Organization for Security and Co-operation in Europe
Office of the Representative on Freedom of the Media

Legal Review of the Draft Law on Better Law Enforcement in Social Networks

Prepared by Prof. Dr. Bernd Holznagel, LL.M.
Commissioned by the Office of the OSCE Representative on Freedom of the Media

May 2017

I. Subject Matter of Assessment

The analysis' subject is the draft bill of the "Draft Act improving law enforcement on social networks" (Network Enforcement Act – NEA) prepared by the German Federal Ministry of Justice and Consumer Protection. The draft was notified to the European Commission (notification number 2017/127/D) on 27 March 2017. The investigation contains:

- A comparison between the draft provisions and the guidelines of international law (international standards) concerning media and freedom of information as well as the relevant OSCE commitments shall be made.
- Draft provisions that are incompatible with media and freedom of information principles (free flow of information) shall be identified.
- Proposals for possibilities to harmonise the legislation with the above mentioned international standards shall be put forward.

II. Research Issue

The growing dissemination of hate crime and other criminal content especially in social networks like Facebook, YouTube and Twitter triggered the NEA draft. In 2016 the Federal Office of Justice (Bundesamt der Justiz) published its annual statistics[1], which showed that in 2015 the number of officially recorded hate crimes with right-wing extremist and xenophobic content on the Internet had tripled compared to 2013 and 2014. Additional surveys reveal a large dark field. In a representative online-survey of German citizens, initiated by the Media Authority of North Rhine-Westphalia (Landesanstalt für Medien Nordrhein-Westfalen, LfM)[2], two-thirds of the users stated that they had already been confronted with hate messages in social networks, Internet forums or blogs. In that survey "hate speech" was defined as comments aimed against a specific person or a specific group of people due to their ethnic or religious affiliation, their national origin, sex, age, disability or sickness, that included statements of hatred, threats of or incitements to violence. Looking at the group of 14- to 24-year-old adolescents 91 percent mentioned corresponding experiences. Roughly every third respondent felt intimidated by such comments.

The effects do not refer to media users only. A survey published in April 2017 by the Council of Europe, based on a sample of 940 journalists reporting from the 47 member states of the Council of Europe and Belarus, shows the significant impact of intimidating interference in journalistic work. Fear of psychological violence (60%), cyberbullying (57%) and intimidation by individuals (51%) or interest groups (45%), and even physical violence (41%) influences journalistic work and leads to self-censorship. Many journalists felt compelled to tone down

---

The author thanks Maximilian Hemmert-Halswick for preparing the manuscript and Sirin Spindler for translation work.

1 https://www.bundesjustizamt.de/DE/Themen/Buergerdienste/Justizstatistik/Straftaten/Strafrechtspflege_node.html.

2 *Forsa*, Ehtik im Netz, Hate Speech, 2016, http://www.lfm-nrw.de/fileadmin/user_upload/lfm-nrw/Service/Veranstaltungen_und_Preise/Medienversammlung/2016/EthikimNetz_Hate_Speech-PP.pdf.

controversial stories (31%), withhold information (23%) or abandon stories altogether (15%).[3] Furthermore, online harassment has a clear gender-bias and thus can be especially harmful to women. In 2016 the Guardian commissioned a research project concerning the users' comments on its website since 2006. Regardless of what the article was about, articles written by women attracted more abuse than those written by men. Eight out of the ten most abused writers were women, the two men were black.[4] It is self-evident, that this can have a chilling effect on internet communication and journalism.

The Ministry of Justice concludes that if hate crimes are not combated properly, "they pose a massive threat to peaceful living in a free, open and democratic society."[5]

Apart from that, the experiences of the United States (US) 2016 presidential election[6] have lead Germany to prioritize the combat against punishable "Fake News" in social networks.[7] There is also the fear that such allegedly journalistic contents are generated by bots, which create artificial traffic through automated communication systems. As a result certain topics are prioritized by the networks algorithm, that in reality are not that popular.[8] The use of bots has been documented in the Brexit-debate or the US 2016 presidential election.[9] In Germany, fake news with xenophobic content spreading rumors and false alarms, which deliberately provoke resentment against foreigners and refugees,[10] have been widely documented[11].

III. Verification standards

1. Problem setting in the light of the leading principles of the OSCE

Freedom of expression and communication are fundamental values in the scope of the OSCE. As early as in the Final Act of the Conference on Security and Co-operation in Europe on 1. August 1975 the signatory states established the importance of information distribution and the media's fundamental role for democracy. Their aim was "to facilitate the freer and wider dissemination

---

3 *Clark/Grech*, Journalists under Pressure. Unwarrented interference, fear and self-censorship in Europe, 2017, https://wcd.coe.int/ViewDoc.jsp?p=&id=2456911&Site=DC&BackColorInternet=F5CA75&BackColorIntranet=F5CA75&BackColorLogged=A9BACE&direct=true.

4 *Gardiner et. al.*, The dark side of Guardian comments, https://www.theguardian.com/technology/2016/apr/12/the-dark-side-of-guardian-comments.

5 Explanatory statement, p. 10.

6 For example: https://www.buzzfeed.com/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook?utm_term=.sxL44PBgJn#.va7GGEveQ0; or: http://www.cbsnews.com/news/fake-news-macedonia-teen-shows-how-its-done/.

7 The ARD (consortium of public broadcasters in Germany) launched the anti-fake news portal "Faktenfinder" on 3 April 2017, which is to clarify how to recognize and deal with fake news, http://faktenfinder.tagesschau.de/.

8 See the hearing in the *Committee on „Digital Agenda"*, Deutscher Bundestag, on Fake News, Social Bots, Hacks und Co. Manipulationsversuche demokratischer Willensbildungsprozesse im Netz vom 25. Januar 2017, p.1 , http://www.bundestag.de/blob/489968/4bb0047446b18c724f27cf23aec24c26/a-drs-18-24-124-data.pdf.

9 *Hartmann*, MMR-Aktuell 2016, 382486.

10 http://www.bundestag.de/blob/489968/4bb0047446b18c724f27cf23aec24c26/a-drs-18-24-124-data.pdf, p. 3.

11 See for example: http://hoaxmap.org/.

of information of all kinds, to encourage co-operation in the field of information and exchange of information with other counties".[12] This principle was confirmed in the outcome documents of the following meeting.[13] Moreover, the participating countries affirmed that everyone has the right to freedom of expression including the right of communication. This right embodies freedom of expression and freedom of receiving and sending messages and ideas without interference of the public authorities and beyond national borders.[14] The OSCE states that restrictions of those freedoms are permissible only if they are prescribed by law and are necessary in a democratic society.[15]

On the other hand, it is one of the no less important objectives of the OSCE to oppose "manifestations of intolerance, and especially of aggressive nationalism, racism, chauvinism, xenophobia and anti-Semitism" and it "will continue to promote effective measures aimed at their eradication".[16] For "these phenomena run directly counter to the principles and commitments of the OSCE". This includes the fight against hate speech[17], whereby a *three-fold target direction* must be followed.

First and foremost, measures have to be designed to protect the *individual's personal rights*. Computer screens are acting as barriers between perpetrators and victims and seem to reduce the sensitivities that exist in face-to-face interactions.

Stigmatization effects, however, can not only violate personal integrity and dignity. They also have a *harmful impact on society* as a whole. For the spreading of hatred and prejudice "can lead to violence, secessionism by the use of force and ethnic strife".[18] Hate speech develops special dangers by its character as a "crime of messages". The polarization of public opinion on the Internet is leading to the escalation of communication as a whole.[19] Statements directed against social groups, such as migrants, refugees, people with disabilities, members of certain religions, homeless people, gays, lesbians or transgender persons even have the potential to carry over into the physical world. Attacks by third parties can be initiated or supported. If, as a result, the public mood is heated up, a *threat to public peace* may arise. Europe has experienced these mechanisms repeatedly, particularly in the thirties.

---

12 Art. 2. Documents of the OSCE are reprinted in: OSCE, Commitments – Freedom of the Media, Freedom of Expression, Free Flow of Information, Conference on Security and Co-operation in Europe (CSCE) and Organisation for Security and Co-operation in Europe (OSCE) 1975-2012, 2nd edition, 2013.

13 Third Follow-up Meeting to the Helsinki Conference on 15 January 1989 in Vienna, point. 34.

14 Copenhagen Meeting of the Conference on the Human Dimension of the CSCE on 29 June 1990, 9.1.

15 Oslo OSCE Seminar of Experts on Democratic Institutions, 15 November 1991, point II.26.

16 Budapest Document: Towards a Genuine Partnership in a New Era, on 5/6 December 1994, point 25.

17 Tenth Meeting of the Ministerial Council on 7 December 2002 in Porto, Rn. 21.7; Decision of the Eleventh Meeting of the Ministerial Council on 2 December 2013 in Maastricht, Decision No. 4/03 (Tolerance and Non-Discrimination).

18 Document of the Fourth Meeting of the CSCE Council of Ministers, 30 November/1 December 1993 in Rome, point 1, 2.

19 *Bock/Harrendorf*, „Strafbarkeit und Strafwürdigkeit tatvorbereitender computervermittelter Kommunikation", ZStW 2014, 337 (379).

Thirdly because of the aforementioned intimidation effects hate communication is associated with a *serious threat to freedom of expression* and unhindered communication itself. For the affected persons or social groups tend to "self-censorship" they can no longer fully exercise their right to freedom of expression.

Consequently, the legal order is faced with the difficult task of balancing these conflicting interests.

2. Securing and limiting freedom of expression and information in international and European law

The first approaches to a human right to freedom of expression and information are found in Article 19 of the Universal Declaration of Human Rights of 1948. There is the right to collect, receive and disseminate messages and ideas through every means of expression and independent of borders. The Universal Declaration of Human Rights was then issued as a *non-committal* recommendation of the UN General Assembly.[20] The right to freedom of expression and information has also been found in Article 19 of the 1966 International Pact on Civil and Political Rights. The pact now applies to 167 states. Germany ratified it in 1973. The pact is binding international law. However, since there is a *lack of effective enforcement mechanisms* the practical importance of this document has remained small.[21]

At the European level, freedom of information and expression is anchored in Article 11 of the EU Charta of Fundamental Rights (ECHR). However, the ECHR applies only to the Member States, such as Germany, "in implementing the law of the Union". It thus applies in all cases where a Member State transposes a European directive into national law.

The most important legal provision in this context is Article 10 (1) of the ECHR as that the ECHR is binding federal law in Germany. According to the Görgülü decision of the Bundesverfassungsgericht (Federal Constitutional Court)[22] it must be taken into account when interpreting national fundamental rights.

In all these documents, however, freedom of expression and information is not guaranteed limitless. *Restrictions are justified* if they are set by law, serve a legitimate aim and are proportionate. In defining the legitimate legislative objective for a measure which interferes with the protection of freedom of expression and/or information, the States are given a wide margin of discretion.

With regard to combating hate crimes, there is no doubt that this objective is ranking high among the EU and its Member States and that it is part of established legal traditions. The importance of the implementation of this objective is demonstrated by the fact that the EU Council of Ministers has addressed this issue in a Council Framework Decision (2008/913/JHA)

---

20 *Fink/Cole/Keber*, Europäisches und Internationales Medienrecht, 2nd Edition, 2008, 211.

21 *Ibidem*, 211.

22 http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2004/10/rs20041014_2.bvr148104.html.

of November 28th 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law made the following recommendation: Each Member State shall take the necessary measures to ensure that racism and xenophobia is punishable by effective, proportionate and dissuasive criminal penalties (Art. 3).

The expression of hatred and racist prejudice or xenophobia on the Internet must – like any other expression – be measured against Article 10 (1) ECHR, taking into account not only its limitations but also its guaranties. The provision protects even insane or unfounded opinions and prejudices, regardless of the means by which the opinion is disseminated or the access to information sought. As far as the (penal) law sets up limitations in order to protect third parties, State security or the public safety, it is necessary to investigate whether this is legitimate and whether the principle of proportionality is respected.

3. The special problem of intermediaries

The liability of communication agents and social networks poses a special problem, because they cannot necessarily claim to exercise the right to freedom of speech. Article 10 (1) of the ECHR presupposes, first of all, that there is an opinion *expressed*. The content provider is *responsible for his or her own content* and opinion. Communication agents can only refer to freedom of speech, if they actively express an opinion. That is the case only if they themselves make content available, select it, or moderate the communication. The host, who by moderating, for example a discussion forum, takes responsibility has certain obligations. In order to effectively limit hate crimes and the infringement of third-party rights, moderating hosts are, to a certain extent, subject to monitoring and deleting duties, in accordance with the jurisprudence of the ECHR.[23]

Intermediaries who transmit information created by a user or a subscriber only in a *technical way* or simply provide access to a communication network, neither express an opinion nor participate in the process of opinion-forming. They merely create the necessary prerequisites for others to make use of the freedom of expression. In this case, the communication agents cannot refer to the right to freedom of expression. They are acting within the scope of their economic profession. Deletion and blocking obligations for such platform operators are therefore an intervention in their economic interests and freedoms, but they do not act in order to enforce Article 10 of the ECHR.[24]

However, deletion and blocking obligations for intermediaries can have an adverse effect on the users' communication process. Only, these effects do not manifest themselves in the relationship between State and citizens. The State does not prohibit the citizens' freedom of expression. The restrictions have a de-facto-effect on the relationship of one citizen (operator of a social

---

23 Delfi AS v. Estonia (No. 64569/09, 1 October 2015), Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary (No. 22947/13, 2 February 2016), Phil against Sweden, (No. 74742/13, 9 March 2017).

24 Explanatory statement, p. 22.

network) to other citizens (users of a social network), because the network operators are given State limitations for the design of their business model.

The validity of fundamental rights in the citizen-to-citizen relation is controversial. In the United States in particular, fundamental rights are often understood as mere defense rights of citizens against State interference. In European legal traditions, an *objective-legal understanding of fundamental rights* is prevalent. In German constitutional law tradition fundamental rights have a so called "radiation effect" on the entire legal system. The constitutional court demands that the communication freedoms are also observed in the shaping of the relationship between the citizens. The State has an active obligation to protect, that can lead to an adjustment of the private law standards similar to the constitutional binding of the state. Such protection of private communications is particularly appropriate when private companies are providing the framework conditions for public communications and are thus placed in functions, which, like the provision of postal and telecommunication services, were previously assigned to the State as the task of services of general interest.[25]

IV. Control models and weighing processes in "notice and take down"

Various models have been developed to balance the relationship between unrestricted communication, providing a nonviolent environment for the free exchange of opinions, protection of personality rights, and the preservation of public peace. The task is to hinder the distribution of racist, xenophobic and anti-Semitic content on the Internet without affecting the freedom of expression too much.

1. The OSCE guidelines

The OSCE strives to find best practice in limiting violating communication.[26] Regarding the possibility of taking advantage of the intermediaries, four international Special Rapporteurs on freedom of expression[27] recently released a Joint Declaration on freedom of expression, "fake news", disinformation and propaganda.[28] The declaration is *not a binding legal instrument*. It lays out standards on disinformation and propaganda, methods by which the State could create an enabling environment for freedom of expression and emphasizes the particular roles played by digital intermediaries. The most important regulations affecting digital intermediaries are:

> *General Principles*
>
> Intermediaries should never be liable for any third party content relating to those services unless they specifically intervene in that content or refuse to obey an order adopted in accordance with

---

25 BVerfG, Urteil vom 22. Februar 2011 – 1 BvR 699/06 –, point 59, juris.

26 Annex to Decision No. 12/04 Permanent Council Decision No. 633.

27 United Nations Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights Special Rapporteur on Freedom of Expression and Access to Information.

28 https://www.article19.org/resources.php/resource/38653/en/joint-declaration-on-freedom-of-expression-and-%E2%80%9Cfake-news%E2%80%9D,-disinformation-and-propaganda.

due process guarantees by an independent, impartial, authoritative oversight body (such as a court) to remove it and they have the technical capacity to do that.

State mandated blocking of entire websites, IP addresses, ports or network protocols is an extreme measure which can only be justified where it is provided by law and is necessary to protect a human right or other legitimate public interest, including in the sense of that it is proportionate, there are no less intrusive alternative measures which would protect the interest and it respects minimum due process guarantees.

Standards on Disinformation and Propaganda
Criminal defamation laws are unduly restrictive and should be abolished. Civil law rules on liability for false and defamatory statements are legitimate only if defendants are given a full opportunity and fail to prove the truth of those statements and also benefit from other defences, such as fair comment.
Enabling Environment for Freedom of Expression
States have a positive obligation to promote a free, independent and diverse communications environment, including media diversity, which is a key means of addressing disinformation and propaganda.

2. The E-Commerce-Directive

Legally binding provisions for the Member States of the European Union are Articles 14 and 15 of the Directive 2000/31/EC of the European Parliament and of the Council of June 8th 2000 on certain legal aspects of information society services, in particular electronic commerce, in the European Single Market. The provisions read as follows:

Article 14 - Hosting

1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the *service provider is not liable* for the information stored at the request of a recipient of the service, *on condition* that:

(a) the provider *does not have actual knowledge* of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or

(b) the provider, *upon obtaining such knowledge or awareness, acts expeditiously to remove* or to disable access to the information.

2. Paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider.

3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information.

Article 15 - No general obligation to monitor

> 1. Member States *shall not impose a general obligation* on providers, when providing the services covered by Articles 12, 13 and 14, *to monitor* the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.

So far, the requirements of the Directive have had an effect on the legislative procedure in Germany as a regulation in a preliminary draft, which obliged network operators to "take effective measures against the re-storage of the unlawful content", has been deleted without substitution. This would have resulted in the host provider's obligation to monitor the system and actively seek out content, as prohibited by the directive.

The other requirements of the Directive, known as "notice and take down", can be defined by the Member States. The Union has so far refrained from regulating clear procedural standards or sanctions. Against this background, *various control models* have developed:

a) The Swedish model

In May 1998 the Swedish parliament passed the Act on Responsibility for Electronic Bulletin Boards[29]. The law provides for sanctions for network operators if they do not eliminate certain clearly legally infringing content intentionally or due to gross negligence:

> ***Article 5***
>
> If a user submits a message to an electronic bulletin board, the supplier must *remove the message*, or in other ways make it inaccessible, if
>
> 1. the message content is obviously such as is referred to in the *penal code*, Section 16, article 5, about instigation of rebellion, Section 16 article 8 about racial agitation, Section 16 article 10 about child pornography, Section 16 article 10 about illegal description of violence, …
>
> In order to be able to fulfill the obligation …, the supplier is allowed to check the content of message in the service. These obligations and rights also apply to those who have been given the task, by the supplier, to supervise the service.
>
> *Article 7*
>
> A person who intentionally or through gross negligence violates article 5, first clause, is *sentenced* to a fine or a prison sentence of not more than six month, or, if the crime is severe, to prison in not more than two years. Slight infringement should not be punished."

[29] Swedish Code of Statutes, SFS 1998, p. 112.

The model is characterized by a combination of a strict deletion obligation with a restrictive selection of the incriminated content. For example libel and fraud are not covered. It also provides for a clear standard of evidence (only "obvious" infringements have to be removed) and a corresponding limitation of the liability to gross negligence.

b) The model of the Federal Court of Justice (Bundesgerichtshof)

In Germany, the Federal Court of Justice (Bundesgerichtshof, short: BGH) has dealt with the obligations of host providers in a series of decisions. The court states, that anyone who, even without being a perpetrator or a participant, *contributes* willingly and adequately to the detriment of another person's rights, is obliged to refrain from that "disturbance".[30] This also applies to the mere host provider, because without his (technical) contribution the user-generated, incriminated content could not be spread (further). But the court does not impose the full liability for the illegal content to the host provider. It just *stipulates an obligation to eliminate the "disturbing contend"* in order to put an end to the ongoing violation of private rights. This obligation exists within the limits of reasonable monitoring according to the following procedure:

A host provider is *not obligated* to check the contributions made by the users for possible infringements before uploading. However, he is responsible for the removal if he is made aware of an infringement. This presupposes that the *notification* of the person claiming a violation of his or her rights is so concrete that the legal offense can be affirmed on the basis of the allegations of that person only.[31]

The complaint then is to be forwarded to the person responsible for the post. If the *content provider* (the perpetrator) fails to give a justifying statement within an appropriate period of time, the complaint must be accepted and the contested entry must be deleted. If the person responsible for the blog answers to the complaint in a substantiated manner that leads to legitimate doubts, the provider is *obliged to re-communicate* this to the person concerned. If necessary, the provider may claim proof of the alleged infringement. If no further statement of the concerned person follows and necessary evidence is not delivered, no further examination or measures are required. If the statement of the concerned person and the submitted evidence does reveal an unlawful violation of the personality right, the rejected entry shall be deleted.[32]

In contrast to the Swedish model, this model intends to eliminate all violations of personal rights, but sets up a clear procedure and standards for obtaining statements. In the end it is still the host provider, who – taking into account any possible statements and presented evidence – stays responsible for balancing interests and making a decision. If the provider does not comply with the wish of the complaining person to delete, he or she is free to sue the host provider for elimination under Section 1004 of the German civil code.

---

30 BGH MMR 2009, 752-754, MMR 2011, 172-174, BGH, Urteil vom 30. Juni 2009 – VI ZR 210/08 –, juris.
31 BGHZ 191, 219-228, point 21.
32 BGHZ 191, 219-228, point 27.

3) The Model of Sec 512 of the Millennium Copyright Act

The US-Online Copyright Infringement Liability Limitation Act (OCILLA) provides another, more formalized way – without any substantive test obligations.[33] It consists of a *three-phases model*, which is intended only for copyright infringements, but can – in principle – also be transferred to any other legal violation:

A service provider, who does neither have actual knowledge nor is aware of facts or circumstances which present an infringing activity is not liable. Upon *notification* of an infringement the provider has to act expeditiously to remove or disable access to the material. To be effective a notification of claimed infringement must inter alia contain a written communication providing a physical or electronic signature of a person authorized to act and sufficient information on the claimed infringement.

The provider then takes reasonable steps promptly to notify the subscriber that the material has been removed or made inaccessible. The subscriber then can file a *counter notification*, which also must be a written communication including a physical or electronic signature of the subscriber, the subscriber's name, address, and telephone number, and a statement that the subscriber consents to jurisdiction. Upon receipt of the counter notification the provider promptly provides the person who provided the first notification with a copy of the counter notification, and informs the person that it will replace the removed material or cease disabling access to it in 10 business days.

The person who had claimed the infringement then has the possibility to file a lawsuit, otherwise the provider will put the material back in place.

This model, on the one hand, frees the provider from any obligation to check the content and on the other hand ensures an immediate response to the complaint. It takes precaution to restore the deleted content if the user demands this and renounces its anonymity, thus opening the way to court for the parties involved.

This seems appealing at first sight, but its transfer from the field of copyright to other infringements would have significant impact especially on ongoing political discourse in the internet and thus on freedom of expression. In fact, it presupposes a presumption of legal infringement in all cases notified and leads (at least temporarily) to the elimination of the content until the counter notification is received.

In addition, it would be necessary to clarify which authority should be notified in case of a disturbance of public peace. Otherwise private individuals would be forced into the role of auxiliary sheriffs.

---

[33] https://www.gpo.gov/fdsys/pkg/USCODE-2010-title17/html/USCODE-2010-title17-chap5-sec512.htm.

V. Legislative history and goal of the NEA

1. The history of the proposed law

In the explanatory statement, the Ministry of Justice refers to its earlier efforts to deal with that problem, which in the end did not have the aspired effect. Because of the increasing prevalence of hate crime on Facebook, YouTube and Twitter, the Ministry of Justice and the management of those social platforms founded a task force to collaboratively tackle these problems.[34] The *companies of the task force* pledged to implement user-friendly mechanisms to denounce critical and supposedly criminal posts. An integral part of this voluntary self-commitment was a fast handling of notifications, an effort which aims towards auditing and removing potentially criminal content *within 24 hours*.

These voluntary self-commitments led to first improvements.[35] Facebook claimed having deleted 100.000 hate speech postings in September 2016.[36] The German government, however, sees the need to implement stricter rules. Jugendschutz.net, the joint competence center for the protection of minors on the internet at federal and State level[37] checked the deletion practices of social networks in January/February 2017 and showed that not all social networks were likewise committed to deal with user complaints in a serious manner. The monitoring report revealed that of all posts of criminal content, 90% were deleted from YouTube, 39% from Facebook, and a mere 1% from Twitter.[38] These statistics suggest that a majority of posts qualifying as criminal are not deleted expeditiously, if at all.

At the same time, Justice Minister, Heiko Maas, urged the operators of social networks to enhance the transparency concerning the handling of complaints by implementing mandatory reporting obligations. It often happens that platforms have difficulties differentiating between xenophobic posts and journalistic articles about xenophobia.[39]

2. Objective and approach

The draft does not take up any of the models presented above. Instead it is based on a steering approach that has been successfully used in recent years to enforce legal standards in economic enterprises and in the financial market. Companies are required to develop measures of corporate *compliance* within a legal framework and according to certain standards. These standards normally include an obligation to provide effective procedures, to take sanctions in the event of an infringement, and to report on them. As an example the German Corporate Governance Code sets out the most important legal requirements for the management and

---

34 https://www.tagesschau.de/inland/facebook-177.html.

35 http://www.faz.net/agenturmeldungen/dpa/maas-zu-hass-im-netz-lage-ist-besser-aber-noch-nicht-gut-14453944.html.

36 Ibidem.

37 Jugendschutz.net is no public authority, but has a legal mandate laid down in the Interstate Treaty for the Protection of Minors on the Internet (JMStV).

38 Explanatory statement, p. 1.

39 http://www.zeit.de/digital/intepointet/2015-12/facebook-heiko-maas-hetze-hasskommentare.

supervision of listed companies. To this extent, it has an informational character. It also provides recommendations and suggestions for good and responsible corporate governance (compliance). Pursuant to Section 161 of the German Stock Corporation Act (AktG), the Management Board and Supervisory Board of listed companies annually declare to what extent the recommendations have been complied with, which recommendations are not applied and why not. The NEA proposes similar compliance regulations for social networks.

Social networks are to be encouraged to speed up the processing of complaints, especially of their users. The blocking and deleting obligation referred to does *not* result from the NEA itself. *It is placed before it and justified in the general laws* in accordance with the jurisprudence of the BGH, which is presented above.[40] In addition to an effective complaint management system, a statutory reporting obligation on dealing with hate criminality and other criminal contents as well as the appointment of a domestic sales representative are planned. Violations of these obligations may be punished with fines against the company and other supervisors.

VI. Scope of application

Section 1 of NEA outlines terms to limit and specify the scope of application.

1. Telemedia service provider

Pursuant to Section 1 (1) NEA, the provisions of the NEA apply to "telemedia service providers which, for profit-making purposes, operate internet platforms that enable users to exchange and share any content with other users or to make such content available to the public". According to the explanatory statement, platforms are included regardless of the form of communication. Targeted are platforms at which users can set content such as images, videos, text, and similar content.[41] According to the explanatory statement of the draft law the definition of social networks also covers the exchange of content with other users in a closed network community (gated community).[42] Also captured are messengers or instant messaging providers, as long as they provide the possibility to communicate in a larger, non-fixed group of people.[43] As to the most recent version of the explanatory statement of the German government, messengers or instant messaging providers are no longer explicitly mentioned.[44]

2. Exceptions for journalistic editorial offers and networks with less than 2 million users

Platforms with journalistic and editorial contents do not count as social networks in this sense. In the second Subsection, the applicability is limited to such social networks with more than 2 million registered users in Germany. According to the law's explanatory statement, "registered

---

40 See above section IV.2.b.
41 Explanatory statement, p. 18.
42 Explanatory statement, p. 11.
43 Explanatory statement, p. 19.
44 Gesetzesentwurf der Bundesregierung vom 21.04.2017, Bundesrats-Drucksache, p. 15.

users" are those who created an account using a German IP address.[45] The degree of user-activity as well as multiple accounts per person are irrelevant to the counting process. The creation of an account by using a non-German VPN would not be regarded as one of the 2 million, even if the actual creation locally took place in Germany.

3. Unlawful content

A central aspect of the draft is the notion of unlawful content. This is not a generally known concept of German law. Accordingly, Section 1 (3) NEA contains a legal definition: unlawful content is the content as defined in paragraph 1 (that is, content exchanged in social networks) that fulfils the elements of 24 individually listed offenses.

These can be subdivided into provisions on State security, offenses against public order and provisions on the protection of the personal honor (for details see the **Annex**).

The draft claims that, with its list of offenses, a clear distinction is made between criminal acts committed in social networks in general (including fraud) and "hate crimes" or criminal "fake news" in social networks.[46] The statement states that by this, the principles of legal certainty and proportionality are taken into account.[47]

In German criminal law doctrine, the criminal liability requires three elements which are: (1) the fulfilment of the offense, (2) unlawfulness and (3) guilt. The fulfilment of the offense consists of an objective component (actus reus) and a subjective component (mens rea, which can be willful intent, conditional intent or negligence). Unlawfulness means that no grounds of justification exist (for example self-defense or consent). The element of guilt is linked to the subjective conditions of the perpetrator, such as insight, maturity or insanity.

Unfortunately, the draft is indeterminate, if not contradictory, as to which elements are precisely necessary to establish "unlawful content". The draft-law itself suggests that "unlawful content" has to fulfill the complete legal definition of at least one of the offenses in the list (including the perpetrator's intent and the absence of justifying reasons)[48], whereas the explanatory statement states that only the objective facts and the unlawfulness of the content are relevant.[49] Clear seems only, that the network operator does not have to assess the element of guilt.

According to the justification of the draft law the definition of social networks also covers "the exchange of content with other users in a closed network community (gated community).[50] This broad interpretation will increase the difficulty of deciding whether a specific content is unlawful or not because some of the offenses require the content to be made accessible to the public (for details see the **Annex**). As it is *not easy* to recognize who has *access to the posted*,

---

45 Explanatory statement, p. 19.
46 Explanatory statement, p. 18.
47 Explanatory statement, p. 20.
48 *Buermeyer*, http://www.lto.de/recht/hintergruende/h/netzwerkdurchsetzungsgesetz-NEA-facebook-strafverfolgung-hate-speech-fake-news/.
49 Explanatory statement, p. 20.
50 Explanatory statement, p. 11.

shared or liked content, the inclusion of gated communities does not make it easier for the user to assess the question of unlawfulness beforehand. One can think of the privacy settings on Facebook. There one can make configurations that only a limited number of users have access to one's content. Due to the still existing uncertainties of such configurations, users can ultimately not be sure that the public effectively does not have access.

This could lead to a deletion of content without the user having expected it, even after thorough considerations before the post. Considering that criminal investigations then must be terminated because the necessary intention (mens rea) cannot be proven, this ambiguity could lead to a considerable widening of the scope of the law.

VII. Obligations of providers

The obligations of the NEA are intended to (merely) ensure that existing obligations according to general laws are complied with quickly and comprehensively. Neither are new contents to be punishable, nor are new deleting obligations to be introduced so far.

1. Handling of complaints by the network operators

One of the main obligations is the duty to put in place structures and procedures that effectively enable users to report unlawful contents.

Section 3 (1) NEA obliges the operators of social networks to maintain an effective and transparent procedure for dealing with user complaints about unlawful content. This process must be readily recognizable, directly accessible and constantly available.

a) Immediate knowledge and examination

Pursuant to Art. 3 (1) NEA, the procedure must ensure that the provider of the social network immediately takes note of the complaint and checks whether the content is unlawful and removes or blocks access to it. This regulation constitutes a concretization and supplementation of the principle "notice and take down", which is regulated in Section 10 of the Telemedia Act (Telemediengesetz – TMG).

A further duty is to remove or block access to a "manifestly" unlawful content within 24 hours on receipt of the complaint. This period may be extended after consultation with the law enforcement authority. This requires that the content has also been reported to the authority.

"Manifestly unlawful" according to the daft requires "no substantive testing" to establish unlawfulness, which means no in-depth examination is necessary to establish the unlawfulness within the meaning of Section 1 (3) NEA.[51] The *goal* is to remove evidence of hate crimes and glorifications of violence as soon as possible. Unless the content is "manifestly unlawful" (but still unlawful) the content shall be removed or blocked within 7 days after receipt of the complaint. This deadline is also intended to make it possible to obtain an opinion from the

[51] Explanatory statement, p. 23.

author or to consult external experts.[52] This is intended to prevent the network operator from rapidly ripping contents due to time pressure or in order to prevent a penalty payment. This could otherwise lead to unwanted "chilling effects".

Section 3 (2) No. 4 NEA obliges the network operators to secure the contents for the purpose of proof in the event of removal and to store them for this purpose for a period of ten weeks in Germany. The obligation to provide storage primarily serves law enforcement interests. A parallel law in the Telecommunications Act (Section 113b) also provides for a period of 10 weeks.

b) Obligation for Information and justification

In addition, the network operator must promptly inform both the complainant and the user of any decision and give reasons for their decisions. In social networks it is already common for complainants to be given a choice of possible reasons for the complaint. This type of reasoning is sufficient according to the legal basis. The purpose of this provision is to allow the applicant to take action against the non-deletion or the author against the deletion.

In addition to deleting the content of the original author, the network operator must also ensure that all copies of unlawful content are also removed or blocked.

c) Compulsory documentation

Pursuant to Section 3 (3) NEA, each complaint and measures that have been taken must be documented in Germany. The obligation to provide documentation is aimed at securing proof for a legal process concerning the legality of the removal of a stored content.

d) Supervision by the management

The handling of complaints must be supervised by the management of the social network through monthly checks. If an organizational deficiency is identified, it must be removed immediately. The staff responsible for the processing of complaints must be offered a training and advisory service by the management every six months. These trainings and consultations must be held in German.

The high-level monitoring of complaints by the management is to be emphasized here. This is intended to meet the social significance of the task.[53]

e) Monitoring by a designated body

The procedures can be monitored by a body commissioned by the Federal Office of Justice. According to the explanatory statement, this was so far Jugendschutz.net (German for youth

---

52 Explanatory statement, p. 23.
53 Explanatory statement, p. 24.

protection). On the basis of good experience so far, the authors of the draft law assume that this cooperation will continue.[54]

2. Reporting obligation

Apart from the obligation to properly process complaints, operators of social networks must produce a report in German explaining to what extent the obligations of the NEA have been met, which must be published in the Federal Gazette. The NEA describes in detail which aspects are required to be addressed by the report.

The report shall deal with the following aspects:

- general observations outlining the efforts undertaken by the provider of the social network to eliminate criminally punishable activity on the platform,
- a description of the mechanisms for submitting complaints relating to unlawful content and the criteria applied in deciding whether to delete or block unlawful content,
- the number of incoming complaints relating to unlawful content in the reporting period, broken down according to whether the complaints were submitted by complaints bodies or by users, and according to the reason for the complaint,
- organisation, personnel resources, specialist and linguistic expertise in the units responsible for processing complaints, as well as training and support of the persons responsible for processing complaints,
- membership of industry associations with an indication as to whether these industry associations have a complaints office,
- the number of complaints for which an external body was consulted in preparation for making the decision,
- the number of complaints in the reporting period that resulted in the deletion or blocking of the content at issue, broken down according to whether the complaints were submitted by complaints bodies or by users, and according to the reason for the complaint,
- the time between complaints being received by the social network and the unlawful content being deleted or blocked, broken down according to whether the complaints were submitted by complaints bodies or by users, according to the reason for the complaint, and according to the periods "within 24 hours"/"within 48 hours"/"within a week"/"at a later point",
- measures to inform the person who submitted the complaint, and the user for whom the content at issue was saved, about the decision on the complaint.

---

54 Explanatory statement, p. 24.

VIII. Monitoring, sanctions and entry into force

1. Person authorised to receive service in Germany

According to Section 5 NEA, providers of social networks are obliged to appoint a person authorized to receive service to the Federal Office of Justice, the public prosecutor's office and the competent court without delay. This is to ensure that there is a contact person available in administrative, criminal and civil proceedings. This duty explicitly applies to all social networks at home and abroad.[55] The background of this regulation is to enable a safe and fast intervention. An authorized delivery agent abroad cannot guarantee a corresponding level of safety and speed.

2. Penalties even if not committed in the country

Violations against certain obligations can lead to administrative fines of up to 50 Mio EUR. In principle, it is not subject to a fine to not carry out a deletion (fast enough). Instead, fines are imposed on behaviors which imply a general failure to implement the necessary structures to comply with the NEA:

1. failing to produce and publish the required report correctly, completely and in due time,
2. failing to provide and supply correctly and completely a procedure for dealing with complaints,
3. failing to monitor the handling of complaints,
4. failing to rectify organizational deficiencies in due time,
5. failing to offer training or support for the responsible personnel or
6. failing to name a person authorized to receive service in Germany in due time.

It should be stressed that the administrative offense can be punished even if the administrative offense it is not committed in Germany. For foreign companies, for example, it may be more practical to offer employee training abroad. According to the NEA, a failure to do so would lead to a fine.

3. Responsible authority

The responsible authority is the Federal Office of Justice. It is responsible for penalizing administrative offenses. In the imposition of fines, the Federal Office is entitled to *discretion*. The Federal Ministry of Justice, in agreement with the Federal Ministry of the Interior, the Federal Ministry of Economics and the Federal Ministry of Transport and Digital Infrastructure[56], substantiates this discretion by setting down guidelines.

---

55 Explanatory statement, p. 28.

56 The Federal Ministry of Transport and Digital Infrastructure was not included in the notification draft; it is only included in the latest version, Gesetzesentwurf der Bundesregierung vom 21.04.2017, Bundesrats-Drucksache, p. 4.

4. Preliminary ruling on the unlawfulness of a court

The Act provides sanctions for the deliberate or negligent violation of the duty to effectively handle the complaints under Section 3 (1), second sentence, and not for individual infringements. According to the explanatory statement that was part of the notification, however, the lack of due diligence in organization can be indicated by a single infringement. This has been change in the latest explanatory statement[57]: In *case of a one-time infringement*, the opposite shall be the case. It cannot generally be assumed that an effective procedure for dealing with complaints has not been put in place, as in that there are "systemic flaws".[58] In case of only isolated violations, which are not based on *systemic errors* in dealing with complaints, it should be noted that the *discretionary principle* of Section 47 (1) OWiG applies.[59] This change is reasonable because it stresses the compliance approach of the NEA.

If the Federal Office of Justice wishes to issue a decision relying on the fact that content which has not been removed or blocked is unlawful and this fact amounts to a *systemic error*, shall first obtain a judicial decision establishing such unlawfulness. This ruling is prerequisite for the imposition of a fine.

As a result, the Federal Office of Justice does not decide on the criminality of content in the dispute itself. According to the explanatory statement, this serves to comply with the principle of division of powers, according to which the courts are competent to decide whether or not content is "unlawful".[60]

According to Section 4 (5) sentence 5 NEA, this decision cannot be appealed. According to the explanatory statement, there is no need for this because the social network, in the event of a penalization by the court ruling, may challenge the penalty notice, in which the preliminary ruling is mandatory[61].

5. Entry into force of the law and transitional provisions

The NEA shall enter into force on the day following its announcement. The report on handling complaints must be prepared for the first time at the end of the second quarter following the entry into force. This is intended to give the social networks time to adapt to the reporting obligation.

The actual procedure for handling complaints must, however, be introduced within three months after the entry into force.

---

57 Gesetzesentwurf der Bundesregierung vom 21.04.2017, Bundesrats-Drucksache, p. 22.
58 Explanatory statement, p. 22.
59 Explanatory statement, p. 22.
60 Explanatory statement, p. 27.
61 Explanatory statement, p. 28.

IX. Model analysis

1. Choice of a compliance model

The regulatory approach taken in the NEA does not follow one of the existing regulatory models. It takes on an approach of encouraging social networks to develop a proper corporate compliance.
This innovative approach is strongly to be welcomed. If States have a positive obligation to promote a free, independent and diverse communications environment, they cannot simply refrain from any intervention in the communication process, but have to protect the communication processes from violence as well as from forms of formal censorship. A compliance-based approach has proved to be successful to regulate complex organizations in civil society in a flexible way using the potential of self-regulation.

However, the legislator must avoid "chilling effects" as far as possible and take into account the principle of proportionality. In this respect, the draft needs to be revised.

2. Restriction on offers which are actually harmful to the general public

a) Social network definition

The main focus of the public debate concerning the draft law and also of the Ministry of Justice's surveys undoubtedly lay on Facebook, Twitter and YouTube.[62] But the actual definition, as stated in the draft law (Section 1 (1) NEA), also includes some services that are usually not within the notion of social networks.

In first regard, this law applies to social networks such as Facebook and Twitter since they provide platforms to enable its users to share digital contents, and this being their main operating objective. Also messenger services like WhatsApp should be included since they also serve to a great deal as a medium to share digital contents. But the definition seems somewhat imprecise, misleading and too broad when it says "or make the contents accessible to the public" because an extensive approach could also include video chat services (Skype), file hosting services (Dropbox) and even one-click hosting services (Flickr, ImageShack). Asked in this regard, the Ministry of Justice denied the inclusion of web mailing services, and was also inclined to not include hosting services like Dropbox.[63] This *vagueness* in terms of the addressees of the obligations has already been heavily criticized in the German discussion.[64]

---

62 This can also be seen in the explanatory statement where only these 3 platforms are explicitly named.

63 *Reuter*, https://netzpolitik.org/2017/analyse-so-gefaehrlich-ist-das-neue-hate-speech-gesetz-fuer-die-meinungsfreiheit/.

64 *Härting*, http://www.cr-online.de/blog/2017/03/14/kurzer-rozess-fuer-die-meinungsfreiheit-entwurf-eines-netzwerkdurchsetzungsgesetzes/.

b) Definition of the term "journalistic-editorial"

Telemedia service providers offering journalistic or editorial content are not covered by the act. This exemption is necessary and correct. The draft mentions correctly, that those who do not merely "manage" the content of third parties technically are themselves protected in their freedom of expression. The legal requirements for such offers are contained in §§ 54 et seq. of the Broadcasting Interstate Treaty (Rundfunkstaatsvertrag).

Journalistic-editorial telemedia services require the intention to influence the process of the formation of public opinion.[65] This is the case if the service is given by professional journalists under recognition of ethical standards. Delimitation problems arise if a "private" blogger is responsible for the content. Can a platform claim to have "journalistic-editorial" contents, if they also provide chat or commenting tools? Is the ratio between journalistic-editorial content and other services and tools crucial in that case? The draft law does not contain a main-purpose criterion. The European AVMS Directive, currently under reform, is already suffering from such delimitation problems (see also ECJ-ruling "New Media Online"[66]). The draft leaves it to the courts to clarify what is meant by journalistic-editorial content. It would be appropriate here if, at least in its explanatory statement, the draft would establish a broad concept of journalism, including the mere moderation of discussions and chats.

c) Exceptions for small platforms

It is also a good approach to subjugate under the compliance requirements only platforms with a large number of users in order to not destroy the variety of smaller internet offers. Platforms with low user numbers and less turnover could not well manage the administrative burdens. Small networks would hardly be able to meet the far-reaching compliance requirements of the NEA.[67] On the other hand, the intensity of a possible infringement of rights is far lower on small platforms, which is why regulation can be dispensed with for reasons of proportionality. The formalization of the method of counting is also comprehensible for reasons of practicability.

3. Expeditious removal versus wide range of offenses

When designing the compliance system in detail, however, it becomes clear that the draft combines different elements of regulation without consistently transferring the associated, fundamental rights-securing precautions of the models. This deficiency leads in fact to disproportionate restrictions on freedom of expression, which go beyond the regulatory objective.

In contrast to the Swedish solution, which provides for an immediate cancellation obligation only for a few, particularly dangerous, manifestations of hate speech, the NEA refers to a large

---

65 VGH Baden-Württemberg, Urteil v. 25.03.2014, Az. 1 S 169/14, https://www.telemedicus.info/urteile/Internetrecht/1459-VGH-Baden-Wuerttemberg-Az-1-S-16914-journalistisch-redaktionell-gestaltete-Telemedienangebote.html.

66 http://curia.europa.eu/juris/liste.jsf?num=C-347/14.

67 Explanatory statement, p. 19.

number of possible infringements which, in the case of "manifest unlawfulness", are to be erased within 24 hours without an in-depth investigation. The draft specifies 24 concrete offenses, in order to outline a precise framework.

However all these offenses have in common that they can only be understood and interpreted in the light of freedom of expression. Whether or not a degrading utterance must be accepted in public discourse always depends on its *context*. All opinions enjoy fundamental rights protection and the protection of human rights, regardless of their assessment as well-balanced, polemical, provoking or repulsive [68]. Citizens are not legally obliged to personally share the values of the Constitution[69].

Freedom of expression, of course, must be rescinded when a statement touches human dignity.[70] According to the Federal Constitutional Court and the Federal Court of Justice the mere violation of the honor of a person is not to be classified as an attack on human dignity.[71] For the human dignity to be concerned, it is necessary that the attacked person is denied their right to live as an equal person in the State community and treated as a subordinate being. The attack must therefore be directed against the essence of personality that represents human dignity.

In the case of value judgements, the protection of the personality takes clear precedence over freedom of expression only if the statement proves to be a mere formal affrontation, abuse or abusive criticism. The Federal Constitutional Court has ruled that the terms "abuse" or "abusive criticism" have to be interpreted restrictively.[72] The mere degrading content of an utterance does not make it an abuse. An overstated or conspicuous critique does also not qualify.[73] On the contrary, an abuse is only assumed when, in an utterance, the focus is no longer on the dispute, but rather on the defamation of the person.[74] The further consideration must take into account all circumstances of the individual case and bring the impairment of freedom of expression into proportion with the impairment of the conflicting constitutional rights protected by law (the general right to privacy). It must be taken into consideration whether it is a private argument or an argument which is essentially relevant to the public.[75] In the latter, there is a presumption of the freedom of expression.[76]

Taking into account these principles, which are enshrined in German constitutional law, it is clear that a duty to promptly remove or block can only be considered in a few exceptional cases.

---

68 *Grimm*, „Die Meinungsfreiheit in der Rechtsprechung des Bundesverfassungsgerichts“, NJW 1995, 1697.
69 BVerfG, Beschluss vom 04.02.2010 - 1 BvR 369/04, NJW 2010, 2193.
70 BVerfG, NJW 1987, 2661 (2662).
71 BGH, NJW 1989, 1365; BVerfG, NJW 2010, 2193.
72 *Ohly*, in: Ohly/Sosnitza, Commentary on the Unfair Competition Act (Gesetz gegen den unlauteren Wettbewerb), 2015, no. 1/17.
73 BVerfG, 24.07.2013, 1 BvR 444/13, ZUM 2013, 793 (795).
74 BVerfG, 24.07.2013, 1 BvR 444/13, ZUM 2013, 793 (795).
75 BVerfG, 24.07.2013, 1 BvR 444/13, ZUM 2013, 793 (795).
76 The BVerfG embraces a large scope of protection for the freedom of expression, cf. *Grabenwarter*, in: Maunz/Dürig Commentary on the Constitution (Grundgesetz), Art. 5 point 62.

An obligation to immediately remove content from the public discourse can only be justified if the unlawfulness of that content results *directly from the utterance itself*. In addition to *clear cases of violations of human dignity* or *outspoken threats to a person*, this comes into question when offenses against public peace entail a risk of further infringement, because the expression is applied to have real impact towards further breaking of law, incitement of hatred, emotionalization or the reduction of inhibitions towards violence against others.[77]

In all *State protection cases* this can be excluded. Also, in these cases neither the context nor the history of a critical statement can be reliably determined by a network operator, let alone in 24 hours. State institutions, unlike private individuals, are not dependent on a legal guarantee of a non-violent communication space in which they can exercise their freedom of expression. In the case of offenses against constitutional bodies, the law enforcement authorities are in a position to intervene ex officio.

4. Procedural standards versus danger of "overblocking"

Due to the NEA the decision regarding unlawful and illegitimate behavior in social networks remains in the hand of the operators of these networks. In contrast to the Federal Court of Justice's model (or the Online Copyright Infringement Liability Limitation Act, OCILLY), there are no concrete guidelines on how the social network has to balance the interests of the author of the reported content and the complaining user involved. No guidelines are given, how to decide when the persons concerned do not answer on request or comply with necessary and reasonable formal requirements.

The clarification of controversial legal questions *cannot* be expected in a social network within a week. Courts regularly deal with offenses of insult and defamation (Section 185-187 of the German Criminal Code, short: GCC) *only after complex processes*.[78] Guidelines can give a certain degree of objectivity here, but each individual case will not be predictable. For assessing the question of whether a specific content is manifestly unlawful, the subjective perception of the responsible employee will almost unavoidably be a decisive factor and the employee will tend to avoid trouble.

With the risk of high fines in mind, the networks will probably be *more inclined to delete* a post than to expose themselves to the risk of a penalty payment.[79] As the differentiation between "unlawful" and "manifestly unlawful" is anything but clear (the draft gives no further information, such as a definition) networks will, in case of doubt, probably erase contributions.

The draft in its current version also nourishes the fear that this will lead to a circumvention of the territorial scope. This is not because the draft law declares German law to be applicable. But

---

77 BVerfG, Beschluss vom 4. November 2009 – 1 BvR 2150/08 –, BVerfGE 124, p. 300 (point 73).

78 Stellungnahme des Deutschen Journalistenverbandes, p. 7, to be found under: https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/DE/NetzDG.html.

79 https://www.bitkom.org/Presse/Presseinformation/Bitkom-zum-Gesetzentwurf-gegen-Hasskriminalitaet-in-sozialen-Netzwerken.html.

it could be because the social networks will probably tend to erase German-language comments without clarifying the situation (e.g. the location of the data entry etc.).

In consequence, this "overblocking" will most likely lead to an *undermining of the freedom of expression*. It already has proved difficult for social networks to differentiate between (criminal) utterances and journalistic reports about these utterances. The Federal Minister of Justice explicitly denounced this problem.[80] This problem is not directly addressed by the NEA and it could be increased due to time pressure and risk of high fines.

The projected jurisdiction of the District Court is *no convincing remedy*. The decision to grant a fine is, in principle, a decision made by the administrative authorities. It does not correspond to the traditional principles of German administrative law that the competent authority should be obliged to consult the district court in advance. Furthermore the competent authority shall be the Federal Agency for Justice based in Bonn. This means that the competent court in *all* cases is the Bonn District Court. This could easily lead to an overload or overburden of the Bonn District Court.

X. Result

The goal of the NEA to take effective measures against hate crime is to be supported. The legislature wants to introduce an effective compliance system with the NEA. The draft is linked to existing blocking and deleting obligations of the social networks and creates incentives for them to fulfill these obligations in practice. Concerning the selection of the regulation model, there is a wide scope of discretion. However, when implementing a model, the legislator should ensure that it is implemented consistently. It is also necessary to ensure that fundamental rights of the parties involved are brought into balance.

---

80 http://www.zeit.de/digital/intepointet/2015-12/facebook-heiko-maas-hetze-hasskommentare; http://www.spiegel.de/netzwelt/netzpolitik/heiko-maas-droht-facebook-wegen-hasskommentaren-a-1103167.html.

Annex

The Offenses of Section 1 (3) NEA

I. Offenses against the democratic State

- **Sections 86 GCC: Dissemination of propaganda material of unconstitutional organisations and using symbols of unconstitutional organisations**

Sec. 86 of the German Criminal Code (GCC) criminalizes the dissemination of propaganda material of unconstitutional organisations or making such material publicly accessible. Most prominent, in this regard, are efforts aimed at strengthening National Socialist resurgence.

Apart from that, the law refers to propaganda material from prohibited parties and organisations. Parties can only be prohibited by the Federal Constitutional Court (Bundesverfassungsgericht, short: BVerfG) according to Art. 21 (2) of the German Constitution, which is called the "party privilege".

It does not qualify when only thoughts and ideas of forbidden parties or organisations are propagated; rather there must be a relationship to the party itself.[81] Forms of action are dissemination, production, stock keeping, import and export of such. In particular, "dissemination" is an element that occurs in many of those GCC sections which are mentioned in Sec. 1 (3) NEA (Sec. 86, 86a, 90, 90a, 90b, 111, 130, 131, 140, 166, 184b, 186, 187 GCC). Representative for these, this element shall be considered in more detail here, also focusing on the Internet context.

Writings or other information can be distributed or disseminated, in particular, via the Internet. For this purpose, the Federal High Court has made it clear that it is necessary that the file is saved onto the computer of another person (another Internet user). It is irrelevant whether the file is stored on the volatile memory or the hard disk.[82]

Dissemination further implies that the criminal content is made accessible to a larger and for the perpetrator no longer controllable group of people[83]. The offender must at least count on the transfer to a multitude of individuals.[84] For this, a single handover can suffice if it happens in the consciousness that the recipient will then make the material accessible to a larger group of people. This would be the case when a certain material is handed over to at least one media representative.[85] The intended influence on a few individuals in the context of an Internet chat or

---

Maximilian Hemmert-Halswick wrote the Annex.

81 *Steinmetz*, Munich-Commentary of the GCC, 3rd ed 2017, Sec. 86 point 16.
82 BGH, MMR 2001, 676 (677).
83 *Steinmetz*, Munich-Commentary of the GCC, 3rd ed 2017, Sec. 86 point 26.
84 BVerfG, NJW 2012, 1498 (1500); OLG Köln, 11.11.1981, 3 Ss 704/81 –, juris.
85 BGH, NJW 2005, 689 (690).

e-mail traffic does not qualify as dissemination as well as the mere abstract risk of passing the content on to third parties through chat partners.[86]

- **Section 86a GCC: Use of symbols of unconstitutional organisations**

Another criminal offense enumerated in Sec. 1 (3) NEA is the use of symbols of unconstitutional organisations in public. The objective is to prevent group effects that are facilitated by recognizing likeminded people and separating individuals from the law-abiding society.

It is not necessary for the perpetrator to identify himself with the aims of the unconstitutional organisation.[87] The aim of this norm is to avoid the impression that unconstitutional organisations, despite their prohibition, are reviving.[88]

Symbols may be: flags, badges, uniforms, but also slogans and salutations, e.g. the "Hitler salute".[89]

- **Section 89a GCC: Preparing a serious state-threatening act of violence**

Sec. 89a GCC criminalizes certain acts that serve the preparation of crimes, such as murder, abduction for the purpose of blackmail or taking hostages, which are (subjectively) "determined" to and (objectively) "suitable" for impairing the existence or security of the State or an international organisation or to remove constitutional principles. This provision is remarkable in the sense that it incriminates an action, which is far ahead of the actual perpetration. The provision was inserted into the GCC in 2009.

- **Section 90 GCC: Defamation of the President of the Federation**

According to Sec. 90 GCC whosoever defames the President of the Federation in a meeting, publicly or through the dissemination of written material shall be liable to imprisonment. Defamation is commonly defined as an insult that is substantial in terms of form, content, situational circumstances and motive.[90] Minor mishaps are not sufficient as well as sharp criticism.[91] It is often difficult to distinguish between statements which are still protected by freedom of opinion or freedom of art, and those who cannot rely on this protection.

The "public" presentation of content requires that the content is accessible to a larger, undefined group of people. The mere accessibility is sufficient. This sets apart the public presentation from the dissemination, in which the user has already downloaded the data, so that he can also reproduce and distribute it.[92]

---

86 BVerfG, NJW 2012, 1498 (1500).
87 *Ellbogen*, Beck-Commentary of the GCC, 33rd ed 2016, Sec. 86a point 2.
88 *Ellbogen*, Beck-Commentary of the GCC, 33rd ed 2016, Sec. 86a point 2.
89 *Ellbogen*, Beck-Commentary of the GCC, 33rd ed 2016, Sec. 86a point 5.
90 *Valerius*, Beck-Commentary of the GCC, 33rd ed 2016, Sec. 90 point 3.
91 *Steinmetz*, Munich-Commentary of the GCC, 3rd ed 2017, Sec. 90 point 6.
92 *Ziegler*, Beck-Commentary of the GCC, 33rd ed 2016, Sec. 184b point 10.

The reason for punishment, the particular danger, lies in the fact that the perpetrator can no longer assess who is ultimately aware of the content. As a consequence, he can no longer estimate or control the impact his post will have. If it is only a small group of possible addressees, it can be assumed that the post or comment does not take place in a public setting. This implies that closed chatrooms are not a public forum. Content within this platform are not open to the public. On the other hand, the use of "secret language" or the (public) use of forms of communication, which only few people understand, does not mean that the content was not made public.[93]

The feature of "public presentation" is also found in Sec. 90a, 90b, 100a, 111, 130, 131, 140, 166, 184b, 184d and also §§ 86, 86a GCC; the same principles apply here.

- **Section 90a GCC: Defamation of the State and its symbols**

Protected objects of the first variant of this offense are the Federal Republic of Germany and its Federal States in their organisation as a free democracy and their constitutional order. The individual State organs are not protected. Conceivable is, however, an offense against the State via degrading utterances against its organs.

Such defamation has been assumed when members of the federal cabinet were called "mass murderers"[94] or when someone claimed that the State would carry out targeted killings and present it as suicides.[95] Calling a minister rogue did not qualify as a defamation.[96]

The second variant of this criminal offense provides a punishment for the denigration of State symbols. Such symbols are the State colors (black, red, gold), the national flag, the coat of arms (eagle in front of a golden background) and the national anthem. A denigration of symbols was, for example, assumed in the portrayal of a male torso, which urinated on the federal flag.[97]

The action in both cases must be carried out in public, in a gathering or through the dissemination of written material.

- **Section 90b GCC: Anti-constitutional defamation of constitutional organs**

According to this section the constitutional bodies of the Federation and the Federal States (legislation, government and the constitutional court) are protected. In contrast to Sec. 90 and 90a GCC, Sec. 90b GCC requires that the reputation of the State is jeopardized by the denigration. The perpetrator must be committed to anti-constitutional endeavors.

---

93 OLG Oldenburg, NStZ 2007, 99.
94 RG, 23.03.1923, – IV 885/22 –, RGSt 57, 209 (211).
95 BayObLG, 23.10.1995 – 3 St 3/95a, b, NStZ-RR 1996, 135.
96 RG, 10.04.1923, – I 157/23 –, RGSt 57, 185.
97 OLG Frankfurt, NJW 1986, 1272.

- **Section 91 GCC: Encouraging the commission of a serious violent offense endangering the state**

The provision of Sec. 91 has been inserted into the GCC together with Sec. 89a. Punishable is a person that hands out a guide about the performance of serious State-threatening acts of violence. The guide must be of such nature that upon reading the provided instruction the averagely informed and interested individual is able to carry out such act.[98]

- **Section 101a GCC: Treasonous forgery**

An unlawful content (Sec. 1 (3) NEA) is also such, whereby treacherous false information is disseminated or made public. It must be an untrue assertion which is capable of endangering Germany's external security or relations with a foreign power. The most important aspect is the falsification of an illegal State secret. This paragraph was not included in earlier versions of the NEA draft. It is a criminal offense that tends to be very rare.[99]

II. Offenses against public order

- **Section 111 GCC: Public incitement to crime**

Public incitement to crime also constitutes an illegal content according to Sec. 1 (3) NEA. The incitement must occur in public, in a gathering or through the dissemination of writings. This offense must be seen in contrast to the general incitement. The general incitement is aimed at a particular individual or a specific group whereas the public incitement is aimed at an uncertain number of people. The incitement has to be meant seriously.[100] For example a song text in form of a rhyme that motivated the use of violence against the police was considered to lack this seriousness.[101] A prayer published on the Internet, in which Allah is called to punish a certain Islamic critic and like-minded people was also considered as not sufficient.[102]

- **Section 126 GCC: Disruption of public peace through threats of criminal offenses**

Closely related to the previously mentioned offense is the breach of the public peace by threatening to commit offenses. The offense that is threatened with must be one of the acts listed in Sec. 126 (1) GCC (for example, murder, manslaughter, genocide, serious physical harm, robbery, predatory extortion or arson). The threat has to be announced publicly. A key aspect of this offense is that the threat must have the potential to disturb the public peace.

---

98 *Von Heintschel-Heinegg*, Beck-Commentary of the GCC, 33rd ed 2016, Sec. 91 point 4.
99 *Lampe/Hegmann*, Munich-Commentary of the GCC, 3rd ed 2017, Sec. 100a point 3.
100 *Paeffgen*, Kindhäuser-Commentary of the GCC, 4th ed 2013, Sec. 111 point 19.
101 OLG Thüringen, 21.11.1994 – 1 Ss 71/93, NStZ 1995, 445.
102 OLG Oldenburg, NStZ 2007, 99.

Criteria for the suitability for disturbance of the public peace are, above all, the semantic content, the intensity and the scale of the attack, the susceptibility of the public – especially young people – to attacks and the sensitivity of the group concerned. The broad and largely uncontrolled transfer of information on the Internet generally leads to the assumption that publications are known to a broader public. Attacks through the Internet can easily take on large proportions. In consequence, the suitability for a disturbance of the public peace is more likely to be assumed. It may be different in the case of forums or chats that are particularly protected by access restrictions and entrance examinations.

The suitability for disrupting public peace is also a requirement in the case of the relevant facts of Sec. 130, 140 and 166 GCC.

- **Section 129 GCC: Forming criminal organisations**

Sec. 129 GCC criminalizes the formation of criminal organisations. This provision (similar to Sec. 89a and § 91 GCC) leads to a shift in the protection of prospective victims. An attack on other individuals is not necessary. The mere formation of such an organisation is incriminated. Thus, the punishable behavior can occur long before the actual attack.

A criminal organisation requires a certain time of existence, a voluntary association of a minimum of three individuals, who will pursue common criminal aims, thereby subordinating the will of the individual member under the will of the whole. The offenses, which the organization plans to perpetrate must pose a significant threat to public.[103]

- **Section 129a GCC: Formation of terrorist groups**

Sec. 129a (1) GCC covers the formation of and the participation in an organisation whose aims or activities are directed at the commission of enumerated capital offenses. On the other hand, Sec. 129a (2) GCC requires the formation of or participation in an organisation whose purpose is the commission of other – less severe than those under Section 129a (1) – criminal offenses and which also aims to intimidate the public in a considerable way, to unlawfully coerce a public authority or an international organisation through the use of force or the threat thereof, or to significantly impair or destroy the fundamental political, constitutional, economic or social structures of a State or an international organisation.

- **Section 129b GCC: Criminal and terrorist groups abroad; extended confiscation and deprivation**

Sec. 129b GCC expands sections 129 and 129a GCC by including international organisations. Without Sec. 129b of the GCC, an act would only be punishable, if it concerned an organization

---

[103] *Von Heintschel-Heinegg*, Beck-Commentary of the GCC, 33rd ed 2016, Sec. 129 point 5.

which exists or operates at least partially in Germany.[104] Due to the international integration of organised crime, this would be an unsatisfactory condition in the sense of effective prosecution.

As for organisations outside the EU, Sec. 129b GCC applies if a special domestic connection exists, as defined in Sec. 129 (1) GCC. For organisations within the EU, the general provisions of Sec. 3 et seq. GCC apply.

- **Section 130 GCC: Incitement of hatred**

Incitement of hatred refers to the hatred against a national, racial, religious group or a group defined by their ethnic origins. It also refers to hatred against segments of the population or individuals because of their belonging to one of the aforementioned groups.

According to Sec. 130 (1) GCC the incitement to hatred against groups of the population is punishable if it is suitable to disturb public peace. Whether a certain incitement is actually capable of disturbing the public peace is measured by the intensity of the attack and the susceptibility of the addressed people.[105] Especially adolescents are very susceptible to agitations against asylum seekers or foreigners in general.[106] It is not necessary that the incitement takes place in a public setting.[107] It is also not required that the group that is being discriminated against is aware of the attack.[108]

Sec. 130 (2) GCC relates to the dissemination of writings which incite hatred against certain groups of the population. It also covers cases where such writings are made available to the public.

Of particular relevance are Subsections 3 and 4. According to Subsection 3, the person who publicly approves, denies or trivializes Nazi crimes and thereby disturbs the public peace shall be punished. According to Subsection 4, publicly approving, denying or trivializing Nazi rule is punishable if this is qualified to disturb public peace. The requirements of Subsection 4 can only be met if the statement refers to human rights violations characterizing the Nazi regime (not covering, for example, the approval of motorway construction during that time).[109]

- **Section 131 GCC: Dissemination of depictions of violence**

Sec. 131 of the GCC criminalizes the glorification and trivialization of violence. This is based on the assumption that certain depiction of violence can lead to adverse behavioral changes among their consumers and even to imitation of the depicted violence.[110]

---

104 *Schäfer*, Munich-Commentary of the GCC, 3rd ed 2017, Sec. 129b point 1.
105 *Schäfer*, Munich-Commentary of the GCC, 3rd ed 2017, Sec. 130 point 24.
106 *Schäfer*, Munich-Commentary of the GCC, 3rd ed 2017, Sec. 130 point 24.
107 *Schäfer*, Munich-Commentary of the GCC, 3rd ed 2017, Sec. 130 point 25.
108 *Schäfer*, Munich-Commentary of the GCC, 3rd ed 2017, Sec. 130 point 25.
109 *Rackow*, Beck-Commentary of the GCC, 33rd ed 2016, Sec. 130 point 38.
110 *Rackow*, Beck-Commentary of the GCC, 33rd ed 2016, Sec. 131 point 4.

The representation of violence must be disseminated through written materials or made available to the public. A computer based document also qualifies, so that such content shared over the Internet can fulfill the provision's criteria.

Violence within the context of Sec. 131 GCC refers to aggressive acts, which are directed against the body of another person and which physically or mentally impair or specifically endanger it. The depicted violence must be cruel or otherwise inhuman. This is the case when it is done with the addition of special pain or torment or a reckless and despising attitude of the person exercising the violence.

- **Section 140 GCC: Rewarding and approving of offenses**

According to the NEA, operators of social networks have to impede the rewarding or approving of offenses by their users. The latter only constitutes a crime (or, in the context of the NEA: an illegal content) when made in public, in a meeting or through dissemination of written materials.

- **Section 166 GCC: Abuse of confessions, religious associations and ideological associations**

Punishable is, according to Sec. 166 GCC, anyone who publicly or through dissemination of written materials defames the religion or world views of others in a manner that is capable of disturbing the public peace. Likewise, punishable is who insults a church or other religious associations in this way.

With regard to the religious nature of this provision, public peace is particularly endangered when the public's trust in mutual respect and tolerance is questioned.[111]

The defamation of religions has been assumed in a case where imprinted on a T-Shirt Jesus Christ was depicted as a pig hanging on the cross.[112] Another example is the mailing of toilet paper with an overprint of Koran suras.[113] On the other hand, the bashing of the Catholic Church as a "childfucker sect" was considered to be not sufficient, since the subject of "abuse in the Catholic Church" was being discussed in the public.[114]

III. Provisions on the protection of the personal rights

Presumably the most common reason for a complaint would be one of the offenses of the enumerated Sec. 185 to 187 which criminalize insult, defamation and intentional defamation.

---

111 *Von Heintschel-Heinegg*, Beck-Commentary of the GCC, 33rd ed 2016, Sec. 166 point 12.
112 OLG Nürnberg, 23.06.1998 – Ws 1603-97, NStZ-RR, 1999, 238.
113 AG Lüdinghausen, 23.02.2006 – 7 Ls 540 Js 1309-05, 31/05, BeckRS 2006, 10355.
114 *Hörnle*, Munich-Commentary of the GCC, 3rd ed 2017, Sec. 166 point 23 with further references.

- **Sections 185 GCC: Insult**

An insult is understood as an attack on the honor of another person by issuing one's own disregard or disrespect.[115]

If someone is confronted with true facts that objectively diminish his honor Sec. 185 GCC does in principle not apply.[116]

With his statement the offender must express his *own* disregard. It is therefore not sufficient if only messages of others are delivered. It may, however, be the case that the nature of the transfer reflects his own disregard. In the case of utterance in social networks, it is particularly important to check whether a separate statement is made by clicking on the "Share"- or "Like"-button.

- **Section 186 GCC: Defamation**

The defamation consists of the assertion or dissemination of unproved facts against a third party, which are capable of causing disregard by others. As a further distinction to Sec. 185 GCC is to be emphasized that Sec. 186 GCC covers only the allegation or distribution of facts, value judgments do not fall under Sec. 186 GCC. The delimitation can be difficult. It is not necessary that the fact is untrue –it is sufficient that the proof of truth is not given.

- **Section 187 GCC: Intentional defamation**

This provision largely corresponds to Sec. 186 GCC. The deciding difference, however, is that the alleged fact has to be untrue.

- **Section 241 GCC: Threatening the commission of a felony**

The listing in Sec. 1 (3) NEA also includes the offense of threatening the commission of a felony. The offender has to address a specific individual or specific group of people. The announced evil has to constitute a felony which is any offense that stipulates a one-year prison sentence as the minimum punishment.

IV. Other offenses

- **Section 184b: Distribution, acquisition and possession of child pornography**

The provision regulates the dealing with child pornography. A child is a person under fourteen. The person who disseminates, publishes, produces, delivers, stores, offers, applies, or possesses written materials of child pornography shall be punished.

In the Internet context „publishing“ is given when a file is put into the network for read access. A "possession" in the Internet traffic is given if the incriminated material is stored onto a data

---

115 *Regge/Pegel*, Munich-Commentary of the GCC, 2nd ed 2012, Sec. 185 point 8.

116 *Valerius*, Beck-Commentary of the GCC, 33rd ed 2016, Sec. 185 point 21.

carrier. With regard to the Federal High Court,[117] however, it is sufficient that the image files are loaded onto the working or cache memory of a computer, which is already the case when simply viewing the images on the monitor via the Internet.[118]

- **Section 184d GCC: Distribution of pornographic performances by broadcasting, media services or telecommunications services**

Sec. 184d GCC criminalizes the dissemination of pornographic content by means of media. According to Subsection 1 someone is punishable who makes such material accessible to another person or to the public by means of broadcasting or telecommunication services. As far as telecommunication services are concerned, criminality is excluded if it is ensured that the content is not accessible to persons below 18 years of age.

- **Section 269 GCC: Forgery of data intended to provide proof**

Ultimately, the online usage of falsified documents is also a variant of illegal content. The most common type of this offense is the sending of so-called phishing mails.[119] Here, the addressee is prompted to disclose sensitive data (banking data, password, PINs etc.) through deceit.

117 BGH, MMR 2001, 676 (677).
118 *Ziegler*, Beck-Commentary of the GCC, 33rd ed 2016, Sec. 184b point 15.
119 *Erb*, Munich-Commentary of the GCC, 2nd ed 2014, Sec. 269 point 33.