2019, ENISA published an opinion paper entitled *Election Cybersecurity: Challenges and Opportunities*, in which it stated that "in a democratic society, a high level of cybersecurity is key for safeguarding the whole election lifecycle" (Election Cybersecurity, 2019, p. 1). Broadening the definition of "cybersecurity" accepted in the Cybersecurity Act and the earlier legislation, the agency admitted that "in a democratic society, 'Cybersecurity' may also involve ensuring the transparent operation of governance or election system. This protection should include the integrity, availability and confidentiality of election processes" (Election Cybersecurity, 2019, p. 4). The paper contains a list of cyber threats to the election process, as well as a set of recommendations to member states. The first included spear phishing, data theft, online disinformation, malware, and Distributed Denial-of-Service (DDoS) attacks. Regarding false information, ENISA issued two recommendations. The first read that a "legal obligation should be considered to classify election systems, processes and infrastructures as critical infrastructure so that the necessary cybersecurity measures are put in place" (Election Cybersecurity, 2019, p. 9). The second called for a law to require political organizations to "deploy a high level of cybersecurity in their systems, processes and infrastructures" (Election Cybersecurity, 2019, p. 9).

One of the latest efforts taken by the EU to combat online disinformation is the creation of the European Digital Media Observatory (EDMO) in June 2020. The project brings scholars, fact-checkers, and journalists together to "understand and analyze disinformation" (European Digital…). The project's first phase is to end in 2022 while its annual budget reaches 2,5 million euros.

Discussion

The research question addressed in this study was: Can the process of Europeanization be observed in the response of the EU to the proliferation of online disinformation?

According to this hypothesis, the efforts made by EU institutions and member states within their cybersecurity policies to combat "fake news" may in the future set foundation for the Europeanization of cyberspace. Since the process of Europeanization is defined here as "a political project aiming at a unified and politically stronger Europe", the analysis of EU institutions and their efforts to stop the proliferation of disinformation conducted here supports the hypothesis. However, this analysis also clarifies that European cyberspace – especially concerning such "soft" cybersecurity threats as disinformation – remains a sphere where the EU and its member states still lack coherent policies concerning security, while cooperation and integration face serious political, legal, and social challenges. The contradiction between the EU's ambition of becoming the "world's safest digital environment" and its indecisive stance on many cyber issues is obvious in the case of "fake news". One may therefore recall the words of Giovanni Ramunno, who has researched EU cybersecurity, stating that it "clearly highlights the limits of national approaches, both due to the transnational character of these threats and to the heterogeneous approach to the field, and, on the other hand, it promotes, in its strategy, a decentralized organization, where cybersecurity governance remains in the member states, while the EU supports capacity building, ensures consistency across member states, and facilitates coordination and outreach" (Ramunno, 2014, p. 1). While keeping such facts in mind, it must be acknowledged that the process of the Europeanization of cyberspace has the potential to accelerate, however slow and alternating its current pace is.

Despite the EU's various initiatives to tackle "fake news", the spread of false information remains largely outside its cybersecurity politics. The spread of disinformation is still considered part of the member states' media systems and the "cyber hygiene" of individual institutions and citizens. When it comes to media systems, it must be remembered that "media policy and regulation has typically been influenced by national variables such as historical experience, culture and values" (Iosifidis, 2011, p. 143). The same reasons make it difficult – if not impossible – to work out common rules of "cyber hygiene", which differs significantly among member states and begins with different definitions of basic terms. Consequently, the EU cedes responsibility for finding the right solutions to the disinformation problem to individual member states. In this strategy, the role of EU institutions, especially the European Commission, seems to be limited to setting out the standard of minimum baseline requirements for cyber security. Such requirements must meet four principles, namely: 1) improve transparency regarding the way information is produced or sponsored; 2) maintain a diversity of information; 3) maintain the credibility of information; 4) implement inclusive solutions with broad stakeholder involvement.

At the same time, the EU is aware of the scale of the problem. In one of its communiqués from September 2019, the European Commission openly states that "the exposure of citizens to large scale disinformation, including misleading or outright false information, is a major challenge to Europe". Thus, a systematic growth in the EU's initiatives can be noticed to raise awareness about the spread of fake news. Here we observe the publication of suggestions, recommendations, and opinions – which may indicate the way of future Europeanization of cyberspace – rather than directives and legislation enforced upon the member states. The same strategy can be observed when it comes to the bottom-up perspective, in which national cybersecurity policies affect the EU's cyber policy. As a result, similar methods of dealing with the spread of information are employed at national and supranational levels. In this case, both the European Union and its member states rely heavily on the private sector, avoiding enacting any laws that could be regarded as censorship. The policy of "self-regulation" that the EU has applied to high-tech companies, such as Facebook, Google, and Twitter, provides an excellent example of how cybersecurity issues are commissioned from political institutions to private enterprises.

This study has shown that the research question does not provide one clear answer. If anything, the process of the Europeanization of cyberspace remains in its early stage. Although this paper's goal is not to opine whether the strategy of combating "fake news" which the EU has undertaken has been exhaustive and successful, it should be underlined that it demonstrates a unique approach to the problem. The structure of cyberspace makes it impossible to separate national and supra-national levels within it. Decisions concerning the spread of disinformation taken by the EU affect the entire European cyberspace. At the same time, the nature of the Europeanization of cyberspace follows other spheres of political, economic, and social life in the European Union that have already experienced this process. In other words, at present, it relies mainly not on directives and legislation but recommendations and opinions, indicating overall goals while giving member states and institutions a great deal of freedom as to the details of how to reach the target.

References:

Allcott, H., & Gentzkow, M. (2017). Social media and fake news in the 2016 election. *Journal of Economic Perspectives, 31*(2), 211-236. DOI: 10.1257/jep.31.2.211

Bakir V., & McStay, A. (2017). Fake news and the economy of emotions. *Digital Journalism, 6*(2), 154-175. DOI: 10.1080/21670811.2017.1345645

Barker, A. (2019, January 23). UK Brexit turmoil changes the tone of other EU opponents. *Financial Times*. https://www.ft.com/content/e13c5c3e-ffc1-11e8-b03f-bc62050f3c4e

Beauchamp, Z. (2019). *Social media is rotting democracy from within*. https://www.vox.com/policy-and-politics/2019/1/22/18177076/social-media-facebook-far-right-authoritarian-populism

Berger, G. (2018). Foreword. In I. Cherilyn, & J. Posetti (Eds.), *Handbook for Journalism Education and Training* (pp. 14-26). UNESCO.

Brennen, B. (2017). Making Sense of Lies, Deceptive Propaganda, and Fake News. *Journal of Media Ethics, 32*(3), 179-181. DOI: 10.1080/23736992.2017.1331023

Bulmer, S., & Padgett, S. (2004). Policy Transfer in the European Union. An Institutionalist Perspective. *British Journal of Political Science, 35*(1), 103-126. DOI: 10.1017/S0007123405000050

Carrapico, H., & Barrhina, A. (2017). The EU as a Coherent (Cyber) Security Actor? *Journal of Common Market Studies*, 55(6), 1254-1272. DOI: 10.1111/jcms.12575

Christou, G. (2016). *Cybersecurity in the European Union. Resilience and Adaptability in Governance Policy*. Palgrave Macmillan.

Cianciara, A. (2015). Europeizacja zewnętrzna: mechanizmy, uwarunkowania, rezultaty. In A. Cianciara, A. Burakowski, P. Olszewski, & J. Wódka (Eds.), *Europeizacja partii politycznych i grup interesu*. Instytut Studiów Politycznych PAN.

Claesson, A. (2019). Coming Together to Fight Fake News. *New Perspectives in Foreign Policy, 17*, 13-19.

CMPF. *European Union competences in respect of media pluralism and media freedom*. European Union Publication Office.

Code of Practice against disinformation. (2019). https://ec.europa.eu/commission/news/code-practice-against-disinformation-2019-jan-29_en

Colomina, C. (2019). Real and virtual threats. Europe's vulnerability to disinformation. *Opinión, 5*. https://www.cidob.org/en/publications/publication_series/opinion/europa/real_and_virtual_threats_europe_s_vulnerability_to_disinformation

Commission of the European Communities. (1992). *Pluralism and Media Concentration in the Internal Market*. https://op.europa.eu/en/publication-detail/-/publication/be71ea95-61ab-44d3-9b14-2d7cb82d8d81/language-en

Dahlberg, L. (1998). Cyberspace and the Public Sphere. Exploring the Democratic Potential of the Net. *Convergence: The International Journal of Research into New Media Technologies, 4*(1), 70-84. DOI: 10.1177/135485659800400108.

Dempsey, J. (2019). *Do These European Parliament Elections Matter?* https://carnegieeurope.eu/strategiceurope/79185

Directorate-General for Internal Policies. (2016). *A comparative analysis of media freedom and pluralism in the EU Member States*. Brussels.

Dominioni, S. (2019). *The (Geo)political Meaning of Europe's Cybersecurity Act*. https://www.ispionline.it/en/pubblicazione/geopolitical-meaning-europes-cybersecurity-act-22870

ENISA. (2018). *Strengthening Network & Information Security & Protecting Against Online Disinformation ("Fake News")*. ENISA.

ENISA. (2019). *Election Cybersecurity: Challenges and Opportunities*. ENISA.

Exadaktylos, T., & Radaelli, C.M. (2009). Research Design in European Studies: The Case of Europeanization. *Journal of Common Market Studies, 47*(3), 507-530. DOI: 10.1111/j.1468-5965.2009.00820.x

European Commission. (2020). *Tackling COVID-19 disinformation – Getting the facts right. Joint communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions*. European Digital Media Observatory Launched. https://www.eui.eu/STG/News/2020/European-Digital-Media-Observatory-launched

Farkas, J., & Schou, J. (2018). Fake News as a Floating Signifier. Hegemony, Antagonism and the Politics of Falsehood. *Javnost – The* Public*, 25*, 298-314. DOI: 10.1080/13183222.2018.1463047

Fioretos, O. (2011). Historical Institutionalism in International Relations. *International Organization, 65*, 367-399. DOI: 10.1017/S0020818311000002

Fletcher, R., Cornia, A., Graves, L., & Nielsen, R.K. (2018). Measuring the reach of "fake news" and online disinformation in Europe. *Digital News Publication*. https://www.digitalnewsreport.org/publications/2018/measuring-reach-fake-news-online-disinformation-europe/

Flochkart, T. (2010). Europeanization or EU-ization? The Transfer of European Norms across Time and Space. *Journal of Common Market Studies, 48*(4), 787-810. DOI: 10.1111/j.1468-5965.2010.02074.x

Fossum, J.E. (2004). Still a Union of Deep Diversity? The Convention and the Constitution of Europe. In E.O. Eriksen, J.E. Fossum, & A.J. Mendez (Eds.), *Developing a Constitution for Europe*. Routledge.

Goetz, K., & Hix, S. (2000). *Europeanised Politics? European Integration and National Political Systems*. Frank Cass.

Habermas, J. (1984). *Theory of Communicative Action*. Beacon Press.

Harcourt, A. (2005). *The European Union and the regulation of media markets*. Manchester University Press.

Ilves, L.K., Evans T.J., Cilluffo F.J., & Nadeau, A.A. (2016). European Union and NATO: Global Cybersecurity Challenges: A Way Forward. *PRISM, 6*(2), 126-141.

Iosifidis, P. (2011). Media and Communication Policy in the European Union. In *Global Media and Communication Policy* (pp. 143-165). Palgrave Macmillan.

Ipsos. (2019). *Internet Security & Trust. Part 3: Social Media, Fake News & Algorithms*. CIGI.

Ivic, S. (2017). The concept of a European public sphere within European public discourse. *Etikk i praksis, 2*, 79-94. DOI: 10.5324/eip.v11i2.1959

Jokela, J. (2010). *Europeanization and Foreign Policy. State Identity in Finland and Britain*. Routledge.

Kellner, D. (2004). *Habermas, the Public Sphere, and Democracy. A Critical Intervention*. https://pages.gseis.ucla.edu/faculty/kellner/papers/habermas.htm

Kshetri, N. (2017). The Economics of "Fake News". *IT Professional, 19*(6), 8-12. DOI: 10.1109/MITP.2017.4241459

Lipowicz, I. (2008). Europeizacja administracji publicznej. *Ruch Prawniczy, Ekonomiczny i Socjologiczny, 70*, 5-17.

Marszałek-Kawa, J. (Ed.) (2019). *Państwo w obliczu współczesnych wyzwań. O cyberbezpieczeństwie i innych zagrożeniach na przykładzie wybranych państw azjatyckich*. Wydawnictwo Adam Marszałek.

Marszałek-Kawa, J., Siemiątkowski, P., Tomaszewski, P., & Polcikiewicz, Z. (2020). The Assessment of the Local Security Policy Efficiency. *European Research Studies Journal, XXIII*(3), 217-237.

Mitchell, A., Gottfried, J., Walker, M., Fedeli, S., & Stocking, G. (2019). *Many Americans Say Made-Up News Is a Critical Problem That Needs To Be Fixed*. https://www.journalism.org/2019/06/05/many-americans-say-made-up-news-is-a-critical-problem-that-needs-to-be-fixed/

Ondarza von, N., & Schenuit, F. (2018). Brexit Tectonics. *Berlin Policy Journal*. https://berlinpolicyjournal.com/brexit-tectonics/

Pacześniak, A. (2014). *Europeizacja polskich partii politycznych*. Scholar.

Peters, G.B. (2019). *Institutional Theory in Political Science. The New Institutionalism*, 4th edition. Edward Elgar Publishing.

Pierson, P., & Skocpol, T. (2002). Historical Institutionalism in Contemporary Political Science. In I. Katznelson, & H.V. Milner (Eds.), *Political Science: State of Discipline* (pp. 693–721). W.W. Norton.

Radaelli, C.M. (2003). The Europeanization of Public Policy. In K. Featherstone, & C. Radaelli (Eds.), *The Politics of Europeanization* (pp. 27–56). Oxford University Press.

Radaelli, C.M. (2006). Europeanization: Solution or Problem? In M. Cini, & A.K. Bourne (Eds.), *Palgrave Advances in European Union Studies* (pp. 56–76). Palgrave Macmillan.

Rammuno, G. (2014). EU Cyberdefence Strategy. *European Union Military Committee, 6*, 1-2.

Rose, J. (2017). Brexit, Trump, and Post-Truth Politics. *Public Integrity, 19*(7), 555-558. DOI: 10.1080/10999922.2017.1285540

Ruszkowski, J. (2010). Europeizacja ad extra w zarządzaniu zewnętrznym (external governance) Unii Europejskiej. *Rocznik Integracji Europejskiej, 4*, 7-27.

Ruszkowski, J. (2019). *Europeizacja. Analiza oddziaływania Unii Europejskiej*. Difin.

Stolton, S. (2018). *EU code of practice on fake news. Tech giants sign the dotted line*. https://www.euractiv.com/section/digital/news/eu-code-of-practice-on-fake-news-tech-giants-sign-the-dotted-line

Tandor, E.C. Jr., Zheng, W.L., & Ling, R. (2017). Defining "fake news". A typology of scholarly definitions. *Digital Journalism, 6*(2), 137-153. DOI: 10.1080/21670811.2017.1360143

The Sounding Board's Unanimous Final Opinion on the so-called Code of Practice. (2018). https://www.euractiv.com/wpcontent/uploads/sites/2/2018/10/3OpinionoftheSoundingboard-1.pdf

Vike-Freiberga, V., Daubler-Gmelin, H., Hammersley, B., & Maduro, L.M. (2013). *A free and pluralistic media to sustain European democracy*. Brussels.

Warde, C., & Derakhshan, H. (2017). *Information Disorder. Toward an Interdisciplinary Framework for Research and Policymaking*. Council of Europe.

Watts, D. (2008). *The European Union*. Edinburgh University Press.

Weizsacker, J., & Wilkens, A. (2017). *It's time for a European Broadcasting Service*. https://voxeurop.eu/en/2017/media-and-information-5120709

Wessel, R.A. (2015). Towards EU cybersecurity law: Regulating a new policy field. In N. Tsagourias, & R. Buchan (Eds.), *Research Handbook on International Law and Cyberspace* (pp. 403–425). Edward Elgar Publishing Ltd.

Wooley, S.C., & Howard, P.P. (2019). Computational Propaganda Worldwide. In S.C. Wooley, & P.P. Howard (Eds.), *Computational Propaganda. Political Parties, Politicians, and Political Manipulation on Social Media* (pp. 3–18). Oxford University Press.

Zhang, X., & Ghorbani, A.A. (2020). An overview of online fake news: Characterization, detection, and discussion. *Information Processing & Management, 57*(2),.DOI: 10.1016/j.ipm.2019.03.004