Deutscher Bundestag Ausschussdrucksache 16(9)1424
16. Wahlperiode 27. Februar 2009
Ausschuss für Wirtschaft und Technologie

Stellungnahme

27.2.2009

zur Öffentlichen Anhörung des Wirtschaftsausschusses des Deutschen Bundestages zum Gesetzentwurf der Fraktion der FDP „Entwurf eines […] Gesetzes zur Änderung des Telemediengesetzes (…Telemedienänderungsgesetz - … TMGAanG) – Drucksache 16/11173

Mittwoch, d. 4. März 2009, 10.00 – 12:30 Uhr

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. vertritt mehr als 1.200 Unternehmen, davon 900 Direktmitglieder mit etwa 135 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu zählen Anbieter von Software, IT-Services und Telekommunikationsdiensten, Hersteller von Hardware und Consumer Electronics sowie Unternehmen der digitalen Medien. Der BITKOM setzt sich insbesondere für bessere ordnungspolitische Rahmenbedingungen, eine Modernisierung des Bildungssystems und eine innovationsorientierte Wirtschaftspolitik ein.

Bundesverband
Informationswirtschaft,
Telekommunikation und
neue Medien e.V.

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

Ansprechpartner
Dr. Guido Brinkel
Rechtsanwalt
Bereichsleiter Medienpolitik
Tel. +49. 30. 27576-221
Fax. +49. 30. 27576-51-221
g.brinkel@bitkom.org

Präsident
Prof. Dr. Dr. h.c. mult.
August-Wilhelm Scheer

Hauptgeschäftsführer
Dr. Bernhard Rohleder

Zusammenfassung

- BITKOM unterstützt das mit dem vorgelegten Gesetzentwurf verfolgte Anliegen, die Verantwortlichkeit der Internet Service Provider auf ein sachgerechtes Maß zu begrenzen und wieder in Einklang mit den grundlegenden Vorgaben der E-Commerce-Richtlinie zu bringen.

- BITKOM sieht die bestehenden Rechtsunsicherheiten in erster Linie durch die Auslegung und Anwendung des TMG und des Prinzips der Störerhaftung durch die deutsche Rechtsprechung begründet. Die dem TMG zugrunde liegende E-Commerce-Richtlinie bewerten wir als ausgewogenes und sachgerechtes Haftungsregime.

- BITKOM unterstützt das in § 7 Abs. 2, S. 2 des Entwurfs angelegte Subsidiaritätsprinzip.

- BITKOM unterstützt die in § 7 Abs. 2, S. 2 und § 7 Abs. 4, S. 4 angelegten Klarstellungen hinsichtlich der Verteilung der Darlegungs- und Beweislast.

- Durch die Konstruktion der Überwachungspflichten werden heute regelmäßig im Urteilstenor selbst nicht die genauen Grenzen der Überwachung bestimmt. Die Frage, ob etwa hinreichende Monitoring-Maßnahmen eingeleitet wurden, bleibt damit einer Beurteilung im Einzelfall im Vollstreckungsverfahren überlassen. BITKOM sieht daher die Notwendigkeit einer stärkeren Konkretisierung des Providern auferlegten Pflichtenprogramms und einer Korrektur in Richtung einer Präzisierung der Pflichten bereits in der gerichtlichen Ausgangs-Entscheidung.

- Wir unterbreiten für die Ausgestaltung des § 7 Abs. 2 TMG folgenden modifizierten Formulierungsvorschlag:

> *„Auf Grundlage allgemeiner Gesetze ergangene gerichtliche oder verwaltungsbehördliche Anordnungen dahingehend, eine begangene Rechtverletzung abzustellen, bleiben auch im Falle der Nichtverantwortlichkeit des Diensteanbieters nach den §§ 8 – 10 [a] unberührt, wenn sich Maßnahmen gegenüber dem Anbieter der Informationen als nicht durchführbar oder Erfolg versprechend erweisen und die Abstellung der Rechtsverletzung technisch möglich und zumutbar ist."*

- BITKOM begrüßt die im Entwurf enthaltene Einbeziehung von Suchmaschinen und Hyperlinks in das Haftungsregime des Telemediengesetzes.

- Die in § 13 Abs. 1 TMG-E vorgesehene Erstreckung der datenschutzrechtlichen Informationspflichten auf die Dauer der Speicherung bewerten wir skeptisch, da die Dauer der Speicherung in der Praxis von verschiedenen Bedingungen abhängig ist, die zu Beginn des Nutzungsvorgangs häufig nicht absehbar sind. Insbesondere differiert die Dauer je nach Datensatz auch aufgrund verschiedener parallel zur Geltung kommender rechtlicher Vorschriften.

- Den in § 13 Abs. 8 TMG vorgesehenen Regelungen zur Behandlung von Cookies stehen wir skeptisch gegenüber. Zum einen ist die Information über die Verwendung von Cookies bereits jetzt übliche Praxis und entsprechende Informationspflichten sind auch Voraussetzung zur Erteilung von Prüfzertifikaten durch Zertifizierungsunternehmen, von denen die namhaften Unternehmen weitestgehend Gebrauch machen. Zum anderen bieten die gängigen Browser dem Nutzer heute bereits differenzierte Einstellungsmöglichkeiten, die wesentlich praktikabler sind, als eine gesetzliche Informationspflicht des Dienstanbieters in Verbindung mit einem Widerspruchsrecht.

- Über den vorgelegten Entwurf hinaus bedarf es Überlegungen für ein Anreizsystem hinsichtlich freiwilliger Maßnahmen durch Host-Provider. Bislang werden solche Maßnahmen durch den Rechtsrahmen nicht gefördert, sondern durch die damit verbundene „Kenntnis" der Inhalte eher bestraft. Die Lösung könnte für Host-Provider in einem Notice-and-Takedown-Verfahren nach gesetzlichen Eckpunkten liegen, bei dessen Einsatz dem Provider weiterreichende Privilegierungen zugute kommen.

Inhalt Seite

1 Einleitung

BITKOM begrüßt die Initiative des Wirtschaftsausschusses, im Rahmen einer öffentlichen Anhörung die Problematik des Verantwortlichkeitsregimes des Telemediengesetzes (TMG) auf Basis des von der FDP-Fraktion vorgelegten Entwurfs aufzugreifen. Wir verbinden hiermit die Hoffnung, dass die seit langem angekündigte und dringend notwendige Überarbeitung der entsprechenden Regelungen nun endlich zeitnah im Rahmen konkreter Gesetzesinitiativen angegangen wird.

BITKOM beschäftigt sich seit langem mit dem Verantwortlichkeitsregime für Internet-Service-Provider (ISP) und hat bereits im Jahr 2007 im Rahmen der vom Bundeswirtschaftsministerium durchgeführten Evaluation der Verantwortlichkeitsregelungen des TMG eine umfassende Einschätzung abgegeben.[1]

Die seit 2007 ergangenen, teils höchstrichterlichen, Entscheidungen haben aus unserer Sicht die grundlegenden Problemstellungen nicht gelöst, sondern insbesondere durch die aufgekommene Tendenz zur Annahme täterschaftlicher Mitwirkungsbeiträge eher noch verschärft. Aktuelle Entscheidungen von Instanzgerichten haben überdies neuen rechtspolitischen Handlungsbedarf erkennen lassen, so etwa im Bereich der urheberrechtlichen Behandlung von Bildersuchdiensten.[2] Schließlich tangieren auch die aktuellen politischen Initiativen im Hinblick auf Zugangshürden bzgl. ausländischer Internetangebote die Frage der Reichweite der Verantwortlichkeit von Internet-Service-Providern. Zu letzterem Punkt verweisen wir auf unsere kürzlich hierzu veröffentlichte eigenständige Stellungnahme.[3]

Nach wie vor gibt es aus Sicht des BITKOM somit dringenden Überarbeitungsbedarf, um Fehlentwicklungen einer teils widersprüchlichen, teils exzessiven Rechtsprechung entgegenzuwirken. Wir sehen die in Deutschland zu Tage getretenen Probleme in erster Linie in den Entwicklungen der Rechtsprechung begründet, die aus unserer Sicht insbesondere zu Widersprüchen gegenüber grundlegenden Prinzipien der E-Commerce-Richtlinie geführt haben. Die E-Commerce-Richtlinie selbst bewerten wir als sachgerechte Leitlinie für die Verantwortlichkeitsverteilung.

Da seitens des BGH in sämtlichen relevanten Verfahren eine Vorlage gegenüber dem EuGH unterblieben ist, konnte bislang die Vereinbarkeit der höchstrichterli-

[1] Abrufbar unter http://www.bitkom.org/files/documents/BITKOM_Stellungnahme_Verantwortlichkeit_TMG_30.08.2007.pdf .
[2] Vgl. LG Hamburg, 308 O 42/06: „Es ist damit Sache des Gesetzgebers und nicht der Gerichte, dieses grundrechtsrelevante Spannungsverhältnis zwischen dem ohne Frage hoch anzusiedelnden Interesse der Allgemeinheit an effizientem Zugang zu grafischen Informationen im Netz sowie den wirtschaftlichen Interessen der Beklagten einerseits und den oben skizzierten, ebenfalls grundrechtlich geschützten Interessen der Urheber andererseits aufzulösen."
[3] Abrufbar unter http://www.bitkom.org/files/documents/090205_BITKOM-Stellungnahme_Expertengespraech_UA_neue_Medien_12_2_2009.pdf.

chen Anwendung des Telemediengesetzes mit den europarechtlichen Vorgaben nicht juristisch geklärt werden. Umso wichtiger erscheint eine Novellierung der einschlägigen Vorschriften des TMG im Sinne einer Klarstellung und Begrenzung der ausufernden Rechtsprechungsentwicklungen.

Der vorgelegte Gesetzentwurf greift die Problemstellungen auf und unterbreitet sinnvolle Lösungsansätze, wenngleich in den Details aus Sicht des BITKOM teils noch Überarbeitungsbedarf besteht. BITKOM begrüßt den Entwurf insgesamt nachdrücklich als geeignete Diskussionsgrundlage für die weiteren Beratungen.

2 Zu den einzelnen Regelungen des Gesetzentwurfs

2.1 § 7 Abs. 2 TMG – Reichweite der Haftung für Rechtsverletzungen Dritter

2.1.1 Problemlagen und jüngste Entwicklungen

Die häufig apodiktisch als „Privilegierungen“ titulierten Haftungsregelungen der §§ 8 bis 10 TMG werden von der Rechtsprechung des Bundesgerichtshofs einschränkend dahingehend ausgelegt, dass sie nur auf Schadensersatzansprüche und strafrechtliche Verantwortlichkeit anwendbar sein sollen, nicht aber auf Unterlassungsansprüche. Dies gründet auf einer sehr weitgehenden Interpretation von § 7 Abs. 2, S. 2 TMG. Dieser greift mit seiner Regelung, wonach

> *„Verpflichtungen zur Entfernung oder Sperrung der Nutzung von Informationen nach den allgemeinen Gesetzen […] auch im Falle der Nichtverantwortlichkeit […] unberührt“*

bleiben sollen, in leicht abgewandelter Formulierung Regelungen der E-Commerce-Richtlinie auf, die allerdings, wie aus der Begründung der entsprechenden Vorschriften hervorgeht, nur einzelfallbezogene Maßnahmen erlauben. Zwei Senate des Bundesgerichtshofs interpretieren § 7 Abs. 2, S. 2 TMG dagegen in mittlerweile ständiger Rechtsprechung derart, dass der gesamte Bereich der verschuldensunabhängigen Haftung, insbesondere auf Unterlassung, von den Begrenzungstatbeständen der §§ 8 bis 10 TMG nicht erfasst wird und hierüber insbesondere auch vorbeugende, in die Zukunft gerichtete Überwachungspflichten entstehen können.

Von der gesetzlich vorgesehenen Haftungsbeschränkung der verschiedenen Provider bleibt in der Praxis kaum etwas übrig. Denn hier dominieren Unterlassungsansprüche in Form der sog. Störerhaftung seit langem das Bild. Dies liegt schon darin begründet, dass im Bereich der Immaterialgüterrechte, die den Hauptanteil der entsprechenden Verfahren vor den Gerichten ausmachen, die Störerhaftung mit dem Ziel von Unterlassungsverfügungen die verschuldensabhängige Haftung auf Schadensersatz praktisch vollständig verdrängt hat.

Insbesondere die Rechtsprechung des BGH in den beiden „Rolex“-Entscheidungen (BGH Urteil vom 11.3.2004 - I ZR 304/01; BGH Urteil vom

19.04.2007 – I ZR 35/04), der „Internetversteigerung III“-Entscheidung (BGH Urteil v. 30. 8. 2008 – I ZR 73/05) sowie in der Foren-Entscheidung (BGH Urteil vom 27. März 2007 - VI ZR 101/06) hat nicht nur im Bereich der Internetauktionen für erhebliche Rechtsunsicherheit gesorgt. Aus den in den Urteilen enthaltenen grundsätzlichen Feststellungen zur Haftung von Hostprovidern folgen auch für andere Geschäftsmodelle wie das Web-Hosting, elektronische Marktplätze oder Foren erhebliche Probleme. Negativen Einfluss wird diese Rechtsprechung auch auf die weitere Marktentwicklung von sog. Web 2.0-Angeboten (soziale Netzwerke und user generated content) haben.

Im Bereich des Wettbewerbsrechts hat außerdem die Entscheidung des Bundesgerichtshofes in der Sache „Jugendgefährdende Medien bei eBay“ (BGH Urteil v. 12. 7. 2008 – I ZR 18/04) eine weitere Verschärfung des Haftungsregimes mit sich gebracht. Mit dem Urteil statuiert der BGH eine täterschaftliche Haftung des Plattformbetreibers für Rechtsverletzungen Dritter und legt zugleich konkrete Pflichten für in die Zukunft gerichtete Überwachungsmaßnahmen fest, die über Fallgestaltungen einer reinen Wiederholung der konkret begangenen Rechtsverletzung weit hinausgehen. Die Entscheidung manifestiert damit zum einen die allgemeine Tendenz der Rechtsprechung zur Entwicklung proaktiver Überwachungspflichten und begründet zum anderen die Gefahr einer Erstreckung der mittelbaren Verantwortlichkeit auf Schadensersatzansprüche und selbst den Bereich strafrechtlicher Verantwortlichkeit.

Die als Intermediäre agierenden Internet Service Provider sind über die Rechtsprechungsentwicklung in Deutschland in den vergangenen Jahren somit ins Zentrum der Verantwortlichkeit im Internet gerückt. Dies widerspricht grundlegenden Erwägungen der E-Commerce-Richtlinie und führt für das Internet faktisch zu einer Art Sonderrecht, in welchem die Inanspruchnahme des eigentlichen Verletzers mehr und mehr zugunsten einer Inanspruchnahme der Intermediäre in den Hintergrund gedrängt wird.

Es bedarf aus den geschilderten Gründen daher dringend gesetzlicher Präzisierungen der Providerverantwortlichkeit im TMG, welche auch den zentralen Bereich der Störerhaftung erfassen, um den Unternehmen die notwendige Rechtssicherheit zu geben, deren Schaffung der eigentliche Ausgangspunkt der E-Commerce-Richtlinie war.

2.1.2 Die vorgeschlagenen Regelungen

Der vorgelegte Gesetzentwurf sieht verschiedene Modifikationen vor, die den dargelegten Problemlagen Rechnung tragen und auf eine Synchronisierung des deutschen Haftungsrechts mit den Vorgaben der E-Commerce-Richtlinie abzielen. Die vorgeschlagene Neuregelung beinhaltet im Wesentlichen vier Elemente zur Korrektur der ausufernden Verantwortlichkeit der ISP:

- Einführung eines Subsidiaritätsprinzips (§ 7 Abs. 2 S. 2, letzter Halbsatz).
- Begrenzung von Entfernungs- und Sperrungspflichten auf die konkrete Rechtsverletzung (§ 7 Abs. 3 TMG-E)

- Klärung der Beweislastverteilung in Bezug auf Verkehrspflichten (§§ 7 Abs. 2, S. 2 letzter Halbsatz, Abs. 4, S. 4)
- Konkretisierung des Pflichtenprogramms (§ 7 Abs. 2, S. 2 letzter Halbsatz, Abs. 4, S. 4)

Die vorgeschlagenen Elemente sind aus Sicht des BITKOM grundsätzlich geeignet, die eingangs beschriebenen Problemstellungen zu lösen und entsprechende Fehlentwicklungen der Rechtsprechung zu korrigieren. In der gesetzestechnischen Umsetzung sehen wir teilweise noch Präzisierungsoptionen. Im Einzelnen haben wir folgende Anmerkungen:

2.1.3 Subsidiaritätsprinzip - § 7 Abs. 2, S. 2, letzter Halbsatz TMG-E

BITKOM stellt nicht in Frage, dass auch rein technische Dienstleister im Internet Pflichten im Zusammenhang mit der Unterbindung von Rechtsverletzungen treffen. Es kann also nicht darum gehen, die Inanspruchnahme von Intermediären generell auszuschließen. Jedoch ist der durch das aktuelle System bewirkte Automatismus einer primären und regelmäßig auch ausschließlichen Inanspruchnahme des Diensteanbieters sachlich nicht gerechtfertigt.

Gerade vor dem Hintergrund sich erweiternder Auskunftsansprüche der Rechteinhaber, etwa im Rahmen der mittlerweile auch in Deutschland erfolgten Umsetzung der Enforcement-Richtlinie, bedarf es daher einer gesetzlichen Richtungsentscheidung, dass der Primärverletzer prinzipiell auch primär haftet und ISP nur nachrangig in Anspruch genommen werden können. Die tatsächlichen Entwicklungen in der Praxis belegen, dass die Inanspruchnahme der eigentlichen Verletzer nicht etwa generell aussichtslos ist. Dort nämlich, wo Rechtinhaber nicht auf einen zentralen Intermediär zurückgreifen können, so insbesondere im Bereich von Urheberrechtsverletzungen in dezentralen Peer-to-Peer-Plattformen, wurde konsequent und durchaus mit Erfolg der Weg gegen die Primärverletzer beschritten.

Dies offenbart, dass die Inanspruchnahme der Service-Provider nicht der einzig gangbare, sondern häufig schlicht der bequemere Weg ist. Haftungsrechtlich darf dies aber nicht das systembestimmende Argument sein. Auch in der obergerichtliche Rechtsprechung zur Providerhaftung lassen sich entsprechende Überlegungen ausmachen. So hat das OLG Düsseldorf im Fall „aufrecht.de“[4] ausgeführt:

> *„Nach den dargestellten Grundsätzen hat der Kläger gegen die Beklagte […] jedoch keinen Anspruch auf Unterlassung […], weil ihm die Identität des Verfassers […] bekannt* ist und er diesen auf Unterlassung in Anspruch hätte nehmen können.“

Schließlich verweisen wir an dieser Stelle auch auf § 52a Abs. 2, S. 3 RfStV, der für die rundfunkrechtliche Plattformregulierung festlegt:

[4] OLG Düsseldorf, Urt. V. 26. April 2006, Az.: 1-15 U 180/05.

> *„Sind Maßnahmen gegenüber dem Verantwortlichen von Programmen und Diensten nach Satz 2 nicht durchführbar oder nicht Erfolg versprechend, können Maßnahmen zur Sperrung von Programmen und Diensten auch gegen den Plattformanbieter gerichtet werden, sofern eine Sperrung technisch möglich und zumutbar ist."*

Die im vorgelegten Entwurf vorgeschlagene Regelung in § 7 Abs. 2, S. 2, letzter Halbsatz TMG entspricht sinngemäß der im Rundfunkstaatsvertrag implementierten Norm und ist geeignet, der zu beobachtenden allgemeinen Tendenz einer vorrangigen und alleinigen Inanspruchnahme des Intermediärs zu begegnen.

Dem steht nicht entgegen, dass es sich bei der Regelung des Rundfunkstaatsvertrages um eine Regelung des öffentlichen Rechts handelt, in welchem der Subsidiaritätsgedanke übergreifend verankert ist. Zum einen gilt das TMG kraft seiner Querschnittsnatur auch für den Bereich der öffentlich-rechtlichen Verantwortlichkeit und präzisiert insoweit diesen Gedanken gerade für die öffentlich-rechtliche Inanspruchnahme von Internet-Service-Providern. Zum anderen existiert kein allgemeiner Grundsatz, der ein solches Stufenverhältnis für das Zivilrecht generell ausschließt. Auch im Zivilrecht existieren vielmehr schon heute an verschiedenen Stellen haftungsrechtliche Stufenverhältnisse. Als Beispiele mögen dienen:

- Subsidiarität der Bürgschaft gegenüber Hauptschuld (§§ 770 Abs. 2 BGB, 771 – 773 BGB)
- Subsidiäre Haftung des Vorerben gem. § 2145 BGB
- Subsidiäre Haftung des Veräußerers im Mietrecht gem. § 566a S. 2 BGB
- Subsidiäre Haftung bei Amtspflichtverletzung, § 839 S. 2 BGB

Notwendig ist aus zivilrechtlicher Perspektive für die im Rahmen der Providerverantwortlichkeit in Rede stehenden Konstellationen eine konkrete gesetzliche Anordnung, da die allgemeine zivilrechtliche Störerhaftung grundsätzlich neben die Haftung des direkt Verantwortlichen tritt. Diese gesetzliche Anordnung erfolgt mit dem unterbreiteten Vorschlag in sachgerechter Weise. Die damit verbundene Stärkung des Verursacherprinzips ist aufgrund der in der Praxis faktisch entstandenen Primär- und Alleinhaftung der ISP auch sachlich gerechtfertigt. In der Praxis hätte die vorgeschlagene Ergänzung des § 7 Abs. 2 TMG nach unserer Einschätzung in erster Linie zur Folge, dass der Verletzte jedenfalls zunächst belegbare Anstrengungen unternehmen muss, die Identität des eigentlichen Verletzers zu eruieren, um ihn ggf. im Anschluss in Anspruch nehmen zu können. Hierbei können ihm auch die zu diesem Zweck geschaffenen Auskunftsansprüche behilflich sein.

Der im Entwurf verwendete Begriff des „verantwortlichen Nutzer[s]" sollte aus Gründen der terminologischen Kohärenz durch die Formulierung „Anbieter der Informationen" ersetzt werden.

2.1.4 Beschränkung auf die konkrete Rechtsverletzung

§ 7 Abs. 3 TMG-E bewirkt eine Konkretisierung und Beschränkung der Verpflichtung des ISP auf eine konkrete Rechtsverletzung, wie sie im vollstreckbaren Titel gegen den Inhaltsanbieter beschrieben ist. Die Regelung greift damit eines der Kernprobleme der geltenden Rechtslage auf, nämlich die allgemeine Tendenz zur Etablierung proaktiver, in die Zukunft gerichteter Überwachungspflichten.

Der Bundesgerichtshof hat die Leitlinien seiner Rechtsprechung zur Störerhaftung in den neueren Urteilen Internetversteigerung II (BGH I ZR 35/04), Internetversteigerung III (BGH I ZR 73/05) sowie zur Forenhaftung (BGH VI 101/06) bestätigt. Mit der Entscheidung „Jugendgefährdende Medien bei eBay“ hat der BGH, gestützt auf eine täterschaftliche wettbewerbsrechtliche Haftung wegen Verletzung von Sorgfaltspflichten, außerdem konkrete Beispiele für die Reichweite der proaktiven Überwachungspflichten skizziert. Die Grundaussagen zur Reichweite der entsprechenden Pflichten lassen sich danach wie folgt zusammenfassen:

- Begangene oder auch nur drohende Rechtsverletzungen begründen eine Prüfungspflicht des Providers.

- Der Provider ist in der Folge nicht nur verpflichtet das konkrete Angebot zu sperren, sondern muss Vorsorge treffen, dass es nicht zu vergleichbaren Verletzungen (etwa Verletzungen der gleichen Marke) kommt. In diesem Zusammenhang führt der BGH den Einsatz von Filtersoftware an, die entsprechende Verdachtsfälle aufdecken könne. Bezogen auf die Verbreitung jugendgefährdender Medien soll dies nach der Entscheidung des Bundesgerichtshofs vom Juli 2007 konkret eine proaktive Prüfungspflicht auf personaler wie sachlicher Ebene bedeuten:

  - Angebot des konkreten Mediums durch andere Anbieter (sachliche Ebene).
  - Angebote desselben Versteigerers innerhalb derselben jugendgefährdenden Kategorie (personal-sachliche Ebene).

- Die Grenze ist nach dem BGH erst dort erreicht, wo entsprechende Pflichten das gesamte Geschäftsmodell in Frage stellen oder wo es keine Merkmale gibt, die als Anknüpfungspunkt für eine (technische) Filterung geeignet sind.

Die Kernproblematik der bestehenden Rechtsprechungspraxis liegt im zweiten Element begründet. Indem der jeweilige Provider hiernach gehalten ist, auch sämtliche vergleichbare Verletzungen zu verhindern, ist er in der Praxis faktisch verpflichtet, sein *gesamtes* Angebot *für immer* proaktiv auf entsprechende Verletzungen durch Drittinhalte zu durchforsten. Unklar ist in diesem Zusammenhang, was im Einzelfall unter wesensgleichen Verstößen zu verstehen ist, ab wann beim Provider von einer Kenntnis einer Rechtsverletzung ausgegangen

und was ihm an Maßnahmen zur Vermeidung wesensgleicher Verletzungen zugemutet werden kann.

Die eigentlich als Unterlassungspflicht konzipierte Pflicht wandelt sich im Übrigen durch die Auslegung des BGH faktisch in eine aktive Rechtsverletzungs-Verhinderungspflicht. Durch die gleichwohl gewählte rechtliche Konstruktion der Überwachungspflichten über den Unterlassungsanspruch werden im Urteilstenor regelmäßig nicht die genauen Grenzen der Überwachung bestimmt. Unterlassungsansprüche sind ihrer Natur nach zunächst absolut und werden nur begrenzt durch das technisch Mögliche und wirtschaftlich Zumutbare.

In aller Regel - das Urteil zu jugendgefährdenden Medien bildet insoweit eine gewisse Ausnahme - fehlt den Entscheidungen dabei eine genauere Vorgabe, welche Maßnahmen der Diensteanbieter zu ergreifen hat, so dass die Frage, ob hinreichende Monitoring-Maßnahmen eingeleitet wurden, der Beurteilung im Einzelfall im Vollstreckungsverfahren überlassen bleibt. Dies bedeutet nicht nur eine Überlastung der Vollstreckungsgerichte (in deren Verfahren die notwendigen Ermittlungen kaum zu leisten sind), sondern verlängert auch die Rechtsunsicherheit für die Diensteanbieter.

Das generelle Ausklammern von Unterlassungsansprüchen von der Privilegierung unterläuft die Wertung und die Zielsetzung der §§ 7 bis 10 TMG, wie auch die Vorgaben der Artikel 12 bis 15 der E-Commerce-Richtlinie. Auch die einschränkenden Regelungen in den Art. 12 Absatz 3, 13 Absatz 2 und 14 Absatz 3 der Richtlinie erlauben nur eine Anordnung, im Einzelfall eine Rechtsverletzung abzustellen oder zu verhindern. In diesem Sinne muss auch der Wortlaut des § 7 Abs. 2, S. 2 TMG verstanden werden.

Eine unbegrenzt in die Zukunft gerichtete Pflicht zur allgemeinen Überprüfung im Hinblick auf wesensgleiche Rechtsverletzungen ist damit von den europäischen Vorgaben nicht erfasst und auch in § 7 Abs. 2, S. 2 TMG nicht vorgesehen. Aufgrund des zwischen § 7 Abs. 2, S. 2 und § 7 Abs. 2, S. 1 TMG bestehenden Regel-Ausnahme-Verhältnisses ist Satz 2 unter Anwendung der allgemein anerkannten Grundsätze der Gesetzesauslegung restriktiv anzuwenden.

Die mit § 7 Abs. 3 TMG-E vorgeschlagene Regelung kann die beschriebenen Problemlagen allerdings aus unserer Sicht nur begrenzt auflösen. Die Novellierung des TMG sollte in allererster Linie eine Rückführung der Verantwortlichkeit auf das von der E-Commerce-Richtlinie vorgesehene Maß ins Auge fassen. Dies kann dadurch geschehen, dass die Formulierung des TMG entsprechend der Vorgabe der E-Commerce Richtlinie dahingehend angepasst wird, dass Anknüpfungspunkt der Überwachungs- bzw. Prüfungspflicht die konkret erfolgte Rechtsverletzung ist und eine Entfernungs- bzw. Sperrungsverpflichtung nur auf konkrete Anordnung im Einzelfall erfolgen kann. § 7 Abs. 2, S. 2 TMG wäre daher insgesamt, unter weiterer Berücksichtigung des Subsidiaritätsgedankens, wie folgt auszugestalten:

> *„Auf Grundlage allgemeiner Gesetze ergangene gerichtliche oder verwaltungsbehördliche Anordnungen dahingehend, eine begangene Rechtverletzung abzustellen, bleiben auch im Falle der Nichtverantwortlichkeit des Diensteanbieters nach den §§ 8 – 10 [a] unberührt, wenn sich Maßnahmen gegenüber dem Anbieter der Informationen als nicht durchführbar oder Erfolg versprechend erweisen und die Abstellung der Rechtsverletzung technisch möglich und zumutbar ist.“*

2.1.5 Rechtsvorschriften zu Sorgfaltspflichten, § 7 Abs. 4, S. 1 TMG-E

§ 7 Abs. 4, S. 1 TMG-E legt fest, dass Rechtvorschriften, welche ISP nach pflichtgemäßen Ermessen Sorgfaltspflichten auferlegen, um bestimmte Arten von Rechtsverletzungen aufzudecken oder zu verhindern, unberührt bleiben.

Zu dieser Vorschrift besteht aus Sicht des BITKOM noch Diskussionsbedarf. Die aus der E-Commerce-Richtlinie folgende Nichterfassung von konkreten Entfernungs- oder Sperrungspflichten nach den allgemeinen Gesetzen ist über die Generalklausel des § 7 Abs. 2 TMG hinreichend umgesetzt. Soweit § 7 Abs. 4, S. 1 TMG-E einen darüber hinaus gehenden Anwendungsbereich hat, müsste dies noch präzisiert werden. Die Begründung verweist hierzu allgemein auf Konstellationen, in welchen Dienstanbietern durch Rechtsverletzungen Dritter Vorteile entstehen. Hier wäre zu erläutern, welche Fallgestaltungen konkret gemeint sind. Wir sehen für eine solche Klarstellung nach den praktischen Erfahrungen aktuell keinen Bedarf. Aus Sicht des BITKOM ist § 7 Abs. 4, S. 1 TMG-E daher entbehrlich.

Zu betonen ist insbesondere, dass § 7 Abs. 4 TMG-E keinesfalls dahingehend verstanden werden darf, dass Diensteanbieter über die durch § 7 Abs. 2 TMG unberührt gelassenen konkreten Entfernungs- oder Sperrungspflichten hinaus allgemeine Sorgfaltspflichten in Form von Überwachungs- oder Prüfpflichten auf Basis allgemeiner Gesetze treffen können. Solche Pflichten ließen sich nicht mit dem aus der E-Commerce-Richtlinie folgenden Verbot allgemeiner Überwachungspflichten in Einklang bringen.

Hinsichtlich der vorgesehenen Informationspflicht nach § 7 Abs. 4, S. 2 TMG-E geben wir zu bedenken, dass diese im Falle freiwillig installierter Systeme in der Praxis zu einer kaum zu bearbeitenden Vielzahl von Meldungen gegenüber Strafverfolgungsbehörden führen würde.

Soweit die Begründung zu § 7 Abs. 4 TMG-E ausführt, es bestehe ein gesetzliches Interesse daran, dass Dienstanbieter selbst an der Bekämpfung von Verletzungen mitwirken, teilen wir diese Ansicht. Die sachgerechte gesetzliche Regelung für ein solches Anreizprinzip erblicken wir allerdings eher in der Etablierung eines Privilegierungs-Ansatzes, der freiwillige Maßnahmen durch weitereichende Haftungsprivilegien fördert. Wir verweisen hierzu auf unsere Ausführungen zu Punkt 3.

2.1.6 Verteilung der Darlegungs- und Beweislast - §§ 7 Abs. 2, S. 2, letzter Halbsatz, Abs. 4, S. 3 TMG-E

Eng verbunden mit der Frage der Zumutbarkeit von Prüfungs- bzw. Sorgfaltspflichten ist die Frage der Darlegungs- und Beweislast. Nachdem die Frage der Zumutbarkeit als solche eine Wertungsfrage ist, konkretisiert sich die Problematik der Beweislast auf den Aspekt der denkbaren Maßnahmen des Providers.

Die Internetversteigerung-II-Entscheidung des BGH mag hier zur Verdeutlichung als Beispiel dienen. Die dort erstmals niedergelegte Einschränkung, wonach Prüfungspflichten nur zumutbar sind, soweit ein geeignetes Anknüpfungsmerkmal für Prüfungsvorgänge besteht, leitet über zur Frage, wem im Streitfall die Darlegung obliegt, dass solche Merkmale existieren bzw. nicht existieren. Nach allgemeinen Grundsätzen der Störerhaftung bildet die Unzumutbarkeit einen Einwand des Beklagten, für den dieser folglich darlegungs- und beweispflichtig ist.[5] Ist der Provider danach gehalten, die Unzumutbarkeit einer Prüfungspflicht zu belegen, müsste er letztendlich die technische Unmöglichkeit und damit eine negative Tatsache beweisen.

Die Führung eines solchen Negativ-Beweises ist dem Internet-Service-Provider aber naturgemäß kaum möglich. Der Bundesgerichtshof hat die Problematik der Darlegungs- und Beweislast auch in den jüngeren Entscheidungen nicht angesprochen, jedoch klingt in obergerichtlichen Urteilen die beschriebene Rechtsauffassung an.[6]

BITKOM hat sich schon 2007 dafür ausgesprochen, die primäre Darlegungslast für die technische Realisierung von Prüfpflichten dem jeweiligen Antragsteller aufzuerlegen. Dieser müsste danach konkrete Maßnahmen benennen, die der Provider ergreifen soll, so dass dem Provider nur die sekundäre Darlegungslast bezüglich der Umsetzbarkeit und des Aufwandes für die konkret vom Rechteinhaber vorgeschlagene Maßnahme zukäme.

Der vorgelegte Gesetzentwurf greift diesen Vorschlag in §§ 7 Abs. 2, S. 2, letzter Halbsatz, Abs. 4, S. 3 TMG-E auf. Wir begrüßen diesen Ansatz, da er dazu beiträgt, dem betroffenen ISP einen konkreten Anknüpfungspunkt für die Bewertung etwaiger technischer Maßnahmen zu bieten. Verhindert wird damit vor allem eine faktische Verpflichtung zur Führung eines allgemeinen Negativ-Beweises. Aus systematischen Gründen sollte die Formulierung des § 7 Abs. 4, S. 3 TMG-E allerdings in § 7 Abs. 2 TMG-E integriert werden.

---

[5] Vgl. etwa BGH I ZR 129/94, Urteil v. 10.10.1996 – Architektenwettbewerb: „Dem als Störer Inanspruchgenommenen muß daher ausnahmsweise der Einwand offenstehen, daß ihm im konkreten Fall eine Prüfungspflicht - etwa weil der Störungszustand für ihn nicht ohne weiteres erkennbar war - entweder überhaupt nicht oder jedenfalls nur eingeschränkt zuzumuten sei."

[6] Vgl. OLG Hamburg, 5 U 78/05 , Urt. v. 8. 2. 2006 – Cybersky: „Erst dann, wenn der Antragsgegner zweifelsfrei nachweist, dass ihm ein Herausfiltern der von der Antragstellerin herrührenden Programmsignale technisch unmöglich ist und er alle auch nur denkbaren (zumutbaren) Bemühungen erfolglos unternommen hat, die Antragstellerin dazu zu veranlassen, ihm die Möglichkeit zugeben, die rechtswidrige Übertragung ihres Programmangebotes mittels der Software "Cybersky" zu unterbinden, könnte eine Situation gegeben sein, in der das dem Antragsgegner auferlegte Verbot einer weiteren Überprüfung unter Verhältnismäßigkeitsgesichtspunkten bedürfte."

2.1.7 Konkretisierung des Pflichtenprogramms, §§ 7 Abs. 2, S. 2, letzter Halbsatz TMG-E

Die mit § 7 Abs. 2 S. 2, letzter Halbsatz vorgesehene (Wieder-[7])Aufnahme der Kriterien der technischen Möglichkeit und Zumutbarkeit trägt außerdem dazu bei, das sich aus den allgemeinen Verkehrspflichten ergebende Pflichtenprogramm für den betroffenen ISP zu konkretisieren und handhabbar zu machen. Indem § 7 Abs. 2 TMG-E die technische Möglichkeit und Zumutbarkeit zur Haftungsvoraussetzung macht, sind Gerichte bereits im Hauptsacheverfahren bzw. Verfahren des vorläufigen Rechtsschutzes angehalten, dies zu konkretisieren. Auf diese Weise hat die vorgeschlagene Formulierung über die Verteilung der Darlegungs- und Beweislast hinaus vor allem die – richtige – Wirkung, die heute in der Praxis faktisch erst im Vollstreckungsverfahren stattfindende Konkretisierung des Pflichtenprogramms wieder dem gerichtlichen Verfahren zu unterwerfen.

2.2 Einbeziehung von Hyperlinks und Suchmaschinen

BITKOM hat schon in 2007 auf die dringende Notwendigkeit hingewiesen, im Rahmen der Novellierung des TMG die bislang ungeregelte Behandlung von Hyperlinks und Suchmaschinen zu präzisieren. Dies muss mit Blick auf die auch in diesem Sektor problematische Entwicklung der Rechtsprechung geschehen, die sich in der jüngsten Entscheidung zur Bildersuche weiter akzentuiert. Sowohl Hyperlinks als auch Suchmaschinen lassen Parallelen zu den von §§ 8 bis 10 TMG heute erfassten Diensten erkennen. Es handelt sich um Kerninstrumente des Internets, deren Bereitstellung dessen sinnvolle Nutzung überhaupt erst ermöglicht und damit dem „Allgemeininteresse an der Funktionsfähigkeit des Internets“[8] entspricht. Der Bundesgerichtshof hat dies in der Paperboy-Entscheidung wie folgt auf den Punkt gebracht:

> *„Ohne die Inanspruchnahme von Suchdiensten und deren Einsatz von Hyperlinks (gerade in der Form von Deep-Links) wäre die sinnvolle Nutzung der unübersehbaren Informationsfülle im World Wide Web praktisch ausgeschlossen.“*

Vor diesem Hintergrund ist es rechtspolitisch überfällig, bestehende Rechtsunsicherheiten für die Anbieter endlich durch eine klare haftungsrechtliche Einordnung zu beseitigen.

2.2.1 Bestehende Rechtslage in Deutschland

Die fehlende Integration von Hyperlinks- und Suchmaschinen in das Verantwortlichkeitsschema führt zu einer massiven Rechtsunsicherheit bei der Beurteilung dieser Dienste. Mit dem „Schöner-Wetten“-Urteil hat der Bundesgerichtshof klargestellt, dass Hyperlinks nicht unter die Begrenzungsnormen des TMG fallen. Die Rechtsprechung hat diese Feststellung in mittlerweile mehreren Urteilen auch für Suchmaschinen bestätigt. Zwar unterliegt sowohl die Beurtei-

[7] Eine entsprechende Formulierung war bereits Gegenstand der Ausgangsfassung des Teledienstegesetzes aus dem Jahre 1997 (§ 5 Abs. 2 TDG 1997).
[8] BGH, Urteil v. 17.07.2003, I ZR 259/00 - Paperboy.

lung von Hyperlinks als auch die haftungsrechtliche Einordnung von Suchmaschinen zumindest noch den Grenzen mittelbarer Haftung nach allgemeinem Recht, wie sie auch für die Störerhaftung der in §§ 8 bis 10 TMG aufgeführten Dienste Anwendung finden.

Jedoch fehlt es durch die Nichterwähnung in den Begrenzungstatbeständen des TMG zum einen an der dadurch vermittelten Indizwirkung. Vor allem aber gilt nach der geltenden Rechtslage für beide Instrumente insbesondere nicht das in § 7 Abs. 2, S. 1 TMG niedergelegte Verbot allgemeiner Überwachungspflichten. Damit ist eines der fundamentalen Prinzipien der Providerhaftung nicht auf Hyperlinks und Suchmaschinen anwendbar ist. Insoweit verschärft sich für Links und Suchmaschinen die durch die oben dargestellte BGH-Rechtsprechung zur allgemeinen Störerhaftung faktisch begründete Überwachungspflicht bzgl. zukünftiger Rechtsverletzungen. Insbesondere in der instanzgerichtlichen Rechtsprechung zu Suchmaschinen lassen sich heute teilweise Entwicklungen ausmachen, die letztendlich auf ein in der Praxis nicht zu realisierendes inhaltliches Monitoring der Inhalte hinauslaufen. Die fehlende Einbeziehung in das Verantwortlichkeitsschema nach §§ 8 - 10 TMG setzt Hyperlink-Setzer und Suchmaschinenbetreiber schließlich potentiell einer Schadensersatzhaftung oder gar strafrechtlichen Verantwortlichkeit aus.

2.2.2 Die Situation der Anbieter

Sowohl Suchmaschinenbetreiber als auch Linksetzer sehen sich heute nahezu unüberwindbaren Problemen bei der Beurteilung der von ihnen indirekt vermittelten Inhalte ausgesetzt. Bereits bei der manuellen Integration eines einzelnen Hyperlinks in eine klassische html-Webseite kann der Linksetzer keine dauerhafte Gewähr für den adressierten Drittinhalt übernehmen, da dieser sich permanent und unabhängig von der Verlinkung ändern kann. Wollte man den Hyperlinksetzer umfassend auch für die in Bezug genommen Inhalte verantwortlich machen, ergäbe sich daher eine permanente Monitoring-Pflicht, der niemand nachkommen könnte. Die Sachlage potenziert sich entsprechend für automatisierte Linksammlungen, redaktionell betreute Linklisten und Web-Kataloge.

Echte Suchmaschinen schließlich können schon im Ausgangspunkt der Erfassung von Drittinhalten keine Inhaltsüberprüfung leisten, da diese Erfassung automatisiert über sog. Robots bzw. Crawler geschieht, die keinerlei semantische und schon gar keine rechtliche Prüfung der Zielinhalte zu leisten imstande sind.

2.2.3 Einordnung von Suchmaschinen, § 8a TMG-E

Neben der Tatsache, dass bei vollautomatischen Suchmaschinen keine inhaltliche Auswahl stattfindet, ist bei der Einordnung von Suchmaschinen in das Verantwortlichkeitsschema des TMG aus technischer Sicht insbesondere zu berücksichtigen, dass Suchmaschinen keine Speicherung fremder Inhalte vornehmen.

Der vorgeschlagene § 8a TMG-E bildet daher aus unserer Sicht eine sachgerechte Regelung in Anlehnung an die für Zugangsdienstleister geltende Regelung. Wir schlagen allerdings vor, die Formulierung „abgefragte Informationen" zu ersetzen durch den Terminus „fremde Informationen", um die Kohärenz mit den übrigen Regelungen der §§ 8 ff. TMG sicherzustellen.

2.2.4 Einordnung von Hyperlinks, § 10a TMG-E

Beim Einsatz von Hyperlinks findet – nimmt man die automatisierte Generierung bei der Ergebnisanzeige von Suchmaschinen aus – eine inhaltliche Auswahl zu den verwiesenen Seiten statt. Andererseits hat der Linksetzer über die in Bezug genommenen Informationen regelmäßig nur eine stark eingeschränkte inhaltliche Kontrolle, besonders wenn die verlinkte Seite ihrerseits auf eine Vielzahl von anderen Informationen verweist. Hier können Hunderte und Tausende von Unterseiten zu verschiedenen Themen bestehen, die wiederum jederzeit verändert werden können. Insofern besteht eher eine Parallele zur Situation des Hostproviders. Dies hat auch der Österreichische Gesetzgeber erkannt, der mit § 17 des Österreichischen E-Commerce-Gesetzes die Verantwortlichkeit für das Setzen von Links derjenigen eines Hostproviders gleichsetzt.

Die vorgeschlagene Regelung der Haftungsbegrenzung für Hyperlinksetzer in §10a TMG-E trägt diesen Erwägungen aus unserer Sicht sachgerecht Rechnung und passt die Haftungssituation für Hyperlinkanbieter der der Hostprovider an.

In redaktioneller Hinsicht ist zu überlegen, die Integration von Hyperlinkanbietern direkt im Rahmen von § 10 TMG umzusetzen.

2.3 § 3a TMG-E – sachliche Zuständigkeit

§ 3a TMG-E sieht eine Ermächtigung für die Landesregierungen vor, durch Rechtsverordnung für Bezirke mehrerer Amtsgerichte eines von diesen als Gericht für Telemedienstreitsachen zu bestimmen. Hiermit würde - auf Ebene der Amtsgerichte - die Möglichkeit eröffnet, eine gewisse Kanalisierungswirkung und Scherpunktbildung für Telemedien-Streitsachen zu generieren.

Die Regelung zielt somit darauf ab, die durch die deutsche Rechtslage ermöglichte Situation des sog. Forum Shoppings, also der Tatsache, dass bei Rechtsverletzungen im Internet faktisch Ansprüche in örtlicher Hinsicht bei jedem sachlich zuständigen Gericht geltend gemacht werden können, einzuschränken.

BITKOM hält es insgesamt für sinnvoll, die Möglichkeiten des bundesweiten Forum Shoppings einzuschränken und gleichzeitig die Bildung von Schwerpunktgerichten bzw. Schwerpunktkammern zuzulassen, etwa nach dem Vorbild der Kammern für Marken- oder Handelsrecht.

Die vorgeschlagene Regelung löst diese Probleme allerdings nur begrenzt. Zwar ermöglicht § 3a TMG-E eine Schwerpunktbildung auf Ebene der Amtsgerichte. Sinnvoll erscheint allerdings auch die Schaffung entsprechender Spezialkammern bei den Landgerichten, da die Eingangsstreitwerte in immaterialgüterrech-

tlichen und wettbewerbsrechtlichen Fragestellungen in der Regel zur Zuständigkeit der Landgerichte führen, so dass eine bloße Kanalisierungswirkung bei den Amtsgerichten gerade in diesen kritischen Verfahren leer liefe.

Im Übrigen löst die Regelung nicht das grundsätzliche Problem der Möglichkeit eines bundesweiten Forum Shoppings. Dem jeweiligen Antragsteller bzw. Kläger bliebe es nach der vorgeschlagenen Regelung weiterhin unbenommen, das Verfahren in einen Bezirk seiner Wahl anhängig zu machen. Die Möglichkeit des Forum Shoppings wäre daher erst auf der 2. Ebene der lokalen Auswahl des konkret zuständigen Gerichts innerhalb dieser Bezirke beschränkt.

2.4 Datenschutzvorschriften, §§ 5 Abs. 1, Nr. 8, 13 Abs. 1, Nr. 1, § 13. Abs. 8 TMG-E

BITKOM befürwortet und unterstützt die hinter den datenschutzrechtlichen Regelungen des Gesetzentwurfs stehende Absicht zur Steigerung der Transparenz.

2.4.1 Kontaktdaten des Datenschutzbeauftragten, § 5 Abs. 1 Nr. 8 TMG-E

Eine Pflicht zur Benennung des Datenschutzbeauftragten im Impressum wäre nicht im Sinne des Datenschutzes. Ausgangspunkt der datenschutzrechtlichen Verpflichtungen und auch Anknüpfungspunkt für die Rechte des Betroffenen ist nicht der betriebliche Datenschutzbeauftragte, sondern die "verantwortliche Stelle" (§ 3 Abs. 4, Nr. 7 BDSG), also das datenverarbeitende Unternehmen. Die Kontaktaufnahme mit der verantwortlichen Stelle wird jedoch schon im Rahmen der bestehenden Impressumspflichten ermöglicht. In der Praxis trägt die verantwortliche Stelle Sorge dafür, dass eine den Datenschutz betreffende an den richtigen Bearbeiter in der Organisation gelangt. Das muss nicht immer der Datenschutzbeauftragte sein. Der Datenschutzbeauftragte hat vielmehr eine beratende und kontrollierende Funktion innerhalb der verantwortlichen Stelle. Dem Kunden, der sich direkt an den betrieblichen Datenschutzbeauftragten wendet, würde also ein Ansprechpartner gegeben, der dem Anliegen häufig nicht Rechnung tragen kann.

In diesem Zusammenhang möchten wir auch zu bedenken geben, dass nach den Erfahrungen in der Praxis Kunden mit Anliegen völlig anderer als datenschutzrechtlicher Natur an den Datenschutzbeauftragten herantreten würden, z.B. mit konkreten Serviceanfragen, um auf diese Weise die Inanspruchnahme der hierfür bereitgestellten Hotlines zu umgehen. Der Arbeit der Datenschutzbeauftragten wäre dies abträglich.

Nicht zuletzt sind auch die Konstellationen häufig, in denen der Betreiber einer Website diese nur zu Präsentationszwecken bereithält (z.B. Website eines Autobauers) und sich der Datenschutzbeauftragte schwerpunktmäßig mit dem Arbeitnehmerdatenschutz bzgl. der verantwortlichen Stelle (Autobauer) beschäftigt. Auch in diesen Fällen wäre dem Kunden mit der Kontaktaufnahme zum betrieblichen Datenschutzbeauftragten nicht gedient.

2.4.2 Informationspflichten, § 13 Abs. 1 Nr. 1 TMG-E

Die im Entwurf geregelten Informationspflichten sind schon jetzt übliche Praxis und im Übrigen weitgehend durch das TMG geregelt, so dass wir eine Notwendigkeit für eine entsprechende gesetzliche Neuregelung im Rahmen des TMG aktuell nicht sehen. Insbesondere die in § 13 Abs. 1 TMG-E geregelten Pflichten entsprechen weitgehend der bereits geltenden Vorschrift des § 13 Abs. 1 TMG. Soweit § 13 Abs. 1 TMG-E auch auf die Dauer der Speicherung rekurriert, geben wir zu bedenken, dass eine Information hierüber schwierig ist, da die Dauer der Speicherung in der Praxis von verschiedenen Faktoren abhängig ist, die zu Beginn des Nutzungsvorgangs teilweise nicht absehbar sind.

So bestehen z.B. insbesondere durch die steuer- und handelsrechtlichen Speicherpflichten sowie durch die Vorratsdatenspeicherung Regelungen, die zum Teil Daten innerhalb eines einzelnen Kundendatensatzes unterschiedlichen Speicherfristen unterliegen lassen. So ist zwar grundsätzlich der Adressdatensatz eines Kunden nach Beendigung eines Vertragsverhältnisses zu löschen. Geschäftsbriefe mit ihm (und dazu gehören z.B. bei der Bestellung von Produkten ausgetauschte Nachrichten und Rechnungen) sind aber bis zu zehn Jahre aufzubewahren, jedoch für den normalen Datenzugriff zu sperren. Verbindungsdaten von Kommunikationsdiensten sind nach Vorratsdatenspeicherung zu speichern. Es ist in der Praxis nahezu unmöglich, diese verschiedenen Bedingungen in einer Datenschutzmitteilung differenziert und sachlich zutreffend darzustellen, womit die entsprechende Pflicht zu einer Abmahnfalle zu werden droht, wie es teilweise von den telemedienrechtlichen Informationspflichten bzw. der Widerrufsbelehrung im Fernabsatz bekannt ist.

Wir halten die vorgeschlagene Überarbeitung des § 13 Abs. 1 TMG-E daher für entbehrlich.

2.4.3 Daten auf dem Endgerät des Nutzers, § 13 Abs. 8 TMG-E

Mit § 13 Abs. 8 TMG-E wird eine Informationspflicht zu auf dem Endgerät des Nutzers gespeicherten Daten vorgeschlagen. Eine Einschränkung auf personenbezogene Daten wird dabei nicht vorgenommen. Es werden somit Informationspflichten und Widerspruchsrechte für Daten konstituiert, die nicht in den Anwendungsbereich des Datenschutzrechts fallen.

Sofern § 13 Abs. 8 TMG-E auf sog. Cookies zugeschnitten sein soll, wird dies nicht deutlich. Denn es werden hier sämtliche Daten erfasst, die im Endgerät des Nutzers gespeichert werden, also z.B. auch der Quellcode der Webseite, die der Nutzer betrachtet, temporäre Dateien die den Aufbau einer Webseite beschleunigen, vom Nutzer heruntergeladene Dateien etc. Eine abschließende Unterrichtung über alle Daten die der Nutzer durch Zugriff auf sein Endgerät herunterlädt, ist nicht möglich und auch nicht sinnvoll.

Es ist auch nicht erkennbar, wie die Umsetzung des hier vorgeschlagenen Widerspruches erfolgen soll. Ein Nutzer, der gegenüber einem Webseitenbetreiber einen Widerspruch gegen die Speicherung bestimmter Daten auf seinem

Endgerät erklärt, müsste sich gegenüber dem Betreiber bei jeder Nutzung authentifizieren, damit der Betreiber jeden Widerspruch individuell berücksichtigen kann. Dies widerspricht dem Gebot der anonymen bzw. pseudonymen Nutzbarkeit nach § 13 Abs. 6 TMG.

Die Ausnahme vom Widerspruchsrecht nach § 13 Abs. 8, S. 2 TMG-E ist zudem unzureichend. Die Speicherung von Daten auf einem Endgerät bei dem Zugriff auf ein Telemedium ist so vielgestaltig, dass mit der hier vorgeschlagenen Formulierung erhebliche Rechtsunsicherheit für die Diensteanbieter verbunden wäre, zumal übliche und notwendige Fälle wie temporäre Dateien nicht erfasst würden.

Auch wenn man § 13 Abs. 8 TMG-E nur auf Cookies beschränken würde, liegt darin keine sinnvolle Regelung, denn zur Verwendbarkeit ggf. pseudonymer Cookie-Daten gibt es mit § 15 Abs. 3 TMG bereits Vorschrift, die eine Widerspruchsmöglichkeit vorsieht und die durch § 13 Abs. 8 TMG-E konterkariert würde.

Außerdem ist die Information über die Verwendung von Cookies bereits jetzt übliche Praxis und entsprechende Informationspflichten sind auch Voraussetzung zur Erteilung von Prüfzertifikaten durch Zertifizierungsunternehmen (z.B. TÜV Süd), von denen die namhaften Unternehmen weitestgehend Gebrauch machen. Aus diesen Gründen hält BITKOM eine gesetzliche Regelung zur Informationspflicht sog. Cookies für nicht erforderlich.

Das fehlende Erfordernis einer gesetzlichen Regelung ergibt sich auch daraus, dass jeder Nutzer bereits jetzt über individuelle Browsereinstellungen differenzierte Möglichkeiten hat, die Nutzung von Cookies einzuschränken bzw. zuzulassen. Dieser technische Mechanismus ist aus Nutzersicht wesentlich praktikabler als eine gesetzliche Informationspflicht des Dienstanbieters in Verbindung mit einem Widerspruchsrecht. Vor diesem Hintergrund halten wir die vorgeschlagene Informationspflicht, die zu einer permanenten Einzelabfrage der Cookie-Verwendung führen würde, auch aus Akzeptanzgesichtspunkten nicht für tragfähig.

Schließlich geben wir zu bedenken, dass im Rahmen der laufenden Novelle des europäischen Telekommunikationsrechtsrahmens hierzu Regelungen zu erwarten sind, weshalb in jedem Fall zunächst der europarechtliche Umsetzungsbefehl abgewartet werden sollte.

3 Weitergehende Initiativen, insbesondere Notice-and-Takedown-Verfahren

Der vorgelegte Gesetzentwurf geht in seiner Begründung auf weitere denkbare Handlungsoptionen ein, die im Rahmen einer Novellierung des Telemediengesetzes mittelfristig zu prüfen wären. Im Hinblick auf das Verantwortlichkeitsregime des TMG wird konkret die Anwendung von Notice-and-Takedown-Verfahren angesprochen. BITKOM bittet nachdrücklich darum, diese Überlegungen weiter

zu verfolgen, da Notice-and-Takedown-Verfahren im Zusammenspiel mit gesetzlichen Regelungen geeignet sind, eines der Grundprobleme des geltenden Rechtsrahmens, die fehlende Anreizfunktion des Haftungsrechts, zumindest teilweise zu lösen. Im Einzelnen:

3.1 Problemlage

Bei der Bewertung des Haftungsregimes und zusätzlicher Überwachungspflichten ist zu berücksichtigen, dass schon heute zahlreiche Diensteanbieter, wie z.B. Anbieter von Handelsplattformen, Communities oder Foren auf freiwilliger Basis Maßnahmen zur Verhinderung von Rechtsverletzungen ergreifen. Hierbei wird teils softwaregestützt versucht, Rechtsverletzungen aufzuspüren, teils werden spezielle Meldemechanismen bereitgestellt, die eine unkomplizierte Benachrichtigung über Rechtsverletzungen und eine unverzügliche Beseitigung der inkriminierten Inhalte sicherstellen.

Jedoch haben solche, rein vertraglich basierten Verfahren naturgemäß den Nachteil, gesetzliche Haftungsrisiken nicht ausschalten zu können, womit der Provider letztlich auf die Kooperationsbereitschaft im Einzelfall angewiesen ist. Entsprechende freiwillige Maßnahmen werden insoweit nach der bestehenden Gesetzeslage für den Anbieter nicht honoriert, sondern sie könnten ihm sogar zum Nachteil gereichen, da mit der Meldung einer Verletzung beim Provider Kenntnis angenommen werden könnte, die noch strengere Haftungsmaßstäbe nach sich zöge. Werden schädliche Inhalte nämlich fälschlicherweise in den freiwilligen Kontrollen nicht als solche identifiziert, könnte dem Provider die Kenntnis des Inhalts haftungsverschärfend angerechnet werden. Aus Sicht des Providers wäre es dann besser gewesen, auf die freiwilligen Anstrengungen zu verzichten. Das geltende Recht leidet insofern unter einem bereits hinlänglich benannten Strukturproblem, weil es eine „Vogel-Strauß-Mentalität“ belohnt und eigene Initiativen der Anbieter eher bestraft.

3.2 Notice & Takedown als Anreizmodell

Eine denkbare Lösung für die beschriebene Anreizproblematik könnte in der Einbeziehung eines Notice- and Takedown-Prinzips (NTD) für Host-Provider in das gesetzliche Haftungssystem liegen. Hierbei muss sichergestellt werden, dass die Etablierung eines NTD nicht das heute bereits bestehende austarierte Haftungsregime für Provider unterläuft, sondern dies präzisiert und ergänzt. Die „Einbeziehung in das gesetzliche Haftungssystem“ meint aus diesem Grund insbesondere nicht ein gesetzlich vorgeschriebenes, allgemein verpflichtendes Verfahren.

Vielmehr sollte die Etablierung eines bestimmten Anforderungen genügenden Verfahrens zu einer umfassenden haftungsrechtlichen Entlastung des Host-Providers führen. Kern der gesetzlichen Regelung wäre somit eine über das heutige Maß hinausgehende und insbesondere auch vollständig die Störerhaftung (bzw. die täterschaftliche wettbewerbsrechtliche Haftung im Zusammenhang mit vorsätzlichen Verletzungshandlungen Dritter) einbeziehende Haftungsfreistellung bei freiwilliger Bereitstellung eines bestimmten Voraussetzungen

unterliegenden Melde- und Entfernungsverfahrens. Das Ziel eines solchen Verfahrens sollte eine Verminderung der Inanspruchnahme der Gerichte und eine konsequente Konzentration des Haftungsrechts auf die originär Beteiligten, nämlich den Verletzer und den Verletzten sein. Wir folgen insoweit den Ausführungen in der Begründung des vorgelegten Gesetzentwurfs und weisen darüber hinaus darauf hin, dass entsprechende Verfahren auch für den im Einzelfall Verletzten den Vorteil einer schnellen Beseitigung der Rechtsverletzung bieten.

3.2.1 Ausgestaltung

Wie auch beim Verfahren des amerikanischen Digital Millennium Copyright Act (DMCA) sollte ein Notice-and-Takedown-Verfahren keine allgemeine gesetzliche Verpflichtung bilden, sondern in erster Linie eine Anreizfunktion für Provider ausüben. Sec 512 U.S. Copyright Act basiert im Ausgangspunkt auf diesem zentralen Grundgedanken: Den Rechtsinhabern ging es darum, Providern einen Anreiz zu geben, rechtsverletzendes Material schnell zu entfernen, während die Rechtsinhaber darauf bedacht waren, aufwändige und kostenintensive Gerichtsverfahren in jedem Einzelfall zu vermeiden.

Ein solches Meldeverfahren müsste daher als zentrales Element bestimmen, dass der Provider, der unter bestimmten formellen Voraussetzungen tätig wird (also Inhalte entfernt), in jedem Fall von einer weitergehenden Haftung frei ist. Voraussetzung für ein solches Einschreiten des Providers sollte zumindest eine schriftliche Versicherung des sich berühmenden Rechteinhabers hinsichtlich seiner Rechtsinhaberschaft, einer eventuellen Vertretungsbefugnis und hinsichtlich der behaupteten Rechtsverletzung sein. Diese schriftliche Versicherung muss das angeblich geschützte Werk/Produkt, den angeblich verletzenden Inhalt sowie einen Ansprechpartner bei dem sich berühmenden Rechteinhaber präzise benennen. Dies könnte es dem Provider ermöglichen, einzuschreiten und so eine Haftung für sich auszuschließen.

Entscheidend in diesem Zusammenhang sind folgende Aspekte: Der Provider ist im Rahmen der Anwendung des Verfahrens nicht verpflichtet, eine materielle Prüfung der Beanstandung vorzunehmen. Er muss also insbesondere nicht die Berechtigung des Antragstellers sowie das Vorliegen einer Rechtsverletzung positiv feststellen, um in den Genuss der Haftungsfreistellung zu gelangen. Daraus leitet sich gleichzeitig ab, dass die Haftungsfreistellung umfassend in beide Richtungen wirkt, also sowohl gegenüber dem Rechtsinhaber als auch gegenüber dem vermeintlichen Verletzer.

Um Missbräuche zu vermeiden bedarf es eines weiteren – hier gesetzlichen – Anspruchs auf Schadensersatz im Verhältnis Rechteinhaber / vermeintlicher Verletzer. War die Versicherung falsch, so soll der sich berühmende Rechteinhaber dem wahren Rechteinhaber bzw. dem behaupteten Verletzer unter bestimmten Voraussetzungen schadensersatzpflichtig sein. Nur so kann verhindert werden, dass eine Flut leichtfertig abgegebener Versicherungen das gesamte Notice-and-Take-Down-System belastet. Denkbar wäre hier zum einen eine Gefährdungshaftung nach dem Vorbild von § 717 Abs. 2 ZPO bei der vorläufigen

Vollstreckung noch nicht rechtskräftiger Urteile. Eine solche Lösung bietet sich an, weil ein Handeln auf Grundlage einer Versicherung im Notice-and-Take-Down-Verfahren im Prinzip auf einem mutmaßlichen Urteil beruht und somit der Sache nach eine noch vorläufigere Form der „Vollstreckung“ darstellt. Alternativ kommt eine Verschuldenshaftung des Versicherungsgebers in Betracht. Hier sollte der Versicherungsgeber allerdings den Entlastungsbeweis erbringen müssen, damit die Haftung für schuldhaft falsch abgegebene Versicherungen nicht leer läuft.

Weiter muss zur Eingrenzung von Missbräuchen auch die Installation eines Widerspruchsverfahrens zur Voraussetzung der Haftungsprivilegierung gemacht werden, um auch außerhalb gesetzlicher Ansprüche für den Inhalteanbieter ein Verteidigungsinstrument bereit zu halten. Zwar wird bei verantwortlicher Nutzung des NTD durch Rechteinhaber nicht oft mit einer Nutzung der Widerspruchsmöglichkeit zu rechnen sein. Für den Fall von Missbräuchen muss diese Möglichkeit aber gegeben sein. Auch insoweit kann auf das sog. „Counter-Notice“-Verfahren nach dem DMCA zurückgegriffen werden. Insgesamt könnte ein Verfahren demnach wie folgt strukturiert sein:

Antragsverfahren

1. Eingang einer formal korrekten Meldung beim Provider.

2. Der konkret beanstandete Inhalt wird umgehend vorläufig entfernt und/oder es wird Auskunft über den Inhalteanbieter als vermeintlichen Primärverletzer erteilt.

3. Gleichzeitig wird der Inhalteanbieter von der Entfernung/Auskunft sowie der Identität des Rechteinhabers in Kenntnis gesetzt.

Widerspruchsverfahren

4. Der Inhalteanbieter widerspricht der Entfernung.

5. Der Provider informiert den Rechteinhaber über den Widerspruch und setzt damit eine vom Gesetz zu definierende Frist zur Einleitung rechtlicher Schritte des Verletzten gegen den vermeintlichen Verletzter zur Klärung der streitigen Rechtsverletzung in Gang.

6. a) Der Rechteinhaber leitet rechtliche Schritte ein und informiert den Provider.
   b) Der Rechteinhaber unterlässt rechtliche Schritte innerhalb der Frist. Der Provider kann die Beseitigung aufheben.

Zur Gewährleistung der notwendigen Rechtssicherheit muss sorgfältig abgewogen werden, welche zentralen Eckpunkte gesetzlich normiert werden sollen. Hierzu zählen nach unserer Auffassung z.B. die formalen Anforderungen an die Meldung einer Verletzung. Auch die notwendige Fristsetzung im Rahmen des Widerspruchsverfahrens kann nur gesetzlich erfolgen.

3.2.2 Anwendungsbereich

Der Anwendungsbereich einer Notice-and-Takedown-Regel ist in zweierlei Hinsicht abzugrenzen. Zum einen wird zu prüfen sein, für welche Art von Rechtsverletzungen ein entsprechendes Verfahren geeignet ist. Zum anderen bedarf es einer Entscheidung, auf welche Art von Dienstleistungen der Provider ein entsprechendes Verfahren Anwendung finden kann.

Aus Sicht es BITKOM kommt ein entsprechendes Verfahren insbesondere für Hosting-Dienstleister in Betracht. Auf Access-Providing ist ein Notice-and-Takedown-Prinzip aus unserer Sicht dagegen generell nicht anwendbar, weil eine Entfernung eines Inhalts nicht vom Zugangsvermittler geleistet werden kann und auch technische Sperrungen bzw. Filterungen praktisch nicht möglich sind. Vor allem aber hat der Access-Provider, anders als der Hoster keinerlei Kontakt zum vermeintlichen Rechtverletzer. Diese Umstände sind auch im amerikanischen DMCA berücksichtigt, der ebenfalls NTD nur für Fälle des Hostings regelt.

Bezogen auf die Art der in Betracht kommenden Rechtsverletzungen spricht sich BITKOM dafür aus, den querschnittsartigen Ansatz der Verantwortlichkeitsregelungen des Telemediengesetzes fortzuschreiben und den Anwendungsbereich, anders als beim Vorbild im US-amerikanischen Recht, nicht auf einzelne Arten von Rechtsverletzungen zu beschränken.

Eine Ausnahme kommt allenfalls für Meinungsäußerungen in Betracht, wenn in diesem Zusammenhang die Verletzung von Persönlichkeitsrechten geltend gemacht wird. Hier müsste zunächst untersucht werden, inwiefern das Grundrecht auf Meinungsfreiheit einem entsprechenden Verfahren entgegensteht. Auch wird in diesem Kontext beachtet werden müssen, dass ein reiner Schadensersatzanspruch im Falle unberechtigter Löschungsaufforderung keine vollständige Kompensation für die dadurch bewirkte Einschränkung der Meinungsfreiheit gewährleisten kann.