Stellungnahme

Referentenentwurf eines 2. Gesetzes zur Änderung des Telemediengesetzes (2. TMGÄndG)
08. April 2015

BITKOM vertritt mehr als 2.200 Unternehmen der digitalen Wirtschaft, davon gut 1.400 Direktmitglieder. Sie erzielen mit 700.000 Beschäftigten jährlich Inlandsumsätze von 140 Milliarden Euro und stehen für Exporte von weiteren 50 Milliarden Euro. Zu den Mitgliedern zählen 1.000 Mittelständler, mehr als 200 Start-ups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Hardware oder Consumer Electronics her, sind im Bereich der digitalen Medien oder der Netzwirtschaft tätig oder in anderer Weise Teil der digitalen Wirtschaft. 76 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, 10 Prozent kommen aus Europa, 9 Prozent aus den USA und 5 Prozent aus anderen Regionen. BITKOM setzt sich insbesondere für eine innovative Wirtschaftspolitik, eine Modernisierung des Bildungssystems und eine zukunftsorientierte Netzpolitik ein.

Bundesverband
Informationswirtschaft,
Telekommunikation und
neue Medien e.V.

Albrechtstraße 10
10117 Berlin-Mitte
Tel.: +49.30.27576-0
Fax: +49.30.27576-400
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner
Judith Steinbrecher, LL.M.
Bereichsleiterin
Gewerblicher Rechtsschutz
& Urheberrecht
Tel.: +49.30.27576-155
Fax: +49.30.27576-51155
j.steinbrecher@bitkom.org

Nick Kriegeskotte
Bereichsleiter
Telekommunikationspolitik
Tel.: +49.30.27576-224
Fax: +49.30.27576-51224
n.kriegeskotte @bitkom.org

Präsident
Prof. Dieter Kempf

Hauptgeschäftsführer
Dr. Bernhard Rohleder

Zusammenfassung

Der BITKOM begrüßt die Absicht des Gesetzgebers, die offene WLAN-Abdeckung in Deutschland zu verbessern und Anbieter von offenen WLAN-Zugängen als Zugangsprovider i.S.d. § 8 TMG zu bewerten. Allerdings ergeben sich hinsichtlich der mit dem Referentenentwurf vorgelegten Gesetzesinitiative zahlreiche rechtliche und auch praktische Fragen, ob damit das intendierte Ziel tatsächlich erreicht werden kann. Die Regelungen zu angemessenen Sicherungsmaßnahmen für WLAN-Zugänge durch anerkannte Verschlüsselungsverfahren gehen an den Erfordernissen und Marktstandards vorbei und bedürfen daher einer grundlegenden Anpassung.

Der Referentenentwurf verknüpft mit dem gesetzgeberischen Ziel zur Erweiterung der WLAN-Abdeckung eine Änderung der Regeln zur Privilegierung von Hosting-Diensten (§ 10 TMG), die eine gänzlich andere, in Teilen sogar sich widersprechende Zielsetzung hat. Eine Verknüpfung beider Änderungen sollte daher vermieden werden.

Dem Vorschlag des Referentenentwurfs zu § 10 TMG steht der BITKOM – wie nachfolgend dargestellt werden wird –aus einer ganzen Reihe von grundsätzlichen Einwänden ablehnend gegenüber.

Insgesamt drohen mit einer Verschärfung von Haftungsregelungen, wie sie hier vorgeschlagen werden, standortpolitische Kollateralschäden. Die gilt es aber insgesamt zu vermeiden. Die durch E-Commerce-Richtlinie und Telemediengesetz vorgegebene, gestufte Haftung für eigene und fremde Rechtsverstöße (Persönlichkeitsrechtsverletzungen, Äußerungsdelikte, Verstöße gegen Urheber- und Markenrechte) hat sich grundsätzlich bewährt. Die damit verbundene Rechtssicherheit war und ist wesentlicher Garant für die Praktikabilität und damit

den Erfolg zahlreicher Internetdienste auf den verschiedensten Wertschöpfungsstufen. Diese unterschiedlichen Stufen der Wertschöpfung im Internet (Access, Hosting, Inhalte) bedürfen auch weiterhin unterschiedlicher Haftungsregelungen. Jede Ergänzung der bestehenden Regelungen um neue Kategorien muss daher sicherstellen, dass das bestehende Haftungsgefüge davon nicht beeinträchtigt wird.

1 Artikel 1 Ziffer 2 des 2. TMGÄndG zur Änderung von § 8 TMG

BITKOM begrüßt es, dass sich die Bundesregierung zum Ziel setzt, die WLAN-Abdeckung in Deutschland zu verbessern. Auch unterstützen wir die geplante gesetzgeberische Klarstellung, Diensteanbieter, die einen Zugang zur Nutzung ihres drahtlosen lokalen Funknetzes vermitteln, als Zugangsprovider i.S.d. § 8 TMG zu bewerten.

Allerdings geht BITKOM nicht davon aus, dass das Gesetz, wie von der Bundesregierung bezweckt, in der vorgeschlagenen Form zu mehr Rechtssicherheit und einer Förderung offener WLAN-Angebote führt. Im Gegenteil verlagert es für WLAN-Betreiber allenfalls die Rechtsunsicherheit. Für Accessprovider die gleichzeitig Hotspots betreiben stellt der Entwurf eine Verschärfung der Haftung und Verschlechterung gegenüber dem Status Quo dar. BITKOM befürchtet deshalb, dass eine weitere Verbreitung offener WLAN-Angebote eher behindert und sogar bestehende Angebote einschränkt werden.

Zudem wird die Verantwortlichkeit von WLAN-Anbietern seit September 2014 in einem Vorlageverfahren beim EuGH thematisiert (C-484/14). Das LG München I hat in dem Verfahren neun Fragen zur Haftung eines WLAN-Anbieters im Gefüge der E-Commerce-RL vorgelegt (Beschl. v. 18.9.2014 – Az. 7 O 14719/12) – u.a. die Frage, unter welchen Bedingungen WLAN-Anbieter als Access-Provider nicht der Störerhaftung unterliegen. Es besteht daher die Gefahr, dass der Gesetzgeber mit dem vorliegenden Entwurf zum TMGÄndG eine Regelung schafft, die auf europäischer Ebene möglicherweise gar keinen Bestand haben kann.

Zudem lässt der Referentenentwurf unberücksichtigt, dass nach der geltenden Rechtslage Access-Provider, die den nunmehr von der Störerhaftung befreiten Diensteanbietern von drahtlosen lokalen Funknetzwerken den eigentlichen Internetzugang zur Verfügung stellen, sich selbst unter Umständen weiterhin Unterlassungsansprüchen ausgesetzt sehen und gezwungen werden könnten, aus diesem Grund Maßnahmen gerade gegen diese Diensteanbieter einzuleiten. Es wäre sinnvoll, diesen Aspekt in die Richtung mit zu regeln, dass auch die den Netzzugang vermittelnden Access-Provider unter vergleichbaren Voraussetzungen von der Störerhaftung befreit werden. Es ist kein Grund ersichtlich, das bestehende und von der E-Commerce-Richtlinie vorgegebene Haftungsgefüge zu verändern, insbesondere nicht, die Abstufungen aufgrund jeweiliger „Risikonähe“ in ihr Gegenteil zu verkehren bzw. den dafür gegebenen sachlichen Hintergrund auszublenden.

Die vorgeschlagene Regelung macht in § 8 Abs. 4 Nr. 1 TMG-E die Verschlüsselung des WLANs bzw. eine vergleichbar wirksame Maßnahme zur ersten Voraussetzung der beabsichtigten Haftungsprivilegierung. Was unter der Maßnahme der „Verschlüsselung“ genau zu verstehen ist und welche Zielrichtung der Referentenentwurf mit dieser Anforderung genau verfolgt, ist jedoch fraglich. Der Entwurf überträgt an dieser Stelle zudem Grundsätze der Rechtsprechung, die im Bereich der Haftung für private WLANs entwickelt wurden, auf den kommerziellen Bereich, ohne die besonderen Gegebenheiten von insbesondere größeren kommerziellen Hotspot-Angeboten zu berücksichtigen.

Terminologie des § 8 Abs. 4 Nr. 1 TMG-E

§ 8 Abs. 4 TMG, wie er in dem Referentenentwurf vorgeschlagen wird, wirft zunächst Fragen bzgl. der dort hinterlegten Anforderungen auf. Zum einen bleibt unklar, was genau unter einer „sicheren Verschlüsselung“ („angemessene Sicherungsmaßnahmen durch anerkannte Verschlüsselungsverfahren oder vergleichbare Maßnahmen“) zu verstehen ist. Des Weiteren stellt sich die Frage, was genau mit „aktueller Firmware/Verschlüsselung“ gemeint ist.

Auch stellt sich die Frage, was unter der in § 8 Abs. 4 Nr.1 TMG-E geforderten „Verschlüsselung“ im Konkreten zu verstehen ist. Technisch könnte die gewählte Terminologie im Sinne einer Verschlüsselung des Datenverkehrs als solchem verstanden werden. Andererseits macht der Gesamtzusammenhang des § 8 Abs. 4 Nr. 1 TMG-E deutlich, dass hier eher die Zugriffskontrolle, etwa im Wege des WPA2-Verfahrens gemeint ist, mithin eine technische Absicherung des jeweiligen WLAN-Netzes durch einen „Zugangsschlüssel“. Diese Interpretation folgt auch aus der Begründung, die ebenfalls auf die Zugriffssteuerung abstellt. Hier wäre indes eine Klarstellung wünschenswert, weil auch die in der Begründung verwendete Terminologie einer „Verschlüsselung des Routers“ nicht hinreichend präzise ist.

Der Referentenentwurf übersieht außerdem, dass der Einsatz von Verschlüsselung eher eine Ausnahme im Bereich von offenen WLAN-Diensten darstellt. Es gibt alternative Maßnahmen, die sehr viel verbreiteter sind und zu dem gleichen Ziel – nämlich der Einschränkung des Nutzerkreises und dem Aufbau einer psychologischen Hürde – führen. Die meisten Hotels und Cafés bieten ihr WLAN aktuell im Wege eines Anmeldeportales an, auf dem Nutzer die Nutzungsbedingungen akzeptieren müssen. Ob bei diesem Beispiel von „Verschlüsselung“ oder einer „vergleichbaren Maßnahme“ gesprochen werden kann, bleibt unklar. Aus Sicht des BITKOM erfüllen gängige Portalsystem-Lösungen, die Maßnahmen wie AGB-Unterzeichnung und Kontrolle des Zugriffs vorsehen, vollumfänglich die notwendigen Voraussetzungen.

Wenn man überhaupt die Haftungsbefreiung von „angemessenen Sicherungsmaßnahmen“ abhängig machen will, dann sollte offen bleiben, ob es sich dabei um eine Verschlüsselung oder aber um z.B. Anmeldeportale handelt.

Verschlüsselungsanforderungen in der bisherigen Rechtsprechung

Eine Verschlüsselung über das WPA2-Verfahren kann dort als eine Form der Zugangskontrolle dienen, wo der Zugang nur einem sehr kleinen Personenkreis im Wege eines insoweit innerhalb dieses Kreises vertraulichen Passworts ermöglicht werden soll. Dies ist vor allem bei der Nutzung von WLAN im privaten Umfeld, etwa bei Familien und Wohngemeinschaften, der Fall. Entsprechend hatte die bisherige Rechtsprechung vor allem für diese spezifischen Konstellationen eine hinreichende Absicherung über WPA2-Keys im Sinne einer Verkehrssicherungspflicht des Anschlussinhabers gefordert. Dies geschah in den entsprechenden Fällen nicht zuletzt, um etwaigen Schutzbehauptungen einer unberechtigten Nutzung eines Dritten aufgrund eines nicht abgesicherten WLAN einen Riegel vorzuschieben.

Vor diesem Hintergrund erscheint es jedoch fraglich, welche Schutzrichtung der Referentenentwurf in § 8 Abs. 4 Nr. 1 TMG-E mit der Vorgabe der Verschlüsselung in seiner Übertragung auf kommerzielle Anbieter verfolgen will.

Zusammenspiel der § 8 Abs. 4 Nr. 1 und Nr. 2 TMG-E

Auch ist BITKOM die Verknüpfung von § 8 Abs. 4 Nr. 1 und § 8 Abs. 4 Nr. 2 TMG-E unklar.

Nimmt man die Begründung des Entwurfs zum Maßstab, soll über § 8 Abs. 4 Nr. 1 TMG-E der gewerbliche Betreiber eines WLANs verpflichtet werden, eine Zugriffskontrolle einzurichten, um insoweit „unberechtigten" Zugriff auf das WLAN zu unterbinden. Die Nr. 1 dient also haftungsrechtlich dem Schutz vor Rechtsverletzungen durch Nutzer des WLANs, die sich gegen den Willen des Betreibers Zugang zu dessen Netz verschafft haben.

§ 8 Abs. 4 Nr. 2 TMG-E soll dagegen – im Sinne der beabsichtigten Förderung „offener" WLAN-Netze die haftungsrechtliche Voraussetzungen für die insoweit intendierte Nutzung durch „berechtigte" Nutzer regeln.

Die Pflicht zur Zugriffskontrolle nach § 8 Abs. 4 Nr. 1 TMG-E böte mithin weder aus IT-Sicherheits-Perspektive noch aus haftungsrechtlicher Perspektive einen eigenständigen Schutz. Sie wäre eine rein rechtliche Formalie, da die entscheidenden haftungsrechtlichen Wertungen letztlich durch § 8 Abs. 2 Nr. 2 TMG-E getroffen werden.

Da insoweit haftungsrechtlich durch § 8 Abs. 4 Nr. 1 TMG-E kein vertiefender Schutz im Verhältnis zu Nr. 2 gewährleistet wird, stellt sich die Frage, ob andere Gründe Basis für diese Regelung sind. Es wäre jedoch systemfremd, IT-Sicherheitsanforderung nunmehr im Bereich der Haftungsregeln des TMG festzulegen, während zugleich im Rahmen des IT-Sicherheitsgesetzes über die entsprechenden Anforderungen an Telemedienanbieter diskutiert wird.

Fazit

Insgesamt weisen wir darauf hin, dass durch die pauschale Forderung nach „Verschlüsselung" die Hürden für das Anbieten eines offenen WLAN-Netzes deutlich erhöht werden. So gibt es im Markt auch aus den Reihen unserer Mitglieder bereits eine Reihe verschiedener Geschäftsmodelle, von denen nur wenige eine Zugangssicherung zum lokalen Funknetz, dafür aber andere Sicherheitsvorkehrungen in Bezug auf den Zugang zum eigentlichen Internetzugang vorsehen und die angesichts des nun vorliegenden Gesetzesentwurfs teilweise nicht oder nur in geänderter Form Bestand haben können.

Eine Verschlüsselungspflicht behindert daher die Verbreitung geschäftsmäßiger offener, auf andere Weise gesicherter WLAN-Angebote und widerspricht damit der politischen Zielsetzung und verschärft die durch die Rechtsprechung geschaffenen präzisierten Haftungsmaßstäbe, indem sie die für private WLAN-Zugänge entwickelten Obliegenheiten unreflektiert auf gewerbliche Angebote überträgt. Dabei wird übersehen, dass die für private WLAN-Zugänge von der Rechtsprechung entwickelten Grundsätze maßgeblich davon getrieben waren,

prozessuale Schutzbehauptungen des Anschlussinhabers im Sinn einer nicht identifizierbaren Drittnutzung durch unberechtigten Zugriff haftungsrechtlich einen Riegel vorzuschieben. Diese Anforderungen sind aber nicht auf die besonderen Gegebenheiten von Betreibern großer Hotspots übertragbar.

Es wird übersehen, dass Betreiber von großen Hotspots mit einer Verschlüsselungspflicht stärker belastet werden als Betreiber von kleineren Hotspots, denn je kleiner der Hotspot, desto leichter lassen sich z.B. Passwörter kommunizieren. Für diese Ungleichbehandlung sehen wir keinen sachlichen Grund. Zudem wirkt dies dem Ziel einer möglichst großflächigen WLAN-Versorgung gerade entgegen.

Auch führt eine Verschlüsselung wie dargelegt alleine zu keiner besseren Durchsetzbarkeit bei Rechtsverletzungen. Allenfalls kann der Nutzerkreis eingeschränkt und dadurch eine psychologische Hürde geschaffen werden. Allerdings bleibt die Frage, ob ein offeneres WLAN-Angebot tatsächlich, wie so häufig behauptet, zu mehr Rechtsverletzungen führt. Erfahrungswerte zeigen, dass selbst aktuell offene Hotspots von Accessprovidern auch ohne Verschlüsselungsmechanismen nicht Gegenstand von Auskunftsersuchen sind, d.h. offensichtlich keine maßgeblichen Rechtsverletzungen über diese offenen Hotspots begangen werden, sondern dass solche Internetanschlüsse ausschließlich zum Zwecke der Information und Kommunikation genutzt werden.

2 Artikel 1 Ziffer 3 des 2. TMGÄndG zur Änderung von § 10 TMG

Auch wenn wir die wirksame Rechtsdurchsetzung von Urheberrechtsverletzungen im Internet grundsätzlich unterstützen, so lehnen wir es dennoch ausdrücklich ab, auf nationaler Ebene den Versuch zu starten, die Regelung des § 10 TMG noch weiter einzuschränken. BITKOM lehnt es auch ab, dass diese gravierende und grundsätzliche Einschränkung der Providerhaftung nahezu beiläufig im Paket mit dem Ausbau von offenem WLAN politisch verhandeln zu wollen. Die Zielsetzung beider Gesetzesvorhaben ist so unterschiedlich, dass die Klarheit der jeweiligen Interessenslage verfälscht zu werden droht.

Der Entwurf ist nicht geeignet, die von ihm selbst formulierten Ziele zu erreichen. Er verstößt gegen europäisches Recht und führt als nationaler Alleingang zu einer Zersplitterung des Binnenmarkts und zu rechtlicher Inkohärenz. Er beseitigt so nicht, er verstärkt die schon bestehenden Rechtsunsicherheiten. Unter anderem mit der Einführung einer Regelung, die die „vermutete“ statt der tatsächlichen Kenntnis von einer rechtswidrigen Handlung ausreichen lassen will, nimmt der Referentenentwurf eine besondere Haftungsverschärfung vor. Damit müsste der Diensteanbieter die gesetzliche Vermutung entkräften, also nachweisen keine Kenntnis von Tatsachen gehabt zu haben, aus denen eine Rechtsverletzung offensichtlich wird. Dies widerspricht der derzeitigen Rechtslage des Art.14 und insoweit auch der die Vollharmonisierung verlangenden E-Commerce-Richtlinie.

Die Begründung ist widersprüchlich: Ein Vorgehen gegen Anbieter, die ihren Sitz in Deutschland haben, ist weder schwierig noch gar unmöglich. Die „gefahrgeneigten Dienste“, die der Entwurf im Blick hat, haben ihren Sitz nicht in Deutschland. Fakt ist daher, dass es im Geltungsbereich des TMG keinen Fall in

Deutschland gibt, auf den diese Regelung Anwendung finden könnte. Umgekehrt wird der Entwurf die Dienste, die er im Blick haben mag, nicht erreichen. Dagegen verstärkt der Entwurf für in Deutschland tätige Hosting-Anbieter die ohnehin schon bestehende Rechtsunsicherheit erheblich, weil er ohne Not einen weiteren unbestimmten Rechtsbegriff einfügt, der jahrelange Gerichtsverfahren nach sich ziehen wird. Dies und die ggf. nur vorsorglich umzusetzenden Verpflichtungen setzen wegen des damit verbundenen Aufwands Marktzutrittsschranken insbesondere für kleine Unternehmen und Start-Ups, ersticken so Innovation und Investition und konterkarieren damit die Ziele der E-Commerce-Richtlinie.

Ebenfalls untragbar ist die Auswirkung von § 10 Abs. 2 lit a) TMG-E auf Cloud-Dienste, da für die zukunftsträchtigen Branchen des Cloud-Hosting neue Rechtsunsicherheiten begründet werden und dies tendenziell innovationsschädlich ist. Upload-Plattformen, deren Geschäftsmodell auf User-Generated-Content basiert und daher nicht auf Urheberrechtsverletzungen zurückzuführen ist, werden unverhältnismäßigen Rechtsunsicherheiten ausgesetzt.
Dasselbe gilt, unter Umständen noch in verstärktem Maße, für die *alternativ* zur Haftungsbegründung vorgeschlagenen lit. b) und d). Mit diesen Regelungen wird der gesamte deutsche und europäische Anbieterkreis von Speicherdiensten einem Generalverdacht ausgesetzt, der für die Wettbewerbsfähigkeit und eine an den Nutzerbedürfnissen orientierte Entwicklung dieses Sektors absolut kontraproduktiv ist. Spätestens an dieser Stelle erweist sich die zur Diskussion gestellte Konstruktion, mit einer Vermutung der Kenntnis und damit der Rechtswidrigkeit zu arbeiten, als nicht tragbar. Die Beachtung der über verschiedene grundrechtliche, einfachgesetzliche und vertragliche Verbürgungen geschützten Rechte von Nutzern von Speicherdiensten verhindert *a priori*, dass sich der Anbieter positive Kenntnis verschafft. Die Begründung des Entwurfs zeigt nicht nur an dieser Stelle bei verständiger Würdigung hinreichend klar auf, dass gerade dies dem Anbieter i. S. d. § 10 TMG zum Nachteil gereichen soll; vorliegend würde es sich also um eine offensichtlich widersprüchliche Wertung durch den Gesetzgeber handeln.

§ 10 TMG in der aktuellen Fassung ist die rechtmäßige Umsetzung der E-Commerce-Richtlinie. Die dort niedergelegten Grundsätze zur Verantwortlichkeit von Host-Providern basieren auf einem bei Erlass der Richtlinie (und national auch zuvor) breit diskutierten Interessensausgleich, sie sind weitgehend unverändert praxisgerecht, unterdessen europaweit erprobt und durch die Rechtsprechung insbesondere des EuGH ausgeprägt.

Schon die Prämisse des Entwurfs, dass er nur unzweideutig festlege, was bei Auslegung des Rechts schon heute der Fall sei, erscheint falsch: Soweit der BGH von „gefahrgeneigten Diensten“ gesprochen hat, führte dies nicht zum Verlust einer Privilegierung oder zu einer vermuteten Kenntnis, sondern löste nur erweiterte Prüfpflichten im Rahmen der Störerhaftung aus, diese zumal nur „anlassbezogen“ auf konkrete Rechtsverletzungen (vgl. BGH GRUR 2013, 1030 Rn. 43, 44, 45 – File-Hosting-Dienst). In seinem jüngsten Urteil (BGH, Urteil vom 19. März 2015 - I ZR 94/13 – Hotelbewertungsportal) spricht der BGH sogar davon, dass erst „ein hochgradig gefährliches Geschäftsmodell […] besondere Prüfungspflichten“ auslösen könne.

Der Referentenentwurf geht damit weit über das hinaus, was der BGH jüngst entschieden hat. Um eine Inanspruchnahme zu vermeiden, wäre ein Diensteanbieter gehalten, stets zu kontrollieren, dass nicht „weit überwiegend“ rechtswidrige Inhalte bei ihm gespeichert werden und erlegte ihm so eine faktische allgemeine Überwachungspflicht auf. Es ist ein elementarer Grundsatz der E-Commerce-Richtlinie, dass einem Vermittler von Internetdiensten keine allgemeine Verpflichtung auferlegt werden darf, wonach dieser die übermittelten oder gespeicherten Informationen überwachen müsse oder aktiv nach Umständen zu forschen habe, die auf eine rechtswidrige Tätigkeit hinweisen würden. In einem vorgelagerten Schritt stellt sich überdies auch schon die Frage, wie ein Diensteanbieter wissen soll, in welchem Umfang sein Dienst möglicherweise für rechteverletzende Inhalte missbraucht wird, ohne die Expertise der ebenfalls betroffenen Rechteinhaber innezuhaben und ohne die Inhalte fortwährend zu überwachen.

Der Referentenentwurf verstößt aber nicht nur damit gegen europäisches Recht, denn die Bestimmungen über die Verantwortlichkeit in der E-Commerce-Richtlinie bezwecken eine Vollharmonisierung; die Mitgliedstaaten dürfen weder weitere noch engere Regelungen im nationalen Recht vorsehen (BGH 2014, 180 Rn. 19 – Terminhinweis mit Kartenausschnitt). Die Regelungen des Referentenentwurfs stellen aber nicht eine Präzisierung, sondern eine Einschränkung der Regeln zur Verantwortlichkeit der Vermittler dar, die die E-Commerce-Richtlinie nicht vorsieht und die auch nicht im Einklang mit der Rechtsprechung des EuGH zur Auslegung der Richtlinie steht. Den Begriff einer „Gefahrgeneigtheit“ kennt der EuGH nicht nur nicht; sie reichte nach dessen Rechtsprechung auch nicht aus. Vielmehr muss der Anbieter seine passive Rolle als Vermittler verlassen, um haftbar zu sein (EuGH, Urt. v. 23.03.2010, Az. C-236, 237, 238/08 – Louis Vuitton/ Google, Tz. 120). Und auch dann ist er nur bezüglich des konkreten Angebots nicht schutzwürdig, für das er z.B. „aktiv“ geworben hat (EuGH GRUR 2011, 1025, Tz. 123 – L’Oréal/eBay). Eine dauerhafte Verantwortung für alle Inhalte, wie sie der Referentenentwurf vorsieht, kennt der EuGH nicht. Umgekehrt greift der Entwurf die vom EuGH formulierten Kriterien nicht auf, sondern formuliert eigene am europarechtlichen Gefüge vorbei. Es erscheint auch gesetzgeberisch weder erforderlich noch sinnvoll, die etablierte und sich ausbildende Rechtsprechung durch systemfremde Begriffe zu unterlaufen.

Unbestimmte Rechtsbegriffe wie „gefahrgeneigte Dienste“, „weit überwiegende Zahl“ und die weiteren Tatbestände des Referentenentwurfs zu § 10 Abs. 2 werden Anlass für eine Vielzahl von Rechtsstreitigkeiten begründen, deren Auslegung und Bedeutungsgehalt bis zu einer höchstrichterlichen Klärung einschließlich Vorabentscheidungsverfahren beim EuGH auf lange Zeit unklar bleiben werden und so Hosting-Dienste zusätzlicher Rechtsunsicherheit aussetzen. Der Entwurf erreicht so seine Ziele nicht nur nicht; er schafft das Gegenteil.

Die bestehenden gesetzlichen Regelungen und die breit praktizierten Notice-and-Take-Down-Verfahren spiegeln die hohe Verantwortung wider, denen sich die Diensteanbieter verpflichtet sehen. Sie stellen sicher, dass die Beurteilung der Rechtswidrigkeit von sachkundiger Stelle erfolgt und nicht einem technischen Dienstleister überantwortet wird. Eine Ausweitung der Verantwortungssphären und Haftungsverpflichtungen zulasten der Diensteanbieter steht daher weder im Einklang mit den verbindlichen Normen und der Rechtsprechung des

EuGH, noch würde diese die technischen Möglichkeiten der Praxis korrekt abbilden. Bereits jetzt sind insbesondere Hostprovider mit einer Rechtsprechung des BGH (z.B. die Entscheidung des Bundesgerichtshofs „Kinderhochstühle II“ im Fall Stokke; Urteil vom 16.05.2013; Az.: I ZR 216/11 und zuletzt „Kinderhochstühle III“ im Fall Stokke, BGH, Urt. v. 05.02.2015 - Az.: I ZR 240/12) konfrontiert, die weit über das hinausgeht, was Gerichte anderer EU-Mitgliedsstaaten vergleichbaren Providern auferlegt haben – ein Zustand der für die deutsche Internetwirtschaft untragbar ist und letztlich über die europaweit und weltweit agierenden Anbieter auch unmittelbar Auswirkungen auf andere Länder hat.

Da es international tätigen Diensteanbietern häufig nicht möglich sein wird, in der Behandlung der Inhalte zu unterscheiden, wird mittelbar eher der deutsche Standard in europäische Nachbarländer exportiert als dass der europäische Haftungsstandard der E-Commerce-Richtlinie in Deutschland Anwendung findet.

Im Gegenteil sollte, wie in 2011 bereits versucht, die Verantwortlichkeit der Internet Service Provider auf ein sachgerechtes Maß begrenzt und wieder in Einklang mit den grundlegenden Vorgaben der E-Commerce-Richtlinie gebracht werden.