III.
AI, Consumer Protection, and Online Governance in a Digital World

The Regulation of Disinformation in the EU – Overview and Open Questions

Alexander Peukert[*]

Abstract: This article provides an overview of the current state of the regulation of disinformation in the EU. It shows that the concept of disinformation, the purpose of anti-disinformation measures and their content and enforcement can only be understood if a holistic view is taken of private, hybrid-co-regulatory and public law norms. The delicate field of disinformation is to a large extent dealt with outside of statutory law. The questions raised thereby are largely unresolved.

A. The Short History of Disinformation Regulation

"Disinformation" is a shimmering term. In the interim, it can be defined as a statement which is false or otherwise misleading and which has a negative impact on public interests, but which is not in itself unlawful.[1] State measures against such "harmful" content are delicate because they constitute an interference with communicative freedoms going beyond the general laws and the rights of third parties.[2] And indeed, Union law knows neither a legal definition nor an explicit legal prohibition of disinformation.[3]

---

* This is a translation of the article "Desinformationsregulierung in der EU: Überblick und offene Fragen", JuristenZeitung 2023, 278-286. Work on this article was completed in March 2023.

1 For more details see below, B.

2 High level group on fake news and online disinformation, A multi-dimensional approach to disinformation, 2018, 19 ('government or EU regulation of disinformation can be a blunt and risky instrument'); preamble lit. c Strengthened Code of Practice on Disinformation 2022, https://disinfocode.eu (in the following: Disinformation Code 2022) ('delicate balance').

3 Cf. European Commission, COM(2020) 825, 10; Pamment, The EU's Role in Fighting Disinformation: Crafting A Disinformation Framework, 2020, 2 et seq. One exception can be found in Lithuanian law, which prohibits the dissemination of disinformation in the media; cf. European Audiovisual Observatory, Mapping of national rules applicable to video-sharing platforms: Illegal and harmful content online, 2022, 290.

Nevertheless, the EU institutions have taken or promoted numerous measures against disinformation since 2015. According to the "European Declaration on Digital Rights and Principles for the Digital Decade" of 15 December 2022, there will be no change to this policy in the foreseeable future. This is because the Commission, Parliament and Council solemnly proclaim in this Declaration to continue their "fight" against disinformation in order to "create a digital environment in which people are protected from disinformation and information manipulation and other forms of harmful content, including harassment and gender-based violence".[4]

This policy goal enjoys broad support in social science and legal literature. According to this view, disinformation in the internet age poses a significant challenge to liberal Western-style democracies that requires regulation.[5] Firstly, due to the openness of political debate, these pluralistic societies are said to be in principle more susceptible to informational manipulation than autocratic systems.[6] Secondly, the functional logic of the Web 2.0 intensifies the dangers that have always emanated from false and misleading statements. Disinformation is easily created with digital tools such as image manipulation, spreads rapidly via social networks and other online services, and can be artificially amplified by manipulative measures such as bots.[7]

Three examples in particular are cited in academia and politics as evidence for these assumptions: disinformation campaigns by the Russian

4 Chapter IV no. 15 and lit. c European Declaration on Digital rights and Principles for the Digital Decade, 26.1.2022, https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles; OECD Declaration on a Trusted, Sustainable and Inclusive Digital Future, OECD/LEGAL/0488, 15.12.2022 (combatting disinformation online).

5 Literature overviews at Kapantai et al, New Media & Society 23(5) (2001), 1301 et seq.; de Place Bak/Walter/Bechmann, New Media & Society 2022, https://doi.org/10.1177/14614448221122146. Support can be found in legal academia, for instance in Hong, Rechtswissenschaft 2022, 126, 173; Kuhlmann/Trute, GSZ - Zeitschrift für das Gesamte Sicherheitsrecht, 2022, 115; with reservations Peukert, Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft, 2022, 57, 75 et seq.

6 Cf. Schünemann, in: Cavelty/Wenger (eds.), Cyber Security: Socio-Technological Uncertainty and Political Fragmentation, 2022, 32, 33 with further references.

7 Recital 5 sentence 2 Regulation 2022/2065 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ L 277/1 (in the following: DSA); European Commission, COM(2018) 236, 6 et seq.; Bennett/Livingston, European Journal of Communication 33(2) (2018), 122 et seq.; de Place Bak/Walter/Bechmann, New Media & Society 2022, https://doi.org/10.1177/14614448221122146.

government in the context of the Ukraine conflict (since 2014/2015),[8] "fake news" in the context of domestic events such as the Brexit referendum and the election of Donald Trump in 2016/2017,[9] and health-related disinformation on vaccines and other public health policies during the COVID-19 pandemic,[10] all of which served as catalysts for the regulation of disinformation.

In March 2015, the Council requested the then High Representative of the EU for Foreign Affairs and Security Policy to develop an action plan to counter Russia's disinformation campaigns.[11] As a result, the "East StratCom [Strategic Communication, A.P.] Task Force" was set up within the framework of the European External Action Service, which since September 2015 has been countering Russian disinformation in three fields of action by making EU communication more effective with regard to the countries of the Eastern Partnership, strengthening free and independent media in this region, and collecting examples of disinformation and presenting and correcting them on the website euvsdisinfo.eu as part of an awareness-raising campaign.[12] Germany reacted to the phenomenon of "fake news" in autumn 2017 with the Network Enforcement Act. At the end of that year, the Commission set up a high-level group of experts, which recommended numerous measures in March 2018, which in turn found their way into the ground-breaking Commission Communication

8 European Commission, JOIN(2018) 36, 5; European Commission, COM(2020) 790, 24.

9 de Place Bak/Walter/Bechmann, New Media & Society 2022, https://doi.org/10.1177/14614448221122146; Zimmermann/Kohring, M&K Medien & Kommunikationswissenschaft 66 (2018), 526 et seq.

10 On vaccination-related disinformation, see European Commission, JOIN(2018) 36, 4 et seq. and no. 9 lit. c Council Recommendation of 7.12.2018 on strengthened cooperation against vaccine-preventable diseases, OJ C 466/1. On the COVID-19 'infodemic' see WHO Coronavirus disease 2019 (COVID-19) Situation Report – 45, 5.3.2020; European Commission, JOIN(2020) 8; Kapantai/Christopoulou/Berberidis, New Media & Society 23(5) (2021), 1301, 1304.

11 http://www.consilium.europa.eu/de/press/press-releases/2015/03/20/conclusions-european-council/; Pamment, The EU's Role in Fighting Disinformation: Taking Back the Initiative, 2020, 7 ('In response to representations from a small group of concerned member states, the European Council ‚stressed the need to challenge Russia's ongoing disinformation campaigns' in March 2015.').

12 https://euvsdisinfo.eu/to-challenge-russias-ongoing-disinformation-campaigns-the-story-of-euvsdisinfo.

"Tackling online disinformation: a European Approach" of 26 April 2018.[13] The most important outcome of these activities was the EU Code of Conduct "tackling online disinformation", signed in October 2018, in which the major platform operators and advertising service providers (Facebook, Google, Twitter, and later also Microsoft and TikTok) committed to taking 15 measures against disinformation, including highlighting the accessibility of trustworthy content.[14] Finally, the COVID-19 pandemic proved to be a "test case" of the anti-disinformation measures previously taken, and a "stress test" for the Code of Conduct.[15] In response to a request from the Commission, the online platforms participating in the Code published monthly reports on their rules and measures against pandemic-related disinformation from August 2020 onwards.[16]

However, in the Commission's view, this additional transparency measure only revealed the structural weaknesses of the first Disinformation Code, which suffered from unclear definitions, unspecific obligations and, not least, a lack of sanctions.[17] For this reason, the Commission called on the signatories of the Code as well as other relevant actors (especially from the advertising industry) to participate in a revision and strengthening of the Disinformation Code 2018. The Commission provided itself with the leverage for this move in December 2020 by proposing the Digital Services Act (DSA).[18] From then on, the Commission emphasized that strengthening the Code "offers an early opportunity for stakeholders to de-

13 Cf. High level group (n 2); European Commission, COM(2018) 236, 3; European Commission, JOIN(2018) 36. On the origins of the German Network Enforcement Act (NetzDG) and its effects, see Peukert, in: Spiecker gen. Döhmann/Westland/Campos (eds.), Demokratie und Öffentlichkeit im 21. Jahrhundert – zur Macht des Digitalen, 2022, 229 et seq. Considerably more hesitant the Joint Declaration of the Special Rapporteur on Freedom of Opinion and Expression of the UN, the OECD, the Organization of American States and the African Commission on Human and Peoples' Rights, 3.3.2017, FOM.GAL/3/17, Freedom of Expression and 'Fake News', Disinformation and Propaganda.

14 No. (ix) Code of Practice on Disinformation https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation (in the following: Disinformation Code 2018); cf. European Commission, SWD(2020) 180.

15 European Commission, JOIN(2020) 8, 19; European Commission, COM(2021) 262, 3 et seq.

16 European Commission, JOIN(2020) 8, 10; the reports are available at https://digital-strategy.ec.europa.eu/en/policies/covid-19-disinformation-monitoring.

17 European Commission, SWD(2020) 180, 18.

18 European Commission, COM(2020) 825.

sign appropriate measures in view of the adoption of the proposed DSA".[19] The "Strengthened Code of Practice on Disinformation 2022" (Disinformation Code 2022) was negotiated in the shadow of the DSA legislation and more recently also of the Ukraine war. It was signed by the major tech companies in June 2022 and explicitly refers to the DSA, which had not yet been enacted at that time.[20] The last building block of the regulation of disinformation in the EU followed on 19 October 2022 with the adoption of the DSA, whose liability rules and due diligence obligations for providers of intermediary services and search engines will enter into force on 17 February 2024.[21] Its recitals use the term "disinformation" no less than 13 times, including in the teleologically central Recital 9, according to which the DSA is to ensure a "safe, predictable and trusted online environment" and to address "the dissemination of illegal content online and the societal risks that the dissemination of disinformation or other content may generate".[22]

The following article provides an overview of the current state of the regulation of disinformation in the EU. It will become apparent that the concept of disinformation (see B), the purpose of anti-disinformation measures (see C) and their content and enforcement (see D) can only be understood if a holistic view is taken of private, hybrid-co-regulatory and public-law norms.[23] The delicate field of disinformation is to a large extent dealt with outside of statutory law. The questions raised thereby are largely unresolved (see E).

B. The Concept of Disinformation

The very definition of "disinformation" is derived from non-state norms. The DSA only defines the term "illegal" content, namely as "any informa-

19 European Commission, COM(2021) 262, 2 et seq. Cf. German Federal Government, Bundestags-Druckssache 20/2308, 5 et seq. ('Moreover, the DSA will raise the previously self-regulatory 'Code of Conduct for Disinformation' to a stronger co-regulatory EU instrument.'); Kuhlmann/Trute, GSZ - Zeitschrift für das Gesamte Sicherheitsrecht, 2022, 115, 119 et seq.

20 Cf. preamble lit. h, i and j as well as Commitment 44 Disinformation Code 2022 (n 2); on this Kuhlmann/Trute, GSZ - Zeitschrift für das Gesamte Sicherheitsrecht, 2022, 115, 122 (cooperative mechanism).

21 Art. 93 DSA.

22 Recitals 2, 9, 69, 83, 84, 88, 95, 104, 106, 108 DSA.

23 Cf. Peukert, Modi der Plattformregulierung, Arbeitspapier des Fachbereichs Rechtswissenschaft der Goethe-Universität Frankfurt am Main 4/2022.

tion that, in itself or in relation to an activity … is not in compliance with Union law or the law of any Member State … irrespective of the precise subject matter or nature of that law".[24] The DSA consistently distinguishes "illegal" from "otherwise harmful" information and activities, which may be incompatible with the terms and conditions of the service providers and therefore may be the subject of content moderation activities.[25] The example most frequently mentioned in the recitals for non-illegal but "otherwise harmful" content is "disinformation".[26] What is meant by this is not precisely defined in the recitals either, but only described by references to incorrect or misleading or deceptive content as well as frequently coordinated manipulations such as the inauthentic use of a service, use of bots or fake accounts.[27]

A fairly precise definition of this term, on the other hand, can be found in the Commission's 2020 Action Plan for Democracy[28] and verbatim in the Disinformation Code 2022. Recital 106 second sentence DSA explicitly refers to these documents and thus incorporates a broad concept of disinformation that encompasses four different phenomena:[29]

- Misinformation is false or misleading content shared without harmful intent though the effects can still be harmful, e.g., when people share false information with friends and family in good faith;
- Disinformation is false or misleading content that is spread with an intention to deceive or secure economic or political gain, and which may cause public harm;
- Information influence operation refers to coordinated efforts by either domestic or foreign actors to influence a target audience using a range of deceptive means, including suppressing independent information sources in combination with disinformation; and
- Foreign interference in the information space, often carried out as part of a broader hybrid operation, can be understood as coercive and deceptive

24 Art. 2 lit. h DSA; on illegal disinformation Kastor/Püschel, Kommunikation und Recht (K&R) 2023, 20, 21 with further references.

25 Cf. art. 2 lit. t and u, art. 34 Abs. 1 sentence 3, recital 5 sentence 2, recital 68 sentence 2, recital 84 in fine, recital 95 sentence 2, recital 104 DSA.

26 Cf. recitals 2 sentence 1, 9 sentence 1, 69 sentence 2, 83 sentence 2, 84, 88 in fine, 95 sentence 2, 104, 108 sentence 2 DSA.

27 Cf. recitals 69 sentence 2, 83 sentence 2, 84, 95 sentence 2, 104 sentence 3 DSA.

28 European Commission, COM(2020) 790.

29 European Commission, COM(2020) 790, 22; preamble lit. a with notes 5-10 Disinformation Code 2022 (n 2).

efforts to disrupt the free formation and expression of individuals' political will by a foreign state actor or its agents.

The extension of the conventional concept of disinformation in the sense of deliberate and malicious deception (alternative 2) to the three other groups of cases is historically related to the COVID-19 pandemic and the Ukraine conflict. In the pandemic, it had become clear that a relevant potential for harm is inherent not only in deliberate disinformation campaigns, but also in false or otherwise misleading information spread in good faith, even if it is only shared among friends or family – such as the advice to treat a COVID infection by drinking bleach.[30] Case groups three and four, on the other hand, come from military intelligence jargon and describe behaviors by a domestic or foreign enemy (adversary) in the context of a hybrid conflict that is also conducted with information.[31] They differ from misinformation and classical disinformation in that they are intended to manipulate the behavior of a target group in a coordinated manner by various means, including by way of disseminating per se true information, e.g., through a coordinated hack-and-leak action.[32]

According to the father of the four-part disinformation concept,[33] strategic communications expert James Pamment, who has, inter alia, worked for the NATO Strategic Communications Centre of Excellence, the case groups are in a graduated, escalating relationship to each other: The most serious form of disinformation in the broad sense is interference from abroad. This can comprise a number of influence operations, which in turn can involve various forms of disinformation in the narrower sense, which then can for their part trigger or be linked to bona fide misinformation.[34] Pamment considers sanctions against disinformation advisable only in the particularly

30 Cf. the definition of misinformation in the documents referenced in note 29 ('e.g. when people share false information with friends and family in good faith'); furthermore European Commission, JOIN(2020) 8, 4; European Commission, COM(2021) 262, 5 et seq.

31 Pamment (n 3), 3 et seq.; recitals 5-10 Regulation (EU) 2022/350 amending Regulation (EU) No. 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine, OJ L 65/1; General Court of the EU, judgment of 27.7.2022 – T 125/22, RT France, ECLI:EU:T:2022:483, paras 52 et seq., 209 et seq.

32 Cf. also art. 34(2) subparagraph 2 DSA as well as Pamment (n 3), 3 et seq.; Pamment (n 11), 16 et seq.

33 Cf. European Commission, COM(2020) 790, 22 with reference to Pamment. On Pamment see also https://www.isk.lu.se/james-pamment.

34 See Pamment (n 11), 16 et seq.

serious cases of coordinated influence operations and interference from abroad.[35] According to Pamment, the four types of disinformation in the broad sense each have different characteristics:[36]

	Misinformation	**Disinformation**	**Influence Operation**	**Foreign Interference**
Actor	Any, less likely a large organization or state actor	Any	Any, but likely a large organization or state actor	State actor and/or its proxies
Behaviour	No evidence of an intent to deceive	Evidence of deliberately deceptive behaviour	Coordination of various techniques aimed at a common goal	Coordination of various techniques aimed at a common goal
Content	Often legitimate expression of an opinion	verifiably deceptive or untrue elements[37]	Any, often multiple types of measures	Any, often multiple types of measures
Degree	Limited evidence of coordination	Any	Scale of the operation indicates coordination	Any
Effect	Any	Any	Any, but should further the objective(s) of the actor	Any, but should further the objective(s) of the actor

According to the Commission and the signatories of the Disinformation Code 2022, the term "disinformation" does not include "misleading advertising, reporting errors, satire and parody, or clearly identified partisan news and commentary".[38] This very list reveals the difficulty of distinguishing harmful disinformation from legitimate expressions of opinion. How many errors does a journalistic medium have to commit before it degenerates into an unreliable source of repeated disinformation? How are "fake parody accounts" to be distinguished from "real", legitimate parodies?[39] Does a single Twitter user suggesting a #hashtag launch a coordinated influence operation? What generally is to be understood under an influence

35 Pamment (n 3), 2-5.
36 Pamment (n 3), 11.
37 The Commission and the Disinformation Code 2022, in contrast, do include false (true) but otherwise misleading content under the concept of misinformation and disinformation; see supra n 29. Likewise the concept of 'misleading' in unfair competition law pursuant to art. 5(2) German Unfair Competition Act ('false statements or other information suited to deception').
38 European Commission, COM(2018) 236, 2; preamble lit. a Disinformation Code 2022 (n 2).
39 European Commission, SWD(2020) 180, 14.

operation if the actor in question is based in the Union and not controlled by a third country?

C. The Purpose of Anti-disinformation Measures

The clarification of these delicate issues is complicated by the fact that the four-element concept of disinformation differentiates between different actors and behaviors but does not explain what is meant by a relevant "harm". The Disinformation Code 2022 only states that the signatories agree with the Commission that disinformation is a major challenge for Europe.[40] What exactly this challenge is and what interests are to be protected from disinformation remains open.

However, the DSA provides information about these purposes, thus reversing the interplay between the Code of Conduct and statutory law. While the Disinformation Code 2022 defines the subject matter of regulation, the DSA specifies the interests protected by the relevant measures.

Informative for this teleology are the terms "systemic risk" (Art. 34(1) DSA) and "crisis" (Art. 36(2) DSA). These terms constitute substantive requirements for special due diligence obligations with regard to illegal and otherwise harmful content, including disinformation, of very large online platforms (hereinafter VLOPs) and very large online search engines (hereinafter VLOSEs) with an average monthly number of at least 45 million active users in the Union.[41] The references to "systemic" risks and "public" security and health in Art. 36(2) of the DSA make it clear that the disinformation regime does not serve to protect the individual legal interests of specific individuals, but rather, on a more abstract level, to protect public goods/interests. The risk management and crisis response measures laid down in the DSA address "societal concerns" with regard to very widespread online services and their effects on the formation of public opinion.[42] The classic, narrow concept of disinformation (now case group 2 of the broad concept of disinformation) already aimed at preventing such

40 Preamble lit. b Disinformation Code 2022 (n 2).

41 Cf. recitals 83 sentence 2, 84, 88 in fine, 95 sentence 2, 104, 108 sentence 2 DSA and infra IV 2 c.

42 Cf. recital 79 DSA; definition of disinformation in the narrow sense, supra n 29.

"public" damage.[43] This general purpose was not affected by the extension to bona fide misinformation.[44]

More details on the protective purposes of disinformation regulation are provided by the enumeration of the systemic risks in Art. 34(1) third sentence DSA that VLOPs and VLOSEs must constantly assess and, if necessary, mitigate. According to this provision, VLOPs and VLOSEs must not only contain the dissemination of illegal content (lit. a), but also any actual or foreseeable negative effects on

- "the exercise of fundamental rights" (lit. b),
- "on civic discourse and electoral processes, and public security" (lit. c) and
- "in relation to gender-based violence, the protection of public health and minors and serious negative consequences to the person's physical and mental well-being" (lit. d).

Three protected interests can be derived from this list. Firstly, risk management is intended to protect the democratic opinion- and consensus-forming processes (elections). This protected interest is considered from two perspectives in Art. 34(1) third sentence lit. b and c DSA. On the one hand, in the view of the Commission and probably also of the Union legislator, disinformation represents a systemic risk to individual freedom of expression.[45] Behind this view, which is by no means self-evident, is the idea that non-governmental disinformation can also go so viral or be artificially amplified that correct statements are pushed to the margins of the debate or are no longer voiced at all because they appear to the individual to be deviant. Secondly, item (c) protects the collective processes of deliberative democracy, namely electoral processes. This regulatory purpose is based on the assumption that disinformation often pushes radical or extremist views, undermines citizens' trust in democratic institutions and contributes to the polarization of debate.[46] This risk profile can be found not only in

43 European Commission, COM(2018) 236, 2; preamble Disinformation Code 2018 (n 14).

44 Cf. European Commission, COM(2021) 262, 5 et seq.

45 European Commission, COM(2018) 236, 1; art. 34(1) sentence 3 lit. a in connection with recital 81 sentence 2 DSA ('submission of abusive notices or other methods for silencing speech'); Pamment (n 11), 6.

46 European Commission, JOIN(2018) 36, 13 et seq.; European Commission, COM(2018) 236, 1 et seq.

coordinated disinformation campaigns but also in misinformation that is shared en masse.

The second protected interest, "public security", is present both in Art. 34(1) third sentence lit. c DSA and in the legal definition of a "crisis" according to Art. 36(2) DSA. While "actual or foreseeable negative effects" on public security are sufficient for a systemic risk, a crisis requires exceptional circumstances that lead to a serious threat to security. The security risks or crises can concern both the internal security of Union citizens (Art. 3(2) TEU) and the security of the Union as such and of its citizens in their relations with the wider world (Art. 3(5) TEU).[47] The focus of the relevant Union measures has for some time been on the second-mentioned public security of the Union in relation to the Russian Federation.[48] After initially strengthening the Union's strategic communication in this regard,[49] in response to the Russian invasion of Ukraine in February 2022, the Council suspended the broadcasting licenses of several Russian television channels and prohibited the transmission or distribution of these programs by any means, and the placing of advertising on them.[50] The immediate aim of these measures is to counter disinformation attributed to the Russian Federation, which is described as part of a comprehensive hybrid threat in the form of systematic war propaganda.[51] According to the four-part concept of disinformation in the broad sense, this is therefore to be qualified as interference from abroad, which, according to Pamment, indeed justifies the most far-reaching countermeasures.[52] The General Court of the

47 On the term 'security' cf. nos. 9 et seq. Action Plan of the Council and the Commission on how best to implement the provisions of the Treaty of Amsterdam on an area of freedom, security and justice, 3.12.1998, OJ C 19 of 23.1.1999, 1.

48 Cf. General Court of the EU, judgment of 27.7.2022 – T 125/22, RT France, ECLI:EU:T:2022:483, paras 52-55; European Commission, JOIN(2018) 36, 2-4; European Commission, JOIN(2018) 16, 4.

49 Supra I with n 12.

50 Art. 2 lit. f Regulation (EU) No. 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine, as amended by Regulation (EU) 2023/250, OJ L 32I/1; Keber, Computer und Recht 2022, 660, 662.

51 Recitals 5-10 Regulation 2022/350 (n 31); General Court of the EU, judgment of 27.7.2022 – T 125/22, RT France, ECLI:EU:T:2022:483, paras 56 et seq., 88, 162, 209 et seq. (war propaganda). On the concept of propaganda, see Joint Declaration (n 13), no. 2 lit. c (state statements which demonstrate a reckless disregard for verifiable information); Baade, Europarecht 2020, 653; Schünemann, in: Dunn Cavelty/Wenger (n 6), 32, 34; Bauer/Nadler, Harvard Kennedy School (HKS) Misinformation Review 2021, https://doi.org/10.37016/mr-2020-64.

52 Cf. Pamment (n 3).

EU sees these measures as pursuing two objectives that are in conformity with primary and fundamental rights, namely the protection of the public security of the Union itself and the protection of peace in Ukraine and thus of international security.[53]

The third protected interest of the anti-disinformation rules is, according to Art. 34(1) third sentence lit. d, Art. 36(2) second alternative DSA, public health, including the well-being of particularly vulnerable sections of the population, such as minors. The separate mention of public health can be attributed to the experience with the COVID-19 pandemic, which showed that, in addition to coordinated disinformation campaigns, other manipulations (= misinformation), possibly spread in good faith, may also harbor health risks.[54]

It is questionable whether measures against disinformation can also be justified with a view to other public goods such as the environment or international peace outside the Union. In my view, the DSA and the Disinformation Code 2022 cannot be used as a basis for such interferences with communicative freedoms. According to the wording of Art. 34(1) third sentence and recital 80 DSA, VLOPs and VLOSEs are only obliged to assess and, if necessary, reduce the four risks expressly listed.[55] From a teleological point of view, the DSA thus leads to a specification of the disinformation regime, which according to the earlier concept was supposed to protect "public goods" of any kind from harm.[56] From the perspective of the rule of law, this clarification appears indispensable, because an obligation backed up by state penalties to deal with unspecific communication risks for all legal goods listed in Art. 3 TEU and referred to in the Charter of Fundamental Rights would be practically impossible for VLOP and VLOSE providers to honor and would thus be disproportionate. The concept of a "crisis" according to Art. 36 and Art. 48 DSA, which requires a serious threat to public security or public health in the Union or in significant parts of it, is even more limited. Only such extraordinary circumstances justify

53 General Court of the EU, judgment of 27.7.2022 – T 125/22, RT France, ECLI:EU:T:2022:483, para 202. The idea to protect international peace goes beyond the concept of the (information) crisis pursuant to art. 36(2) DSA, which requires a serious threat to public security 'in the Union or in significant parts of it'.

54 Cf. recital 83 DSA.

55 Cf. also recital 80 sentence 1 DSA.

56 European Commission, COM(2018) 236, 2 and Preamble Disinformation Code 2018 (n 14) ('Public harm comprises threats to democratic political and policy-making processes as well as public goods such as the protection of EU citizens' health, the environment or security.').

the far-reaching powers of the Commission in a "crisis". Communicative threats to democracy or the environment are not sufficient.

The limited protective purpose of the DSA does not preclude anti-disinformation measures from being founded on other legal bases though, namely the law on common foreign and security policy.[57] Disinformation about the dangers of climate change could furthermore be qualified as a security risk and thus indirectly become subject to DSA and Disinformation Code obligations. However, such broad interpretations run the risk of undermining the horizontally comprehensive and at the same time teleologically limited approach of the DSA. Disinformation regulation is generally delicate. Extending it beyond the already far-reaching wording of the DSA is therefore, in the event of doubt, neither necessary nor justified.

D. Content and Enforcement of Measures Against Disinformation

The previous two sections have shown that the current regulation of disinformation in the EU results from an interplay between private self-regulation and formal statutory law. The Disinformation Code 2022 provides the definition of the subject matter of regulation, while the DSA states the regulatory objectives. Private norms and statutory due diligence obligations also intertwine with regard to the content and enforcement of anti-disinformation measures.

I. Risk-based Approach, Proportionality and Precautionary Principle

The hybrid disinformation regime follows a risk-based approach committed to the principle of proportionality. Accordingly, duties to reduce disinformation must be appropriate, necessary and not unduly burdensome in order to effectively reduce the potential harm of a statement or campaign in view of the severity of the potential impact and the probability of its occurrence.[58] Risk assessment and mitigation duties must, in other words,

57 General Court of the EU, judgment of 27.7.2022 – T 125/22, RT France, ECLI:EU:T:2022:483, paras 52 et seq.

58 Cf. art. 5(4) TEU in connection with art. 34(1) sentence 3 and recital 79 sentence 5 DSA; on the risk-based approach cf. eg Art. 3 no. 18 Regulation (EU) 2019/1020 on market surveillance and compliance of products, OJ L 169/1; art. 2 no. 6 Directive

be proportionate in view of the nature of the danger and the probability of its realization.[59] On the one hand, online services are not required to reduce the risk of disinformation to zero.[60] On the other hand, the (self-)obligations to take measures against disinformation take effect at a very early stage in order to prevent public harm from the outset:

The preventive nature of disinformation regulation already follows from the concept of disinformation, which extends to all content that *can* be harmful.[61] Thus, it is generally sufficient that there is an informational potential for harm, the realization of which does not have to be demonstrated and proven. A systemic risk for a relevant public good pursuant to Art. 34(1) DSA is accordingly present if certain content is likely or "foreseeable" to have adverse effects. Moreover, according to the fiction of Art. 36(2) DSA, an informational "crisis" is already considered to have arisen when extraordinary circumstances such as "armed conflicts or acts of terrorism, including emerging conflicts or acts of terrorism, natural disasters such as earthquakes and hurricanes, as well as from pandemics and other serious cross-border threats to public health" occur.[62] In contrast to the concept of risk, the concept of crisis is therefore not linked to the dissemination of disinformation, which has the potential to cause harm (disinformation → harm), but even earlier to events that are so exceptional that they trigger a public debate in which disinformation can occur, which in turn threatens public safety or health (circumstance → disinformation → harm). Art. 36(2) DSA logically does not presuppose a threat to public security or health, but a situation (= extraordinary circumstances) that can lead to a serious threat.[63] If the concept of crisis is interpreted broadly, the Commission could make use of its powers under Art. 36 even if it cannot be determined with certainty whether there is a disinformation risk at all and

(EU) 2022/2557 on the resilience of critical entities, OJ L 333/164; European Commission, COM(2021) 206, 3 et seq.

59 Cf. also Pamment (n 3), 5 et seq. (ABCDE framework covering disinformation actors, their behaviour, the content of the information, the degree of harm and the effects of disinformation).

60 Cf. art. 19(2) Regulation (EU) 2019/1020 (n 58); on over-blocking through filter systems in copyright law see the opinion of AG Saugmandsgaard Øe of 15.7.2021 – C 401/19, Poland / Parliament and Council, ECLI:EU:C:2021:613, para 184.

61 Supra II.

62 Cf. recital 91 sentence 3 DSA, see also Art. 48(1) sentence 2 DSA.

63 Although 'can' is missing in the English and French versions of art. 36(2) DSA, it is found in all the language versions of the explanatory recital 91 sentence 2 ('can lead to a serious threat', 'peuvent entraîner une menace grave').

how serious it is.[64] According to this interpretation, the DSA would extend the precautionary principle known from environmental and health law to the regulation of the public debate.

This is achieved, as already mentioned, through the new substantive legal terms of "disinformation", "systemic risk" and "crisis", which trigger special duties of care on the part of VLOPs and VLOSEs as well as powers of intervention on the part of the Commission. The DSA thus by no means establishes a purely procedural compliance regime that merely serves to effectively combat content that has otherwise been declared illegal. On the contrary, the DSA establishes new substantive requirements and sanctions precisely in the particularly sensitive area of non-illegal but otherwise harmful content. These measures are only limited to the extent that they are not directly aimed at the individual speaker, but rather at Big Tech companies, which have to incorporate the prohibitions of disinformation into their private regulations and enforce them against their users.

II. The Three Levels of Disinformation Regulation

In line with this approach, the regulation of disinformation is always based on private norms, namely the platform terms and conditions and other internal service rules, such as the rules governing the ranking of search results. This micro level of regulation is subject to collective self-commitments (meso level) for signatories of the Disinformation Code, and to the legal due diligence obligations of the DSA on a societal macro level for VLOPs and VLOSEs.

1. Micro Level: Private Rules of Online Services

Information society services are in principle free to prohibit all forms of disinformation in their terms and conditions and to enforce this contractual prohibition through automated content moderation measures, if neces-

64 Cf. on the precautionary principle see CJEU, judgment of 5 May 1998 – C-157/96, The Queen / Ministry of Agriculture, Fisheries and Food and Commissioners of Customs & Excise, ex parte National Farmers' Union and others, ECLI:EU:C:1998:191, para 63; CJEU, judgment of 1 October 2019 – C-616/17, Blaise and others, ECLI:EU:C:2019:800, para 43.

sary.[65] The large US Big Tech companies have been doing this for years, sometimes at short notice under informal pressure from politicians and the public, but especially in the COVID-19 pandemic even acting before the event.[66] As correctly observed by the German Federal Court of Justice, the willingness to fight all kinds of "harmful" expression follows from the fact that Facebook and the like have a vital business interest in "creating an attractive communication and advertising environment for both their users and their advertisers".[67] This interest is incompatible not only with hate speech, but also with false or otherwise misleading information that undermines users' trust in the reliability and security of the content provided via the service and thus ultimately trust in the service as such.[68]

However, the freedom of online services to establish and enforce contractual prohibitions on disinformation is not unlimited. According to the German Federal Constitutional Court and the Federal Court of Justice, very large services such as Facebook are under the spell of an indirect third-party effect of both the fundamental rights of freedom and the principle of equality.[69] They may therefore not arbitrarily delete or otherwise downgrade content without an objective, comprehensible reason, for example to suppress a particular political opinion.[70] Art. 14(4) DSA further obliges all providers of intermediary services, regardless of their size, to proceed "in a diligent, objective and proportionate manner" when applying and

65 Cf. the definitions in Art. 2 lit. a, t and u DSA and German Federal Constitutional Court, order of 11 April 2018 – 1 BvR 3080/09, Stadionverbot, ECLI:DE:BVerfG:2018:rs20180411.1bvr308009, para 40 (English translation available at http://www.bverfg.de/e/rs20180411_1bvr308009en.html); German Federal Court of Justice, judgment of 29 July 2021 – III ZR 179/20, Hassrede-AGB, ECLI:DE:BGH:2021:290721UIIIZR179.20.0, para 78; Pamment, The EU's Role in Fighting Disinformation: Developing Policy Interventions for the 2020s, 9 et seq.

66 Cf. Peukert, in: Spiecker gen. Döhmann/Westland/Campos (n 13), 229, 240 et seq. with further references; High level group (n 2), 15 et seq.; European Commission, JOIN(2020) 8, 9.

67 On the regulation of private hate speech see German Federal Court of Justice, judgment of 29 July 2021 – III ZR 179/20, Hassrede-AGB, ECLI:DE:BGH:2021:290721UIIIZR179.20.0, para 92.

68 Schmid/Braam/Mischke, MultiMedia und Recht 2020, 19, 23 with further references.

69 German Federal Constitutional Court, order of 20.9.2021 – 1 BvQ 100/21, Der III. Weg, ECLI:DE:BVerfG:2021:qk20210920.1bvq010021, para 15; German Federal Court of Justice, judgment of 29 July 2021 – III ZR 179/20, Hassrede-AGB, ECLI:DE:BGH:2021:290721UIIIZR179.20.0, para 64.

70 German Federal Court of Justice, judgment of 29 July 2021 – III ZR 179/20, Hassrede-AGB, ECLI:DE:BGH:2021:290721UIIIZR179.20.0, paras 80-82.

enforcing contractual moderation rules, and to take into account "the rights and legitimate interests of all parties involved, including the fundamental rights of the recipients of the service", including freedom of expression. Consequently, they too must not moderate user content arbitrarily or on the basis of purely hypothetical assumptions about the potential for harm.[71] Online platforms must even reverse unfounded measures according to Art. 20(4) DSA without undue delay.

2. Meso Level: Self-commitments per Disinformation Code

The micro level of the fight against disinformation is thus characterized by private autonomous decisions of the service providers. Those who have not been designated by the European Commission as a VLOP or VLOSE can but are not obliged to take action against disinformation.[72]

The meso level of disinformation regulation in the EU is the Disinformation Code 2022. Although the Code is aimed at VLOPs and VLOSEs through its link to Art. 34 et seq. DSA, smaller service providers are free to submit to the Code's voluntary obligations, and some indeed do.[73] On 40 tightly printed pages, the Code sets out no less than 44 commitments to 128 concrete measures, the structure, and objectives of which can only be outlined in this article.

A crucial aspect for understanding the functioning of the Code is the insight that it is by no means only directed at online platforms and search engines, but at all "relevant" actors who can influence the dissemination of disinformation.[74] These include, firstly, organizations that assess whether content qualifies as disinformation and whether websites repeatedly make disinformation accessible. This category comprises fact checkers, actors who assess the trustworthiness of news sites (e.g., the US company "NewsGuard" and the British "Global Disinformation Index") as well as

71 Fundamental rights thereby require a showing of causality between disinformation and public harm based on objective facts; cf. German Federal Court of Justice, judgment of 29 July 2021 – III ZR 179/20, Hassrede-AGB, ECLI:DE:BGH:2021:290721UIIIZR179.20.0, para 82.

72 Cf. art. 16, 19 DSA.

73 Cf. preamble lit. a, k and l Disinformation Code 2022 (n 2) and e.g. https://disinfocode.eu/signatory-report/vimeo-inc/?chapter=integrity.

74 Cf. commitment 41 Disinformation Code 2022 (n 2) and European Commission, COM(2021) 262, 7 et seq.; art. 45(2) DSA ('civil society organisations and other relevant stakeholders').

academics. The Code obliges the platforms and search engines to cooperate with this diverse disinformation monitoring community, to fund the corresponding services or research activities and to integrate their findings into their own services.[75]

Secondly, the Code has been signed by organizations that can be classified as belonging to the military-intelligence cybersecurity sector and have expertise in countering coordinated disinformation campaigns from within and outside a country.[76] The online platforms and search engines bound by the Code have undertaken to design their services in cooperation with these intelligence actors in such a way that as far as possible all forms of disinformation in the broad sense are not disseminated and in any event are not recommended or otherwise amplified.[77]

Thirdly, numerous advertising companies and advertising industry associations have joined the Code. Their participation aims to reduce the financial incentives for the dissemination of often scandalous disinformation that promises high engagement.[78] For this purpose, the automated online advertising systems are fed with the ratings of fact checkers and other content monitoring actors. Sources flagged as distributing disinformation are to be cut off from the advertising market.

The ongoing cooperation and decision-making in this disparate, not a-priori limited circle of "relevant actors" is institutionalized in a permanent task force. This task force is chaired by the European Commission, although it is not formally involved in the Code.[79]

3. Macro level: DSA Obligations for VLOPs and VLOSEs

However far-reaching and sophisticated the voluntary obligations of the Disinformation Code may be, its weak point is and remains the enforcement of its measures. Failure to participate in the Code, failure to comply with voluntary commitments and withdrawal from the Code without giv-

75 Commitments 26-33 Disinformation Code 2022 (n 2).
76 E.g. https://www.crispthinking.com/, https://www.globsec.org/.
77 Commitments 14-16 ('integrity of services') and 17-25 ('empowering users') Disinformation Code 2022 (n 2).
78 Commitments 1-3 Disinformation Code 2022 (n 2); European Commission, COM(2021)262, 9.
79 Commitment 37 Disinformation Code 2022 (n 2) (decisions are reached by consensus).

ing reasons does not trigger any legal consequences.[80] This enforcement deficit is remedied at the societal macro-level by the DSA.

First, the DSA establishes a legal framework for the elaboration and further development of codes of conduct. According to Art. 45(1) of the DSA, the Commission and the European Board for Digital Services, which comprises the Member State Digital Services Coordinators, shall encourage and facilitate the drawing up of voluntary codes of conduct at Union level to contribute to the proper application of the DSA, taking into account in particular the specific challenges of tackling different types of illegal content and systemic risks. According to paragraph 4 of this Article, "the Commission and the Board shall assess whether the codes of conduct meet the aims ... and shall regularly monitor and evaluate the achievement of their objectives ... In the case of systematic failure to comply with the codes of conduct, the Commission and the Board may invite the signatories to the codes of conduct to take the necessary action". According to its wording and its position in the section on "Other provisions concerning due diligence obligations", this power also applies to small and medium-sized intermediary services. However, it only empowers the Commission and the Board to "invite" the Code signatories to comply with their voluntary commitments, and the provision does not stipulate a mandatory obligation to comply with the Disinformation Code. Accordingly, the recitals state that the provisions on the conclusion of codes of conduct should not impair "the voluntary nature of such codes and the freedom of interested parties to decide whether to participate".[81] Finally, this restrictive interpretation is supported by the fact that a more far-reaching proposal of the European Parliament to empower the Commission and the Board, "in case of systematic failure to comply with the codes of conduct", to "decide as a last resort to temporarily suspend or definitively exclude platforms that do not meet their commitments as signatories to the codes of conduct", has not become law.[82]

The legal situation is different for VLOPs and VLOSEs. Due to their size and social importance – one could also speak of systemic relevance – they are generally subject to the most intensive due diligence obligations under the graduated system of the DSA. This also includes the obligation to

80 Regarding the Disinformation Code 2018 see European Commission, SWD(2020) 180, 18; preamble lit. u and v Disinformation Code 2022 (n 2).

81 Recital 103 sentence 4 DSA.

82 See European Parliament, 9_TA(2022)0014, amendment no. 371 to art. 35(5).

"put in place reasonable, proportionate and effective mitigation measures" against systemic risks, including disinformation, as stipulated in Art. 35(1) sentence 1 DSA. Compliance with this due diligence obligation can be enforced in two ways.

On the one hand, the Commission can oblige VLOP or VLOSE providers to initiate or adjust cooperation with other providers through codes of conduct or "voluntary" crisis protocols (Art. 48 DSA). If a service provider refuses to enter into this commitment "without proper explanations", this can, according to the recitals, be taken into account when determining whether such a recalcitrant provider violates its DSA obligations.[83] On the other hand, the Commission can directly order a VLOP or VLOSE provider to adopt the risk mitigation measures listed in Art. 35(1) second sentence DSA. This could include an order to cooperate with trusted flaggers and/or to adapt the terms and conditions, content moderation processes, advertising systems and features or functioning of their services.[84] As a result, the DSA empowers the Commission to force uncooperative VLOPs and VLOSEs to take measures that the signatories of the Disinformation Code take voluntarily.

The same is true in a "crisis", which, as explained, is even further upstream. Art. 36(1) and (7) DSA grant the Commission, upon recommendation of the Board, the power to "require" VLOP and VLOSE providers to take temporary special measures, including highlighting reliable information. The Board may also recommend that the Commission initiate the drawing up of voluntary crisis protocols for addressing crisis situations. Moreover, as soon as an "exceptional circumstance" in the sense of Art. 36(2) DSA has occurred, systemic disinformation risks can usually be identified, the management of which can be enforced via Art. 34 et seq. DSA. Finally, experience teaches that Big Tech will not refuse to follow certain communication protocols in future crisis situations.[85]

---

83 Cf. recital 104 sentence 6 and arts. 66(1), 73(1) lit. a, 74(1) lit. a, 75(2) sentence 3 and (3) sentence 3 DSA (commitment to adhere to relevant codes of conduct).

84 The powers of the exclusively competent (cf. art. 56(2) DSA) commission result from arts. 70(1) (interim measures 'where there is an urgency due to the risk of serious damage for the recipients of the service … on the basis of a prima facie finding of an infringement'), 73(3) (non-compliance decision), 75(4) in connection with 76(1) lit. e (penalty payments) and 82(1), 51(3) sentence 1 lit. b (temporary restriction of access of recipients to the service).

85 Pamment (n 65), 13 ('This collaboration already exists to a certain degree but could be developed particularly for crises like the coronavirus pandemic.').

E. Unresolved Issues

In the light of all the above, disinformation regulation in the EU is based on a complex web of private and public communication norms involving numerous actors. The subject matter of regulation – "disinformation" – is defined by the Disinformation Code 2022, the regulatory purposes are specified by the DSA, and the concrete measures against disinformation are to be found in the private platform rules (micro-level), the voluntary commitments of the Disinformation Code (meso-level) and, for the societal macro-level of VLOPs and VLOSEs, in the risk management rules of the DSA, which at the same time links all three regulatory levels together. The practical implementation and further development of the Code and DSA requirements also take place in a coordinated-cooperative manner, namely on the private side in the permanent working group of the signatories of the Disinformation Code (see above) and on the state side in the "European Board for Digital Services" (Arts. 61-63 DSA). The connection between these two central institutions of the fight against disinformation is established via the Commission, which chairs all the meetings.[86]

The reason for this complex structure is the fact that a conventional state order to suppress content that is "harmful", yet covered by freedom of expression and also otherwise legal, has so far been correctly considered unconstitutional for lack of a legal basis.[87] Whether the EU legislature has succeeded in finding a sustainable solution in terms of the rule of law appears extremely doubtful and requires detailed analysis. Questions in need of clarification include:

(1) What is the factual significance and effect of objectively false (untrue) and otherwise misleading content at the societal level? In this respect, the state of empirical research is much less clear-cut than the constantly repeated, consistently anecdotal references to "Trump", the "Infodemic" or "Russia" would have one believe.[88] On several occasions, subsequent investigations could not confirm suspected disinformation

86 Commitment 37 Disinformation Code 2022 (n 2); art. 62(2) DSA.

87 Cornils, Designing platform governance, 2020, 32; Ferreau, Archiv für Presserecht 2021, 204, 209. For a critical view of the crisis protocols see German Bundesrat, Bundesrats-Drucksache 96/21, 21.

88 Pamment (n 11), 3 ('evidence of harm caused by disinformation and influence operations is patchy'); Schünemann, in: Cavelty/Wenger (n 6), 32, 40 et seq. with further references.

campaigns.[89] Against this backdrop, there are increasing voices in communication studies research that see an empirically unsubstantiated alarmism at work in the fight against disinformation.[90]

(2) Does the TFEU, and in particular the internal market competence referenced in Art. 1(1) DSA, authorize the EU to regulate legal but otherwise harmful speech of a non-specific nature in the interests of democracy, public safety and health?[91]

(3) Are platform-based measures against disinformation attributable to the EU if the service providers thereby wish to comply with their DSA obligations?[92]

(4) Is the protection of "civic discourse" in a deliberative democracy a constitutionally permissible goal of repressive measures against per se legal expression?[93] Does freedom of expression imply a state duty to

89 European Commission, COM(2020) 790, 4 with n 8 ('isolated cyberattacks, data protection and other elections-related complaints had been received, but that a covert, coordinated large-scale effort to interfere in the elections had not been identified'); https://digital-strategy.ec.europa.eu/en/policies/covid-19-disinformation-monitoring (no coordinated disinformation campaigns related to Covid-19); Beyer/Almeida Saab, Verfassungsblog, DOI: 10.17176/20221223-121639-0 (no decisive influence of Russian disinformation campaigns on the elections in Italy); Benkler/Faris/Roberts, Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics, 2018, 235 et seq. (no decisive Russian influence on Trump's election); without examples Kommunikationsbericht der Bundesregierung 2021, Bundestags-Drucksache 19/31165, 2 et seq.; critically also Baade, Europarecht – EuR 2020, 653, 683.

90 See Schünemann, in: Cavelty/Wenger (n 6), 32, 43; Anderson, Communication Theory 31(1) (2021), 42 et seq.; Jungherr/Schroeder, Social Media and Society 7(1) (2021), https://doi.org/10.1177/2056305121988928 (Disinformation not a driver of social or political divisions); Altay/Berriche/Acerbi, Social Media and Society 9(1) (2023), https://doi.org/10.1177/20563051221150412 ('misinformation on misinformation'). Critically on the conceptual and theoretical vagueness of the sociological fake news literature e.g. Tandoc/Lim/Ling, Digital Journalism 6(2) (2018), 137 et seq.; Zimmermann/Kohring, M&K Medien & Kommunikationswissenschaft 66 (2018), 526 et seq.; Camargo/Simon, Harvard Kennedy School (HKS) Misinformation Review 2022, https://doi.org/10.37016/mr-2020-106.

91 Upheld for anti-war propaganda by the General Court of the EU, judgment of 27.7.2022 – T 125/22, RT France, ECLI:EU:T:2022:483, paras 52 et seq.

92 Upheld for the copyright liability of platforms by the CJEU, Judgment of 26 April 2022 – C-401/19, Poland / Parliament and Council, ECLI:EU:C:2022:297, para 56 (overblocking is the 'direct' consequence of a copyright liability norm); generally Eifert, in: Voßkuhle/Eifert/Möllers (eds.), Grundlagen des Verwaltungsrechts, vol. 1, 3rd ed. 2022, § 19 para 163 (question of attributability with complex control mechanisms is highly disputed).

93 German Bundesrat, Bundesrats-Drucksache 96/21, 3.

protect citizens from disinformation?[94] What image of man is this assumption based on?[95] Do statements that are spread in good faith and are true per se, which, as explained, may well fall under the concept of disinformation in the broad sense, also trigger a corresponding duty to protect?

(5) Is it proportionate to preventively suppress legal but otherwise potentially harmful content using a risk-based approach or should the self-regulatory forces of open debate be trusted, especially in unclear crisis situations?[96] How much communicative deviance does the current disinformation regime still allow?[97]

(6) Does the repeatedly mediated disinformation regulation, with its coercive instruments directly aimed only at a small number of VLOPs and VLOSEs, undermine legal recourse of the alleged disseminators of disinformation, including possibly professional journalists and entire media companies, in a way that is inadmissible under the rule of law? Against this background, can it be assumed that Art. 20(4) second sentence DSA establishes a subjective right to the restoration of content that is neither illegal nor in breach of contract, which can be enforced before the civil courts of the Member States?

94 Cf. also General Court of the EU, judgment of 27.7.2022 – T 125/22, RT France, ECLI:EU:T:2022:483, para 197 (obligation to display a banner or a warning insufficient).

95 On the concept of the 'informational citizen' Anderson, Harvard Kennedy School (HKS) Misinformation Review 2021, https://doi.org/10.37016/mr-2020-64.

96 Generally Grimm, Die Zukunft der Verfassung, 1991, 216 (preventive measures require sufficient suspicion of serious threats to a high-ranking legal interest); critically Cornils, Zeitschrift für Urheber- und Medienrecht 2019, 89, 103; Ingold, MultiMedia und Recht 2020, 82, 85; Joint Declaration (n 13), no. 3 lit. a; undecided Holznagel, Computer und Recht 2021, 733 para. 19 (weakness or strength). See also CJEU, judgment of 10 June 2021 – C-65/20, KRONE – Verlag, ECLI:EU:C:2021:471, para 40 (strict liability for inaccurate health advice 'would be detrimental to the objective of ensuring that risk is fairly apportioned between the injured person and the producer'). There is, as a matter of principle, contrary to the Commission (JOIN(2018) 36, 9), no 'manipulation-free' discourse, not even, and particularly not, if disinformation is regulated.

97 Regarding the broadcasting and distribution ban on Russian TV channels cf. General Court of the EU, judgment of 27.7.2022 – T 125/22, RT France, ECLI:EU:T:2022:483, paras 97, 187 (the applicant's media coverage of the aggression did not maintain 'a balance in so far as concerns the choice of participants, content, images and views communicated in those sequences').

(7) Should the sensitive area of legal but otherwise harmful content not be regulated at a greater distance from the state or with greater involvement of the European Parliament?[98]

Given the shaky empirical and normative foundation of the regulation of disinformation at EU level, it is irritating that in its relevant papers the Commission itself reports violations of media freedom under the pretext of combating disinformation, even in Member States.[99] With all the trust that the Commission can claim for itself, it seems downright naïve to consider such abuse at EU level impossible in principle, especially since the daily fight against disinformation is controlled and executed by private organizations, often not based in the EU.[100] Accordingly, the open-ended scholarly accompaniment of the further development of the EU disinformation regulation is all the more important. The observers of the social debate need critical observation.

98 On the creation of so-called platform boards cf. Koalitionsvertrag zwischen SPD, Bündnis 90/Die Grünen und FDP 2021, 17.

99 European Commission, JOIN(2020) 8, 12 et seq.; European Commission, COM(2020) 790, 14; Pamment (n 11), 4 ('Experts also express increasing concerns that EU member states themselves are becoming a source of misinformation and disinformation.').

100 In addition to the US and Chinese Big Tech companies, this also includes evaluation and rating organizations based in the USA (e.g. https://www.newsguardtech.com) or the United Kingdom (e.g. https://www.disinformationindex.org). Both of these organizations have received payments from the US federal government budget, NewsGuard even directly from the US Department of Defense; cf. Shellenberger, The Censorship-Industrial Complex, 2023, 51 et seq.