

DGRI e. V. • Emmy-Noether-Straße 17 • D-76131 Karlsruhe

Per E-Mail: poststelle@bmjv.bund.de

Bundesministerium der Justiz und für Verbraucherschutz Herrn Dr. Meyer-Seitz Referat V B 2 11015 Berlin Veronika Fischer Geschäftsführung Emmy-Noether-Str. 17 76131 Karlsruhe

Telefon: 0721 782027-29 Telefax: 0721 782027-27 E-Mail: kontakt@dgri.de

Hamburg/Karlsruhe, 29.03.2017

Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz – Entwurf eines Gesetzes zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (NetzDG)

Hier: Stellungnahme der Deutschen Gesellschaft für Recht und Informatik (DGRI) e.V.

Ihr Zeichen: V B 2-6100/61 - 54 66/2017

Sehr geehrter Herr Dr. Meyer-Seitz, sehr geehrte Damen und Herren,

wir nehmen Bezug auf das Schreiben des Bundesministeriums der Justiz und für Verbraucherschutz vom 14. März 2017 an die beteiligten Verbände, mit dem das Ministerium um die Übermittlung von Stellungnahmen bis zum 30. März 2017 zum Referentenentwurf eines Gesetzes zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (NetzDG) bat (im Folgenden der "RE" oder "Referentenentwurf"; Angaben zu Vorschriften ohne Angabe des Gesetzes beziehen sich auf den Entwurf eines NetzDG). Dieser Bitte kommen wir für die DGRI gerne nach.

Die Deutsche Gesellschaft für Recht und Informatik e.V. (DGRI) ist eine der in Deutschland führenden unabhängigen wissenschaftlichen Vereinigungen, die sich mit Fragen im Bereich der Schnittstellen zwischen Informationstechnologie einerseits sowie Recht und Wirtschaft anderseits befasst. Zu ihren Mitgliedern zählen Wissenschaftler und Praktiker sowohl aus dem Gebiet der Rechtswissenschaft als auch der Technik. Mittels von der Gesellschaft veröffentlichter Stellungnahmen begleitet die DGRI Ge-

 Deutsche Gesellschaft für Recht und Informatik (DGRI) e.V.	Vorstand: Prof. Dr. Dirk Heckmann (1. Vors.)
 Geschäftsstelle: Veronika Fischer (Geschäftsführung)	Prof. Dr. Peter Bräutigam, DrIng. Peter J. Hoppen (stellv. Vors.) —
 Emmy-Noether-Str. 17, 76131 Karlsruhe	Steuer-Nr.: 35022/21902 (Finanzamt Karlsruhe-Stadt)
 - Tel.: +49(0)721 782027-29 • Fax: +49(0)721 782027-27	Bankverbindung: Sparkasse Karlsruhe
 E-Mail: kontakt@dgri.de • Internet: www.dgri.de	SWIFT-BIC: KARSDE66 • IBAN: DE27660501010022404743 —



setzgebungsvorhaben auf nationaler wie europäischer Ebene als neutrale Institution, die den Partikularinteressen einzelner Unternehmen oder Branchen nicht verpflichtet ist.

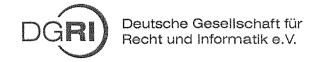
Einen Schwerpunkt ihrer Arbeit sieht die DGRI bei der Begleitung der rechtlichen Gestaltung der zunehmenden Digitalisierung unserer Informationsgesellschaft, die sich einer trennscharfen Unterordnung unter die klassischen Rechtsbereiche wie z.B. Medienrecht und Urheberrecht einerseits und Informationstechnologie- und Telekommunikationsrecht andererseits entzieht. Seit Inkrafttreten der Richtlinie 2000/31/EG (im Folgenden "ECRL") verfolgt die DGRI die Entwicklung dieser für die Entwicklung der Informationsgesellschaft zentralen Richtlinie und dort insbesondere die umfangreiche Rechtsprechung und Literatur zu deren Abschnitt 4 ("Verantwortlichkeit der Vermittler").

## I. Vorbemerkung zum Referentenentwurf

Die DGRI erlaubt sich den Hinweis, dass die Erstellung des vorliegenden Entwurfes von großer Eile geprägt und dem folgend die Frist zur Stellungnahme für die beteiligten Verbände äußerst knapp bemessen ist. Eine substantielle Stellungnahme zu den durch den Referentenentwurf aufgeworfenen komplexen Fragen im Umfeld der Providerverantwortlichkeit und mehr noch der betroffenen Meinungs- und Informationsfreiheit ist innerhalb dieser kurzen Frist nicht zu leisten.

Wir vermuten, dass die stark zunehmende öffentliche Diskussion um den Begriff der "Fake-News", die offenbar erfolgten Einflussnahmen auf Wahlen sowie die auf den 24. September 2017 festgelegte Bundestagswahl den Hintergrund für diese Eile bilden. Dazu kommt die erforderliche Notifizierung nach Art. 5 Abs. 1 der Richtlinie 2015/1535 mit ihrer dreimonatigen Stillhaltefrist. Die Notifizierung erfolgte offenbar am 27. März 2017, die Stillhaltefrist endet am 28. Juni 2017. Dies führt nach Ansicht unserer Organisation zu einem Zeitplan, der für ein ordnungsgemäßes Gesetzgebungsverfahren in einem grundrechtssensiblen Bereich wie vorliegend nicht einzuhalten ist. Die DGRI warnt davor, ein Gesetzesvorhaben in diesem ebenso wichtigen wie schwierigen Umfeld nicht unter den Zeitdruck eines imminenten Ereignisses zu stellen. Zudem hat sich in der Vergangenheit wiederholt gezeigt, dass besonders im Umfeld von Diensten der Informationsgesellschaft mit ihren schnellen Innovationszyklen gesetzliche Regelungen, die in Eile gefasst wurden, oft ihren eigentlichen Gegenstand verfehlen und Ursache für erhebliche Kollateralschäden sind.

Dem Referentenentwurf sieht man die Eile, mit der er erstellt wurde, an. Das belegen auch die kurzfristigen Änderungen unmittelbar vor der Notifizierung, die – soweit möglich – in dieser Stellungnahme berücksichtigt sind. Dem vorliegenden Entwurf eines NetzDG stehen auch in der geänderten Fassung schwerwiegende europarechtliche, verfassungsrechtliche und völkerrechtliche Einwände entgegen.



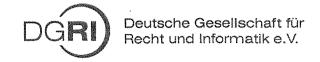
Auch die DGRI ist der Auffassung, dass Hasskriminalität wirksam bekämpft werden muss und dass auch strafbare Falschmeldungen nicht hingenommen werden können. Leitend für die Erwägungen bei einem Gesetzesvorhaben wie dem vorliegenden sollten dabei aber nicht die krassen Fälle z.B. offensichtlich rassistischer Schmähungen sein (die Anbieter sozialer Netzwerke schon nach der geltenden Rechtslage in Erfüllung ihrer Pflichten nach § 10 TMG entfernen werden), denn die ganz überwiegenden Fälle der Anwendung des NetzDG werden die nicht eindeutigen Fälle unterhalb solcher krassen Schmähungen darstellen. "Fake News" zudem werden häufig im Gewand der Nachricht, d.h. der Tatsachenbehauptung auftreten, deren Wahrheit bzw. Unwahrheit für den Anbieter sozialer Netzwerke nicht ohne weiteres feststellbar ist. Die DGRI begrüßt den Weg des BMJV, gemeinsam mit den Anbietern sozialer Netzwerke Lösungen für die schwierigen Probleme der Hasskriminalität und der Falschnachrichten zu suchen. Einer unter erheblichem zeitlichem Druck stehenden gesetzlichen Regelung in diesem sowohl technisch wie rechtlich komplexen Umfeld sollte der Gesetzgeber, zumal mit einem nationalen Alleingang widerstehen; die Meinungs- und Informationsfreiheit würde leiden.

## II. Rechtliche Einwände gegen den Gesetzesentwurf

### 1. Fehlende Gesetzgebungskompetenz des Bundes

Es fehlt für den Entwurf eines NetzDG an der Gesetzgebungskompetenz des Bundes. Unzutreffend stützt sich auf eine Gesetzgebungskompetenz im Hinblick auf das Recht der Wirtschaft (Art. 74 Abs. 1 Nr. 11 GG). Bei den Regelungen stehen keine wirtschaftlichen Interessen im Vordergrund (es geht auch nicht um geistiges Eigentum; dann wäre ggf. Art. 73 Abs. 1 Nr. 9 GG einschlägig). Vielmehr geht es dem Entwurf um die Eindämmung von Hasskriminalität und strafbaren Falschnachrichten in sozialen Netzwerken, da diese "eine große Gefahr für das friedliche Zusammenleben einer freien, offenen und demokratischen Gesellschaft" berge (RE, S. 1, 11). Die im RE enthaltenen Normen enthalten keinen wirtschaftsfördernden Zweck, sondern betreffen die Kommunikation in sozialen Netzwerken und regeln damit die Ausübung der Meinungsund Informationsfreiheitsrechte aus Art. 5 GG, bzw. sind als Ausfluss der öffentlichen Sicherheit und Ordnung anzusehen. Auch auf Art. 74 Abs. 1 Nr. 1 GG kann der NetzDG-E nicht gestützt werden, denn der Referentenentwurf legt keine Strafbarkeit von sozialen Netzwerken fest. Nur soweit es im Entwurf um Bußgeldvorschriften wegen Verstoßes gegen die Verpflichtungen geht, könnte sich die Gesetzgebungskompetenz des Bundes aus Art. 74 Abs. 1 Nr. 1 GG ergeben.

Neu stützt sich der RE nun auf eine Gesetzgebungskompetenz des Bundes nach Artikel 74 Abs. 1 Nr. 7 GG (öffentliche Fürsorge), da "das Schutzziel des Gesetzentwurfes, das sich gegen die Verrohung der Debattenkultur in sozialen Netzwerken richtet, auch den Schutzzweck des Jugendmedienschutzes berührt, nämlich die Entwicklung von Kindern und Jugendlichen oder ihre Erziehung zu einer eigenverantwortlichen und gemeinschaftsfähigen Persönlichkeit" (RE, S. 12).



Dies überrascht, denn im Vorentwurf führte das BMJV noch ausführlich dazu aus, wie gut und effektiv die Entfernung von Inhalten im Bereich der Kinder- und Jugendpornografie funktioniere. Es hieß dort u.a.:

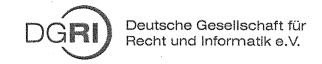
"Insbesondere die Pornografiedelikte der §§ 184ff des Strafgesetzbuches sind nicht in Absatz 3 aufgeführt, da diese Straftaten im Internet bereits effektiv verfolgt werden. Hier besteht bereits eine enge Kooperation zwischen dem Bundeskriminalamt (BKA), der länderübergreifenden Stelle jugendschutz.net, der Hotline des eco-Verbandes der Internetwirtschaft e.V. (eco e.V.), der Hotline der Freiwilligen Selbstkontrolle Multimedia Diensteanbieter e.V. (FSM e.V.), im Weiteren als "Beschwerdestellen" bezeichnet, und der Bundesprüfstelle für jugendgefährdende Medien (BPJM). Grundlage für die Zusammenarbeit von BKA, Beschwerdestellen und BPJM ist eine Kooperationsvereinbarung, in der die Verfahrensweise bei deutschen und ausländischen Fällen und die Grundlagen für eine einheitliche statistische Auswertung festgehalten sind."

Sofern diese Änderung kompetenzrechtlichen Erwägungen geschuldet sein sollte, ist darauf hinzuweisen, dass die Straftatbestände betr. die Kinder- und Jugendpornografie allenfalls einen Randbereich der eigentlich mit dem Referentenentwurf adressierten Probleme der Hasskriminalität und strafbaren Falschnachrichten ("Fake News") darstellen und dient damit nicht spezifisch dem Kinder- und Jugendschutz; eine Gesetzgebungskompetenz des Bundes für ein NetzDG kann darauf nicht gestützt werden.

### 2. Verstoß gegen Artikel 14, 15 ECRL

Soziale Netzwerke sind Hosting-Dienste im Sinne von Art. 14 ECRL. Regelungen zu sozialen Netzwerken, wie sie im Referentenentwurf vorgenommen werden, betreffen daher den durch diese Vorschrift harmonisierten Bereich. Das erkennt auch der Referentenentwurf (S. 12f.). Der Entwurf verkennt aber die Grenzen mitgliedsstaatlicher Regelungen und verstößt gleich mehrfach gegen die verbindlichen Vorgaben der ECRL:

Nach Art. 14 Abs. 1 lit. b) ECRL sind Hosting-Dienste verpflichtet, "unverzüglich" tätig zu werden, wenn sie von einem Rechtsverstoß Kenntnis erlangen. Die ECRL legt damit einen flexiblen Maßstab fest, der Raum für erforderliche Anpassungen im Einzelfall zulässt. Der Referentenentwurf sieht demgegenüber starre und zudem enge Fristen (24 Stunden bei offensichtlich rechtswidrigen, sowie 7 Tage für "jeden rechtswidrigen Inhalt") vor. Der BGH hat festgehalten, dass der deutsche Gesetzgeber den in Art. 14 ECRL enthaltenen Begriffen wegen der damit beabsichtigten Vollharmonisierung keinen über Art. 14 hinausgehenden Inhalt geben könne; "die Mitgliedsstaaten dürfen weder weitere noch engere Regelungen im nationalen Recht vorsehen" (BGH, AfP 2014, 145 Rn. 19 - Terminhinweis

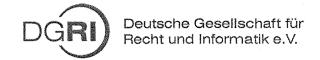


mit Kartenausschnitt). Die starren und kurzen Fristen des Referentenentwurfs stellen eine engere Regelung dar als sie Art. 14 ECRL mit dem flexiblen Begriff "unverzüglich" vorsieht.

Soweit der Referentenentwurf demgegenüber auf die Erwägungsgründe 46 und 48 ECRL verweist, greift dies nicht, denn diese gestatten Verfahren vor der unverzüglichen Entfernung bzw. Anordnungen von Gerichten und Behörden, lassen den Tatbestand des Art. 14 Abs. 1 und damit auch den Rechtsbegriff "unverzüglich" unberührt.

Eine Pflicht zum Tätigwerden begründet Art. 14 der ECRL für den Hosting-Dienst, wenn dieser die tatsächliche, positive menschliche Kenntnis erlangt hat, dass ein konkreter Inhalt auf seiner Plattform rechtswidrig ist. Dies umfasst nach h.M. auch die Kenntnis von der Rechtswidrigkeit der inkriminierten Information (Spindler/Schuster, Recht der elektronischen Medien, § 10 TMG Rn. 18 m.w.N.). Der Referentenentwurf geht demgegenüber da-Anbieter sozialen von aus. dass der eines Netzwerkes bei behaupteten Rechtsverletzungen durch die Einholung einer Stellungnahme des Verfassers bzw. durch externen Rechtsrat Ermittlungen zur Rechtswidrigkeit durchführt. Eine solche Pflicht, sich die Kenntnis erst zu verschaffen, ist mit den Vorgaben der Richtlinie nicht zu vereinbaren. Damit ist das Grundproblem der vom Referentenentwurf betroffenen Rechtsverletzungen berührt: Abgesehen von krassen z.B. rassistischen Schmähungen lässt sich einer Äußerung eben nicht auf den ersten Blick ansehen, ob sie rechtsverletzend oder unter dem Gesichtspunkt zulässiger Meinungsäußerung rechtmäßig ist. Dafür sind schwierige und komplexe Abwägungen unter Heranziehung des Kontextes der Äußerung erforderlich, die einem Anbieter sozialer Netzwerke, der weder Bezug zu den Beteiligten einer Äußerung noch Kenntnis von deren Kontext hat, nicht möglich ist. In Bezug auf Suchmaschinen führt Masing der Richter am Bundesverfassungsgericht Prof. Dr. aus (vgl. http://verfassungsblog.de/ribverfg-masing-vorlaeufige-einschaetzung-der-googleentscheidung-des-eugh/):

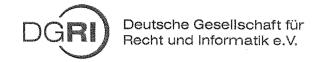
"Wann eine Äußerung als Beleidigung untersagt werden darf und wann sie als Wahrnehmung der Meinungsfreiheit hinzunehmen ist, unterliegt vielfach gestuften Rechtsvermutungen, Deutungsanforderungen und Abwägungsvorbehalten. Ebenfalls unterliegt ausdifferenzierten Regelungen, wann eine Person über eine andere welche Tatsachen behaupten darf, wie hierbei die Frage der Wahrheit der Tatsachenbehauptung zu beurteilen ist und diesbezüglich Darlegungs- und Beweislast zu verteilen sind; hierbei ist etwa auch zwischen der Presse und Privatpersonen zu unterscheiden. Wiederum spezifische Regeln gelten für die Frage was als "Privatsphäre" der Berichterstattung in welchen Situationen entzogen ist. [...] Das Spannungsverhältnis zwischen Äußernden und Betroffenen ist bisher grundsätzlich zwischen den sich insoweit mit je eigenen Rechten gegenüberstehenden Parteien ausgetragen und entschieden worden."



Art. 14 der ECRL sieht ein Notice-And-Takedown-Verfahren in Bezug auf konkret (gemeldete) Inhalte vor. Die Erstreckung dieser Pflicht in § 3 Abs. 2 Nr. 6 auf "sämtliche auf den Plattformen des sozialen Netzwerks befindlichen Kopien des rechtswidrigen Inhalts" stellt daher nicht eine "Konkretisierung und Klarstellung der Löschungsverpflichtung" (so RE, S. 24), sondern deren europarechtswidrige Erweiterung dar. Die Streichung der im Vorentwurf noch enthaltenen Vorschrift § 3 Abs. 2 Nr. 7, mit dem die Anbieter verpflichtet werden sollten, "wirksame Maßnahmen gegen das erneute Hochladen bereits entfernter rechtswidriger Inhalte zu treffen" (RE, S. 24), ist wegen des offensichtlichen Verstoßes gegen die ECRL zu begrüßen, kann aber die Europarechtswidrigkeit des Entwurfs nicht ausräumen.

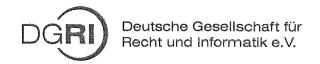
Soweit die Verfasser des Referentenentwurfs bei den über ein Notice-And-Takedown hinausgehenden Pflichten an die Rechtsprechung des EuGH (Rs. C-324/09 - L'Oréal/eBay) und die ihr folgenden Urteile des BGH (z.B. BGH GRUR 2011, 1038 - Stiftparfüm) denken, verkennen sie, dass es in diesen Fällen um Verletzungen von Rechten des geistigen Eigentums ging, und dass sich die vom EuGH erkannten weitergehenden Pflichten der Hosting-Dienste auf entsprechende europarechtliche Gestattungsnormen stützen konnten, nämlich Art. 8 Abs. 3 Richtlinie 2001/29 bzw. Art. 11 S. 3 Richtlinie 2004/48. Entsprechende Regelungen bestehen in Bezug auf die hier in Rede stehenden Verletzungen des allgemeinen Persönlichkeitsrechts (bzw. Schutzgüter des Staatsschutzes) nicht. Darin liegt auch kein Versäumnis des europäischen Gesetzgebers, denn Persönlichkeitsrechtsverletzungen, die stets im Einzelfall eine umfassende kontextbezogene Abwägung erfordern, eignen sich nicht für generelle oder gar vorbeugende Maßnahmen losgelöst vom Einzelfall. Auch hier zeigt sich wieder das Grundproblem des RE: Die erforderliche umfassende Abwägung ist einem Diensteanbieter, der ohne Kenntnis vom Kontext und ohne Beziehung zu den Beteiligten einer angegriffenen Äußerung eine Tätigkeit rein technischer, automatischer und passiver Art ausführt, in der Regel schon nicht möglich; ausgeschlossen ist dies jedenfalls für "vorbeugende Maßnahmen gegen zukünftige Rechtsverletzungen".

Die Verpflichtung in § 3 Abs. 2 Nr. 6 führt entgegen Art. 15 ECRL auch dazu, dass soziale Netzwerke die von ihnen gespeicherten Informationen überwachen und aktiv nach Umständen forschen müssen, die auf eine rechtswidrige Tätigkeit hinweisen. Es handelt sich dabei nicht um eine gemäß Erwägungsgrund 47 zulässige spezifische Überwachungspflicht, da jeder gespeicherte Inhalt auf der betreffenden Plattform mit solchen Inhalten abgeglichen werden müsste, die gesperrt worden sind, um weitere Kopien ausfindig zu machen. Damit beträfen die Überwachungspflichten alle Inhalte auf der Plattform (vgl. EuGH, Rs. 360/10 – SABAM/Netlog; BGH GRUR 2015, 485 Rn. 51, 59 – Kinderhochstühle im Internet III). Der RE verkennt den Pflichtenumfang seiner Regelungen, wenn er meint, damit würde keine "allgemeine Recherchepflicht" statuiert (S. 12). Im Übrigen führte die Tatsache, dass eine Verhinderung technisch möglich wäre, wie der Entwurf dies für Bildin-



halte annimmt, und von sozialen Netzwerken ggf. eingesetzt wird (S. 24), nicht zugleich dazu, dass dies zulässigerweise rechtlich verbindlich festgeschrieben werden kann.

- Die ECRL (v.a. bei Art. 14) unterscheidet nicht zwischen großen und kleinen Unternehmen oder gar Unternehmen mit Marktmacht. Eine Differenzierung, wie sie mit dem RE folgte, verstößt gegen die Richtlinie, aber auch gegen den allgemeinen Gleichheitssatz und führte zu einer Fragmentierung des Binnenmarkts. Mit der Streichung des Kriteriums "registriert" zur Bestimmung der Nutzerzahl wird eine Ermittlung, welche Anbieter unter diese Regelung fallen, im Übrigen kaum möglich sein.
- Auch die Berichtspflichten gemäß § 2, die Informations- und Begründungspflichten gegenüber einem Beschwerdeführer und dem betroffenen Nutzer gemäß § 3 Abs. 2 Nr. 5, die Dokumentations-, Kontroll- sowie weitere Pflichten nach § 3 Abs. 3 und Abs. 4, die Pflicht zur unverzüglichen Kenntnisnahme in § 3 Abs. 2 Nr. 1 und die Pflicht zur Beweissicherung und Speicherung im Inland gemäß § 3 Abs. 2 Nr. 4 stehen nicht im Einklang mit den Vorgaben der ECRL.
  - Die Regelungen des RE verstoßen gegen das Herkunftslandprinzip in Art. 3 Abs. 1 ECRL. Entgegen seiner Begründung (RE, S, 12 f.) greift keine Ausnahmeregelung, Das Herkunftslandprinzip verbietet es, über die durch die Richtlinie gesetzten Höchststandards hinauszugehen und den Diensteanbieter schärferen Regelungen als in seinem Herkunftsstaat zu unterwerfen (vgl. EuGH, AfP 2011, 265, Tz. 54-56 - eDate Advertising). Betreiber sozialer Netzwerke, die ihren Sitz im EU-Ausland haben, sind den dort geltenden Regelungen unterworfen. Auf eine Ausnahme durch abstrakt-generelle Normen, wie sie abschließend in Art. 3 Abs. 3 ECRL i.V.m. Anhang zu Art. 3 geregelt sind, stützt sich der RE nicht; eine solche Ausnahme liegt auch nicht vor. Maßnahmen i.S.d. Art. 3 Abs. 4 ECRL, auf die die Begründung des Referentenentwurfs hinweist, sind hingegen ausschließlich behördliche Schutzmaßnahmen nach Abwägung im konkreten Einzelfall; abstrakt-generelle Normen, die gezielt auf die Beschränkung der Ausübung eines Dienstes abzielen, sind unangemessen (vgl. Gersdorf/Paal, Informations- und Medienrecht, § 3 TMG, Rn. 32; Spindler/Schuster, Recht der elektronischen Medien, § 3 TMG Rn. 22). Eine solche Regelung richtete sich auch nicht "auf einen bestimmten Dienst" i.S.d. Art. 3 Abs. 4 ECRL, sondern auf die gesamte Kategorie "Anbieter sozialer Netzwerke". Es sind aber nur solche Maßnahmen zulässig, die sich gegen einen ganz bestimmten, konkret bezeichneten Anbieter richten (vgl. Mitteilung der EU-Kommission v. 14. Mai 2003, KOM(2003) 259 endg., S. 5). Zudem müsste vor einer Maßnahme gegen einen bestimmten Dienst der Informationsgesellschaft zunächst der Mitgliedstaat, in dem der betroffene Diensteanbieter seinen Sitz hat, erfolglos aufgefordert worden sein, Maßnahmen gegen den Diensteanbieter zu ergreifen; auch die Kommission wäre über geplante Maßnahmen zu unterrichten.



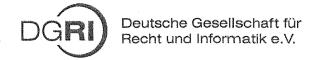
Fehlerhaft ist auch die Annahme (RE, S. 13), es läge ein dringlicher Fall im Sinne des Art. 3 Abs. 5 ECRL vor, der eine Abweichung von diesem Verfahrensablauf ermöglichte. Der Entwurf gibt selbst an, mit den Betreibern von sozialen Netzwerken bereits im Jahr 2015 eine Task Force ins Leben gerufen zu haben, um der zunehmenden Verbreitung von Hasskriminalität entgegenzuwirken. Die Thematik ist bereits seit mehreren Jahren bekannt, wird zudem auch auf EU-Ebene diskutiert und es sind Lösungsansätze mit unterschiedlichen sozialen Netzwerken besprochen worden. Unvorhergesehene Entwicklungen, die ein sofortiges Einschreiten gegen sämtliche großen Anbieter sozialer Netzwerke erforderte, sind nicht ersichtlich.

Entsprechendes gälte im Übrigen auch im Rahmen der Notifizierung nach der Richtlinie 2015/1535, die der deutsche Gesetzgeber offenbar am 28. März 2017 eingeleitet hat. Eine Dringlichkeit für die Umsetzung des NetzDG, die eine Ausnahme von der dreimonatigen Sperrfrist der Notifizierung nach Art. 6 Abs. 7 der Richtlinie 2015/1535 begründete, besteht aus den eben dargestellten Gründen nicht. Eine solche Dringlichkeit käme bei dringenden Gründen in Betracht, die auf einer unvorhergesehenen, plötzlich eingetretenen Situation "ohne die Möglichkeit einer vorherigen Konsultation" beruhen (Art. 6 Abs. 7 lit. a) der Richtlinie 2015/1535). Das liegt hier nicht vor, zumal das Thema Hasskriminalität auch auf europäischer Ebene adressiert wird. Es wäre zudem erforderlich, dass sich die Dringlichkeit gerade auf Deutschland bezieht. Auch das ist hier nicht ersichtlich.

### 3. Verfassungsrechtliche Aspekte

#### a) Übertragung der "Rechtsdurchsetzung" auf Private; fehlerhafte Anreize

Mit der umfangreichen Pflichtenübertragung auf die Anbieter sozialer Netzwerke sind aber zugleich weitere, verfassungsrechtliche Probleme verbunden, die mit dem von Bundesministerin Zypries geprägten Begriff der "Privatisierung der Rechtsdurchsetzung" treffend umschrieben sind. In Widerspruch zu dieser Pflichtenübertragung hebt der Referentenentwurf selbst hervor, dass nach der Kompetenzverteilung des Grundgesetzes allein die Gerichte dazu berufen sind, über die Strafbarkeit einer Handlung zu entscheiden, und ergänzt: "Zudem trägt die enge Einbeziehung der Gerichte zur notwendigen Klärung der Strafbarkeit von Handlungen und Äußerungen in sozialen Netzwerken bei" (RE, S. 27). Vom Anbieter eines sozialen Netzwerks verlangt der Entwurf, dass dieser über die Strafbarkeit derselben Handlungen innerhalb starrer und sehr kurzer Fristen nicht nur entscheidet, sondern die betreffenden Inhalte auch (endgültig) entfernt. Hinsichtlich der Auferlegung ähnlicher Pflichten bei Suchmaschinenbetreibern kritisierte der Richter am Verfassungsgericht Masing, dass diese damit zu privaten Schiedsinstanzen mit weitreichenden Entscheidungsbefugnissen über die Kommunikation im Netz auch in inhaltlicher Hinsicht würden (a.a.O.).



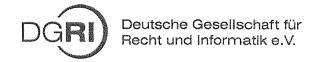
Mit dieser Übertragung von (Staats-)Aufgaben auf private Instanzen incentiviert der Referentenentwurf für den Dienstanbieter, Inhalte auf eine Meldung hin ohne Prüfung zu sperren. Denn warum sollte sich ein privates Unternehmen dem Risiko eines Bußgeldes aussetzen? Umgekehrt wird damit zugleich für den vermeintlich Betroffenen ein starker Anreiz gesetzt, gegen den Anbieter sozialer Netzwerke auch dann vorzugehen, wenn ihm der sich Äußernde bekannt ist, da er hier in kurzen Fristen und ohne rechtliches und finanzielles Risiko sein Ziel ohne eine langwierige und schwierige Auseinandersetzung mit ungewissem Ausgang erreichen kann. Das rechtliche Gehör des sich Äußernden bleibt dabei auf der Strecke. Inhalte würden so aus dem Netz entfernt, ohne dass deren Rechtswidrigkeit festgestellt worden wäre. Auch das weitere Verfahren, sofern es nicht zu einer Entfernung gemeldeter Inhalte kommt, ist vor dem Hintergrund der Verfahrensgrundrechte bedenklich: Soweit - wie erwähnt - die Feststellung der Strafbarkeit einer Äußerung dem Amtsgericht Bonn vorbehalten bleibt, erfolgt dessen Entscheidung weder in einem Verfahren noch sind die Beteiligten, insbesondere der sich Äußernde in die Entscheidungsfindung eingebunden. Die gerichtliche Entscheidung nach § 4 Abs. 5 kann (und würde wohl im Regelfall) ohne mündliche Verhandlung erfolgen; sie ist nicht anfechtbar (§ 4 Abs. 5 S. 4 und S. 5). Auch dies ist mit Grundsatz auf rechtliches Gehör (Art. 103 Abs. 1 GG) nicht zu vereinbaren.

# b) Einschnürende Effekte für die Kommunikationsgrundrechte

Mit großer Besorgnis sieht die DGRI, dass der RE die Meinungsfreiheit kaum anspricht. Zu den wahrscheinlichen Folgen der fehlerhaften Anreize durch den NetzDG-E wurde schon ausgeführt. Dabei geht sogar der Gesetzgeber davon aus, dass nur 2% der an das Bundesamt für Justiz gerichteten Anzeigen begründet sein werden (Referentenentwurf, S. 16). Damit wird das Risiko für die Entfernung zulässiger Inhalte spürbar. Der Gesetzesentwurf wird einschnürende Effekte auf die Meinungs- und Informationsfreiheit haben, vor denen das Bundesverfassungsgericht stets warnt (vgl. nur BVerfG, AfP 2009, 480 – Pressespiegel).

Dieses Risiko ist umso greifbarer, als der Entwurf des NetzDG keinerlei Vorgaben zum Inhalt eines Hinweises und zur Substantiierung der Rechtswidrigkeit macht. Damit wird es für den Betreiber eines sozialen Netzwerkes im Zweifel nicht immer sicher feststellbar sein, ob tatsächlich ein "rechtswidriger Inhalt" i.S.d. § 1 Abs. 3 vorliegt. Auch dies verstärkt mit Blick auf die drohenden Bußgelder den Anreiz, im Zweifel eine Löschung vorzunehmen, auch wenn diese dem Schutz der Kommunikationsfreiheit nicht gerecht wird.

Man kann dabei davon ausgehen, dass nicht die offenkundige, schwerwiegende Verletzung etwa durch unzweifelhafte rassistische Schmähungen den Regelfall des Anwendungsbereiches des NetzDG-E darstellen wird (wobei der auf solche Verletzungen hingewiesene Anbieter schon nach der geltenden Rechtslage regelmäßig seinen Entfernungspflichten nach § 10 TMG nachkommen wird), sondern diejenigen Fälle, bei denen die Rechtswidrigkeit nicht offensichtlich ist. Daran ist



der RE zu messen, zumal der Katalog in § 1 Abs. 3 sich auch nicht auf Straftatbestände beschränkt, die Hasskriminalität erfassen. Mit der Einbeziehung insbesondere der Vorschrift des § 185 StGB unterfällt vielmehr jede einfache Beleidigung dem Anwendungsbereich des Referentenentwurfs. Der Dammbruch durch Meldungen von vermeintlich Betroffenen, die sich die kurzen Fristen und erheblichen finanziellen Risiken der Betreiber sozialer Netzwerke zu Nutze machen wollen, ist vorprogrammiert.

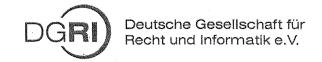
Die erforderliche Berücksichtigung der Meinungsfreiheit scheitert beim RE schon aufgrund seiner starren und kurzen Fristen: Wenn nach § 3 Abs. 2 eine Löschung innerhalb von 24 Stunden bzw. 7 Tagen zu erfolgen hat, können die Belange des sich Äußernden nicht angemessen berücksichtigt werden. Das gilt gerade auch in Bezug auf sog. "Fake News", bei denen es sich regelmäßig (wohl) um unwahre Nachrichten, also regelmäßig um Tatsachenbehauptungen handeln wird. Die Prüfung, ob eine Behauptung unwahr ist, wird aber in vielen Fällen eine aufwändige Prüfung mit sich bringen, die zumindest innerhalb einer Frist von 24 Stunden bzw. 7 Tagen nicht zu bewältigen ist.

Mit seinen weitergehenden Pflichten, dass "sämtliche Kopien" des Inhalts entfernt bzw. die Inhalte nicht noch einmal eingestellt werden dürfen (§ 3 Abs. 2 Nr. 6 und Nr. 7), verkennt der RE die Vorgaben der ständigen Rechtsprechung des Bundesverfassungsgerichts, wonach eine Äußerung stets in ihrem Kontext und unter Abwägung aller betroffenen Interessen zu beurteilen ist (vgl. nur BGH, AfP 2013, 57, Tz. 32 – IM Christoph; BGH, AfP 2012, 50 – Blog-Eintrag; zu Bildnisveröffentlichungen BGH, AfP 2009, 406 – Casiraghi mit Fliege). Der Entwurf blendet die Gesamtumstände aus, auf die es stets ankommt. Denn aus dem jeweiligen Kontext kann sich etwa ergeben, dass ein zulässiges Zitat vorliegt, eine Polemik, Satire oder ähnliches gegeben ist.

# c) Zur neuen datenschutzrechtlichen Ermächtigung einer Auskunftserteilung über Dritte

Gänzlich neu eingefügt wurde in den notifizierten Änderungsentwurf vom 27. März 2017 eine Ergänzung des § 14 Abs. 2 TMG. Diese in letzter Sekunde eingefügte Vorschrift dehnt die Anwendung der datenschutzrechtlichen Ermächtigungsnorm nicht nur aus; sie geht weit über die für den Gesetzeszweck des RE notwendige Gestattung hinaus, denn es werden Hosting-Dienste ermächtigt, Daten über Dritte herauszugeben betreffend die Durchsetzung von allen absolut geschützten Rechten. Auch hier führt die gesetzgeberische Eile zu nicht hinnehmbaren Beeinträchtigungen wesentlicher Verfassungsgüter und Grundrechte.

Einer Ergänzung von § 14 Abs. 2 TMG, um Strafverfolgungsbehörden zu ermöglichen, Daten von Anbietern sozialer Netzwerke übermittelt zu bekommen, bedurfte es nicht, denn diese Ermächtigung enthält der geltende § 14 Abs. 2 TMG schon ("für Zwecke der Strafverfolgung"). Der Wirkungsbereich der Ergänzung richtet sich damit auf die Durchsetzung zivilrechtlicher Ansprüche. Dabei stellt § 14 Abs. 2 TMG nur eine datenschutzrechtliche Ermächtigung dar; die Vorschrift be-

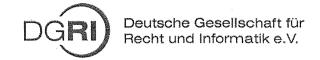


sagt, dass Diensteanbieter bestehende Auskunftsansprüche nicht aus datenschutzrechtlichen Erwägungen zurückweisen können (vgl. BT-Drs. 16/3078, S. 16). Eine Anspruchsgrundlage auf Auskunft über Dritte beinhaltet § 14 Abs. 2 TMG nicht. Soweit der RE in seiner geänderten Fassung auf die sog. *Jameda*-Entscheidung des BGH verweist (BGHZ 201, 380), folgt daraus ein allgemeiner Auskunftsanspruch über Dritte gerade nicht. Zwar hat der BGH in Einzelfällen den Auskunftsanspruch aus §§ 242, 259, 260 BGB auch auf eine Auskunft über Dritte ausgedehnt, dabei jedoch stets betont, dass es sich um Einzelfallentscheidungen unter einer gründlichen Verhältnismäßigkeitsprüfung handelt. Anders ließe sich diese Rechtsprechung auch nicht zu den ausdrücklichen Drittauskunftsansprüchen im gewerblichen Rechtsschutz und Urheberrecht (vgl. z.B. § 101 UrhG) abgrenzen.

Dem Auskunftsanspruch, den der RE ins Auge fasst, stehen wesentliche Rechtsgrundsätze entgegen: Nach § 13 Abs. 6 TMG sollen Diensteanbieter die Nutzung von Telemedien anonym oder unter Pseudonym ermöglichen, soweit dies technisch möglich und zumutbar ist. Diese Norm ist eine Konkretisierung des Datenvermeidungsgebots und Ausfluss des Rechts auf informationelle Selbstbestimmung der Nutzer. Darüber hinaus wäre eine Beschränkung der Meinungsäußerungsfreiheit auf Äußerungen, die einem bestimmten Individuum zugeordnet werden können, nicht mit Art. 5 Abs. 1 S. 1 GG vereinbar. Die Verpflichtung, sich namentlich zu einer bestimmten Meinung zu bekennen, würde die Gefahr begründen, dass der Einzelne aus Furcht vor Repressalien oder sonstigen negativen Auswirkungen sich dahingehend entscheidet, seine Meinung nicht zu äußern. Dieser Gefahr der Selbstzensur soll durch das Grundrecht auf freie Meinungsäußerung entgegen gewirkt werden (vgl. BGH, NJW 2009, 2888 Rn. 38 – spickmich.de).

Mit einem schlichten Verweis auf ein früheres und ein laufendes Gesetzgebungsverfahren und ohne eigene Begründung und Prüfung führt der RE eine weit über den Zweck des Entwurfes hinausgehende Ermächtigung ein. Im bezogenen Gesetzgebungsverfahren hatte der Gesetzgeber eine entsprechende Regelung diskutiert, aber nach Anhörung verschiedener Sachverständiger verworfen (vgl. dazu BGHZ 201, 380 Rn. 16). Eine solche gründliche Prüfung ist unabdingbar und im vorliegenden Verfahren nicht erfolgt. Der Verweis auf § 24 BDSG n.F. kann schon deshalb nicht hinreichen, weil es sich hierbei selbst nur um einen Entwurf handelt; zudem deutet die dortige Begründung darauf hin, dass jene Regelung nicht zur Durchsetzung von Rechten Dritte zu dienen bestimmt ist (vgl. BT-Drs. 18/11325, S. 96).

Es mag eine zu schließende Lücke bestehen, für bestimmte Verletzungen des Persönlichkeitsrechts einen Auskunftsanspruch zu ermöglichen. Dafür wäre aber ein geordnetes Gesetzgebungsverfahren, in dem die widerstreitenden Interessen und Rechte ermittelt und gegeneinander abgewogen werden, notwendig. Das Versäumnis eines solchen Verfahrens führt im vorliegenden Fall führt zu einer nicht akzeptablen, einseitigen Regelung.

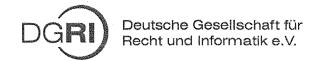


# d) Zur Speicherungspflicht zu Beweiszwecken auf inländischen Servern

Die Pflicht für ausländische Unternehmen, in Deutschland Server zu betreiben und hier zu "Beweiszwecken" entfernte Inhalte im Inland zu speichern (§ 3 Abs. 2 Nr. 4), ist beispiellos; diesen Pflichten stehen schwerwiegende verfassungsrechtliche Bedenken entgegen:

Zum einer wird diese Speicherpflicht auch personenbezogene Daten betreffen, ohne dass die Speicherung auf eine bestimmte Dauer, einen näheren Zweck oder bestimmte Verwendungsund Zugriffsrechte beschränkt wäre. Die Einfügung einer zeitlich beschränkten Speicherung im geänderten Entwurf vom 27. März 2017 (begrenzt auf 10 Wochen) führt nicht zur Zulässigkeit der Regelung. Denn die weiterhin pauschale und unbeschränkte Speicherungspflicht "auf Vorrat" ist unvereinbar mit dem Recht des Betroffenen auf informationelle Selbstbestimmung. Einschränkungen bedürfen einer verfassungsgemäßen gesetzlichen Grundlage, die insbesondere den rechtsstaatlichen Geboten der Normenklarheit und Verhältnismäßigkeit entsprechen muss. Auch fehlte es an den erforderlichen organisatorischen und verfahrensrechtlichen Vorkehrungen, die der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken (BVerfG, 1 BvR 209/83, Urt. v. 15.12.1983, juris, Leitsatz 2 - Volkszählungsurteil). Zur fehlenden Rechtsmäßigkeit der Vorratsdatenspeicherung bemängelte der EuGH zudem, dass die Regelungen zur Vorratsdatenspeicherung keine materiell- und verfahrensrechtlichen Voraussetzungen für den Zugang der zuständigen nationalen Behörden zu den Daten und deren spätere Nutzung und kein objektives Kriterium vorsah, das es erlaubt, die Zahl der Personen, die zum Zugang zu den auf Vorrat gespeicherten Daten und zu deren späterer Nutzung befugt sind, auf das angesichts des verfolgten Ziels absolut Notwendige zu beschränken (EuGH, NJW 2014, 2169, Tz. 61f.). Diese Erwägungen gelten in noch stärkerem Maße für den Referentenentwurf: Der NetzDG-E beschränkt sich in seiner Regelung zur Speicherungspflicht zu Beweiszwecken (vgl. § 3 Abs. 2 Nr. 4 NetzDG-E) auf einen lapidaren Halbsatz, jegliche Konkretisierung fehlt. Dem datenschutzrechtlichen Erforderlichkeitsgrundsatz wird nicht Rechnung getragen, es erfolgt keinerlei Begrenzung hinsichtlich der Art der Daten und der möglichen Betroffenen oder Vorgaben zu notwendigen Sicherheitsvorkehrungen. Es ist nicht geregelt, wer in die Daten Einsicht nehmen kann und wann und unter welchen Voraussetzungen welche Stelle Auskunft verlangen kann bzw. wie mit den Daten im weiteren Verlauf verfahren werden soll und wie (und wann) eine Löschung gegebenenfalls zu erfolgen hat.

Daneben fehlt der Regelung die notwendige verfassungsgemäße gesetzliche Grundlage, wie dies der aus dem Rechtsstaats- und Demokratieprinzip erwachsende Vorbehalt des Gesetzes verlangt. Schon ein Gesetzeszweck für die Speicherung im Inland lässt sich mit der erforderlichen Bestimmtheit weder aus den Regelungen selbst noch aus der Begründung entnehmen: In § 3 Abs. 2 Nr. 4 heißt es nur "zu Beweiszwecken", ohne dass klar würde, welcher Beweis zu sichern und zu welchen Zwecken dies erfolgen soll. Aber auch die Begründung bleibt ungenau: "in erster Linie" soll die Sicherung der Strafverfolgung gegen den "Absender" einer Nachricht dienen.



Eine konkrete Beschlagnahmemaßnahme nach den Vorgaben der StPO muss gerade nicht vorliegen; vielmehr sollen Pflichten der sozialen Netzwerke im Vorfeld begründet werden, an die ggf. z.B. Beschlagnahmeentscheidungen nach § 94 Abs. 2 StPO anschließen könnten. Auch das wird aber nicht näher konkretisiert. Mangels eines Gesetzeszwecks fehlt für die erforderliche Verhältnismäßigkeitsprüfung schon eine Grundlage, an der die Geeignetheit, Erforderlichkeit und Verhältnismäßigkeit i.e.S. zu messen wäre.

## 4. Zur Frage der internationalen Anwendbarkeit des deutschen Strafrechts

Der Referentenentwurf will (tut dies aber letztlich nicht) den Begriff des rechtswidrigen Inhalts bewusst eng definieren und knüpft ihn an einen Katalog enumerativ aufgezählter Strafrechtsvorschriften, nämlich der §§ 86, 86a, 90, 90a, 111, 126, 130, 140, 166, 185 bis 187, 241 und 269 des Strafgesetzbuchs; dazu treten mit den Änderungen vom 27. März 2017 zusätzlich die Vorschriften §§ 90b, 91, 100a, 129 bis 129b, 131, 184b und 184d StGB. Nicht "begangene Ordnungswidrigkeiten oder bloße unerlaubte Handlungen", sondern "ausschließlich die Rechtsdurchsetzung bei der Bekämpfung von Hasskriminalität und strafbaren Falschnachrichten" soll geregelt werden (RE, S. 19). Dieses Ziel gibt der Katalog in § 1 Abs. 3 nicht wider. Insbesondere der Tatbestand der Beleidigung nach § 185 StGB geht weit über das Ziel hinaus, denn er erfasst nicht nur "Hasskriminalität und strafbare Falschnachrichten", sondern jede einfache Beleidigung.

Zudem spricht der RE die naheliegende Frage der Grenzen der internationalen Anwendbarkeit des deutschen Strafrechts nicht einmal an. Denn Äußerungen und anderen im Internet abrufbaren Inhalten auf den Plattformen, die der Referentenentwurf in sein Blickfeld genommen hat – Facebook, Twitter, YouTube – ist immanent, dass sie nicht vor Staatengrenzen haltmachen. Dieses Versäumnis überrascht auch vor dem Hintergrund einer kürzlich ergangenen Entscheidung des 3. Strafsenats des BGH (NStZ 2015, 81), in dem eine Person von einem Computer aus Tschechien auf der Plattform YouTube einen Kanal mit der Bezeichnung "Arische Musikfraktion" betrieb, in dem er u.a. Abbildungen von Hakenkreuzen hochlud. Der BGH verneinte die Anwendbarkeit deutschen Strafrechtes auf diesen Sachverhalt. Das wird entsprechend für die überwiegende Anzahl der in § 1 Abs. 3 genannten Vorschriften jeweils dann gelten, wenn ein Upload nicht von Deutschland aus erfolgte. Das führt nicht nur dazu, dass dieses Gesetz in einer Vielzahl von Fällen nicht anwendbar sein wird; es erschwert auch den Anbietern sozialer Netzwerke die Feststellung rechtswidriger und offensichtlich rechtswidriger Inhalte.

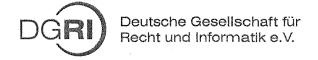
Nach § 3 StGB gilt das deutsche Strafrecht für Inlandstaten, d.h. solche, die in Deutschland begangen wurden. Daneben dehnt das in §§ 5 – 7 StGB festgelegte Schutzprinzip die nationale Strafgewalt auf Taten aus, die zwar im Ausland begangen werden, jedoch bestimmte inländische Rechtsgüter gefährden oder verletzen. Dies gilt etwa für die §§ 90, 90a, und 90b, dort teilweise mit der Einschränkung, dass der Täter Deutscher ist und seine Lebensgrundlage im Geltungsbe-



reich des StGB hat (vgl. § 5 Nr. 3 StGB), für § 100a StGB – Landesverräterische Fälschung und die §§ 184b, 184d StGB (Straftaten in Bezug auf kinder- und jugendpornographische Inhalte). Von diesen Tatbeständen lässt sich nur § 100a StGB unter die beiden Oberbegriffe Hasskriminalität und strafbare Falschnachrichten ("Fake News") subsumieren. Bei den Tatbeständen der §§ 90, 90a und 90b StGB erscheint fraglich, ob dabei die Bekämpfung von Hasskriminalität und strafbaren Falschnachrichten im Vordergrund stehen. Zudem reicht die internationale Anwendbarkeit dieser Vorschriften überwiegend nur soweit, als ein deutscher Staatsbürger mit Lebensgrundlage in der Bundesrepublik Deutschland die Straftaten begeht, was ein Anbieter sozialer Netzwerke kaum jemals wird feststellen können, insbesondere nicht innerhalb der vom RE gesetzten Fristen.

Für alle übrigen in der Auflistung des § 1 Abs. 3 genannten Straftatbestände gilt das Territorialitätsprinzip: Sie gelten nur für Straftaten *im Inland*, d.h. der Ort der Handlung oder teilweise der Erfolgsort müssen in Deutschland liegen. Als Handlungsort wird bei Internetdelikten der Ort angesehen, an dem der Täter körperlich gehandelt hat. Das wird bei den vom Referentenentwurf verfolgten Inhalten häufig – und wie in dem vom BGH entschiedenen Fall – nicht der Fall sein. Bei Internetsachverhalten wird eine "*virtuelle Anwesenheit*" des Täters im Inland dann angenommen, wenn dieser Daten mit rechtswidrigem Inhalt vom Ausland her gezielt und kontrolliert auf einem in Deutschland installierten Server ablegt (Münchener Kommentar zum StGB, § 9 Rn. 29). Bei den vom Referentenentwurf in Aussicht genommenen Plattformen wird es, sofern diese überhaupt über Server in Deutschland verfügen, jedenfalls an dieser gezielten und kontrollierten Ablage fehlen, denn der Standort der Server wird von technischen Zufälligkeiten abhängig sein, die sich in der Regel nicht vom Täter steuern lassen.

Zwar kommt eine Anwendbarkeit deutschen Strafrechts teilweise auch dann in Betracht, wenn der Täter zwar im Ausland handelt, aber der Erfolgsort in Deutschland belegen ist. Hierbei ist zwischen Verletzungs- und Gefährdungsdelikten zu unterscheiden. Während Verletzungsdelikte stets Erfolgsdelikte sind, kommt es bei einem Gefährdungsdelikt auf die Schaffung einer Gefahr an. Daher lehnt der BGH bei abstrakten Gefährdungsdelikten die Existenz eines Erfolgsortes grundsätzlich ab, weil diese Delikte keinen Gefahrenerfolg im Sinne der allgemeinen Tatbestandslehre besitzen. Für die Bestimmung des anwendbaren Rechts wird bei abstrakten Gefährdungsdelikten daher allein auf den Handlungsort und nicht auch auf einen etwaigen Erfolgsort abgestellt. Die in § 1 Abs. 3 genannten Straftatbestände §§ 86, 86a, 111, sowie mit Einschränkungen auch die Vorschriften der §§ 126, 130, 140 StGB sind abstrakte Gefährdungsdelikte. Mit dem BGH bedürfte es zur Feststellung der Anwendbarkeit des deutschen Strafrechts daher einer Untersuchung des im einzelnen Fall einschlägigen Straftatbestands sowie des Aufenthalts- bzw. Tätigkeitsorts des Täters bzw. Teilnehmers. Das wird den Betreibern der vom NetzDG-E angesprochenen Plattformen schon nicht ohne weiteres möglich sein. Es überrascht, dass der Referentenentwurf diese naheliegende und für seinen Wirkungsgrad wichtige Frage nicht einmal anspricht.



Für Rückfragen oder ergänzende Erläuterungen steht Ihnen die Gesellschaft gerne zur Verfügung.

Mit freundlichen Grüßen,

RAin Veronika Fischer Geschäftsführung der DGRI e.V.

RA Jörg Wimmers, LL.M. (NYU) Mitglied des Vorstands der DGRI e.V.