Wolfgang Schulz

Regulating Intermediaries to Protect Privacy Online – the Case of the German NetzDG

HIIG DISCUSSION PAPER SERIES 2018-01

ABSTRACT

With the shift of communication to the internet, conflicts between freedom of communication and personal rights are also shifting to the Net. With the enactment of a so-called "Network Enforcement Act" (Netzwerkduchsetzungsgesetz - NetzDG), Germany has taken a path to address this problem by regulating platforms, which has received much international attention. This article presents the regulatory concept of the NetzDG and examines the consequences, especially for freedom of communication. Alternatives will be discussed on the basis of a recent recommendation of the Council of Europe on roles and responsibilities of online intermediaries.

This is a preprint of an essay that was written for the volume by Marion Albers and Ingo Sarlet (editors), Personality and Data Protection Rights on the Internet.

KEYWORDS

Netzwerkdurchsetzungsgesetz, Network Enforcement Act, Intermediary Regulation, Freedom of Speech, Law and Technology

AUTHOR

Wolfgang Schulz is Professor of Media Law, Public Law and Legal Theory, University of Hamburg; Director Hans-Bredow-Institut; Director Humboldt Institute for Internet and Society; UNESCO Chair on Freedom of Communication and Information. The author wants to thank Florian Wittner for valuable feedback and research support.

CONTENTS

1 INTRODUCTION

With the shift of communication to the internet, conflicts between freedom of communication and personal rights are also shifting to the Net. This article examines the peculiarities of online communication and poses the question of the role of intermediaries in these conflicts, both de facto and legally. The consequences of a curation of content at the intermediary level are examined using the German "Network Enforcement Act" as an example. Finally, the paper discusses what a human rights-friendly solution might look like.

2 PRIVACY RISKS ONLINE

For lawyers – other than for politicians from time to time – it is evident that what is illegal offline is also illegal online. That is especially true for libel, defamation and other privacy infringements. Nevertheless, internet based communication makes a structural difference in many aspects that may lead to a re-assessment of existing rules and of traditional means of implementation of legal requirements. Here are the most basic specifics:

Volume – The mere number of cases can become a structural challenge. Facebook, to take an example, stated that it makes over 100,000 content-related decisions per month in the German version of Facebook alone.[1]

This means that the suggestion to let the national courts decide on all content-related user-user or user-platform conflicts has to be ruled out as a solution.

Acceleration – While some content put on a social media platform might never be read by anyone apart from the authors, some can go viral across platforms and reach many people in a very short period of time.[2] Therefore, governance mechanisms have to be very fast to come into effect before the content has been widely distributed, since one can assume that after the distribution the content cannot be located and addressed. There are so far no mechanisms to control access to the content after distribution.[3]

Observability – Online communication makes it easy for third parties or even the general public to observe communication among groups or between individuals. This has made services like rating platforms possible but also poses distinct challenges: observers may not know the contexts in and social rules under which individuals or groups discuss. Many of the problems that societies have with the internet in general and social media in particular result from the fact that the talks at the "regulars' tables" are now visible to everyone, with all their exaggerations, polemics and stereotypes.

Persistence – It has become a popular saying that the internet never forgets. That is true in the sense that at least so far there is no technology that can make sure that a piece of information can be deleted from all servers, wherever they are. The so-called "right to be forgotten" is no more than a right to deletion that can provide a data subject with a claim against a specific controller.[4] In case of search engines that can help making the information in question far harder to find, however, it is not gone.

[1] Köver 2016.
[2] Goel et al. 2009.
[3] For the technical possibilities and limits, see cf. Federrath 2015.
[4] cf. Paal 2018, Rt1.

Attribution problems – Online it can be hard to identify the speaker, e.g. in case one wants to file a claim against him or her. Even if there is a clear name policy that does not mean to say that the users are identifiable for their vis-à-vis in the online communication. Anonymity is common online and many state that the option to not disclose the name is essential for many functions the internet fulfils for public communication.[5] Often it is also unclear whether other actors like the platform claim ownership of a piece of information as well, so that attribution can be generally fuzzy.

Weak social control – Coupled with the attribution problem is the aspect of social control. Legal concepts like privacy and its protection depend in their implication largely on the relevant norms becoming internalised. Social norms and social control make the main difference, not legal enforcement. That mechanism might be weaker online, especially when the speakers do not know each other in "real life". There are studies that show that when people communicate in anonymous forums, they are more uninhibited - and ultimately more hurtful - than usual.[6]

Jurisdiction issues – As a global technical medium the internet enables access by anybody to any content, at least in principle. Though people initially worried about the internet being a legal vacuum it now has become apparent that, to the contrary, the main challenge is that all legal orders can be applicable at the same time. Since legal systems frame privacy in different ways there is the risk of jurisdictional problems.[7]

Those are only some important structural characteristics of online communication. Against this background there are political initiatives to tackle the problem of harmful content online, including content that hampers the privacy of others. The effects mentioned above make it unlikely that the problem can be solved by means of traditional legal instruments, e.g. users suing each other before national courts. The eyes of policy makers have therefore turned to the actor that might solve the problem in an easy way: the provider of the intermediary service like the social media platform provider. They – as a rule – have mechanisms in place to assess the conformity of content with their own community standards, they can act before things go viral and they can act even if the user who posted the content cannot be identified. Addressing the intermediaries is supposedly the easy way.

3 APPROACHES TO REGULATE INTERMEDIARIES

This article focuses on approaches within the European Union, especially Germany. Under Article 12 to 14 of Directive 2000/31/EC (e-Commerce Directive), there is a limit to the liability of service providers for third party content.[8] The e-Commerce Directive (Article 14) has led to the development of take-down procedures, but does not regulate them in detail. Even though there are differences in scope and concept this can be seen as the European equivalent of section 230 of the US Communications Decency Act.[9] The Directive 2000/31/EC also establishes the country of origin principle that asserts that member states where the service does not originate do not have the competence to regulate the service for pursuits that are covered by the directive.

On a European level, the Commission has – against this background – so far refrained from regulating intermediaries specifically but has opted to encourage measures of self-regulation. In 2016, the Commission negotiated a Code of Conduct on illegal online hate speech with big players of the IT industry, the

[5] Especially emphasized by the German Federal Court (BGH) in its spickmich.de decision, BGH 23.06.2009 – VI ZR 196/08.
[6] cf. Pötzsch 2010.
[7] See for a comprehensive discourse on the topic Internet & Jurisdiction Policy Network 2018.
[8] In Germany implemented in §§8-10 TMG. Liability in such cases is contingent on the service provider taking note of the unlawfulness of third party content.
[9] Wang 2018, 36-7.

compliance with which is evaluated on a regular basis.[10]

Germany started with a similar approach, i.e. the Ministry of Justice motivated the industry to improve their complaints mechanisms. However, the Government declared in 2017 that they were not satisfied with the performance of these self-regulatory efforts. According to the German Ministry of Justice, Facebook in particular reacted too slowly to complaints while Twitter had generally low response rates.[11]

Driven by fears that fake news and hate messages could influence the Bundestag[12] election campaign in autumn 2017, the German government hurriedly worked on a draft Network Enforcement Act. Even though during a hearing at the judicial committee of the Bundestag most experts advised against the approach on which the act was based, the coalition used its majority to push it through parliament before the summer break 2017.[13] It came into force on October 1, 2017 and has been fully applicable since January 1, 2018.

The regulatory model has since been adopted by Russia[14] and other countries are considering a similar approach[15].

3.1 The German Network Enforcement Act

The act defines the networks that shall fall within its scope: some rules are applicable only to big networks (based on the number of users in German), some to all. There is no definition of hate speech or fake news; instead, the act refers to existing definitions of criminal offences under the German Penal Code. There is a long list of offences partly aiming at protecting general rights and public safety but also norms safeguarding individuals' rights like insulting, slander and defamation (§§ 185-189 German Penal Code). The latter is the link to protecting privacy, which is the main focus of this article.

The provider of a social network shall maintain an effective and transparent procedure for handling complaints about unlawful content. This is the main obligation under the act. While in early versions of the draft, the emphasis was on individual cases, it is now the complaints systems the platform providers have to put in place.

The NetzDG indicates what a functioning complaints system shall provide the following: Providers have to make sure that they delete content that appears to be evidently unlawful within 24 hours after a complaint has been filed. When content is not evidently unlawful, deletion has to be achieved within 7 days. Review period may exceed 7 days when more time is required for the decision-making to reduce "overblocking", when the provider makes use of self-regulation.

This inclusion of an element of self-regulation comes from a debate in the law-making process where critics referred to the model of co-regulation in Germany within the minor protection law, which is widely regarded as a success, as an alternative to the NetzDG approach. The lawmakers, however, just included this element, which, as of May 2018, has not yet been used by the industry.

Under the NetzDG, providers of social networks shall immediately name a person authorized to receive

[10] The challenges of enforced self-regulation in terms of the rule of law principle and human rights aspects cannot be discussed here. There is the obvious risk of states or supranational bodies like the EU Commission trying to convince the industry to "voluntarily" implement measures that the state could not legally enact.
[11] Press release by the GMJ 2017.
[12] The German Parliament.
[13] Bundesgesetzblatt Jahrgang 2017 Teil I Nr. 16, issued September 07 2017, 3352.
[14] cf. Rötzer 2018.
[15] cf. Bröckling 2018.

complaints in the Federal Republic of Germany and a contact point for law enforcement.

Providers of social networks that receive more than 100 complaints per calendar year about unlawful content shall also produce half-yearly German-language reports on the handling of complaints.

The responsible authority is the Federal Office of Justice, which is directly subordinated to the Ministry of Justice. The breach of the obligations in line with sec. 2 para 1 or the obligation to remove unlawful content can be punished with a regulatory fine of up to five million euros (restricted to structural malfunction?). The fine complies with sec. 4 para 2 NetzDG: it refers to sec. 30 para 2 OWiG and hence the fine can add up to 50 million euros. Fines can only be issued in case of systematic failure of the complaints-handling system. The administrative offence may be sanctioned even if it is not committed in the Federal Republic of Germany.

Until April 2018, the Federal Office of Justice received approximately 400 submissions claiming that providers have not adequately responded to complaints they received. So far, no fines have been issued.

Furthermore, the NetzDG has established a right to disclosure: Anyone whose general personality rights are violated by the criminal offences covered by the new act will, as a rule, be able to demand that the social network concerned disclose details of the person that committed the offence. Such entitlement to information is founded in existing general principles of civil law. With the new legislation, we are ensuring that these entitlements can actually be asserted. Operators of social networks will be given the power under data protection law to disclose the subscriber information of the infringer to the injured party. In order to do so, however, the social network must have been ordered to disclose this data by a civil court with jurisdiction over the matter (judicial scrutiny reservation).[16]

3.2 Critical Analysis

Apart from the more formal points – like the notion that the federal state in Germany lacks legislative competence to regulate the issue[17] and the NetzDG being invalid under art. 5 para 1 (EU) 2015/1535 because criminal offences and the concept of regulated self-regulation were added without re-notification of the EU Commission[18] – the general criticism mainly refers to violations of the e-Commerce Directive and to fundamental rights concerns.[19]

3.2.1 Aspects of European Law

The assessment of European Law focusses on the liability privilege under Art. 14 e-Commerce Directive. According to article 14 liability of hosting services is possible when the provider has positive knowledge of illegal content. It loses the privilege if it does not react "expeditiously". This leads to the question of whether Member States are just substantiating the term "expeditiously" when naming specific time frames,

[16] Whether this is helpful or not depends on what information the provider itself has, i.e. whether the service requires a logon with a clear name.
[17] Cf. Statement of the German Bar Association (DAV) 2017, 5. Bitkom statement 2017, 3. For a dissenting opinion see Roßnagel et al. 2017, 9, arguing that the law does not regulate content but only substantiates §10 TMG, which is itself a (lawful) federal provision.
[18] Member States must notify again a draft which has already been examined under the provisions of art. 5 para 1 (EU) 2015/1535, if they make significant amendments to the draft in the following. The third subparagraph of Article 5 (1) specifies that amendments made to the text are considered to be significant if they have the effect of altering its scope, shortening the timetable originally envisaged for implementation, adding specifications or requirements, or making the latter more restrictive. (Cf. CJEU in case C-433/05, Lars Sandström.). Criminal offences protecting the state's reputation were removed (§§ 90, 90a, 90b StGB) and § 201a StGB was added on the recommendation of the committee on legal affairs on 28th June 2017 which can be regarded as a „significant change".
[19] See the Statement by Digitale Gesellschaft e.V 2017, 3. See also the statements by BVDW e.V 2017, 1f, and OSCE 2017, 8f, as well as Article 19 2017, 12ff and Global Network Initiative 2017.

like the German NetzDG does, or whether they are deferring to the e-Commerce Directive which might have specifically opted for not giving a rigid time frame. There is good reason to believe that Germany overstepped the mark because the whole purpose of the directive is to harmonize cross-border service provision in Europe and different time frames in different Member States would hamper that aim.[20]

Even if Member States could substantiate the time frame, it would under the concept of the e-Commerce Directive be the responsibility of the country of origin to make a provider comply with its legal framework. Other Member States could only enforce their regulation under the exemption clause of art. 3 sec. 4 e-Commerce Directive. This exception is, however, restricted to individual cases and does not allow member states to apply their jurisdiction all together "through the backdoor".[21]

The obligation to name a domestic authorized recipient might also violate Art. 3 e-Commerce Directive and hamper the freedom of establishment as laid down in the EU treaties[22].

3.2.2 Human rights aspects

Even when limiting the consideration to possible infringements of freedom of communication and no other freedoms, the multi-level fundamental rights system in Europe, a system that has not been constructed purposefully but rather emerged over time, makes for a rather complex situation. Since this article does not only target European readers, the relevant sources of fundamental rights shall be described briefly[23]:

The European Convention on Human Rights (ECHR) – an international treaty that is part of the Council of Europe and enforced by the European Court on Human Rights. Freedom of speech is protected under art. 10 para 1 ECHR. In Germany, it is ratified as binding law on the level of a federal act, thus ranking behind the national constitution. The EU itself has not signed and ratified the Convention.

The EU Charter of Fundamental Rights (ChFR) – part of the European Union's legal system and binding to European institutions and Member States, but only when they are implementing and applying Union law. Freedom of speech is protected under art. 11 para 1 ChFR.

The National constitution, here the Grundgesetz (GG, Basic Law) – in accordance to which all laws like the NetzDG have to be. The freedom of speech is protected under Art. 5 para 1 GG.

This analysis will not go into specifics of the freedom of speech guarantees under those fundamental rights systems but will just name points of criticism that might be relevant in all legal assessments. The complexity of the analysis is also increased by the fact that there are fundamental rights interests of various actors involved:

[1] The "victim" offended by speech on the platform, which might or might not also be the complainant,

[2] the provider of the social media platform,

[3] the author of illegal content that is taken down,

[20] See Recital 5, DIRECTIVE 2000/31/EC.
[21] Cf. Spindler 2017, 14f.
[22] Cf. Ladeur/Gostomzyk 2017, 93.
[23] For a further referral to the law's (non)compatibility with the International Covenant on Civil and Political Rights (ICCPR) see Kaye 2017 and Article 19 2017, 5ff.

[4] the author of legal content that is (wrongly) taken down,

[5] the recipients of content.

The legal status of intermediaries like social media services under freedom of speech protection is still unclear.[24] They clearly enjoy freedom of speech protection for their own statements on the platform, but whether the provision of the platform as such and specific functions provided for the users are protected as well is heavily debated. The central question is whether an establishment of a complaint system as required by the NetzDG is encroachment on the fundamental rights of the provider[25].

There is a limited number of types of content where publication is illegal under any circumstances. In any other case, the protection of freedom of speech requires a context-sensitive determination of the meaning of the act of speech. That is especially true for possible infringements of personal rights. Under German constitutional law, there is a complex balancing to be performed when reporting about a person without consent. It is unlikely to encounter any "obvious" case in this field.

If a state law is likely to make a provider remove content that is legal, this law interferes with the freedom of speech (art. 5 para. 1 GG, art. 10 para 1 ECHR, art. 11 para 1 CFR)[26].

To begin with, the deadline of 24 hours for removing content that is "obviously illegal" triggers freedom of speech concerns. First, there is doubt whether obviously illegal content can be identified easily, given that context always has to be taken into account. Second, each piece of content that has been flagged has to be assessed to identify the "obviously illegal" parts. According to Facebook, defamation and hate speech alone account for 100,000 takedowns per month in Germany. Given that figure, it seems rational for a provider to take down any flagged content if in doubt, just to save costs.

The seven-day deadline for the remaining (not obviously) illegal content also causes doubts. The assessment whether a speech is a statement of fact or a proclamation of an opinion is essential for an assessment under German law. This is a complex issue, and it might be that even different courts disagree on the result[27]. The same is true for the question whether a statement of fact is evidentially true or not. To conduct such assessments within the given time frame puts pressure on a provider and might again push it to the simple but human rights-adverse solution to take down the content in almost any case. Furthermore, the providers lack the information about the context – and the necessary information gathering tools – to make a proper assessment.

Early versions of the draft stated a specific obligation to make sure that similar content is not uploaded again. This triggered fears of over-blocking since this the most effective way of doing this is by using upload filters, which – at the current state of development – fail to detect irony or critical reference to content. This part of the draft has been removed, but the draft still requires that the same content on the platform should be detected and removed, which again is best done by automated systems that are as of yet not context-sensitive.

In case there is an encroachment on fundamental rights and we have to assess whether it is justified, we have to perform a proportionality test. At least under the German methodology the first step of that test is to see whether the legislation follows a "legitimate aim". While enforcing criminal law is without any

[24] In the case of Delfi AS v Estonia (64569/09) the ECHR ruled against a news platform that had been deemed liable for anonymous defamatory comments posted under an article on their website.
[25] See cf. Ladeur/Gostomzyk 2017, 32ff. and 93f. for an emphasis on (and an argument for the violation of) the provider's fundamental right on occupational freedom.
[26] Cf. Reporter ohne Grenzen 2017, 7f; Ladeur/Gostomzyk 2017, 76f.
[27] See Lee 2017 for a discussion on the difficulties of context and statistics on German court decisions.

doubt a legitimate aim, we have to consider that parts of the rules of the NetzDG do not really help finding the culprit. However, reducing the effect of criminal acts might be also legitimate. It is noteworthy however, that the official statement of reasons for the NetzDG begins by referring not to this aim, but rather to the need to maintain a political debate culture. That is understandable due to the rise of right wing populist movements at the time the law was made. However, the desire for protecting the political culture – plausible as it is – does not suffice to limit human rights; it puts the complexity of an act of moral regulation to the NetzDG[28].

Another point of criticism is that the Federal Office of Justice has a crucial role in the enforcement of the act and directly reports to the Minister of Justice, making it by no means politically independent[29]. That is especially notable in Germany where the independence of the media system is firmly protected by the Federal Constitutional Court, one of the reasons for that being the history of Germany with the state making use of the new media during the Nazi dictatorship.

Those were only the broad lines of criticism, showing the structural problems with this kind of regulation. It can thus already be said that trying to make use of the intermediaries might not be the silver bullet after all[30].

4 TOWARDS AN INTERNET-SENSITIVE SOLUTION

4.1 Regulating Intermediaries

Online intermediaries in various forms – including search engines, social media, or app platforms – play a constitutive role in today's digital environment. They have become a new type of powerful institution in the 21st century that shape the public networked sphere, and are subject to intense and often controversial policy debates.[31] As mentioned before, their intermediary function puts them in a position that is tempting for lawmakers and regulators to utilize.

Driven by the need to better understand the governance structure in the online area, a four-component system that we have developed building on a concept by Larry Lessig proved to be helpful.[32] Legal norms set by the state, contracts, social norms and computer code are considered in their interaction. In the context of intermediaries, it is significant that computer code and contracts and – to some extent – social norms are developed by them and that the state tries to influence all of these factors by using the law. The power of intermediaries also raises questions about "private ordering" by intermediaries[33], which is not the focus of this article but is important nonetheless. This article discusses the law making use of the power of intermediaries especially by using code like filters and their contractual right to remove content.

In case of legislation that creates incentives for a rational intermediary to act in a way that makes it likely that freedom of speech suffers, this has to be seen as an interference with freedom of expression.[34] That means that it can only be justified when it complies with the limitations set up in the GG, the CFR or the ECHR.

[28] Similarly focusing on the law's lack of an empirical basis Reporter ohne Grenzen 2017, 2.
[29] Cf. Kaye 2017, 4.
[30] For a more nuanced conclusion and an emphasis on the positive effects of the law, see, inter alias, Roßnagel et al. 2017 and Theil 2018.
[31] Cf. Gasser/Schulz 2015, 3f.
[32] See Niva Elkin-Koren 2011, 16f.
[33] Cf. Niva Elkin-Koren 2011, 17f. and Balkin 2018, 1182f.
[34] For the freedom of expression granted by the GG, this follows from the modern interpretation of an interference with fundamental rights as any act by the state that makes the exercise of the affected right impossible or substantially more difficult. Cf. Grabenwarter 2017, Rt.100.

There is an incentive to fulfil the legal demands by using technology. Detection and deletion of harmful speech online is already common practice. It is being done for child pornography and for terrorist activities.[35] Technology is also used in the area of copyright infringements.[36] What is significant, however, is how the technical possibilities of regulating via code influences the legal requirements – and vice-versa.

4.2 The Significance of Context as a Law and Technology Problem

Privacy infringements are a special case since at least in Germany the constitution demands a proper construction of the meaning of the statement in question. This in turn requires – as mentioned before – an assessment of the context.[37] It makes, to take an example, a big difference for the legal assessment whether there is critical reflection or irony involved. Child pornography is one of the few examples where no context is conceivable that would justify publication.

A case that was discussed intensely in Germany was a selfie taken by a refugee with Chancellor Angela Merkel. This picture was used by right wing groups with the false statement that the refugee was indeed involved in terrorist activities and that fake got viral. There was much discussion about that case which also used the picture. So just using the indicator of this picture in connection with the word "terrorist" would lead to the removal of many posts who critically examined the use of the image of right-wing extremists.

This makes the state of the art in context detection the deciding factor for an automated system to produce legally acceptable results. Despite all progress in the field of artificial intelligence, it appears that there are currently no systems that can detect irony with sufficient certainty. Therefore, the legal assessment – especially the proportionality of a measure – depends on the technological state of the art.

This is not unheard of, but legal requirements for content regulation belong to the rare cases where it becomes relevant on a constitutional level. It has to be taken into account when discussing a human rights-compatible solution for the privacy challenges online.

4.3 Council of Europe Recommendation on the Roles and Responsibilities of Internet Intermediaries

The most recent and rather comprehensive attempt to give guidance to states on how to regulate intermediaries in a human rights-friendly manner is the Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries adopted by the Council of Europe in April 2018.[38]

The recommendation states that protection of privacy and personal data is fundamental for the enjoyment and exercise of most of the rights and freedoms guaranteed in the Convention. However, the internet has facilitated an increase in privacy-related risks and infringements and has spurred the spreading of certain forms of harassment, hatred and incitement to violence, in particular on the base of gender, race and religion, which remain underreported and are rarely remedied or prosecuted. Moreover, the rise of the internet and related technological developments have created substantial challenges for the maintenance of public order and national security, for crime prevention and law enforcement, and for the protection of the rights of others, including intellectual property rights. Targeted disinformation campaigns online, designed

[35] Cf. Iqbal et al. 2018.
[36] See. Dewey 2016 on how Youtube uses automated takedown measures and the complications that arise, especially in connection to citations and Fair Use.
[37] This means, inter alia, that due to the importance of this right for a democratic society, where different interpretations of a statement are equally possible, one must assume the one that is still protected by freedom of speech. Cf. Grabenwarter 2017, Rt.139f.
[38] Available at: https://rm.coe.int/1680790e14. The author of this article has been the chairman of the Committee that drafted the Recommendation.

specifically to sow mistrust and confusion and to sharpen existing divisions in society, may have destabilising effects on democratic processes.

A wide, diverse and rapidly evolving range of players, commonly referred to as "internet intermediaries", facilitate interactions on the internet between natural and legal persons by offering and performing a variety of functions and services. The recommendation highlights that intermediaries may carry out several functions in parallel. They may also moderate and rank content, including through automated processing of personal data, and may thereby exert forms of control that influence users' access to information online in ways comparable to media, or they may perform other functions that resemble those of publishers. Intermediary services may also be offered by traditional media, for instance, when space for user-generated content is offered on their platforms. The regulatory framework governing the intermediary function is without prejudice to the frameworks that are applicable to the other functions offered by the same entity.

Remarkably, the recommendation is nearly equally divided in proposals towards states and towards intermediaries themselves. The latter are based on the Ruggie principles, stating that companies, while not directly bound by human rights, should nevertheless have a responsibility to observe them in their decision-making.

There are some recommendations that set limits on the NetzDG-style of regulation in the interest of protecting human rights. No. 1.3.2 is of particular importance, requiring state authorities to obtain an order by a judicial authority or other independent administrative authority whose decisions are subject to judicial review, when demanding intermediaries to restrict access to content. This does not apply in cases concerning content that is illegal irrespective of context, such as content involving child sexual abuse material, or in cases where expedited measures are required in accordance with the conditions prescribed in Article 10 of the Convention.

Crucial in this context is 1.3.7, stating: "States should ensure, in law and in practice, that intermediaries are not held liable for third-party content which they merely give access to or which they transmit or store. 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. Notices should contain sufficient information for intermediaries to take appropriate measures. Notices submitted by states should be based on their own assessment of the illegality of the notified content, in accordance with international standards. Content restrictions should provide for notice of such restriction being given to the content producer / issuer as early as possible, unless this interferes with ongoing law-enforcement activities. Information should also be made available to users seeking access to the content, in accordance with applicable data protection laws."

This offers several valuable points like the need for specifications for complaints and the explicit mentioning of the time frame, which has been one of the main points of criticism of the NetzDG approach.

5 CONCLUSIONS

The core of the legal assessment of measures taken by the state is the proportionality test. The Council of Europe Recommendation already marks some consequences of applying the test. Conflicts between privacy and freedom of communication are especially tricky due to context-sensitivity. Intermediaries do not have the knowledge base to do a proper assessment and technical means are not yet at hand. In consequence measures that lead to an ad hoc assessment and / or to the use of technology for content moderation will not meet the proportionality test and, in consequence, infringe on freedom of communication. The

proportionality test should also guide the regional scope of measures.[39]

This insight - which is bitter for the protection of privacy - can only be mitigated by accompanying measures. One is obviously enhancing the knowledge about counter speech. In political debates, this is sometimes used as an argument against regulation without actually getting into the issue. However, extensive research about various practices and its effects exists.[40]

Furthermore, it can be in the best interest of intermediaries – and should be encouraged by lawmakers and courts alike – to design and implement instruments of dispute resolution so that the conflicts can be brought back to its primary parties.[41] Finally, we will almost certainly see that social norms will adapt to the new means of communication. When we realise that people do not attach so much significance to an incidental statement on an online platform, this will reduce the actual harm done by those pieces of communication and consequently reduce the need for legal action to protect privacy online.

6 REFERENCES

Article 19 (2017) Germany: The Act to Improve Enforcement of the Law in Social Networks – Legal Analysis. https://www.article19.org/wp-content/uploads/2017/09/170901-Legal-Analysis-German-NetzDG-Act.pdf. Accessed 29 May 2018.

Balkin J (2018) Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation. UCLA Law Rev. 51:1149-1209.

Bitkom (2017) Stellungnahme zum Regierungsentwurf NetzDG. https://www.bitkom.org/Bitkom/Publikationen/Stellungnahme-zum-Regierungsentwurf-NetzDG.html. Accessed 28 May 2018.

Bröckling M (2018) Ein NetzDG für Frankreich. https://netzpolitik.org/2018/ein-netzdg-fuer-frankreich/. Accessed 24 May 2018.

Bundesverband Digitale Wirtschaft e.V. (2017) Stellungnahme zum Entwurf eines Gesetzes zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken des BMJV vom 14. März 2017. https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Stellungnahmen/2017/Downloads/03302017_Stellungnahme_BVDW_RefE_NetzDG.pdf?__blob=publicationFile&v=2. Accessed 28 May 2018.

Cheung A, Schulz W (2018) Reputation Protection on Online Rating Sites. Stanford Law and Technology Journal (forthcoming).

Dewey C (2016) How we're unwittingly letting Robots censor the Web. https://www.washingtonpost.com/news/the-intersect/wp/2016/03/29/how-were-unwittingly-letting-robots-censor-the-web/?noredirect=on&utm_term=.e1efcfb456a2. Accessed 28 May 2018.

Digitale Gesellschaft e.V. (2017) Stellungnahme zum Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz für ein Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken. https://digitalegesellschaft.de/wp-content/uploads/2017/03/Stellungnahme_DigiGes_NetzDG.pdf. Accessed 28 May 2018.

Elkin-Koren N (2011) Mapping the Frontiers of Governance in Social Media. Draft Paper prepared for the 1st Berlin Symposium on Internet and Society, 25-27 October 2011.

Federrath H (2015) Geoblocking und die Möglichkeiten der Technik. ZUM 59/12:929-932.

Gasser U, Schulz W (2015) Governance of Online Intermediaries – Observations From a Series of National Case Studies. https://ssrn.com/abstract=2566364. Accessed on 28 May 2018.

German Bar Association DAV (2017) Stellungnahme des Deutschen Anwaltsvereins durch die Ausschüsse Informationsrecht und Strafrecht – Regierungsentwurf des Bundesministeriums der Justiz und für Verbraucherschutz – Entwurf eines Gesetzes zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG). https://www.cr-online.de/DAV_SN_41-2017.pdf. Accessed 28 May

[39] In its Google Spain decision (C-131/12) the CJEU purposefully limited the deletion obligation to the search results on European search queries, leaving open the possibility of still finding the results when using, for example, Google.com.
[40] See for example the work of Susan Benesch, especially the Dangerous Speech Project, https://dangerousspeech.org/.
[41] For early encouragement of such ideas, see Lide C 1996 and Perritt H 2000. New perspectives cf. Cheung/Schulz 2018. For the advantages of modes of self-regulation see Article 19 2017, 11.

2018.

German Federal Ministry of Justice and Consumer Protection (2017) Löschung von strafbaren Hasskommentaren durch soziale Netzwerke weiterhin nicht ausreichend. http://www.bmjv.de/SharedDocs/Pressemitteilungen/DE/2017/03142017_Monitoring_SozialeNetzwerke.html. Accessed 24 May 2018.

Global Network Initiative (2017) Proposed German Legislation threatens Free Expression around the World. https://globalnetworkinitiative.org/proposed-german-legislation-threatens-free-expression-around-the-world/. Accessed 29 May 2018.

Goel S, Anderson A, Hofmann J, Watts D (2016) The Structural Virality of Online Diffusion. Management Science 62(1)

Grabenwarter C (2017) Art. 5. In: Maunz/Dürig (eds) Grundgesetz-Kommentar. Beck, München.

Internet & Jurisdiction Policy Network (2018) Data & Jurisdiction Work Plan. https://www.internetjurisdiction.net/uploads/pdfs/Papers/Data-Jurisdiction-Work-Plan.pdf. Accessed 28 May 2018.

Iqbal F, Marrington A, Hung P, Yankson B (2018) A Study of Detecting Child Pornography on Smart Phone. Conference Paper for the International Conference on Network-Based Information Systems. https://www.researchgate.net/publication/319268051_A_Study_of_Detecting_Child_Pornography_on_Smart_Phone . Accessed May 28 2018.

Kaye D – Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression – Office of the High Commissioner for Human Rights (2017) Open letter to the German Chancellor concerning the draft law "Netzwerkdurchsetzungsgesetz" (OL-DEU-1-2017). http://www.ohchr.org/Documents/Issues/Opinion/Legislation/OL-DEU-1-2017.pdf. Accessed 28 May 2018.

Köver C (2016) Facebook verrät, wie viele Hasskommentare es wirklich löscht. https://www.wired.de/collection/life/facebook-verraet-wie-viele-hasskommentare-wirklich-geloescht-werden. Accessed 23 May 2018.

Ladeur K-H, Gostomzyk T (2017) Gutachten zur Verfassungsmäßigkeit des Entwurfs eines Gesetzes zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG) i.d.F. vom 16. Mai 2017 – BT.Drs. 18/12356 – Erstattet auf Ansuchen des Bitkom. https://www.cr-online.de/NetzDG-Gutachten-Gostomzyk-Ladeur.pdf. Accessed 28 May 2018.

Lee D (2017) Germany's NetzDG and the Threat to Online Free Speech. https://law.yale.edu/mfia/case-disclosed/germanys-netzdg-and-threat-online-free-speech. Accessed 29 May 2018.

Lide C (1996) ADR and Cyberspace: The Role of Alternative Dispute Resolution in Online Commerce, Intellectual Property and Defamation. Ohio St. J. on Disp. Resol. 12:1, 193-222.

Organization for Security and Co-operation in Europe (2017) Legal Review of the Draft Law on Better Law Enforcement in Social Networks. https://www.osce.org/fom/333541. Accessed 28 May 2018.

Paal B (2018) Art. 17. In: Paal B, Pauly D (eds) Beck'sche Kompakt-Kommentare Datenschutzgrundverordnung Bundesdatenschutzgesetz. Beck, München

Perritt H (2000) Dispute Resolution in Cyberspace: Demand for New Forms of ADR. Ohio St. J. on Disp. Resol. 15.3, 675-703.

Pötzsch S (2010) Einfluss wahrgenommener Privatsphäre und Anonymität auf Forennutzer. In: Ziegler J, Schmidt A (ed) Mensch & Computer 2010: Interaktive Kulturen. Oldenbourg Verlag, München, p 129-138

Reporter ohne Grenzen (2017) Stellungnahme zum Entwurf eines Gesetzes zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken der Fraktionen von CDU/CSU und SPD (BT DS 18/12356) zur Anhörung im Rechtsausschuss des Bundestages am 19. Juni 2017. https://www.reporter-ohne-grenzen.de/fileadmin/Redaktion/Internetfreiheit/20170619_Stellungnahme_oeA_BT-Rechtsausschuss_NetzDG_Reporter_ohne_Grenzen.pdf. Accessed 28 May 2018.

Roßnagel A, Bile T, Friedewald M, Geminn C, Heesen J, Karaboga M, Krämer N, Kreutzer M, Löber L, Martin N, Nebel M, Ochs C (2017) Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt: Policy Paper Das Netzwerkdurchsetzungsgesetz. http://www.forum-privatheit.de/forum-privatheit-de/publikationen-und-downloads/veroeffentlichungen-des-forums/positionspapiere-policy-paper/Policy-Paper-NetzDG.pdf. Accessed 28 May 2018.

Rötzer F (2017) Russland kopiert deutsches Netzwerkdurchsetzungsgesetz. https://www.heise.de/tp/features/Russland-kopiert-deutsches-Netzwerkdurchsetzungsgesetz-3773642.html. Accessed 23 May 2018.

Spindler G (2017) Legal Expertise commissioned by BITKOM concerning the notified German Act to Improve

Enforcement of the Law in Social Networks. https://www.bitkom.org/noindex/Publikationen/2017/Sonstiges/Legal-Expertise-Official-2-0.pdf. Accessed 28 May 2018.

Theil S (2018) The German NetzDG: A Risk Worth Taking?. https://verfassungsblog.de/the-german-netzdg-a-risk-worth-taking/. Accessed 29 May 2018.

Wang J (2018) Regulating Hosting ISPs' Responsibilities for Copyright Infringement. Springer, Singapore.