10-9-2023

What Measures Can Government Institutions in Germany Take Against Digital Disinformation? A Systematic Literature Review and Ethical-Legal Discussion

Stefan Stieglitz
University of Potsdam, stefan.stieglitz@uni-potsdam.de

Jennifer Fromm
University of Duisburg-Essen, jennifer.fromm@uni-due.de

Alexander Kocur
University of Potsdam, alexander.kocur@uni-potsdam.de

Frauke Rostalski
University of Cologne, frauke.rostalski@uni-koeln.de

Michelle Duda
University of Cologne, michelle.duda@uni-koeln.de

See next page for additional authors

What Measures Can Government Agencies in Germany Take Against Digital Disinformation? A Systematic Literature Review and Ethical-Legal Discussion

Research Paper

Stefan Stieglitz[1], Jennifer Fromm[2], Alexander Kocur[1], Frauke Rostalski[3], Michelle Duda[3], Alison Evans[3], Jonas Rieskamp[4], Luzia Sievi[5], Maria Pawelec[5], Jessica Heesen[5], Wulf Loh[5], Christoph Fuchss[6], Kaan Eyilmez[6]

[1] University of Potsdam, Faculty of Economics and Social Sciences, Potsdam, Germany
{firstname.lastname}@uni-potsdam.de
[2] University of Duisburg-Essen, Faculty of Engeneering, Duisburg, Germany
jennifer.fromm@uni-due.com
[3]University of Cologne, Faculty of Law, Cologne, Germany
{firstname.lastname}@uni-koeln.de
[4]University of Paderborn, Faculty of Business Administration and Economics, Paderborn, Germany
{firstname.lastname}@uni-paderborn.de
[5]University of Tuebingen, International Center for Ethics in the Sciences and Humanities, Tuebingen, Germany
{firstname.lastname}@izew.uni-tuebingen.de
[6]Virtimo AG, Berlin, Germany
{firstname.lastname}@virtimo.de

Abstract. Disinformation campaigns spread rapidly through social media and can cause serious harm, especially in crises, ranging from confusion about how to act to a loss of trust in government agencies. Therefore, the prevention of digital disinformation campaigns represents an important research topic and concern that needs to be considered by government agencies to protect public security. However, previous research in the field of information systems focused on the technical possibilities to detect and combat disinformation (e.g., by social bots). In this article, we synthesize information systems literature on disinformation prevention measures by government agencies and discuss these measures from an ethical and legal perspective. We conclude by proposing questions for future research on the prevention of disinformation campaigns by government agencies from an IS, ethical, and legal perspective. Thereby, we contribute to a balanced discussion on the prevention of digital disinformation campaigns and encourage interdisciplinary collaboration in future research.

Keywords: Disinformation Campaigns, Social Media, Ethical Implications, Legal Implications, Government Agencies.

18th International Conference on Wirtschaftsinformatik,
September 2023, Paderborn, Germany

1 Introduction

Early in the COVID-19 pandemic, the documentary *Plandemic* (Plandemic, 2022) falsely claimed that the global elite had planned the coronavirus to control the population. The creators encouraged viewers to share the video on social media and thus acted strategically to spread misleading information (Nazar & Pieters, 2021). This strategic or coordinated action to mislead an audience with false information in a digital environment is commonly referred to as a digital disinformation campaign. It can take place on any digital medium that allows for the exchange of information. Some users deliberately pollute the information climate, e.g., to worsen an opponent's political image or to spread ideologies and manipulate public opinion (Meel & Vishwakarma, 2020). The *Plandemic* disinformation campaign increased engagement with anti-vaccination content and reduced the willingness to comply with containment measures (Nazar & Pieters, 2021). This illustrates how disinformation can have severe consequences in humanitarian crises, such as confusion, loss of trust, emotional suffering, economic costs and mortal danger (Tran et al., 2019). Furthermore, disinformation campaigns can challenge societal cohesion, democratic processes and the rule of law (Arayankalam, 2020).

During the 2018 general elections in Brazil, coordinated efforts of a few top users to spread misinformation in multiple groups (Nobre et al., 2021) showing that influential spreaders often act strategically to get disinformation to the widest possible audience. In addition, a study on Twitter communication during the COVID-19 pandemic found that 20.5% of highly active users could be classified as bot accounts; however, these retweeted both information and misinformation (Marx et al., 2020). Bots are computer algorithms that automatically create content and interact with social media users, attempting to mimic and influence human behavior (Ferrara et al., 2016). Measures to prevent digital disinformation aim to counteract the belief and spread of false information. Balakrishnan et al. (2021) identified altruism and ignorance as the strongest motivators for spreading fake news suggesting that many spreaders are unaware of the falsity of the information. Accordingly, literature on disinformation prevention highlights media literacy as a preventive measure (Apuke & Omar, 2021). Regarding users' belief of misinformation, researchers found that fake news flags increase cognitive activity, but are unable to influence the subjects' beliefs (Moravec et al., 2019). Thus, social media users are more likely to believe information that supports their own political views, a phenomenon also known as "confirmation bias" (Nickerson, 1998).

Previous research also emphasizes the central role of official actors such as government agencies, e.g., showing that a single tweet from official sources can be sufficient to counter misinformation (Vraga & Bode, 2017). Therefore, our contribution focuses on those agencies, specifically on authorities tasked with protecting public security such as disaster control authorities and police departments. In this vein, the Munich police department received high praise for their social media activities during the 2016 shooting in Munich (Germany) because it actively countered rumors (Akkaya et al., 2019). However, the effectiveness thereof depends heavily on the politicization of the issue. During the COVID-19 pandemic, many did not listen to official sources such as the police (Jarolimek & Melzer, 2022). Besides corrective statements, research recommends collaboration between trusted actors on social media as a prevention measure

(Crook et al., 2016). In addition, government agencies could use social bots to automatically disseminate verified information or answer questions from the public (Brachten et al., 2018; Hofeditz et al., 2019). However, governmental agencies in liberal democracies face conflicting demands concerning their engagement with disinformation: While they must ensure security, they must also protect fundamental rights such as the freedom of expression. This ethical and legal dilemma needs to be considered with regard to measures against disinformation.

Most related articles in information systems (IS) research focus on *technical* issues such as detection algorithms (e.g., Al-Asadi & Tasdemir, 2022; da Cardoso Durier Silva et al., 2019; Lahby et al., 2022). Ethical and legal issues are seldom addressed. Rare exceptions are e.g., contributions on ethical issues surrounding algorithmic content moderation (Gorwa et al., 2020) and ethical-legal implications of new laws to fight disinformation (Ivanova, 2019; Nagasako, 2020; Radu, 2020). Additionally, there is a lack of research evaluating preventive measures for government agencies. More interdisciplinary research is needed that equally discusses technical, ethical, and legal issues in the prevention of disinformation (Piccolo et al., 2021). We address this shortcoming and focus on an ethical-legal discussion of measures taken by government agencies, especially government agencies ensuring the safety of citizens.

To do so, we first briefly present our definition of disinformation. Thereafter, we present the methodology and results of a systematic review synthesizing the current state of IS research on disinformation prevention measures. We then discuss the identified measures from an ethical and legal perspective, focusing on democratic states, and Germany, specifically. Finally, we then propose open questions for future research on the prevention of disinformation campaigns from an IS, ethical, and legal perspective, and synthesize our findings in a brief conclusion.

2 Definition of Disinformation

IS research often uses the terms misinformation, disinformation, fake news, and rumors interchangeably (Kapantai et al., 2021). However, there have been attempts at a clearer distinction based on the dimensions of falseness, harm, and the intention to deceive (Allcott & Gentzkow, 2017; DiFonzo & Bordia, 2007; Fallis, 2009; Wardle & Derakhshan, 2017). For example, rumors are understood as "unverified and instrumentally relevant information statements in circulation that arise in contexts of ambiguity, danger or potential threat, and that function to help people make sense and manage risk" (DiFonzo & Bordia, 2007). Furthermore, Wardle & Derakshan (2017) conceptualized both misinformation and disinformation as false information, with disinformation being deliberately shared to cause harm. This aligns with Fallis (2009) who defined disinformation as "misleading information that is intended to be (or at least foreseen to be) misleading". Fake news could be considered a subset of disinformation focusing on news articles "that are intentionally and verifiably false and could mislead readers" (Allcott & Gentzkow, 2017). In this article, we focus on disinformation because it offers a particular challenge for prevention, as it is created to mislead and cause harm.

3 Systematic Literature Review

3.1 Method

To find out which measures IS literature suggests preventing the spread of digital disinformation, we conducted a systematic literature review (Webster & Watson, 2002). We selected the following databases for our search: (1) AIS eLibrary and (2) litbaskets.io (based on SCOPUS). While the former yields a comprehensive set of AIS conferences, the litbaskets.io interface provides access to 847 relevant to IS to obtain journal articles (Boell & Wang, 2019). Hence, this selection of databases offered a comprehensive review of the IS literature. We obtained the relevant articles from the databases using a keyword search, followed by forward and backward searches.

The following search string was specified for the literature retrieval: *abstract:((prevent* OR counter* OR block* OR debunk* OR prebunk* OR combat*) AND (misinformation OR disinformation OR "fake news" OR infodemic))*. Test searches indicated that further synonyms (e.g., rumor or hoax) did not improve the relevance of the retrieved articles. We defined the following inclusion and exclusion criteria to assess the relevance of the search results based on a manual assessment of the title and abstract: (1) The article describes one or more measures to prevent digital disinformation and (2) the measure described must possess a preventive character (i.e., it must not be applied after disinformation is already spread). We excluded articles with a focus on (1) factors contributing to the spread of disinformation and (2) the technical implementation of detection algorithms. The query resulted in 70 articles (no duplicates were found) of which eleven articles remained after applying the inclusion and exclusion criteria. Subsequently, we performed forward and backward searches (vom Brocke et al., 2015; Webster & Watson, 2002), resulting in a final set of 18 relevant articles.

3.2 Results of Measures to Prevent Digital Disinformation in the IS Literature

Our qualitative analysis adhered to the concept-centric literature synthesis according to Webster and Watson (2002). We employed an inductive approach that led to four dimensions along which we synthesized the literature. Articles including more than one prevention measure were assigned to every corresponding concept. Table 1 depicts the concept matrix.

Table 1. Concept matrix.

Actor	Government agencies	(Eccles et al., 2021; Seo et al., 2021; Vemprala et al., 2021)
	Platform operators	(Amoruso et al., 2020; Cao et al., 2015; Eccles et al., 2021; Figl et al., 2020; Gimpel et al., 2021; Hasan & Salah, 2019; Jeong et al., 2020; Jin et al., 2016; Kim & Dennis, 2019; Ng et al., 2021; Nguyen et al., 2020; Ozturk et al., 2015; Wang et al., 2021)
	Individuals	(Eccles et al., 2021; Seo et al., 2021)

	Media and journalists	(Chen et al., 2020; Eccles et al., 2021; Narayan & Attili, 2021; Saad et al., 2019; Seo et al., 2021)
Automation	Partially	(Amoruso et al., 2020; Cao et al., 2015; Eccles et al., 2021; Hasan & Salah, 2019; Jin et al., 2016; Kim & Dennis, 2019; Narayan & Attili, 2021; Nguyen et al., 2020; Ozturk et al., 2015; Seo et al., 2021)
	Manually	(Chen et al., 2020; Eccles et al., 2021; Gimpel et al., 2021; Jeong et al., 2020; Ng et al., 2021; Saad et al., 2019; Vemprala et al., 2021; Wang et al., 2021)
Addressee	Creator	(Cao et al., 2015; Chen et al., 2020; Eccles et al., 2021; Hasan & Salah, 2019; Wang et al., 2021)
	Multiplier	(Amoruso et al., 2020; Cao et al., 2015; Eccles et al., 2021; Figl et al., 2020; Gimpel et al., 2021; Hasan & Salah, 2019; Jeong et al., 2020; Jin et al., 2016; Kim & Dennis, 2019; Narayan & Attili, 2021; Ng et al., 2021; Nguyen et al., 2020; Vemprala et al., 2021; Wang et al., 2021)
	Audience	(Cao et al., 2015; Eccles et al., 2021; Figl et al., 2020; Gimpel et al., 2021; Hasan & Salah, 2019; Jin et al., 2016; Kim & Dennis, 2019; Narayan & Attili, 2021; Ng et al., 2021; Nguyen et al., 2020; Vemprala et al., 2021)
Type	Policy	(Jeong et al., 2020)
	Technical	(Amoruso et al., 2020; Chen et al., 2020; Hasan & Salah, 2019; Jin et al., 2016; Kim & Dennis, 2019; Narayan & Attili, 2021; Ng et al., 2021; Nguyen et al., 2020; Ozturk et al., 2015; Saad et al., 2019; Wang et al., 2021)
	Social / psychological	(Eccles et al., 2021; Gimpel et al., 2021)
	Education	(Eccles et al., 2021; Seo et al., 2021)
	Debunking	(Cao et al., 2015; Vemprala et al., 2021)
	Moderation	(Figl et al., 2020; Ng et al., 2021)

Firstly, we distinguished the prevention measures according to the actors. Most prevention measures are designed for the platform operator with only a few measures proposed for implementation by government agencies. Moreover, journalists and media outlets, or individual users are suggested to act. Secondly, there are differences in the degree of automation. Although there are no completely autonomous measures, many can be executed partially automatically. Conversely, certain measures require manual execution. Thirdly, we discovered that the measures differ in terms of whom they address. Respectively, we distinguish between initial creators, multipliers, and audience of disinformation. Creators initially post disinformation and multipliers are users who play a role in its diffusion while the audience is reached by the information without spreading.

Finally, we summarized the type of measure into six groups. The first group comprises policies and regulations enacted by the platform operator such as the introduction

of an "activity-capping policy" intended to reduce harmful actions (Jeong et al., 2020). The group of technical measures includes algorithms (e.g., identification of the disinformation's origin (Amoruso et al., 2020)), changes in the structure of the platform (e.g., source ratings (Kim & Dennis, 2019; Ng et al., 2021), identity verification (Wang et al., 2021), displaying counter information (Jin et al., 2016; Ozturk et al., 2015), limitation of forwarding postings (Ng et al., 2021)) and additional information systems that inhibit the diffusion of false information (e.g., blockchain-based solutions (Chen et al., 2020; Hasan & Salah, 2019; Narayan & Attili, 2021; Saad et al., 2019)). Moreover, we observed measures addressing social and/or psychological levels (e.g., emphasizing social norms (Gimpel et al., 2021), psychological inoculation (Eccles et al., 2021)). Additionally, we found measures aimed at improving users' media literacy in dealing with false information (e.g., Seo et al., 2021). In contrast, measures with a debunking character provide information that directly corrects specific false information (e.g., Cao et al., 2015; Vemprala et al., 2021). Lastly, moderating measures comprise efforts to mark false information or to delete respective postings (e.g., Figl et al., 2020; Ng et al., 2021).

4 Discussion

Only few measures are proposed specifically for government agencies. Firstly, government agencies can create and conduct *educational* programs to teach digital *media literacy* (Eccles et al., 2021; Seo et al., 2021). Secondly, they can engage in *debunking* false information (Vemprala et al., 2021). However, government agencies could take further steps that are not explicitly designed for them. Specifically, they could incorporate the *psychological inoculation* theory in the creation of their content and in media literacy training (Eccles et al., 2021). Similarly, they could create content that highlights *descriptive and injunctive social norms* (Gimpel et al., 2021). Further, government agencies could draw upon *technical* support, e.g., by using *social bots to debunk and provide content automatically* (Hofeditz et al., 2019) or to improve *education* with media literacy on false information with a chatbot (Kocur et al.,2023). Given computational facilities, they could employ *algorithms* to trace down the origin of a specific false information and place debunking messages strategically (Amoruso et al., 2020). Beyond this analytical step, government agencies could take the initiative to provide additional information systems to support or enable prevention measures. Our literature review reveals the ability of blockchain technology to verify the authenticity of content (Chen et al., 2020; Hasan & Salah, 2019; Narayan & Attili, 2021; Saad et al., 2019).

In sum, government agencies have options for preventing the spread of digital disinformation, but few measures are explicitly designed for them. However, it is important to reflect these ethically and legally – aspects that IS literature often neglects.

4.1 Ethical Discussion of Government Measures against Disinformation

In pluralistic democracies, the public sphere, including social media, performs important functions (Puppis, 2014): Public debates inform citizens, enable them to develop political interests, and to translate these into the political sphere (Habermas, 2022;

Warren, 2017). Publicly voiced opinions and information can expose governmental deficits. This enables citizens to control political institutions (Loh, 2021). A democratic state must thus ensure that the opinion-forming process can take place without major distortions (Habermas, 2022; Heesen, 2021) and must safeguard the freedom of speech, opinion and expression, access to relevant and reliable information, freedom of the press, independence of the media, and the right to privacy (Reporters without Borders, 2018). Interference in public communication by government agencies requires a special degree of justification and is only legitimate if the functioning of the public sphere is seriously endangered. Digital disinformation campaigns – by governments, the private sector, or political groups – can cause such serious disruptions (Farkas, 2018; Giusti & Piras, 2021; Tenove, 2020). They distort opinion formation through false or misleading information (Brown, 2018). They also impede the translational function of the public sphere by "morally denigrat[ing] certain groups" (McKay & Tenove, 2021), helping others gain disproportionate attention, or discouraging victims e.g., of deepfakes from political participation (Pawelec, 2022). Disinformation also leads to a loss of trust in public agencies (European Parliament, 2021; Wardle, 2019). In so doing, it inhibits the media and civil societies' ability to control and criticize governmental actions.

Therefore, the challenge for democratic states and government agencies is to contain the harmful effects of disinformation without undermining democratic values like the freedom of speech, of information, and of the press, and privacy rights. In fact, civil liberties were originally developed as defensive rights against the state (Plattner, 1999), and there is always a danger that the state will use its power and resources to suppress unpopular opinions (Kaul, 2022). The literature frequently advises *educational* and empowering measures to improve citizens and state employees' *digital media literacy* and critical faculties (Apuke & Omar, 2021; Eccles et al. 2021; Seo et al., 2021; Vese, 2022). This aligns with the democratic concept of free and equal citizens participating in the political process, and it is an important task for democracies to encourage their citizens to become well informed and critical (Kellner & Share 2007). However, one strategy of disinformation actors is to assert that they are the 'real' critical thinkers who decry state policies and ideologies. Thus, for Jarvis (2017), "our problem isn't 'fake news.' Our problem is trust". People tend to believe right-wing populists because "of a lack of basic trust in liberal institutions" (Mounk, 2017). Therefore, educational strategies should include why certain media and agencies can be trusted more than others (e.g., due to (self-)regulation, institutional standards, established scientific and journalistic methods), and how to identify trustworthy sources. Government security agencies themselves can increase citizens' trust through trustworthy communication. Such communication by public authorities is fair, responsible, transparent, appreciative, empowering, and reliable (Gabel & Krüger, 2020). This also holds true if *psychological inoculation* becomes part of media literacy trainings by government agencies. People should agree to it beforehand, and government agencies should be transparent. The highlighting of *descriptive and injunctive social norms* is, however, problematic: In democracies, government agencies can communicate laws, regulations, and democratic norms, but they should be cautious when promoting social behaviors. It may be perceived as patronizing and disadvantage groups, e.g., if users are encouraged to report disinformation (Gimpel et al., 2021), this could increase reports of certain minority opinions.

Debunking (e.g., publishing corrections) by government agencies can directly counter disinformation. In a democracy, this must not undermine the public opinion-forming process (requirement of objectivity, no exaggerated evaluative tendency, see Ferreau (2020) and the legal perspectives). In any case, agencies must create transparency about the source of information. There is also the risk that debunking will be abused for propaganda or to discredit and suppress legitimate opinions with state resources and authorities. Fact-checking institutions should therefore be independent (Ferreau, 2020).

As a *technical measure*, government agencies can employ *detection algorithms* to identify disinformation automatically. However, monitoring citizens' communication may violate privacy and data protection, requiring special justification. In addition, citizens may feel restricted in their freedom of expression: The mere uncertainty as to whether disadvantages could arise from automated monitoring can reduce political participation (Loh, 2021). Besides, automatic detection should be transparent and the affected must be able to appeal against potential false positives. *Social bots* could also automate debunking and informing the public. Bots operate on a large scale and are widely used by states and political groups to influence public opinion (Woolley, 2020). Their use is highly controversial. Arguments range from ideas on how "good" bots can counter misinformation to a complete ban on bots used by states (Ferreau, 2020).

4.2 Legal Discussion of Government Measures against Disinformation

The use of *technical measures* to detect and prevent disinformation raises several legal issues (Milker, 2018). The evaluation of these in this paper, considering the sovereignty of European nation states, can only refer to the German legal system and German legal literature. Here, the focus is on the German Basic Law, the foundation of a functioning democratic constitutional state, as this is the standard against which state action by the government agencies focused on in this project is to be measured (Starck, 2005; Schmidt-Jortzig, 2009). Especially where *social bots* are used by government agenices, a violation of various German Basic Law may ensue. Above all, the right to freedom of expression, protected by Article 5 (1) of the German Basic Law, which guarantees individuals the right to express themselves (publicly) according to their individual views, can be violated (on this already in the previous (ethical) section; Bethge, 2021; Müller-Franken, 2013). Whether a statement is protected or not depends on whether it is considered a value judgment or a statement of fact (Holznagel, 2018; Starck/Paulus, 2018). Intentionally made, untrue statements of fact as well as value judgments, which sole purpose is to defame another person, do not fall within the remit of protection of Art. 5 sec. 1 GG (Schulze-Fielitz, 2013; Starck/Paulus, 2018 and Hillgruber, 2016). All other statements fall within the scope of freedom of expression (Holznagel, 2018). In addition to protecting freedom of expression, this fundamental right also protects the freedom to form opinions, i.e. the right to obtain information from all publicly accessible sources (Bethge, 2021; Schmidt-Jortzig, 2009; Starck/Paulus, 2018; Kloepfer, 2005).

The prevention of disinformation by governmental agencies may infringe the freedom of expression in different ways. It is commonly accepted, that the mere dissemination of information by the state to its citizens – e.g., regarding a roadblock due to an ongoing protest – does not amount to an infraction of freedom of opinion (Tschorr,

2020). However, *debunking* by publishing corrections by the government agencies may violate freedom of expression if it relates to a specific person and his or her previous statement that differs from the state's communication content, as it may lead to stigmatization of that person, which in turn may affect social reputation (Schoch, 2011).

Based on those distinctions, different requirements must be met by the government agencies. Where a basic law is violated, the reservation of the law (Art. 20 sec. 3 GG) requires that the government agencies may only act, where it was enabled to do so by an Act of Parliament (Grzeszick, 2021; Kokott, 2004). In the context of *debunking*, the state must further adhere to the principles of neutrality, objectivity, and correctness (Tschorr, 2020; Starck/Paulus, 2018; Battis/Edenharter, 2022; Masing, 2012; Ingold, 2017; on the requirement of objectivity see in the previous section). More recent case law found *debunking* by the government agencies to be a functional equivalent of the "classic" violation of a basic right, if it equals such in its aim and effects (Schoch, 2011; Ingold, 2017). As well as regarding the use of *social bots* an infringement must be considered separately against the background in each individual case - under consideration of the problematic content and its ability to affect the basic rights of individuals.

It must further be taken into account, that *debunking* by the government agencies aims to enable independent opinion forming and participation in social matters – however without formative influence by the governmnet agencies (Tschorr, 2020; Starck/Paulus, 2018; Kloepfer, 2005; Müller-Franken, 2013; Hillgruber, 2016; Masing, 2012). If and to what extent this can be realized by using *social bots* must be analyzed critically. Especially when considering that the state uses its own far-reaching social media accounts, this may be regarded as an infringement on the citizens' freedom to voice an opinion (Milker, 2018). The same applies, where government agencies *correct* statements made by third parties using *social bots* (Sachs, 2021). However, violations of the freedom of expression may be constitutionally justified. This is determined by the principle of reasonableness, whereby a violation of freedom may be acceptable if it is suitable, necessary, and appropriate to achieve a legitimate aim (Kotzur, 2021; Battis/Edenharter, 2022; BVerfGE 65, 1 (54)). In addition, the agencies must openly declare the use of *social bots* (Laude, 2021) and limit its action to the person who poses a threat to public safety and order (Goldhammer, 2021; Herzog, 2006).

5 Open Research Questions

Based on our systematic review of IS research on disinformation prevention as well as the ethical and legal discussion above, we outline key questions for further research.

5.1 IS Research Questions Regarding Measures against Disinformation

From an IS perspective, the questions of how disinformation spreads on social networks and what content and network characteristics can be used to automatically detect disinformation are of particular interest. Nevertheless, the scientific literature lacks more detailed analyses to identify (influential) spreaders to prevent the dissemination process. While previous studies also revealed that personal dispositions such as the user's

online trust, self-disclosure, or fear of missing out are positively associated with intentionally sharing fake news (Talwar et al., 2019), it remains an open question what and how further information about a user can be automatically inferred from their historical and behavioral social media data to predict likely spreaders of disinformation. Furthermore, the question arises as how to address these users appropriately.

Moreover, countering disinformation raises the fundamental question of which design elements can encourage users to engage critically with the information. However, while there are promising results demonstrating the effectiveness of fact-checking flags (Gaozhao, 2021), there are also conflicting results (Moravec et al., 2019) which suggests that further research is required. In addition, labeling assessments made by professional fact-checkers or through crowdsourcing have been found to be equally influential (Gaozhao, 2021) but the question of the acceptance and influence of automated fact-checking, e.g., by bots, remains unanswered. With respect to social bots, Guzmán Rincón et al. (2022) included them as spreaders in simulation environments to analyze and educate in behavioral patterns of disinformation for decision making, but the authors address the need to deepen various analyses and to complement this educational simulation model. In this regard, it remains of interest to not only examine how governmental agencies can strategically employ social bots to spread verified information but also how bots can be integrated in an educational simulation environment to support decision-making processes by also evaluating the accountability of algorithmic decision-making. In doing so, further research questions such as how psychological strategies can be implemented to reach social media users should be considered.

5.2 Ethical Questions Regarding Measures against Disinformation

There is a broad debate about disinformation harming democracy (for a summary thereof see McKay & Tenove (2021). Likewise, observers fear that measures to counter disinformation can also negatively affect democracy (Vese, 2022; European Parliament, 2021). Government agencies thus need more research as to whether they should counter specific pieces of disinformation or not. We raise fundamental ethical questions that government agencies should always consider anew and context-specifically when countering disinformation. More case-specific research – e.g., in form of best practices – is needed to help government agencies with these fundamental questions.

The first question for government agencies is who gets to decide what counts as disinformation. Are automated algorithmic decision-making mechanisms suitable here, or do humans ultimately have to decide? The second question is how actors can distinguish disinformation from legitimate expressions of opinion in a pluralistic society. Next, they must decide whether a specific piece of disinformation restricts the democratic functions of the public sphere or whether it is merely an expression of pluralism and the freedom of opinion in the "marketplace of ideas" (Mill, 1859). A functioning deliberative democracy should be able to withstand some false or misleading statements because it "filters out and discards the worst ideas" (Mansbridge, 1999). Such statements may even serve a function, e.g., by raising the tensions that motivate political debates (Mouffe, 2005). In any case, decision-makers must communicate their decisions transparently, and in a way that allows those affected to appeal against them.

To decide whether to counter disinformation, actors need to conduct a context-sensitive evaluation in each case to determine potential value conflicts. Open questions are how can decision-makers balance value conflicts between the functioning of the public sphere, freedom (including free speech), security, privacy, personal expression, and transparency? E.g., may they restrict freedom rights in the name of security when false information endangers life? Under which circumstances would this be justified? Do they consider broader dimensions, such as balancing individual and collective interests? The fundamental question here is how government agencies can strengthen the resilience of the open society against disinformation without sacrificing the principle of tolerance that is central to liberal democracies. Finally, beyond considering citizens' defensive and protective rights, citizens should also be enabled to use the digital space productively in the sense of informational self-determination and empowerment.

5.3 Legal Research Questions Regarding Measures Against Disinformation

After a view over the German Basic Law, which sets the ground rules for government agencies' action, it can be said that the constitutional state should be a guarantee for freedom on the one hand, but also for security on the other (Starck, 2005). The individual's freedom finds its limits where it inappropriately curtails another's. The German state is granted a monopoly of force to meet this security objective (Papier, 2017; Herzog, 2006). Though, this objective may not run counter to the liberal and freedom-guaranteeing function of the state. The state must thus limit itself (Kloepfer, 2005; Volkmann, 2004). For the sake of a functioning democratic constitutional state, the source of voluntary loyalty to the law must be located and, if necessary, strengthened, or at least prevented from weakening. To bring about such acceptance of the laws and the rule of law among the population, reliance is placed on the communicative reason of the individual, derived from communicative action (Habermas 1998; Hill, 1988).

If society relies too strongly on the government agencies' duty to protect in the fight against and prevention of disinformation campaigns, it will come at the expense of the citizens' self-responsibility. A central question (from an ethical and legal perspective) is therefore how much individual responsibility should be transferred to the state in dealing with disinformation campaigns. The goal in preventing disinformation, including the tools used (e.g., *social bots*), should not be to limit the individual's autonomy, but to enhance it (Mafi-Gudarzi (2019); "self-defensive democracy" as called by Bayer et al. (2021); also "informational self-determination" as in the previous (ethical) section; Müller-Franken, 2013; Hillgruber, 2016; Masing, 2012), 2016; Masing, 2012)

A first and controversial (German) national approach to deal with disinformation is the passage of the Network Enforcement Act (Netzwerkdurchsetzungsgesetz = NetzDG). This legislation is to be used to fight against criminal fake news and hate speech on *social media* networks (BT-Drs. 18/12356): Social network providers are obligated to produce an effective and transparent procedure to deal with illegal content. Content, which is obviously illegal, must be *removed* within 24h, other illegal content within 7 days acc. to the NetzDG. This approach is criticized for shifting the responsibility to ensure public order onto private social networks (Guggenberger, 2017; Dank-

ert, 2018). Another important point of criticism is, that it gives rise to the risk that content containing opinions are deleted by provider "preventatively" as the NetzDG stipulates high monetary fines but simultaneously very short time frames for deletion (Papier, 2017; Rostalski, 2017). Thus, even with the passage of the NetzDG, the state runs the risk that it opens the scope for invasive infringement of the basic rights of users and the creation of a "censorship authority" (Guggenberger, 2017). This must be considered when creating means to fight disinformation campaigns. Following on from this, the Digital Services Act (DSA, COM (2020) 825 final) of November 16, 2022, is intended to contribute to a safe, predictable and trustworthy online environment at European level from February 17, 2024, by imposing due diligence obligations and liability exclusions for intermediary services such as online platforms. This includes, for example, a Europe-wide uniform design of procedures for reporting and prompt removal of illegal content, as well as additional due diligence requirements for very large online platforms and search engines. The focus is on a form of *regulated self-regulation* by platform operators in which the role of state actors in action against illegal content remains an indirect one, for example through the preferential treatment of reports from various (also state) actors when they are qualified as "trusted flaggers" (Article 19).

6 Conclusion

This article identified measures government agencies can apply to counter digital disinformation campaigns based on a systematic literature review of IS research. It then discussed these measures from an ethical and legal perspective. Due to the nature of systematic literature reviews, our study has some limitations. Subjective decisions regarding the selection of databases, keywords, and exclusion criteria may have resulted in a neglect of relevant articles. Furthermore, the ethical discussion on democratic states and the legal discussion focusing on German law cannot be directly applied to other political and legal systems. Lastly, further research is needed to apply our findings to real-world disinformation campaigns, tracing their origin and spread and discussing government agencies' responses combining IS, legal, and ethical perspectives.

Notwithstanding, our paper contributes to a nuanced discussion of measures against disinformation in IS research, but also in practice, with a focus on government agencies. As shown, the literature discusses only few preventative measures explicitly designed for government agencies, so there is a need for more research on measures against disinformation suitable for government agencies. From a technical view, open research questions include how psychological insights can be used to, e.g., strategically employ social bots for educational purposes, to spread verified information or counter disinformation. From an ethical and legal perspective, government agencies must contribute to a safe, predictable, and trustworthy online environment at the national, but also the European level and strengthen the self-defensive democracy. At the same time, they must consider the risks that countering disinformation may constitute an invasive infringement of users' basic rights and create a censorship authority. Government agencies thus need to balance value conflicts between the functioning of the public sphere, freedom, security, privacy, and personal expression.

References

Akkaya, C., Fedorowicz, J. & Krcmar, H. (2019). Successful Practices for Using Social Media by Police Departments: A Case Study of the Munich Police. *European Conference on Information Systems*.

Al-Asadi, M. A. & Tasdemir, S. (2022). Using Artificial Intelligence Against the Phenomenon of Fake News: A Systematic Literature Review. In M. Lahby, A.-S.K. Pathan, Y. Maleh & W.M.S. Yafooz (Hrsg.), *Studies in Computational Intelligence. Combating Fake News with Computational Intelligence Techniques* (S. 39–54). Springer.

Allcott, H. & Gentzkow, M. (2017). Social media and fake news in the 2016 election. *Journal of Economic Perspectives*, *31* (2), 211–236.

Amoruso, M., Anello, D., Auletta, V., Cerulli, R., Ferraioli, D. & Raiconi, A. (2020). Contrasting the Spread of Misinformation in Online Social Networks. *Journal of Artificial Intelligence Research*, *69*, 847–879.

Apuke, O. D. & Omar, B. (2021). Modelling the antecedent factors that affect online fake news sharing on COVID-19: The moderating role of fake news knowledge. *Health Education Research*, *35* (7), 490–503.

Arayankalam, J. (2020). Disinformation as a strategic weapon: Roles of societal polarization, government's cybersecurity capability, and the rule of law. *International Conference on Information Systems*.

Balakrishnan, V., Ng, K. S. & Rahim, H. A. (2021). To share or not to share – The underlying motives of sharing fake news amidst the COVID-19 pandemic in Malaysia. *Technology in Society*, *66*.

Battis, U., Edenharter, A. (2022). Einführung in das Verfassungsrecht, 291 f., 335 ff.

Bayer, J., Holznagel, B., Lubianiec, K., Pintea, A., Schmitt, J. B., Szakács, J. et al. (2021). *Disinformation and propaganda: impact on the functioning of the rule of law and democratic processes in the EU and its Member States - 2021 update -*. Brussels. Availabale at: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653633/EXPO_STU(2021)653633_EN.pdf (Accessed: 01 March 2023)

Bethge, H. (2021). Art. 5 GG, Rn.18, 24. *Grundgesetz Kommentar* (9. Auflage). Sachs.

Boell, S. & Wang, B. (2019). www.litbaskets.io, an IT Artifact Supporting Exploratory Literature Searches for Information Systems Research. *Australian Conference on Information Systems*.

Brachten, F., Mirbabaie, M., Stieglitz, S., Berger, O., Bludau, S. & Schrickel, K. (2018). Threat or Opportunity?-Examining Social Bots in Social Media Crisis Communication. *Australasian Conference on Information Systems*.

vom Brocke, J., Simons, A., Riemer, K., Niehaves, B., Plattfaut, R. & Plattfaut, R. (2015). Standing on the Shoulders of Giants: Challenges and Recommendations of Literature Search in Information Systems Research. *Communications of the Association for Information Systems*, *37* (9), 205–224.

Brown, É. (2018). Propaganda, Misinformation, and the Epistemic Value of Democracy. *Critical Review*, *30* (3), 194–218.

Cao, C., Hu, Y. & Yu, L. (2015). Containment of Rumors under Limit Cost Budget in Social Network. *Wuhan International Conference on E-Business*.

da Cardoso Durier Silva, F., Vieira, R. & Garcia, A. C. (2019). Can Machines Learn to Detect Fake News? A Survey Focused on Social Media. *Hawaii International Conference on System Sciences*.

Chen, Q., Srivastava, G., Parizi, R. M., Aloqaily, M. & Ridhawi, I. al. (2020). An incentive-aware blockchain-based solution for internet of fake media things. *Information Processing & Management*, *57* (6), 102370.Coleman, S. (2012). Believing the news: From sinking trust to atrophied efficacy. *European Journal of Communication*, 27(1), 35–45.

Crook, B., Glowacki, E. M., Suran, M., K. Harris, J. & Bernhardt, J. M. (2016). Content Analysis of a Live CDC Twitter Chat During the 2014 Ebola Outbreak. *Communication Research Reports*, *33* (4), 349–355.

Dankert, K. (2018). Verfälschung von Datenbeständen durch Social Bots. In W. Hoffmann-Riem (Hrsg.). Big Data - Regulative Herausforderungen, 157-166.

DiFonzo, N. & Bordia, P. (2007). *Rumor Psychology: Social and Organizational Approaches*. Washington, DC: American Psychological Association.

Eccles, D., Kurnia, S., Dingler, T. & Geard, N. (2021). Three Preventative Interventions to Address the Fake News Phenomenon on Social Media. *Australian Conference on Information Systems*.

European Parliament, Directorate-General for External Policies of the Union, Colomina, C., Sánchez Margalef, H., Youngs, R.et al. (2021). *The impact of disinformation on democratic processes and human rights in the world.* European Parliament, 2021, https://data.europa.eu/doi/10.2861/59161.

Fallis, D. (2009). A conceptual analysis of disinformation. *iConference*.

Farkas, J. (2018). Disguised Propaganda on Social Media. Addressing Democratic Dangers and Solution. *Brown Journal of World Affairs*, *25* (1), 1–16.

Ferrara, E., Varol, O., Davis, C., Menczer, F. & Flammini, A. (2016). The rise of social bots. *Communications of the ACM*, *59* (7), 96–104.

Ferreau, F. (2020). Desinformation aus rechtswissenschaftlicher Perspektive. In J. Möller, M. Hameleers & F. Ferrau (Hrsg.), *Typen von Desinformation und Misinformation. Verschiedene Formen von Desinformation und ihre Verbreitung aus kommunikationswissenschaftlicher und rechtswissenschaftlicher Perspektive* (S. 44–78). ALM GbR.

Figl, K., Kießling, S., Rank, C. & Vakulenko, S. (2020). Fake News Flags, Cognitive Dissonance, and the Believability of Social Media Posts. *International Conference on Information Systems*.

Gabel, F. & Krüger, M. (2020). Leitfaden für eine ethisch reflektierte Krisenkommunikation - Eine Analyse wertbezogener Spannungsfelder in der Krisenkommunikation. *Materialien zur Ethik in den Wissenschaften, Band 15*. IZEW.

Gaozhao, D. (2021). Flagging fake news on social media: An experimental study of media consumers' identification of fake news. *Government Information Quarterly*, *38* (3).

Gimpel, H., Heger, S., Olenberger, C. & Utz, L. (2021). The Effectiveness of Social Norms in Fighting Fake News on Social Media. *Journal of Management Information Systems*, *38* (1), 196–221.

Giusti, S. & Piras, E. (2021). *Democracy and Fake News: Information Manipulation and Post-Truth Politics*. Routledge.

Goldhammer, M. (2021). Verantwortlichkeit im Polizeirecht. *Juristische Ausbildung*, *43* (6), 638–650.

Gorwa, R., Binns, R. & Katzenbach, C. (2020). Algorithmic content moderation: Technical and political challenges in the automation of platform governance. *Big Data and Society*, *7* (1).

Grzeszick, B. (2021). Art. 20 GG, Rn. 81. *Grundgesetz Kommentar*. Dürig/Herzog/Scholz.

Guggenberger, N. (2017). Das Netzwerkdurchsetzungsgesetz – schön gedacht, schlecht gemacht. *Zeitschrift für Rechtspolitik*, *98*, 89–101.

Guzmán Rincón, A., Carrillo Barbosa, R. L., Segovia-García, N. & Africano Franco, D. R. (2022). Disinformation in Social Networks and Bots: Simulated Scenarios of Its Spread from System Dynamics. *Systems*, *10* (2).

Habermas, J. (1998). Faktizität und Geltung. Beiträge zur Diskurstheorie des Rechts und des demokratischen Rechtsstaats. Frankfurt a. M.: Suhrkamp.

Habermas, J. (2022). Reflections and hypotheses on a further structural transformation of the political public sphere. *Theory, Culture & Society*, *39*(4), 145-171.

Hasan, H. R. & Salah, K. (2019). Combating Deepfake Videos Using Blockchain and Smart Contracts. *IEEE Access*, *7*, 41596–41606.

Heesen, J. (2021). Responsible Freedom. The Democratic Challenge of Regulating Online Media. In L.T. Price, K. Sanders & W.N. Wyatt (Hrsg.), *The Routledge Companion to Journalism Ethics* (S. 435–442). Routledge.

Herzog, R. (2006). § 72 Ziele, Vorbehalte und Grenzen der Staatstätigkeit. In J. Isensee, P. Kirchhof (Hrsg.). Handbuch des Staatsrechts, Band IV, 38 f., 47, 49.

Hill, H. (1988). Akzeptanz des Rechts — Notwendigkeit eines besseren Politikmanagements, *Juristen Zeitung* (377-381).

Hillgruber, C. (2016). Meinungsfreiheit als Grundrecht der Demokratie: Der Schutz des demokratischen Resonanzbodens in der Rechtsprechung des BVerfG, *Juristen Zeitung* (495-501).

Hofeditz, L., Ehnis, C., Brachten, F. & Stieglitz, S. (2019). Meaningful Use of Social Bots? Possible Applications in Crisis Communication during Disasters. *European Conference on Information Systems*.

Holznagel, B. (2018). Phänomen „Fake News" – Was ist zu tun? *Multimedia und Recht*, *18*, 18–22.

Ingold, A. (2017). »Polizei 2.0«: Grenzen der behördlichen Öffentlichkeitsarbeit in sozialen Netzwerken, *Verwaltungsarchiv* (240-265).

Ivanova, Y. (2019). Can EU Data Protection Legislation Help to Counter "Fake News" and Other Threats to Democracy? *International Conference on e-Democracy*.

Jarolimek, S. & Melzer, A. (2022). Öffentliche Kommunikation, Polizei und Corona. In H.-J. Lange (Hrsg.), *Politik zwischen Macht und Ohnmacht, Studien zur inneren Sicherheit* (S. 341–361). Wiesbaden: Springer.

Jarvis, J. (2017, Juni 12). Our problem isn't 'fake news.' Our problems are trust and manipulation. *Medium*. Zugriff am 13.6.2022. Verfügbar unter: https://medium.com/whither-news/our-problem-isnt-fake-news-our-problems-are-trust-and-manipulation-5bfbcd716440

Jeong, D., Han, S.-P., Park, S. & Lee, S. K. (2020). Fighting Abuse while Promoting Free Speech: Policies to Reduce Opinion Manipulation in Online Platforms. *Hawaii International Conference on System Sciences*.

Jin, Z., Cao, J., Zhang, Y. & Luo, J. (2016). News Verification by Exploiting Conflicting Social Viewpoints in Microblogs. *AAAI Conference on Artificial Intelligence*.

Kapantai, E., Christopoulou, A., Berberidis, C. & Peristeras, V. (2021). A systematic literature review on disinformation: Toward a unified taxonomical framework. *New Media & Society*, *23* (5), 1301–1326.

Kaul, V. (2022). Freedom of speech in liberal and non-liberal traditions. *Philosophy & Social Criticism*, *48*(4), 460–472.

Kellner, D., & Share, J. (2007). Critical media literacy: Crucial policy choices for a twenty-first-century democracy. *Policy Futures in Education*, *5*(1), 59-69.

Kim, A. & Dennis, A. R. (2019). Says Who? The Effects of Presentation Format and Source Rating on Fake News in Social Media. *MIS Quarterly*, *43* (3), 1025–1039.

Kloepfer, M. (2005). § 42 Öffentliche Meinung, Massenmedien. In J. Isensee, P. Kirchhof (Hrsg.). Handbuch des Staatsrechts, Band III, 11 f., 44 f., 51.

Kocur, A., Clausen, S., Hofeditz, L., Brünker, F., Fromm, J., Stieglitz, S. 2023. Figthing False Information - Designin a Conversational Agent for Public Sector Organizations. *European Conference on Information Systems.*

Kokott, J. (2004). § 22 Grundrechtliche Schranken und Schrankenschranken. In D. Merten, H.-J. Papier (Hrsg.), Handbuch der Grundrechte, Band I, 20 f.

Kotzur, M. (2021). Art. 20 GG, Rn. 163. *Grundgesetz Kommentar* (7. Auflage). Münch/Kunig.

Lahby, M., Pathan, A.-S. K., Maleh, Y. & Yafooz, W. M. S. (2022). *Combating Fake News with Computational Intelligence Techniques*. (M. Lahby, A.-S.K. Pathan, Y. Maleh & W.M.S. Yafooz, Hrsg.). Springer.

Laude, L. (2021). *Automatisierte Meinungsbeeinflussung: Der Schutz des Kommunikationsprozesses in sozialen Online-Netzwerken*. Mohr Siebeck.

Li, M.-H., Chen, Z. & Rao, L.-L. (2022). Emotion, analytic thinking and susceptibility to misinformation during the COVID-19 outbreak. *Computers in Human Behavior*, *133*.

Loh, W. (2021). Soziale Medien. In M.G. Festl (Hrsg.), *Handbuch Liberalismus* (S. 543–551). Metzler.

Mafi-Gudarzi, N. (2019). Desinformationen: Herausforderungen für die wehrhafte Demokratie. *Zeitschrift für Rechtspolitik*, *3*, 65–68.

Mansbridge, J. (1999). Everyday Talk in the Deliberative System. In S. Macedo (Hrsg.), *Deliberative Politics: Essays on Democracy and Disagreement* (S. 1–211). Oxford University Press.

Marx, J., Brünker, F., Mirbabaie, M. & Hochstrate, E. (2020). 'Conspiracy Machines'-The Role of Social Bots during the COVID-19 „Infodemic". *Australasian Conference on Information Systems*.

Masing, J. (2012), Meinungsfreiheit und Schutz der verfassungsrechtlichen Ordnung, *Juristen Zeitung* (585-592).
McKay, S. & Tenove, C. (2021). Disinformation as a Threat to Deliberative Democracy. *Political Research Quarterly*, *74* (3), 703–717.
Meel, P. & Vishwakarma, D. K. (2020). Fake news, rumor, information pollution in social media and web: A contemporary survey of state-of-the-arts, challenges and opportunities. *Expert Systems with Applications*, *153*. Elsevier Ltd.
Milker, J. (2018). Die Polizei auf Twitter – Brauchen wir ein Social-Media-Gesetz für staatliche Stellen? *Neue Zeitschrift für Verwaltungsrecht*, *23*, 1751–1758.
Mill, J. S. (1859). *On Liberty*. Hackett Publishing Company.
Moravec, P., Minas, R. & Dennis, A. R. (2019). Fake News on Social Media: People Believe What They Want to Believe When it Makes No Sense at All. *MIS Quarterly*, *43* (4), 1343–1360.
Mouffe, C. (2005). *On the Political*. Routledge.
Mounk, S. (2017, Juli 13). Rechtspopulismus. Anti. Autoritär. *Zeit-Online*. Available at: https://www.zeit.de/2017/29/rechtspopulismus-bildung-neue-rechte (Accessed 13 June 2022).
Müller-Franken, S. (2013). *Meinungsfreiheit im freiheitlichen Staat*, 27, 51, 53.
Nagasako, T. (2020). A Consideration of the Case Study of Disinformation and Its Legal Problems. *IFIP International Conference on Human Choice and Computers*.
Narayan, S. & Attili, V. S. P. (2021). Combating the spread of fake news ons ocial media through a blockchain-led intervention. *American Conference on Information Systems*.
Nazar, S. & Pieters, T. (2021). Plandemic Revisited: A Product of Planned Disinformation Amplifying the COVID-19 "infodemic". *Frontiers in Public Health*, *9*.
Ng, K. C., Tang, J. & Lee, D. (2021). The Effect of Platform Intervention Policies on Fake News Dissemination and Survival: An Empirical Examination. *Journal of Management Information Systems*, *38* (4), 898–930.
Nguyen, H. T., Cano, A., Vu, T. & Dinh, T. N. (2020). Blocking Self-Avoiding Walks Stops Cyber-Epidemics: A Scalable GPU-Based Approach. *IEEE Transactions on Knowledge and Data Engineering*, *32* (7), 1263–1275.
Nickerson, R. S. (1998). Confirmation Bias: A Ubiquitous Phenomenon in Many Guises. *Review of General Psychology*, *2* (2), 175–220.
Nobre, G. P., Ferreira, C. H. G. & Almeida, J. M. (2021). A Hierarchical Network-Oriented Analysis of User Participation in Misinformation Spread on WhatsApp. *Information Processing & Management*, *59* (1).
Ozturk, P., Li, H. & Sakamoto, Y. (2015). Combating Rumor Spread on Social Media: The Effectiveness of Refutation and Warning. *Hawaii International Conference on System Sciences*.
Papier, H.-J. (2017). Rechtsstaatlichkeit und Grundrechtsschutz in der digitalen Gesellschaft. *Neue Juristische Wochenschrift*, *42*, 3025–3031.Parvin, P. (2015). Is Deliberative Democracy Feasible? Political Disengagement and Trust in Liberal Democratic States. *The Monist*, 98(4), 407–423.

Pawelec, M. (2022). Deepfakes and Democracy (Theory): How Synthetic Audio-Visual Media for Disinformation and Hate Speech Threaten Core Democratic Functions. *Digital Society*, *1* (19), 1–37.

Piccolo, L. S. G., Bertel, D., Farrell, T. & Troullinou, P. (2021). Opinions, Intentions, Freedom of Expression, ..., and Other Human Aspects of Misinformation Online. *Conference on Human Factors in Computing Systems*.

Plandemic. (2022). Plandemic – 100% Censored. 0% Debunked. *Plandemic*. Zugriff am 30.5.2022. Verfügbar unter: https://plandemicseries.com/

Plattner, M.F. (1999). From Liberalism to Liberal Democracy. *Journal of Democracy 10*(3), 121-134.

Puppis, M. (2014). The regulation of political communication. In C. Reinemann (Hrsg.), *Political communication. Series: Handbooks of Communication Science* (S. 39–62). De Gruyter Mouton.

Radu, R. (2020). Fighting the 'Infodemic': Legal Responses to COVID-19 Disinformation. *Social Media and Society*, *6* (3).

Reporters without Borders. (2018). Global communication and information space: a common good of humankind. *Reporters without Borders*. Zugriff am 13.6.2022. Verfügbar unter: https://rsf.org/en/global-communication-and-information-space-common-good-humankind

Rostalski, F. (2017). „Fake News" und die „Lügenpresse" – ein (neuer) Fall für das Straf- und Ordnungswidrigkeitenrecht? *Rechtswissenschaft*, *4*, 436–460.

Saad, M., Ahmad, A. & Mohaisen, A. (2019). Fighting Fake News Propagation with Blockchains. *IEEE Conference on Communications and Network Security*.

Sachs, M. (2021). Art. 20 GG, Rn. 113. *Grundgesetz Kommentar* (9. Auflage). Sachs.

Schmidt-Jortzig, E. (2009). § 162 Meinungs- und Informationsfreiheit. In J. Isensee, P. Kirchhof (Hrsg.). Handbuch des Staatsrechts, Band VII, 9, 22, 33 f.

Schoch, F. (2011). Die Schwierigkeiten des BVerfG mit der Bewältigung staatlichen Informationshandelns. *Neue Zeitschrift für Verwaltungsrecht*, *4*, 193–197.

Schulze-Fielitz, H. (2013). Art. 5 Abs. 1-2 GG. *Grundgesetz Kommentar* (3. Auflage). Dreier.

Seo, H., Thorson, S., Blomberg, M., Appling, S., Bras, A., Davis-Roberts, A. et al. (2021). Country Characteristics, Internet Connectivity and Combating Misinformation: A Network Analysis of Global North-South. *Hawaii International Conference on System Sciences*.

Starck, C. (2005). § 33 Grundrechtliche und demokratische Freiheitsidee. In J. Isensee, P. Kirchhof (Hrsg.). Handbuch des Staatsrechts, Band III, 14 f., 8 f., 11.

Starck, C, Paulus, A. (2018). Art. 5. In H. v. Mangoldt, F. Klein, C. Starck, Grundgesetz Band 1, 76, 81 ff, 166, 169.

Talwar, S., Dhir, A., Kaur, P., Zafar, N. & Alrasheedy, M. (2019). Why do people share fake news? Associations between the dark side of social media use and fake news sharing behavior. *Journal of Retailing and Consumer Services*, *51*, 72–82.Tenove, C. (2020). Protecting democracy from disinformation: Normative threats and policy responses. *The International Journal of Press/politics*, 25(3), 517–537.

Tran, T., Valecha, R., Rad, P. & Rao, & H. R. (2019). An Investigation of Misinformation Harms Related to Social Media during Two Humanitarian Crises. *International conference on secure knowledge management in artificial intelligence era*.

Tschorr, S. (2020). Verfassungsrechtliche Grenzen der twitternden Polizei im Rahmen von Großveranstaltungen und Versammlungen. *Neue Juristische Wochenschrift*, 3755–3759.

Vemprala, N., Gudigantala, N. & Chaganti, R. (2021). Debunking Misinformation Using a Game Theoretic Aprpoach. *American Conference on Information Systems*.

Vese, D. (2022). Governing Fake News: The Regulation of Social Media and the Right to Freedom of Expression in the Era of Emergency. *European Journal of Risk Regulation*, *13* (3), 477–513.

Volkmann, U. (2004). Sicherheit und Risiko als Probleme des Rechtsstaats, *Juristen Zeitung (696-703)*.

Vraga, E. K. & Bode, L. (2017). Using Expert Sources to Correct Health Misinformation in Social Media. *Science Communication*, *39* (5), 621–645.

Wang, S. (Ada), Pang, M.-S. & Pavlou, P. A. (2021). Cure or Poison? Identity Verification and the Posting of Fake News on Social Media. *Journal of Management Information Systems*, *38* (4), 1011–1038.

Wardle, C. (2019). A New World Disorder. *Scientific American*, *321* (3), 88–93.

Wardle, C. & Derakhshan, H. (2017). *INFORMATION DISORDER: Toward an interdisciplinary framework for research and policy making Information Disorder Toward an interdisciplinary framework for research and policymaking*. Zugriff am 1.3.2023. Verfügbar unter: https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277cWarren, M. E. (2017). A Problem-Based Approach to Democratic Theory. *American Political Science Review*, 111(1), 39–53.

Waszak, P. M., Kasprzycka-Waszak, W. & Kubanek, A. (2018). The spread of medical fake news in social media – The pilot quantitative study. *Health Policy and Technology*, *7* (2), 115–118.

Webster, J. & Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly*, *26* (2), 13–23.

Woolley, S. C. (2020). Bots and Computational Propaganda: Automation for Communication and Control. In N. Persily & J.A. Tucker (Hrsg.), *Social media and democracy. The state of the field, prospects for reform* (S. 89–110). Cambridge University Press.

Zhou, C., Li, K. & Lu, Y. (2021). Linguistic characteristics and the dissemination of misinformation in social media: The moderating effect of information richness. *Information Processing and Management*, *58* (6).