WALDORF FROMMER Rechtsanwälte • Beethovenstraße 12 • 80336 München

Bundeswirtschaftsministerium Berlin
Scharnhorststr. 34-37
10115 Berlin

Per Mail tmg@bmwi.bund.de

Telefon 089 / 52 05 72 0
Telefax 089 / 52 05 72 751
Datum 08.04.2015

Stellungnahme zum Referentenentwurf eines Zweiten Telemedienänderungsgesetzes

Sehr geehrte Damen und Herren,

WALDORF FROMMER ist eine auf das Urheber- und Medienrecht spezialisierte Rechtsanwaltskanzlei, die zahlreiche namhafte Film-, Musik- und Verlagsmandanten berät und vertritt. Die Kanzlei ist seit vielen Jahren mit der Durchsetzung der Rechte am geistigen Eigentum in Fällen von gewerblichen bzw. nicht gewerblichen Rechtsverletzungen im Internet betraut.

Aufgrund der langjährigen Erfahrungen im Bereich der Rechtsdurchsetzung sehen wir uns veranlasst, zum Referentenentwurf eines Zweiten Telemedienänderungsgesetzes eingehend Stellung zu nehmen.

Der Referentenentwurf sieht zum einen vor, dass WLAN-Betreiber zukünftig dem Haftungsregime und damit zugleich auch dem Haftungsprivileg des § 8 TMG unterfallen sollen. Voraussetzung hierfür soll jedoch die Erfüllung näher geregelter Sorgfaltspflichten sein, die das zentrale Kernstück der neuen Regelungen darstellen. Für das Maß der aufzuerlegenden Sorgfaltspflichten ist entscheidend, ob und inwieweit anonym zugängliche Hotspots die Gefahr von Urheberrechts- und anderen Rechtsverletzungen erhöhen.

Zum anderen soll mit dem Referentenentwurf die Haftungsprivilegierung nach § 10 TMG für besonders gefahrgeneigte Host-Provider eingeschränkt werden.

Die nachfolgenden Ausführungen sollen sich beiden Änderungsvorschlägen widmen.

Änderungen des § 8 TMG
– Haftungsprivilegierung für WLAN-Betreiber –

A. Über Hotspots begangene Urheberrechtsverletzungen in P2P-Netzwerken

I. Auswertung von über Hotspots begangenen Rechtsverletzungen

Die Kanzlei WALDORF FROMMER verfügt über eine umfassende Expertise im Bereich der rechtlichen und technischen Verfolgung sämtlicher Formen von Internetpiraterie für weltweit führende Medienunternehmen. Insbesondere liegen Erkenntnisse aus der jahrelangen Überwachung von P2P-Netzwerken für zahlreiche Medienunternehmen vor.

Gleichwohl ist eine Auswertung der ermittelten Rechtsverletzungen dahingehend, ob diese über einen für jedermann zugänglichen Hotspot oder über ein auf bestimmte Nutzer beschränktes privates oder gewerbliches Netzwerk begangen wurden, nicht ohne Weiteres möglich.

Bei der eigentlichen Ermittlung von Rechtsverletzungen lässt sich zunächst nur die IP-Adresse feststellen, die zu einem bestimmten Zeitpunkt einem Internetanschluss zugeordnet war. Diese IP-Adresse allein lässt jedoch keinen Rückschluss darauf zu, ob eine Rechtsverletzung über einen Hotspot oder über ein geschlossenes Netzwerk begangen wurde. Die Art und Weise des Betriebs eines WLAN liegt allein in der Sphäre des Anschlussinhabers.

Erkenntnisse über die Anzahl von Rechtsverletzungen, die über Hotspots begangenen werden, lassen sich daher nicht über die IP-Adressen bzw. deren Zugehörigkeit zu einem bestimmten IP-Adressbereich[1], sondern nur anhand bzw. unter Mithilfe der Anschlussinhaber selbst gewinnen.

Um die ermittelten IP-Adressen den jeweiligen Anschlussinhabern zuordnen zu können, führen die in ihren Rechten verletzten Medienunternehmen fortlaufend Auskunftsverfahren nach § 101 Abs. 2, 9 UrhG unter Beteiligung nahezu sämtlicher deutscher Access-Provider.

Erst die auf diese Weise ermittelten Anschlussinhaber und/oder deren außergerichtliche bzw. gerichtliche Einlassungen erlauben überhaupt Rückschlüsse darauf, ob die Rechtsverletzung über einen Hotspot begangen wurde. Von Bedeutung hierfür ist auch, auf welche Art und Weise die Bereitstellung eines Hotspots erfolgt ist:

1. Von Access-Providern betriebene Hotspots

In den meisten Fällen werden Hotspots von den Access-Providern selbst auf zwei unterschiedliche Arten bereitgestellt:

[1] Sollten Access-Provider für von ihnen selbst bereitgestellte Hotspots etwa bestimmte IP-Adressbereiche reservieren, so werden auch diese IP-Adressbereiche nicht veröffentlicht.

Zum einen werden den Kunden des Access-Providers WLAN-Router zur Verfügung gestellt, über die nicht nur ein privates, sondern zusätzlich auch ein öffentliches WLAN-Netzwerk betrieben werden kann. An diesem öffentlichen Netzwerk, dem eine eigene IP-Adresse zugewiesen ist, können sich andere Kunden des Providers mit ihren Zugangsdaten anmelden. Derartige Lösungen werden z.B. von Kabel Deutschland unter der Bezeichnung „Homespot“ angeboten.

Daneben unterhalten diverse Access-Provider auch eigens eingerichtete Hotspots, z.B. an öffentlichen Plätzen, Bahnhöfen und Flughäfen (etwa „T-Hotspot“ von der Deutschen Telekom).

Beiden Hotspot-Varianten ist es gemeinsam, dass sie in der Regel nicht anonym genutzt werden können. Sie stehen nur Kunden des jeweiligen Access-Providers zur Verfügung, die sich für die Nutzung mit ihren individuellen Zugangsdaten authentifiziert haben.

Sofern ein Nutzer eines derartigen Hotspots eine Rechtsverletzung etwa über ein P2P-Netzwerk begeht, kann vom Access-Provider zwar der konkrete Nutzer nach § 101 Absatz 2, 9 UrhG beauskunftet werden. Der so genannte „physikalische Ursprung“ der Rechtsverletzung, also ob die ermittelte IP-Adresse dem eigenen Internetanschluss des Nutzers oder einem von ihm genutzten Hotspot zugewiesen war, wird vom Access-Provider jedoch nicht offen gelegt. Anhand der beauskunfteten Daten ist somit nicht ersichtlich, ob die Rechtsverletzung über einen vom Access-Provider betriebenen Hotspot erfolgt ist. Um den Nutzer als Hotspot-Nutzer einordnen zu können, müsste sich dieser vielmehr selbst als solcher zu erkennen geben. In keinem einzigen der von WALDORF FROMMER geführten Verfahren hat ein ermittelter Anschlussinhaber bislang jedoch vorgetragen, Nutzer eines solchen Hotspots gewesen zu sein. Dies verwundert nicht, da entweder die Rechtsverletzung als solche oder aber die eigene Verantwortlichkeit nahezu immer in Abrede gestellt werden und Ausführungen dazu, wie der Zugang zum Internet hergestellt wurde, daher von vornherein unterbleiben.

Im Ergebnis ist also der Hotspot-Nutzer bei der hier dargestellten Hotspot-Variante zwar nicht anonym. Er kann jedoch nicht von einem Nutzer unterschieden werden, der das Internet zu Hause über seinen eigenen Internetanschluss nutzt.

2. Unverschlüsselte private WLAN-Zugänge

Neben den von Access-Providern unterhaltenen Hotspots werden auch von Privaten unverschlüsselte WLAN-Zugänge betrieben. Diese können grundsätzlich in unbewusst sowie in – etwa aus altruistischen bzw. politischen Motiven – bewusst unverschlüsselte WLAN-Zugänge unterteilt werden:

Private unverschlüsselte WLAN stellen in Deutschland eher die Ausnahme[2] dar, da private Anschlussinhaber ein persönliches Interesse daran haben, ihr WLAN vor einem unkontrollierten Zugriff Dritter auf das eigene Netzwerk abzusichern.

Daneben werden unverschlüsselte WLAN aber auch von bestimmten Initiativen bereitgestellt, die darauf abzielen, jedermann ein offenes WLAN zur Verfügung zu stellen, etwa die Initiative

[2] Vgl. Erhebung des Verbandes der deutschen Internetwirtschaft e.V. eco vom November 2014.

„Freifunk“. Die Nutzer- bzw. Mitgliederzahlen dieser Initiativen sind aktuell im Verhältnis zur Bevölkerungszahl verschwindend gering.

Bei sämtlichen unverschlüsselten WLAN-Zugängen agieren die Nutzer in völliger Anonymität, da entweder überhaupt keine Zugangsdaten benötigt oder jedenfalls nicht im Zusammenhang mit den Nutzungsdaten gespeichert werden.

Dementsprechend wird vom Access-Provider stets nur der Inhaber des jeweiligen Internetanschlusses beauskunftet, wenn über ein unverschlüsseltes WLAN eine Rechtsverletzung begangen wird.

Eine mangelnde Absicherung des WLAN oder eine Beteiligung des Anschlussinhabers an einer Freifunk-Initiative ergibt sich allenfalls aus dessen außergerichtlicher bzw. gerichtlicher Einlassung. Inwieweit die Rechtsverletzung durch den Anschlussinhaber selbst oder einen Dritten begangen wurde, bleibt dabei letztlich meist unklar, da die eigene Verantwortlichkeit nahezu immer (pauschal) in Abrede gestellt wird.

Auch wenn unverschlüsselte WLAN inzwischen die Ausnahme darstellen und Initiativen wie Freifunk nicht die breite Bevölkerung erreichen, ist davon auszugehen, dass der Anteil an Rechtsverletzungen, die über unverschlüsselte WLAN erfolgen, weiterhin signifikant ist.

3. Frei zugängliche Hotspots in Beherbergungs- und Bewirtungsbetrieben

Zudem stellen zahlreiche Beherbergungs- und Bewirtungsbetriebe sowie öffentliche Einrichtungen ihren Kunden Hotspots zur Verfügung.

Die Nutzung derartiger Hotspots ist dabei entweder ohne jedwede Zugangsbeschränkung möglich oder setzt die Eingabe eines für alle Nutzer einheitlichen bzw. eines individuellen Kennwortes voraus. Eine tatsächliche Identifizierung der Nutzer erfolgt dabei jedoch in den seltensten Fällen, da die Daten der Nutzer zumeist nicht erhoben werden.

Es ist daher davon auszugehen, dass Nutzer dieser Hotspots im Wesentlichen anonym agieren – entweder, da der einzelne Nutzer aus der Masse anderer, unter demselben Kennwort eingeloggter Nutzer, nicht identifizierbar ist oder aber, da der über ein individuelles Kennwort eingeloggte Nutzer keine persönlichen Daten hinterlegen musste.

Bei Rechtsverletzungen über derartige Hotspots wird im Rahmen des Auskunftsverfahrens nach § 101 Absatz 2, 9 UrhG ebenfalls nur der Anschlussinhaber, also etwa das Hotel, beauskunftet. Da es sich hierbei jedoch um einen Betrieb oder eine öffentliche Einrichtung handelt, ist für den Rechteinhaber meist bereits vor einer Stellungnahme des Anschlussinhabers erkennbar, dass die Rechtsverletzung von einem Kunden des Anschlussinhabers begangen wurde.

Dabei entfallen allein auf Beherbergungs- und Bewirtungsbetriebe sowie öffentliche Einrichtungen derzeit **ca. 10% aller in Deutschland ermittelten,** über P2P-Netzwerke begangenen **Rechtsverletzungen**. Zum Vergleich: In Deutschland stehen derzeit ca. 80 Millionen Einwohnern etwa 2 Millionen Hotelbetten gegenüber.

4. Zwischenergebnis

Trotz der bislang relativ geringen Verfügbarkeit von anonym zugänglichen Hotspots wird bereits heute mit mindestens 10% ein wesentlicher Teil der Rechtsverletzungen über anonym nutzbare gewerbliche Hotspots begangen.

Hinzu kommt die Dunkelziffer der Rechtsverletzungen, die anonym über einen unverschlüsselten privaten Zugang begangen werden.

Der Anteil an Rechtsverletzungen, die über diese anonym zugänglichen Hotspots erfolgen, ist damit überdurchschnittlich hoch.

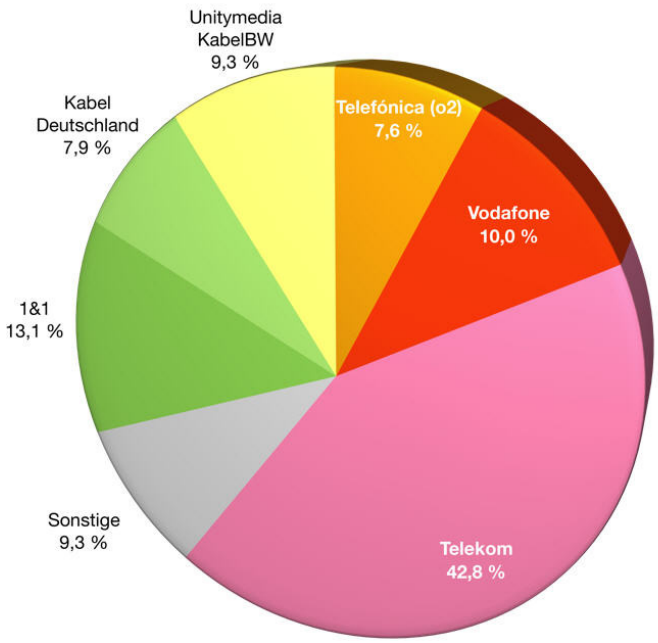
II. Auswirkungen der Anonymität auf P2P-Rechtsverletzungen bei Vodafone

Der Einfluss von Anonymität auf Urheberrechtsverletzungen in P2P-Netzwerken lässt sich darüber hinaus auch am Beispiel des Access-Providers Vodafone belegen:

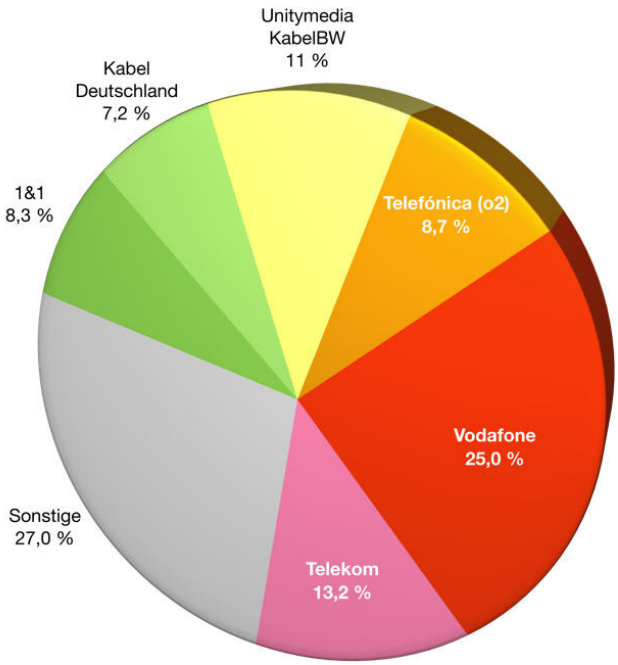
Bei Vodafone werden derzeit die Verbindungsdaten der Kunden nach eigenen Angaben nicht gespeichert und daher auch keine Auskünfte im Rahmen der Auskunftsverfahren nach § 101 Absatz 2, 9 UrhG erteilt. Die Kunden von Vodafone können daher – vergleichbar einem Nutzer eines anonym zugänglichen Hotspots – anonym und sicher vor jedweder Rechtsverfolgung agieren.

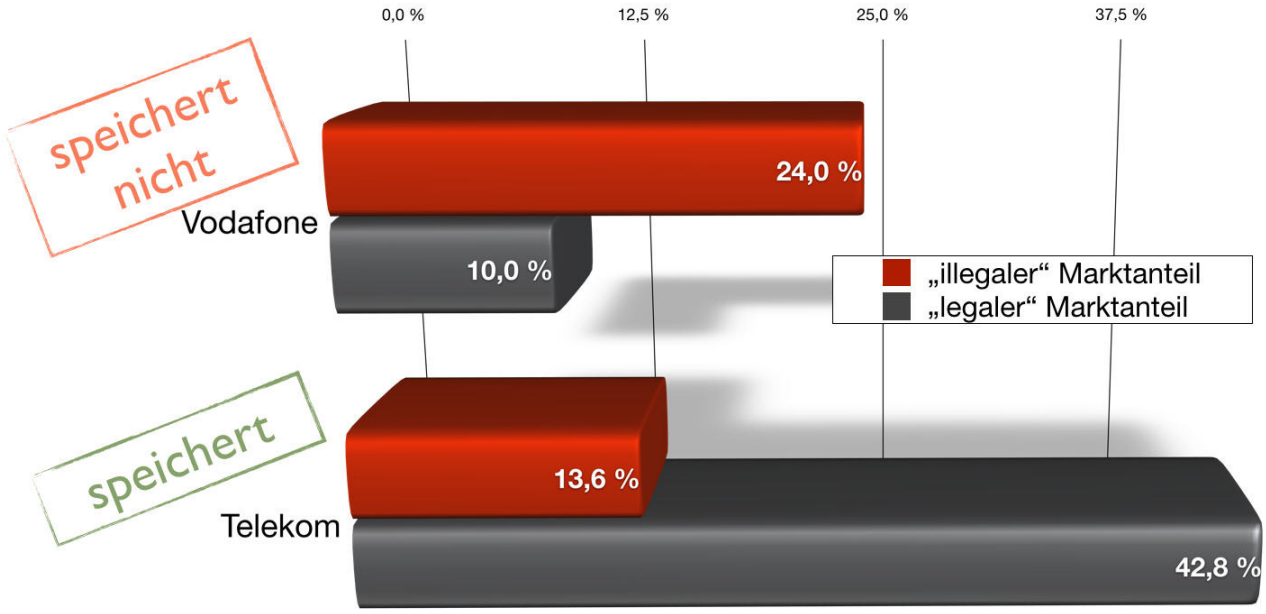
Welchen Einfluss diese Anonymität auf Urheberrechtsverletzungen hat, lässt sich am besten anhand eines Vergleichs der „legalen“ Breitband-Marktanteile von Vodafone mit den „illegalen“ Marktanteilen der Vodafone-Kunden an P2P-Rechtsverletzungen veranschaulichen:

„Legale“ Marktanteile
Breitband-Marktanteile Endkunden, VATM TK-Markstudie 2014



„Illegale“ Marktanteile
P2P-Rechtsverletzungen, ipoque Dezember 2014





Unangefochtener Marktführer (42,8%) bei den Access-Providern ist nach wie vor die Deutsche Telekom. Diese beauskunftet bereits seit Jahren die Anschlussinhaber zu den im Zusammenhang mit Rechtsverletzungen ermittelten IP-Adressen. Kunden der Deutschen Telekom können Rechtsverletzungen folglich nicht anonym begehen. Der Anteil der Kunden der Deutschen Telekom an ermittelten Rechtsverletzungen liegt daher lediglich (nur noch) bei 13,6%.

Dagegen handeln Vodafone-Kunden, wie oben dargestellt, praktisch in völliger Anonymität. Einem tatsächlichen Marktanteil von lediglich 10% steht hier ein Anteil von 24% an den ermittelten Rechtsverletzungen gegenüber.

Die Anonymität der Nutzer hat somit einen direkten Einfluss auf die Begehung von Rechtsverletzungen.[3] Ein Nutzer, der im Schutz der Anonymität handeln kann, wird naturgemäß eher Rechtsverletzungen begehen, als einer, der befürchten muss, für seine Rechtsverletzungen belangt zu werden.

III. Ergebnis

Bereits heute ist der Anteil der über anonym zugängliche Hotspots begangenen P2P-Urheberrechtsverletzungen mit über 10% beträchtlich. Unter Zugrundelegung der vorstehenden Erkenntnisse ist davon auszugehen, dass sich die Zahl der Urheberrechtsverletzungen bei einem Ausbau von anonym zugänglichen Hotspots massiv erhöhen würde.

Vor diesem Hintergrund soll nachfolgend die Einführung eines Haftungsprivilegs und korrespondierender Sorgfaltspflichten für WLAN-Betreiber bewertet werden.

---

[3] Vgl hierzu: http://www.webschauder.de/raubkopierer-lieben-hansenet-und-vodafone-telekom-verliert-weiterhin-marktanteile/

B. Anmerkungen zu den geplanten Änderungen des § 8 TMG

I. § 8 Absatz 3 TMG-E – Haftungsprivileg bei Schadenersatzansprüchen und strafrechtlicher Verantwortlichkeit

§ 8 Durchleitung von Informationen

(1) Diensteanbieter sind für fremde Informationen, die sie in einem Kommunikationsnetz übermitteln oder zu denen sie den Zugang zur Nutzung vermitteln, nicht verantwortlich, sofern sie

1. die Übermittlung nicht veranlasst,
2. den Adressaten der übermittelten Informationen nicht ausgewählt und
3. die übermittelten Informationen nicht ausgewählt oder verändert haben.

Satz 1 findet keine Anwendung, wenn der Diensteanbieter absichtlich mit einem Nutzer seines Dienstes zusammenarbeitet, um rechtswidrige Handlungen zu begehen.

(2) Die Übermittlung von Informationen nach Absatz 1 und die Vermittlung des Zugangs zu ihnen umfasst auch die automatische kurzzeitige Zwischenspeicherung dieser Informationen, soweit dies nur zur Durchführung der Übermittlung im Kommunikationsnetz geschieht und die Informationen nicht länger gespeichert werden, als für die Übermittlung üblicherweise erforderlich ist.

(3) Die vorstehenden Absätze gelten auch für Diensteanbieter nach Absatz 1, die Nutzern einen Internetzugang über ein drahtloses lokales Netzwerk zur Verfügung stellen. […]

1. Erweiterung des Haftungsprivilegs nach § 8 Absatz 1 (Schadenersatz und strafrechtliche Verantwortlichkeit) auf sämtliche WLAN-Betreiber (auch Private) faktisch ohne Auswirkungen

§ 8 Absatz 3 TMG-E soll klarstellen, dass sich zukünftig **sämtliche WLAN-Betreiber** – insbesondere auch Private[4] – auf das Haftungsprivileg des § 8 Absatz 1 TMG berufen können. Das Haftungsprivileg des Absatzes 1 umfasst dabei neben der strafrechtlichen Verantwortlichkeit allerdings **nur Ansprüche auf Schadenersatz**. Dies stellt auch der Referentenentwurf in der Begründung ausdrücklich klar:

> *„WLAN-Betreiber erhalten damit dahingehend Rechtssicherheit, dass sie für Rechtsverletzungen ihrer Nutzer, Kunden etc.* ***weder zum Schadensersatz*** *verpflichtet* ***noch strafrechtlich verantwortlich*** *sind. […] Durch § 8 Absatz 3 TMG wird der Anbieter eines drahtlosen lokalen Funknetzes* ***nicht zugleich von seiner Haftung als sog. Störer befreit****."* (Referentenentwurf vom 11.03.2015, S. 10 f.)

Die Gerichte dürften somit sämtliche WLAN-Betreiber zukünftig als Diensteanbieter i.S.d. § 8 TMG ansehen.

Selbst ein privater WLAN-Betreiber haftet jedoch bereits heute nicht auf Schadenersatz, wenn er keine der von § 8 Absatz 1 TMG vorgesehenen Ausnahmen erfüllt, also weder Täter noch Teilnehmer der Urheberrechtsverletzung ist. Sofern er Täter oder Teilnehmer ist, wird aber auch § 8 Absatz 3 TMG-E seine Schadenersatz-Haftung nicht ausschließen.

[4] Dass in den Anwendungsbereich auch Private fallen sollen, folgt dabei aus einer Zusammenschau mit Absatz 5, der eine ausschließlich auf private WLAN-Betreiber anwendbare Sonderregel enthält.

2. Nachbesserungsbedarf

Nachbesserungsbedarf besteht im Hinblick auf das Verhältnis zum TKG.

Im Referentenentwurf vom 11.03.2015[5] finden sich nämlich keine Ausführungen (mehr) dazu, dass die Pflichten des TKG auch für WLAN-Betreiber gelten sollen. Vielmehr heißt es dort nur:

> *„Diese Klarstellung führt zu keinen Änderungen an der bisherigen Rechtslage für **Diensteanbieter, die den Zugang zu einem Kommunikationsnetz nach dem TKG vermitteln**. **Für diese Diensteanbieter** gelten die sich aus dem TKG ergebenden Pflichten weiterhin fort."* (Referentenentwurf vom 11.03.2015, S. 8)

Diese Formulierung lässt daher befürchten, dass die Pflichten des TKG nur für diejenigen WLAN-Anbieter gelten sollen, die auch bisher vom Anwendungsbereich des TKG umfasst waren.

Private WLAN-Anbieter müssten die Pflichten des TKG somit gerade nicht erfüllen, da die Pflichten des TKG grundsätzlich **nicht für private Diensteanbieter** gelten.

Sofern die Privilegierungen des TMG auch privaten WLAN-Betreibern zuerkannt werden sollen, sollten diese jedoch gleichermaßen verpflichtet werden, die insbesondere aus dem TKG resultierenden Pflichten[6] von Access-Providern zu erfüllen.

II. § 8 Absatz 4 und 5 TMG-E – Haftungsprivileg bei Unterlassungsansprüchen (i.R.d. Störerhaftung)

§ 8 Durchleitung von Informationen

[…]

(4) Diensteanbieter, die einen Internetzugang nach Absatz 3 **geschäftsmäßig** oder **als öffentliche Einrichtung** zur Verfügung stellen, **können** wegen einer rechtswidrigen Handlung eines Nutzers **nicht auf Unterlassung in Anspruch genommen werden**, wenn sie **zumutbare Maßnahmen** ergriffen haben, um eine Rechtsverletzung durch Nutzer zu verhindern. Dies ist insbesondere der Fall, wenn der Diensteanbieter

1. angemessene Sicherungsmaßnahmen durch anerkannte Verschlüsselungsverfahren oder vergleichbare Maßnahmen gegen den unberechtigten Zugriff auf das drahtlose lokale Funknetz durch außenstehende Dritte ergriffen hat **und**
2. Zugang zum Internet nur dem Nutzer gewährt, der erklärt hat, im Rahmen der Nutzung keine Rechtsverletzungen zu begehen.

(5) **Sonstige** Diensteanbieter, die einen Internetzugang nach Absatz 3 zur Verfügung stellen, **können** wegen einer rechtswidrigen Handlung eines Nutzers **nicht auf Unterlassung in Anspruch genommen werden**, wenn sie zumutbare

[5] Hierbei handelt es sich um den offiziell vom BMWi veröffentlichten Ref-E, der gegenüber dem ersten inoffiziellen Ref-E vom 17.02.2015 bereits einige Änderungen erfahren hat.

[6] Etwa die Meldepflicht nach § 6 TKG, die Pflicht nach § 109 Abs. 1 TKG zur Ergreifung technischer Vorkehrungen und sonstiger Maßnahmen zum Schutz des Fernmeldegeheimnisses und gegen die Verletzung des Schutzes personenbezogener Daten, die Pflicht nach § 109 Abs. 2 TKG zur Ergreifung technischer Schutzmaßnahmen zum Schutz gegen Störungen, die Pflicht nach § 109 Abs. 4 TKG zur Erstellung eines Sicherheitskonzeptes sowie die Pflicht nach § 111 TKG zur Erhebung und Speicherung von bestimmten Kundendaten für Auskunftsersuchen von Sicherheitsbehörden.

Maßnahmen **im Sinne des Absatzes 4** ergriffen haben **und** die Namen der Nutzer kennen, denen sie den Zugang gewährt haben.

Mit den Absätzen 4 und 5 sollten eigentlich die Bedingungen für einen Ausschluss der Störerhaftung kodifiziert und damit die Störerhaftung präzisiert werden.

> *„Die Vorgaben der E-Commerce Richtlinie (Richtlinie 2000/31/EG) sind zu beachten. Die Bestimmungen präzisieren lediglich die bestehenden Regelungen des TMG und die von der Rechtsprechung entwickelte Störerhaftung und stehen damit im Einklang mit der E-Commerce Richtlinie. […]*
> *Die Vorschriften zur Anwendbarkeit des Haftungsprivilegs und zu den Bedingungen für einen Ausschluss der Störerhaftung führen zu einer Präzisierung der bestehenden rechtlichen Regelungen und schaffen damit Rechtssicherheit für die Betreiber von WLAN."* (Referentenentwurf vom 11.03.2015, S. 9)

Im Referentenentwurf vom 11.03.2015 wurde jedoch die (im ursprünglichen Entwurf vom 17.02.2015 noch vorhandene) Bezugnahme auf die Störerhaftung gestrichen. In der neuen Fassung ist nur noch allgemein von Unterlassungsansprüchen die Rede, so dass sich nunmehr sogar Teilnehmer (!) von Rechtsverletzungen hinsichtlich eines Unterlassungsanspruchs auf das Haftungsprivileg nach Absatz 4 bzw. 5 berufen könnten.
In § 8 Absatz 4 Satz 1 TMG-E wird geregelt, dass WLAN-Betreiber dann nicht auf Unterlassung in Anspruch genommen werden können (früher: „haften nur dann nicht **als Störer** auf Unterlassen"), wenn sie zumutbare Maßnahmen zur Verhinderung von Rechtsverletzungen durch ihre Nutzer ergriffen haben. Ungeachtet dessen wurde an der Begrifflichkeit des Störers in der gesamten Entwurfsbegründung festgehalten, wie die untenstehenden Zitate belegen.

Mit § 8 Absatz 4 Satz 2 und Absatz 5 TMG-E wird durch eine *„beispielhafte"* Aufzählung von Maßnahmen festgelegt, unter welchen Voraussetzungen (generell) von einer Erfüllung dieser zumutbaren Maßnahmen auszugehen ist, wobei die Beschreibung dieser Maßnahmen äußerst unbestimmt bleibt.

> *„Die Haftung der Anbieter von WLAN-Internetzugängen für Rechtsverletzungen ihrer Nutzer ist im Telemediengesetz zu präzisieren. Hierzu ist zum einen klarzustellen, dass solche Anbieter Zugangsanbieter im Sinne des TMG sind. Des Weiteren ist klarzustellen, dass für Anbieter von WLAN auch eine Haftung als Störer nicht in Betracht kommt, wenn diese bestimmte, im Gesetz zumindest beispielhaft aufzuführende, Sorgfaltspflichten erfüllt haben."* (Referentenentwurf vom 11.03.2015, S. 2)

> *„Um auch eine Haftung als Störer ausschließen zu können, wird in diesem Gesetzentwurf ebenfalls **kodifiziert, dass gegen Zugangsanbieter**, insbesondere WLAN-Betreiber, **kein Anspruch auf Unterlassung besteht, sofern diese zumutbare Maßnahmen ergriffen haben, um eine Rechtsverletzung durch Dritte zu verhindern**. Für WLAN-Anbieter werden diese zumutbaren Maßnahmen im Einzelnen beschrieben. Mit der **beispielhaften** Aufzählung der zumutbaren Maßnahmen für WLAN-Betreiber wird dem bestehenden Bedürfnis nach Rechtssicherheit potentieller Anbieter von WLAN entsprochen."* (Referentenentwurf vom 11.03.2015, S. 6)

> *„Daneben wird der bereits von der Rechtsprechung entwickelte Grundsatz kodifiziert, dass WLAN-Anschlussinhaber nicht als Störer haften, wenn sie zumutbare Pflichten erfüllt haben, um Rechtsverletzungen zu verhindern. Mit dem Gesetz werden die Anforderungen an Diensteanbieter, die Zugang zum Internet über WLAN vermitteln, präzisiert. Bei Einhaltung der im Gesetz genannten Vorgaben wird davon ausgegangen, dass der WLAN-Anbieter die ihm zumutbaren Vorkehrungen getroffen hat, um eine Rechtsverletzung durch Dritte zu*

verhindern. In diesen Fällen haftet er nicht als Störer auf Unterlassen und kann dann auch nicht abgemahnt werden. Die im Gesetz genannten Vorgaben sind in der Regel von WLAN-Anbietern erfüllbar. Dies schließt indes nicht aus, dass der Anschlussinhaber in bestimmten Fällen seinen Pflichten ***auch durch andere zumutbare Maßnahmen nachkommen kann****."* (Referentenentwurf vom 11.03.2015, S. 8)

„Durch § 8 Absatz 3 TMG wird der Anbieter eines drahtlosen lokalen Funknetzes nicht zugleich von seiner Haftung als sog. Störer befreit. Haftpflichtiger Störer kann nach der Rechtsprechung jeder sein, der in irgendeiner Weise willentlich und adäquat-kausal zur Verletzung eines geschützten Rechtsguts beiträgt, ***sofern er zumutbare Prüfpflichten verletzt hat****. Diese Haftung ist auf Unterlassung, nicht aber auf Schadensersatz gerichtet (BGH, Urt. v. 15.5.2010, Az. I ZR 121/08 – ‚Sommer unseres Lebens', abgedruckt in BGHZ 185, 330). In diesem* ***Sinne kodifiziert § 8 Absatz 4 Satz 1 TMG****, dass Diensteanbieter, die geschäftsmäßig oder als öffentliche Einrichtung handeln, grundsätzlich* ***dann nicht als Störer*** *in Anspruch genommen werden können,* ***wenn sie die ihnen zumutbaren Maßnahmen ergriffen haben****, um eine Rechtsverletzung durch unberechtigte Dritte zu verhindern.*
Da die Rechtsfortentwicklung der Störerhaftung im Wege richterrechtlicher Einzelfallentscheidungen erfolgt, besteht in allen anderen Fällen Rechtsunsicherheit, welche Pflichten dem Störer jeweils zuzumuten sind. Eine Fortdauer dieser Rechtsunsicherheit würde potenzielle Anbieter von Internetzugängen über WLAN wegen des Haftungsrisikos weiter davon abhalten, ihren Kunden einen solchen zur Verfügung stellen. ***Neben der Klarstellung zum Haftungsprivileg präzisiert der Gesetzentwurf*** *daher in Satz 2 auch* ***die Voraussetzungen, unter denen bei diesen Zugangsanbietern davon ausgegangen werden kann, dass sie ihre zumutbaren Pflichten erfüllt haben****, um eine missbräuchliche Nutzung des Internetzugangs durch Dritte zu verhindern. Die bisherigen, von der Rechtsprechung entwickelten Grundsätze werden dabei im Sinne von Regelbeispielen aufgegriffen und fortentwickelt, um möglichst weitgehend Rechtssicherheit zu schaffen.* ***Dabei sollen die von der Rechtsprechung für private WLAN-Anschlussinhaber entwickelten Grundsätze gleichermaßen für gewerbliche und andere kommerzielle Anbieter von WLAN sowie für öffentliche Einrichtungen gelten****. Dies schließt nicht aus, dass* ***auch andere zumutbare Maßnahmen*** *ergriffen werden können, wodurch nicht zuletzt die dauerhafte Anwendbarkeit der Vorschrift im fortschreitenden technologischen Veränderungsprozess sichergestellt wird."* (Referentenentwurf vom 11.03.2015, S. 10 f.)

1. Präzisierung der Störerhaftung grundsätzlich zu begrüßen

§ 8 Absatz 4 Satz 1 soll nach der Entwurfsbegründung lediglich eine seit Jahren anerkannte Rechtsprechung wiedergeben: Keine Störerhaftung der WLAN-Betreiber ohne Verletzung zumutbarer Prüfpflichten.

Positiv ist dabei, dass mit den Absätzen 4 und 5 ergänzend zu § 7 Absatz 2 Satz 2 TMG nun **klargestellt** wird, **dass eine Haftungsprivilegierung nach Absatz 1 nur für Schadenersatzansprüche, nicht jedoch für Unterlassungsansprüche besteht**, sofern seitens des WLAN-Betreibers keine zumutbaren Sicherungsmaßnahmen ergriffen wurden. Mit anderen Worten: Auch der WLAN-Betreiber, der sein WLAN überhaupt nicht sichert, genießt zwar das Haftungsprivileg nach Absatz 1 und haftet somit nicht auf Schadenersatz, eine Inanspruchnahme auf Unterlassung bleibt aber gleichwohl möglich. Nur wenn zumutbare Sicherungsmaßnahmen ergriffen wurden, scheiden selbst Unterlassungsansprüche aus.

Ebenso ist aus Sicht der Rechteinhaber zu begrüßen, dass nach dem Wortlaut die **Beweislast** für das „Ergreifen der zumutbaren Maßnahmen" **beim WLAN-Betreiber** liegt (*„können nicht […] in*

Anspruch genommen werden, wenn").

2. Nachbesserungsbedarf

Erheblicher Nachbesserungsbedarf besteht jedoch beim Umfang des Haftungsprivilegs sowie beim Umfang und der Formulierung der *„beispielhaft"* aufgezählten zumutbaren Maßnahmen, die für eine „Exkulpation" vom WLAN-Betreiber ergriffen werden müssen (Absätze 4 und 5):

a. Haftungsprivileg erfasst auch Teilnehmer

Nach der aktuellen Fassung der Absätze 4 und 5 könnten sich nunmehr sogar Teilnehmer (!) von Rechtsverletzungen auf das Haftungsprivileg berufen. Dies ist vermutlich von den Entwurfsverfassern nicht gesehen worden und sollte daher unbedingt korrigiert werden.

Eine Korrektur könnte beispielsweise erfolgen, indem entsprechend § 8 Satz 2 TMG auch in den Absätzen 4 und 5 das Haftungsprivileg bei einem kollusiven Zusammenwirken von WLAN-Betreibern und Nutzern ausgeschlossen wäre. Ein Ausschluss sollte zudem entsprechend § 8 Absatz 1 Satz 1 Halbsatz 2 TMG auch in denjenigen Fällen erfolgen, in denen WLAN-Betreiber die Übermittlung veranlasst, den Adressaten der übermittelten Information ausgewählt und die übermittelte Information ausgewählt oder verändert haben. Dies könnte etwa durch einen Verweis auf die Geltung des Absatzes 1 Satz 1 Halbsatz 2 und des Absatzes 1 Satz 2 in den Absätzen 4 und 5 erfolgen: *„Absatz 1 Satz 1 Halbsatz 2 sowie Absatz 1 Satz 2 gelten entsprechend."*

b. Haftungsprivileg gilt auch dann, wenn nicht alle „zumutbaren Maßnahmen" ergriffen wurden

Der vorgeschlagene **Gesetzeswortlaut** des § 8 Absatz 4 Satz 1 TMG könnte zur Folge haben, dass sich WLAN-Betreiber schon dann auf das Haftungsprivileg berufen können, wenn sie überhaupt irgendwelche zumutbaren Maßnahmen ergriffen haben (*„wenn sie zumutbare Maßnahmen ergriffen haben"*). Zur Klarstellung, dass für den Ausschluss der Störerhaftung sämtliche zumutbaren Maßnahmen ergriffen werden müssen, sollte der Wortlaut daher unbedingt nachgebessert werden, z.B. wie folgt:

„Diensteanbieter […] können wegen einer rechtswidrigen Handlung eines Nutzers nur dann nicht auf Unterlassung in Anspruch genommen werden, wenn sie ***sämtliche*** *(bzw. „die")* ***zumutbaren Maßnahmen*** *ergriffen haben, um eine Rechtsverletzung durch Nutzer zu verhindern."*

Dies entspräche nicht nur der Rechtsprechung zur Störerhaftung, sondern wohl auch der mutmaßlichen Absicht der Entwurfsverfasser, denn in der Begründung des Regierungsentwurfs vom 11.03.2015 steht:

„In diesem Sinne kodifiziert § 8 Absatz 4 Satz 1 TMG, dass Diensteanbieter, die geschäftsmäßig oder als

*öffentliche Einrichtung handeln, grundsätzlich dann nicht als Störer in Anspruch genommen werden können, wenn sie **die** ihnen zumutbaren Maßnahmen ergriffen haben, um eine Rechtsverletzung durch unberechtigte Dritte zu verhindern."* (Referentenentwurf vom 11.03.2015, S. 11)

c. Zumutbare Maßnahmen sind nicht als Regelbeispiele, sondern als Maximalanforderungen ausgestaltet

Der Referentenentwurf stellt klar, dass die aufgezählten Maßnahmen auch durch andere geeignete Maßnahmen ersetzt werden können. Die Aufzählung stellt demnach keine Minimalanforderungen auf, sondern wohl eher Maximalanforderungen. Die gegenwärtige Formulierung (*„Dies ist insbesondere der Fall"*) muss daher als nach oben abschließende Aufzählung zumutbarer Maßnahmen verstanden werden.

Eine nach oben abschließende Aufzählung hätte zur Folge, dass gegenüber geschäftsmäßigen WLAN-Betreibern ein Unterlassungsanspruch generell und ausnahmslos ausgeschlossen wäre, wenn a) das WLAN irgendwie gegen unberechtigte Zugriffe abgesichert war und b) Zugang zum Internet nur denjenigen Nutzern gewährt wurde, die erklärt haben, im Rahmen der Nutzung keine Rechtsverletzungen zu begehen. Selbst dann, wenn weitere Maßnahmen zumutbar wären, müsste der Betreiber diese also generell nie ergreifen.

Anstelle der Formulierung *„Dies ist insbesondere der Fall, wenn der Diensteanbieter…"* sollten die Beispiele daher **zumindest als echte *„Regelbeispiele"*** formuliert werden: *„Dies ist in der Regel der Fall, wenn der Diensteanbieter …".* Die aufgezählten Beispiele würden dann die grundsätzlich geltenden Anforderungen darstellen und nicht die Maximalanforderungen.

Zudem würde diese Formulierung der übrigen Gesetzessystematik des 2. TMGÄndG entsprechen, da die Voraussetzungen, unter denen nach § 10 Absatz 2 Satz 2 TMG-E ein besonders gefahrgeneigter Dienst anzunehmen ist, auch als Regelbeispiele ausgestaltet sind: *„Ein besonders gefahrgeneigter Dienst liegt in der Regel dann vor, wenn…"*

Die Formulierung als Regelbeispiel ermöglicht darüber hinaus eine Abweichung nach unten für Härtefälle und nach oben für andere Sonderfälle.

d. Unklares Verhältnis zu § 7 Absatz 2 Satz 2 TMG

Unklar ist darüber hinaus, ob durch eine Erfüllung der Pflichten nach § 8 Absatz 4 Satz 2 TMG-E sämtliche – in der Rechtsprechung anerkannten – Ansprüche auf Entfernung oder Sperrung rechtswidriger Inhalte ausgeschlossen wären.

Die Vorgaben der Art. 8 Absatz 3 InfoSoc-RL, Art. 11 Enforcement-RL, Art. 12 Absatz 3 E-Commerce-RL verpflichten die Mitgliedstaaten, sicher zu stellen, dass Diensteanbieter zur Abstellung bzw. Verhinderung von Rechtsverletzungen verpflichtet werden können. Um den europäischen Vorgaben zu entsprechen, muss somit ein Beseitigungs- und Unterlassungsanspruch geltend gemacht werden können. Im deutschen Recht ist dies gegenwärtig nur über die Störerhaftung bzw. den hieraus resultierenden

Unterlassungsanspruch möglich.

Entsprechende Verpflichtungen auf Beseitigung bzw. Unterlassung lassen sich zwar weiterhin aus § 7 Absatz 2 Satz 2 TMG herleiten, der unverändert erklärt: *„Verpflichtungen zur Entfernung oder Sperrung der Nutzung von Informationen nach den allgemeinen Gesetzen bleiben auch im Falle der Nichtverantwortlichkeit des Diensteanbieters nach den §§ 8 bis 10 unberührt."* § 7 Absatz 2 TMG stellt somit zwar klar, dass die Haftungsprivilegierungen nach den §§ 8 bis 10 TMG keinerlei Auswirkungen auf Unterlassungs- und Beseitigungsansprüche haben. Gleichwohl könnte die Neuregelung als lex specialis zu § 7 Absatz 2 Satz 2 TMG-E missverstanden werden, da mit § 8 Absatz 4 Satz 2 TMG-E nunmehr ein in Widerspruch zu § 7 Absatz 2 Satz 2 TMG-E stehender Haftungsausschluss bei Unterlassungsansprüchen eingeführt werden soll.

Ein derartiger Haftungsausschluss wäre jedoch mit den oben aufgeführten Richtlinienbestimmungen sowie der Rechtsprechung des EuGH („UPC Telekabel"[7], „Scarlet Extended"[8]) unvereinbar. Die europarechtlichen Vorgaben überlassen den Mitgliedstaaten zwar einen gewissen Spielraum bei der Ausgestaltung der gerichtlichen Beseitigungs- und Unterlassungsanordnungen (vgl. Erwägungsgrund 59 der InfoSoc-RL), sie sind jedoch hinsichtlich des zu erreichenden Ziels verbindlich.

Es wäre daher europarechtswidrig, wenn eine gesamte Kategorie von (Zugangs)Vermittlern (WLAN-Anbieter) generell nicht mehr zur Beseitigung und Verhinderung von Rechtsverletzungen verpflichtet werden könnte.

e. Unklare Formulierung der Pflichten nach § 8 Absatz 4 TMG-E

Die vom Referentenentwurf in Absatz 4 vorgeschlagenen Pflichten zur Absicherung und Zugangsgewährung nur bei Erklärung der Nutzer, keine Rechtsverletzungen zu begehen, sind als Maßnahmen grundsätzlich positiv zu bewerten.

Die Formulierung der Beispiele ist allerdings zu unbestimmt, so dass die gewünschte Rechtsklarheit und Rechtssicherheit durch das Gesetz allein nicht hergestellt werden kann. Auch aus der Begründung des Referentenwurfs lässt sich die erforderliche Klarheit nicht entnehmen.

> *„Im Einzelnen kann davon ausgegangen werden, dass der kommerzielle WLAN-Anbieter bzw. die öffentliche Einrichtung die ihnen zumutbaren Pflichten erfüllt, wenn sie:*
> *1. angemessene Sicherungsmaßnahmen, insbesondere durch anerkannte Verschlüsselungsverfahren oder vergleichbare Maßnahmen, gegen den unerlaubten Zugriff getroffen haben*
> *Erste Voraussetzung für eine Befreiung von der Störerhaftung ist, dass der WLAN-Betreiber sein Funknetz in angemessener Form technisch gegen die Nutzung durch Unberechtigte sichert. Einem Diensteanbieter, der mit dem WLAN einen Zugang zum Internet eröffnet, ist dies zumutbar, da er andernfalls eine potentielle Gefahrenquelle zur Begehung rechtswidriger Taten schafft, ohne noch die Kontrolle darüber zu haben, wer*

[7] EuGH, 27.03.2014, Rs. C-314/12

[8] EuGH, 24.11.2011, Rs. C-70/10

sich über sein WLAN Zugang zum Internet verschafft hat. Insbesondere vor dem Hintergrund zunehmender Cyberkriminalität entspricht dies auch dem ureigensten Interesse des Anschlussinhabers. Denn so wird gewährleistet, dass seine Daten und die der Nutzer des WLAN so weit wie möglich gegen den Zugriff durch Unbefugte gesichert werden. Der Diensteanbieter genügt dieser Verpflichtung in der Regel, wenn er seinen Anschluss verschlüsselt. Dabei sollen sichere Verschlüsselungsverfahren zur Anwendung kommen. Unter „Verschlüsselung" ist in der Regel die Verschlüsselung des Routers, wie vom Hersteller vorgesehen, oder eine vergleichbare Maßnahme zu verstehen. Zumutbar kann u. U. sein, dass der WLAN-Anbieter die aktuelle Firmware/Verschlüsselung einrichtet (z.B. WPA2). Mit der Formulierung „oder vergleichbare Maßnahmen" wird die gebotene Technologieneutralität sichergestellt.

2. Zugang zum Internet nur dem Nutzer gewährt, der erklärt hat, im Rahmen der Nutzung keine Rechtsverletzungen zu begehen

Dem Diensteanbieter ist es außerdem zuzumuten, sicherzustellen, dass der Nutzer nur dann Zugang zum Internet erhält, wenn er in die Bedingung eingewilligt hat, keine rechtswidrigen Handlungen zu begehen. Dies kann bei der Überlassung eines WLAN–Zugangs durch Nutzungsbedingungen erfolgen, denen der Nutzer vor Öffnung der WLAN-Verbindung, möglichst durch Setzen eines Häckchens, ausdrücklich zustimmen muss. Das Gesetz macht hier jedoch keine Vorgaben, so dass die Einwilligung auch durch Zustimmung zu veröffentlichten AGB, aus denen sich die Nutzungsbedingungen ergeben, erfolgen kann. In der Regel wird der Diensteanbieter dem Nutzer den Internetzugang durch Mitteilung eines Passwortes zur Nutzung überlassen. Dieses kann beispielsweise auf der Eintritts- oder Speisekarte veröffentlicht oder dem Nutzer auf anderem Wege mitgeteilt werden. Möglich ist auch die Einrichtung einer Vorschaltseite, auf der lediglich die Nutzungsbedingungen - mit einem Klick - akzeptiert werden können."

(Referentenentwurf vom 11.03.2015, S. 12 f.)

Insbesondere die zahlreichen unbestimmten Rechtsbegriffe der Regelung werden es auch zukünftig erforderlich machen, dass die genaue Ausgestaltung der zumutbaren Maßnahmen der Rechtsprechung überlassen bleibt. Dies dürfte zwar sinnvoll sein, da sich v.a. die Angemessenheit von Sicherungsmaßnahmen nur im Einzelfall und unter Berücksichtigung der sich stets wandelnden technischen Entwicklungen bewerten lässt, führt jedoch zu der Gefahr einer divergierenden Rechtsprechung. Diese Gefahr könnte dadurch entschärft werden, dass die Störerhaftung maßgeblich davon abhängig gemacht wird, ob der für die Rechtsverletzung primär Verantwortliche vom WLAN-Betreiber identifiziert wird (dazu im Folgenden).

f. Fehlende Registrierungs- und Auskunftspflicht

Der Referentenentwurf erkennt mit Absatz 5 an, dass einem WLAN-Betreiber durchaus zuzumuten ist, dass er die Namen seiner Nutzer kennt. Der private WLAN-Betreiber soll bei gleichzeitiger Erfüllung der Pflichten nach § 8 Absatz 4 Satz 2 Ziff. 1 und 2 TMG-E nämlich nur dann nicht (als Störer) auf Unterlassung haften, *„wenn er darlegen kann, dass er nur denjenigen Nutzern sein WLAN zur Verfügung gestellt hat, die er zumindest namentlich kennt."* Hieraus folgt zumindest eine **faktische Registrierungspflicht**.

Leider beschränkt der Referentenentwurf die Registrierungspflicht jedoch ohne nachvollziehbare Begründung auf private WLAN-Betreiber.

„Im Unterschied zum geschäftsmäßig handelnden Diensteanbieter müssen sonstige WLAN-Betreiber, die einen Internetzugang nach Absatz 3 zur Verfügung stellen. über die Voraussetzungen des Absatzes 4, Ziffern

1. und 2. hinaus, zusätzlich den oder die Nutzer namentlich kennen, denen sie den Zugang gewährt haben, um nicht als Störer in Anspruch genommen werden zu können." (Referentenentwurf vom 11.03.2015, S. 13)

Auch aus § 8 Absatz 4 Satz 2 Ziff. 2 TMG-E lässt sich für geschäftsmäßig handelnde WLAN-Betreiber keine konkludente Registrierungspflicht ableiten. Denn die Erklärung eines Nutzers, sich rechtstreu zu verhalten, soll bereits durch das einfache Setzen eines Hakens möglich sein. Eine namentliche Registrierung ist hierzu gerade nicht erforderlich. Im Ergebnis dürfte sogar genügen, dass der Betreiber auf seiner Login-Seite schreibt: *„Mit dem Aufbau der Verbindung erklärt der Nutzer, im Rahmen der Nutzung keine Rechtsverletzungen zu begehen"*.

Wie die Ausführungen unter A.I.3. zeigen, werden jedoch über geschäftsmäßig betriebene WLAN mindestens 10 % sämtlicher P2P-Rechtsverletzungen begangen. Gerade diese WLAN-Zugänge werden somit besonders häufig zu Urheberrechtsverletzungen missbraucht.

Zudem versäumt der Referentenentwurf, die in § 8 Absatz 5 TMG-E vorgesehene faktische Registrierungspflicht für private WLAN-Betreiber auf die zwangsläufig gebotene Auskunftspflicht zu erweitern.

Schließlich ist unklar, wo die Grenzen zwischen geschäftsmäßig und privat betriebenem WLAN verlaufen sollen. Nachdem für „geschäftsmäßiges Handeln" lediglich „Nachhaltigkeit", nicht aber eine Gewinnerzielungsabsicht gefordert wird, lässt sich auch jeder Private unter Absatz 4 subsumieren, sofern er sein WLAN nicht nur gelegentlich, sondern dauerhaft Dritten zur Verfügung stellt. Diese Abgrenzungsschwierigkeiten könnten somit dazu führen, dass die in Absatz 5 normierte, faktische Registrierungspflicht für private WLAN-Betreiber sehr leicht umgangen werden könnte.

*„Geschäftsmäßig im Sinne der ersten Alternative ist **jede nachhaltige Tätigkeit mit oder ohne Gewinnerzielungsabsicht**. Für geschäftsmäßiges Handeln ist **weder erforderlich, dass der Hauptzweck der Geschäftstätigkeit in der Überlassung von WLAN-Netzen besteht**, **noch** dass der **Internetzugang gegen Entgelt** gewährt wird. Ausreichend ist daher bereits, dem Gast, Kunden etc. das WLAN-Netz als unentgeltliche, untergeordnete Nebenleistung zum eigentlichen Geschäftszweck zu überlassen, um so etwa eine größere Kundenbindung zu erreichen oder die Attraktivität des Hauptangebots zu steigern. Für die Geschäftsmäßigkeit ist **auch die Trägerschaft oder Rechtsform der Geschäftstätigkeit des Diensteanbieters unerheblich**. Beispielsweise wären ein Internet-Café oder ein Sportverein demzufolge in der Regel geschäftsmäßig tätige WLAN-Anbieter."* (Referentenentwurf vom 11.03.2015, S. 11 f.)

(1) Registrierungspflicht bedarf korrespondierender Auskunftspflicht

Die reine Verpflichtung, einen Nutzer namentlich zu kennen, kann keinesfalls als zureichende Maßnahme angesehen werden. Geboten ist vielmehr, dass der WLAN-Betreiber die ihm bekannten Namen auch auf Basis eines gesetzlichen Auskunftsanspruches mitteilen muss. Andernfalls würde die reine Kenntnis zu einer Haftungsfreistellung führen. Der wahre Täter bliebe aber unbekannt, da keinerlei korrespondierende Verpflichtung zur Offenlegung des Namens bestünde.

Auch der bestehende Auskunftsanspruch nach § 101 UrhG würde in seiner heutigen

Fassung nicht greifen, da er nach Absatz 2 nur bei gewerblichen Anbietern gilt. Der private Betreiber könnte sich also stets wie folgt exkulpieren: *„Mir sind zwar alle Nutzer namentlich bekannt, da ich nur namentlich Bekannten den Zugang gewähre. Wer diese Personen sind, muss ich jedoch nicht mitteilen und tue dies daher auch nicht."*

Es ist daher zu fordern, dass eine Störerhaftung für Rechtsverletzungen Dritter nur dann entfällt, wenn der WLAN-Betreiber dem Verletzten die Identität des für die Rechtsverletzung vermeintlich verantwortlichen Nutzers mitteilt (Name und Anschrift oder Mobilfunknummer).

Entsprechende Vorschläge wurden u.a. bereits von **Prof. Dr. Gerald Spindler** in den zuständigen Ausschüssen und Arbeitsgruppen vorgebracht. Hierauf sollte hingewiesen werden:

> *„**Öffentliche WLANs, Störerhaftung ist ja bereits adressiert worden: Meines Erachtens sollte man hier eine heilige Kuh nicht aufrechterhalten, nämlich Stichwort Anonymität. Das heißt es ist heute schon Praxis, dass wenn man WLANs hat, an Flughäfen etc., dass man einfach nur eine Telefonnummer angibt, irgendwas mit dem man sich identifizieren muss und dann sollte der Grundsatz der Subsidiarität eingreifen. Das heißt, wenn ich den jeweiligen Störer, den wirklichen Rechtsverletzer ausfindig machen kann, dann sollte der Access-Provider nicht haften.** [...] **Also Subsidiarität plus sozusagen Identifizierungspflichten**."*
> (Prof. Dr. Gerald Spindler, 25. Sitzung des Ausschusses Digitale Agenda vom 03.12.2014, Öffentliches Fachgespräch zum Thema „Stand der Urheberrechtsreform auf deutscher und europäische Ebene und weiteres Vorgehen beim Leistungsschutzrecht für Presseverlage", **zweite** Fragerunde)

> *„**Wenn Sie sich UPC Telekabel vom EuGH anschauen, den Art. 8 Abs. 3 der Enforcement Richtlinie** [Anm. gemeint ist die InfoSoc Richtlinie] eben über diese Schiene, **ist es schwierig nur die Privaten hier irgendwie zu privilegieren. Die Richtlinie sieht hier überhaupt keine Differenzierung vor und dementsprechend hat der EuGH auch keinerlei Differenzierung vorgesehen, was Sperrverfügungen gegen Access-Provider angeht und hier geht es eben um die Störerhaftung.** Das heißt, das wird sehr sehr schwierig für Sie, in diesem Bereich europarechtskonform in irgendeiner Weise zu handeln. Das heißt, da kommen wir nicht darum herum, dass es also rudimentär zumindest in der Art eine Störerhaftung gibt. **Man kann sie versuchen, national näher auszuziselieren und die Vorschläge hatte ich vorhin versucht, schon einmal klarzumachen. Das heißt also einmal eine Identifizierungspflicht, wenn die da ist, raus aus der Störerhaftung, mit einer Subsidiarität**."*
> (Prof. Dr. Gerald Spindler, 25. Sitzung des Ausschusses Digitale Agenda vom 03.12.2014, Öffentliches Fachgespräch zum Thema „Stand der Urheberrechtsreform auf deutscher und europäische Ebene und weiteres Vorgehen beim Leistungsschutzrecht für Presseverlage", **dritte** Fragerunde)

> *„Hostprovider-Betreiber, die*
> *(A) die Durchleitung oder Speicherung von Inhalten auf Host-Provider-Ebene im Rahmen ihrer Plattform oder ihres Dienstes in öffentlichen Räumen ermöglichen,*
> *(B) die Anonymisierung ihrer Nutzer gewährleisten, und dann*
> *(C) die Verantwortlichkeit für die Inhalte dieser Nutzer ablehnen,*
> *erzeugen Verantwortungsdiffusion für die nutzergenerierten Inhalte auf ihren Plattformen.*
> *Es gilt also zunächst, die Kombination aus (A), (B) und (C) auszuschließen. [...]*
> ***Ein Portal, welches demnach seine Nutzer in öffentlichen Räumen anonymisiert, haftet selbst nach presserechtlichen Maßstäben. Hiermit werden Leaking-Portale rechtssicher ermöglicht, sie haben aber***

umfangreiche Prüfpflichten für die Inhalte, die sie veröffentlichen, und können nicht ungeprüfte vertrauliche Dokumente einfach im Internet veröffentlichen, und gleichzeitig eine Haftungsfreistellung erwarten. Ein Portal, welches seine Nutzer dagegen nur pseudonymisiert und auf Anfrage bei rechtsverletzenden Inhalten die Identität des Nutzers vermittelt, sowie rechtsverletzende Inhalte weiterhin löscht, profitiert weiterhin von der Haftungsprivilegierung durch das TMG.

[…]

Der ‚A/B/C-Approach' fordert also ein neues kontextuelles Unterscheidungskriterium in der Haftungsfrage: Nämlich, ob die Anonymität des Informationen oder Inhalte veröffentlichenden Nutzers auf Hostprovider-Plattformen durch das Portal gewährleistet wird oder nicht. *Als Referenz sei hier das Auktionshaus eBay genannt, das Rechtssicherheit auf seiner Plattform auch durch die gezielte Verwaltung bzw. Aufhebung der Pseudonymität ihrer Mitglieder bei Rechtsverletzungen herstellt. Im Gegensatz zu den meisten Hostprovidern unternimmt eBay erhebliche proaktive Anstrengungen, um rechtsverletzende Auktionen aus seinem Angebot zu entfernen.*

Es entstünden bei Implementierung dieses Ansatzes im TMG also zwei neue Haftungsrahmen für Hostprovider, die entweder zumindest rudimentäre Verwaltungsmaßnahmen erforderlich machen, bzw. den Hostbetreiber verantwortlich für die von ihm verbreiteten Inhalte macht, dafür aber anonyme Kommunikation und Whistleblowing rechtssicher ermöglichen. Die Kombination dieser Haftungsrahmen würden der grassierenden Verantwortungsdiffusion im Netz entgegenwirken, und gleichzeitig mehr Rechtssicherheit im Umgang mit nutzergenerierten Inhalten schaffen. Verantwortlichkeit für Inhalte würde i.R.d. „A/B/C-Approach" nach einem klaren Schema aufgeteilt: Wer aktiv anonymisiert, haftet selber, wobei der Host die freie Entscheidung hat, welche Haftungsverantwortung er wählt. *Dies würde ein grundlegendes strukturelles Fundament schaffen, auf dem Durchsetzung von Persönlichkeitsrechten, Urheberrechten oder Jugendmedienschutz im Internet überhaupt erst aufbauen können. Ohne ein sinnvolles strukturelles Fundament treten dagegen entweder Durchsetzungsdefizite oder Überregulationen auf.* ***Die zusätzlichen Vorteile wären erheblich, denn wenn die Identifikation von Nutzern nicht mehr auf technischer Ebene stattfände, wäre z.B. ein ungehinderter Zugang zu öffentlichem W-LAN prinzipiell möglich. Auch die Störerhaftungsproblematik für W-LAN könnte weitgehend entfallen****."*

(Stefan Herwig, Austarierung von Anonymität und Verantwortung im Netz, ZD 2012, 558)

(2) Ungerechtfertigte Begünstigung geschäftlicher WLAN

Die Registrierungs- und Auskunftspflicht (als „Exkulpationsvoraussetzung") sollte zudem für sämtliche WLAN-Betreiber gelten. Dies würde eine Abgrenzung zwischen privatem und geschäftsmäßig betriebenem WLAN überflüssig machen. Es gibt auch keine Rechtfertigung, geschäftsmäßige und öffentlich-rechtliche Betreiber besser zu stellen als private. Insbesondere ist die Annahme der Entwurfsverfasser unzutreffend, die Gefahren illegaler Nutzung seien über privat betriebene WLAN deutlich höher als über geschäftsmäßig bereitgestellte.

„Grund für diese zusätzliche Anforderung ist die Tatsache, dass die Möglichkeit, dass ein Nutzer im geschützten Bereich bzw. in Privaträumen unbemerkt Straftaten wie Kinderpornografie oder Urheberrechtsverletzungen begeht, erheblich größer ist als im öffentlichen Raum. Dort muss der rechtswidrig Handelnde stets damit rechnen, vom Diensteanbieter oder anderen Personen beobachtet bzw. entdeckt zu werden. Der geschäftsmäßig handelnde Diensteanbieter hat zudem grundsätzlich die Möglichkeit, einem Nutzer, der entgegen seiner Zusicherung gem. Absatz 4, Ziffer 2., rechtswidrige Handlungen begeht, die weitere Nutzung des WLAN zu untersagen. Die namentliche Kenntnis des

> *Nutzers ist daher verzichtbar. Hierdurch wird dem Interesse des Nutzers am Schutz seiner personenbezogenen Daten Rechnung getragen und im Übrigen eine praktikable Handhabung ermöglicht. Demgegenüber soll der private Anschlussinhaber nur dem oder den Nutzern sein WLAN überlassen, die er kennt. Er haftet folglich dann nicht als Störer, wenn er darlegen kann, dass er nur denjenigen Nutzern sein WLAN zur Verfügung gestellt hat, die er zumindest namentlich kennt. Sodann kann der Anschlussinhaber dem ihm bekannten Nutzer sein WLAN-Netz mündlich oder (sozialadäquat) konkludent überlassen."* (Referentenentwurf vom 11.03.2015, S. 13)

Der Referentenentwurf übersieht bereits, dass öffentliche WLAN auch von Privaträumen aus genutzt werden können. Der **Nutzer muss sich nämlich nicht zwingend selbst in der Öffentlichkeit befinden**, um ein öffentliches WLAN zu nutzen, sondern kann auch von einer an ein Lokal angrenzenden Wohnung, einem parkenden Auto etc. auf das WLAN zugreifen.

Unabhängig davon sieht aber auch im *„öffentlichen Raum"* in der Regel niemand über die Schulter, zumal z.B. bei Internettauschbörsen der Inhalt der übertragenen Dateien auf dem Bildschirm überhaupt nicht ersichtlich ist. Ein Dritter würde somit eine Urheberrechtsverletzung selbst dann nicht erkennen, wenn er dem Nutzer tatsächlich über die Schulter schauen würde. Sämtliche in der Öffentlichkeit (und auch im Freien) nutzbaren WLAN-Angebote bieten damit ausreichend Privatsphäre, um gefährlichste Anwendungen zu nutzen. Dies wird auch dadurch belegt, dass mindestens 10 % sämtlicher P2P-Rechtsverletzungen gerade über derartige öffentliche WLAN-Zugänge begangen werden.[9]

Im Ergebnis ist der **„Schutz" vor Entdeckung bei Nutzung eines geschäftsmäßigen bzw. öffentlichen WLAN somit sogar größer** als bei privaten WLAN, deren Nutzerkreis kleiner und damit überschaubarer ist. Bei privaten WLAN muss ein Verletzer stets damit rechnen, dass er zumindest in seinem privaten Umfeld (Familienmitglieder, Partner u.ä.) regelmäßig enttarnt wird, wenn sich ein Rechteinhaber oder die Staatsanwaltschaft (z.B. wegen Straftaten wie Kinderpornographie) an einen ermittelten Anschlussinhaber wendet. Gerade hier greift also das Element der sozialen Kontrolle, d.h. der Überprüfung sozialadäquaten Verhaltens durch Dritte. Bei einem geschäftsmäßig betriebenen bzw. öffentlichen WLAN geht der einzelne Nutzer hingegen regelmäßig in der großen Masse der anderen Nutzer unter. Der rechtswidrig Handelnde muss erst dann mit einer Entdeckung und Sanktionen rechnen, wenn der Betreiber seinen Namen und seine Anschrift (bzw. alternativ dessen Mobilfunknummer) registriert und zudem Maßnahmen ergreift, um Rechtsverletzungen einem Nutzeraccount zuordnen und später beauskunften zu können.

Der Referentenentwurf weist zudem darauf hin, dass der geschäftsmäßig handelnde Diensteanbieter die Möglichkeit hätte, einem Nutzer die Nutzung zu untersagen, wenn dieser rechtswidrige Handlungen begeht. Hierbei übersieht der Referentenentwurf jedoch, dass auch um eine derartige „Nutzungsuntersagung" aussprechen und durchsetzen zu können, der Betreiber die Rechtsverletzung einem Nutzer oder zumindest dessen Endgerät **überhaupt zuordnen** können muss. Auch insofern ist also eine Pflicht zur Registrierung und Identifizierung der Nutzer geboten.

[9] Vgl. hierzu unter A.I.3.

Schließlich ergibt sich auch aus der Entscheidung des Bundesgerichtshofs „Sommer unseres Lebens“[10], dass eine Besserstellung geschäftsmäßiger WLAN-Betreiber beim Umfang der Prüfpflichten nicht geboten ist. So hat der Bundesgerichtshof in seinen Entscheidungsgründen mehrfach zum Ausdruck gebracht, dass seine Ausführungen „**auch** für eine Privatperson“ gelten. A maiore ad minus müssen diese somit gleichermaßen auch auf geschäftsmäßige WLAN-Betreiber Anwendung finden.

(3) Registrierung und Auskunftspflicht mit geringstem Aufwand erfüllbar

Eine Pflicht zur Registrierung und Identifizierung der Nutzer ist für die Betreiber öffentlicher WLAN bereits heute mit geringstem Aufwand erfüllbar und muss daher generell als zumutbar gelten. Die Identifizierung entspricht dabei grundsätzlich der Zuordnung von IP-Adressen zu einem Festnetzanschluss, deren Zulässigkeit allgemein anerkannt ist und von Access-Providern tagtäglich praktiziert wird. Eine Speicherung oder gar Kontrolle von Inhalten der Kommunikation ist hierfür nicht erforderlich.

Geeignete Systeme, die WLAN-Betreibern die **Registrierung und Identifizierung ihrer Kunden/Nutzer ermöglichen**, sind bereits **für wenige hundert Euro** erhältlich. Zahlreiche Unternehmen (Hotels, Gaststätten etc.) setzen entsprechende Systeme auch heute schon ein.

Exemplarische Angebote:

- Envel WLAN-BS (http://www.envel.com/Produkte/WLAN-BS/Envel-WLAN-Hotspot),
- Contello Hotspot (http://www.wlanticket.de/die-professionelle-hotspot-wlanloesung.html) und
- ZYXel Basic (http://www.zyxel-hotel.de/hotellerie/loesungen/basic.html).

Alternativ können Hotspots auch mittels **Komplettlösungen der klassischen Access-Provider** bereitgestellt werden. Hierbei wird dem Hotspot-Anbieter von seinem Access-Provider zum Festnetzanschluss entsprechende Hardware für die Bereitstellung eines Hotspots zur Verfügung gestellt. Der Access-Provider übernimmt dabei die Registrierung der Nutzer sowie weitere erforderliche Sicherungsmaßnahmen (insbesondere auch die Erteilung von Auskünften nach § 101 Absatz 2 UrhG). Die für den „Betreiber“ eines solchen Hotspots anfallenden Kosten liegen in der Regel bei **unter 50 Euro im Monat**.

Exemplarische Angebote:

- Kabel Deutschland WLAN-Hotspot für Unternehmen (http://www.kabeldeutschland.de/wlan-hotspots/hotspot-fuer-ihr-business.html),
- Telekom Hotspot Partnerprogramm (http://www.hotspot.de/content/partner.html) und
- BSkyB The Cloud (http://www.thecloud.eu/).

[10] BGH, 12.05.2010, Az. I ZR 121/08

3. Konkreter Formulierungsvorschlag

(1) Diensteanbieter sind für fremde Informationen, die sie in einem Kommunikationsnetz übermitteln oder zu denen sie den Zugang zur Nutzung vermitteln, nicht verantwortlich, sofern sie
1. die Übermittlung nicht veranlasst,
2. den Adressaten der übermittelten Informationen nicht ausgewählt und
3. die übermittelten Informationen nicht ausgewählt oder verändert haben.
Satz 1 findet keine Anwendung, wenn der Diensteanbieter absichtlich mit einem Nutzer seines Dienstes zusammenarbeitet, um rechtswidrige Handlungen zu begehen.
(2) Die Übermittlung von Informationen nach Absatz 1 und die Vermittlung des Zugangs zu ihnen umfasst auch die automatische kurzzeitige Zwischenspeicherung dieser Informationen, soweit dies nur zur Durchführung der Übermittlung im Kommunikationsnetz geschieht und die Informationen nicht länger gespeichert werden, als für die Übermittlung üblicherweise erforderlich ist.
(3) Die vorstehenden Absätze gelten auch für Diensteanbieter nach Absatz 1, die Nutzern einen Internetzugang über ein drahtloses lokales Netzwerk zur Verfügung stellen.
(4) Diensteanbieter können wegen einer rechtswidrigen Handlung eines Nutzers nur dann nicht auf Unterlassung in Anspruch genommen werden, wenn sie sämtliche zumutbaren Maßnahmen ergriffen haben, um eine Rechtsverletzung durch Nutzer zu verhindern. Dies ist in der Regel der Fall, wenn der Diensteanbieter
1. angemessene Sicherungsmaßnahmen durch anerkannte Verschlüsselungsverfahren oder vergleichbare Maßnahmen gegen den unberechtigten Zugriff auf das drahtlose lokale Funknetz durch außenstehende Dritte ergriffen hat und
2. Zugang zum Internet nur dem Nutzer gewährt, der erklärt hat, im Rahmen der Nutzung keine Rechtsverletzungen zu begehen und
3. dem Verletzten Auskunft über den Namen und die Anschrift oder die Mobiltelefonnummer des Nutzers erteilt, der die rechtswidrige Information übermittelt hat.
Absatz 1 Satz 1 Halbsatz 2 sowie Absatz 1 Satz 2 gelten entsprechend.

Änderungen des § 10 TMG
– Haftungsverschärfung bei gefahrgeneigten Host-Providern –

§ 10 TMG – Speicherung von Informationen

(1) Diensteanbieter sind für fremde Informationen, die sie für einen Nutzer speichern, nicht verantwortlich, sofern

1. sie keine Kenntnis von der rechtswidrigen Handlung oder der Information haben und ihnen im Falle von Schadensersatzansprüchen auch keine Tatsachen oder Umstände bekannt sind, aus denen die rechtswidrige Handlung oder die Information offensichtlich wird, oder
2. sie unverzüglich tätig geworden sind, um die Information zu entfernen oder den Zugang zu ihr zu sperren, sobald sie diese Kenntnis erlangt haben.

Satz 1 findet keine Anwendung, wenn der Nutzer dem Diensteanbieter untersteht oder von ihm beaufsichtigt wird.

(2) Die Kenntnis von Tatsachen oder Umständen nach Absatz 1, aus denen die rechtswidrige Handlung oder die Information offensichtlich wird, wird vermutet, wenn es sich bei dem angebotenen Dienst um einen besonders gefahrgeneigten Dienst handelt. Ein besonders gefahrgeneigter Dienst liegt in der Regel dann vor, wenn:

a) die Speicherung oder Verwendung der weit überwiegenden Zahl der gespeicherten Informationen rechtswidrig erfolgt oder

b) der Diensteanbieter durch eigene Maßnahmen gezielt die Gefahr einer rechtsverletzenden Nutzung fördert oder

c) in vom Diensteanbieter veranlassten Werbeauftritten mit der Nichtverfolgbarkeit bei Rechtsverstößen geworben wird oder

d) keine Möglichkeit besteht, rechtswidrige Inhalte durch den Berechtigten entfernen zu lassen.

I. Einschränkung des Haftungsprivilegs bei Schadenersatzansprüchen

Mit § 10 Absatz 2 TMG-E soll das Haftungsprivileg für Schadenersatzansprüche gegenüber „besonders gefahrgeneigten“ Host-Providern eingeschränkt werden.

Die Begründung zum Referentenentwurf deutet dabei an, dass sich besonders gefahrgeneigte Host Provider generell nicht mehr auf ein Haftungsprivileg nach § 10 TMG berufen können sollen:

> *„Schließlich leiden Inhaber geistiger Eigentumsrechte zunehmend darunter, dass mit Hilfe des Internet Rechtsverletzungen leichter und in größerem Ausmaß begangen werden können. Vor diesem Hintergrund* ***erscheint es nicht gerechtfertigt, dass Plattformen, deren Geschäftsmodell im Wesentlichen auf der Verletzung geistiger Eigentumsrechte aufbaut, sich auf das Haftungsprivileg für Hostprovider nach dem TMG berufen können****.“* (Referentenentwurf vom 11.03.2015, S. 2)
>
> *„Im Koalitionsvertrag wurde ferner vereinbart, dass sich Betreiber von Plattformen, deren Geschäftsmodell im Wesentlichen auf der Verletzung von Urheberechten beruht,* ***nicht auf das Haftungsprivileg für Host-Provider berufen können sollen*** *(Seite 133 des Koalitionsvertrages). Auch dies stellt der Gesetzentwurf klar.“* (Referentenentwurf vom 11.03.2015, S. 6)

> ***„Schließlich wurde ebenfalls im Koalitionsvertrag vereinbart, dass Plattformen, deren Geschäftsmodell im Wesentlichen auf der Verletzung von Urheberrechten aufbaut, sich nicht länger auf das Haftungsprivileg, das sie als sog. Host-Provider genießen (§ 10 TMG), berufen können sollen*** *(S. 93 des Koalitionsvertrages). Bei der Umsetzung der Forderung sind die europarechtlichen Vorgaben zu beachten. Nach Art. 14 Abs. 1 Buchst. a) der Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte*

rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr") haftet ein Host-Provider nicht für die im Auftrag eines Nutzers gespeicherten Informationen, sofern er „keine tatsächliche Kenntnis" von der Rechtsverletzung hat. Von Kenntnis ist nach dem vorliegenden Gesetzentwurf insbesondere dann auszugehen, wenn das Geschäftsmodell weit überwiegend auf der Verletzung von z.B. Urheberrechten aufbaut, ***was bei Auslegung des geltenden Rechts auch heute schon der Fall sein dürfte. Dies unzweideutig festzulegen, bezweckt der Gesetzentwurf.****"* (Referentenentwurf vom 11.03.2015, S. 7)

„Darüber hinaus benennt das Gesetz verschiedene Konstellationen, bei deren Vorliegen von Kenntnis des Host-Providers von einer rechtswidrigen Handlung ausgegangen werden kann."
(Referentenentwurf vom 11.03.2015, S. 8)

„Bei bestimmten Diensten ***kann nach der allgemeinen Lebenserfahrung davon ausgegangen werden, dass dem Diensteanbieter ausreichend viele Tatsachen oder Informationen bekannt sind, aus denen die rechtswidrige Handlung oder die Information offensichtlich wird.*** *Diese Dienste bezeichnet die Rechtsprechung mittlerweile als ‚gefahrgeneigte Dienste'. Um hier für mehr Rechtsklarheit und Rechtssicherheit zu sorgen, zählt das Gesetz, dieser folgend, Fallkonstellationen auf, bei denen von einem* ***besonders gefahrgeneigten*** *Dienst ausgegangen werden kann. Hierdurch trägt die Bundesregierung dem Umstand Rechnung, dass bei Urheberrechtsverletzungen im Internet ein Vorgehen der betroffenen Inhaber des Rechts auf geistiges Eigentum gegen Diensteanbieter, deren Geschäftsmodelle im Wesentlichen auf Rechtsverletzungen beruht, vielfach schwierig, wenn nicht unmöglich ist."* (Referentenentwurf vom 11.03.2015, S. 14)

Nach dem Gesetzeswortlaut wird jedoch lediglich formuliert, dass bei einem besonders gefahrgeneigten Dienst die Kenntnis von Tatsachen oder Umständen i.S.d. § 10 Absatz 1 TMG, aus denen eine rechtswidrige Handlung oder Information offensichtlich wird, vermutet wird.

Diese Vermutung sorgt grundsätzlich zwar für eine Beweiserleichterung, die Kenntnis bleibt jedoch widerlegbar. Sollte für die Widerlegung der Kenntnis zudem der bloße Vortrag genügen, dass der Host-Provider „keine Kenntnis habe", hätte die Neuregelung keinen echten Mehrwert. Die Vermutung sollte daher als „unwiderlegbar" normiert werden.

Dies wäre gerade in den im Entwurf aufgezählten Fallkonstellationen auch vertretbar:

„Von einem besonders gefahrgeneigten Dienst ist im Einzelnen bei folgenden Konstellationen auszugehen:
a) Wenn die Speicherung oder Verwendung der weit überwiegenden Zahl der gespeicherten Informationen rechtswidrig erfolgt
Werden ganz überwiegend Informationen mit rechtswidrigen Inhalten gespeichert, bzw. die ganz überwiegende Zahl der gespeicherten Informationen in rechtswidriger Weise verwendet, ***spricht die allgemeine Lebenserfahrung dafür, dass dem Diensteanbieter dies auch bekannt ist.*** *Entscheidend ist hierbei nicht die absolute Zahl der rechtswidrigen Inhalte, sondern der relative Anteil der rechtswidrigen Inhalte. Liegt dieser bei weit über 50% der gespeicherten Informationen kann davon ausgegangen werden, dass dem Diensteanbieter dies nicht verborgen geblieben ist.*
b) der Diensteanbieter durch eigene Maßnahmen gezielt die Gefahr einer rechtsverletzenden Nutzung fördert
Fördert der Dienstanbieter gezielt die Gefahr einer rechtswidrigen Nutzung, ***kann ebenfalls Kenntnis vermutet werden.*** *Entscheidend ist, dass die rechtswidrige Nutzung gezielt gefördert wird. Die Maßnahmen und Angebote des Diensteanbieters müssen also zielgerichtet so beschaffen sein, dass die Gefahr einer rechtswidrigen Nutzung gefördert wird. Nicht ausreichend ist, wenn Maßnahmen lediglich auch die Gefahr einer rechtsverletzenden*

Handlung fördern.
c) in vom Diensteanbieter veranlassten Werbeauftritten mit der Nichtverfolgbarkeit bei Rechtsverstößen geworben wird
Wird in der Werbung des Diensteanbieters zielgerichtet darauf hingewiesen, dass das Angebot so konstruiert ist, dass auch bei Rechtsverstößen keine Verfolgung droht, ***kann davon ausgegangen werden, dass der Diensteanbieter ebenfalls Kenntnis darüber hat,*** *dass sein Dienst in erheblichem Maße für rechtswidrige Handlungen genutzt wird.*
d) keine Möglichkeit besteht, rechtswidrige Inhalte durch den Berechtigten entfernen zu lassen
Diensteanbieter sind verpflichtet, rechtswidrige Inhalte zu entfernen, sobald sie Kenntnis hiervon erlangen. Der Berechtigte, z.B. ein Rechteinhaber, muss daher die Möglichkeit haben, den Diensteanbieter hiervon in Kenntnis zu setzen und der Diensteanbieter muss die Möglichkeit haben, den Inhalt dann zu entfernen. Auch wenn diese Möglichkeiten nicht bestehen, kann daher davon ausgegangen werden, dass der Diensteanbieter sich diesen Verpflichtungen bewusst entziehen will. ***Auch dies lässt darauf schließen, dass er Kenntnis von der Rechtswidrigkeit der Informationen hat****."* (Referentenentwurf vom 11.03.2015, S. 14 f.)

Gerade bei besonders gefahrgeneigten Diensten wäre zudem geboten, dass ein Haftungsprivileg von der Deanonymisierung des verantwortlichen Uploaders abhängt. Dies könnte dadurch erreicht werden, dass der besonders gefahrgeneigte Dienst die Vermutung – und damit die Schadenersatzhaftung für Rechtsverletzungen Dritter – grundsätzlich nur in den Fällen widerlegen kann, in denen er die Identität des verantwortlichen Uploaders offen legt. Zu diesem Zweck könnte der folgende Satz als Absatz 2 Satz 3 eingefügt werden:

„Die Vermutung kann nur dann widerlegt werden, wenn der besonders gefahrgeneigte Dienst Auskunft über den Namen und die Anschrift oder die Mobiltelefonnummer des Nutzers (Uploader) erteilt, der die rechtswidrige Handlung begangen oder die rechtswidrige Information gespeichert hat."

II. Keine Regelung zum „Diensteanbieter hinter dem Dienst"

Der Referentenentwurf zu § 10 TMG-E enthält auch keine klare Regelung zu weiteren Diensteanbietern, die ihrerseits den gefahrgeneigten Host-Providern Speicherplatz zur Verfügung stellen (Rechenzentren u.ä.).

Diese weiteren Diensteanbieter sollten jedoch ebenfalls von dem Haftungsprivileg ausgeschlossen werden, sofern sie Kenntnis von der Gefahrgeneigtheit des Dienstes haben. Anders als die meisten gegenüber den Nutzern auftretenden Host-Provider (Briefkastenfirmen), haben diese weiteren Diensteanbieter ihren Sitz oft in Europa und können daher auch tatsächlich in Anspruch genommen werden.

Björn Frommer
Rechtsanwalt