

Protecting Democratic Elections Against Online Influence via “Fake News” and Hate Speech – The French Loi Avia and Loi No. 2018–1202, the German Network Enforcement Act and the EU’s Digital Services Act in Light of the Right to Freedom of Expression

*Dominik Steiger*¹

This book chapter will focus on different legislatures’ efforts to protect the integrity of their elections against ‘fake news’ and hate speech. These efforts are a reaction to an unprecedented rise of private dissemination of ‘fake news’ and hate speech in general and Russian undertakings to undermine the legitimacy of elections worldwide in particular. Elections must be protected as they are ‘a characteristic principle of democracy’² and consequently ‘of prime importance in the Convention system.’³ Equally of prime importance for democracy is ‘freedom of expression [which] constitutes one of the essential foundations of a democratic society and one of the basic conditions for its progress and for each individual’s self-fulfilment.’⁴ While ‘[f]ree elections and freedom of expression, particularly freedom of political debate, together form the bedrock of any democratic system [and] are inter-related and operate to reinforce each other’,⁵ tensions also exist between them that need to be resolved. After having introduced the facts that are foundational for these tensions (A.), this chapter will resolve them by turning to the law (B.). The focus will be on Article 10 of the European Convention of Human Rights (‘ECHR’) and the European Court of Human Rights’ (‘ECtHR’) pertinent case law.

1 The author thanks Laura Lepsy for her valuable help.

2 ECtHR, Judgement, 2 March 1987, *Mathieu-Mohin and Clerfayt v Belgium*, Application No. 9267/81, para. 47.

3 *Ibid.*

4 ECtHR, Judgment, 8 July 1986, *Lingens v Austria*, Application No. 9815/82, para. 41.

5 ECtHR, Judgment, 21 February 2017, *Orlovskaya Iskra v Russia*, Application No. 42911/08, para. 110.

A. *The Facts: Old Habits of Influencing Elections Die Hard – And How Legislatures Deal With It*

Elections are supposed to be secret, free, and fair.⁶ As the cornerstone of every democratic society, even authoritarian states that want to keep a democratic appearance invest much energy and money in holding elections and upholding the impression that these elections are secret, free, and fair. Since elections decide who will be in power for the years to come, much is at stake, and, thus, the temptation to influence the outcome of elections is high.

I. *A Very Short History of Influencing Elections*

It comes as no surprise that influencing elections is not a new phenomenon and has been undertaken by all kinds of states and in all kinds of times. For example, in the early 18th century, Russia and other major powers regularly influenced the elections of the King of Poland.⁷ In the 1796 US presidential campaign, France tried to intimidate voters by publishing official notes addressed to the US Secretary of State in a newspaper that barely concealed that France was threatening the use of force against the US, if Thomas Jefferson was not elected US President.⁸ The political opponent's, *i.e.* John Adams', side judged that '[i]n short there never was so barefaced and disgraceful an interference of a foreign power in any free country.'⁹ The United States, according to some estimates, influenced 81 presidential elections worldwide between 1947 and 2000, inter alia by using bribes and 'fake news':¹⁰ 'We've used posters, pamphlets, mailers, banners – you name it. We've planted false information in foreign newspa-

6 Art. 3 of Protocol No. 1 ECHR; ECtHR, Judgement (GC), 6 October 1976, *X v UK*, Application No. 7140/75; ECtHR, Judgment, 2 March 1987, *Mathieu-Mohin and Clerfayt v Belgium*, Application No. 9267/81, para. 54; Inter-Parliamentary Union, Inter-Parliamentary Council at its 154th session in Paris, *Declaration on Criteria for Free and Fair Elections*, 26 March 1994, <http://archive.ipu.org/cnl-e/154-free.htm>.

7 Roberts, 'Peter the Great in Poland' (1927) 5 *The Slavonic Review*, 537 (550).

8 DeConde, 'Washington's Farewell, the French Alliance, and the Election of 1796' (1957) 43 *The Mississippi Valley Historical Review*, 641 (653).

9 *Ibid.*

10 Shane, 'Russia Isn't the Only One Meddling in Elections. We Do It, Too', *The New York Times*, 17 February 2018, <https://www.nytimes.com/2018/02/17/sunday-review/russia-isnt-the-only-one-meddling-in-elections-we-do-it-too.html>.

pers. We've used what the British call 'King George's cavalry': suitcases of cash.'¹¹

II. Today's Story of Influencing Elections – Manipulating the Democratic Process via “Fake News” and Hate Speech

While some of the means of influencing elections have changed today, the deed as such still continues. Democratic states, on the one hand, mainly – but not exclusively¹² – do this overtly. For example, Germany supports democratic initiatives, e.g., via its political foundations and the US via tax-funded groups such as the National Democratic Institute and the International Republican Institute. While this is seen as problematic in some states such as Russia and Hungary, which have adopted so called “foreign agent laws” that aim at minimizing financial and other support to political actors,¹³ there is a difference between this kind of overt influence and the influence of elections that this book chapter is about: these organisations, in principle, do not try to get certain candidates elected but to empower citizens to make use of their democratic rights.¹⁴ Instead of manipulating the democratic process, they foster it. Authoritarian States, on the other

11 *Ibid.*

12 *Ibid*; Levin, ‘Partisan electoral interventions by the great powers: Introducing the PEIG Dataset’ (2019) 36 *Conflict Management and Peace Science*, 88; Tharoor, ‘The long history of the U.S. interfering with elections elsewhere’, The Washington Post, 13 October 2016, <https://www.washingtonpost.com/news/worldviews/wp/2016/10/13/the-long-history-of-the-u-s-interfering-with-elections-elsewhere/>.

13 For Russia see Tysiachniouk et al., ‘Civil Society under the Law ‘On Foreign Agents’: NGO Strategies and Network Transformation’ (2018) 70 *Europe-Asia Studies*, 615; for Hungary see Bárd, ‘The Hungarian “Lex NGO” before the CJEU: Calling an Abuse of State Power by its Name’, *Verfassungsblog*, 27 January 2020, <https://verfassungsblog.de/the-hungarian-lex-ngo-before-the-cjeu-calling-an-abuse-of-state-power-by-its-name/>.

14 Shane, ‘Russia Isn’t the Only One Meddling in Elections. We Do It, Too.’, The New York Times, 17 February 2018, <https://www.nytimes.com/2018/02/17/sunday-review/russia-isnt-the-only-one-meddling-in-elections-we-do-it-too.html>. See for a distinction between process-oriented election intervention (for or against democracy) and actor-oriented election intervention (for or against a particular candidate): Bubeck et al., ‘Why Do States Intervene in the Elections of Others? The Role of Incumbent–Opposition Divisions’ (2020) *British Journal of Political Science*, 1 (2). For a similar distinction also see Shulman and Bloom, ‘The legitimacy of foreign intervention in elections: The Ukrainian response’ (2012) 38 *Review of International Studies*, 445 (450 f.).

hand, tend to influence foreign elections via covert operations that make use of information in a devious way and use “fake news” and hate speech to manipulate the electorate.¹⁵

1. “Fake News” and the Difference between Mis-, Dis- and Mal-Information

The International Organization in which the European Court of Human Rights is embedded – i.e., the Council of Europe – differentiates three different types of ‘fake news’.¹⁶ The first type is called misinformation and is understood to be false information not created with the intent of causing harm. Misinformation may thus be a pure mistake or satire.¹⁷ The second type is called disinformation and is equally understood to be false information, but one which is deliberately created to cause harm.¹⁸ Lastly, the third type is mal-information, which is information based on reality, and thus in principle is true, but shared in order to inflict harm.¹⁹ This form of ‘fake news’ is the most dangerous one as it is based on reality but distorts it.²⁰ An aphorism by *William Blake*, coined already in 1807, describes well how much influence this last category of ‘fake news’ may have: ‘A truth that’s told with bad intent / Beats all the lies you can invent.’²¹

2. Hate Speech: Spreading Hatred based on Intolerance

Closely connected to ‘fake news’ is the problem of hate speech. Some ‘fake news’ might be hate speech and vice versa – e.g., the denial of the holocaust. ‘Fake news’ might also lead to hate speech by others and might intended to do so. While the ECHR does not know the term hate speech, the ECtHR uses it²² and understands it to encompass ‘all forms

15 See Cardenal et al., *Sharp power: rising authoritarian influence* (2017).

16 CoE, *Information Disorder: Toward an interdisciplinary framework for research and policy making*, September 2017, CoE report DGI (2017) 09.

17 *Id.*, 16.

18 *Id.*, 20.

19 *Ibid.*

20 Baade, ‘Fake News and International Law’ (2019) 29 *EJIL*, 1357 (1358 ff.).

21 *Ibid.*; Blake, ‘Auguries of Innocence’, *The Pickering Manuscript* (1807), line 23 f., available at www.blakearchive.org/copy/bb126.1?descId=bb126.1.ms.15.

22 See e.g. ECtHR, Judgement (GC), 16 June 2015, *Delfi AS v Estonia*, Application No. 64569/09, e.g. paras. 151, 152, 154, 155, 156, 157, 158; See also ECtHR, Judgement, 4 December 2003, *Gündüz v Turkey*, Application No. 35071/97, e.g.

of expression which spread, incite, promote or justify hatred based on intolerance.’²³

3. The Recent Rise of “Fake News” and Hate Speech in the Context of Elections

In the last years, the dissemination of disinformation, mal-information and hate speech in general has been unprecedented.²⁴ This is inseparably connected to the rise of the internet. While the upsurge of ‘fake news’ and hate speech is already a worrisome development, from a democratic point of view, this becomes even worse when the cornerstone of democracy, i.e., elections, is the target of disinformation, mal-information and hate speech.

The impact of ‘fake news’ and hate speech on the 2016 US presidential election has been considerable.²⁵ European elections have been the target of ‘fake news’ and hate speech as well. For example, the UK House of Commons Digital, Culture, Media and Sports Committee, in its 2018 Interim Report on Disinformation and ‘Fake News’ found that ‘156,252 Russian accounts [were] tweeting about #Brexit and that they posted over 45,000 Brexit messages in the last 48 hours of the campaign.’²⁶ In short,

paras. 21, 22, 40, 44, 51; ECtHR, Judgement, 9 May 2018, *Stomakhin v Russia*, Application No. 52273/07, e.g. paras. 6, 70, 71, 72, 96, 117; ECtHR, Decision, 12 May 2020, *Lilliendahl v Iceland*, Application No. 29297/18, e.g. paras. 4, 13, 17, 32, 33, 34, 35, 39.

23 ECtHR, Judgement, 4 December 2003, *Gündüz v Turkey*, Application No. 35071/97, para. 40; ECtHR, Judgement, 5 December 2019, *Tagiyev and Huseynov v Azerbaijan*, Application No. 13274/08, para. 38

24 For an exploration see e.g. Martens et al., ‘The digital transformation of news media and the rise of disinformation and fake news’, JRC Digital Economy Working Paper No. 2018–02, <https://www.econstor.eu/bitstream/10419/202231/1/jrc-dewp201802.pdf>.

25 The United States District Court for the District of Columbia 16.02.2018 – Case 1:18-cr-00032-DLF – *United States of America v Internet Research Agency LLC A/K/A Mediasintez*, www.justice.gov/file/1035477/download, para. 32; Scola, ‘How chatbots are colonizing politics’, Politico, 10 November 2016, www.politico.com/story/2016/10/chatbots-are-invading-politics-229598; Robertson et al., ‘How to Hack an Election’, Bloomberg Businessweek, 31 March 2016, www.bloomberg.com/features/2016-how-to-hack-an-election/; Steiger, ‘International Law and New Challenges to Democracy in the Digital Age: Big Data, Privacy and Interferences with the Political Process’ in Witzleb et al. (eds), *Big Data, Political Campaigning and the Law: Privacy and Democracy in the Age of Micro-Targeting* (2020), 71 (73).

26 DCMSC, HC 363, Disinformation and ‘fake news’: Interim Report, 29 July 2018, <https://publications.parliament.uk/pa/cm201719/cmselect/cmcomeds/363/36302.htm>, para. 162.

Russia followed the US election campaign playbook by using *personae* who pretended to be ordinary citizens and posted offensive and often divisive comments aimed at sowing 'mistrust and confusion and to sharpen existing divisions in society, [which] may also have destabilising effects on democratic processes.'²⁷ Further, Russia deployed social bots, i.e. automated software programs that perform tasks within social networks and pretend to be human beings and behave like trolls, programmed to post controversial and divisive comments on websites and on Facebook, or use fake Twitter accounts and other means to magnify comments of trolls and make their work more effective.²⁸

Also, the notorious company Cambridge Analytica, is said to have worked for Brexit.²⁹ The by now dissolved company and its methods, which have survived the dissolution of the company,³⁰ are able to have a tremendous impact on elections, as was shown in the 2016 US presidential election. Here, the company used direct marketing tools in order to manipulate voters. This manipulation became possible via an algorithm that used data available via Facebook³¹ to create a so called Ocean Score that divided people into five basic types.³² It is said that the algorithm already knows you better than a friend by taking into account only 70 Facebook

27 CoE Committee of Ministers, 1309th Meeting, CM/Rec(2018)2, preamble para. 3.

28 Gorodnichenko et al., 'Social Media, Sentiment and Public Opinions: Evidence from #Brexit and #Uselection' (2018) NBER Working Paper No. 24631.

29 Scott, 'Cambridge Analytica did work for Brexit groups, says ex-staffer', Politico, 30 July 2019, <https://www.politico.eu/article/cambridge-analytica-leave-eu-ukip-brexit-facebook/>; but see BBC News, 'Cambridge Analytica 'not involved' in Brexit referendum, says watchdog', 7 October 2020, <https://www.bbc.com/news/uk-politics-54457407>; Gehrke, 'UK probe finds no evidence that Cambridge Analytica misused data to influence Brexit', Politico, 7 October 2020, <https://www.politico.eu/article/no-evidence-that-cambridge-analytica-misused-data-to-influence-brexit-report/>; U.K. Information Commissioner's Office (ICO), RE: ICO investigation into use of personal information and political influence, 2 October 2020, https://ico.org.uk/media/action-weve-taken/2618383/20201002_ico-o-ed-l-rtl-0181_to-julian-knight-mp.pdf, para. 7.

30 Goldhill, 'A 'big data' firm sells Cambridge Analytica's methods to global politicians, documents show', Quartz, 14 August 2019, <https://qz.com/1666776/data-firm-idea-uses-cambridge-analytica-methods-to-target-voters/>.

31 See generally Fuster and Scherrer, Big data and smart devices and their impact on privacy, Directorate-General for Internal Policies of the Union Study, September 2015, [http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536455/IPOL_STU\(2015\)536455_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536455/IPOL_STU(2015)536455_EN.pdf), 10 f.

32 See generally John et al., 'Paradigm Shift to the Integrative Big Five Trait Taxonomy' in John et al. (eds), *Handbook of Personality: Theory and Research* (3rd edn., Guildford Press 2008) 114 (114–117).

likes.³³ With 150 likes, it knows you better than your parents and with 300 likes it knows you better than your partner.³⁴ With this knowledge, personalized ads, called dark posts because they could only be seen by the target person and will often not even be disclosed as an ad, were directed at Facebook users, often with a racist undertone or with at least misleading information.³⁵ A comparison between ordinary commercials and these micro-targeted dark posts shows the effectiveness of this tool: click rates increase by 60 % compared to non-personalised advertising.³⁶ The conversion rate, which indicates the percentage of those who click and those who actually become buyers, rises by an extraordinary 1,400 %.³⁷

In the French presidential election campaign of 2017, disinformation shared on Twitter included assertions that Emmanuel Macron was homosexual or an agent for financial interests of the United States.³⁸ This election campaign included also the most notorious hack in a European election context: The – probably – Russian hacks by the hacker group APT 28, also called Fancy Bear, into the servers of the Emmanuel Macron's presidential campaign led to the subsequent release of 21,000 e-mails and nine gigabytes of stolen files, aimed to influence the French election.³⁹ While the publication of the material in principle has to be understood as a mal-information attack, according to the campaign managers, the leaked material included fake material,⁴⁰ and thus also disinformation. Because of the very quick response by the Macron campaign, it is being assumed that it itself planted the fake material in order to be prepared for and be able to counter any possible leaks.⁴¹

33 Quenqua, 'Facebook Knows You Better Than Anyone Else', The New York Times, 19 January 2015, <www.nytimes.com/2015/01/20/science/facebook-knows-you-better-than-anyone-else.html>.

34 *Ibid.*

35 Cf. Grassegger and Krogerus, 'Cambridge Analytica / Big data and the Future of Democracy: The Matrix world behind the Brexit and the US Elections', *Diplomat Magazine*, 5 March 2017, www.diplomatmagazine.nl/2018/03/22/cambridge-analytica-big-data-and-the-future-of-democracy-the-matrix-world-behind-the-brexit-and-the-us-elections/.

36 *Ibid.*

37 *Ibid.*

38 Brattberg and Maurer, Russian Election Interference – Europe's Counter to Fake News and Cyber Attacks, Carnegie Endowment for International Peace, May 2018, https://carnegieendowment.org/files/CP_333_BrattbergMaurer_Russia_Elections_Interference_FINAL.pdf, 10 f.

39 *Ibid.*

40 *Id.*, 11.

41 *Ibid.*

In the European Election of 2019, 500 suspicious pages and groups on Facebook were named that emitted disinformation. 32 million people followed these groups; 67 million people liked, commented, or shared them; and the content received 533 million views.⁴² Facebook banned 77 pages und groups and blocked 230 accounts.⁴³

The aim of foreign interference is to sow discord and division,⁴⁴ and they are quite successful in inspiring individuals in partaking. Hate speech against politicians for example is massively on the rise, especially against female politicians.⁴⁵ In Germany, for instance, the number of criminal offences against politicians increased from 1,674 in 2019 to 2,629 in 2020, which is a rise of 57 %.⁴⁶ A multitude of these crimes were insults and threats uttered in the anonymity of the internet.⁴⁷ 64 % of the female Members of German Parliament who participated in a 2021 survey by the weekly news magazine SPIEGEL said they experienced misogynistic hatred expressed in messages, mostly online.⁴⁸ Small extremist groups reportedly used hate postings to exert control over online discussions and in that way influenced the outcome of elections.⁴⁹ For example, in the time leading up to the 2017 German federal elections, Reconquista Germania, a right-wing troll factory, gained 7,000 members within a few weeks and succeeded in placing seven of its hashtags among the top 20 hashtags in Germany only

42 Lomas, 'Facebook found hosting masses of far right EU disinformation networks', Tech Crunch, 22 May 2019, <https://techcrunch.com/2019/05/22/facebook-found-hosting-masses-of-far-right-eu-disinformation-networks/>.

43 *Ibid.*

44 Ohlin, *Election Interference – International Law and the Future of Democracy* (2020), 14.

45 Knight, 'Germany: Hate speech, threats against politicians rise', Deutsche Welle, 9 February 2021, <https://www.dw.com/en/germany-hate-speech-threats-against-politicians-rise/a-56512214>.

46 Deutscher Bundestag, Drucksache 19/26419, 3 February 2021, Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Dr. André Hahn, Gökyay Akbulut, weiterer Abgeordneter und der Fraktion DIE LINKE.– Drucksache 19/26017 -Straftaten gegen Amts- und Mandatsträger.

47 *Id.*, 5.

48 SPIEGEL online, 'SPIEGEL-Umfrage unter Parlamentarierinnen – Frauenfeindlichkeit im Bundestag durch AFD gestiegen', 12 February 2021, <https://www.spiegel.de/politik/deutschland/bundestag-frauenfeindlichkeit-durch-afd-gestiegen-a-4c8c425c-6b08-4ac5-b049-61ad65d1240c>.

49 CoE, ECRI Report on Germany (sixth monitoring cycle), 17 March 2020, <https://rm.coe.int/ecri-report-on-germany-sixth-monitoring-cycle-/16809ce4be>, para. 38.

two weeks before the election.⁵⁰ Also ‘fake news’ played a role before the 2017 German federal election: BuzzFeed News found that seven of the ten most commented, linked, and liked articles about Angela Merkel on Facebook could be classified as disinformation.⁵¹ While other studies rather suggest that the circulation of disinformation played a comparatively small role in the German elections,⁵² they problematize that once disinformation is spread, it cannot easily be corrected: only in one out of ten cases did the corrected information achieve a greater circulation than the disinformation.⁵³ To conclude, dis- and mal-information attacks are obviously real, as is a rise in hate speech. Especially since not only Russia but also China and Iran are stepping up their hybrid and disinformation warfare capabilities,⁵⁴ it seems to be mandatory that Europe finds effective – and legal – answers to this threat.

III. *Fighting Back – European States’ and the EU’s Response to Counter Election Influence*

Politics and academia have not been oblivious to the phenomena identified above. Since 2017, States around the world have introduced legislation

-
- 50 Köhler and Ebner, ‘Strategies and tactics: communication strategies of jihadists and right-wing extremists’ in Baldauf et al. (eds), *Hate Speech and Radicalisation Online – The OCCI Research Report* (2019), 18 (24), <https://www.isdglobal.org/wp-content/uploads/2019/06/ISD-Hate-Speech-and-Radicalisation-Online-English-Draft-2.pdf>.
- 51 Schmehl and Lytvynenko, ‘7 Out Of The 10 Most Viral Articles About Angela Merkel On Facebook Are False’, BuzzFeed News, 27 July 2017, <https://www.buzzfeednews.com/article/karstenschmehl/top-merkel-news>.
- 52 Schwarz and Holnburger, ‘Disinformation: what role does disinformation play for hate speech and extremism on the internet and what measures have social media companies taken to combat it?’ in Baldauf et al. (eds), *Hate Speech and Radicalisation Online – The OCCI Research Report* (2019), 35 (36), <https://www.isdglobal.org/wp-content/uploads/2019/06/ISD-Hate-Speech-and-Radicalisation-Online-English-Draft-2.pdf>.
- 53 *Ibid.*; Sänglerlaub et al., *Fakten statt Fakes – Verursacher, Verbreitungswege und Wirkungen von Fake News im Bundestagswahlkampf 2017*, Stiftung Neue Verantwortung, März 2018, https://www.stiftung-nv.de/sites/default/files/snv_faktenstatt_fakes.pdf, 79.
- 54 Shearer, *The Evolution of Hybrid Warfare and Key Challenges*, Statement Before the House Armed Services Committee, 22 March 2017, https://csis-website-prod.s3.amazonaws.com/s3fs-public/congressional_testimony/170322_shearer_testimony_evolution_of_hybrid_warfare.pdf.

to combat ‘fake news’ and hate speech on the internet in order to protect democracy.⁵⁵ They do so by creating new obligations for online intermediaries with regard to the speech that is published on their platforms. While the idea behind these new rules is, in principle, to protect the democratic discourse, these laws have been criticized for impeding the right to freedom of expression.⁵⁶ Furthermore, in some legislations, there have been accusations that the laws serve to silence dissent and hinder democratic discourse.⁵⁷ The most outstanding examples of current legislation aimed at countering hate speech and ‘fake news’ will form the focus of the following legal analysis. These are, namely, two French laws, ‘Loi Avia’ and ‘Loi No. 2018–1202’ respectively (1.), the German Network Enforcement Act (‘GNEA’) (2.), and the proposed EU Digital Services Act (3.).

-
- 55 For an overview see Funke and Flamini, A guide to anti-misinformation actions around the world, Poynter, <https://www.poynter.org/ifcn/anti-misinformation-actions/>; Hacıyakupoglu et al., Policy Report Countering Fake News – A Survey of Recent Global Initiatives, Rajaratnam School of International Studies, March 2018, https://www.rsis.edu.sg/wp-content/uploads/2018/03/PR180307_Counterin-g-Fake-News.pdf; Article 19, Responding to ‘hate speech’: Comparative overview of six EU countries, 2018, https://www.article19.org/wp-content/uploads/2018/03/ECA-hate-speech-compilation-report_March-2018.pdf; Laub, Hate Speech on Social Media: Global Comparisons, Council on Foreign Relations, 11 April 2019, <https://www.cfr.org/backgrounder/hate-speech-social-media-global-comparisons>.
- 56 See for Germany e.g.: Hong, ‘The German Network Enforcement Act and the Presumption in Favour of Freedom of Speech’, *Verfassungsblog*, 22 January 2018, <https://verfassungsblog.de/the-german-network-enforcement-act-and-the-presumption-in-favour-of-freedom-of-speech/>; Peukert, ‘Put it back: Ein Vorschlag für ein NetzDG, das die Meinungsfreiheit wahrt’, *Verfassungsblog*, 14 June 2018, <https://verfassungsblog.de/put-it-back-ein-vorschlag-fuer-ein-netzdg-das-die-meinungsfreiheit-wahrt/>; Lang, ‘Netzwerkdurchsetzungsgesetz und Meinungsfreiheit’ (2018) 143 *AöR*, 220 (225 f.); for France: Wienfort, ‘Blocking Overblocking – Frankreichs Verfassungsrat kippt das Gesetz gegen Hasskriminalität im Netz’, *Verfassungsblog*, 20 June 2020, <https://verfassungsblog.de/blocking-overblocking/>; Smith, ‘Fake news, French Law and Democratic Legitimacy: Lessons for the United Kingdom?’ (2019) 11 *Journal of Media Law*, 52 (53).
- 57 For example in Russia, see International Press Institute, New ‘fake news’ law stifles independent reporting in Russia on Covid-19, 8 May 2020, <https://ipi.media/new-fake-news-law-stifles-independent-reporting-in-russia-on-covid-19/>; Pollicino, ‘Fundamental Rights as Bycatch – Russia’s Anti-Fake News Legislation’, *Verfassungsblog*, 28 March 2019, <https://verfassungsblog.de/fundamental-rights-as-bycatch-russias-anti-fake-news-legislation/>.

1. The French Approach: Generally Combatting Hate Speech; “Fake News” only in Election Times

The French legislator chose to enact two different laws, one directed against hate speech in general (a) and the other against fake news in election times (b).

a) Loi Avia Against Hate Speech: Not Enough Time and Too Much Discretion

The Loi Avia, the French law to combat hate speech,⁵⁸ which was declared unconstitutional by the French Conseil Constitutionnel,⁵⁹ obliged all online intermediaries, understood in a very broad sense to include any provider of online communication services or storage, independent of the number of users, to remove all posts with terrorist or child pornography content within one hour after notice by an administrative authority (art 1^{er} (I) 1° (b)). Other manifestly illegal content, which was explicitly listed, such as content condoning the commission of certain crimes or incitement to discrimination, hatred or violence (art 1^{er} (II)), had to be taken down within 24 hours after the online intermediary had been notified about the post (art 1^{er} (II), so called notice and takedown procedure). Article 4 required an internal complaint handling system against takedown decisions as well as against decisions not to take down certain posts. The Conseil Supérieur de l'Audiovisuel would have supervised this process. In the case of non-compliance, the online intermediaries, in the case of art 1^{er} (II) only professional online platform operators whose activity on French territory exceeded a certain monetary threshold that was to be determined by decree, faced fines of up to 250,000 € (art 1^{er} (II)). In case of violations of art 1^{er} (I), up to one year of imprisonment was foreseen.

The Conseil Constitutionnel mainly differentiated between the two different paragraphs of Article 1: for the unconstitutionality of paragraph I, the main reasons given were that the one-hour time limit did not allow for any judicial review of the administrative takedown decision, that a request

58 Assemblée Nationale, Proposition de loi n° 388, adoptée par l'Assemblée nationale, en nouvelle lecture, visant à lutter contre les contenus haineux sur internet, 13 Mai 2020, https://www.assemblee-nationale.fr/dyn/15/textes/l15t0388_texte-adopt-e-seance#.

59 Conseil Constitutionnel, 18 June 2020, Décision no 2020–801 DC – JORF, n° 0156 du 25/06/2020, Texte 2 sur 181, para. 8, para. 19.

to review the decision would not have any suspensive effect, and that finally the law foresaw no requirement that the content had to be “manifestly illegal” and thus allowed the administrative authority too much discretion.⁶⁰

With regard to paragraph II, the Conseil Constitutionnel held it to be problematic that, instead of a court order, a notice by any individual sufficed to obligate the online intermediary to act; underlined the difficulties for online intermediaries in ascertaining whether a post is obviously unlawful, especially within such a short time limit, and that the norm lacked specific possibilities for online intermediaries to be exempted from liability.⁶¹ These reasons read together with the high penalties that would be incurred already for the first infringement⁶² would lead online intermediaries to block content that had been flagged by users as manifestly illegal just to be on the safe side.⁶³ The Law Avia, , according to the Conseil Constitutionnel, thus violated the right to freedom of expression in a disproportionate manner.

b) Loi No. 2018–1202 Against the Manipulation of Information: A much more Differentiated and Precise Approach

The Loi No. 2018–1202, which entered into force in November 2018, is directed against ‘fausses informations’ (‘false information’), in the sense of ‘inaccurate or misleading allegations or imputations of a fact likely to affect the integrity of [a] forthcoming election.’⁶⁴ If such false information whose ‘incorrect or misleading nature is apparent’,⁶⁵ is disseminated deliberately, artificially or automatically, and on a mass scale via an online public communication service that has more than five million visitors per month or is paid 100 € for each piece of content that is related to a debate of general interest, has been subjectively transmitted to cause harm and ob-

60 *Id.*, para. 7.

61 *Id.*, para. 19.

62 *Id.*, para. 18.

63 *Id.*, para. 19.

64 Loi no 2018–1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l’information, JORF n° 0297 du 23 décembre 2018, Texte 2 sur 191, art. 1^{er} 2°; original wording: “allégations ou imputations inexactes ou trompeuses d’un fait de nature à altérer la sincérité du scrutin à venir”.

65 Conseil Constitutionnel, 20 December 2018, Décision no 2018–773 DC- JORF, n°0297 du 23 décembre 2018, Texte 5 sur 191, para. 23.

jectively possesses the apparent effect of undermining the reliability of the election,⁶⁶ a judge may order its removal or the blockage of certain websites. The judge has to act within 48 hours after such a request – which can be filed by everyone during the three months before elections. The Conseil Constitutionnel in December 2018 held that the law struck a ‘balance [between] the constitutional principle of the honesty of elections with the constitutional freedom of expression.’⁶⁷ Decisive arguments of the Conseil Constitutionnel in favor of the constitutionality of Loi No. 2018–1202 were, *inter alia*, that it only applies in the three months before elections;⁶⁸ that instead of a notice and takedown procedure⁶⁹ a judge has to order the takedown of the posts; the preconditions that allow the judge to act are precisely framed; that the fines, which may be imposed on the users and the platforms alike, only reach up to 75,000 €⁷⁰; and that the online intermediaries are rather narrowly defined. These arguments also indirectly highlight the differences between the two French Laws and show why the first law violates the right to freedom of expression and the other does not.

2. The German Approach: Generally Combatting Hate Speech and – less so – “Fake News”

The GNEA’s⁷¹ express motivation is to combat hate speech and other unlawful content including punishable ‘fake news’.⁷² These terms, however, do not feature in the text. Instead, the GNEA obligates online intermediaries with more than two million registered users in Germany to help in enforcing – hence the name ‘Network Enforcement Act’ – certain sections of the German Criminal Code, in particular, the prohibition of public

⁶⁶ *Ibid.*

⁶⁷ *Id.*, paras. 17, 25.

⁶⁸ *Id.*, paras. 8, 9, 19.

⁶⁹ *Id.*, para. 21.

⁷⁰ *Id.*, para. 7.

⁷¹ Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG) vom 1. September 2017, BGBl. Jahrgang 2017 Teil 1 Nr. 61; for an overview see Lauber-Rönsberg, ‘Hate Speech – ein Überblick über rechtliche Rahmenbedingungen, ihre Durchsetzung und das neue NetzDG’ (2017) 13 *Aptum*, 100.

⁷² Deutscher Bundestag, Drucksache 18/12727, 18. Wahlperiode, 14 June 2017, Gesetzentwurf der Bundesregierung Entwurf eines Gesetzes zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG), 1 f.

incitement to crime or incitement to hatred.⁷³ A closer look reveals that, while hate speech is indeed targeted by the GNEA, ‘fake news’ is only marginally touched upon: of the 21 sections of the Criminal Code that are explicitly named by the GNEA, only the defamation of religions, religious and ideological associations, insults, and the general prohibition of defamation encompass an element of falsehood. While some types of disinformation, e.g., those that refer to financial dependencies of politicians, might be subsumed under these norms, many other types of disinformation, especially politically misleading ones, such as that Chancellor Angela Merkel ‘hopes’ for 12 million immigrants by 2060,⁷⁴ will not. While the GNEA is not specifically designed to protect elections, it aims to protect a ‘free, open and democratic society’⁷⁵ by civilizing the public discourse.

Posts that contravene these prohibitions have to be taken down within seven days by the online intermediary after having received the complaint (§ 3 (2) Nr. 3 GNEA). If the post is manifestly unlawful, it must be blocked or taken down within 24 hours (§ 3 (2) Nr. 3 GNEA).⁷⁶

There are some similarities between the GNEA and the Loi Avia, such as the notice and takedown procedure, the difficulties to determine whether a post is manifestly unlawful or not and that no specific grounds for online intermediaries to exempt themselves from liability exist.⁷⁷ However, there are important differences: while the GNEA regulates that social media companies face fines of up to five million Euros, it only requires

73 Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG) vom 1. September 2017, BGBl Jahrgang 2017 Teil 1 Nr. 61, § 1 (3).

74 Röttger, ‘Nein – Merkel „hofft“ nicht auf 12 Millionen Einwanderer’, Correctiv, 5 March 2018, <https://correctiv.org/fakten-check/2018/03/05/nein-merkel-hofft-nicht-auf-12-millionen-einwanderer/>.

75 Deutscher Bundestag, Drucksache 18/12727, 18. Wahlperiode, 14 June 2017, Gesetzentwurf der Bundesregierung Entwurf eines Gesetzes zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG), 1.

76 Katsirea, ‘“Fake news”: reconsidering the value of untruthful expression in the face of regulatory uncertainty’ (2018) 10 *Journal of Media Law*, 159 (181).

77 Assemblée Nationale, Proposition de loi n° 388, adoptée par l'Assemblée nationale, en nouvelle lecture, visant à lutter contre les contenus haineux sur internet, 13 May 2020, https://www.assemblee-nationale.fr/dyn/15/textes/115t0388_texte-adoptee-seance#; Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG) vom 1. September 2017, BGBl Jahrgang 2017 Teil 1 Nr. 61.

that these fines are paid for systematic violations of their obligations.⁷⁸ Furthermore, the time frame is not as strict and the GNEA even allows for the possibility to prolong the time frame under specific circumstances.⁷⁹ One of the major shortcomings of the original 2017 GNEA is that, even though online intermediaries are obligated to give reasons for their decision (§ 3 (2) Nr. 5 GNEA), no remedies were provided against the social media companies in case they block or delete a post, not even an internal complaint mechanism as installed by the art 4 Loi Avia. However, German lawmakers just recently tackled this shortcoming. In June 2021, an amendment to the GNEA, obliged online intermediaries to install an internal complaint-handling system⁸⁰ and an out-of-court settlement procedure.⁸¹ Furthermore, German civil law courts have successfully obligated Facebook to restore deleted or blocked posts on the basis of the German Civil Law Code ('put-back').⁸² The basis for such put-back claims are the private law contracts between online intermediaries and users, including the terms and conditions, but also the right to freedom of expression.⁸³ While online intermediaries are not directly bound by human rights, the German constitutional doctrine of indirect third party effect or horizontal effect ('mittelbare Drittwirkung') allows for some indirect impact of human rights within private law relationships.⁸⁴

78 Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG) vom 1. September 2017, BGBl Jahrgang 2017 Teil 1 Nr. 61, § 4.

79 Peukert, 'Put it back: Ein Vorschlag für ein NetzDG, das die Meinungsfreiheit wahrt', Verfassungsblog, 14 June 2018, <https://verfassungsblog.de/put-it-back-ein-vorschlag-fuer-ein-netzdg-das-die-meinungsfreiheit-wahrt/>.

80 Gesetz zur Änderung des Netzwerkdurchsetzungsgesetzes vom 03. Juni 2021, BGBl Jahrgang 2021 Teil 1 Nr. 29, § 3b.

81 *Id.*, § 3c.

82 Kettemann and Tiedeke, 'Back up: can users sue platforms to reinstate deleted content?' (2020) 9 *Internet Policy Review*, 1 (10f.); Peukert, 'Gewährleistung der Meinungs- und Informationsfreiheit in sozialen Netzwerken. Vorschlag für eine Ergänzung des NetzDG um sog. Put-back-Verfahren' (2018) *MMR*, 572.

83 Kalbhenn and Hemmert-Halswick, 'Der Regierungsentwurf zur Änderung des NetzDG – Vom Compliance-Ansatz zu Designvorgaben' (2020), *MMR*, 518 (519).

84 BVerfG, Decision, 11 April 2018, 1 BvR 3080/09, http://www.bverfg.de/e/rs20180411_1bvr308009.html; OLG München Decision, 17 July 2018 – 18 W 858/18, *Juris*; OLG Dresden Decision, 8 August 2018 – 4 W 577/18, <https://www.debi er.de/debi er-datenbank/?dbnr=olgd0004W-2018-00577>; BVerfG, Decision, 22 May 2019, 1 BvQ 42/19, http://www.bverfg.de/e/qk20190522_1bvq004219.html; OLG Oldenburg, Judgement, 1 July 2019, – 13 W 16/19; OLG München Judgement, 7 January 2020 – 18 U 1491/19 Pre, *Juris*; Schleswig-Holsteinisches Oberlandesgericht Judgement, 26 February 2020 – 9 U 125/19, *Juris*; see also

3. *The EU Approach: Adding an Additional Layer to the Protection of Elections*

Purely national approaches to regulate the internet seem to be rather outdated given the internet's ubiquity. Consequently, in December 2020, the EU Commission has proposed a new comprehensive EU regulation, i.e., a directly applicable set of legally binding rules that will take precedence over national law (Article 288 (2) TFEU), in order to regulate online intermediaries.

a) Personal and Material Scope of Application

The Digital Services Act Draft⁸⁵ ('DSA-Draft') aims to contribute to the proper functioning of the internal market for intermediary services and to help in creating a safe, predictable, and trusted online environment where fundamental rights are effectively protected (Article 1 (2) lit. b) DSA-Draft). The DSA-Draft differentiates between 'online platforms', i.e., a provider of a hosting service that, at the request of a recipient of the service, stores and disseminates information to the public (Article 2 lit. h) DSA-Draft) and 'very large online platforms', i.e., those platforms that provide their services to more than 45 million active users (Article 25 (1) DSA). The draft further differentiates between illegal content, which 'means any information that [...] is not in compliance with Union law or the law of a Member State' (Art. 2 lit. g) DSA-Draft), and manifestly illegal content that is, according to recital 47 DSA-Draft, information 'where it is evident to a layperson, without any substantive analysis, that the content is illegal.' While hate speech will be such manifestly illegal content, 'fake news' as 'harmful content' (recital 52 DSA-Draft) often will not – but the DSA-Draft has found an additional way on how to deal with 'fake news' (see below d).

Kettemann and Tiedeke, 'Back up: can users sue platforms to reinstate deleted content?' (2020) 9 *Internet Policy Review*, 1 (9).

85 European Commission, *Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC*, 15 December 2020, COM (2020) 825 final.

b) (Excluding) Liability of Online Platforms

The DSA itself does not regulate that *illegal content* has to be taken down. It only obliges online platforms to suspend, for a reasonable period of time and after having issued a prior warning, the provision of their services to recipients of the service that frequently provide *manifestly illegal content* (Article 20 DSA-Draft). However, since Article 5 (1) lit. b) DSA-Draft excludes online platforms' liability only before they have been notified of illegal content, platforms are under an indirect obligation to take down illegal content 'expeditiously' after having been notified, or else they will be liable for it. Additionally, Article 8 DSA-Draft institutes procedural rules for situations in which national judicial or administrative authorities issue orders with regard to illegal content: online intermediaries need to be transparent about the actions taken and the authorities need to issue a statement of reasons explaining, *inter alia*, why the information is illegal content and inform about the redress available to the provider of the service and to the recipient of the service who published the content.

c) Notice and Takedown Procedure and Legal Remedies

With regard to the notice and takedown procedure, online platforms shall put mechanisms in place that allow them to be notified of illegal content (Article 14 DSA-Draft). If a takedown decision has been made, the platform has to inform the user whose post has been blocked or whose access has been disabled of the decision and provide the user with a clear and specific statement of reasons (Article 15 DSA-Draft). Users have the right to access an effective internal complaint-handling system (Article 17 DSA-Draft), which, if the post is not illegal, obliges the platform to reverse its decision without undue delay,⁸⁶ and to access an out-of-court dispute settlement body which shall be established with the Digital Services Coordinator of the Member State. Further judicial remedies based on domestic law are not prejudiced by this multi-step approach (Article 18 DSA-Draft).

⁸⁶ Kaesling, 'Evolution statt Revolution der Plattformregulierung' (2021) *ZUM*, 177 (182).

d) “Fake News” and Advertisement Regulation

While the depicted rules will mainly help against hate speech, ‘fake news’ will often not be illegal but ‘only’ harmful. Here, the DSA-Draft adds a further layer of protection, if and insofar ‘fake news’ come via paid (political) advertisements as in the case of Cambridge Analytica. The nexus between ‘fake news’ and advertisements is highlighted by the DSA-Draft itself as it obligates online intermediaries to be transparent about their activities in this area by, *inter alia*, having

to facilitate supervision and research into emerging risks brought about by the distribution of advertising online, for example in relation to illegal advertisements or manipulative techniques and disinformation with a real and foreseeable negative impact on public health, public security, civil discourse, political participation and equality (recital 63 DSA-Draft).

Article 24 DSA provides that advertising shall be marked as such, that the person on whose behalf the advertisement is displayed shall be named and that the main parameters used to determine the recipient to whom the advertisement is displayed are indicated, including means of profiling (recital 52 DSA-Draft). Moreover, the Commission has already announced a legislative act on political advertisement.⁸⁷

e) Further Duties of Very Large Online Platforms

This standard is further raised for very large online platforms that have to compile and make publicly available the content of the advertisement and the natural or legal person on whose behalf the advertisement is displayed; the period during which the advertisement was displayed; whether the advertisement was intended to be displayed specifically to one or more particular groups of recipients of the service and if so, the main parameters used for that purpose; the total number of recipients of the service reached and, where applicable, aggregate numbers for the group or groups of recipients at whom the advertisement was targeted specifically (Article 30 DSA-Draft).

87 European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*, 3 December 2020, COM(2020) 790 final, 6.

Another way to combat ‘fake news’ – and also hate speech – comes via very large online platforms’ special duties to identify, analyse, assess and mitigate so called ‘significant systemic risks’ that include any intentional manipulation of the platforms’ services, including by means of inauthentic use or automated exploitation of the service, which has or might have a negative effect on the protection of, *inter alia*, civic discourse or electoral processes (Articles 26 ff. DSA-Draft).

f) Fines and Penalties

While Member States shall lay down the rules on penalties applicable to infringements (Article 42 DSA-Draft), very large online platforms may have to pay fines imposed by the EU Commission not exceeding 6 % of their total turnover (Article 59 DSA-Draft). Like the GNEA, but different from the Loi Avia, these fines may not be imposed for failing to take down single illegal posts but for more systematic omissions like not installing a functional notice and takedown procedure or failing to identify, analyse, assess and mitigate so called ‘significant systemic risks’ (Art. 26 DSA-Draft).

g) Summary – Regulating “Fake News” and Hate Speech, Not Only in Election Times

To conclude, the DSA-Draft regulates mainly hate speech but also ‘fake news’ – and not only in election times. It does not only foresee different remedies against over-blocking by containing a right of redress that is directed against the platform itself, it also installs a specific dispute settlement between the user and the platform and tackles the problem of ‘fake news’ and manipulation via advertisements. The electoral process is identified as particularly vulnerable. Fines are severe and can be as high as 6 percent of the yearly turnover, which, in the case of Facebook could be nearly 5 billion US Dollar.

4. Conclusion: Regulating Online Intermediaries in Different Ways

While the new regulations concentrate on online intermediaries, they also indirectly affect individuals. The French approach concentrates on hate speech on the one hand and ‘fake news’ on the other hand. Its ‘fake news’

legislation is specifically tailored to fight disinformation during election times. The takedown of disinformation has to be ordered by a judge. The German approach, just like the unconstitutional French approach to hate speech, relies on users notifying the online intermediaries about certain content. They have to decide whether content is legal, illegal – which needs to be taken down within a week – or manifestly illegal – which needs to be taken down within 24 hours. This duty mainly applies to hate speech and only marginally to ‘fake news’. Specific procedural rules to mitigate over-blocking do not yet exist but are in the making. Lastly, the European DSA-Draft not only tackles the problem of hate speech but also of micro-targeting and disinformation and foresees specific remedies against the deletion of posts and the blockage of individual access to online intermediaries. Just as the GNEA and the Loi Avia, the DSA-Draft obligates the online intermediaries to decide whether certain speech is lawful or not and thus ‘formalize[s] the role of social media platforms as the governors of [...] speech.’⁸⁸ Since all approaches are aimed at suppressing speech, it is questionable whether they are in conformity with the right to freedom of expression.

B. The Law: Applying the ECHR to Laws Regulating “Fake News” and Hate Speech

In order to answer the question of whether these rules are in conformity with the ECHR, the first question to be answered is who is protected and who is bound by human rights (I.), then the material scope of the ECHR’s substantive protection needs to be determined (II.), and lastly interferences with the right to freedom of expression need to be justified (III.). Here, *inter alia*, the right to freedom of expression must be balanced with the right to free elections.

I. Who is Protected and Who is Bound by the ECHR? Of Individuals and States, the EU, Companies, and Bots

Elections are influenced by individuals, by companies, and also by third States. In order to protect democracy from such interferences, States have

88 Helberger, ‘The Political Power of Platforms: How Current Attempts to Regulate Misinformation Amplify Opinion Power’ (2020) 8 *Digital Journalism*, 842 (844).

started to regulate online intermediaries, i.e., companies. These regulations have an indirect effect on those influencing elections, i.e., individuals, companies, and also third States. But neither are all of these actors protected nor are all of them bound by the ECHR.

1. Individuals – Protected by the ECHR

First and foremost, private individuals are protected by the ECHR. The regulations on hate speech and ‘fake news’ certainly have an impact on the freedom of expression of individuals as they obligate companies to take action against specific forms of online speech. While this is only an indirect effect – since the online intermediaries are specifically targeted, not the users of their service – this effect is so closely connected to the regulation of the state that the freedom of expression of the individual users might be interfered with.

2. Companies and Bots – Protected and Indirectly Bound by the ECHR

Further, a company that uses online intermediaries in order to express itself is protected by the ECHR.⁸⁹ But what about the online intermediaries? Here, it seems questionable whether they may rely on freedom of expression guarantees as it is not their speech act that is being interfered with but their users’. However, the ECtHR held that online intermediaries may rely on the right of freedom of expression.⁹⁰ Again, the situation is different

89 Cf. ECtHR, Judgment, 22 May 1990, *Autronic AG v Switzerland*, Application No. 12726/87, para. 47.

90 ECtHR, Judgment, 18 December 2012, *Ahmet Yildirim v Turkey*, Application No. 3111/10, paras. 49 f.; ECtHR, Judgment (GC), 20 January 2020, *Magyar Kétfarkú Kutya Párt (MKKP) v Hungary*, Application No. 201/17, paras. 87 f., 91; ECtHR, Decision, 19 September 2017, *Tamiz v UK*, Application No. 3877/14, para. 90; ECtHR, Decision, 19 February 2013, *Neij and Sunde Kolmisoppi v Sweden*, Application No. 40397/12; ECtHR, Judgment (GC) 16 June 2015, *Delfi AS v Estonia*, Application No. 64569/09, para. 118; ECtHR, Judgment, 2 February 2016, *MTE v Hungary*, Application No. 22947/13, para. 45; ECtHR, Decision, 7 February 2017, *Pihl v Sweden*, Application No. 74742/14, para. 29; ECtHR, Judgment, 19 March 2019, *Hoiness v Norway*, Application No. 43624/14, para. 68; see also Lauber-Rönsberg ‘Persönlichkeitsschutz in der EMRK und im EU-Recht, § 57. Europäische Menschenrechtskonvention’ in Götting et al. (eds), *Handbuch des Persönlichkeitsrechts* (2019), 1197 (mn. 87).

for bots that are often used in disinformation and hate speech contexts as amplifiers. They may not rely on the right to freedom of expression.⁹¹

Lastly, online intermediaries are not directly bound by human rights obligations. Individuals thus cannot claim that their right to freedom of expression has been violated by an online intermediary. However, indirectly, human rights may play a role in these purely private relationships as human rights are applied to private individuals via a State's 'duty to protect'.⁹² According to this duty, a State must, under certain circumstances, protect individuals from *de facto* human rights violations by other private actors, *inter alia* by creating 'a safe and enabling environment for everyone to participate in public debate and to express opinions and ideas without fear'.⁹³ Another way to indirectly bind online intermediaries is via the German Federal Constitutional Court's indirect third party effect doctrine.⁹⁴ Lastly, the UN Guiding Principles on Business and Human Rights hold that companies have a responsibility to respect human rights, including freedom of expression.⁹⁵

3. States and the EU – Bound but not Protected by the ECHR

If certain posts are attributed to a State, there will be no protection by the ECHR: States are bound, not protected by human rights treaties. Since attribution in cyber space, however, often is a very difficult if not an impossible task,⁹⁶ in case of doubt, the post will have to be understood as

91 Sardo, 'Categories, Balancing, and Fake News: The Jurisprudence of the European Court of Human Rights' (2020) *Canadian Journal of Law & Jurisprudence*, 435 (455).

92 Akandji-Kombe, *Positive Obligations under the European Convention on Human Rights* (2007), 14.

93 CoE Committee of Ministers, *Recommendation to member States on the roles and responsibilities of internet intermediaries*, 7 March 2018, CM/Rec(2018)2, para. 6.

94 See e.g. BVerfG, Decision, 11 April 2018, 1 BvR 3080/09, mn. 31 ff., http://www.bverfg.de/e/rs20180411_1bvr308009.html; see also Engle, 'Third Party Effect of Fundamental Rights (Drittwirkung)' (2009) 5 *Hanse Law Review*, 165; Kettemann and Tiedeke, 'Back up: can users sue platforms to reinstate deleted content?' (2020) 9 *Internet Policy Review*, 1 (8 ff.).

95 UNGA, *Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises*, 21 March 2011, A/HRC/17/31, 13 ff.

96 Krieger, 'Krieg gegen anonymous – Völkerrechtliche Regelungsmöglichkeiten bei unsicherer Zurechnung im Cyberwar' (2012) 50 *AVR*, 1 (3); Zimmermann, 'International Law and „Cyber Space“' (2014) 3 *ESIL Reflections*, 1 (3).

having emanated from a private individual and thus the ECHR's personal scope applies.

While France and Germany as High Contracting Parties have to obey their treaty obligations, the EU is not a High Contracting Party (yet⁹⁷). Nevertheless, it is indirectly bound because of Article 6 (3) TEU and since all the EU member states are High Contracting Parties of the ECHR. Furthermore, the guarantees on freedom of expression in the Charter of Fundamental Rights of the European Union are basically equivalent to the regulations in the ECHR. Lastly, from the point of view of the ECHR, the ECtHR in its *Bosphorus* decision has clarified that it reserves scrutiny even in cases in which the EU exercises exclusive competence.⁹⁸

4. *Summary – Personal Application as a Mainly Procedural Question, not a Material Question*

The repercussions of the involvement of so many different actors are mainly situated on the procedural level – e.g., who may claim a human rights violation; against whom can a human rights violation be claimed; with whom lies the burden of proof – but not on the material level. It is decisive that States as well as the EU have to comply with human rights obligations and have to refrain from violations of freedom of expression of individuals and online intermediaries alike. Whether this is the case is the subject matter of the next section.

II. *The Scope of the ECHR's Substantive Protection in Light of the French, German and EU Legislation Regulating Online Speech*

While the French legislation is concerned with hate speech on the one hand and disinformation on the other hand, the German and the EU legislation are mainly directed against hate speech and only partly touch upon disinformation. Since the legal rules in question are aimed at the deletion of online speech, we first need to turn to general questions of the application of Article 10 ECHR to the online world (1.). In a second

97 See Art. 6 (2) TEU and also CJEU, Opinion 2/13, 18 December 2014, *Opinion pursuant to Article 218 (11) TFEU*, ECLI:EU:C:2014:2454, para. 153.

98 ECtHR, Judgment (GC), 30 June 2005, *Bosphorus v Ireland*, Application No. 45036/98, para. 153.

step, the material scope of the right to freedom of expression (2.) will be examined. Lastly, the right to receive information (3.) deserves special attention.

1. Freedom of Expression on the Internet – Offline Rules also Apply Online

Although some might argue that in cyberspace ‘code is law’⁹⁹ and that cyberspace exists outside any state’s sovereignty,¹⁰⁰ the ECtHR very early on held that the rules that apply offline, in principle, also apply online.¹⁰¹ At the same time, it understood that these rules need to be applied keeping in mind the peculiarities of the online world.¹⁰² It held

that in the light of its accessibility and its capacity to store and communicate vast amounts of information, the Internet plays an important role in enhancing the public’s access to news and facilitating the dissemination of information in general¹⁰³

and that it ‘provides an unprecedented platform for the exercise of freedom of expression.’¹⁰⁴ The Court also underlined the importance of the Internet for political speech as it

99 Lessig, *Code: And Other Laws of Cyberspace* (1999), 6; Lessig, *Code: And Other Laws of Cyberspace, Version 2.0* (2006), 1.

100 Barlow, A Declaration of the Independence of Cyberspace, Electronic Frontier Foundation, 8 February 1996, <https://www.eff.org/cyberspace-independence> : “Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.”

101 ECtHR, Judgment, 1 July 2008, *Liberty v UK*, Application No. 58243/00, 64 ff.

102 Kettemann and Benedek, ‘Freedom of expression online’ in Susi (ed), *Human Rights, Digital Society and the Law: A Research Companion* (2019), 58 (62).

103 See ECtHR, Judgment, 18 December 2012, *Ahmet Yildirim v Turkey*, Application No. 3111/10, para. 48; ECtHR, Judgments, 10 March 2009, *Times Newspapers Ltd. (Nos. 1 and 2) v The United Kingdom*, Application No. 3002/03 and 23676/03, para. 27; ECtHR, Judgment, 19 January 2016, *Kalda v Estonia*, Application No. 17429/10, para. 44; ECtHR, Judgment, 23 June 2020, *Engels v Russia*, Application No. 61919/16, para. 25; ECtHR, Judgment, 4 December 2018, *Magyar Jeti Zrt v Hungary*, Application No. 11257/16, para. 66.

104 See ECtHR, Judgment, 18 December 2012, *Ahmet Yildirim v Turkey*, Application No. 3111/10, para. 48; and ECtHR, Judgment, 10 March 2009, *Times Newspapers Ltd. (Nos. 1 and 2) v The United Kingdom*, Application No. 3002/03 and 23676/03, para. 27.

has now become one of the principal means by which individuals exercise their right to freedom to receive and impart information and ideas, providing as it does essential tools for participation in activities and discussions concerning political issues and issues of general interest.¹⁰⁵

This very positive view of the internet is contrasted with the Court's understanding that 'the risk of harm posed by content and communications on the Internet to the exercise and enjoyment of human rights and freedoms, particularly the right to respect for private life, is certainly higher than that posed by the press.'¹⁰⁶ Other dangers recognized by the Court are '[d]efamatory and other types of clearly unlawful speech, including hate speech and speech inciting violence [which] can be disseminated like never before, worldwide, in a matter of seconds, and sometimes remain persistently available online.'¹⁰⁷

All in all, the Court approaches the internet in a cautious manner, highlighting its positive aspects for making use of human rights on the one hand and being aware of its dangers for human rights on the other hand. While this seems to be the right approach in general, in the end it remains crucial how the Court finds the right balance between the different rights at stake in this new and still partly uncharted space.

2. *The Material Scope of Freedom of Expression*

Freedom of expression is understood broadly by the ECtHR and

is applicable not only to 'information' or 'ideas' that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector

105 ECtHR, Judgment, 1 December 2015, *Cengiz and others v Turkey*, Application No. 48226/10 and 14027/11, para. 49; ECtHR, Judgment, 18 December 2012, *Ahmet Yildirim v Turkey*, Application No. 3111/10, para. 54; ECtHR, Judgment, 4 December 2018, *Magyar Jeti Zrt v Hungary*, Application No. 11257/16, para. 66.

106 ECtHR, Judgment (GC), 16 June 2015, *Delfi AS v Estonia*, Application No. 64569/09, para. 133; ECtHR, Judgment, 5 May 2011, *Editorial Board of Pravoye Delo and Shtekel v Ukraine*, Application No. 33014/05, para. 63; ECtHR, Judgment, 4 December 2018, *Magyar Jeti Zrt v Hungary*, Application No. 11257/16, para. 66; ECtHR, Judgment, 7 November 2017, *Egill Einarsson v Iceland*, Application No. 24703/15, para. 46.

107 ECtHR, Judgment (GC), 16 June 2015, *Delfi AS v Estonia*, Application No. 64569/09, para. 11.

of the population. Such are the demands of pluralism, tolerance and broadmindedness without which there is no democratic society.¹⁰⁸

Both, value judgments ('opinions' and 'ideas') and factual allegations ('information') are generally protected, no matter whether the factual allegations are true or false.¹⁰⁹ Disinformation is thus protected¹¹⁰ as can be seen in the case *Perinçek v. Switzerland*.¹¹¹ Here, the Court had to decide about a Swiss Court's decision to sentence the Chairman of the Turkish Workers' Party, Doğu Perinçek, for different statements made about Armenian Genocide. Mr. Perinçek inter alia said that 'the allegations of the 'Armenian genocide' are an international lie.' While the genocide is a proven historic fact, the Court nevertheless concluded that Mr. Perinçek's right to freedom of expression had been interfered with and in the end even had been violated.

However, if 'fake news' is connected with hate speech, i.e. 'all forms of expression which spread, incite, promote or justify hatred based on intolerance,'¹¹² e.g. in the case of Holocaust denial, it may not be protected anymore. The ECtHR has 'no doubt that, like any other remark direct-

108 ECtHR, Judgment, 7 December 1976, *Handyside v UK*, Application No. 5493/72, para. 49.

109 Value judgement can neither be "true" nor "false" as there is no way to prove them, ECtHR, Judgment, 8 July 1986, *Lingens v Austria*, Application No. 9815/82, para. 46; ECtHR, Judgment, 29 March 2005, *Ukrainian Media Group v Ukraine*, Application No. 72713/01, para. 41. See also Grabenwarter, *European Convention on Human Rights: Commentary* (2014), Art. 10, mn. 31 with further references.

110 Grabenwarter, *European Convention on Human Rights: Commentary* (2014), Art. 10, mn. 5; Rainey et al., *Jacobs, White, and Ovey: The European Convention on Human Rights* (7th edn. 2017), 490; ECtHR, Judgment, 7 May 2002, *Mc Vicar v United Kingdom*, Application No. 46311/99, para. 87; see also ECtHR, Judgment, 25 July 2019, *Brzezinski v Poland*, Application No. 47542/07, para. 58. But see for a different view Pollicino, 'Judicial Protection of Fundamental Rights in the transition from the world of atoms to the word of bits: The case of freedom of speech' (2019) 25 *Eur Law J*, 155 (158 f.); Kettemann and Benedek, 'Freedom of expression online' in Susi (ed), *Human Rights, Digital Society and the Law: A Research Companion* (2019), 58 (Fn. 39), referring to ECtHR, Decision, 3 June 2014, *Schuman v Poland*. Application No. 52517/13. Here, however, the Court found misinformation to be protected by Article 10 ECHR and did not express itself on neither dis- nor mal-information.

111 ECtHR, Judgment (GC), 15 October 2015, *Pernicek v Switzerland*, Application No. 27510/08.

112 ECtHR, Judgment, 4 December 2003, *Gündüz v Turkey*, Application No. 35071/97, para. 40.

ed against the Convention's underlying values, expressions that seek to spread, incite or justify hatred based on intolerance, including religious intolerance, do not enjoy the protection afforded by Article 10 of the Convention.¹¹³ While this sounds like a very clear statement, the Court is not consequently following this approach. Glorifying terrorism for example is not considered to be hate speech,¹¹⁴ neither was the denial of the Armenian Genocide in *Perinçek v. Switzerland*.¹¹⁵ Equally, in *Kühnen v. Germany*,¹¹⁶ which was about denial of the Holocaust, the Court afforded Article 10 ECHR protection. However, in *Garaudy v. France*, which was also about the denial of the Holocaust, the Court found that Article 10 ECHR does not protect the speech in question.¹¹⁷ In order to avoid such contradictions, hate speech should fall under the general protection of Article 10 ECHR as well. Of course, interferences in such cases will mostly be justified.¹¹⁸

Advertisements, whether political or commercial, are also protected by Article 10 ECHR.¹¹⁹ When dealing with commercial advertisements, State parties enjoy a wide margin of appreciation. The ECtHR only scrutinizes whether a proportionality test was undertaken by national courts but does not carry one out itself.¹²⁰ This however changes in case the advertisement is a political one.¹²¹

113 *Ibid.* also ECtHR, Judgment (GC), 23 September 1994, *Jersild v Denmark*, Application No. 15890/89, para. 35.

114 ECtHR, Judgment, 2 October 2008, *Leroy v France*, Application No. 36109/03.

115 ECtHR, Judgment (GC) 15 October 2015, *Perinçek v Switzerland*, Application No. 27510/08, partly concurring partly dissenting opinion Judge Nußberger.

116 European Commission of Human Rights, Decision, 12 May 1988, *Kühnen v. Federal Republic of Germany*, Application No 12194/86.

117 ECtHR, Decision, 7 July 2003, *Garaudy v France*, Application No. 65831/01.

118 See Schiedermaier, in Pabel and Schmahl (eds), *Internationaler Kommentar zur Europäischen Menschenrechtskonvention* (2010), Art. 10 EMRK, mn. 29 with further references.

119 ECtHR, Judgment, 20 November 1989, *Markt Intern Verlag GmbH and Klaus Beerkann v Germany*, Application No. 10572/83, para. 26; ECtHR, Judgment, 23 June 1994, *Jacobowski v Germany*, Application No.15088/89, para. 25; ECtHR, Judgment, 11 December 2003, *Krone Verlag GmbH & Co KG (No. 3) v Austria*, Application No. 39069/97, paras. 33 ff.; ECtHR, Decision, 23 October 2007, *Brzank v Germany*, Application No. 7969/04; (all misleading advertisements); ECtHR, Judgment, 28 June 2001, *VgT Verein gegen Tierfabriken v Switzerland*, Application No. 24699/94, para. 48, (see Grabenwarter, *European Convention on Human Rights: Commentary* (2014), Art. 10, mn. 19.

120 *Id.*, mn 42.

121 ECtHR, Judgment, 5 March 2009, *Hachette Filipacchi Presse Automobile a Dupuy v France*, Application No. 13353/05, para. 63; ECtHR, Judgment, 28 June 2001,

The French, German, and proposed EU legislation are directed against hate speech, dis- and mal-information and also partly regulate advertisements. While dis- and mal-information as well as advertisements are protected by Article 10 ECHR, the scope of protection is unclear for hate speech. As argued, hate speech should also be protected by the material scope of Article 10 ECHR. Thus, the laws in question interfere with the right to freedom of expression.

3. *Right to Receive Information*

Article 10 ECHR does not only protect the right to express oneself but also the right to receive information from third parties. This may, in principle, also allow users of online intermediaries to challenge the takedown of posts or the blocking of profiles. The ECtHR up until now only had to decide on cases where access to entire platforms had been disabled. Here, the Court held that at least in cases where the applicant was not only passive but also an active user and the speech was political and not (easily) obtainable somewhere else,¹²² the right to receive information had been interfered with. In principle, this approach can be transferred to the deletion of single posts. Since the French, the German, and the proposed EU legislation aim at blocking certain content that shall thus not be received by third parties, they also lead to interferences with the right to receive information.

III. *Freedom of Expression v. Protection of Elections – Justifying the French, German, and EU Legislation Regulating Online Speech*

Neither freedom of expression nor the right to receive information is absolute, interferences may be justified (Article 10 (2) ECHR). States are allowed to interfere with the right to freedom of expression and receive information in order to protect elections as long as this interference is prescribed by law (1.) and done in a proportionate manner (2.).

VgT Verein gegen Tierfabriken v Switzerland, Application No. 24699/94, paras. 69 ff.

122 ECtHR, Judgment, 1 December 2015, *Cengiz and others v Turkey*, Application No. 48226/10 and 14027/11, para. 51; see also ECtHR, Judgment, 18 December 2012, *Abmet Yildirim v Turkey*, Application No. 3111/10; ECtHR, Decision, 11 March 2014, *Akdeniz v Turkey*, Application No. 20877/10.

1. Protection of Elections as a Legitimate Aim Prescribed by Law

The interference must not only be prescribed by law (b.) but also follow a specific and legitimate aim (a.).

a) Protection of Elections as a Legitimate Aim

The ECHR does not expressly provide the protection of elections as a specific aim that allows for interferences with human rights. Article 10 (2) ECHR, however, foresees that the rights of others may serve as a legitimate aim for an interference. Article 3 (1) of the First Optional Protocol to the ECHR provides for such a right as it guarantees a right to free elections. Elections are ‘a characteristic principle of democracy’,¹²³ without them there is no democracy. Thus, the protection of democracy also might serve as a legitimate aim. In addition, Article 10 (2) ECHR refers to a ‘democratic society’. While the limitation clause is not primarily concerned with the legitimate aim but with the standard of proportionality, it nevertheless indirectly shows that the protection of democracy is able to justify interferences with human rights. This is especially true as democracy is the only form of government foreseen by the Convention:¹²⁴

Democracy constitutes a fundamental element of the ‘European public order.’ [T]he Convention establishes a very clear connection between the Convention and democracy by stating that the maintenance and further realisation of human rights and fundamental freedoms are best ensured on the one hand by an effective political democracy and on the other by a common understanding and observance of human rights. [D]emocracy is the only political model contemplated by the Convention and, accordingly, the only one compatible with it.¹²⁵

123 ECtHR, Judgment, 2 March 1987, *Mathieu-Mohin and Clerfayt v Belgium*, Application No. 9267/81, para. 47.

124 ECtHR, Judgment (GC), 13 February 2003, *Refah Partisi (The Welfare Party) and others v Turkey*, Application Nos. 41340/98, 41342/98, 41343/98 and 41344/98, para. 86.

125 ECtHR, Judgment (GC), 16 March 2006, *Zdanoka v Latvia*, Application No. 58278/00, para. 98.

b) Prescribed by Law, especially Foreseeability and Effective Judicial Review

The interference must be prescribed by law. This requirement does not only demand the formal existence of a law but also certain material preconditions, ‘the quality of the law in question,’¹²⁶ namely the accessibility and foreseeability of the domestic law as well as its compatibility with the rule of law.¹²⁷ Blocking of entire websites has been held to be a violation of Article 10 ECHR, *inter alia*, in the cases *Cengiz and others v. Turkey* and *Yildirim v. Turkey*.¹²⁸ These cases are instructive insofar as they highlight that the applicants have to be able to regulate their own conduct according to legal rules and that domestic law must afford a measure of legal protection against arbitrary interference by public authorities with the rights guaranteed by the Convention.¹²⁹ Thus, ‘a legal framework is required, ensuring both tight control over the scope of bans and effective judicial review to prevent any abuse of power.’¹³⁰ This includes that the national

126 ECtHR, Judgment, 1 December 2015, *Cengiz and others v Turkey*, Application No. 48226/10 and 14027/11, para. 59; ECtHR, Judgment, 18 December 2012, *Ahmet Yildirim v Turkey*, Application No. 3111/10, para. 57.

127 *Ibid.*

128 ECtHR, Judgment, 1 December 2015, *Cengiz and others v Turkey*, Application No. 48226/10 and 14027/11; ECtHR, Judgment, 18 December 2012, *Ahmet Yildirim v Turkey*, Application No. 3111/10; ECtHR, Judgment, 23 June 2020, *Bulgakov v Russia*, Application No. 20159/15, paras. 34 ff.; ECtHR, Judgment, 23 June 2020, *Engels v Russia*, Application No. 61919/16, paras. 31 ff.; ECtHR, Judgment, 23 June 2020, *Kharitonov v Russia*, Application No. 10795/14, paras. 43 f.; ECtHR, Judgment, 23 June 2020, *OOO Flavus and others v Russia*, Application No. 12468/15 and 2 others, para. 40–42.

129 ECtHR, Judgment, 18 December 2012, *Ahmet Yildirim v Turkey*, Application No. 3111/10, para. 59; ECtHR, Judgment, 1 December 2015, *Cengiz and others v Turkey*, Application No. 48226/10 and 14027/11, para. 65; see also ECtHR, Judgment, 26 April 1979, *The Sunday Times v UK*, Application No. 6538/74, para. 49; ECtHR, Judgment (GC), 17 February 2004, *Maestri v Italy*, Application No. 39748/98, para. 30; (see, among other authorities, ECtHR, Judgment, 28 June 2001, *VgT Verein gegen Tierfabriken v Switzerland*, Application No. 24699/94, para. 52; ECtHR, Judgment (GC), 16 June 2015, *Delfi AS v Estonia*, Application No. 64569/09, para. 120; ECtHR, Judgment, 15 May 2018, *Unifraun Theatre Productions Limited and Others v Malta*, Application No. 37326/13, para. 78; ECtHR, Judgment, 23 June 2020, *Bulgakov v Russia*, Application No. 20159/15, paras. 35–37; ECtHR, Judgment, 23 June 2020, *Engels v Russia*, Application No. 61919/16, paras. 31 f.

130 ECtHR, Judgment, 18 December 2012, *Ahmet Yildirim v Turkey*, Application No. 3111/10, para. 64; see also ECtHR, Judgment, 1 December 2015, *Cengiz and*

law obligates the national courts to weigh the competing interests at stake and to strike a balance between them.¹³¹ While the laws in question are all laws in a formal manner (or, for the DSA-Draft, will be), it is questionable whether the exact duties of the individuals concerned as well as of the on-line intermediaries are foreseeable (aa.) and whether an effective judicial review exists (bb.).

aa) Foreseeability: What is Manifestly Illegal Content?

The GNEA defines rather precisely its illegal content by referring to well-established national criminal law. The DSA equally refers to other norms as does the Loi Avia, and the definitions and requirements in Loi No. 2018–1202 are very precise. However, the differentiation between illegal content and manifestly illegal content in the DSA-Draft, the GNEA and the Loi Avia has been criticized as being too imprecise.¹³² While the differentiation does not change the duty to take down posts as such, it makes a difference whether a post has to be taken down within 24 hours or within seven days as prescribed by the GNEA and the unconstitutional French Loi Avia. It also makes a difference whether a profile will be suspended – and not only a singular post deleted – if manifestly illegal content is posted on

others v Turkey, Application No. 48226/10 and 14027/11, para. 62; ECtHR, Judgment, 30 April 2019, *Kablis v Russia*, Application Nos. 48310/16 and 59663/17, paras. 67, 80; ECtHR, Judgment, 17 July 2001, *Association Ekin v France*, Application No. 39288/98, para. 58. See also CJEU, Judgment, 27 March 2017, *UPC Telekabel Wien*, Case C-314/12, ECLI:EU:C:2014:192, para. 57, where the CJEU held that “the national procedural rules must provide a possibility for internet users to assert their rights before the court once the implementing measures taken by the internet service provider are known.”

131 ECtHR, Judgment, 18 December 2012, *Ahmet Yildirim v Turkey*, Application No. 3111/10, para. 64.

132 For DSA see Frosio and Geiger, ‘Taking Fundamental Rights seriously in the Digital Services Act’s Platform Liability Regime’ (2020) available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3747756 SSRN, 37; for GNEA see Bassini, ‘Fundamental rights and private enforcement in the digital age’ (2019) 25 *Eur Law J*, 182 (195); Claussen, ‘Fighting hate speech and fake news. The Network Enforcement Act (NetzDG) in Germany in the context of European legislation’ (2018) *Rivista di Diritto dei Media*, 110 (123); Ladeur and Gostomzyk, ‘Das Netzwerkdurchsetzungsgesetz und die Logik der Meinungsfreiheit’ (2017) 21 *K&R*, 390 (391). For the Loi Avia see Conseil Constitutionnel 18.6.2020 – Décision no 2020–801 DC – JORF, n° 0156 du 25/06/2020, Texte 2 sur 181, para. 7.

a frequent basis as foreseen by the DSA-Draft. The difficult differentiation between illegal and manifestly illegal might lead to over-blocking and thus might have ‘a chilling effect’¹³³ on the right of freedom of expression. In order to contravene such an over-blocking, it is necessary that, just as in the GNEA and the DSA-Draft, fines are not imposed for a single failure to block manifestly illegal content but only for systematic failure to do so. Furthermore, fines should be imposed not only for under-blocking but also for over-blocking.¹³⁴

bb) Effective Judicial Review: Some Work to be Done

With regard to effective judicial review, Loi No. 2018–1202 is certainly lawful as only court injunctions lead to a duty to take down a certain post. The other three laws are based on a notice and takedown procedure, which is seen as highly critical *per se* as private parties and not the State decide about the legality or illegality of a specific speech.¹³⁵ While it is true that online intermediaries ‘are less well-placed than courts to consider the lawfulness of comments on their website domains [and that] qualifying speech as hate speech is a very difficult and delicate exercise, not only for domestic courts, but also for the European Court of Human Rights,’¹³⁶

133 See e.g. ECtHR, Judgment, 10 July 2014, *Axel Springer AG v Germany* (No.2), Application No. 48311/10, para. 76.

134 Hong, ‘The German Network Enforcement Act and the Presumption in Favour of Freedom of Speech’, *Verfassungsblog*, 22 January 2018, <https://verfassungsblog.de/the-german-network-enforcement-act-and-the-presumption-in-favour-of-free-dom-of-speech/>.

135 See e.g. Bassini, ‘Fundamental rights and private enforcement in the digital age’ (2019) 25 *Eur Law J*, 182; Helberger, ‘The Political Power of Platforms: How Current Attempts to Regulate Misinformation Amplify Opinion Power’ (2020) 8 *Digital Journalism*, 842; Kalbhenn and Hemmert-Halswick, ‘Der Regierungsentwurf zur Änderung des NetzDG – Vom Compliance-Ansatz zu Designvorgaben’ (2020), *MMR*, 518 (519); Guggenberger, ‘Das Netzwerkdurchsetzungsgesetz – schön gedacht, schlecht gemacht’ (2017) *ZRP*, 98 (100); Lang, ‘Netzwerkdurchsetzungsgesetz und Meinungsfreiheit – Zur Regulierung privater Internet-Intermediäre bei der Bekämpfung von Hassrede’ (2018) 143 *AöR*, 220 (225); UNHCR, OSCE, OAS, AU ‘Joint Declaration on Freedom of Expression and „Fake News, Disinformation and Propaganda’’, FOM. GAL/3/17, 3 March 2017, preambular clause 12.

136 Voorhoof and Lievens, ‘Offensive Online Comments – New ECtHR Judgement’, *ECHR Blog*, 15 February 2016, <https://www.echrblog.com/2016/02/offensive-online-comments-new-ecthr.html>.

one also needs to keep in mind that online intermediaries are making this decision a million times a day.¹³⁷ This is due to their adherence to community standards on the one hand and due to their liability for illegal content after they have been notified about it on the other hand.

While online intermediaries are able to make such decisions, they need to be supervised by courts. The original GNEA neither foresaw any effective judicial review nor installed an internal dispute settlement mechanism. The Loi Avia at least installs an internal dispute settlement mechanism. While German courts have ordered posts to be reinstated and profiles to be unblocked,¹³⁸ this right is based on the private law contract between the online intermediary and the user, which is only informed by the right to freedom of expression.¹³⁹ This is a rather weak remedy that has partly been fortified by the 2021 bill amending the GNEA through providing for out of court settlements.¹⁴⁰ Furthermore, the original GNEA already made it easier for legal processing to take place by obligating online intermediaries to name a person authorized to receive service (§ 5 GNEA). Before that, the absence of such a specific rule has led to factual difficulties in starting civil court proceedings against online intermediaries. Still, even the amended GNEA does not stipulate any specific legal remedies in case a post or a user (profile) has been blocked or deleted.

While the original GNEA was deficient but has been improved in 2021, the DSA-Draft is much more developed. It explicitly calls for different forms of dispute settlement mechanisms and installs an elaborate multi-step system in order to make sure that users may take redress against the deletion of posts and suspension of profiles. Article 18 (1) DSA-Draft explicitly states that national remedies are not prejudiced by the out-of-court settlements. Such proceedings are made much easier by the online intermediaries' duty to name a legal representative in each member state (Article 11 DSA-Draft). They may, *inter alia*, have to receive service for the on-

137 Lang, 'Netzwerkdurchsetzungsgesetz und Meinungsfreiheit – Zur Regulierung privater Internet-Intermediäre bei der Bekämpfung von Hassrede' (2018) 143 *AöR*, 220 (239).

138 Kettemann and Tiedeke, 'Back up: can users sue platforms to reinstate deleted content?' (2020) 9 *Internet Policy Review*, 1 (10 f.); Peukert, 'Gewährleistung der Meinungs- und Informationsfreiheit in sozialen Netzwerken. Vorschlag für eine Ergänzung des NetzDG um sog. Put-back-Verfahren' (2018) *MMR*, 572.

139 XY; see Kalbhenn and Hemmert-Halswick, 'Der Regierungsentwurf zur Änderung des NetzDG – Vom Compliance-Ansatz zu Designvorgaben' (2020), *MMR*, 518 (519).

140 Gesetz zur Änderung des Netzwerkdurchsetzungsgesetzes vom 03. Juni 2021, BGBl Jahrgang 2021 Teil 1 Nr. 29, § 3c.

line intermediary and may even be held individually liable (Article 11 (3) DSA-Draft). Furthermore, with regard to the duty to balance different interests, the DSA-Draft states in Recital 105 that it should be interpreted and applied in accordance with those fundamental rights, including the freedom of expression.¹⁴¹ Lastly, very large online platforms are obligated to take into account the effect of their actions on freedom of expression (Article 26 (1) lit b. DSA-Draft). Such provisions are missing in the national laws and should be explicitly added.

cc) Summary: DSA-Draft as a Model for National Legislation

While there is some doubt with regard to the foreseeability of the laws since they use a differentiation between illegality and manifest illegality, such doubts can be overcome by imposing fines not for single failures to block manifestly illegal content but only for systematic failure to do so and by instituting internal review procedures and strengthening judicial review. Here, the DSA-Draft is a model for national legislation.

2. *The Right Balance between Protecting Elections and Ensuring Freedom of Expression*

Lastly, the proportionality test limits the power of the public authorities to interfere with human rights by requiring the public authority to use the least intrusive means and to balance the competing interests.¹⁴²

a) Different Rights and Interests to be taken into Account

For the balancing act, different rights and interests have to be taken into account, *inter alia* whether the act in question is a statement of fact or a

141 See also Article 1 (2) DSA-Draft.

142 ECtHR, Decision, 29 June 2006, *Weber and Saravia v Germany*, Application No. 54934/00, 106; see ECtHR, Judgment (GC), 7 February 2012, *Axel Springer AG v Germany*, Application No. 39954/08, para. 84; and ECtHR, Judgment (GC), *Von Hannover v Germany* (no. 2), 7 February 2012, Application Nos. 40660/08 and 40641/08, para. 106 and the cases cited therein.

value judgment,¹⁴³ the form of the expression,¹⁴⁴ whether it is a commercial speech act or political speech act,¹⁴⁵ the function and context of the expression, its place and its time,¹⁴⁶ its objective,¹⁴⁷ its object,¹⁴⁸ the severity of the state's interference¹⁴⁹ as well as the human rights of other non-state actors involved.¹⁵⁰ In essence, 'the Court consistently gives a higher level of protection to publications and speech which contribute towards social and political debate, criticism, and information – in the broadest sense.'¹⁵¹

b) Dis- and Mal-Information and Hate Speech

Dis- and mal-information may fall in the category of commercial speech acts if they are created not for political purposes but in order to generate traffic that in turn will lead to revenue through advertisements.¹⁵² Com-

143 ECtHR, Judgment, 8 July 1986, *Lingens v Austria*, Application No. 9815/82, para. 46.

144 ECtHR, Judgment, 10 January 2013, *Ashby Donald and others v France*, Application No. 36769/08, para. 39; ECtHR, Decision, 19 February 2013, *Neij and Sunde Kolmisoppi v Sweden*, Application No. 40397/12; ECtHR, Judgment, 5 March 2009, *Hachette Filipacchi Presse Automobile a Dupuy v France*, Application No. 13353/05, para. 63; ECtHR, Judgment, 28 June 2001, *VgT Verein gegen Tierfabriken v Switzerland*, Application No. 24699/94, paras. 69 ff.

145 ECtHR, Judgment, 26 April 1979, *Sunday Times v The United Kingdom*, Application No. 6538/74; ECtHR, Judgment, 8 July 1986, *Lingens v Austria*, Application No. 9815/82.

146 ECtHR, Judgment (GC), 15 October 2015, *Pernicek v Switzerland*, Application No. 27510/08, paras. 242 ff.

147 'This is based on the idea that a free political debate is of fundamental importance for a democracy.', Grabenwarter, *European Convention on Human Rights: Commentary* (2014), Art. 10, mn. 36.

148 ECtHR, Judgment, 11 April 2006, *Brasilier v France*, Application No. 71343/01, para. 41; ECtHR, Judgment, 21 February 2012, *Tusalp v Turkey*, Application Nos. 32131/08 and 41617/08, para. 45; ECtHR, Judgment, 23 April 1992, *Castells v Spain*, Application No. 11798/85, para. 46; Grabenwarter, *European Convention on Human Rights: Commentary* (2014), Art. 10, mn. 36 with further reference.

149 ECtHR, Judgment (GC), 15 October 2015, *Pernicek v Switzerland*, Application No. 27510/08, paras. 272 f.

150 Rainey et al., *Jacobs, White, and Ovey: The European Convention on Human Rights* (7th edn. 2017), 486 f.

151 *Id.*, 428; ECtHR, Judgment, 2 October 2008, *Leroy v France*, Application No. 36109/03, para. 41: "debate of public interest".

152 See e.g. Hughes and Waismel-Manor, 'The Macedonian Fake News Industry and the 2016 US Election' (2021) 54 *Political Science & Politics*, 19.

mercial speech acts are afforded less protection; the margin of appreciation is wider. But dis- and mal-information may also be political acts. While information as well as value judgments are protected, false information or misleading information is less protected than value judgments and correct information, as sufficient steps need to be taken to verify the truth.¹⁵³

In cases of hate speech, even if the Court considered that hate speech fell within the scope of application of Article 10 ECHR,¹⁵⁴ the States' interference was always justified.¹⁵⁵

c) The Online Speech Case Law of the ECtHR

In the four cases that involved online intermediaries and the takedown of (defamatory) speech and possible Article 10 ECHR violations, the ECtHR in principle applied its offline jurisprudence to the online world. In none of the cases could the online intermediary in question be classified as a social media company. Rather, users' comments on news websites and private blogs¹⁵⁶ were at question, and the ECtHR understood the sites to be publishers.¹⁵⁷ Nevertheless, these cases provide decisive guidance in how the ECtHR might decide cases involving social media companies and the deletion of speech. This is especially true since the Court in 2020 had to decide a case in which the applicants contended that they had suffered discrimination on the grounds of their sexual orientation because the public authorities refused to launch a pre-trial investigation into hateful comments left on the first applicant's Facebook page. The Court explicitly 'reject[ed] the Government's argument that comments on Facebook are less dangerous than those on the Internet news portals.'¹⁵⁸

153 ECtHR, Judgment, 14 February 2008, *Rumyna Ivanova v Bulgaria*, Application No. 36207/03, paras. 64 ff.

154 See above p. 191.

155 ECtHR, Judgment (GC), 16 June 2015, *Delfi AS v Estonia*, Application No. 64569/09; ECtHR, Judgment, 10 July 2008, *Soulas and others v France*, Application No. 15948/03, paras. 43; 47; ECtHR, Judgment, 13 September 2005, *I.A. v Turkey*, Application No. 42571/98, paras. 29, 32.

156 ECtHR, Decision, 7 February 2017, Application No. 74742/14, *Pihl v Sweden*.

157 ECtHR, Judgment (GC), 16 June 2015, *Delfi AS v Estonia*, Application No. 64569/09, para. 129. But see ECtHR, Judgment (GC), 16 June 2015, *Delfi AS v Estonia*, Application No. 64569/09, dissenting opinion of Judges Sajó and Tsotsoria, para. 27.

158 ECtHR, Judgment, 14 January 2020, *Beizara and Levickas v Lithuania*, Application No. 41288/15, para. 127.

aa) *Delfi v. Estonia* (2015) – Demanding a Notice and Takedown Procedure

In the first case, *Delfi v. Estonia*, the ECtHR held that States may hold providers of a professionally managed and commercial news portal liable for certain posts, in this case '[d]efamatory and other types of clearly unlawful speech, including hate speech and speech inciting violence',¹⁵⁹ without violating Article 10 ECHR. The news portal Delfi was asked by the victim of threatening and offensive comments to take down the posts and pay damages. While Delfi took down the posts, it refused to pay any damages. In the ensuing civil action, Delfi was held liable and ordered to pay damages. Important aspects in the balancing test include that while the company immediately deleted the incriminated comments after having been notified about them, the comments were still six weeks online; that the comments were 'of a clearly unlawful nature'¹⁶⁰ by being qualified as 'hate speech or incitements to violence';¹⁶¹ that information posted on the Internet will remain public and 'accessible forever';¹⁶² that Delfi created the original content as well as the electronic infrastructure for the posts;¹⁶³ and that the portal allowed the authors to remain anonymous. The Court also took into consideration that the compensation Delfi was ordered to pay, 320 €, was rather low.¹⁶⁴ With this decision, the ECtHR clarified that online intermediaries' liability for users' speech interferes with Article 10 ECHR but will be justified in cases of hate speech.

The Court was highly criticized for this judgment, which, in the opinion of the critics, did not do enough to protect freedom of expression.¹⁶⁵ One main point of critique was that contrary to Article 15 of the EU's E-Commerce Directive, which is the blueprint for Article 5 DSA-Draft and excludes any online intermediaries' duty to generally monitor content

159 ECtHR, Judgment (GC), 16 June 2015, *Delfi AS v Estonia*, Application No. 64569/09, para. 110.

160 *Id.*, para. 140.

161 *Ibid.*

162 *Id.*, para. 92.

163 *Id.*, para. 116.

164 *Id.*, para. 160.

165 See van der Sloot 'The Practical and Theoretical Problems with 'Balancing': Delfi, Coty and the Redundancy of the Human Rights Framework' (2016) 23 *Maastricht Journal of European and Comparative Law*, 439; Brunner, 'The Liability of an Online Intermediary for Third Party Content: The Watchdog Becomes the Monitor: Intermediary Liability after Delfi v Estonia' (2016) 16 *Human Rights Law Review*, 163.

and instead establishes a ‘notice and takedown procedure’, the decision can compel online intermediaries to use automatic filter technology to monitor online speech. The use of such filters, however, is said to have a chilling effect on freedom of expression as it will lead to over-blocking and risks undermining freedom of speech.¹⁶⁶ Consequently, none of the laws in question require an automated filtering system to take down illegal posts before notice.¹⁶⁷

bb) *MTE and Index.hu ZRT v. Hungary* (2016) – But not in all Cases

In contrast to *Delfi*, in its next case on online intermediaries’ liability for speech of third parties, *MTE and Index.hu ZRT v. Hungary*, the ECtHR found a violation of Article 10 ECHR because Hungarian courts held two online intermediaries liable for defamatory speech of third parties. While not explicitly deviating from the standards developed in *Delfi*, the Court clearly supported a more liberal view with regard to freedom of speech.

The Court, *inter alia*, underlined that ‘the notice-and-takedown-system could function in many cases as an appropriate tool for balancing the rights and interests of all those involved’.¹⁶⁸ Contrary to *Delfi*, it was a legal person that sued the applicants;¹⁶⁹ the applicant MTE was a ‘non-profit self-regulatory association of Internet service providers’ without commercial interests; the applicants were not notified of the comments but were sued directly – and took down the comments after they learned about the lawsuit; and lastly, and most importantly, the posts in the *MTE* and *Index.hu* were ‘devoid of [their] pivotal elements of hate speech and incitement of violence’¹⁷⁰ and thus did not constitute clearly unlawful speech.

166 Voorhoof, ‘The Court’s subtle approach for online media platform’s liability for user-generated content since the ‘Delfi Oracle’’, Strasbourg Observers, 10 April 2020, <https://strasbourgobservers.com/2020/04/10/the-courts-subtle-approach-of-online-media-platforms-liability-for-user-generated-content-since-the-delfi-oracle/>. See also CJEU, Judgment, 16 February 2012, *SABAM v. Netlog NV*, Case C-360/10, ECLI: EU:C:2012:85.

167 For a critique of automated decision making see Frosio and Geiger, ‘Taking Fundamental Rights seriously in the Digital Services Act’s Platform Liability Regime’ (2020) available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3747756 SSRN, 26.

168 ECtHR, Judgment, 2 February 2016, *MTE v Hungary*, Application No. 22947/13, para. 91.

169 *Id.*, para. 83.

170 *Id.*, paras. 64, 75.

The Court even held that the Internet's communication style might be a bit rougher: 'For the Court, the expressions used in the comments, albeit belonging to a low register of style, are common in communication on many Internet portals'.¹⁷¹ Further, the topic of the comments was of public interest.¹⁷² Lastly, the Hungarian judgment in question was too far reaching, not well tailored and 'effectively preclude[d] the balancing between the competing rights according to the criteria laid down in the Court's case law'¹⁷³ as it held that defamatory content must not appear at all – which created 'foreseeable negative consequences' for freedom of expression.¹⁷⁴

cc) *Pihl v. Sweden* (2017) – Limited Liability for Small Blogs

In the next case, *Pihl v. Sweden*, the Court strengthened its *MTE* approach. Again, the case did not concern hate speech but 'only' defamatory speech, in the form of an online comment, which had been published anonymously on a blog. The subject of the comments, Mr. Pihl, raised an unsuccessful civil claim against a small non-profit association responsible for the blog. He claimed that it should be held liable for the comment. The Court rejected this claim and thus again argued in favour of freedom of expression. The decisive factors were that the blog had a rather small audience and was of a non-commercial nature,¹⁷⁵ that the post had been taken down the day after the applicant had made a complaint (the blog even apologized for the comments), and the comments had only been online 'for about nine days in total'.¹⁷⁶ *Pihl* thus privileges small blogs that are run on a non-profit basis. Here, the content neither has to be pre-monitored nor does an effective notice and takedown procedure need to be installed.¹⁷⁷

171 *Id.*, para. 77.

172 *Id.*, para. 72.

173 *Id.*, para. 89.

174 *Id.*, para. 86.

175 ECtHR, Decision, 7 February 2017, *Pihl v Sweden*, Application No. 74742/14, para. 35; see also ECtHR, Decision, 19 September 2017, *Tamiz v UK*, Application No. 3877/14, para. 85.

176 ECtHR, Decision, 7 February 2017, *Pihl v Sweden*, Application No. 74742/14, para. 32.

177 Voorhof, 'Pihl v. Sweden: non-profit blog operator is not liable for defamatory users' comments in case of prompt removal upon notice', Strasbourg Observers, 20 March 2017, <https://strasbourgobservers.com/2017/03/20/pihl-v-sweden-non-p>

dd) *Høiness v. Norway* (2019) – Reiteration of the Court’s Cautious Approach

The last case in this line is *Høiness v. Norway*, which concerned sexist comments on a news portal below the threshold of defamation and hate speech. Comparable to *Pihl*, Ms. Høiness was the victim of the comments and applied to the ECtHR as the national courts did not help her. As in *Pihl*, the ECtHR did not find a violation of the ECHR and thus argued again in favor of freedom of expression. It reiterated that it follows a cautious approach in limiting freedom of expression as long as the speech in question does not amount to hate speech or incitement to violence.¹⁷⁸

d) Application of the Court’s Case Law: Has the Right Balance Been Found?

Applying this case law to regulations at hand, one first has to highlight that while the ECtHR accepts automatic filtering system, at least for commercial news portals and in the case of hate speech, none of the laws obligate online intermediaries to use such systems. Here, the Court seems to be more restrictive than the legislator. Second, the Court also takes a very strict stance against hate speech and consequently allows for national rules that obligate online intermediaries to take down hate speech.¹⁷⁹ Third, the Court is cautious in allowing States to hold online intermediaries liable for illegal speech that falls below the threshold of hate speech.¹⁸⁰ Fourth, while this jurisprudence applies to online intermediaries, the Court differentiates between different intermediaries: commercial news portals are under more obligations, non-commercial news portals and small blogs¹⁸¹ carry less obligations than commercial news portals and blogs with a

profit-blog-operator-is-not-liable-for-defamatory-users-comments-in-case-of-prompt-removal-upon-notice/.

178 ECtHR, Judgment, 19 March 2019, *Høiness v Norway*, Application No. 43624/14, para. 69.

179 Brings-Wiesen and Damberg-Jänsch, ‘Der *free flow of information* im Wandel des digitalen Zeitalters: Eine Bestandsaufnahme der internetbezogenen Rechtsprechung des EGMR zu Art. 10 EMRK’ (2020) 84 *UFITA*, 284 (310 ff.).

180 See e.g. ECtHR, Judgment (GC), 15 October 2015, *Pernicek v Switzerland*, Application No. 27510/08; ECtHR, Judgment, 2 February 2016, *MTE v Hungary*, Application No. 22947/13.

181 E.g. ECtHR, Decision, 19 September 2017, *Tamiz v UK*, Application No. 3877/14, para. 85; ECtHR, Decision, 7 February 2017, *Pihl v Sweden*, Application

larger audience. Thus, ‘the greater the degree of editorial control over and entrepreneurial interest in the data in question, the more likely it is that the court will find that the defences are not available.’¹⁸² The Court, however, has not yet decided about online intermediaries that do not provide content themselves, like Facebook, YouTube, Instagram etc.¹⁸³ These online intermediaries are very large, have a very high commercial interest and possess editorial control via the algorithms that decide which content the user will see.¹⁸⁴ This, together with the Court’s pronouncement that comments on platforms like Facebook are not less dangerous than those on the Internet news portals¹⁸⁵ speaks in favor of applying the depicted Court’s jurisprudence, at least generally, to those service providers that the DSA-Draft calls very large online platforms.¹⁸⁶ Fifth, the content and the context of the speech in question matters.¹⁸⁷ While monitoring obligations

No. 74742/14, para. 31; ECtHR, Judgment, 2 February 2016, *MTE v Hungary*, Application No. 22947/13, para. 86.

- 182 Proops, ‘Comment is (not) free – E-Commerce back in the limelight’, Panopticon, 22 June 2015, <https://panopticonblog.com/2015/06/22/comment-is-not-free-e-commerce-back-in-the-limelight/>.
- 183 But see ECtHR, communicated 24 May 2019, *Glubkov v Russia*, Application No. 42633/18, and ECtHR, communicated 9 January 2018, *Sanchez v France*, Application No. 45581/15, both communications have not yet been decided.
- 184 Two referrals to the CJEU have asked to clarify whether YouTube is neutral, i.e. “mere technical, automatic and passive” (CJEU, Judgment, 23 March 2010, *Google France SARL, Google Inc. v Louis Vuitton Malletier*, Joint Cases C-236/08 to C-238/08, ECLI:EU:C:2010:159, paras.42, 113.). In the sense of Art. 14 e-commerce directive: Opinion of Advocate General Saugmandsgaard Øe, 16 July 2020, *LF v Google LLC, YouTube Inc, YouTube LLC, Google Germany GmbH*, C-682/18, ECLI:EU:C:2020:586; request for a preliminary ruling from the Oberster Gerichtshof (Austria), 1 July 2019, *Puls 4 TV GmbH & Co KG v. YouTube LLC and Google Austria GmbH*, C-500/19.
- 185 ECtHR, Judgment, 14 January 2020, *Beizara and Levickas v Lithuania*, Application No. 41288/15, par. 127.
- 186 See also CJEU, Judgment, 3 October 2019, *Glawischnig-Piesczek v Facebook Ireland*, Case C-18/18, ECLI:EU:C:2019:821, paras. 19, 53, which left out the question of fundamental rights in its preliminary ruling and thus does not play a role in our context. It however showed that the CJEU allows for a national Court injunction to seek and identify identical as well as equivalent posts to the information that has been characterised as illegal – because of its defamatory nature – although this means that automated filters need to be used.
- 187 ECtHR, Judgment (GC), 15 October 2015, *Pernicek v Switzerland*, Application No. 27510/08, paras. 228, 239, 242 ff; ECtHR, Judgment (GC), 16 June 2015, *Del-fi AS v Estonia*, Application No. 64569/09, paras. 144 ff; ECtHR, Judgment, 2 February 2016, *MTE v Hungary*, Application No. 22947/13, paras. 72 ff; ECtHR, Decision, 7 February 2017, *Pihl v Sweden*, Application No. 74742/14, para. 30; see

for hate speech for news portals do not violate Article 10 ECHR, other forms of illegal speech only allow for liability of online intermediaries under specific circumstances. The Court also takes into account whether the topic of the comments is of public interest or not.¹⁸⁸ Sixth, the reaction time and the measures applied by the company in order to remove a defamatory comment play a role in the balancing act.¹⁸⁹ Seventh, a proper balancing between the competing rights involved has to take place.¹⁹⁰ Eighth, and lastly, the liability of the actual authors of the comments as an alternative to the intermediary's liability, and the consequences of the domestic proceedings for the company need to be considered.¹⁹¹

The essence of the ECtHR jurisprudence is thus that a domestic law that holds a content provider of a certain size and with commercial interests liable for third party postings that amount to hate speech and incitement to violence does not violate Article 10 of the ECtHR. Illegal posts that fall below that threshold in principle need to be taken down without delay on receiving constructive knowledge of their existence in order to avoid liability. Certain conditions, however, apply.

Taking all these points into consideration, the GNEA and the DSA-Draft rules that apply to large online intermediaries that have a large commercial motivation and obligate them only to take down illegal con-

also Lauber-Rönsberg 'Persönlichkeitsschutz in der EMRK und im EU-Recht – § 57. Europäische Menschenrechtskonvention' in Götting et al. (eds), *Handbuch des Persönlichkeitsrechts* (2019), 1197 (mn. 87).

188 ECtHR, Judgment (GC), 15 October 2015, *Pernicek v Switzerland*, Application No. 27510/08, paras. 197, 230, 241; ECtHR, Judgment, 2 February 2016, *MTE v Hungary*, Application No. 22947/13, para. 72; see also Lauber-Rönsberg 'Persönlichkeitsschutz in der EMRK und im EU-Recht – § 57. Europäische Menschenrechtskonvention' in Götting et al. (eds), *Handbuch des Persönlichkeitsrechts* (2019), 1197 (mn. 46 ff.).

189 ECtHR, Judgment (GC), 16 June 2015, *Delfi AS v Estonia*, Application No. 64569/09, paras. 152 ff.; ECtHR, Judgment, 2 February 2016, *MTE v Hungary*, Application No. 22947/13, paras. 80 ff; ECtHR, Decision, 7 February 2017, *Pihl v Sweden*, Application No. 74742/14, para. 32.

190 ECtHR, Judgment (GC), 7 February 2012, *Von Hannover v Germany* (no. 2), Application Nos. 40660/08 and 40641/08, para. 106; ECtHR, Judgment (GC), 16 June 2015, *Delfi AS v Estonia*, Application No. 64569/09, para. 139; ECtHR, Judgment, 19 March 2019, *Høiness v Norway*, Application No. 43624/14, para. 65.

191 ECtHR, Decision, 7 February 2017, *Pihl v Sweden*, Application No. 74742/14, para. 28; see also ECtHR, Judgment, 19 March 2019, *Høiness v Norway*, Application No. 43624/14, para. 67.

tent¹⁹² – not harmful content or unwanted content – are in principle proportionate. This is especially true with regard to hate speech. The laws in question, however, should clarify that online intermediaries have to take into consideration the importance of freedom of expression like the DSA-Draft already does. Highly problematic was that the GNEA foresaw not even out of court remedies against the deletion of posts and users profiles by social media companies, leading to possible over-blocking and thus to a chilling effect of the GNEA on freedom of expression. This has partly been rectified by the 2021 amendment. In its former version, however, the GNEA seemed not to be in conformity with the ECHR.¹⁹³ Recognizing a freedom to receive information claim would help against over-blocking as would a fine against over-blocking, and not only under-blocking.¹⁹⁴ The Loi Avia was also not formulated in a way that would stop over-blocking – one of the reasons it was declared unconstitutional. Another reason was the highly problematic strict time frame, which constitutes one of the major differences to the GNEA.¹⁹⁵ The Loi Avia has a chilling effect on free speech that is out of balance. The Loi 2018–1202 on the other hand, while directed against speech that is in principle not illegal but wrong, holds up to the Court's requirements, especially because it is so narrowly construed.

192 See Wischmeyer, 'Making social media an instrument of democracy' (2019) 25 *Eur Law J*, 169 (176), who argues that these takedowns are marginal compared to those based on the "community standards."

193 Claussen, 'Fighting hate speech and fake news. The Network Enforcement Act (NetzDG) in Germany in the context of European legislation' (2018) *Rivista di Diritto dei Media*, 110 (124 ff.); Gersdorf, 'Hate Speech in sozialen Netzwerken – Verfassungswidrigkeit des NetzDG-Entwurfs und grundrechtliche Einordnung der Anbieter sozialer Netzwerke', (2017) *MMR*, 439 (446).

194 Hong, 'The German Network Enforcement Act and the Presumption in Favour of Freedom of Speech', *Verfassungsblog*, 22 January 2018, <https://verfassungsblog.de/the-german-network-enforcement-act-and-the-presumption-in-favour-of-free-dom-of-speech/>.

195 See also CoE Committee of Ministers, *Recommendation to member States on the roles and responsibilities of internet intermediaries*, 7 March 2018, CM/Rec(2018)2, para. 1.3.7.: 'State authorities may hold intermediaries co-responsible with respect to content that they store if they do not act expeditiously to restrict access to content or services as soon as they become aware of their illegal nature, including through notice-based procedures. State authorities should ensure that notice-based procedures are not designed in a manner that incentivises the take-down of legal content, for example due to inappropriately short timeframes'.

IV. Conclusion: Regulating Online Intermediaries while Ensuring Freedom of Expression

Human rights law ensures freedom of expression of individuals as well as of online intermediaries. At the same time, it allows for certain interferences in order to protect democracy. As long as the regulation is proportionate, online intermediaries may be obligated to counter “fake news” and hate speech, stop the manipulation and censorship of its users and break up their echo chambers and filter bubbles. The Loi Avia does not meet the ECHR’s standard. This is different for the other three laws. While the original GNEA was problematic, the amended versions seems to be in conformity with the ECHR. Also, the proposed DSA-Draft and the French Loi 2018–1202 – which is well balanced because it restricts its negative effects on freedom of speech to the three months before elections – are in conformity with the ECHR. These are also the laws that protect elections against manipulation via online tools. In order for democracy to survive and thrive, it needs to be protected – as do human rights, especially the right to freedom of expression. Neither can live without the other as democracy and human rights are two sides of the same coin. The preamble’s understanding, that human rights are ‘the foundation of justice and peace in the world and are best maintained on the one hand by an effective political democracy and on the other by a common understanding and observance of the Human Rights upon which they depend’, is as true today as it was in 1950.

Bibliography

- Akandji-Kombe, Jean-François: Positive Obligations under the European Convention on Human Rights (2007), 14 ff.
- Article 19: Responding to ‘hate speech’: Comparative overview of six EU countries (2018), https://www.article19.org/wp-content/uploads/2018/03/ECA-hate-speech-Compilation-report_March-2018.pdf.
- Baade, Björnstjern: Fake News and International Law, EJIL 2018, 1357 ff.
- Bárd, Petra: The Hungarian “Lex NGO” before the CJEU: Calling an Abuse of State Power by its Name, Verfassungsblog, 27 January 2020, <https://verfassungsblog.de/the-hungarian-lex-ngo-before-the-cjeu-calling-an-abuse-of-state-power-by-its-name/>.
- Barlow, John Perry: A Declaration of the Independence of Cyberspace, Electronic Frontier Foundation, 8 February 1996, <https://www.eff.org/cyberspace-independence>.

- Bassini, Marco: Fundamental rights and private enforcement in the digital age, *Eur. Law J.* 2019, 182 ff.
- BBC News: Cambridge Analytica ‘not involved’ in Brexit referendum, says watchdog, 7 October 2020, <https://www.bbc.com/news/uk-politics-54457407>.
- Blake, William: Auguries of Innocence, *The Pickering Manuscript* (1807), www.blakearchive.org/copy/bb126.1?descId=bb126.1.ms.15.
- Brattberg, Erik/Maurer, Tim: Russian Election Interference – Europe’s Counter to Fake News and Cyber Attacks, *Carnegie Endowment for International Peace* 2018, https://carnegieendowment.org/files/CP_333_BrattbergMaurer_Russia_Elections_Interference_FINAL.pdf.
- Brings-Wiesen, Tobias/ Damberg-Jänsch, Alicia: *Der free flow of information* im Wandel des digitalen Zeitalters: Eine Bestandsaufnahme der internetbezogenen Rechtsprechung des EGMR zu Art. 10 EMRK, *UFITA* 2020, 284 ff.
- Brunner, Lisl: The Liability of an Online Intermediary for Third Party Content: The Watchdog Becomes the Monitor: Intermediary Liability after *Delfi v Estonia*, *Human Rights Law Review* 2016, 163 ff.
- Bubeck, Johannes/Jäger, Kai/Marinov, Nikolay/Nanni, Federico: Why Do States Intervene in the Elections of Others? The Role of Incumbent–Opposition Divisions, *British Journal of Political Science* 2020, 1 ff.
- Cardenal, Juan Pablo/Kucharczyk, Jacek/Mesežnikov, Grigorij/Pleschlová Gabriela: *Sharp power: rising authoritarian influence* (2017).
- Claussen, Victor: Fighting hate speech and fake news. The Network Enforcement Act (NetzDG) in Germany in the context of European legislation, *Rivista di Diritto dei Media* 2018, 110 ff.
- DCMSC: Disinformation and ‘fake news’: Interim Report, HC 363, 29 July 2018, para. 162 <https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/36302.htm>.
- DeConde, Alexander: Washington’s Farewell, the French Alliance, and the Election of 1796, *The Mississippi Valley Historical Review* 1957, 641 ff.
- Deutscher Bundestag: Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Dr. André Hahn, Gökay Akbulut, weiterer Abgeordneter und der Fraktion DIE LINKE.– Drucksache 19/26017 -Straftaten gegen Amts- und Mandatsträger, Drucksache 19/26419, 03 February 2021.
- Engle, Eric: Third Party Effect of Fundamental Rights (Drittwirkung), *Hanse Law Review* 2009, 165 ff.
- Frosio, Giancarlo/Geiger, Christophe: Taking Fundamental Rights seriously in the Digital Services Act’s Platform Liability Regime (2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3747756.
- Funke, David/ Flamini, Daniela: A guide to anti-misinformation actions around the world, *Poynter* 2018, <https://www.poynter.org/ifcn/anti-misinformation-actions/>.

- Fuster, Gloria González/Scherrer, Amandine: Big data and smart devices and their impact on privacy, Directorate-General for Internal Policies of the Union Study (2015), [http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536455/IPO_L_STU\(2015\)536455_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536455/IPO_L_STU(2015)536455_EN.pdf).
- Gehrke, Laurenz: UK probe finds no evidence that Cambridge Analytica misused data to influence Brexit, Politico, 7 October 2020, <https://www.politico.eu/article/no-evidence-that-cambridge-analytica-misused-data-to-influence-brexit-report/>.
- Gersdorf, Hubertus: Hate Speech in sozialen Netzwerken – Verfassungswidrigkeit des NetzDG-Entwurfs und grundrechtliche Einordnung der Anbieter sozialer Netzwerke, MMR 2017, 439 ff.
- Goldhill, Olivia: A 'big data' firm sells Cambridge Analytica's methods to global politicians, documents show, Quartz, 14 August 2019, <https://qz.com/1666776/data-firm-idea-uses-cambridge-analytica-methods-to-target-voters/>.
- Gorodnichenko, Yuriy/Pham, Tho/Talavera, Oleksandr: Social Media, Sentiment and Public Opinions: Evidence from #Brexit and #Uselection, NBER Working Paper No. 24631, May 2018.
- Grabenwarter, Christoph: European Convention on Human Rights: Commentary (2014)Grassegger, Hannes/Krogerus, Mikael: Cambridge Analytica / Big data and the Future of Democracy: The Matrix world behind the Brexit and the US Elections, Diplomat Magazine, 5 March 2017, www.diplomatmagazine.nl/2018/03/22/cambridge-analytica-big-data-and-the-future-of-democracy-the-matrix-world-behind-the-brexit-and-the-us-elections/.
- Guggenberger, Nikolaus: Das Netzwerkdurchsetzungsgesetz – schön gedacht, schlecht gemacht, ZRP 2017, 98 ff.
- Haciyakupoglu, Gulizar/Hui, Jennifer Yang/ Suguna, V.S./Leong, Dymples/Bin Abdul Rahman, Muhammad Faizal: Policy Report Countering Fake News – A Survey of Recent Global Initiatives, Rajaratnam School of International Studies (2018), https://www.rsis.edu.sg/wp-content/uploads/2018/03/PR180307_Countering-Fake-News.pdf.
- Helberger, Natali: The Political Power of Platforms: How Current Attempts to Regulate Misinformation Amplify Opinion Power, Digital Journalism 2020, 842 ff.
- Hong, Mathias: The German Network Enforcement Act and the Presumption in Favour of Freedom of Speech, Verfassungsblog, 22 January 2018, <https://verfassungsblog.de/the-german-network-enforcement-act-and-the-presumption-in-favour-of-freedom-of-speech/>.
- Hughes, Heather/Waismel-Manor, Israel: The Macedonian Fake News Industry and the 2016 US Election, Political Science & Politics 2021, 19 ff.
- Inter-Parliamentary Union: Inter-Parliamentary Council at its 154th session in Paris. Declaration on Criteria for Free and Fair Elections, 26 March 1994, <http://archive.ipu.org/cnl-e/154-free.htm>.
- International Press Institute: New 'fake news' law stifles independent reporting in Russia on Covid-19, 8 May 2020, <https://ipi.media/new-fake-news-law-stifles-independent-reporting-in-russia-on-covid-19/>.

- John, Oliver/Naumann, Laura/Soto Christopher: Paradigm Shift to the Integrative Big Five Trait Taxonomy, in: John, Oliver/Pervin, Lawrence/Robins, Richard (eds), *Handbook of Personality: Theory and Research*, 3rd edn. (2008), 114 ff.
- Kaesling, Katharina: Evolution statt Revolution der Plattformregulierung, *ZUM* 2021, 177 ff.
- Kalbhenn, Jan Christopher/Hemmert-Halswick, Maximilian: Der Regierungsentwurf zur Änderung des NetzDG – Vom Compliance-Ansatz zu Designvorgaben, *MMR* 2020, 518 ff.
- Katsirea, Irini: “Fake news”: reconsidering the value of untruthful expression in the face of regulatory uncertainty, *Journal of Media Law* 2018, 159 ff.
- Kettemann, Matthias/Benedek, Wolfgang: Freedom of expression online, in: Susi, Mart (ed), *Human Rights, Digital Society and the Law: A Research Companion* (2019), 58 ff.
- Kettemann, Matthias/Tiedeke, Anna: Back up: can users sue platforms to reinstate deleted content?, *Internet Policy Review* 2020, 1 ff.
- Knight, Ben: Germany: Hate speech, threats against politicians rise, *Deutsche Welle*, 9 February 2021, <https://www.dw.com/en/germany-hate-speech-threat-s-against-politicians-rise/a-56512214>.
- Köhler, Daniel/Ebner, Julia: Strategies and tactics: communication strategies of jihadists and right-wing extremists, in: Baldauf, Johannes/Ebner, Julia/Guhls, Jakob (eds), *Hate Speech and Radicalisation Online – The OCCI Research* (2019), 18 ff. <https://www.isdglobal.org/wp-content/uploads/2019/06/ISD-Hate-Speech-and-Radicalisation-Online-English-Draft-2.pdf>.
- Krieger, Heike: Krieg gegen anonymous – Völkerrechtliche Regelungsmöglichkeiten bei unsicherer Zurechnung im Cyberwar, *AVR* 2012, 1 ff.
- Ladeur, Karl-Heinz/Gostomzyk, Tobias: Das Netzwerkdurchsetzungsgesetz und die Logik der Meinungsfreiheit, *K&R* 2017, 390 ff.
- Lang, Andrej: *Netzwerkdurchsetzungsgesetz und Meinungsfreiheit – Zur Regulierung privater Internet-Intermediäre bei der Bekämpfung von Hassrede*, *AöR* 2018, 220 ff.
- Laub, Zachary: Hate Speech on Social Media: Global Comparisons, Council on Foreign Relations, 11 April 2019, <https://www.cfr.org/backgrounders/hate-speech-social-media-global-comparisons>.
- Lauber-Rönsberg, Anne: Hate Speech – ein Überblick über rechtliche Rahmenbedingungen, ihre Durchsetzung und das neue NetzDG, *Aptum* 2017, 100 ff.
- Lauber-Rönsberg, Anne: Persönlichkeitsschutz in der EMRK und im EU-Recht – § 57. Europäische Menschenrechtskonvention, in: Götting, Horst-Peter/Schertz, Christian/Seitz, Walter (eds), *Handbuch des Persönlichkeitsrechts* (2019), 1197 ff.
- Lessig, Lawrence: *Code: And Other Laws of Cyberspace* (1999), 6 ff.
- Lessig, Lawrence: *Code: And Other Laws of Cyberspace*, Version 2.0 (2006), 1 ff.
- Levin, Dov: Partisan electoral interventions by the great powers: Introducing the PEIG Dataset, *Conflict Management and Peace Science* 2019, 88 ff.

- Lomas, Natasha: Facebook found hosting masses of far right EU disinformation networks, Tech Crunch, 22 May 2019, <https://techcrunch.com/2019/05/22/facebook-found-hosting-masses-of-far-right-eu-disinformation-networks/>.
- Martens, Bertin/Aguiar, Luis/Gomez-Herrera, Maria/Muller-Langer, Frank: The digital transformation of news media and the rise of disinformation and fake news, JRC Digital Economy Working Paper, No. 2018–02, <https://www.econstor.eu/bitstream/10419/202231/1/jrc-dewp201802.pdf>.
- Ohlin, Jens David: Election Interference – International Law and the Future of Democracy (2020), 14 ff.
- Quenqua, Douglas: Facebook Knows You Better Than Anyone Else, The New York Times, 19 January 2015, www.nytimes.com/2015/01/20/science/facebook-knows-you-better-than-anyone-else.html.
- Peukert, Alexander: Gewährleistung der Meinungs- und Informationsfreiheit in sozialen Netzwerken. Vorschlag für eine Ergänzung des NetzDG um sog. Put-back-Verfahren, MMR 2018, 572 ff.
- Peukert, Alexander: Put it back: Ein Vorschlag für ein NetzDG, das die Meinungsfreiheit wahrt, Verfassungsblog, 14 June 2018, <https://verfassungsblog.de/put-it-back-ein-vorschlag-fuer-ein-netzdg-das-die-meinungsfreiheit-wahrt/>.
- Pollicino, Oreste: Fundamental Rights as Bycatch – Russia’s Anti-Fake News Legislation, Verfassungsblog, 28 March 2019, <https://verfassungsblog.de/fundamental-rights-as-bycatch-russias-anti-fake-news-legislation/>.
- Pollicino, Oreste: Judicial Protection of Fundamental Rights in the transition from the world of atoms to the word of bits: The case of freedom of speech, Eur. Law J. 2019, 155 ff.
- Proops, Anya: Comment is (not) free – E-Commerce back in the limelight, Panopticon, 22 June 2015, <https://panopticonblog.com/2015/06/22/comment-is-not-free-e-commerce-back-in-the-limelight/>.
- Rainey, Bernadette/Wicks, Elizabeth/Ovey, Clare: Jacobs, White, and Ovey: The European Convention on Human Rights, 7th edn. (2017), 486 ff.
- Roberts, Louise: Peter the Great in Poland, The Slavonic Review 1927, 537 ff.
- Robertson, Jordan/Riley, Michael/Willis, Andrew: How to Hack an Election, Bloomberg Businessweek, 31 March 2016, www.bloomberg.com/features/2016-how-to-hack-an-election/.
- Röttger, Tania: Nein – Merkel „hofft“ nicht auf 12 Millionen Einwanderer, Correctiv, 5 March 2018, <https://correctiv.org/fakten-check/2018/03/05/nein-merkel-hofft-nicht-auf-12-millionen-einwanderer/>.
- Sängerlaub, Alexander/Meier, Miriam/Rühl, Wolf-Dieter: Fakten statt Fakes – Verursacher, Verbreitungswege und Wirkungen von Fake News im Bundestagswahlkampf 2017, Stiftung Neue Verantwortung 2018, 79 ff., https://www.stiftung-nv.de/sites/default/files/snv_faktenstattfakes.pdf.
- Sardo, Alessio: Categories, Balancing, and Fake News: The Jurisprudence of the European Court of Human Rights, Canadian Journal of Law & Jurisprudence 2020, 435 ff.

- Schmehl, Karsten/Lytvynenko, Jane: 7 Out Of The 10 Most Viral Articles About Angela Merkel On Facebook Are False, BuzzFeed News, 27 July 2017, <https://www.buzzfeednews.com/article/karstenschmehl/top-merkel-news>.
- Schwarz, Karolin/Holnburger, Josef: Disinformation: What role does disinformation play for hate speech and extremism on the internet and what measures have social media companies taken to combat it?, in: Baldauf, Johannes/Ebner, Julia/Guhls, Jakob (eds), *Hate Speech and Radicalisation Online – The OCCI Research* (2019), 35 ff., <https://www.isdglobal.org/wp-content/uploads/2019/06/ISD-Hate-Speech-and-Radicalisation-Online-English-Draft-2.pdf>.
- Scola, Nancy: How chatbots are colonizing politics, Politico, 10 November 2016, www.politico.com/story/2016/10/chatbots-are-invading-politics-229598.
- Scott, Mark: Cambridge Analytica did work for Brexit groups, says ex-staffer, Politico, 30 July 2019, <https://www.politico.eu/article/cambridge-analytica-leave-eu-uk-ip-brexit-facebook/>.
- Shane, Scott: Russia Isn't the Only One Meddling in Elections. We Do It, Too., The New York Times, 17 February 2018, <https://www.nytimes.com/2018/02/17/sunday-review/russia-isnt-the-only-one-meddling-in-elections-we-do-it-too.html>.
- Shearer, Andrew: The Evolution of Hybrid Warfare and Key Challenges, Statement Before the House Armed Services Committee, 22 March 2017, https://csis-website-prod.s3.amazonaws.com/s3fs-public/congressional_testimony/170322_shearer_testimony_evolution_of_hybrid_warfare.pdf.
- Shulman, Stephen/Bloom, Stephen: The legitimacy of foreign intervention in elections: The Ukrainian response, *Review of International Studies* 2012, 445 ff.
- van der Sloot, Bart: The Practical and Theoretical Problems with 'Balancing': Delfi, Coty and the Redundancy of the Human Rights Framework, *Maastricht Journal of European and Comparative Law* 2016, 439 ff.
- Smith, Rachael Craufurd: Fake news, French Law and Democratic Legitimacy: Lessons for the United Kingdom?, *Journal of Media Law* 2019, 52 ff.
- SPIEGEL online: SPIEGEL-Umfrage unter Parlamentarierinnen – Frauenfeindlichkeit im Bundestag durch AFD gestiegen, 12 February 2021, <https://www.spiegel.de/politik/deutschland/bundestag-frauenfeindlichkeit-durch-afd-gestiegen-a-4c8c425c-6b08-4ac5-b049-61ad65d1240c>.
- Steiger, Dominik: International Law and New Challenges to Democracy in the Digital Age: Big Data, Privacy and Interferences with the Political Process, in: Witzleb, Normann/Paterson, Moira/Richardson, Janice (eds), *Big Data, Political Campaigning and the Law: Privacy and Democracy in the Age of Micro-Targeting*, Abingdon (2020), 71 ff.
- Tharoor, Ishaan: The long history of the U.S. interfering with elections elsewhere.
- The Washington Post, 13 October 2016, <https://www.washingtonpost.com/news/worldviews/wp/2016/10/13/the-long-history-of-the-u-s-interfering-with-elections-elsewhere/>.
- Tysiachniouk, Maria/Tulaeva, Svetlana/Henry, Laura: Civil Society under the Law 'On Foreign Agents': NGO Strategies and Network Transformation, *Europe-Asia Studies* 2018, 615 ff.

- U.K. Information Commissioner's Office (ICO): RE: ICO investigation into use of personal information and political influence, 2 October 2020, https://ico.org.uk/media/action-weve-taken/2618383/20201002_ico-o-ed-l-rtl-0181_to-julian-knight-mp.pdf.
- UNGA: Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, A/HRC/17/31, 21 March 2011, 13 ff.
- Voorhof, Dirk: Pihl v. Sweden: non-profit blog operator is not liable for defamatory users' comments in case of prompt removal upon notice, Strasbourg Observers, 20 March 2017, <https://strasbourgobservers.com/2017/03/20/pihl-v-sweden-non-profit-blog-operator-is-not-liable-for-defamatory-users-comments-in-case-of-prompt-removal-upon-notice/>.
- Voorhof, Dirk: The Court's subtle approach for online media platform's liability for user-generated content since the 'Delfi Oracle', Strasbourg Observers, 10 April 2020, <https://strasbourgobservers.com/2020/04/10/the-courts-subtle-approach-of-online-media-platforms-liability-for-user-generated-content-since-the-delfi-oracle/>.
- Voorhof, Dirk/Lievens, Eva: Offensive Online Comments – New ECtHR Judgement, ECHR Blog, 15 February 2016, <https://www.echrblog.com/2016/02/offensive-online-comments-new-ecthr.html>.
- Wienfort, Nora: Blocking Overblocking – Frankreichs Verfassungsrat kippt das Gesetz gegen Hasskriminalität im Netz, Verfassungsblog, 20 June 2020, <https://verfassungsblog.de/blocking-overblocking/>.
- Wischmeyer, Thomas: Making social media an instrument of democracy, Eur. Law J. 2019, 169 ff.
- Zimmermann, Andreas: International Law and „Cyber Space“, ESIL Reflections 2014, 1 ff.