DeutscherAnwaltVerein

Stellungnahme

des Deutschen Anwaltvereins durch die Ausschüsse Gefahrenabwehrrecht und Informationsrecht

zum Vorschlag für eine Verordnung des Europäischen Parlamentes und des Rates zur Verhinderung der Verbreitung terroristischer Online-Inhalte

Stellungnahme Nr.: 4/2019 **Berlin/Brüssel, im Januar 2019**

Mitglieder des Ausschusses Gefahrenabwehrrecht

- Rechtsanwältin Lea Voigt, Bremen (Vorsitzende)
- Rechtsanwalt Wilhelm Achelpöhler, Münster (Berichterstatter)
- Rechtsanwalt Dr. Nikolas Gazeas, LL.M., Köln
- Rechtsanwalt Dr. Stefan König, Berlin
- Rechtsanwältin Dr. Regina Michalke, Frankfurt / Main
- Rechtsanwältin Kerstin Oetjen, Freiburg

Ständige Gäste im Ausschuss Gefahrenabwehrrecht

- Professor Dr. Annika Dießner, Berlin
- Professor Dr. Mark A. Zöller, Trier (Berichterstatter)

Zuständig in der DAV-Geschäftsführung

- Rechtsanwalt Max Gröning

Mitglieder des Ausschusses Informationsrecht

- Rechtsanwalt Dr. Helmut Redeker, Bonn (Vorsitzender)
- Rechtsanwalt Dr. Simon Assion, Frankfurt am Main
- Rechtsanwältin Dr. Christiane Bierekoven, Köln
- Rechtsanwältin Isabell Conrad, München
- Rechtsanwalt Dr. Malte Grützmacher, LL.M., Hamburg
- Rechtsanwalt Prof. Niko Härting, Berlin (Berichterstatter)
- Rechtsanwalt Peter Huppertz, LL.M, Düsseldorf
- Rechtsanwältin Birgit Roth-Neuschild, Karlsruhe
- Rechtsanwalt Dr. Robert Selk, LL.M. (EU), München
- Rechtsanwalt Prof. Dr. Holger Zuck, Stuttgart

Zuständig in der DAV-Geschäftsführung

- Rechtsanwältin Nicole Narewski

Ansprechpartner in Brüssel:

- Rechtsanwältin Eva Schriever, LL.M.

Deutscher Anwaltverein
Littenstraße 11, 10179 Berlin
Tel.: +49 30 726152-0
Fax: +49 30 726152-190
E-Mail: dav@anwaltverein.de

Büro Brüssel
Rue Joseph II 40
1000 Brüssel, Belgien
Tel.: +32 2 28028-12
Fax: +32 2 28028-13
E-Mail: bruessel@eu.anwaltverein.de
Transparenz-Registernummer:
87980341522-66

www.anwaltverein.de

Verteiler

Verteiler Deutschland

Bundesministerium der Justiz und für Verbraucherschutz
Bundesministerium für Wirtschaft und Energie
Bundesministerium des Innern, für Bau und Heimat

Deutscher Bundestag – Ausschuss für Recht und Verbraucherschutz
Deutscher Bundestag – Innenausschuss
Deutscher Bundestag – Ausschuss für Wirtschaft und Energie
Deutscher Bundestag – Ausschuss Digital Agenda

Arbeitsgruppen Inneres der im Deutschen Bundestag vertretenen Parteien
Arbeitsgruppen Recht der im Deutschen Bundestag vertretenen Parteien

Justizministerien und -senatsverwaltungen der Länder
Landesministerien und Senatsverwaltungen des Innern
Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Landesdatenschutzbeauftragte
Innenausschüsse der Landtage
Rechtsausschüsse der Landtage

Europäische Kommission - Vertretung in Deutschland
Bundesrechtsanwaltskammer
Bundesnotarkammer
Deutscher Notarverein
Deutscher Richterbund
Bund deutscher Verwaltungsrichter
Bundesverband der Freien Berufe
Bundesverband der Deutschen Industrie
Gewerkschaft der Polizei (Bundesvorstand)
Deutsche Polizeigewerkschaft im DBB
Deutscher Steuerberaterverband
Verd.di, Recht und Politik
stiftung neue verantwortung e.V.
Institut für Deutsches und Europäisches Strafprozessrecht und Polizeirecht (ISP) der Universität Trier
GRUR
BITKOM
DGRI
EDV-Gerichtstag
Gemeinsame Kommission elektronischer Rechtsverkehr des Deutschen EDV-Gerichstages
Europäische Kommission – Vertretung in Deutschland

Vorstand und Landesverbände des DAV
Vorsitzende der Gesetzgebungs- und Geschäftsführenden Ausschüsse des DAV
Vorsitzende des FORUM Junge Anwaltschaft des DAV

Frankfurter Allgemeine Zeitung
Süddeutsche Zeitung
Berliner Zeitung
Berliner Verlag GmbH
Juris Newsletter
JurPC
NJW
Juve Verlag
Redaktion MultiMedia und Recht (MMR)
Chefredakteurin MMR/ZD
Redaktion Zeitschrift für Datenschutz ZD
Redaktion Heise Online
Redaktion Der Spiegel
Redaktion FAZ
Redaktion Anwaltsblatt
LTO

Verteiler Europa

Europäische Kommission
- Generaldirektion Justiz
- Generaldirektion Kommunikationsnetze, Inhalte und Technologien
- Generaldirektion Migration und Inneres

Europäisches Parlament
- Ausschuss für Bürgerliche Freiheiten, Justiz und Inneres
- Ausschuss für Binnenmarkt und Verbraucherschutz
- Ausschuss für Kultur und Bildung

Rat der Europäischen Union
Ständige Vertretung der Bundesrepublik Deutschland bei der EU
Justizreferenten der Landesvertretungen

Rat der Europäischen Anwaltschaften (CCBE)
Vertreter der Freien Berufe in Brüssel
DIHK Brüssel
BDI Brüssel

Der Deutsche Anwaltverein (DAV) ist der freiwillige Zusammenschluss der deutschen Rechtsanwältinnen und Rechtsanwälte. Der DAV mit derzeit über 63.000 Mitgliedern vertritt die Interessen der deutschen Anwaltschaft auf nationaler, europäischer und internationaler Ebene.

Stellungnahme des Deutschen Anwaltsvereins zum Vorschlag für eine Verordnung des Europäischen Parlamentes und des Rates zur Verhinderung der Verbreitung terroristischer Online-Inhalte

Zusammenfassung

Der Vorschlag für eine Verordnung zur Verhinderung der Verbreitung terroristischer Online-Inhalte beinhaltet Löschungs- und Unterrichtungspflichten für Hostingdiensteanbieter in Bezug auf durch Dritte hochgeladene terroristische Inhalte (Art. 4, 5). Die gelöschten Daten müssen zur Erleichterung der Strafverfolgung von den Hostingdiensteanbietern für einen Zeitraum von mindestens sechs Monaten gespeichert werden (Art. 7). Kommen die Hostingdiensteanbieter ihren Pflichten nicht nach, so sollen die Mitgliedstaaten ihnen entsprechende Sanktionen auferlegen (Art. 18). Aus Sicht des DAV bestehen bereits erhebliche Zweifel an einer ausreichenden Kompetenzgrundlage für den Erlass eines derartigen Rechtsaktes in Gestalt einer Verordnung. Hostingdiensteanbieter werden damit verpflichtet, in ihre Nutzungsbedingungen entsprechende Bestimmungen aufzunehmen und die Verbreitung dieser Inhalte zu verhindern. Unklarheiten in den Begrifflichkeiten können Hostingdiensteanbieter dazu veranlassen, Informationen „im Zweifel“ aus dem Internet zu entfernen. Darin liegt nicht nur das Fehlen einer verbindlichen Handlungsanweisung für die Praxis, sondern auch eine erhebliche Gefahr für die Meinungsfreiheit.

Summary

The proposal for a regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online includes removal and notification obligations for hosting service providers regarding terrorist content uploaded by third parties (Art. 4, 5). Hosting service providers are required to preserve removed content for six months for investigative purposes (Art. 7). If the hosting service providers do not follow their obligations, Member States shall lay down appropriate penalties (Art. 18). The DAV has considerable doubts as to whether the EU has sufficient competence to

adopt such a legal instrument. Hosting service providers would be obliged to include certain provisions in their terms and conditions and to prevent the dissemination of terrorist content. Due to ambiguity in the chosen terminology, hosting service providers may feel compelled to remove information from the internet “in case of doubt”. This not only leads to a lack of binding instructions for action in practice, but also constitutes a serious threat to freedom of expression.

I. Allgemeines

Hostingdiensteanbieter nutzen auf freiwilliger Basis bereits heute in erheblichem Umfang automatisierte Filterverfahren um zu verhindern, dass bestimmte Inhalte auf ihren Plattformen verbreitet werden.

Der am 12.09.2018 von der Europäischen Kommission vorgelegte Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Verhinderung der Verbreitung terroristischer Online-Inhalte[1] beinhaltet Löschungspflichten für Hostingdiensteanbieter in Bezug auf durch Dritte hochgeladene terroristische Inhalte (Art. 4, 5). Die gelöschten Daten müssen zur Erleichterung der Strafverfolgung von den Hostingdiensteanbietern für einen Zeitraum von mindestens sechs Monaten gespeichert werden (Art. 7)[2]. Werden Inhalte online gestellt, die eine Gefahr für Leben oder Sicherheit darstellen, müssen die Strafverfolgungsbehörden unterrichtet werden. Kommen die Hostingdiensteanbieter ihren Pflichten nicht nach, so sollen die Mitgliedstaaten ihnen entsprechende Sanktionen auferlegen (Art. 18). Diese seien erforderlich, damit gewährleistet werde, dass die Hostingdiensteanbieter die ihnen auferlegten Pflichten wirksam umsetzen[3].

Diese von der Kommission vorgeschlagene Verordnung zielt darauf ab, dass Hostingdiensteanbieter ihre Maßnahmen zur Verhinderung der Verbreitung bestimmter Inhalte intensivieren. Sie werden verpflichtet, in ihre Nutzungsbedingungen entsprechende Bestimmungen aufzunehmen und die Verbreitung dieser Inhalte zu verhindern. Da die Hostingdiensteanbieter zum Einsatz von Filterwerkzeugen nicht

[1] COM(2018) 640 final.
[2] COM(2018) 640 final, S. 10, 22.
[3] COM(2018) 640 final, S. 10, 22.

gezwungen werden können[4], sollen verschiedene Maßnahmen sie dazu anhalten, „freiwillig“ mit proaktiven Maßnahmen gegen die Verbreitung von unerwünschten Inhalten vorzugehen.

Damit wird die Verhinderung der Verbreitung unerwünschter Inhalte in die Hände und die Verantwortung privater Unternehmen gelegt. Diese Unternehmen sind selbst nicht an die Grundrechte der EU GRCh gebunden, da nach Art. 51 EU-GRCh die Grundrechte nur die Organe der EU verpflichten. Damit kann die Indienstnahme privater Unternehmen die Meinungsfreiheit im Internet gefährden. Zudem können gerade kleinere Unternehmen durch die von ihnen erwarteten Maßnahmen überfordert werden.

II. Fehlende Gesetzgebungskompetenz

Aus Sicht des DAV bestehen bereits erhebliche Zweifel an einer ausreichenden Kompetenzgrundlage für den Erlass eines derartigen Rechtsaktes in Gestalt einer Verordnung.

Rechtsgrundgrundlage für die Verordnung soll nach dem eindeutigen Wortlaut des Entwurfstextes Art. 114 AEUV sein.[5] Gemäß Art. 114 Abs. 1 S. 2 AEUV können Maßnahmen zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten zur Errichtung und Förderung des Binnenmarktes erlassen werden. Die Art der Maßnahme wird durch den Wortlaut der Vorschrift nicht näher bestimmt. „Maßnahmen“ nach Art. 114 Abs. 1 S. 2 AEUV können somit nach vorherrschender Ansicht im Schrifttum im Gegensatz zu solchen nach Art. 115 AEUV sämtliche Rechtsinstrumente i. S. des Art. 288 AEUV sein, sodass auf der Grundlage von Art. 114 AEUV auch der Erlass von Verordnungen in Betracht kommt.[6] Allerdings muss der Rückgriff auf das einschneidende, weil unmittelbar geltende Sekundärrechtsinstrument einer EU-Verordnung im Einzelfall stets besonders begründet werden.[7] Inhaltlich muss sich eine auf Art. 114 AEUV gestützte Verordnung dabei an den spezifischen

[4] EuGH, Urteil v. 16.02.2012, Az. C‑360/10 (SABAM) /Netlog NV
[5] COM(2018) 640 final, S. 5.
[6] *Terhechte*, in: Frankfurter Kommentar EUV, GRC, AEUV, Art. 114 AEUV, Rn. 64; *Korte*, in: Callies/Ruffert EUV AEUV, Art. 114 AEUV, Rn. 65.
[7] *Terhechte*, in: Frankfurter Kommentar EUV, GRC, AEUV, Art. 114 AEUV, Rn. 66.

Erfordernissen des Binnenmarktes orientieren.[8] Gemäß Art. 26 Abs. 2 AEUV umfasst der Binnenmarkt einen Raum ohne Binnengrenzen, in dem der freie Verkehr von Waren, Personen, Dienstleistungen und Kapital gemäß den Bestimmungen der Europäischen Verträge gewährleistet wird. Infolgedessen muss es sich auch bei einem Rückgriff auf die Kompetenznorm des Art. 114 AEUV im Schwerpunkt um Maßnahmen handeln, mit deren Hilfe Hindernisse zur Verwirklichung der Grundfreiheiten oder Wettbewerbsverfälschungen beseitigt werden. Die Verwirklichung des Binnenmarktes auf diese Art und Weise bedarf zudem der Berücksichtigung der Kompetenzzuweisung der Verträge sowie der Beachtung des Prinzips der begrenzten Einzelermächtigung nach Art. 5 Abs. 2 EUV.[9]

Begründet wird die Heranziehung des Art. 114 AEUV als Kompetenzgrundlage von den Entwurfsverfassern damit, dass mit Hilfe der Verordnung das reibungslose Funktionieren des digitalen Binnenmarktes gewährleistet werden soll.[10] Konkret sollen die Bereitstellung von Online-Diensten erleichtert, gleiche Wettbewerbsbedingungen für die Hostingdiensteanbieter geschaffen und zudem ein Rechtsrahmen für die Erkennung und Entfernung terroristischer Inhalte geboten werden.[11] Im Hinblick auf die für die Hostingdiensteanbieter angedachten Speicherungspflichten und die geplanten Sanktionierungspflicht der Mitgliedstaaten bleibt diese Begründung jedoch aus Sicht des DAV unzureichend. Vielmehr zeigt eine Gesamtbetrachtung des Verordnungsentwurfs, dass der Schwerpunkt der Maßnahme hier jedenfalls nicht eindeutig im Bereich des Binnenmarktes, sondern primär in einer Stärkung der Abwehr von durch terroristische Internetinhalte drohenden Gefahren sowie der Verfolgung damit einhergehender Straftaten liegt. Dieser Schluss wird durch eine ganze Reihe von Erwägungsgründen nahegelegt, von denen hier lediglich drei Beispiele herausgegriffen werden können:

So heißt es in Erwägungsgrund (2): *„Besonders besorgniserregend ist der Missbrauch von Hostingdiensten durch terroristische Vereinigungen und ihre Unterstützer mit dem Ziel terroristische Online-Inhalte zu verbreiten und so ihre Botschaften weiterzutragen,*

[8] *Terhechte*, in: Frankfurter Kommentar EUV, GRC, AEUV, Art. 114 AEUV, Rn. 6.
[9] *Terhechte,* in Frankfurter Kommentar EUV, GRC, AEUV, Art. 26 AEUV, Rn. 6.
[10] COM(2018) 640 final, S. 15, 26.
[11] COM(2018) 640 final, S. 3.

Menschen zu radikalisieren und anzuwerben sowie terroristische Aktivitäten zu erleichtern und zu lenken."

In Erwägungsgrund (4) heißt es: *„Die 2015 begonnenen Bemühungen der Union zur Bekämpfung terroristischer Inhalte durch einen Rahmen für die freiwillige Zusammenarbeit zwischen den Mitgliedstaaten und den Hostingdienstanbietern müssen durch einen klaren Rechtsrahmen ergänzt werden, um den Zugang zu terroristischen Online-Inhalten weiter zu verringern und dem sich rasch verändernden Problem gerecht zu werden."*

Und Erwägungsgrund (7) formuliert: *„Diese Verordnung trägt zum Schutz der öffentlichen Sicherheit bei und enthält gleichzeitig angemessene und solide Vorkehrungen zum Schutz der betreffenden Grundrechte."*

Zwar kann eine Sanktionierungspflicht der Mitgliedstaaten bei der Umsetzung von Richtlinien oder der Durchführung von Verordnungen generell auch dem Loyalitätsgebot aus Art. 4 Abs. 3 UA 2 EUV entnommen werden. Bei dem vorliegenden Verordnungsvorschlag werden allerdings konkrete Anweisungen an die Mitgliedstaaten vorgegeben, die über das bisher übliche Maß des Umgangs mit gelöschten terroristischen Inhalten von Hostingdiensteanbietern deutlich hinausgehen. Speziell die in Art. 7 vorgesehene Speicherungspflicht für gelöschten Daten lässt sich letztlich nur mit Blick auf Ermittlungsinteressen der Strafverfolgungsbehörden im Terrorismusbereich überzeugend begründen.[12] Im Bereich des Strafrechts und der Bekämpfung des internationalen Terrorismus besitzt die EU aber grundsätzlich keine supranationale Gesetzgebungskompetenz, weil die Mitgliedstaaten diesen Bereich als besondere Ausprägung ihrer Souveränität nur ansatzweise vergemeinschaften haben.[13] Art. 75 AEUV ermöglicht zu präventiven Terrorismusbekämpfung lediglich die Schaffung eines Rahmens für Verwaltungsmaßnahmen in Bezug auf Kapitalbewegungen und Zahlungen durch Verordnungen. Und Art. 83 AEUV erlaubt lediglich Harmonisierungsmaßnahmen durch EU-Richtlinien, nicht aber durch Verordnungen. Diese klare Wertentscheidung des EU-Primärrechts würde umgangen, wenn man im Rahmen von Art. 114 AEUV unter formaler Berufung auf den

[12] Vgl. auch *Zöller* GA 2007, 393 (407) zur Richtlinie 2006/24/EG.
[13] Näher hierzu *Zöller*, FS Schrenke, 2011, S. 579 ff.

Binnenmarkt in weitreichendem Maße auch Verordnungen zur Gefahrenabwehr oder Strafverfolgung zuließe. Dies entspricht auch der Argumentation des EuGH in seiner Entscheidung zur Übermittlung von Fluggastdaten. Hier lehnte der EuGH die binnenmarktbezogene Kompetenz aus Art. 95 EGV (Art. 114 AEUV n.F.) zu Recht ab, da der primäre Zweck der Maßnahme in der Gewährleistung der öffentlichen Sicherheit und strafrechtlichen Tätigkeit der Mitgliedstaaten zu sehen sei.[14] Im Unterschied dazu wurde die kompetenzrechtliche Zuweisung der Richtlinie zur Vorratsdatenspeicherung auf Art. 95 EGV (Art. 114 AEUV n.F.) nur deshalb bejaht, da sie lediglich die Tätigkeiten der Diensteanbieter im Binnenmarkt betraf und keine Regelungen der Handlungen staatlicher Stellen zu Strafverfolgungszwecken enthielt.[15] Generell vertritt der EuGH die Leitlinie, dass das bloße Tangieren des Binnenmarktes den Rückgriff auf Art. 114 AEUV n.F. nicht rechtfertige.[16] Schließlich kann die Verwirklichung des Binnenmarktes gerade bei extensiver Handhabung mit grundlegenden Verfassungsprinzipien des Unionsrechts konfligieren.[17]

Nicht entscheidend ist bei alledem die Frage der Notwendigkeit einer effektiven Terrorismusbekämpfung und die entsprechende Geeignetheit einer Verordnung zur Erreichung dieses Zwecks. Dies entspricht bereits der Argumentation des EuGH hinsichtlich der Ungültigkeit der Richtlinie zur Vorratsdatenspeicherung, wonach die Bekämpfung schwerer Kriminalität, insbesondere der organisierten Kriminalität und des Terrorismus, zwar von größter Bedeutung für die Gewährleistung der öffentlichen Sicherheit ist und ihre Wirksamkeit in hohem Maß von der Nutzung moderner Ermittlungstechniken abhängen kann.[18] Die wichtige gesamtgesellschaftliche Aufgabe der Terrorismusbekämpfung kann aber nicht zur Heilung des hier bestehenden, kompetenzrechtlichen Mangels führen.

III. Unklare Definition „terroristischer Inhalte“

Ziel der Verordnung ist die Verhinderung der Verbreitung „terroristischer Inhalte“ im Internet. Die Werbung für terroristische Vereinigungen oder auch Hasspredigen sind

[14] EuGH, Urteil vom 30.5.2006 – C-317/04 u. C-318/04, Rn. 54-56, Rn. 67.
[15] EuGH, Urteil vom 10.2.2009 – C-301 06, Rn. 91.
[16] Vgl. *Zöller* GA 2007, 393 (409); *Terhechte* EuZW 2009, 199 (203).
[17] *Terhechte* EuZW 2009, 199 (202).
[18] EuGH, Urteil vom 08.04.2014 – C-293/12, Rn. 51.

nach der Rechtsprechung des EGMR zur EMRK nicht vom Schutzbereich der Meinungs- und Informationsfreiheit nach Art 10 EMRK umfasst[19]. An dieser Rechtsprechung orientiert sich auch die Auslegung von Art. 11 EU GRCh. Die Entfernung terroristischer Inhalte beeinträchtigt damit die Meinungs- und Informationsfreiheit nicht. Eine Beeinträchtigung der Meinungsfreiheit liegt indessen vor, wenn Inhalte zu Unrecht als „terroristische Inhalte“ angesehen und aus dem Internet entfernt werden. Der Schutz der Meinungsfreiheit gebietet daher eine genaue Bestimmung des Begriffs der „terroristischen Inhalte“.

Nach Art. 2 Nr. 5 sind „terroristischen Inhalte“ Informationen, die einen Aufruf zu oder die Befürwortung von terroristischen Straftaten darstellen, die Ermutigung, an terroristischen Straftaten mitzuwirken, sowie die Förderung der Aktivitäten einer terroristischen Vereinigung, insbesondere durch Ermutigung zur Beteiligung an oder Unterstützung einer terroristischen Vereinigung im Sinne des Artikels 2 Absatz 3 der Richtlinie (EU) 2017/541. Schließlich gehören auch technische Anleitungen oder Methoden für das Begehen terroristischer Straftaten zu den terroristischen Inhalten.

Damit knüpft der Begriff des „terroristischen Inhalts“ an den ohnehin wenig trennscharfen Begriff der „terroristischen Straftat“ in Art. 3 Abs. 1 der Richtlinie 2017/541 an und erfasst auch Handlungen, die selbst keine terroristische Straftat sind. Bereits die Weitergabe von Informationen, die als „Ermutigung“ derartige Straftaten zu begehen aufgefasst werden können, werden danach zu den „terroristischen Inhalten“ gerechnet. Auch ist sehr zweifelhaft, wann die Weitergabe von Informationen im Internet als „Förderung der Aktivitäten einer terroristischen Vereinigung“ anzusehen ist. Das Erfordernis einer mit der Verbreitung der Informationen „einhergehenden Gefahr, dass solche Taten begangen werden könnten“, stellt keine wirkliche tatbestandliche Eingrenzung dar. Denn eine solche Gefahr kann bei der Verbreitung von Informationen immer nur eine abstrakte Gefahr sein. Gerade die journalistische Berichterstattung über die Aktivitäten von als terroristisch angesehenen Organisationen kann durch diese weite Definition beschränkt werden.

[19] EGMR Entscheidung vom 27.06.2017, Az.: 34367/14

Immerhin besteht auch innerhalb der Mitgliedstaaten der EU keine Einigkeit darüber, welche Organisationen als „terroristisch“ anzusehen sind. Und auch auf völkerrechtlicher Ebene hat sich die internationale Staatengemeinschaft bislang nicht zu einer allseits anerkannten Definition des Terrorismusbegriffs durchringen können. Noch immer gilt angesichts der Tatsache, dass der Begriff „Terrorismus“ politisch massiv aufgeladen ist, der wenig tröstliche Allgemeinplatz „One man´s terrorist is another man´s freedom fighter.“[20]

Diese Unklarheiten in der Begrifflichkeit können Hostingdiensteanbieter veranlassen, Informationen „im Zweifel“ aus dem Internet zu entfernen. Darin liegt nicht nur das Fehlen einer verbindlichen Handlungsanweisung für die Praxis, sondern auch eine erhebliche Gefahr für die Meinungsfreiheit.

IV. Die Maßnahmen in Einzelnen

1. Entfernungsanordnung nach Art. 4

Die Entfernungsanordnung in Art. 4 der Verordnung ermächtigt die zuständigen Behörden, die Hostingdiensteanbieter zu verpflichten, bestimmte, als „terroristische Inhalte“ benannte Informationen zu entfernen oder zu sperren. Der jeweilige Hostingdienst hat den betreffenden Inhalt gemäß Art. 4 Abs. 2 der Verordnung innerhalb einer Stunde nach Erhalt der Anordnung zu entfernen. Zu diesem Zwecke haben die Hostingdiensteanbieter gemäß Art. 14 Abs. 1 der Verordnung eine sog. Kontaktstelle einzurichten, welche die zügige Bearbeitung von Entfernungsanordnungen ermöglicht.

Mit einer Entfernungsanordnung wird ein Hostingdiensteanbieter einem umfangreichen Überwachungsregime unterworfen: er hat innerhalb von drei Monaten nach Eingang der Aufforderung und danach mindestens einmal jährlich einen Bericht über die von ihm ergriffenen spezifischen „proaktiven Maßnahmen“, einschließlich der Verwendung automatisierter Werkzeuge, vorzulegen, um ein erneutes Hochladen von Inhalten, die zuvor entfernt oder gesperrt wurden, zu verhindern, sowie terroristische Inhalte zu

[20] *Zöller*, Terrorismusstrafrecht – Ein Handbuch, 2009, S. 154 ff. m.w.N.

erkennen, zu ermitteln und unverzüglich zu entfernen oder zu sperren, Art. 6 Nr. 2 VO. Hält die zuständige Behörde die gemeldeten proaktiven Maßnahmen nicht für ausreichend, kann sie den Hostingdiensteanbieter auffordern und letztlich auch verpflichten, zusätzliche Maßnahmen zu ergreifen, Art. 6 Nr. 3 VO. Bei einem systematischen Verstoß gegen die Verpflichtungen aus Artikel 4 Absatz 2 können finanzielle Sanktionen in Höhe von bis zu 4 % des weltweiten Jahresumsatzes des Hostingdiensteanbieters im vorangegangenen Geschäftsjahr verhängt werden. Dies führt entgegen der klaren Wertentscheidung (nicht nur) des deutschen Strafrechtssystems gegen eine Verbandsstrafe zu einer erheblichen Ausweitung des Arsenals an Sanktionsmöglichkeiten gegenüber Unternehmen.

Dieses Sanktionsregime soll Hostingdiensteanbieter dazu verlassen, von vornherein durch verstärkte freiwillige Maßnahmen zu vermeiden, dass es überhaupt zu Entfernungsanordnungen kommt.

Eine Entfernungsanordnung beeinträchtigt das Recht auf unternehmerische Freiheit nach Art. 16 EU-GRCh. Die Entfernungsanordnung sieht vor, dass der Hostingdiensteanbieter eine Kontaktstelle einzurichten hat, die personell so ausgestattet ist, dass eine Entfernung innerhalb einer Stunde umgesetzt werden kann. Hierin liegt daher ein Eingriff in die freie Disposition über die Ressourcen des Anbieters. In der Verordnung findet mehrfach Erwähnung, dass die einzelnen Maßnahmen je nach wirtschaftlicher Größe oder tatsächlicher Nutzerzahl auf jeden Hostingdiensteanbieter individuell zuzuschneiden ist. Bei Art. 4 der geplanten Verordnung fehlt ein solcher Hinweis jedoch. Unabhängig von den tatsächlichen Möglichkeiten des jeweiligen Diensteanbieters hat dieser daher innerhalb einer sehr kurzen Zeitspanne zu reagieren. Diese sehr restriktiven Vorgaben dürften durch größere Diensteanbieter zu bewältigen sein, bei kleineren Anbietern, die nur geringe personelle Ressourcen haben, dürfte eine solche Struktur allerdings schwer umsetzbar sein und kann eine erdrosselnde Wirkung haben. Hier könnte in Einzelfällen daher der Wesensgehalt der unternehmerischen Freiheit beeinträchtigt und die geplante Verordnung somit teilweise grundrechtsverletzend sein.

Art. 47 EU-GRCh sieht vor, dass jede Person, deren Rechte verletzt wurden, das Recht hat, bei einem Gericht einen wirksamen Rechtsbehelf einzulegen. Zum effektiven

Rechtsschutz zählt insbesondere, dass die Rechtsordnung eines Mitgliedstaats die Möglichkeit vorsieht, vorläufige Maßnahmen zu treffen, wenn dies erforderlich ist, um die volle Wirksamkeit der späteren Gerichtsentscheidung über das Bestehen der betreffenden Rechte sicherzustellen[21]. Art. 4 Abs. 4 der geplanten Verordnung sieht vor, dass auf Antrag des Hostingdiensteanbieters oder des Inhalteanbieters die zuständige Behörde eine ausführliche Begründung vorzulegen hat. Ungeachtet dessen ist die Entfernung des Inhaltes vorzunehmen. Hier stünden daher dem Inhalteanbieter erst nach Information durch den Hostingdiensteanbieter (Art. 11 Abs. 1) – sofern er wegen Art. 11 Abs. 3 der Verordnung überhaupt informiert wird – mögliche Rechtsmittel zur Verfügung. Diese können im Rahmen des Eilrechtsschutzes auch geeignet sein, eine vorläufige Entscheidung über die Entfernung des Inhaltes zu treffen. Das Recht auf effektiven Rechtsschutz ist durch die Entfernungsanordnung daher nicht beeinträchtigt.

2. Meldung an den Hostingdiensteanbieter Art. 5

Nach Artikel 5 der Verordnung können die zuständigen Behörden eine Meldung – die ausreichend detaillierte Informationen darüber enthält, warum die Behörde den Inhalt als terroristisch einstuft – an den Hostingdiensteanbieter richten. Dieser hat den gemeldeten Inhalt auf die Vereinbarkeit mit seinen eigenen Nutzungsbedingungen zu prüfen und entscheidet, ob der Inhalt gesperrt oder entfernt wird. Über das Ergebnis der Prüfung und die ergriffenen Maßnahmen hat der Hostingdiensteanbieter die Behörde zu unterrichten.

Allein die Meldung eines terroristischen Online-Inhaltes an den Hostingdiensteanbieter und die Bitte, diesen Inhalt anhand der Nutzungsbedingungen zu prüfen, stellt zwar keinen unmittelbaren Eingriff in Grundrechte dar. Denn der Hostingdiensteanbieter wird allein durch die Meldung nicht zu einer Entfernung der Inhalte verpflichtet. Eine Gefährdung der Meinungsfreiheit ist gleichwohl zu befürchten. Die genaue Prüfung der Inhalte kostet den Hostingdiensteanbieter Zeit und Personalressourcen. Für den Fall des Nicht-Entfernens kann die Entfernung nach Art. 4 angeordnet werden. Nach einer solchen Anordnung kann der Hostingdiensteanbieter einer Berichtspflicht nach Art. 6 Abs. 2 der Verordnung unterworfen werden, die auch die Verpflichtung zur

[21] EuGH, C-432/05, Urteil vom 13. 3. 2007 Unibet [London] Ltd u.a. / Justitiekansler

Implementierung proaktiver Maßnahmen beinhaltet. Nimmt der Hostingdiensteanbieter den Inhalt hingegen zügig aus dem Netz, so erspart er sich diesen zusätzlichen Aufwand.

Werden die Inhalte durch den Hostinganbieter unter Bezugnahme auf seine Nutzungsbedingungen gesperrt, stehen dem betroffenen Inhalteanbieter zwar Rechtsmittel gegen den Hostingdiensteanbieter zur Verfügung. Jedoch kann dieser – sofern keine Monopolstellung vorliegt – nach dem Grundsatz der Privatautonomie den Vertrag mit dem Inhalteanbieter auch kündigen, wenn er kein Interesse an langfristigen Rechtsstreitigkeiten hat. Die Wirksamkeit eines Rechtsbehelfes des Inhalteanbieters gegen eine Maßnahme, mit welcher der Hostingdiensteanbieter seine Inhalte gesperrt hat, ist daher eingeschränkt. Auch dies dürfte Hostingdiensteanbieter im Zweifel zu einer Sperrung der Inhalte veranlassen.

3. Proaktive Maßnahmen Art. 6

Artikel 6 der Verordnung ist an die Hostingdiensteanbieter adressiert und stellt fest, dass diese gegebenenfalls proaktive Maßnahmen ergreifen, um ihre Dienste vor der Verbreitung terroristischer Inhalte zu schützen. Was genau proaktive Maßnahmen sind, legt die Verordnung nicht fest. Gemeint sind wohl auf Algorithmen basierende Programme, die nach gewissen Kriterien die Inhalte beim Upload prüfen. Die freiwilligen Maßnahmen müssen wirksam und verhältnismäßig sein, wobei der möglichen Beeinflussung durch terroristische Inhalte und den Grundrechten der Nutzer auf Meinungs- und Informationsfreiheit Rechnung zu tragen ist. Die freiwillige Umsetzung proaktiver Maßnahmen kann mittelbar die tatsächliche Möglichkeit der Inanspruchnahme der Meinungs- oder Informationsfreiheit der Inhalteanbieter und der Nutzer des Internet beeinträchtigen. Werden durch Filteralgorithmen Inhalte automatisch aus dem Internet entfernt, oder ihre Verbreitung gar präventiv verhindert, kann es in einem unübersehbaren Maße zu einer Beschränkung der Meinungs- und Informationsfreiheit kommen.

Hier findet somit eine Verlagerung staatlicher Aufgaben auf privatrechtlich organisierte Hostingdiensteanbieter statt. Soweit durch die Verordnung bestimmt wird, dass er bei der Verwendung proaktiver Maßnahmen den Grundzügen der demokratischen

Gesellschaft Rechnung zu tragen hat, ist dies zwar positiv, aber wohl kaum justiziabel. Die Beachtung der Meinungsfreiheit durch die Hostingdiensteanbieter unterliegt keiner Kontrolle durch die Behörden, Sanktionen sind bei einer Verletzung der Meinungs- und Informationsfreiheit nicht vorgesehen.

Der direkte Zwang spezielle automatisierte Instrumente in die Systeme der jeweiligen Diensteanbieter zu implementieren, stellt einen massiven Eingriff in das Recht auf Unternehmerische Freiheit dar. Die Hostingdiensteanbieter müssen technische und personelle Ressourcen aufbringen, um der Pflicht nachzukommen. Auch definiert die Behörde, nach welchen Parametern die Algorithmen filtern sollen. Ein wirksamer Rechtsbehelf hiergegen steht zwar dem Diensteanbieter zu, der Inhalteanbieter – dessen Inhalt z.B. wegen einer speziellen Filtervorschrift nicht zugelassen wird – hat jedoch keinerlei Rechtsbehelfe hiergegen. Er ist auf eine Beschwerde nach Art. 10 der Verordnung beim Diensteanbieter verwiesen.