HateAid gGmbH

Öffentliche Anhörung im Rechtsausschuss

des Deutschen Bundestages

Stellungnahme

zum Gesetzentwurf zur Änderung

des Netzwerkdurchsetzungsgesetzes

Inhaltsverzeichnis

I. Einleitung

Das NetzDG hat seit seiner Einführung am 01.09.2017 immer wieder für kontroverse Diskussionen gesorgt. Dabei ging und geht es vor allem weiterhin um die zentrale Frage, inwiefern die Meinungsfreiheit durch dieses Gesetz gewahrt oder beschnitten wird. Ziel des Gesetzes war zunächst die Entfernung von nach deutschem Recht rechtswidrigen Inhalten aus den Netzwerken. Um dies umzusetzen, wurden den sozialen Netzwerken Pflichten und bei Nichterfüllung Sanktionen auferlegt. Große Sorge gab es darüber, ob Netzwerke nun aus Angst vor Sanktionen übermäßig löschen würden und wie sich Nutzer*innen gegen eine unberechtigte Löschung wehren können. Gleichzeitig gab es aufgrund der zunehmenden Instrumentalisierung der Netzwerke durch rechte und rechtsextremistische Propagandagruppen, die gezielt Menschen einschüchtern und aus dem öffentlichen Diskurs herausdrängen, großen Handlungsdruck. Denn diese massiv invasiven politischen Guerillataktiken zeigen in aktuellen Studien schon eine erhebliche Wirkung – und zwar auch auf die Meinungsfreiheit. Denn eine Mehrheit der Internetnutzer*innen begann sich selbst bei bestimmten Themen in den sozialen Netzwerken zu zensieren aus Angst selbst Opfer von Digitaler Gewalt zu werden.

In diesem Spannungsfeld bewegt sich das NetzDG und der Ausgleich im Sinne der Meinungsfreiheit aller Nutzer*innen ist und bleibt die große Herausforderung des Gesetzesentwurfes. Klar ist, dass es Reformen geben musste, viele haben sich aus der Praxis ergeben. In dem jetzt vorliegenden Entwurf sind gute Ansätze zur Stärkung der Rechte von betroffenen Nutzer*innen zu erkennen, die es zum Ziel haben, den Nutzer*innen vermehrt Kontrolle über die Inhalte zu geben. Deswegen ist es umso bedauerlicher, dass die konkrete Ausgestaltung der Maßnahmen teilweise nur zaghaft, wenig aussagekräftig und mitunter auch nur oberflächlich erfolgte. Die Folge: Viele Regelungen sind zwar bedacht, werden aber in der Praxis ins Leere laufen, wenn der Gesetzgeber diese nicht noch einmal konkretisiert und mit der juristischen Praxis abgleicht. Dies gilt vor allem für die Effizienz der Rechtsdurchsetzung und die Nachvollziehbarkeit von Entscheidungen und Prozessen bei Netzwerken. Es betrifft aber auch maßgeblich die Transparenzberichte, die den Netzwerken weiterhin große Spielräume einräumen, um zu definieren was hineingelangt.

Zu begrüßen sind auch die Bemühungen, Regularien zur Überprüfung von Löschentscheidungen einzuführen. Diese müssen aber für Nutzer*innen eindeutig erkennbar und simpel anwendbar sein, anstatt ein Nebeneinander verschiedener Instrumente zu schaffen, die eher abschreckend, wirken könnten. Gleiches gilt für die Regelung zur Auskunft von Daten mutmaßlicher Täter*innen. Hier muss der Gesetzgeber sicherstellen, dass völlig klar ist, welche Daten Strafverfolgungsbehörden und Geschädigte bekommen, und dass diese Daten dann auch zur Identifikation von Täter*innen führen und nicht völlig wertlos sind. Weiterhin ist es elementar, dass sichergestellt wird, dass sich die Netzwerke dem NetzDG nicht durch Anwendung von Gemeinschaftsstandards oder den Verweis auf eine Datenspeicherung im Ausland entziehen können.

Ein weiterer zentraler Punkt: Die großen zumeist US-amerikanischen Netzwerke haben mit ihren sogenannten Gemeinschaftsstandards, Algorithmen und Strukturen ein Parallelsystem zu unserem Rechtssystem geschaffen. An nationales Recht sehen sie sich weiterhin kaum gebunden. Das hat zur Folge, dass noch immer der weitaus größte Teil von Inhalten nicht etwa deshalb gelöscht wird, weil sie gegen deutsches Recht verstoßen. Die Content-Entscheidungen erfolgen vielmehr nach den Gemeinschaftsstandards. Die Prüfung aufgrund dieser plattforminternen Regelungen wird der Prüfung auf Grundlage des deutschen Rechtes nach NetzDG sogar in der Regel vorangestellt. Hinzu kommt, dass die Netzwerke selbst

Inhalte mithilfe künstlicher Intelligenz (KI) herausfiltern, überprüfen und löschen. Welche Maßstäbe hier angelegt werden, ist der Öffentlichkeit kaum bekannt. Daher sollte unseres Erachtens ein Vorrang des NetzDG vor den Gemeinschaftsstandards der Netzwerke unmissverständlich im Gesetz artikuliert werden. Eine nachfolgende Prüfung nach Gemeinschaftsstandards ist den Netzwerken dabei unbenommen. Die Prüfung nach NetzDG - also nach deutschem Recht - sollte aber Priorität haben.

Hinzu kommt, dass für Telemedien zwingend das Marktortprinzip eingeführt werden sollte, denn nur so kann eine Identifikation von Täter*innen auch in Deutschland durch Auskunftsersuchen im Zivilprozess oder Strafverfahren sichergestellt werden. Denn bisher berufen sich die Netzwerke gegenüber Gerichten und Strafverfolgungsbehörden meist darauf, dass die begehrten Daten nicht in Deutschland, sondern in Irland oder den USA gespeichert seien und daher im Inland nicht beauskunftet werden könnten. Solange dies der Fall ist, droht jede nationale Verpflichtung zur Mitwirkung zwangsläufig ins Leere zu laufen. Die Netzwerke haben in der Vergangenheit gezeigt, dass ihnen nicht daran gelegen ist, an der Rechtsdurchsetzung mitzuwirken. Die Herausgabe von Daten erfolgt höchst selten und unsystematisch. Die angeblichen rechtlichen Risiken, die die Netzwerke in Bezug auf eine Datenherausgabe anführen, ließen sich aus unserer Sicht leicht ausräumen, z.B. durch eine Anpassung der Gemeinschaftsstandards. Dennoch wurden diesbezüglich keinerlei Anstrengungen unternommen. Nur durch die Einführung des Markortprinzips kann eine zuverlässige Rechtsdurchsetzung gewährleistet werden. Denn auf die Weise würden die sozialen Netzwerke verpflichtet, Daten der inländischen Geschäftstätigkeit im Inland vorzuhalten und somit auch aus Deutschland heraus zu beauskunften.[1]

Schließlich sind noch einige Regelungslücken verblieben, die das Verhältnis zwischen Nutzer*innen und Netzwerken betreffen. Es empfiehlt sich hier, sich am Urheber- und im Datenschutzrecht zu orientieren. Einige Lösungsansätze, die z.B. im Urheberrecht für die Durchsetzung zivilrechtlicher Ansprüche gefunden wurden, könnten als Blaupause auch für die Rechte der Nutzer*innen Sozialer Medien dienen.

Klar ist: Die Kontroverse um das NetzDG wird dieser neue Entwurf nicht auflösen können. Er kann aber dafür sorgen, dass viele Unklarheiten und Interpretationsmöglichkeiten beseitigt werden und die Rechte der Nutzer*innen - sowohl der Betroffenen von Digitaler Gewalt als auch derjenigen, deren Inhalte zu Unrecht entfernt wurden - gestärkt werden. Dafür braucht es aber konkrete Nachbesserungen mit Blick auf die Effekte und Durchsetzbarkeiten in der Praxis. Vorschläge dafür wollen wir in dieser Stellungnahme dank unserer Expertise aus der konkreten Arbeit mit Betroffenen und der Rechtsdurchsetzung im Zivilrecht ausführen.

II. Änderung des § 14 Abs. 3 TMG

Die beabsichtigte Änderung des § 14 TMG ist grundsätzlich zu befürworten und geeignet, die Rechtsdurchsetzung der Betroffenen auf zivilrechtlichem Wege zu erleichtern. Von allen

[1] vgl. Auch Stellungnahme zum Gesetzesentwurf zur Bekämpfung von Rechtsextremismus und Hasskriminalität: https://hateaid.org/wp-content/uploads/2020/05/Stellungnahme-Sachverstaendigenanhoerung-Rechtsextremismus-HateAid.pdf

gemäß § 14 Abs. 3 TMG auf Kosten von HateAid geltend gemachten Auskunftsersuchen wurden bisher nur drei beauskunftet. Es ist anzunehmen, dass der Grund hierfür das mediale Aufsehen war, welches diese Fälle erregten. Es konnten dennoch nicht alle Anschlussinhaber ermittelt werden, insbesondere wenn diese nicht unter Klarnamen agierten. Die bisherige Regelung einer Auskunftsgestattung hat demnach kaum praktische Relevanz, da seitens der Netzwerke keinerlei Bereitschaft zur Mitwirkung besteht. Aus Sicht der Netzwerke werden hier vorgeblich rechtliche Risiken gegenüber den betroffenen Nutzer*innen gesehen. Das Erfordernis einer Einzelfallabwägung verkompliziert den Prozess für die Netzwerke zusätzlich. Dies ist einerseits nachvollziehbar, da die Herausgabe von Nutzerdaten den wirtschaftlichen Interessen der Netzwerke grundsätzlich zuwiderläuft. Andererseits zeigt es, dass die Netzwerke aus eigenem Antrieb nicht bereit sind, sich Ihrer Verantwortung zu stellen, die ihnen bereits aufgrund ihrer Marktmacht und Reichweite zukommt. Vor diesem Hintergrund erscheint die gerichtliche Feststellung einer Beauskunftungspflicht sachgerecht.

Voranstellen möchten wir, dass das Verfahren gemäß § 14 Abs. 3 TMG im Beschlusswege nicht nur aufgrund ausdrücklicher gesetzlicher Anordnung von den Verletzten zu zahlen ist, sondern für sich genommen bereits ca. 4-5 Monate bis zu einem Jahr dauert. Diesen Zustand halten in vielerlei Hinsicht für nicht haltbar:

1. Es handelt sich lediglich um eine Vorstufe zur eigentlichen Rechtsdurchsetzung.
2. Die Auskunftserteilung an für sich lässt in der überwiegenden Zahl der Fälle keine Rückschlüsse auf die Identität der Täter*innen zu. Es bedarf stets eines weiteren Auskunftsersuchens, z. B. beim Internetprovider, um die Nutzer*innendaten zur IP-Adresse zu erlangen.
3. Begehrt wird die Auskunft extrem zeitkritischer Daten, wie z.B. der IP –Adresse. Diese wird maximal 6 Tage beim Internetprovider gespeichert.

Angesichts dessen, dass dieses Verfahren nur eine Vorstufe der eigentlichen Rechtsdurchsetzung darstellt und die Beauskunftung zeitkritischer Daten zum Gegenstand hat, halten wir diesen Zustand für nicht haltbar. Wir sprechen uns daher unbedingt dafür aus, eine Möglichkeit des einstweiligen Rechtsschutzes in Anlehnung an § 101 Abs. 7 UrhG zu normieren.

§ 14 TMG erlaubt den Zugriff ausschließlich auf Bestandsdaten. Bestandsdaten sind gemäß § 3 Nr. 3 TKG “Daten eines Teilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden”. Die Herausgabe der Bestandsdaten wird mit dem Ziel gestattet, die Ermittlung der Täter*innen sicherzustellen. Dies läuft in der juristischen Praxis aber regelmäißg ins Leere. Vielfach hängt es nämlich von der Rechtsauffassung des Gerichts ab, welche Daten als Verkehrs- oder Bestandsdaten bewertet werden. Dies ist bspw. Bei dynamischen IP – Adressen, Tag und Uhrzeit der Nutzung und Telefonnummern der Fall. Wir plädieren daher dafür nicht am Begriff der Bestandsdaten zu haften, sondern die Auskunft in aller Deutlichkeit auf die zur Täter*innenermittlung erforderlichen Daten zu erstrecken. Der Inhalt der Auskunft kann über die gespeicherten Bestandsdaten einschließlich der hinterlegten Rufnummern und E-Mail-Adressen (die nach unserem Dafürhalten zwingend erhoben werden sollten, s.o.) und die IP-Adresse der mutmaßlichen Rechtsverletzer*innen zum Zeitpunkt der Äußerung sowie den Tag und die Uhrzeit der Persönlichkeitsrechtsverletzung hinaus auch eine Dokumentation der Wahrnehmung und Verbreitung des Inhalts durch Dritte umfassen.

Letzteres ist insbesondere für die Einschätzung der Schwere und des Umfangs der Persönlichkeitsrechtsverletzung relevant, da die Bemessung der Höhe von Schadenersatz und Schmerzensgeld hiervon abhängt.

Auch bei Ausgestaltung von § 14 Abs. 3 TMG als verpflichtendem Auskunftsanspruch, sehen wir viele Hürden für eine erfolgreiche Rechtsdurchsetzung. Es ist vielmehr zu befürchten, dass der Anspruch aus mehreren Gründen ins Leere läuft. Diese sind vor allem auf zwei Erkenntnisse zurückzuführen:

1. Mangels gesetzlicher Regelung ist wie schon ausgeführt unklar, welche Daten bei sozialen Netzwerken überhaupt als Bestandsdaten erhoben und gespeichert werden. Die Vollständigkeit der Auskunft kann nicht nachvollzogen werden und die Identitätsermittlung ist nicht sichergestellt.

    a. Bislang ist es nicht erforderlich, dass sich Nutzer*innen bei der Registrierung auf den Netzwerken mit ihren **zutreffenden Personalien** anmelden. Die Anmeldeformulare der großen Netzwerke verlangen zwar die Angabe von Vor- und Nachnamen, Geburtstag und Geschlecht. Verifiziert werden müssen diese Angaben allerdings nicht. Weiter ist eine Handynummer oder eine E-Mail-Adresse anzugeben. Es kommt sogar vor, dass gar kein Vor- und/oder Zuname vorliegt oder dies zumindest von den Plattformbetreiber*innen so angegeben wird. Mangels rechtlicher Möglichkeiten die Vollständigkeit anzuzweifeln, ist eine solche Auskunft hinzunehmen.

    b. Wurde eine **E-Mail-Adresse** angegeben, dann handelt es sich häufig um kostenfreie Webmail-Accounts. D.h. selbst, wenn die Mail-Provider bereit sind, den bei der Anmeldung hinterlegten Namen herauszugeben, ist eine Identifizierung noch immer nicht sichergestellt. Die Anbieter kostenfreier Webmail-Angebote unterliegen unseres Wissens nicht den Pflichten nach § 111 TKG. Somit ist es nicht nur einfach, unter Angabe von falschen persönlichen Daten an einen E-Mail-Account zu gelangen. Mit dieser E-Mail-Adresse kann dann auch ein Account bei den Netzwerken angelegt werden, dessen Inhaber*in anhand dieser Daten praktisch nicht zurückverfolgt werden kann.

    c. Beauskunften die Netzwerke die **IP-Adressen** und Zeitpunkte des Zugriffs oder Uploads, wird hieraus in der Regel kein Erkenntnisgewinn zu ziehen sein, wenn dieser mehr als sechs bis sieben Tage zurückliegt. Zur Täteridentifizierung kann die IP-Adresse nur verhelfen, wenn sie so zügig beauskunftet wird, dass im nächsten Schritt innerhalb von sieben Tagen vom Internet-Zugangsprovider die zugehörigen Verkehrsdaten angefordert werden können. Allenfalls die IP-Adresse des letzten Logins ist idR überhaupt geeignet, um einen Anschlussinhaber zu ermitteln. Das gesamte Prozedere wird dennoch letztlich so viel Zeit in Anspruch nehmen, dass die benötigten Daten von den Zugangsprovidern gar nicht mehr herausgegeben werden können. Denn wegen des verfassungsrechtlich gebotenen und deswegen nicht in Zweifel zu ziehenden Verbots der anlassunabhängigen Vorratsdatenspeicherung werden die IP-Adressen und die weiteren

zugehörigen Verkehrsdaten bei den Providern nur maximal eine Woche vorgehalten. Dies hat zur Folge, dass diese nach Ablauf dieser sehr kurzen Frist schlicht keinen Erkenntnisgewinn mehr herbeiführen können.

d. Wenn allerdings tatsächlich eine **Handynummer** hinterlegt wurde, bestehen aufgrund der Identitätsprüfungspflicht nach § 111 TKG gute Aussichten, dass die den Account nutzende Person ermittelt werden kann. Jedenfalls ist die Auskunft über den Anschlussinhaber einer Telefonnummer weitaus weniger zeitkritisch als bei einer IP – Adresse. Diese wird von einigen Plattformbetreibern zur Wiederherstellung des Accounts oder im Rahmen der Zwei-Faktor-Authentifizierung ohnehin schon erhoben. Wir empfehlen, die Netzwerke zur Erhebung der Telefonnummer zu verpflichten. Nur so kann eine effektive Strafverfolgung sichergestellt werden, denn nur so gibt es die Möglichkeit für Strafverfolgungsbehörden als auch in Zivilverfahren, die Täter*innen überhaupt sicher zu ermitteln.

2. Selbst wenn man die Bestandsdaten inkl. IP-Adresse des Uploads, bzw. letzten Logins im Wege der Auskunft erlangt, gibt es keine Verpflichtung auf Herausgabe der dazugehörigen Anschlussinhaberdaten beim Internetprovider oder Telekommunikationsanbieter.

a. **Personalien:** Vor- und Zuname allein genügen nicht für die Ermittlung einer ladungsfähigen Anschrift. Zur Durchführung einer Einwohnermeldeamtsanfrage bedarf es darüber hinaus einer früheren Adresse oder eines Geburtsdatums.

b. **E-Mail:** Nach unserem Kenntnisstand ist eine Auskunftspflicht der Mail-Provider - soweit es sich nicht um Telekommunikationsdienstanbieter handelt - gesetzlich nicht geregelt. Eine Herausgabe der Daten wird daher allenfalls bei Vorliegen eines berechtigten Interesses aus Kulanz erfolgen.

c. **IP-Adresse:** Selbst, wenn man die IP-Adresse des letzten Logins erhält und dieser weniger als sechs Tage zurückliegt, mangelt es an einer auf Herausgabe der Nutzerdaten gerichteten Anspruchsgrundlage gegen den Internetprovider. Im Urheberrecht ist ein solcher Auskunftsanspruch in § 101 UrhG geregelt. Ähnliche Vorschriften finden sich auch in anderen Bereichen des gewerblichen Rechtsschutzes, wie dem Marken- und Patenrecht. Für den Fall der Abfrage von Nutzer*innendaten nach Erlangung der IP-Adresse gemäß § 14 Abs. 3 TMG bedürfte es eines vergleichbaren Tatbestandes, der allerdings anders als § 101 UrhG kein weiteres Gerichtsverfahren zum Gegenstand haben sollte. Wir empfehlen daher eine solche Anspruchsgrundlage mit § 14 TMG zu verknüpfen, da die im Wege der Auskunft nach 14 TMG erlangte IP-Adresse bis zum Abschluss eines weiteren Verfahrens gelöscht ist.

d. **Telefonnummer:** Auch hierfür bedürfte es einer rechtssicheren Anspruchsgrundlage gegen den Mobilfunkanbieter.

Gängige Praxis ist, dass die Strafverfolgungsbehörden Ermittlungsverfahren wegen Beleidigungsdelikten in der überwiegenden Zahl der Fälle einstellen und/oder auf den Privatklageweg verweisen. **Daher ist es bereits unter rechtsstaatlichen Gesichtspunkten erforderlich, eine zuverlässige und rechtssichere Durchsetzung zivilrechtlicher Ansprüche sicherzustellen.** Entscheiden sich couragierte Betroffene nämlich, auf eigene Kosten gemäß § 14 Abs. 3 TMG gegen die Täter*innen vorzugehen, müssen im Erfolgsfall die erlangten Daten auch tauglich sein, um diese zu ermitteln. Alles andere hätte lediglich einen weiteren Vertrauensverlust der Bevölkerung in den Rechtsstaat zur Folge und würde ein zivilrechtliches Vorgehen in der Praxis völlig aushebeln. Besonders gravierend ist das in Anbetracht der Tatsache, dass die Beleidigungsdelikte als reine Antragsdelikte somit praktisch straffrei immer ungeahndet bleiben könnten. Auch der im Gesetzesentwurf zur Bekämpfung von Hasskriminalität und Rechtsextremismus vorgesehene erhöhte Strafrahmen für Beleidigungen würde so ins Leere laufen.

Denkbar sind an dieser Stelle verschiedene (kumulative) Lösungsansätze:

a. Aktuell wird über eine **Authentifizierungspflicht** für Nutzer*innen Sozialer Medien diskutiert. Angestoßen wird diese Debatte derzeit von den Bundesländern Niedersachsen und Mecklenburg-Vorpommern über einen in den Bundesrat eingebrachten Gesetzesantrag. Eine solche Identitätsprüfungspflicht sehen wir aus datenschutzrechtlichen und anderen Gründen allerdings sehr kritisch. Bislang schreibt das Gesetz den Telemediendiensteanbietern aus gutem Grunde ausdrücklich vor, dass sie eine anonyme oder unter Pseudonym erfolgende Nutzung ermöglichen müssen.

   Der Gedanke an die persönlichen Daten aller Nutzer*innen in der Hand der Plattformbetreiber bereitet ein großes Unwohlsein. Denn diese können sodann mit einer Unmenge von Daten zum Nutzungsverhalten der nun vom Unternehmen identifizierbaren Nutzer*innen verknüpft und gezielt für Microtargeting genutzt werden. Es ist außerdem zu befürchten, dass durch eine Identitätsprüfungspflicht auch Menschen aus den Sozialen Medien ferngehalten werden, die nicht etwa aus unlauteren Motiven, sondern aus Gründen des Selbstschutzes vermeiden möchten, ihre korrekten persönlichen Daten anzugeben.

b. **Uneingeschränkt abzulehnen ist eine Klarnamenpflicht** in dem Sinne, dass die Nutzer*innen mit ihrem authentischen Namen auf der Plattform auftreten müssen. Ohne Klarnamen im Netz aktiv sein zu können, ist für viele Internetnutzer*innen immens wichtig. Dies gilt vor allem für diejenigen, die in besonderem Maße gefährdet sind, zur Zielscheibe von Anfeindungen zu werden – sei es wegen ihrer Herkunft, ihrer Religion, ihres Geschlechts, ihrer sexuellen Ausrichtung oder ihrer politischen Haltung.

c. Eine vergleichsweise einfache, weit weniger eingriffsintensive Maßnahme mit hohem Nutzen könnte es dem gegenüber sein, wenn die Plattformbetreiber bei Anmeldung zwingend die **Mobilfunknummer** der Nutzer*innen erfragen und sie verifizieren müssten. Die Handynummer wäre bei der Anmeldung über einen per SMS zugesandten Code zu bestätigen. Diese Maßnahme würde es ermöglichen, dass Bestandsdaten erhoben und beauskunftet werden, die relativ zuverlässig weitere Nachforschungen zu der dahinterstehenden Person durch entsprechende Auskunftsersuche bei den Telekommunikationsdiensteanbietern ermöglichen. Die Zulässigkeit der in § 111 TKG geregelten Identifizierungspflicht, welche dem Missbrauch von anonym erworbenen "Wegwerf-SIM-Karten" vor allem im Bereich der Rauschgift-, organisierten Kriminalität und Terrorismus entsprungen ist, hat der EGMR jüngst bestätigt (Urt. v. 30.01.2020, Az. 50001/12).

d. Soll weiterhin gleichermaßen eine Registrierung unter Angabe einer **E-Mail-Adresse** möglich sein, so wäre es erforderlich, dass künftig auch Webmail-Anbieter verpflichtet werden, eine Verifizierung der angegebenen persönlichen Daten vorzunehmen. Für das Prozedere und die sich hieraus ergebenden Ermittlungsmöglichkeiten gilt das für die Authentifizierung mittels Mobilfunknummer Gesagte.

Weiterhin sehen wir Handlungsbedarf bei der Schaffung **beschleunigter Auskunftsverfahren** für IP-Adressen. Es muss verhindert werden, dass diese durch Zeitablauf wertlos werden. Hier bietet es sich an, sich für eine Lösung am Urheberrecht zu orientieren. Gängige Praxis seitens der Gerichte ist es bei Abmahnungen wegen Filesharing auf Grundlage des § 101 Abs. 1 UrhG, der § 14 Abs. 3 TMG strukturell ähnlich ist, einen sogenannten Sicherungsbeschluss zu erlassen. Dieser verpflichtet die Provider zur Aufbewahrung der IP-Adresse. Die Provider werden so veranlasst, die betroffene IP-Adresse nunmehr anlassbezogen über 6 Tage hinaus zu speichern ("Quick Freeze"), bis eine richterliche Gestattung vorliegt. Wird diese nicht binnen einer Frist vorgelegt, löschen die Provider die IP-Adresse. Dies wird aus Kulanz praktiziert, ist jedoch zur Vermeidung weitergehender Ermittlungsmaßnahmen auch im Interesse der Provider.

Darüber hinaus sollte die **Kostenregelung** überdacht werden. Derzeit regelt § 14 Abs. 4 TMG die jederzeitige Kostentragung des Verletzten. Zwar ist nach derzeitiger Gesetzeslage die Kostentragungsregelung dogmatisch richtig. Mit der Einführung einer Auskunftspflicht bei Vorliegen eines rechtswidrigen Inhalts, sollte diese Regelung überdacht werden. Die Regelung einer Kostentragung nach den Grundsätzen des § 91 ZPO sollte hier erwogen werden. Der Gesetzgeber ist hier aufgefordert, eine Lösung zu erarbeiten, bei der Betroffene von rechtswidriger Hassrede nicht in Vorkasse gehen bzw. das Kostenrisiko gänzlich allein tragen müssen.

III. Berichtspflichten, § 2 NetzDG - E

Die geplanten Änderungen des § 2 NetzDG, welche die Berichtspflichten anpassen und weiter ausgestalten sollen, sind grundsätzlich zu begrüßen. Im Ergebnis reichen Sie jedoch nicht weit genug und drohen teilweise ins Leere zu laufen.

Grundsätzlich sind die halbjährlichen Berichte geeignet den Umgang der sozialen Netzwerke mit rechtswidrigen Inhalten offenzulegen. Sie geben so der Wissenschaft und der Öffentlichkeit Einblicke in das Phänomen der Hasskriminalität im Netz. Auch der Gesetzgeber kann hieraus Erkenntnisse über die Auswirkungen und Wirksamkeit des NetzDG gewinnen und ggf. Regelungsbedarfe ableiten. Auch die Netzwerke können auf diese Weise Transparenz schaffen, wo häufig der Eindruck der Willkür herrscht. Nach wie vor sind Entscheidungen der Netzwerke im Zusammenhang mit der Content-Moderation für Betroffene häufig nicht nachvollziehbar und wirken unsystematisch. Es bleibt zu hoffen, dass eine Ausweitung der Berichtspflichten den Netzwerken als Anreiz dafür dient, diese Praktiken zu vereinheitlichen. Valide Erkenntnisse lassen sich aus den Berichten jedoch nur dann ableiten, wenn diese auch vergleichbar sind. Aus diesem Grund sind klare und ausdifferenziert formulierte Anforderungen an die Berichte wichtig, um eine einheitliche Gestaltung sicherzustellen.

Insoweit der Entwurf eine Erweiterung der Berichtspflicht auf die Zurverfügungstellung von Daten für wissenschaftliche Zwecke vorsieht, droht die Regelung aber ins Leere zu laufen. Denn mangels Verpflichtung und Bereitschaft der Netzwerke (anonymisierte) Daten zu Forschungszwecken zur Verfügung zu stellen, findet dies bisher schlicht kaum statt. Im Gegenteil: Netzwerke haben den Zugang zu zwischenzeitlich öffentlich zugänglichen Daten, die für Forschungszwecke genutzt wurden, restringiert und gekappt. Teilweise wird ein Zugang nur kostenpflichtig angeboten. Bisherige Studien waren stets auf eigene empirische Erhebungen angewiesen. Auch eine Bereitschaft zur **Schaffung von Schnittstellen**, welche eine automatisierte Auswertung der Daten sozialer Netzwerke zulassen würden, besteht seitens der Netzwerke nicht. Diese wären jedoch Voraussetzung um große Datenmengen automatisiert auszuwerten und so eine unabhängige Forschung zu gewährleisten. Hierüber ließen sich ggf. auch Erkenntnisse darüber ableiten, gegen welche Bevölkerungsgruppen sich die Äußerungen richten. Eine Berichtspflicht, welche die Kategorisierung der Betroffenen vorsieht, wurde mit guten Gründen aus dem Regierungsentwurf gestrichen. Denkbar ist jedoch eine Analyse nicht der Betroffenen, sondern der Kommentare. Hieraus lassen sich wertvolle Erkenntnisse für Wissenschaft und Forschung ableiten. Diese sollte auch in Zukunft entsprechende Erhebungen durchführen können, die Rückschlüsse auf die Motivation und Hintergründe von Hassrede im Netz zulassen. Solche Schnittstellen wären auch geeignet, um die Funktionsweise der Algorithmen nachvollziehen zu können. Hieraus ließen sich Rückschlüsse darauf ableiten, warum welchen Inhalten eine bessere Sichtbarkeit zukommt als anderen. Die Kosten für entsprechende Forschungsprojekte sollten die Netzwerke tragen, allerdings muss die Zusammenarbeit so ausgestaltet werden, dass die Unabhängigkeit der Forschung gewahrt bleibt.

Im Ergebnis sollten alle öffentlichen Daten für wissenschaftliche Zwecke über eine Schnittstelle kostenlos durchsuchbar sein. Hierfür sollte ein Prozess eingerichtet werden, über den sich Wissenschaftler für ein spezifisches Projekt registrieren können, z.B. über eine App. Hierüber könnte auch abgefragt werden, wie bspw. datenschutzrechtliche Bestimmungen im Rahmen des Projekts eingehalten werden sollen. Ablehnungen der Registrierung bedürfen einer Begründung, um eine unabhängige Forschung zu gewährleisten. Praktikable Ansätze zur Wahrung des Datenschutzes gibt es bereits: So werden bspw. Teilweise nicht volle Datensätze, sondern lediglich sog. IDs ausgetauscht, über die ein Datensatz/Kommentar wiederum aufgerufen werden kann. Wird dieser gelöscht, ist auch die ID nicht mehr verwendbar, wodurch Nutzer*innen die Kontrolle über die Inhalte behalten.

Mangels Zugangs zu Daten für wissenschaftliche Zwecke, sind die Berichte der Netzwerke nicht überprüfbar. Auf diese Weise kommt den sozialen Netzwerken das wohl einzigartige Privileg zu, sich allein selbst zu evaluieren und zu kontrollieren. Dass eine solche Kontrolle erforderlich ist, zeigen bspw. Erhebungen des Counter Extremism Project (CEP). Diese haben gezeigt, dass die realen Löschquoten rechtswidriger Inhalte erheblich von den offiziell durch die Netzwerke kommunizierten abweichen.[2] Hiermit soll den Netzwerken keineswegs eine Meldung unzutreffenden Zahlenmaterials unterstellt werden. Die aktuelle Ausgestaltung der Berichtspflicht lässt jedoch enorme Spielräume zu, sodass nicht nachvollziehbar ist, welche Meldungen überhaupt in diese Statistik eingeflossen sind.

Dies ist nicht zuletzt dem Umstand geschuldet, dass die Netzwerke jede Gelegenheit nutzen, um sich den Vorgaben des NetzDG zu entziehen. Hierauf wird auch im Zusammenhang mit der geplanten Änderung des § 5 NetzDG noch einmal einzugehen sein. Denn: Solange ein **Vorrang des NetzDG** vor Gemeinschaftsstandards der Netzwerke nicht gesetzlich verankert ist, werden die Netzwerke Meldungen stets zuerst auf die Vereinbarkeit mit internen Richtlinien prüfen. Erfolgt eine Meldung also nach Gemeinschaftsstandards, wird sie auch nur an diesem Maßstab gemessen also nach den Richtlinien der s.g. Gemeinschaftsstandards, die sich nicht an deutschem Recht orientieren. Eine Meldung nach NetzDG hingegen wird zuerst auf die Vereinbarkeit mit Gemeinschaftsstandards überprüft und erst dann nach deutschem Recht auf Basis des NetzDG geprüft. Man folgt dem Grundsatz: Wenn ein Inhalt ohnehin gegen interne Richtlinien verstößt, kommt es aufs NetzDG nicht an. Hinzu kommt, dass der Meldeweg nach NetzDG in der Regel schwer auffindbar und nicht annähernd so niedrigschwellig ausgestaltet ist wie der nach Gemeinschaftsstandards. Dem wird durch die geplante Neufassung des § 1 Abs. 4 NetzDG-E nur teilweise abgeholfen. Dies hat zweierlei Auswirkungen: Zum einen schlägt sich weder die Meldung noch die Löschung (verbindlich) im Bericht nieder, da sie nicht “nach NetzDG”, sondern nach Gemeinschaftsstandards erfolgte. Zum anderen finden auch die weiteren Vorschriften des NetzDG pro forma keine Anwendung. So wird in Bezug auf diesen Inhalt kein Gegenvorstellungsverfahren stattfinden und sich auch kein Zustellungsbevollmächtigter im Inland verantwortlich fühlen. Man darf hierbei auch nicht außer Acht lassen, dass sich nicht nur das NetzDG im Spannungsfeld der Meinungsfreiheit bewegt. Auch die Gemeinschaftsstandards schränken die Meinungsfreiheit ein und gehen hierbei häufig weit über gesetzliche Regelungen hinaus. Dabei unterliegen sie allein den Vorstellungen der sozialen Netzwerke - losgelöst von nationalem oder europäischen Recht. Für eine effektive Stärkung der Nutzer*innenrechte ist also der Vorrang des NetzDG vor den Gemeinschaftsstandards unabdingbar. Wir plädieren dafür, dass die Netzwerke genau im Gegensatz zur bisherigen Praxis alle Meldungen zunächst nach NetzDG und dann ggf. noch nach ihren Gemeinschaftsstandards prüfen.

Im Einzelnen:

Zur geplanten Nr. 2:

Dass die Plattformbetreiber der Öffentlichkeit nachvollziehbar über die angewandten Methoden der KI und den Umgang der mithilfe derartiger automatisierter Verfahren herausgefilterten Inhalte berichten, ist im Sinne der Transparenz unerlässlich. Es ist wichtig,

[2] https://www.counterextremism.com/sites/default/files/CEP%20NetzDG%202.0%20Policy%20Paper.pdf (Stand: 14.6.2020)

die Wirkungsweise und die Überprüfung der bereits jetzt zahlreich durch soziale Netzwerke eingesetzten Technologien nachzuvollziehen.

Bei allen berechtigten Bedenken, die in Bezug auf das “Ob” einer automatisierten Erkennung rechtswidriger Inhalte bestehen mögen, muss folgendes berücksichtigt werden:

In sozialen Netzwerken werden täglich unzählige Inhalte hochgeladen. Auf YouTube sind es 12.000 Stunden Videomaterial, bei Facebook ca. eine Milliarde Beiträge, inklusive 300 Millionen Bilddateien[3]. Wir haben es hier also mit einer schier nicht greifbaren Masse an potenziell rechtswidrigen Inhalten zu tun. Deren händische Bearbeitung scheint unmöglich, bzw. wirtschaftlich unzumutbar. Der Einsatz von KI ist daher aus unserer Sicht unerlässlich, wenn man sich für eine effektive Bekämpfung der Verbreitung rechtswidriger Inhalte einsetzen will. Umso wichtiger ist es, hierüber Transparenz zu schaffen.

Es wäre vor diesem Hintergrund falsch, den Einsatz von KI pauschal zu verteufeln. Stattdessen sollte die Anwendung, die längst Realität ist und nicht mehr zur Debatte steht, nachvollzogen und auf Sinnhaftigkeit geprüft werden. Eine Ausweitung der Berichtspflichten ist unerlässlich, um nachzuvollziehen wie KI eingesetzt und vor allem kontrolliert wird. Denn auch die Nutzung von Technologie ist nicht in jedem Fall geeignet, um über eine Löschung zu entscheiden. Dies gilt vor allem dann, wenn es auf den Kontext ankommt, zu dessen Beurteilung es einer manuellen Einschätzung zwingend bedarf. Um beurteilen zu können, ob dies hinreichend berücksichtigt wird, bedarf es jedoch einer Kenntnis von Entscheidungskriterien. Die Informationen hierüber können nur von den Netzwerken selbst erlangt werden, weswegen die Auskunft hierüber zu befürworten ist. Die Berichtspflicht sollte weiterhin zwingend auf die Frage erweitert werden, in wie vielen Fällen durch KI getroffene Einschätzungen manuell oder nach Gegenvorstellung revidiert werden.

Zur geplanten Nr. 3:

In der Tat wurde bislang in den Transparenzberichten über die Entscheidungskriterien, die die Netzwerke dem Umgang mit Beschwerden zugrunde legen, nur unzureichend berichtet. Nicht aufgeschlüsselt wurde außerdem, welcher Anteil der gemeldeten Inhalte nach Gemeinschaftsstandards weltweit gelöscht wurde und welcher Anteil lediglich in Deutschland gesperrt wurde. Dies ist zur Beurteilung der Auswirkungen des NetzDG von Bedeutung.

Zur geplanten Nr. 11:

Wir begrüßen, dass künftig auch die Abhilfequote nach erfolgter Gegenvorstellung mitgeteilt werden soll. Allerdings können Inhalte auch aufgrund einer anderweitigen außergerichtlichen Einigung oder einer von einem Gericht ausgesprochenen Verpflichtung wiedereingestellt werden, bzw. es kann vom Gericht festgestellt werden, dass ein Inhalt zu Unrecht entfernt wurde. Auch diese Zahlen sind relevant und sollten mitgeteilt werden. Die “Fehlerquote” kann Aufschluss darüber geben, ob das von Kritiker*innen des NetzDG befürchtete Overblocking stattfindet oder nicht. Sie ist ein Indikator dafür, ob die Plattformbetreiber willkürlich die Meinungsäußerungsfreiheit der Nutzer*innen durch die Anwendung des NetzDG einschränken oder nicht.

[3] https://www.counterextremism.com/sites/default/files/CEP%20NetzDG%202.0%20Policy%20Paper.pdf (Stand: 14.06.2020)

Zur geplanten Nr. 13

Dass Unterstützungsmaßnahmen für Betroffene von strafbarer Hassrede durch die Plattformbetreiber auch in den Transparenzberichten Niederschlag finden sollen, ist zu begrüßen. Wir hoffen, dass die Netzwerke dadurch, dass sie über Unterstützungsangebote berichten sollen, stärker angehalten werden, in dieser Hinsicht auch praktisch tätig zu werden.

Zur geplanten Nr. 14

Die geplante Einführung einer Berichtspflicht über die Anzahl von Meldungen und Anteilen der Löschungen, bzw. Wiederherstellung ist zu begrüßen. Sie erscheint geeignet, um Erkenntnisse über das Löschverhalten der Netzwerke zu gewinnen. Bzgl. der Aussagekraft im Hinblick auf möglicherweise nach Gemeinschaftsstandards gelöschte Inhalte wird auf die obigen Ausführungen verwiesen. Aus den bereits genannten Gründen erachten wir es jedoch für notwendig innerhalb dieses Berichts nach Meldungen und Löschungen aufgrund Gemeinschaftsstandards und NetzDG zu differenzieren. Gleichfalls sollte der Anteil, der aufgrund von KI gelöschten Inhalte erfasst werden. Wir empfehlen zudem die Berichtspflicht auf die Anzahl der identifizierten und gelöschten sogenannten Fake Profile oder Social Bots.

IV. Beschwerdeverfahren und Gegenvorstellung - §§ 3 – 3 c) NetzDG – E

Die §§ 3 – 3 c) NetzDG sehen nunmehr insgesamt drei Verfahren vor, um eine außergerichtliche Klärung über die Rechtswidrigkeit von Kommentaren herbeizuführen.

Zunächst erlangt das jeweilige Netzwerk durch eine Beschwerde gemäß § 3 NetzDG Kenntnis von einem potenziell rechtswidrigen Kommentar. Daraufhin ergeht entweder fristgerecht eine Entscheidung über die Löschung oder das Netzwerk gibt das Verfahren an eine Stelle der regulierten Selbstregulierung ab, deren Entscheidung es sich unterwirft.

Wird der Beschwerde nicht oder nach Auffassung des von der Löschung betroffenen Nutzers zu Unrecht abgeholfen, kann nunmehr gemäß § 3 b NetzDG – E ein Antrag auf Gegenvorstellung gestellt werden. Wann diesem Antrag stattzugeben ist, bleibt hingegen unklar. Wird der Beschwerde nicht abgeholfen und nimmt das Netzwerk freiwillig an der Schlichtung teil oder wurde zuvor erfolglos ein Gegenvorstellungsverfahren durchgeführt, kann eine beim BfJ registrierte Schlichtungsstelle vermitteln.

Fraglich ist in erster Linie, ob die Einrichtung von gleich drei verschiedenen Verfahren zur außergerichtlichen Streitbeilegung sinnhaft ist. Dies gilt vor allem vor dem Hintergrund, dass nach dem derzeitigen Stand des Entwurfs weder für die Gegenvorstellung noch für die Schlichtung materiellrechtliche Vorgaben für eine Wiederherstellung, zeitliche Vorgaben für die Verfahrensdauer oder eine Bindungswirkung der Entscheidung formuliert sind. Wir fragen uns daher, ob die Parallelität und fehlende Spezifizierung der beiden Verfahren Betroffene nicht eher abschreckt und wünschen und regen an hier Klarheit über den Ablauf, bzw. die

Rangfolge zu schaffen oder die Verfahren zusammenzuführen. Grundsätzlich erscheint die Einbeziehung einer dritten unabhängigen Stelle hierfür vorzugswürdig.

Hiervon zu Recht unabhängig ist die Möglichkeit der Anrufung der ordentlichen Gerichte und einer Beschwerde beim BfJ gemäß § 4 NetzDG, welches möglicherweise ein Bußgeldverfahren nach sich zieht.

1. Beschwerdeverfahren, § 3 NetzDG-E

Die vorgesehenen Änderungen zur Ausgestaltung der Meldewege erscheinen uns grundsätzlich sachgerecht, sollten jedoch in wesentlichen Punkten nachgebessert werden.

a) Meldeweg - § 3 Abs. 1 NetzDG-E

Einzelne Netzwerke haben die Meldung nach dem NetzDG strikt von dem allgemeinen Meldeweg nach Gemeinschaftsstandards getrennt. Dies war eine Spitzfindigkeit, die den starken Verdacht erwecken musste, dass das neue Gesetz umgangen werden soll. Hierauf wurde bereits in § 1 Abs. 4 NetzDG-E des Entwurfes eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität reagiert. Dort wird klargestellt, dass jede Beanstandung von Inhalten mit dem Ziel, dass diese entfernt oder gesperrt werden, eine Beschwerde über rechtswidrige Inhalte ist. Dies sollte den getrennten Meldewegen den Boden entzogen haben. Unklar geblieben ist jedoch, ob sicher hieraus auch ein zwingender Vorrang der Bewertung nach NetzDG ergeben soll. Dies ist nach unserem Dafürhalten durch den Wortlaut nicht sichergestellt. Aus diesem Grund sprechen wir uns für die Normierung eines darüberhinausgehenden Vorrangs des NetzDG vor Gemeinschaftsstandards aus. Um weiteren Ausweichmanövern vorzubeugen, halten wir es – wie im Referentenentwurf vorgesehen - für dennoch sinnvoll, dass in § 3 Abs. 1 NetzDG-E die Anforderungen an den Meldeweg weiter spezifiziert werden.

Grundsätzlich zu begrüßen ist, dass der Meldeweg künftig “bei der Wahrnehmung des Kommentars” erkennbar sein muss. Dass Meldeformulare derart gut versteckt sind, wie es bekanntermaßen bislang bei einzelnen der großen Anbieter der Fall ist, wird damit hoffentlich der Vergangenheit angehören. Abzuwarten bleibt, wie dies durch die Netzwerke ausgestaltet wird. Wünschenswert wäre, dass eine Meldung durch eine neben dem Kommentar befindliche Schaltfläche vorgenommen werden kann und nicht lediglich ein Hinweis auf die Beschwerdemöglichkeit erkennbar ist.

Zu kritisieren ist die geplante Änderung, wonach das Beschwerdeverfahren “leicht bedienbar” sein soll. Wir empfehlen diese Formulierung dringend nachzubessern und konkrete Vorgaben für die Ausgestaltung des Meldeformulars zu geben. Derartige Vorgaben könnten bspw. sein:

- Ohne Angabe eines Rechtsgrundes
- Begründung durch kurze Darlegung von Tatsachen

Die Alternative ist sonst, abzuwarten, was die Netzwerke unter einer “leichten Bedienbarkeit” verstehen. Aktuell ist zu beobachten, was unter der bereits geregelten “leichten Auffindbarkeit” und “unmittelbaren Erreichbarkeit” nach § 3 Abs. 1 S. 2 NetzDG verstanden wird. Wie bereits

dargelegt, wird auch hieran berechtigte Kritik geübt, da die Meldewege teilweise sehr versteckt und entsprechend schwer auffindbar sind.

Zu den Anforderungen, die an das Beschwerdevorbringen zu stellen sind, ist aus unserer Sicht zweierlei anzumerken: Einerseits erscheint es weit überzogen und widerspricht dem Zweck des Gesetzes, wenn nur juristisch vorgebildete Personen sich in der Lage sehen, ein Meldeformular auszufüllen. Denn neben diversen Angaben zur eigenen Person wird eine (straf-)rechtliche Subsumtion und eine umfangreiche Begründung verlangt. Derartige Meldeformulare schrecken die Nutzer*innen ab und führen dazu, dass diese entweder gar nicht melden oder den Umweg über eine Beschwerdestelle wählen werden. Andererseits ist eine einfache Meldemöglichkeit auch missbrauchsanfällig. Es kommt vor, dass – teils in geschlossenen Gruppen verabredet – Inhalte massenhaft gemeldet werden, die offensichtlich nicht rechtswidrig sind. Ziel derartiger Aktionen ist es, missliebige Nutzer*innen zu schikanieren. Wir halten es deshalb für durchaus angebracht, dass die Netzwerke den meldenden Nutzer*innen ein Mindestmaß an Begründung abverlangen und die Nutzer*innen nicht wirksam eine Beschwerde erheben können, indem sie sich lediglich auf Gutdünken durch mehrere Multiple-Choice-Eingabemasken “klicken”.

Letztlich sollte sich die Gestaltung der Meldeformulare durch die Plattformbetreiber zwischen den beiden vorgenannten Extremen bewegen. Hier wird gegebenenfalls das Bundesamt für Justiz als zuständige Aufsichtsbehörde, deren Aufgaben und Befugnisse mit dem neuen § 4a NetzDG-E ausgeweitet werden, steuernd eingreifen müssen.

b) Beweissicherung - § 3 Abs. 2 Ziff. 4 NetzDG-E

Im Zusammenhang mit den in § 3 Abs. 2 Ziff. 4 NetzDG geregelten Beweissicherungspflichten sei erneut auf das Problem hingewiesen, dass bislang ein Vorrang des NetzDG nicht formuliert ist. Uns ist nicht bekannt, wie die Netzwerke verfahren, wenn ein Inhalt nach dem NetzDG gemeldet wurde, er jedoch – wie nach Auskunft der großen Betreiber in der ganz überwiegenden Zahl der Fälle – wegen Verstoßes gegen die Gemeinschaftsstandards weltweit gelöscht wird. In diesen Fällen hat der Betreiber letztlich für sich keine Entscheidung darüber getroffen, ob einer der in § 1 Abs. 3 NetzDG genannten Straftatbestände erfüllt ist und deshalb eine Pflicht zur Speicherung des Inhalts und der hiermit verknüpften Daten besteht. Es ist zu befürchten, dass eine Beweissicherung unter diesen Voraussetzungen nicht stattfindet. Um dem zuvorzukommen, müssen die Betreiber dazu angehalten werden, Meldungen nach NetzDG in einem ersten Schritt immer auch nach NetzDG zu prüfen und erst dann ggf. nach Gemeinschaftsstandards. Dies sollte im Gesetz verankert sein.

Aus Sicht der Strafverfolgungsbehörden und auch der individuell Geschädigten von digitaler Hasskriminalität, die ihre Belange auf dem zivilrechtlichen Weg geltend machen wollen, ist es immens wichtig, dass die Beweissicherung vorgenommen wird. Rechtsdurchsetzung darf nicht daran scheitern, dass sämtliche Daten weltweit gelöscht sind. Das weltweite Löschen beanstandeter Inhalte wegen Verstoßes gegen Gemeinschaftsstandards ist im Übrigen auch problematisch in den Fällen, in denen es seitens der Plattform zu einer Fehlentscheidung gekommen ist und die Inhalte wieder einzustellen sind. Es wird angeregt, auch insoweit über eine Lösung nachzudenken. Inhalte könnten generell von den Plattformbetreibern zunächst nicht gelöscht, sondern nur verborgen werden. Dies würde die Beweissicherung in allen Fällen erleichtern.

Darüber hinaus bedarf es einer Regelung, wonach die Netzwerke zur Kooperation mit Ermittlungsbehörden verpflichtet werden. Andernfalls läuft auch die Pflicht zur Beweissicherung ins Leere, wenn eine Herausgabe an die Ermittlungsbehörden nicht erfolgt. Dies wurde teilweise durch den Gesetzentwurf zur Bekämpfung von Rechtsextremismus und Hasskriminalität und die dort vorgesehenen Änderungen der StPO angegangen. Ob sich diese Regelung auch für die ebenfalls in § 1 Abs. 3 NetzDG erfassten § 185 ff. StGB als effektiv erweist oder die Ermittlungsbehörden weiterhin an ein Rechtshilfeersuchen in das Land der Datenspeicherung verwiesen werden, bleibt abzuwarten. Durch eine Klarstellung im Gesetz könnte hier in der Praxis eine klare Regelung geschaffen werden.

c) Informationspflichten - § 3 Abs. 2 Ziff. 5 NetzDG-E

Die Notwendigkeit, auf die Möglichkeit der Gegenvorstellung hinzuweisen, ergibt sich aus § 3b NetzDG-E. Zu begrüßen ist aus Opferschutzgesichtspunkten auch, die Hinweispflicht, um einen Hinweis auf die Frist der Gegenvorstellung und die Möglichkeit der Weitergabe des Inhalts zu erstrecken.

Für begrüßenswert halten wir grundsätzlich auch, dass Beschwerdeführer*innen über die Möglichkeiten von Strafanzeige und Strafantrag belehrt werden sollen. Vielen Nutzer*innen, die in den Sozialen Medien beleidigt oder bedroht werden, ist weder bewusst, dass derartige Äußerungen strafrechtlich verfolgt werden können, noch ist ihnen bekannt, wie sie eine Strafverfolgung veranlassen können. Allerdings halten wir den bloßen pauschalen Hinweis auf “Informationen auf Internetseiten” nicht für ausreichend. Vielen Nutzer*innen wird es an der Kenntnis darüber mangeln, wie eine solche Strafanzeige gestellt werden kann und welche Voraussetzungen hierfür erfüllt sein müssen. Gleiches gilt für die Strafantragsfrist gemäß § 77 b StGB.

Wir empfehlen daher die Einführung einer Pflicht zur Information über:

1. Informationen über die zuständige Polizeidienststelle, ggf. Eine Auflistung derer mit Hinweisen darauf, ob eine Anzeige über eine Onlinewache, andere elektronische Wege oder nur persönlich/per Post erstattet werden kann.

2. Hinweise auf Form, § 158 Abs. 2 StPO, und Frist, § 77 b StGB, des Strafantrages.

3. Hinweise darauf, wie ein Kommentar rechtssicher unter Erfassung von Datum, Uhrzeit und Kontext gesichert werden kann. Einige Netzwerke erschweren die Sicherung des Datums und der Uhrzeit eines Kommentars, in dem diese nicht angezeigt werden. Teilweise ist eine rechtssichere Sicherung bei Nutzung über eine Smartphone - App sogar unmöglich. Hierdurch droht ein Beweisverlust, wenn der Inhalt bspw. zwischenzeitlich durch den Nutzer gelöscht oder das Profil gesperrt wurde. Den meisten Nutzer*innen ist dies ebenso wenig bewusst wie der Umstand, dass es eines solchen Screenshots zur Rechtsdurchsetzung bedarf.

Für wünschenswert halten wir auch die Vorhaltung einer “Musterstrafanzeige” durch die Netzwerke, welche die Nutzer*innen ausfüllen können.

2. Gegenvorstellungsverfahren - § 3b NetzDG-E

Ein Gegenvorstellungsverfahren ist eine unserer zentralen Empfehlungen für eine Stärkung der Nutzer*innenrechte im Rahmen des NetzDG und des Umgangs der Plattformbetreiber mit der Beanstandung rechtswidriger Inhalte. Es muss den Nutzer*innen, die mit der Entscheidung der Plattform nicht einverstanden sind, möglich sein, Kontakt zu den Verantwortlichen aufzunehmen. Sie müssen die Möglichkeit haben, in einem definierten Verfahren eine Revision der getroffenen Entscheidung herbeizuführen.

Aus Nutzer*innensicht ist bislang zu bemängeln, dass die Plattformbetreiber Beschwerden zu rechtswidrigen Inhalten allzu lapidar und regelmäßig nur mit formelhafter, nicht einzelfallbezogener Begründung abtun. Es mag auch umgekehrt vorkommen, dass Inhalte gelöscht werden, die die Grenzen der Meinungsäußerungsfreiheit nicht überschreiten und nicht einmal einen Verstoß gegen die Gemeinschaftsstandards erkennen lassen. Hierbei würde es sich dann um das Overblocking handeln, das von Kritiker*innen des NetzDG bei der Verabschiedung des Gesetzes prognostiziert wurde. Ob ein solches Overblocking stattfindet, lässt sich gegenwärtig in Ermangelung wirklich aussagekräftiger Transparenzberichte nicht valide feststellen.

Bislang stehen Nutzer*innen den Entscheidungen der Netzwerke relativ macht- und hilflos gegenüber. Nicht jede*r kann und möchte allerdings sogleich die Gerichte in Anspruch nehmen. Es muss beiden Seiten, sowohl der meldenden als auch der gemeldeten Person, der Weg eröffnet sein, die Plattformbetreiber dazu zu bewegen, ihre Entscheidung zu überprüfen und ggf. abzuändern.

Wir begrüßen dabei die in § 3 b Abs. 2 Nr. 5 NetzDG-E vorgesehene Regelung, dass die Identität der am Verfahren beteiligten Personen nicht offenbart werden darf. Dies ist aus Opferschutzgesichtspunkten unerlässlich.

Die Einführung eines außergerichtlichen, niedrigschwellig erreichbaren Rechtsbehelfs in Gestalt des in § 3b NetzDG-E vorgesehenen, bei der Plattform selbst angesiedelten Gegenvorstellungsverfahrens begrüßen wir sehr. Allerdings erscheinen einige Details der vorgeschlagenen Regelung noch unklar oder diskussionswürdig:

1. § 3 b Netz-DG – E regelt zwar das Verfahren der Gegenvorstellung, lässt jedoch eine materiellrechtliche Grundlage vermissen. Es mangelt an einer Regelung nach welchen Grundsätzen das Netzwerk über eine Beschwerde und den Antrag auf Gegenvorstellung zu entscheiden hat. Nach dem gegenwärtigen Stand des Entwurfs können Beschwerden nach Belieben zurückgewiesen werden. Das Gesetz selbst regelt zwar, wann ein “rechtswidriger Inhalt” vorliegt, nicht jedoch, wann ein Inhalt veröffentlicht werden darf.

   Wünschenswert wäre es daher, zu normieren, dass eine Löschung nur dann erfolgen darf, wenn ein Verstoß gegen deutsches Recht oder ein Verstoß gegen die Gemeinschaftsstandards vorliegt. Gegen eine mit den Gemeinschaftsstandards begründete Entscheidung sind zu Unrecht von einer Löschung betroffene Nutzer*innen bisher schutzlos gestellt.

2. Netzwerke orientieren sich nach eigenen Angaben bei Entscheidungen über die Löschung von Kommentaren meist ohnehin vorrangig und ausschließlich an den hauseigenen Gemeinschaftsstandards. Die Ausgestaltung dieser Gemeinschaftsstandards ist bisher gesetzlich nicht geregelt. Die weitläufige Kritik wonach das NetzDG eine massive Bedrohung für die Meinungsfreiheit darstelle, wird insbesondere von den Netzwerken gern bedient. Diese Kritik ist nach unserem Dafürhalten unverständlich. Besonders deutlich wird dies, bei einem genaueren Blick auf die Gemeinschaftsstandards, die weitaus großzügigere Kriterien für eine Löschung ansetzen als das NetzDG.

   Exemplarisch sei auf die Gemeinschaftsstandards von Facebook verwiesen. Dort heißt es unter 12.: "Ist diese Absicht unklar, wird der Inhalt unter Umständen entfernt". Es folgt ein nahezu uferloser Katalog von Begriffen und Aussagen, die eine Löschung zur Folge haben können. Hierzu zählen: "kein Respekt für, nicht mögen, nicht ausstehen können".[4] Die Praxis zeigt, dass dies zu Recht keinesfalls der Maßstab für eine Löschungsentscheidung ist. Vielmehr dient die Formulierung der Gemeinschaftsstandards dem Zweck den Ermessenspielraum so groß wie möglich zu halten. Im Ergebnis kann daher nahezu jede Entscheidung der Content – Moderatoren gerechtfertigt sein. Eine Löschentscheidung kann so keiner sinnvollen Überprüfung unterzogen werden. Dies bedeutet, wenn eine Überprüfung nach NetzDG erfolglos bleibt, kann das Netzwerk dennoch auf eine Löschung bestehen. Die Gemeinschaftsstandards von Facebook wurden deswegen bereits mehrfach von den Gerichten als intransparent und im Rahmen der AGB Kontrolle als unwirksam befunden.[5] Hierbei ist auch die mittelbare Drittwirkung der Meinungsfreiheit zu berücksichtigen. Vor diesem Hintergrund empfehlen wir zum Schutz vor unberechtigter Löschung die Gemeinschaftsstandards einer spezifischen Inhaltskontrolle zu unterwerfen, um willkürlichen Entscheidungen vorzubeugen. Hierfür bedürfte es einer Klarstellung an welchen Maßstäben sich die Gemeinschaftstandards zu orientieren haben.

3. Zu empfehlen wäre nach diesen Ausführungen, dass das Gegenvorstellungsverfahren für **alle** Content-Entscheidungen eröffnet ist und nicht nur dann, wenn die ursprüngliche Beschwerde ausdrücklich nach dem NetzDG erfolgt ist. Dies ist im Interesse der Nutzer*innen und sollte etwaigen Tendenzen zum Overblocking insgesamt entgegenwirken. Ein solches Gegenvorstellungsverfahren wäre dann auch der erste Baustein des vielfach geforderten Put-Back-Verfahrens. Nach derzeitigem Stand können die Betreiber willkürlich oder rechtswidrig Löschentscheidungen treffen. Den betroffenen Nutzer*innen steht dabei keine leicht erreichbare Auskunfts- und Gegendarstellungsmöglichkeit zur Verfügung. Derartige Praktiken sorgen in hohem Maße für Unmut bei den Nutzer*innen. Sie können zu dem Eindruck beitragen, dass die Meinungsfreiheit eingeschränkt und Overblocking betrieben werde. Es besteht zwar die Möglichkeit, über ein Zivilgericht die Rechtswidrigkeit der Löschung oder Sperrung oder die Verpflichtung zu einer Entfernung von Inhalten feststellen zu lassen. Dieses Vorgehen ist jedoch mit einem Kostenrisiko für die Betroffenen verbunden und ausgesprochen langwierig. Eine zeitnahe Klärung im Rahmen des hausinternen

[4] Gemeinschaftsstandards von Facebook, Nr. 12: https://www.facebook.com/communitystandards/objectionable_content?_rdc=1&_rdr (Stand 14.06.2020)

[5] z.B. LG Mosbach, Beschluss vom 01. Juni 2018 – 1 O 108/18 –, Rn. 23, juris, OLG München, Beschluss vom 24. August 2018 – 18 W 1294/18 –, juris, OLG München, Urteil vom 07. Januar 2020 – 18 U 1491/19 Pre –, juris

Gegenvorstellungsverfahrens würde ebenfalls der Rechtsdurchsetzung im Netz dienen. Es würde die Rechte der Nutzer*innen, nicht in ihrer Meinungsäußerungsfreiheit beschnitten zu werden, stärken und mittelbar auch die Plattformbetreiber binden. Insofern erscheint es nicht unsystematisch, eine entsprechende Regelung in das NetzDG aufzunehmen.

4. Um einen Missbrauch zu vermeiden, dürfen die Netzwerke den Nutzer*innen unser Ansicht nach abverlangen, dass diese ihre Gegenvorstellung substanziell begründen. Dies ist aus unserer Sicht erforderlich, um einen massenhaften Missbrauch zu verhindern. Es geschieht nicht selten, dass sich Nutzer*innen dazu verabreden, Profile massenhaften zu melden, um deren Sperrung zu erwirken. Für die Betroffenen bedeutet dies nicht selten den Verlust des Profils oder wenigstens eine langwierige Odyssee, um die Wiederherstellung durchzusetzen.

5. Unklar erscheint uns, **wer** innerhalb der Netzwerke für die Entscheidung über die Gegenvorstellung berufen sein soll. In § 3 b Abs. 2 Nr. 3 NetzDG-E ist nunmehr geregelt, dass dies eine mit der Ausgangsentscheidung nicht befasste Person sein soll. Daraus geht hervor, dass es sich hierbei lediglich um eine*n anderen Content – Moderator*in handeln kann. Zu präferieren wäre unseres Erachtens eine hausinterne übergeordnete Stelle, die sich mit derartigen strittigen Fällen befasst. Im Idealfall wären hier Mitarbeiter*innen mit der Entscheidung befasst, die auf strittige und fachlich fordernde Fälle spezialisiert sind. Andernfalls ist zu befürchten, dass eine neuerliche Prüfung angesichts des hohen Zeitdrucks im Regelbetrieb nicht mit der gebotenen Sorgfalt ergeht.

6. Zu kritisieren ist, dass § 3 b NetzDG – E keine Regelung zu zeitlichen Vorgaben für das Gegenvorstellungsverfahren trifft. Es steht zu befürchten, dass derartige Entscheidung wegen Überlastung oder schlichten Unwillens hinausgeschoben werden. Dies kann Rechtsunsicherheit und einen Beweisverlust hervorrufen. Dies ist vor allem deswegen denkbar, weil die Entscheidung über eine Beschwerde gemäß § 3 NetzDG erwartungsgemäß bereits wegen der Bußgeldandrohung, § 4 NetzDG, prioritär behandelt werden wird. Dadurch verliert das Gegenvorstellungsverfahren an Attraktivität.

3. Schlichtung - § 3b NetzDG-E

Die Einrichtung einer privatrechtlich organisieren Schlichtungsstelle ist grundsätzlich zu befürworten. Sie ist tendenziell eine weitere Möglichkeit der außergerichtlichen Streitbeilegung. Die praktische Relevanz dieser Regelung ist jedoch zweifelhaft. Es besteht die Gefahr, dass ein Schlichtungsverfahren und eine Gegenvorstellung wegen der Ausgestaltung des § 3 c Abs. 3 NetzDG-E in seltenen Fällen parallel durchgeführt werden könnten. Ggf. wäre es Aufgabe der Netzwerke dies zu erkennen. Fraglich ist, was in einem solchen Fall mit dem Gegenvorstellungsverfahren geschieht. Es ist aus unserer Sicht unschädlich, eine Regelung zu treffen, wonach beide Verfahren einander ausschließen. Aus den oben geschilderten Gründen ist die Schlichtung gemäß § 3 c NetzDG – E ohnehin vorzugswürdig, wenn die Qualifikation der Schlichtungsstelle noch genauer definiert wird. Dies gilt bereits deswegen, weil hierdurch eine Dritte unabhängige und auf streitige Fälle spezialisierte Partei zur Entscheidung berufen wird. Dennoch gilt auch hier, dass unklar ist, nach welchen materiellrechtlichen Vorgaben die Überprüfung durch die Schlichtungsstelle

erfolgen soll und ob in diese Entscheidung auch die Gemeinschaftsstandards einfließen. Darüber hinaus ist unklar, inwiefern die Entscheidung der Schlichtungsstelle für das Netzwerk bindend sein soll. Wir empfehlen daher zu normieren, dass sich das Netzwerk der Entscheidung der Schlichtungsstelle ebenso zu unterwerfen hat, wie der Entscheidung der Einrichtung zur regulierten Selbstregulierung gemäß § 3 Abs. 2 Nr. 3 b) NetzDG.

Unklar ist auch, welche **Qualifikation** die in den Schlichtungsstellen tätigen Personen haben sollen. Sollen hier allein juristische Fragen geklärt werden, oder ist auch die Expertise anderer Berufsgruppen (z.B. aus den Bereichen Medien, soziale Arbeit, Psychologie) gefragt?

Fragen stellen sich auch bezüglich der **Finanzierung**. Geringfügige Gebühren für die Nutzer*innen sollten zwar erhoben werden, um einer Missbrauchsgefahr entgegenzuwirken. Diese dürften aber nicht kostendeckend sein. Es erscheint sachgerecht, die Kostenlast für das Betreiben von Schlichtungsstellen den Netzwerken aufzuerlegen. Denn die Notwendigkeit der Einrichtung von Schlichtungsstellen ergibt sich aus dem Geschäftsmodell der Netzwerke und den hieraus resultierenden Risiken für den gesellschaftlichen Frieden. Gleichzeitig muss aber sichergestellt sein, dass durch eine Finanzierung seitens der Netzwerke nicht die Unabhängigkeit und Unparteilichkeit der Schlichter*innen gefährdet ist.

Ergänzend sei angemerkt, dass die Schaffung von Schlichtungsstellen die Einführung wirksamer **gerichtlicher Rechtsbehelfe** gegen falsche Content-Entscheidungen der Netzwerke nicht wird ersetzen können. Bislang fehlt es an wirksamen und schnellen Rechtsbehelfen, die im Falle unberechtigter Löschungen oder Sperrungen den betroffenen Nutzer*innen zügig zu ihrem (vorläufigen) Recht verhelfen könnten. Weil die Hauptsacheentscheidung nicht vorweggenommen und keine Tatsachen geschaffen werden sollen, wird in der Regel im Eilverfahren die Anordnung einer Wiedereinstellung von Inhalten nicht erfolgen. Wenn aber nach einem mehrmonatigen Hauptsacheverfahren ein Gericht feststellt, dass ein Inhalt nicht hätte gelöscht werden dürfen, dann ist den betroffenen Nutzer*innen damit kaum mehr gedient und die Beeinträchtigung der Meinungsäußerungsfreiheit nur zum geringsten Teil behoben.

V. Videosharingplattformen - §§ 3c bis 3f NetzDG-E

Nach unserem Verständnis ist die Ausweitung auf sogenannte Videosharingplattformen weitestgehend der Umsetzung der europäischen AVMD-Richtlinie geschuldet. Diese Netzwerke fielen bereits zuvor unter das NetzDG. Die Unterbringung der Umsetzung im NetzDG überrascht und wirft einige Fragen auf. Offen bleibt bspw. Inwiefern die für Videosharing anwendbaren Vorschriften parallel zu denen des NetzDG auswirkt und was dies bspw. für große Netzwerke wie YouTube bedeutet.

1. Schaffung einer Doppelstruktur

Es ist auffällig, dass der Entwurf einerseits versucht die Umsetzung der AVMD-RL in das NetzDG zu integrieren und andererseits hierfür umfangreiche Sonderregelungen schafft. So

wird in § 3 e Abs. 2 und 3 NetzDG-E die Geltung des Herkunftslandsprinzips in Anwendung der europarechtlichen Vorgaben ausdrücklich angeordnet.

Bereits die Ausgestaltung der Regelung zur Festlegung des Sitzlandes zeigen, dass sich dies nur schwer in das Regelungskonstrukt des NetzDG einzufügen vermag. Streitigkeiten hierüber sind vorprogrammiert und schüren Zweifel an der Vereinbarkeit des NetzDG mit europarechtlichen Vorgaben insgesamt. Letztlich kann in Bezug auf Videosharingplattformen eine Steuerung nach nationaler Regelung nur noch aufgrund von Anordnungen des BfJ erfolgen. Unklar bleibt, ob bspw. YouTube nach diesen Vorgaben überhaupt noch oder nur noch teilweise, nämlich in den Kommentarspalten, den Vorgaben des NetzDG unterworfen werden kann. Zuzugeben ist der berechtigten Kritik, wonach die Aufsicht durch das BfJ möglicherweise nicht dem Erfordernis der Staatsferne, welches Art. 30 Abs. 1 der AVMD-RL normiert, genügt.

2. Beschränkung des Geltungsbereichs des NetzDG

Zum anderen bieten die jetzt neu eingefügten Regelungen für Videosharingplattformen erneut Anlass, über die Sinnhaftigkeit der Beschränkung des Anwendungsbereichs des NetzDG auf große Netzwerke mit zwei Millionen Nutzer*innen oder mehr, nachzudenken. Gemäß § 3 e Abs. 2 NetzDG-E erstreckt sich die Geltung des NetzDG teilweise auch auf Videosharinganbieter, die die Grenze von 2 Mio. Nutzer*innen unterschreiten. Hierdurch wird ein zweigleisiges Regelungssystem geschaffen, dessen Sinnhaftigkeit allein in der Umsetzung der Vorgaben der AVMD-RL zu suchen ist. Nach unserem Verständnis sind werden Abgrenzungsschwierigkeiten u.a. durch die Regelung des § 3 d Abs. Nr. 1. b) NetzDG-E können Netzwerke auch teilweise als soziales Netzwerk und teilweise als Videosharingplattform behandelt werden, hervorgerufen. Im Gesamtzusammenhang führt dies zu dem widersinnigen Ergebnis, dass für Netzwerke mit unter 2 Mio. Mitgliedern Videoinhalte unter das NetzDG fallen und die darunter befindlichen Kommentarspalten nicht reguliert sind - selbst, wenn Sie sich unmittelbar auf das Video beziehen und dessen Inhalt möglicherweise nur rezitieren. Diese Unterscheidung erscheint insbesondere angesichts der völlig gleichgelagerten Interessen widersinnig. Es besteht aus unserer Sicht auch unabhängig von der Behandlung von Videonetzwerken Anlass dazu die 2 Mio. Grenze zu überdenken.

Gerade kleine alternative Netzwerke aber auch Messenger- und Gaming-Apps sowie Imageboards sind in den letzten Jahren verstärkt zu Orten der Radikalisierung geworden. Es ist kein Zufall, dass die rechtsextremistischen Attentäter von Christchurch, El Paso oder Halle auf diesen Netzwerken und Apps nicht nur aktiv waren, sondern diese auch als Bühne für die Zurschaustellung und Weiterverbreitung ihrer Verbrechen nutzten.[6]

Aktuelle Studien zeigen, dass diese Netzwerke eine überproportional hohe Anzahl an rechtsextremistischen und vor allem auch antisemitischen Äußerungen enthalten[7], die die in § 1 Abs. 3 NetzDG genannten Straftatbestände verwirklichen. Hier werden gezielt

[6] Ebner, Guhl, Rau: Das Online Ökosystem rechtsextremer Akteure. Institute for Strategic Dialogue, London, 2019. S. 16.
[7] Ebenda. S.10.

Unterstützer*innen akquiriert, radikalisiert und mobilisiert.[8] Trotzdem fallen sie aufgrund ihrer Größe nicht unter die Regulierung durch das NetzDG.

Dies ist vor allem gravierend, insofern es bei den s.g. libertären Netzwerken wie 8chan, Minds, Gab oder Telegram keine Bemühungen gibt, den rechtswidrigen Content zu regulieren oder zu entfernen. Im Gegenteil: Hier werden extremistische Inhalte toleriert und nationale gesetzliche Regelungen rundheraus abgelehnt, wie im Fall von Telegram[9], das angibt, sich nicht an "lokale Beschränkungen der Meinungsfreiheit" halten zu wollen.[10] Am Beispiel von Telegram ist zu sehen, dass es sich hierbei längst nicht mehr um einen reinen Dienst zum Versenden privater Nachrichten handelt. Der größte Kanal hat insgesamt 40.000 Follower, der Kanal der Identitären Bewegung kommt auf insgesamt 35.000,00 Follower.[11]

Vor diesem Hintergrund sprechen wir uns dafür aus, den Anwendungsbereich des NetzDG auf solche Gamingplattformen und Messengerdienste auszudehnen, insofern diese über derartige Kanäle und Gruppen genutzt werden.

Aus aktuellen Studien wissen wir, dass gerade auf diesen Netzwerken eine zunehmende Radikalisierung und eine Akkumulation von extremistischen Gruppen stattfindet.[12] Insbesondere werden hier Kennzeichen verfassungsfeindlicher Organisationen und hetzerische Inhalte verbreitet. Derartige kleine Netzwerke sind Brutstätte und Sprungbrett zugleich für Hasskampagnen, die sodann auf den großen Netzwerken umgesetzt werden. Es ist nicht nachvollziehbar, warum nicht auch diese kleineren und themenspezifischen Netzwerke in die Pflicht genommen werden. Einer drohenden organisatorischen und wirtschaftlichen Überforderung kann durch eine Abstufung der Pflichten begegnet werden, wie es auch die §§ 3 c - f NetzDG-E vorsehen. Die §§ 3 c-f NetzDG-E sehen insbesondere gänzlich von einer Beschränkung für in Deutschland ansässige Netzwerke ab.

Nicht zu empfehlen wäre es allerdings, sich bei einer Ausweitung des Anwendungsbereichs explizit auf sogenannte Gaming-Netzwerke zu beschränken, wie dies immer wieder diskutiert wird und auch der aktuell in den Bundesrat eingebrachte Gesetzesantrag der Bundesländer Niedersachsen und Mecklenburg-Vorpommern vorsieht.

Es ist daher zu erwägen, den Anwendungsbereich des NetzDG auch auf diese Netzwerke zu erweitern.

VI. Bundesamt auch als Aufsichtsbehörde - § 4a NetzDG-E

Die Ausweitung der Aufgaben und Befugnisse der Verwaltungsbehörde i. S. d. § 4 NetzDG, also des Bundesamtes für Justiz, befürworten wir. Die Überwachungsmöglichkeit nebst

[8] Ebenda. S. 16.
[9] https://www.mdr.de/nachrichten/politik/inland/telegram-rechtsextreme-hetze-whatsapp-100.html (Stand: 16.06.2020)
[10] Ebenda. S. 21.
[11] Ebenda S. 16.
[12] Jakob Guhl, Julia Ebner und Jan Rau, Institute for Strategic Dialogue, Februar 2020: Das Online-Ökosystem Rechtsextremer Akteure (Zusammenfassung in deutscher Sprache)

Informations- und Anordnungsbefugnis verspricht die Aufdeckung und Behebung struktureller Defizite. Denn die Wahrscheinlichkeit der Entdeckung von Verstößen durch das Bundesamt in seiner aktuellen Funktion als Verfolgungsbehörde ist gering. Dies ermöglicht es den Netzwerken, mögliche Bußgelder als kalkuliertes Risiko im Rahmen einer Kosten-Nutzen-Abwägung in Kauf zu nehmen. Müssen sie jedoch eine systematische Überwachung und Kontrollen fürchten, wird dieses Risiko unübersichtlich. Gleichzeitig müssen sie befürchten, dass Beschwerden oder die Meldung von Verstößen Aufsichtsmaßnahmen zur Folge haben. Diese können strukturelle Defizite zu Tage fördern oder weitergehenden Erfüllungsaufwand produzieren. Unseres Wissens nach beklagen die Netzwerke derzeit selbst einen unzureichenden Informationsaustausch zwischen dem Bundesamt und ihnen. Sie wünschen sich ferner konkrete Hinweise, wie die Regelungen des NetzDG aus Sicht des Bundesamtes auszufüllen sind. Dem kommt die geplante Regelung in § 4a NetzDG-E entgegen.

Bewährt hat sich ein vergleichbarer Ansatz bei der Überwachung datenschutzrechtlicher Vorgaben. Auch wenn sich die Datenschutzbeauftragten in den meisten Bundesländern wohl keiner allzu großen Beliebtheit erfreuen, ist ihr Vorgehen effizient. Spätestens seit nach Inkrafttreten der DSGVO einige empfindliche Bußgelder (z.B. gegen “Deutsche Wohnen” oder “1&1”) verhängt wurden, werden die Datenschutzbeauftragten in ihrer Funktion ernst genommen. Die Maßnahmen der Aufsichtsbehörde haben hier jedenfalls unzweifelhaft eine Disziplinierung zur Folge, die über die Sanktionierung einzelner Verstöße hinaus Wirkung entfaltet.

Insoweit hieraus teilweise Überschneidungen mit Zuständigkeitsbereichen der Landesmedienanstalten resultieren, sind diese nach unserem Dafürhalten hinzunehmen. Auch wenn hier teilweise gleiche Prüfungsmaßstäbe anzulegen sind, dient der hier maßgebliche JMStV einem gänzlich anderen Schutzbereich und anderen Aufsichtsbefugnissen. Den Landesmedienanstalten kommt als staatsferne Aufsicht dennoch eine wichtige Aufgabe vor allem im Bereich des Jugendschutzes zu. Wünschenswert wäre es dennoch, einen Austausch dieser Stellen zu ermöglichen, um eine Doppelbefassung zu koordinieren und Abstimmung zu ermöglichen.

VII. Zustellungsbevollmächtigte*r - § 5 NetzDG

Der Entwurf erkennt an, dass der Zuständigkeitsbereich de*r Zustellungsbevollmächtigten uneinheitlich und vor allem von den Netzwerken sehr restriktiv ausgelegt wird. Die Erstreckung auf Wiederherstellungsklagen erscheint daher sachgerecht. Darüber hinaus halten wir jedoch auch eine Erstreckung auf sämtliche Belange in Bezug auf rechtswidrige Inhalte für erforderlich. In diesem Sinne empfiehlt sich eine Klarstellung, dass die Pflicht zur Benennung eine*r inländischen Zustellungsbevollmächtigten auch für die außergerichtliche Durchsetzung von Ansprüchen, bspw. die Durchsetzung gerichtlich festgestellter Auskunftspflichten gem. TMG, und nicht nur für das Vollstreckungsverfahren gilt. Auch Strafverfolgungsbehörden werden für Anfragen regelmäßig an Ansprechpartner*innen aus Irland und den USA verwiesen. Dem liegt die Auffassung zugrunde, dass sich § 5 NetzDG nur auf Anfragen nach dem NetzDG beschränken könne. Auch dies gehört wohl zu den bereits erwähnten Spitzfindigkeiten, derer sich die Netzwerke bedienen.

Wir fragen uns an dieser Stelle, warum man statt einer Ausweitung der Pflichten de*r Zustellungsbevollmächtigten nicht den weitaus effektiveren Schritt zur Einführung des Markortprinzips für Telemediendienste gegangen ist. Ein solches Marktortprinzip ist bereits in der DSGVO (Art. 3 II DSGVO i. V. m. Erwägungsgrund 23 der DSGVO) vorgesehen und hat sich - trotz eines kurzzeitigen medialen Aufschreis überforderter Unternehmen - doch bewährt.

Die Erwägungsgründe hierfür sind der aktuellen Situation in den sozialen Netzwerken nicht unähnlich. Im Datenschutzrecht geht es in erster Linie darum, Verbraucher*innen vor dem Missbrauch ihrer Daten im Internet vor allem für Werbezwecke zu schützen. Auch in sozialen Netzwerken haben wir es mit einer neuartigen und schwer abzugrenzenden Bedrohungslage für Nutzer*innen zu tun.

Bisher ist es nicht gelungen, die international tätigen Konzerne im Inland zuverlässig greifbar zu machen, da sich diese darauf verstehen, das NetzDG zu umgehen. So ist bspw. eine Kontaktaufnahme zu Facebook für alle Anliegen, die nach der Einschätzung des Betreibers nicht unmittelbar das NetzDG betreffen, ausschließlich über streng vordefinierte Kontaktformulare oder per Post möglich. Es ist nicht möglich, allgemeine Anfragen per E-Mail oder Fax an den Konzern zu richten. Auch die Postadresse ist nur über verschlungene Pfade in einem gut versteckten Impressum zu ermitteln. Sollen Daten beauskunftet werden, wird selbst gegenüber Strafverfolgungsbehörden wechselseitig auf die USA oder Irland verwiesen. Es ist absehbar, dass bei Einführung einer Auskunftspflicht in § 14 Abs. 3 TMG ein Gerichtsbeschluss aus Deutschland von den Netzwerken als nicht geeignet angesehen wird, um Daten von Servern, die in einem anderen Mitgliedstaat oder gar in Übersee stehen, heraus zu verlangen.

VIII. Ergänzende Anmerkungen und Empfehlungen

1. Rechtsgrundlage für Accountsperrungen schaffen

Ein weiteres Problem besteht darin, dass vielfach auch aus dem Ausland mit strafbaren Hasspostings Einfluss auf die Debatte in den Sozialen Medien genommen wird. Dem ist mit keiner der bestehenden oder angedachten Regelungen beizukommen. Bezüglich solcher ausländischen Accounts sollte die Möglichkeit geschaffen werden, sie jedenfalls im Bundesgebiet dauerhaft zu sperren, wenn sie – und sei es wiederholt - Inhalte posten, die nach deutschem Recht strafbar sind. Darüber hinaus deuten aktuelle Studien darauf hin, dass die Sperrung rechtsextremistischer Accounts offenbar tatsächlich geeignet ist, deren Reichweite zu verringern und nicht unmittelbar zur Abwanderung der Mitglieder zu "alternativen" Netzwerken führt.[13]

[13] Ebner, Guhl, Rau: Das Online Ökosystem rechtsextremer Akteure. Institute for Strategic Dialogue, London, 2019. S. 11.

2. Schulung von und Unterstützung für Content-Manager*innen - § 3 Abs. 4 S. 2 NetzDG

Die Mitarbeiter*innen der Löschzentren, die täglich im Massenverfahren gemeldete rechtswidrige Inhalte sichten und bewerten müssen, tragen eine große Last. Sie müssen nach einer Schulung von lediglich wenigen Wochen eine hochkomplexe Aufgabe bewältigen. Die strafrechtliche Würdigung von Äußerungen ist überdurchschnittlich anspruchsvoll. So stellt die Frage, ob eine Äußerung z.B. den Tatbestand der Volksverhetzung erfüllt oder eine strafbare Beleidigung darstellt, selbst erfahrene Strafverfolger*innen regelmäßig vor eine große Herausforderung. Hinzu kommt, dass die Content-Manager*innen einer derartigen Fülle von digitaler Gewalt ausgesetzt sind, dass dies massiven psychischen Stress verursacht. Die Anforderungen, die das NetzDG an die Schulungs- und Betreuungsangebote stellt, erscheinen in Anbetracht dessen nicht ausreichend. Es sollten stets in ausreichender Zahl Ansprechpartner*innen mit mindestens dem 1. juristischen Staatsexamen zumindest für Rückfragen und Beratung zur Verfügung stehen. Psychologische Beratung und Supervision muss im Zweifel ebenfalls ständig sofort oder jedenfalls kurzfristig zur Verfügung stehen. Dies gilt umso mehr, wenn sämtliche Gesetzesänderungen tatsächlich wie derzeit vom Ministerium geplant umgesetzt werden und in der Folge die Anforderungen an die Content-Manager*innen noch beträchtlich steigen.

HateAid gGmbH

Die gemeinnützige Organisation HateAid gGmbH unterstützt Betroffene von digitaler Gewalt. Durch Hassattacken werden Menschen gezielt aus den Debatten im Netz herausgedrängt, aber selten werden Täter*innen zur Verantwortung gezogen. Hier setzt HateAid an und bestärkt Betroffene durch stabilisierende Erst-, Sicherheits-, und Kommunikationsberatung und rechtliche Durchsetzung. Als Prozesskostenfinanzierer unterstützt HateAid Betroffene gegen Täter*innen (zivil-)rechtlich vorzugehen. Im Rahmen des Bündnisses “Keine Macht dem Hass” kooperiert HateAid mit der Schwerpunktstaatsanwaltschaft ZIT in Hessen.