CEP POLICY PAPER

NetzDG 2.0

Recommendations for the amendment of the German Network Enforcement Act (NetzDG)

and

Investigation into the actual blocking and removal processes of YouTube, Facebook and Instagram

April 2020

COUNTER EXTREMISM PROJECT

Background on Germany's Network Enforcement Act (NetzDG law)

Throughout 2015 and 2016, Germany accepted approximately one million refugees, mostly from the Middle East. A backlash against immigrants ensued, leading to a dramatic rise in anti-immigrant crimes often committed by Germans who had no prior affiliation with extremist right-wing groups. Hate speech proliferated on social media, targeting both refugees and government officials who were deemed responsible for Germany's open immigration policy. At the same time, the online propaganda and recruitment efforts of the so-called "Islamic State" (IS) were at their peak, and several IS-claimed terrorist attacks were carried out within the European Union and Germany. In 2016 and 2017, the German federal government initiated an investigation into online activities that violated Article 130 (incitement to hatred and Holocaust denial) and Article 86a (use of symbols from unconstitutional organizations) of the penal code, and violations against the Youth Protection Act. The organization charged with the investigation reported 200 pieces of content per tested social media company (SMC). Facebook removed 39%, YouTube 90% and Twitter 1%. Looking solely at content removed within 24 hours of being flagged, the rates fell to 31% for Facebook, 82% for YouTube and 0% for Twitter.

NetzDG did not create new categories of illegal content. Rather, the law sought to provide a binding structure for SMCs for an effective compliance system. In German legal tradition, the contribution to or the support of illegal actions (by providing a platform for example) results in the obligation to remove them. This is called "Störerhaftung", which also applies to SMCs. As a result, SMCs need to remove illegal content once they are aware of it within 24 hours if the content is "manifestly illegal", or within 7 days if the legality of the content needs to be verified.

NetzDG applies to all social media platforms with at least two million registered users in Germany who receive at least 100 complaints regarding suspected illegal content per year. Direct messaging services like WhatsApp, Telegram and Signal as well as media outlets are exempt.

In the context of this policy paper it is important to note that in Germany, the public display of designated logos and symbols of banned organizations, e.g. the Nazi Party or the "Islamic State", is "manifestly illegal" if not done so for educational, artistic or media related purposes.

More information on the existing NetzDG can be found at https://bit.ly/33uaeiz and https://bit.ly/2Wvgwga.

Executive Summary

In February 2020, the Counter Extremism Project (CEP) Berlin carried out a sample analysis to test the extent to which YouTube, Facebook and Instagram block “manifestly illegal” content and characteristics of banned organizations upon notification.

The results of the study indicate that the logic behind the procedure of "notice and take down", which is the basis of the German Network Enforcement Act (NetzDG), is not sufficient to reduce illegal content online. YouTube only blocked or deleted just 35% of the illegal videos reported by CEP. Videos with identical content were blocked in some cases but not others (see Appendix 1). Facebook blocked the reported illegal photos according to NetzDG but did not do so with unreported, manifestly illegal content in the same photo folder (see page 11).

The aim of the "notice and take down" procedure prescribed by the NetzDG is to make social media safer for users. This can only succeed if illegal content is “seen”, found, reported and blocked effectively. Currently, this procedure is largely based on trust and chance since content on the platforms is monitored on an ad hoc basis by the companies themselves, users and the Internet Reporting Office of the Federal Criminal Police Office (BKA). There is no effective, systematic and continuous monitoring of the platforms covered by the NetzDG in relation to violations of German laws. This means that manifestly illegal content can remain online in large quantities.

Due to the fact that the companies for themselves decide what they can “see”, what is or is not being removed and are not required to be transparent about the relevant figures, processes and systems applied, it is possible for companies to claim that they remove or block 99,9% of illegal content while illegal content remains abundant on those very same platforms.

Our study thus raises doubts that companies' reports of success correspond with reality.

An estimated 500,000 hours of video content are uploaded to YouTube every day, and around one billion posts, including 300 million image files, are shared on Facebook each day. These amounts of data show that the goals of the NetzDG can only be achieved with proactive technological solutions in combination with content moderators. Companies are already using upload and re-upload filters to keep illegal or unwanted content off their platforms (e.g. copyright infringement, child pornography, legal nudity, legal pornography). According to their own statements, the companies also use this technology, in particular image and logo recognition software, to find illegal extremist and terrorist content. Reservations against proactive measures and automated systems used by the platforms are understandable. It is a fact, however, that companies are already using them for legal, commercial or other reasons, including against illegal extremist and terrorist content.

The question therefore is *not IF (*upload-)filters should be applied to prevent the dissemination of terrorist content online, *but HOW* to apply them.

Smart regulation that focuses on transparency, verifiability and effectiveness would therefore protect civil liberties more than no regulation.

Recommendations for the draft bill to amend the Network Enforcement Act (NetzDG):

1) Transparency and verifiability are crucial

In order to make “social media” safer, the functions, resources and results of the internal compliance processes, including the corresponding automated detection techniques, must be made so transparent that they are replicable. The same applies to the way content moderators work. Concerns that too much transparency can be misused by criminal actors or could risk core business interests should be taken seriously. Therefore, a two-tier system should be introduced. The Federal Office of Justice (BfJ), which is to be the new supervisory authority, could be granted the necessary powers of inspection. At the same time, the BfJ must then have the necessary technological expertise to be able to exercise actual supervision. The published form of the transparency reports must also go significantly beyond the current level of detail (especially regarding processes, technologies and systems).

2) Proactive search for manifestly illegal content

The procedural logic of "notice and take down" on which the NetzDG is based requires a systematic and continuous search for manifestly illegal content online and its subsequent reporting so that it can take effect. This cannot be left to the companies, users and few and small Police Internet Referral Units alone. Organizations such as Jugenschutz.Net, or civil society organizations, should be commissioned and financed accordingly.

3) Use appropriate technology for protection of civil rights

Automated image recognition algorithms for logos and symbols of banned organizations should be increasingly used just as is done in the field of copyright protection. Reservations against proactive measures and automated systems used by the platforms are understandable. It is a fact, however, that companies are already using them for legal, commercial or other reasons, including against illegal extremist and terrorist content. Regulation that focuses on transparency, verifiability and effectiveness would therefore protect civil rights more than no regulation.

4) Support EU legislation

The "Terrorist Content Online Regulation (TCO)" and the "Digital Services Act" are currently being negotiated at EU level. In order to be able to make “social media” safer for users in the long term, the transparency requirements described in this paper should urgently be integrated into both legislative proposals. The same applies to the regulation of proactive automated detection techniques (e.g. upload-filter), which is currently only considered as an option for the TCO.

About CEP and the authors

The Counter Extremism Project (CEP) is a not-for-profit, non-partisan, international policy organization formed to combat the growing threat from extremist ideologies. Led by a renowned group of former world leaders and diplomats it combats extremism by pressuring financial and material support networks; countering the narrative of extremists and their online recruitment; and advocating for smart laws, policies, and regulations.

Alexander Ritzmann is a CEP senior advisor. He is a member of the Steering Committee of the *European Commission's Radicalisation Awareness Network (RAN)* and co-chair of its Communication and Narratives (C&N) Working Group.

Dr. Hans-Jakob Schindler is senior director at CEP and head of its Berlin/Germany office. He is the former Coordinator of the *ISIL, Al-Qaida and Taliban Monitoring Team of the United Nations Security Council*.

Please direct inquiries regarding this report or CEP's activities to **Marco Macori**, CEP research fellow: mmacori@counterextremism.com; Phone +49 30 300 149 3369.

Contents

Part I - Background

1) Draft bill to amend the Network Enforcement Act (NetzDG)

On January 28, 2020, the Federal Ministry of Justice and Consumer Protection (BMJV) submitted a draft bill (Referentenentwurf) to amend the NetzDG. The procedural changes proposed therein are generally welcomed by CEP. In particular the simplification of the reporting forms for users, the expansion of user rights, and the supervisory and regulatory powers for the Federal Office of Justice are effective improvements to the current law.

CEP would also like to emphasize the necessity of the extension and clarification of the transparency report requirements (§ 2 Paragraph 2 NetzDG). The major tech companies repeatedly claim that they block or delete between 80% and 99% of the illegal content or content that violates community guidelines uploaded by users. However, there is a lack of transparency and, above all, a lack of verifiability as to which processes and technologies are used in which contexts and what exactly the removal and blocking figures refer to. Our research raises doubts that the success stories correspond to reality.

Since the companies themselves decide what is or is not removed, they do not have to provide a clear and comprehensive account of it. In addition, plenty of illegal content remains online because it has not yet been reported by users. Therefore, it is possible for SMCs to claim that they delete or block 99% of illegal content while illegal content remains abundant on those very same platforms.

As stated in the draft bill, there is therefore a considerable overall public interest in the background and functioning of corresponding automated processes. The same applies to the way content moderators operate. Concerns that too much transparency can be misused by criminal actors should, of course, be taken seriously. Therefore, a two-tier system should be introduced. The Federal Office of Justice (BfJ), which is to be the new supervisory authority, should be granted the necessary powers of inspection to perform its tasks. At the same time, the BfJ must have the necessary expertise to be able to exercise legitimate supervision, even on technological matters. The published form of the transparency reports must also go significantly beyond the current level of detail.

2) How to build verifiable transparency for automated systems

An estimated 500,000 hours of video content are uploaded to YouTube every day, and some one billion posts, including 300 million image files, are shared on Facebook each day. Social media companies routinely apply upload and re-upload filters to keep illegal or unwanted content off their platforms.

Reservations against proactive measures and automated systems are justified. Yet, the question is no longer *if* (upload-)filters should be applied to prevent the dissemination of terrorist content online, but *how* to apply them. Smart regulation that focuses on transparency, verifiability, and effectiveness will protect civil liberties more than no regulation.

The “Ethics Guidelines for Trustworthy Artificial Intelligence” of the EU High-Level Expert Group on AI highlight the importance of transparency and explainability of automated systems that have significant impact on people’s lives[1].

Transparency is essential to allow policy makers, researchers, and users to understand the structures of governance and compliance on social media platforms, particularly regarding the application of content classifiers and filters, whether used for recommendation, ranking, blocking, or removal of content.

The current reporting mechanisms on preventing the dissemination of terrorist content do not provide enough data or information to properly understand how social platforms are being used by terror-groups. More transparency is therefore required to allow policy makers and civil society to understand how social media platforms are being weaponized against society and democracies. Such transparency would lead to more accountability and would allow regulators to apply sanctions when appropriate. A more transparent reporting mechanism must include an understanding of the individual automated moderation tools, the technical compliance system as a whole as well as a better understanding of the application of moderation policies in practice.

An appropriately transparent system requires two main features. First, a suitable entity, with the appropriate technical and domain expertise, should be designated as an external observer with full access to moderation policies and procedures. Second, as enumerated below, published transparency reports must provide more detail regarding policies to.

15 main features of transparency and questions to be addressed in a transparency report
1) What are the underlying “theories of change” and theoretical concepts for the moderation tools and systems?
2) What classification criteria are used to search for content?
3) What is considered “terrorist”, “extremist”, or “illegal” content?
4) Which content categories (e.g., text, images, videos) are being searched and classified?
5) Which AI or machine-learning systems are being applied for content moderation? What is the accuracy of these systems?
6) How is machine-based training data validated to avoid bias?
7) What quality assurance or evaluation procedures are used?
8) To what extent and in what function are human moderators involved? Which processes are in place to account for potential moderation bias?
9) How many notices are received through users or trusted third parties?
10) How many posts were detected by automated systems?

[1] https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

11) How long, from the time a report is filed, did it take to remove content or decide not to remove content? How long does it take to inform all parties involved?

12) Of all notices received, what percent of content was removed?

13) Of all notices received, what percent are duplicates from previous reports (re-uploads)?

14) Of all notices received, how many views did each posting/file receive before takedown?

15) How is the well-being of human moderators monitored and addressed?

3) Social media - public conversations in private spaces

Although users may believe Facebook, YouTube, Twitter and other platforms operate as public discussion spaces, these platforms are de facto and de jure private. Anyone who agrees to these SMCs' terms of use, which is the prerequisite for participation in the platforms, submits to that platform's rules within the framework of German and European law. It is important to emphasize this fact in the political discourse surrounding the further development of the NetzDG.

CEP appreciates critics who are skeptical about the enforcement of German law by private companies. After all, the companies covered by the NetzDG primarily pursue for-profit interests. They are not committed to the common good. On the other hand, companies, like other branches of the economy, have an interest and a general social obligation to offer their users safe products, services and "experiences". Therefore, a common interest can be derived in this manner. In addition, under German law, any individual or company, for example hosts of festivals or major sporting events, are mandated to take precautions to protect visitors in the event of likely legal violations, to follow them up on those violations and, if necessary, to notify the authorities (see also "liability for interference" (Störerhaftung) or ex officio crimes).

However, SMCs historically come from an "all carrots - no sticks" era, in which they were able to conduct their business in a largely unregulated environment. The call for stricter compliance systems and regulations were mostly in response to legal disputes, fines and scandals, such as those relating to data protection and copyright violations. In order for publicly traded companies to invest significant resources, which could otherwise be invested to increase sales, into more effective compliance systems, processes and technologies, appropriate incentives and framework conditions must be set by legislators, which make such expenditures then justifiable for shareholders.

As part of the "EU Internet Forum", and particularly under pressure from the EU Commission and the EU Council, Microsoft, Google, Twitter and Google committed in 2016 to invest more in technological solutions, especially in the identification and automated removal of designated terrorist content. To that end, a "Database of Hashes" was created in December 2017 by the Global Internet Forum to Counter Terrorism (GIFCT), a cooperation between Facebook, Google, Microsoft and Twitter, on the basis of which a "re-upload filter" prevents or flags repeated terrorist content uploads.

According to an official statement by GIFCT before the Counter Terrorism Committee (CTC) of the United Nations Security Council in January 2020, the database currently contains "more than 200,000 entries".[2] This figure appears strikingly low when compared against the global size of GIFCT's platforms.

As a reminder, YouTube experiences uploads about 500,000 hours of video content a day, while Facebook sees uploads about one billion posts a day, including 300 million image files. Interestingly, this "re-upload filter" technology has been in use for years at Microsoft, Google and Facebook to prevent the repeated upload of child pornography content. Professor Hany Farid, who co-developed the algorithm for preventing the distribution of child pornography online (PhotoDNA), presented an analogously functioning "re-upload filter" called eGLYPH in 2015 in cooperation with CEP, which can report or delete known extremist content. Professor Farid's work has hence contributed to the creation of the “Database of Hashes” as a consequence of the EU Internet Forum. However, there is a complete lack of transparency and verifiability with regard to the selection and removal criteria of the “Database of Hashes”.

For some time, several SMCs have been calling for an “informed” regulation and compliance framework that will make the platforms safer for users. CEP is engaged in a critical and constructive dialogue with those companies.

4) EU - Internet Regulation

Due to the 2000 EU E-Commerce Directive, which aimed to keep regulation for SMCs to a minimum, EU member states can only oblige intermediaries such as social media companies to proactively monitor their platforms for harmful/ or illegal content to a limited extent.
The directive is to be replaced by a "Digital Services Act" before the end of 2020. In addition, the EU is currently undergoing the legislative process for a binding "regulation" to "prevent the distribution of terrorist content online"[3], in which platforms are to be obliged to take proactive security measures.

The members of the German Bundestag and the European Parliament, as well as the Federal Government, should use the opportunity that is currently presented to regulate extremist and terrorist content on social media with a view to improve transparency, verifiability and effectiveness. Reservations against mandating proactive measures and automated systems (e.g. upload filters) are understandable. The fact is, however, that these are already being used by some companies for legal or commercial reasons. A regulation that is geared towards transparency, verifiability and effectiveness would thus protect civil rights more adequately than no regulation.

[2] http://webtv.un.org/watch/countering-terrorist-narratives-and-preventing-the-use-of-the-internet-for-terrorist-purposes-open-meeting-of-the-counter-terrorism-committee/6127452700001/, Remarks starting at 1:42:45.
[3] https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-preventing-terrorist-content-online-regulation-640_en.pdf

Part II

Analysis of the blocking and removal processes of YouTube, Facebook and Instagram

CEP Berlin has, in the context of the current discussion on the amendment of the NetzDG, carried out an investigation during the period from January 31, 2020 to February 14, 2020with the aim of testing the extent to which YouTube, Facebook and Instagram block "manifestly illegal" content and labels of organizations banned under German law, following notification through the companies' respective NetzDG forms.

Findings: Overview

Of the 92 apparently illegal contents reported by CEP, 24 were blocked in accordance with NetzDG and 16 were deleted in accordance with platform guidelines. **This corresponds to a** blocking / removal rate of 43.5%.

- On **YouTube**, the blocking / removal rate was 35%. Videos with identical content were blocked in some cases and not others (Annex 1).
- **Facebook** blocked the reported content but did not block manifestly illegal content found in the same folder.
- **Instagram** deleted all content reported under NetzDG but did so in accordance with its own community standards.

Analysis

- The analysis was based on the published list of banned right-wing extremist and Islamist organizations of Germany's Federal Ministry of the Interior[4]. The platforms were searched manually with a focus on:

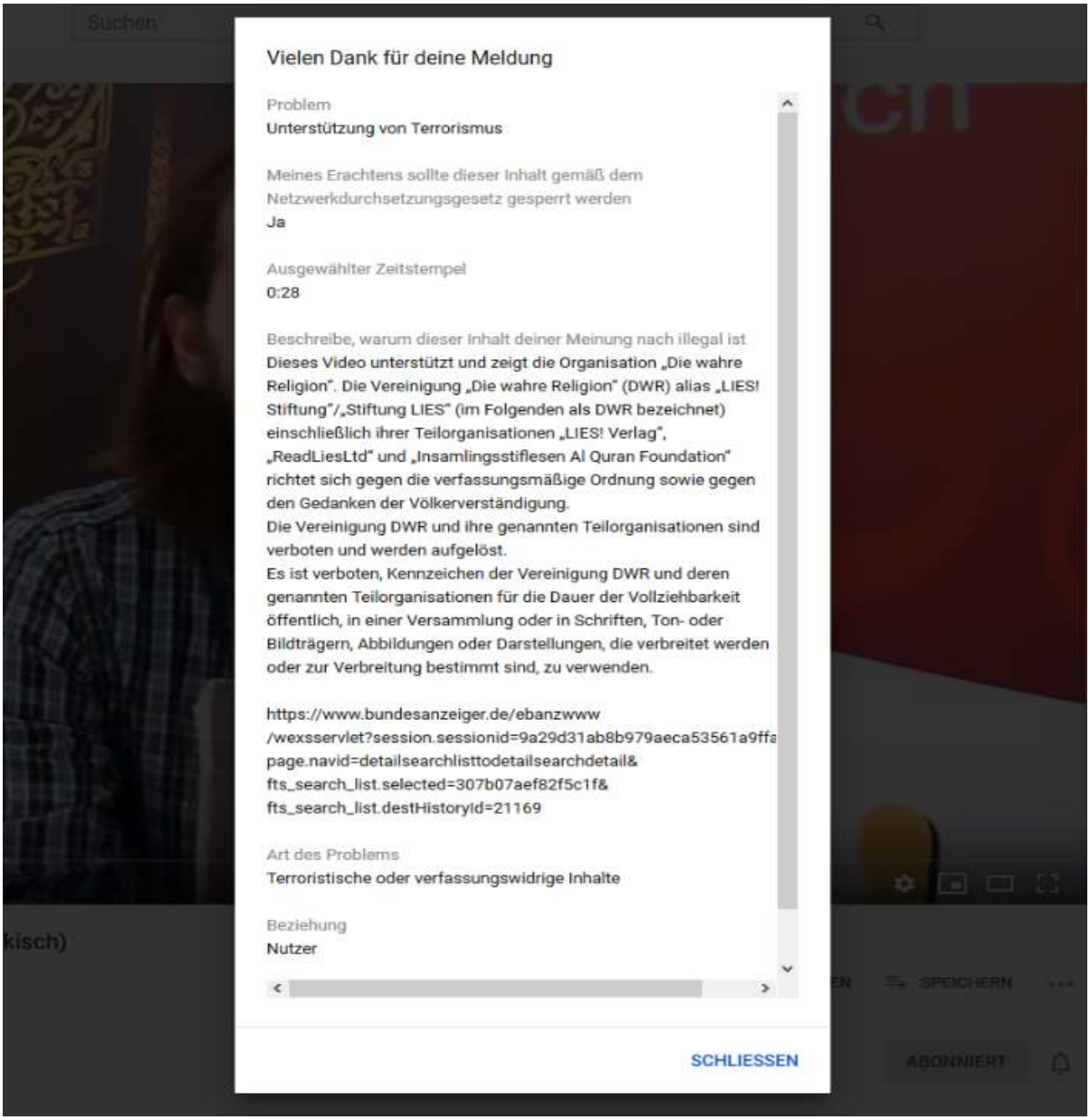
  a) Islamist:
  „Die Wahre Religion/Lies!", „Islamischer Staat", „Milatu Ibrahim", „DawaFFM", „Tauhid Germany", „an-nusra", „Hizb ut Tahrir", „HAMAS Izz-al-Din al-Qassam-Brigaden"
  „HAMAS IHH (Internationale Humanitäre Hilfsorganisation e. V.)"

  b) Right-wing extremist:
  „Weiße Wölfe Terrorcrew", „Combat 18 Deutschland"
  Furthermore, we identified indexed songs/videos of the radical right-wing band "Oidoxie".

- In the course of the investigation, a total of 92 videos, channels and image files in which the logos of the banned organizations were visible, and which were operated by the organizations themselves or by supporters, were reported via the respective NetzDG forms. Media reports or analyzes/comments by third parties about the banned organizations were not reported.

[4] https://www.bmi.bund.de/DE/themen/sicherheit/extremismus-und-terrorismusbekaempfung/vereinsverbote/vereinsverbote-node.html

- In each report, reference was made to the respective association ban order per German law (see Annex 2 for an example). In addition, the web link to the announcement of the ban order in the *Bundesanzeiger* was included. All findings and reports according to NetzDG, as well as the feedback from the platforms, are documented.

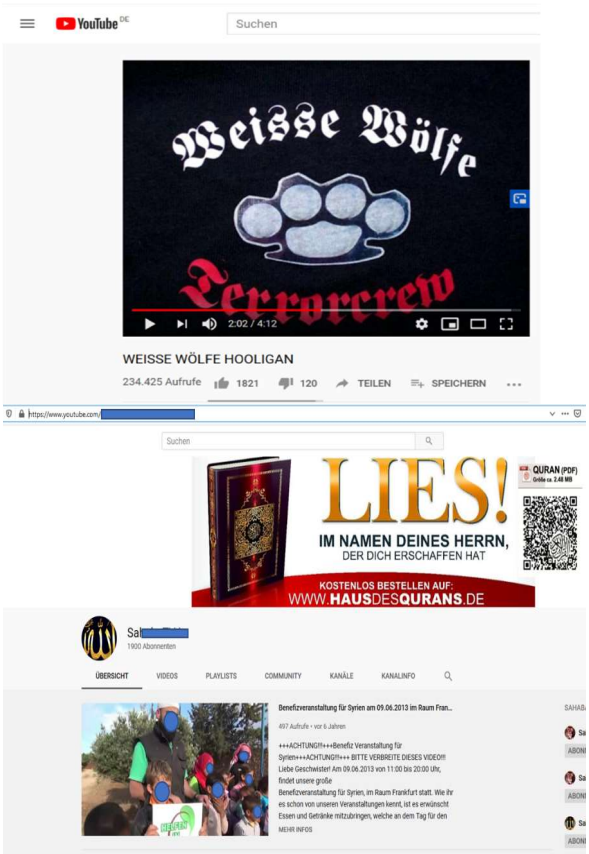


(Example of a completed reporting form according to NetzDG)

Findings

Of the 92 manifestly illegal pieces of content reported, 24 were blocked according to NetzDG and 16 were deleted according to the platform's guidelines. This corresponds to a **blocking / removal rate of 43.5%.**

- **YouTube** – CEP reported 80 pieces of content. YouTube blocked 22 cases in accordance to NetzDG. In six cases, removal occurred in accordance with the Community Guidelines. This results in a **blocking / removal rate of 35%.** It is conspicuous that videos with nearly identical content and images, with the same logos of the banned organizations, including some cases where the same persons were shown, were blocked in some cases but often not others (see Annex 1). This was especially the case concerning videos of the banned organization "Die Wahre Religion/Lies!" (DWR), which saw about 140 German supporters join Islamist Jihadist organizations in Syria and Iraq. During the investigation, almost three thousand additional DWR videos with a total of more than 18 million views were identified. These additional videos were not reported by CEP for capacity reasons.
  Update 1 as of March 9, 2020 - most DWR videos are now blocked for German IP addresses "due to an official notice or order".
  Update 2 as of April 22, 2020 – YouTube informed CEP that all videos reported by CEP have been blocked now.

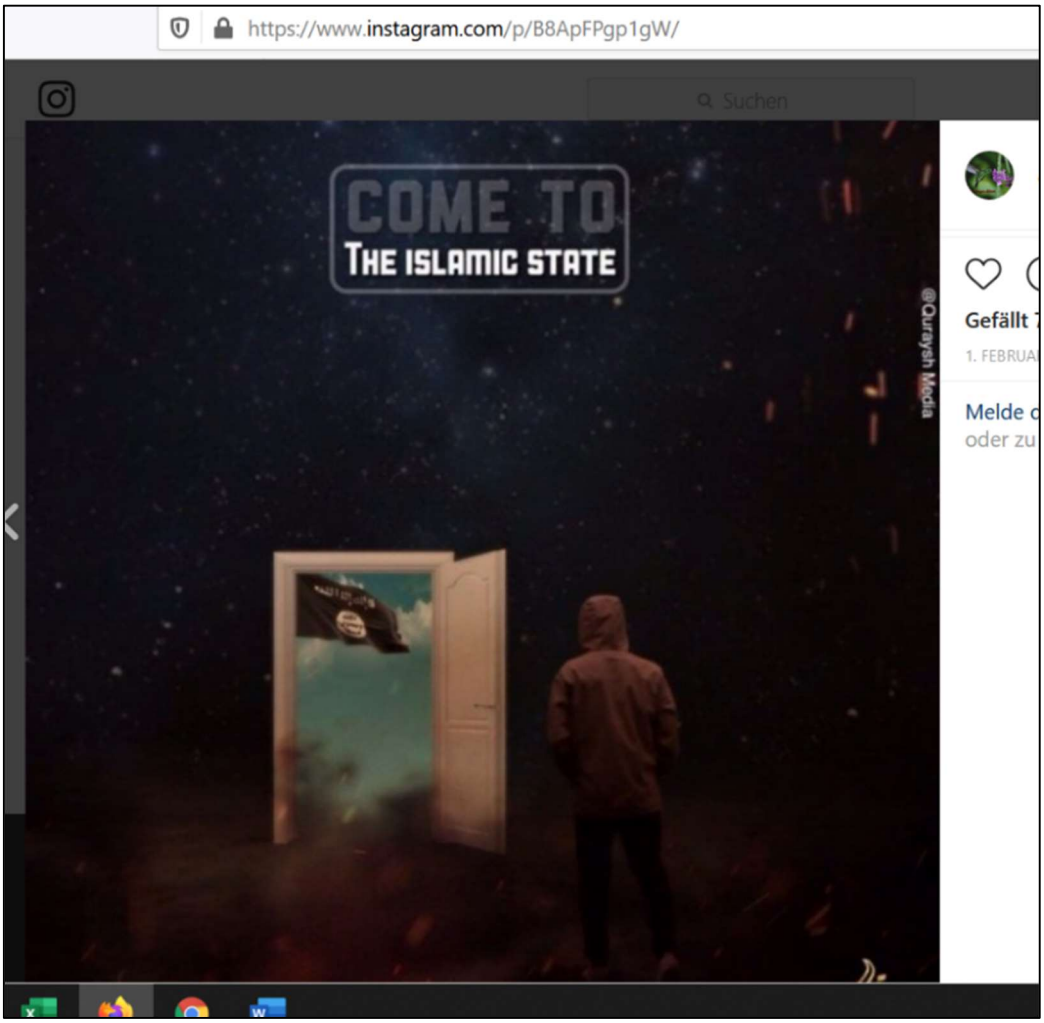


- **Facebook** – Two photos from folders of the profile of "Ibrahim Abu Nagie", the leader of DWR, were reported as an example. The two photos show advertising/recruitment activities. The forbidden DWR logo "Lies!" is clearly visible on most of the originals.

  These photos were both blocked within a few hours after NetzDG. **The approximately 400 other manifestly illegal photos in the said profile, which show the same symbols and activities as the contents reported by CEP and blocked according to NetzDG, are still freely accessible.** These additional photos were not reported by CEP for capacity reasons.
  Update as of March 9, 2020 - the profile "Ibrahim Abu Nagie" appears to have been deleted.

Zur Wahrung der Persönlichkeitsrechte der abgebildeten Personen sind diese unkenntlich gemacht worden.

- **Instagram** – CEP reported 10 profiles according to NetzDG, in which propaganda of the "Islamic State", mostly recognizable by the flag of the IS, was shown. **These profiles were all removed according to Instagram community guidelines, but not according to NetzDG**. If they are removed according to community standards, no further prosecution is possible, as the companies are not obliged to keep the data.



Evaluation

social media are currently not legally obliged to proactively monitor their platforms for harmful/illegal content. Instead, content on these platforms is primarily monitored on an ad hoc basis through voluntary activities of companies and through reports from users. **The results of our study indicate that there is no effective, systematic and continuous monitoring of the platforms covered by the NetzDG for violations of German law.**

- CEP's study on the operational implementation of the NetzDG for the platforms examined suggests that the "notice and take down" procedure (blocking / removal after complaint) does not currently work at two levels:

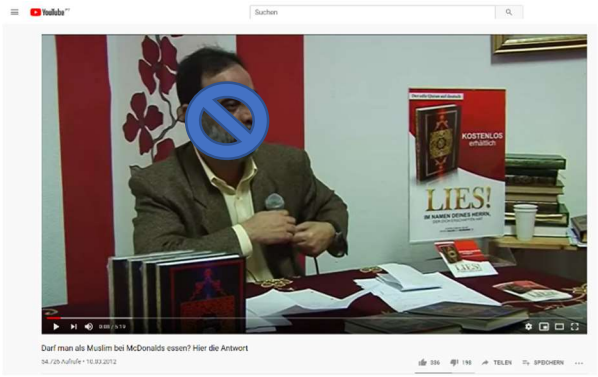
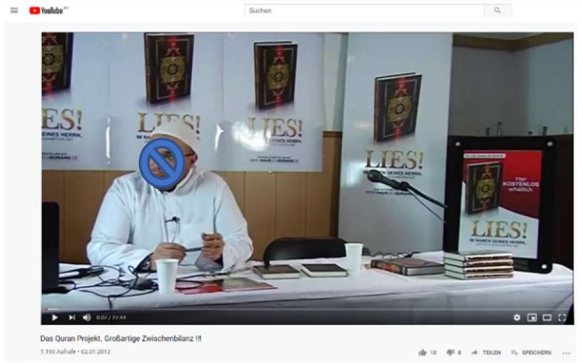
    1) "Notice and take down" can only achieve the desired success if the platforms are continuously and systematically searched for illegal content that is then reported for removal. This is apparently not the case currently. CEP is not aware of any organization or institution that can do this on the scale required. **As a result, unreported illegal content can remain online in abundance.**

    2) The blocking / removal rate of 43.5% in this sample, and in particular the 35% on YouTube, show that even with proper notification according to NetzDG, including reference to specific association bans, **the majority of illegal content is neither blocked nor removed**. Greater transparency and traceability of processes and technologies used to implement NetzDG requirements and community guidelines therefore appear to be urgently needed.

- YouTube experiences uploads about 500,000 hours of video content per day, while Facebook sees uploads about one billion posts per day, including 300 million image files. These data volumes show that the goals of NetzDG can only be achieved with **technological solutions in combination with content moderators.**

- The companies already apply (re-)upload filters to keep illegal or unwanted content off their platforms (e.g. copyright infringements, child pornography, legal nudity, legal pornography). According to their own statements, the companies also use this technology, especially image and logo recognition software, to find illegal extremist and terrorist content.

COUNTER EXTREMISM PROJECT

Appendix 1) Association ban by Federal Ministry of the Interior (BMI)	**Reported** and **blocked** by CEP	**Reported** by CEP and **NOT blocked**
Announcement of the non-appealability of the association ban against the association “Die Wahre Religion“ (DWR) alias “LIES! Stiftung “/” Stiftung LIES “, Jan. 8, 2018: “It is forbidden to use the logos of the DWR association and its sub-organizations for the duration of enforceability in public, in a meeting or in writings, sound or image carriers, pictures or representations that are distributed or are intended for distribution. The prohibition particularly affects the following logos”: DIEWAHRERELIGION.DE LIES! IM NAMEN DEINES HERRN, DER DICH ERSCHAFFEN HAT	  *To protect the personal rights of the people depicted, they have been made unrecognizable.*	  

Update as of April 22, 2020 – YouTube informed CEP that all videos reported by CEP have been blocked now.

Appendix 2) Example: Association ban “Die Wahre Religion”

[Translation of the German original document]

Federal Ministry of the Interior

Announcement

of the non-appealability of the association ban concerning the association

“Die wahre Religion“ (DWR) alias “LIES! Stiftung”/”Stiftung LIES“

January 8, 2018

On 25 October 2016 (Federal Gazette AT 15.11.2016 B1), the Federal Minister of the Interior issued the following order pursuant to section 3 subsection (1) sentence 1 alternative 2 and 3 in conjunction with section 17 no. 3 of the Associations Act of 5 August 1964 (Federal Law Gazette I p. 593), last amended by Article 1 of the Act of 10 March 2017 (Federal Law Gazette I p. 419):

1. The association "Die wahre Religion " (DWR) alias "LIES! Stiftung"/"Stiftung LIES" (hereinafter referred to as DWR) including its sub-organizations "LIES! Verlag“, “ReadLiesLtd“ und “Insamlingsstiflesen Al Quran Foundation " is directed against the constitutional order as well as against the idea of international understanding.

2. The DWR Association and its sub-organizations mentioned in No. 1 are prohibited and will be dissolved.

3. It is prohibited to use logos of the DWR Association and its sub-organizations mentioned in No. 1 for the duration of their enforceability in public, in a meeting or in writings, audio or video carriers, illustrations or representations which are distributed or intended for distribution. This prohibition concerns in particular the following logos:

On a red background in golden and white script, a calligraphic representation of the Arabic words al-din al-haqq (translated: " die wahre Religion"). Below it in white Latin script DIEWAHRERELIGION.DE.

In capital letters and golden letters, the word LIES with exclamation mark. Beneath it in capital letters and black letters the words " IM NAMEN DEINES HERRN, DER DICH ERSCHAFFEN HAT”.

In capital letters and golden letters, the word LIES with exclamation mark. Behind it the word "Stiftung".

4. The websites

http://www.diewahrereligion.de (*.eu, *.com, *.org, *.biz., *.info., *.tv)

http://hausdesqurans.de

http://www.lies-stiftung.de

http://www.infostaende.info

http://www.fatwah.de

http://www.kinderimislam.de

http://islamblog.tv

https://www.facebook.com/diewahrereligion

https://www.youtube.com/user/allahsreligion

https://twitter.com/diewahrereligio [sic!]

https://plus.google.com/+Diewahrereligion.tv

https://www.youtube.com/channel/UCjENDiLCAtwnuLIOEQJ17uA

https://www.youtube.com/user/AbuMouJahiiid

https://www.youtube.com/user/AbuMouJahid

https://www.youtube.com/user/AnsarudDinilHaqq

https://www.youtube.com/user/IslamErobertEuropa

including their provision, hosting and further use are prohibited.

5. The assets of the DWR Association and its sub-organizations mentioned in No. 1 shall be confiscated and confiscated for the benefit of the German Federation.

6. Third-party property shall be seized and confiscated if the rightful owner has promoted the unconstitutional efforts of the Association DWR or its sub-organizations mentioned in No. 1 by handing over the property to the Association DWR or its sub-organizations mentioned in No. 1 or if the property is intended to promote these efforts.

7. Claims of third parties against the DWR Association or its sub-organizations referred to in No. 1 shall be seized and confiscated if they represent an intentional promotion of the unconstitutional endeavors of the Association in terms of their nature, scope or purpose or if they have been substantiated in order to withdraw assets of the Association or its sub-organizations from official access or to reduce the value of the assets of the Association or its sub-organizations. If a creditor has acquired such a claim by assignment, it shall be collected to the extent that he knew the facts referred to in the first sentence at the time of acquisition of the claim.

8. The immediate execution of this order shall be ordered; this shall not apply to the recovery order.

This order is unappealable since 19 December 2017, after the actions brought against it have been withdrawn.

In accordance with § 7 paragraph 1 of the Law on Associations, the decision will be published again because of its non-appealability.

The Federal Office of Administration, 50728 Cologne, Germany, has been commissioned with the confiscation and liquidation of the association's assets.

Berlin, January 8, 2018

ÖS II 2 - 20106/8#2

Federal Ministry of the Interior

By order of

Nötges