STELLUNGNAHME

An: Deutscher Bundestag,
Ausschuss für Wirtschaft und
Energie

Von: Dr. jur. Reto Mantz, Dipl.-Inf.,
Richter am Landgericht Frankfurt am Main

Datum: 22. Juni 2017

GESETZENTWURF DER BUNDESREGIERUNG: ENTWURF EINES DRITTEN GESETZES ZUR ÄNDERUNG DES TELEMEDIENGESETZES

A. ZUSAMMENFASSUNG

- Die Neuregelung der Haftungsprivilegierung für Anbieter von öffentlich zugänglichen WLANs ist grundsätzlich begrüßenswert. Angesichts der derzeitigen Rechtsprechungslage ist eine zeitnahe Novellierung zwingend erforderlich.

- Sowohl in § 7 als auch in § 8 TMG sind allerdings noch Änderungen vorzunehmen, um die gesetzgeberischen Ziele, insbesondere der Rechtssicherheit zu erreichen und die Vereinbarkeit mit europäischen Vorgaben herzustellen:

  - Mit Blick auf § 8 TMG verbleiben aufgrund gesetzestechnischer Mängel Unklarheiten, die der beabsichtigten Rechtssicherheit im Wege stehen können.
  - Zu § 7 Abs. 4 TMG ist festzuhalten, dass Websperren generell äußerst problematisch sind. In § 7 Abs. 4 TMG sind weitere Verfahrensmaßnahmen wie ein Richtervorbehalt und die Einbindung der durch die Websperren Betroffenen vorzusehen, um den Bedenken wenigstens teilweise zu begegnen. § 7 Abs. 4 TMG ist falsch verortet und sollte in § 8 Abs. 5 TMG verschoben werden.

- Die geplanten Regelungen dürften aufgrund des beabsichtigten Ausgleichs der sich widerstreitenden Interessen europarechtlich zulässig sein.

B. HINTERGRUND, STAND DER GESETZGEBUNG UND RECHTSPRECHUNG

Es besteht allgemeine Einigkeit darüber, dass die Verbreitung von öffentlichen WLANs und damit einhergehend ein möglichst flächendeckender Zugang zu Informationsdiensten und –

infrastrukturen wünschenswert ist. Seit den 2000er Jahren verbreiten sich WLANs insbesondere bei Privatpersonen, aber auch bei Unternehmen stark. Die WLANs von Privaten waren häufig ungesichert und ermöglichten praktisch jedem einen einfachen und unkomplizierten Zugang zum Internet.

Dieser positive Anfangsbefund gilt bereits seit Jahren nicht mehr. Im Gegenteil: Deutschland liegt bei der Verbreitung öffentlicher WLANs mittlerweile weit zurück. Ende 2014 standen in Deutschland gerade einmal rund 15.000 freie, öffentliche WLAN-Hotspots zur Verfügung, das entsprach einer Quote von rund 1,9 Hotspots pro 10.000 Einwohner. Südkorea wies zu diesem Zeitpunkt bspw. eine Quote von über 37 WLAN-Hotspots pro 10.000 Einwohner auf.[1] Gleichzeitig betont die deutsche und europäische Politik seit Jahren die hohe Bedeutung flächendeckenden Breitbandzugangs inklusive der Verbreitung öffentlicher WLANs.

Die wesentliche Ursache für die geringe Verfügbarkeit von öffentlich zugänglichen WLANs ist bereits häufig dargestellt worden: Insbesondere zeichnet die bestehende Rechtsunsicherheit im Hinblick auf die Haftung des Betreibers für die Handlungen seiner Nutzer, zurückgehend auf verschiedene Gerichtsurteile,[2] hierfür verantwortlich. In diesen frühen Entscheidungen spielte die Haftungsprivilegierung in § 8 TMG, wonach derjenige, der Nutzern den Zugang zum Internet ermöglicht, für Handlungen seiner Nutzer nicht haften soll, allerdings jeweils keine Rolle. Dass § 8 TMG dem Grunde nach Anwendung auch auf WLANs findet, war in der juristischen Literatur nie umstritten.[3] Dennoch war und ist § 8 TMG (und dessen Anwendung in der Rechtsprechung) Kernpunkt der weiterhin bestehenden Rechtsunsicherheit bezüglich der Haftung des Betreibers eines öffentlich zugänglichen WLANs.

Die Politik griff die Thematik der Haftung bei WLANs auf, nachdem der Digitale Gesellschaft e.V. 2012/2013 einen konkreten Gesetzesentwurf veröffentlichte. Dieser wurde zwar im Bundestag eingebracht, letztlich aber abgelehnt. Ende 2013 vereinbarten die Regierungsparteien im Rahmen ihres Koalitionsvertrages, dass in der folgenden Legislaturperiode ein Gesetzesentwurf angestrebt werden solle.

Auch auf europäischer Ebene wurde das Potenzial der flächendeckenden Verbreitung von WLANs erkannt, wobei die Diskussion um die Haftung hier keine Rolle spielte. 2009 erklärte die EU-Kommission: „Europe loves Wi-Fi“ und legte im Entwurf für eine Verordnung zur Schaffung eines einheitlichen europäischen Binnentelekommunikationsmarktes Vorschriften zur Förderung der Verbreitung von WLANs vor, die allerdings ebenfalls nicht verabschiedet wurden.

---

[1] eco Microresearch, November 2014, https://www.eco.de/wp-content/blogs.dir/eco-microresearch_verbreitung-und-nutzung-von-wlan.pdf.

[2] LG Hamburg MMR 2006, 763; BGH MMR 2010, 565 – Sommer unseres Lebens m. Anm. *Mantz*.

[3] Eingehend *Sassenberg/Mantz*, WLAN und Recht, 2014, Rn. 211 m.w.N.

Im Jahr 2015 bereitete die Regierungskoalition einen Gesetzesentwurf[4] vor, der einerseits in § 8 Abs. 3 TMG-E eine Klarstellung enthielt, dass Betreiber von WLANs in den Anwendungsbereich von § 8 TMG fallen sollten. Nach § 8 Abs. 4 TMG-E sollte die Privilegierung unter bestimmten zusätzlichen Voraussetzungen auch für Unterlassungsansprüche gelten.[5] Der Gesetzesentwurf wurde vielfach kritisiert.[6] Beeinflusst wurde das Gesetzgebungsverfahren von einem Verfahren, das vor dem LG München I seinen Ausgang nahm: Das LG München I hatte dem EuGH in der Sache „McFadden" verschiedene Fragen zum Anwendungsbereich der Haftungsprivilegierung in § 8 Abs. 1 TMG vorgelegt.[7] Im März 2016 wurden in diesem Verfahren die Schlussanträge des Generalanwalts beim EuGH veröffentlicht,[8] der eine Haftung des Betreibers von öffentlich zugänglichen WLANs weitgehend verneinte. Unter dem Eindruck der Schlussanträge strich die Regierungskoalition die weiteren Voraussetzungen für eine Haftungsprivilegierung in § 8 Abs. 4 TMG-E und verzichtete im Gesetzeswortlaut auf eine Regelung zur Anwendung der Privilegierung auf Unterlassungsansprüche. Diese Absicht wurde lediglich in der Gesetzesbegründung verankert.[9] Diese Fassung, die im Grunde nur noch aus der Klarstellung in § 8 Abs. 3 TMG bestand, wurde beschlossen und veröffentlicht.[10] An der Neuregelung wurde insbesondere kritisiert, dass sie keine Rechtssicherheit schaffe. Die Änderung des Anwendungsbereichs der Privilegierung lediglich durch Klarstellung in der Gesetzesbegründung reiche nicht aus, da sich diese nicht im Wortlaut der Neuregelung wiederspiegele.[11]

Wenige Monate nach der Gesetzesnovellierung entschied der EuGH und folgte dem Generalanwalt in wesentlichen Punkten nicht.[12] Insbesondere stellte er fest, dass die E-Commerce-Richtlinie einer gerichtlichen (Unterlassungs-)Anordnung nicht im Wege stehe. Ferner liege kein Verstoß gegen die E-Commerce-Richtlinie vor, wenn vom Betreiber eines öffentlich zugänglichen WLANs verlangt werde, sein WLAN zu verschlüsseln.

Einen Tag vor der EU-Entscheidung gab die EU-Kommission bekannt, im Rahmen des Programms „WiFi4EU" 120 Millionen Euro für die Förderung öffentlicher WLANs

---

[4] BR-Drs. 440/15.

[5] Eingehend *Mantz/Sassenberg*, CR 2015, 298.

[6] *Mantz/Sassenberg*, CR 2015, 298; *Spindler*, CR 2016, 48.

[7] LG München I GRUR Int. 2014, 1166 – Bring mich nach Haus; dazu *Mantz/Sassenberg*, MMR 2015, 85.

[8] Generalanwalt beim EuGH BeckRS 2016, 80483 – McFadden; dazu *Mantz*, 17.3.2016, http://www.offenenetze.de/2016/03/17/schlussantraege-des-eugh-generalanwalts-im-fall-c-48414-mcfadden-und-das-deutsche-wlan-gesetz-eine-analyse.

[9] BT-Drs. 18/6745.

[10] BGBl. I 2016, 1766.

[11] Vgl. dazu *Franz/Sakowski*, CR 2016, 524 (527); *Spindler*, NJW 2016, 2449; *Jaeschke*, MMR 2016, 221 (222).

[12] EuGH EuZW 2016, 821 – McFadden; dazu *Mantz*, EuZW 2016, 817; *Obergfell*, NJW 2016, 3489.

bereitzustellen.[13] Am 29.5.2017 einigten sich die EU-Verhandlungsführer dann auf die Initiative WiFi4EU.[14] Die Initiative soll die Einrichtung kostenloser öffentlicher WLAN-Hotspots in Städten und Gemeinden in der ganzen EU auf öffentlichen Plätzen sowie in Parks, Krankenhäusern und sonstigen öffentlichen Räumen unterstützen.

In der Folge nahmen das OLG Düsseldorf und das KG Berlin an, dass Betreiber von WLANs grundsätzlich auf Unterlassung in Anspruch genommen werden könnten.[15] Auf dieser Grundlage ist der Status Quo der Haftung beim Betrieb von öffentlichen WLANs derzeit als negativ anzusehen. Während bisher eine Haftung in der Regel verneint wurde, haben nunmehr zwei Obergerichte eine Haftung angenommen bzw. nicht ausgeschlossen. Die derzeitige Lage ist daher geeignet, den weiteren Aufbau und Betrieb von öffentlichen WLANs zu behindern. Eine Novellierung tut daher dringend not.

C. STELLUNGNAHME

Im folgenden sollen die Regelungen des Gesetzesentwurfs bewertet werden. Dabei soll der Schwerpunkt auf die Frage gerichtet werden, ob der Entwurf dem übergeordneten Ziel – Rechtssicherheit – gerecht wird.

I. Wesentlicher Inhalt der geplanten Änderungen

Der Gesetzesentwurf sieht im Kern zwei wesentliche Änderungen des TMG vor:

- § 8 Abs. 1 S. 2 TMG soll eine Klarstellung enthalten, dass die Privilegierung in § 8 Abs. 1 TMG sich (auch) auf Unterlassungs- und Beseitigungsansprüche bezieht und für die Geltendmachung und Durchsetzung solcher Ansprüche keine Kostenerstattung geschuldet ist. § 8 Abs. 4 TMG enthält zudem die Regelung, dass Anbieter von WLANs „von einer Behörde“ nicht zur Einstellung des Dienstes oder der Gewährung des Zugangs nur bei Registrierung und Eingabe eines Passworts verpflichtet werden können.
- Nach § 7 Abs. 4 TMG wird gegen Anbieter von WLANs ein Anspruch auf Einrichtung von Websperren geschaffen.

II. Bewertung

1. Begrenzung der Haftung, § 8 Abs. 1 S. 2 TMG

Die Neuregelung zielt insbesondere auf eine Ausweitung der Privilegierung in § 8 Abs. 1 TMG auch auf eine Störerhaftung des Anbieters des WLANs ab.

---

[13] WiFi4EU, https://ec.europa.eu/digital-single-market/en/wifi4eu-kostenloses-wlan-fur-alle; Factsheet zu WiFi4EU, 14.9.2016, https://ec.europa.eu/digital-single-market/en/news/factsheet-wifi4eu.

[14] http://europa.eu/rapid/press-release_IP-17-1470_de.htm.

[15] OLG Düsseldorf, Urt. v. 16.03.2016 – I-20 U 17/16; KG Berlin, Urt. v. 08.02.2017 – 24 U 117/15.

a. Haftungsausschluss

Die Begrenzung der Haftung ist durchweg zu begrüßen. Die Regelung in § 8 Abs. 1 S. 2 TMG erscheint insoweit klar: Unterlassungs- und Beseitigungsansprüche sind ebenso ausgeschlossen wie Ansprüche auf Schadensersatz.[16] Als Ausgleich für diesen Ausschluss soll der Anspruch auf Websperren nach § 7 Abs. 4 TMG etabliert werden.

Leider ist dieses Ergebnis nur nach Auslegung nach den Grundsätzen der Systematik und des gesetzgeberischen Willens im Kontext ermittelbar. Daher verbleibt leider dennoch Unsicherheit. Diese beruht insbesondere auf der Regelung in § 8 Abs. 4 TMG. Nach § 8 Abs. 4 TMG sollen WLAN-Anbieter von einer Behörde nicht verpflichtet werden können, Nutzer zu registrieren, ein Passwort einzurichten oder das Anbieten des Dienstes einzustellen. Die Gesetzesbegründung offenbart nicht, welchen Grund diese Spezifizierung hat.[17] Es besteht die Gefahr, dass § 8 Abs. 4 TMG im Umkehrschluss so verstanden wird, dass eine Verpflichtung „durch ein Gericht" weiterhin möglich ist.[18] Dementsprechend hat der Bundesrat angeregt, die Worte „von einer Behörde" zu streichen.[19] Die Bundesregierung hat hierauf lediglich erwidert, dass dies das Ergebnis einer Ressortabstimmung gewesen sei.[20] Es bleibt also letztlich unklar, warum § 8 Abs. 4 TMG eine Einschränkung nur auf Behörden enthält und es bleibt unsicher, wie die Gerichte hierauf reagieren werden.

Dem Sinn und Zweck der Regelung in § 8 Abs. 1 S. 2 TMG folgend sowie entsprechend der Gesetzesbegründung sollte § 8 Abs. 4 TMG im Grunde nicht so verstanden werden, dass Gerichte (im Gegensatz zu Behörden) den Betreibern von WLANs Maßnahmen entsprechend § 8 Abs. 4 TMG auferlegen könnten. Insbesondere die Pflicht zur Verschlüsselung des WLANs und zur Registrierung der Nutzer entstammt nämlich dem „McFadden"-Urteil des EuGH.[21] Der Gesetzesentwurf weist mit Blick darauf ausdrücklich darauf hin, dass das Gesetz Ergebnis einer Abwägung ist. Dem Rechteinhaber soll auf der einen Seite der Unterlassungsanspruch genommen werden, auf der anderen Seite wird ihm aber der Anspruch auf Einrichtung von Websperren nach § 7 Abs. 4 TMG eingeräumt. Dies stellt aus Sicht der Regierungskoalition den Ausgleich der betroffenen Interessen sicher. Könnten Gerichte hingegen Maßnahmen nach § 8 Abs. 4 TMG anordnen, würde § 8 Abs. 1 S. 2 TMG praktisch negiert.[22]

---

[16] Die an einer Vorversion des Gesetzesentwurfs geäußerte Kritik, dass in § 7 Abs. 4 TMG-E durch ein „insbesondere" Unsicherheiten geschaffen werden, ist in der aktuellen Fassung des Gesetzesentwurfs berücksichtigt worden.

[17] Vgl. insoweit BT-Drs. 18/12202, S. 14.

[18] *Mantz*, http://www.offenenetze.de/2017/03/08/wlan-haftung-refe-zur-3-aenderung-des-tmg-in-der-kurzanalyse/; *Spindler*, CR 2017, 262 (267).

[19] So auch Stellungnahme des Bundesrats, BT-Drs. 18/12496, S. 3.

[20] So auch Stellungnahme des Bundesrats, BT-Drs. 18/12496, S. 3.

[21] EuGH EuZW 2016, 821 – McFadden.

[22] Vgl. ebenso *Spindler*, CR 2017, 262 (267).

Der Gesetzesentwurf sollte daher an diesem Punkt zwingend nachgebessert werden. Mindestens müsste der Gesetzgeber erklären, welchen Hintergrund die Begrenzung auf Anordnungen „von einer Behörde“ hat. Der Verweis auf Ressortabstimmungen hilft insoweit nicht.

Außerdem ist § 7 Abs. 4 TMG systematisch falsch verortet.[23] Auch dies birgt das Risiko, dass eine Auslegung von § 8 Abs. 1 S. 2 TMG nicht zu dem vom Gesetzgeber intendierten Ergebnis führt.

Unterbleiben Änderung oder Erläuterung, verbleibt erhebliche Rechtsunsicherheit, so dass die Gefahr besteht, dass das gesetzgeberische Ziel verfehlt wird.

b. Kosten

Nach § 8 Abs. 1 S. 2 Hs. 2 TMG werden alle Kosten für die Durchsetzung von Ansprüchen auf Schadensersatz, Unterlassung und Beseitigung ausgeschlossen. Diese Regelung ist der Rechtssicherheit ohne Zweifel förderlich. Da Ansprüche auf Unterlassung nach § 8 Abs. 3 TMG ausgeschlossen sind, kann der betroffene Rechteinhaber weder Abmahnkosten, noch Schadensersatz (wie schon zuvor) fordern. Auch Gerichtskosten muss der Anbieter des WLANs nicht tragen. Dies alles ist im Wesentlichen schon logische Folge des Ausschlusses von Ansprüchen nach § 8 Abs. 1 S. 2 TMG. Die Klarstellung ist jedoch sinnvoll und bedarf keiner Änderung.

2. Anspruch auf Websperren, § 7 Abs. 4 TMG

§ 7 Abs. 4 TMG sieht eine neue Anspruchsgrundlage für die Einrichtung von Websperren vor. Die Einführung von Websperren ist bereits in der Vergangenheit zu Recht vehement kritisiert worden.[24] So war im Jahr 2010 das Zugangserschwerungsgesetz trotz heftiger Kritik in Kraft getreten, aber im Ergebnis nie zur Anwendung gelangt.[25]

Zu berücksichtigen ist insoweit, dass einerseits der EuGH festgestellt hat, dass die E-Commerce-Richtlinie einer Anordnung zur Errichtung von Websperren nicht entgegen steht[26] und andererseits der BGH auf dieser Grundlage gegenüber Access Providern einen Anspruch auf Einrichtung von Websperren richterrechtlich verankert hat.[27] Die Regelung in § 7 Abs. 4 TMG kodifiziert diese Rechtsfortbildung, wobei auch die vom BGH dargelegten Voraussetzungen praktisch identisch geblieben sind.

---

[23] S.u. 2.b.dd.

[24] *Obergfell*, K&R 2017, 361 (363) m.w.N.

[25] Spindler/Schuster-*Gercke*, Recht der elektronischen Medien, 3. Aufl. 2015, § 184b StGB Rn. 6 ff; *Obergfell*, K&R 2017, 361 (362).

[26] EuGH GRUR 2014, 468 – UPC Telekabel/Constantin Film.

[27] BGH GRUR 2016, 268 – Access Provider II; BGH, Urt. v. 26.11.2015 – I ZR 174/14 – Access Provider I; kritisch *Heidrich/Heymann*, MMR 2016, 370

a. Inhalt der Regelung

§ 7 Abs. 4 TMG sieht vor, dass gegen den „Diensteanbieter nach § 8 Abs. 3“, also den Anbieter eines WLANs,[28] ein Anspruch auf „Sperrung der Nutzung von Informationen“ bestehen soll.

Erst dann kann er vom WLAN-Anbieter die Einrichtung von Websperren verlangen. Der Anspruch hängt weiter davon ab, dass ein „Dienst der Informationsgesellschaft von einem Nutzer in Anspruch genommen [wurde], um das Recht am geistigen Eigentum eines anderen zu verletzen.“ § 7 Abs. 4 TMG ist also ausdrücklich auf Rechte des geistigen Eigentums beschränkt. Beispielsweise wegen Persönlichkeitsrechtsverletzungen kann der Anspruch daher nicht geltend gemacht werden.[29]

Eine Sperrung soll zusätzlich zumutbar und verhältnismäßig sein, wobei im Einzelfall eine Interessenabwägung aller grundrechtlich geschützten Interessen sowie des Telekommunikationsgeheimnisses, „z.B. [durch] ein Gericht“, erfolgen muss. Overblocking soll verhindert werden.[30] Konkrete Maßnahmen nennt die Gesetzesbegründung nur beispielhaft: Portsperren, Webseitensperren (ggf. zeitlich befristet) und Datenmengenbegrenzungen.

Dem BGH folgend ordnet § 7 Abs. 4 TMG ausdrücklich eine Subsidiarität des Anspruchs an. Der Rechteinhaber muss daher zuvor vergeblich versucht haben, den Webseiteninhaber und den Host Provider zur Löschung zu bewegen.

b. Bewertung

Websperren sind generell als problematisch und sollten stets die Ausnahme darstellen.[31] Zu Recht wird insoweit die Gefahr von Zensur, Missbrauch und vorauseilendem Gehorsam angeführt.[32] Ob die durch den BGH eingeführte und nunmehr kodifizierte Subsidiarität dem ausreichend Rechnung trägt, darf bezweifelt werden.

Bei der derzeit vorgesehenen Regelung stellt sich insbesondere die Frage nach der Zumutbarkeit einzelner Maßnahmen, der Gefahr des vorauseilenden Gehorsams und der verfahrensrechtlichen Ausgestaltung. Außerdem ist die Regelung gesetzessystematisch fehlerhaft verortet.

aa. Zumutbarkeit

Im Hinblick auf die Zumutbarkeit ist zunächst zu berücksichtigen, wie öffentlich zugängliche WLANs typischerweise angeboten werden. Der Erfolg des Technikstandards WLAN ist

---

[28] Insoweit ist der Anwendungsbereich gegenüber der Vorfassung eingeschränkt worden, wobei es sich dort möglicherweise zuvor um ein Redaktionsversehen gehandelt hat.

[29] Dazu *Mantz*, EuZW 2016, 817 (820); *Spindler*, CR 2017, 262 (265).

[30] BT-Drs. 18/12202, S. 12.

[31] *Obergfell*, K&R 2017, 361 (363) m.w.N.

[32] Vgl. *Marberth-Kubicki*, NJW 2016, 1792.

nämlich weitgehend dem Umstand geschuldet, dass Einrichtung und Betrieb von WLANs einfach und günstig sind. Für das öffentliche Angebot eines WLANs ist im Grunde nicht viel mehr erforderlich als ein Internetanschluss und ein WLAN-Router, der bereits für rund € 25,- erworben werden kann. Millionenfach werden solche WLANs privat betrieben, vieltausendfach werden in solch kleinem Rahmen öffentlich zugängliche WLANs angeboten.

Als klassischer Fall ist insoweit ein kleines Café anzusehen, das ein WLAN zur Kundengewinnung und/oder Kundenbindung einsetzt.[33] Generell werden WLANs als ein wichtiges Instrument zur Kundengewinnung und Kundenbindung verstanden. Außerdem sollen durch die Neuregelung in §§ 7, 8 TMG auch von Privaten betriebene öffentliche WLANs erfasst werden.

Diesem „klassischen Fall" gegenüber stehen semi-professionelle oder professionelle Anbieter, wie z.B. Hotels, die eine Vielzahl von Nutzern und Zimmern ggf. in verschiedenen Gebäuden mit WLAN versorgen. Diese bauen entweder selbst eine größere Infrastruktur auf oder lassen dies durch entsprechende Unternehmen einrichten und/oder betreiben. Weiter werden WLANs von professionellen Anbietern wie der Deutschen Telekom oder anderen Telekommunikationsunternehmen angeboten und betrieben. Es ist leicht ersichtlich, dass hier andere Zumutbarkeitsmaßstäbe gelten können.

Die nach § 7 Abs. 4 TMG vorgesehenen Websperren können auf verschiedene Weisen realisiert werden.[34] Namentlich sind **DNS-Sperren, IP-Sperren, URL-Sperren und Verkehrsfilter** technisch möglich. Während OLG Hamburg[35] und OLG Köln[36] diese noch sämtlich als unzumutbar angesehen hatten, wobei insbesondere URL-Sperren und Verkehrsfilter unzulässige Eingriffe in das Fernmeldegeheimnis darstellen sollen, geht der BGH teilweise von deren grundsätzlicher Zulässigkeit aus.[37] Verkehrsfilter sind aber schon nach Art. 15 E-Commerce-Richtlinie unzulässig. Auch der BGH räumt ein, dass die Maßnahmen weitgehend unwirksam und leicht zu umgehen sind[38] und dass sie dazu führen, dass nicht nur rechtswidrige Inhalte blockiert werden, sondern auch andere, legale Inhalte („**Overblocking**").[39] Insoweit hat der BGH die Sperrung einer konkreten Webseite als zulässig erachtet, auf der der Anteil legaler Inhalte lediglich bei 4% lag.[40] Ein geringer Anteil

---

[33] Zu den Modellen *Sassenberg/Mantz*, (o. Fn. 3), Rn. 11 ff.

[34] Dazu *Heidrich/Heymann*, MMR 2016, 370 (371).

[35] OLG Hamburg GRUR-RR 2014, 140 – 3dl.am.

[36] OLG Köln GRUR 2014, 1081 – Goldesel.

[37] BGH GRUR 2016, 268 – Access Provider II.

[38] BGH GRUR 2016, 268 (Rn. 48) – Access Provider II; vgl. OLG Hamburg, MMR 2009, 631 – Usenet; dazu auch *Heidrich/Heymann*, MMR 2016, 370 (371).

[39] BGH GRUR 2016, 268 – Access Provider II; OLG Hamburg MMR 2009, 631 – Usenet; OLG Hamburg GRUR-RR 2014, 140 (147) – 3dl.am; OLG Köln GRUR 2014, 1081 – Goldesel.

[40] BGH GRUR 2016, 268 (Rn. 56) – Access Provider II.

an Overblocking soll danach hinnehmbar sein. Wo hier die Grenze zu ziehen ist und wie dies auf andere Sperren als Webseiten, z.B. Portsperren, zu übertragen ist, ist noch unklar.

Nach dem Gesetzesentwurf soll Overblocking im Rahmen einer Einzelfallabwägung verhindert werden. Einer Sperrung anhand von DNS- oder IP-Sperren ist das Overblocking aber praktisch immanent: Bei einer DNS-Sperre wird der Zugang zu einer ganzen Domain verhindert. Insoweit wäre im Einzelfall festzustellen, welche Inhalte unter der gesamten Domain enthalten sind. Nur wenn diesbezüglich der Anteil legaler Inhalte verschwindend gering wäre, könnte mit dem BGH eine Zulässigkeit dieses Overblockings angenommen werden. Bei IP-Sperren besteht die Gefahr, dass nicht nur eine Domain, sondern die Webangebote vieler Anbieter betroffen wären. Ferner kann sowohl bei DNS- wie bei IP-Sperren auch der Zugang zu nicht öffentlich zugänglichen Bereichen einer Webseite, beispielsweise firmeninterne Teile, die nur von Mitarbeitern eingesehen werden können, durch eine Websperre verhindert werden. Dadurch kann ggf. massiv in die Rechte Dritter eingegriffen werden, die mit der Rechtsverletzung nicht in Verbindung stehen.

Als überhaupt möglicherweise zumutbar kommen aufgrund des oben dargestellten Overblocking daher im Grunde nur **URL-Sperren** in Betracht. Diese wiederum weisen das Problem auf, dass durch einen Zwangsproxy Einblick in den Datenverkehr genommen werden muss, um erkennen zu können, welche konkrete Webseite abgerufen werden soll.[41] Außerdem ist die Einrichtung eines solchen Zwangsproxy aufwändig, da ein zusätzlicher Server eingerichtet und betrieben werden muss.[42] Auch sind URL-Sperren leicht zu umgehen. Bereits der Einsatz von verschlüsselten Abrufen macht URL-Sperren praktisch unmöglich, soweit nicht durch den Anbieter zusätzlich die Verschlüsselung gebrochen wird.

Wird sodann ein Anspruch nach § 7 Abs. 4 TMG erhoben, muss der Anbieter die URL prüfen, ob dort rechtsverletzende Inhalte hinterlegt sind und ob die Gefahr eines nicht mehr hinnehmbaren Overblocking besteht. Anschließend muss er die URL ggf. in seinem System eintragen. Dies alles verkompliziert sowohl Aufbau wie Betrieb von öffentlichen WLANs. Typischerweise kleinen WLAN-Anbietern ist bereits dieser Aufwand in aller Regel kaum zumutbar.[43] Ein weiteres Problem können gerade bei kleinen WLANs die Sperrlisten an sich sein. Die Gesetzesbegründung geht davon aus, dass Listen wie diejenige der Bundesprüfstelle für jugendgefährdende Schriften eingespielt werden könnten. Tatsächlich ist gerade bei günstigeren WLAN-Routern der Speicher des Geräts stark begrenzt. Dies begrenzt selbstverständlich auch die Anzahl der im Speicher vorhaltbaren, zu sperrenden URLs. Die umfassende Pflicht zu Websperren kann daher Einfluss gerade auf Kleinanbieter haben, da diese zur Erfüllung von Websperren auf größere, teurere und ggf. nur von professionellen Anbietern bedien- bzw. wartbare Geräte umsteigen müssten. Es ist zu befürchten, dass dies im Ergebnis die beabsichtigte Verbreitung von WLANs behindert.

---

[41] Eingehend dazu BGH GRUR 2016, 268 – Access Provider II.

[42] Dazu *Heidrich/Heymann*, MMR 2016, 370 (371).

[43] Ebenso AG Berlin-Charlottenburg CR 2015, 192; *Spindler*, GRUR 2016, 451 (459); *Obergfell*, K&R 2017, 361 (363); *Franz/Sakowski*, CR 2016, 524; *Grigorjew/Bile*, ZD-Aktuell 2017, 05621.

Die im Gesetzesentwurf angesprochenen **Portsperren** wiederum sind ebenfalls hochproblematisch. Auf der einen Seite sind sie sehr leicht zu umgehen:[44] Filesharing-Programme sehen in der Regel die Möglichkeit vor, die verwendeten Ports einzustellen. Zudem führt die Nichtverfügbarkeit der eingestellten Ports häufig nicht zur Verunmöglichung des Datenaustauschs, sondern verlangsamt ihn nur.[45] Auf der anderen Seite wird häufig vergessen, dass Tauschbörsen nicht per se nur zum illegalen Austausch urheberrechtlich geschützter Werke verwendet werden. Über Tauschbörsen werden auch Software-Updates, Linux-Distributionen etc. verteilt. Selbst Windows 10 verteilt seine Updates standardmäßig über Peer-to-Peer-Techniken und damit vergleichbar einer Tauschbörse. Die Einrichtung von Port-Sperren betrifft daher zwangsläufig auch legale Inhalte, so dass ein Overblocking nahe liegt.[46] Es bleibt aus diesem Grunde sogar unklar, ob Gerichte nach § 7 Abs. 4 TMG überhaupt Websperren anordnen würden. Verweise in der Begründung auf Portsperren sollten daher gänzlich entfernt werden.

Auch die neu in der Gesetzesbegründung erwähnten **Datenmengenbegrenzungen** sind grundsätzlich problematisch. Es ist insbesondere unklar, ob die Datenmengen nur einzelner Nutzer oder aller Nutzer eingeschränkt werden sollen, ferner ob nur „Volumenbegrenzungen" oder auch „Bandbreitenbegrenzungen" gemeint sein sollen oder ob gar eine Kombination gemeint ist, wie sie von Tarifen mit „Inklusivvolumen" beim Mobilfunk bekannt ist, dass also nach Erreichen der Volumengrenze die Bandbreite gedrosselt wird.

Datenmengenbegrenzungen sind zudem bereits begrifflich nicht unter die in § 7 Abs. 4 TMG genannte „Sperrung der Nutzung von Informationen" zu fassen. Selbst bei Einrichtung einer Datenmengenbegrenzung wären die betroffenen, rechtsverletzenden Inhalte daher weiterhin zugänglich, bei einer strengen Volumenbegrenzung zumindest solange die Datenmengengrenze nicht erreicht ist. Für den Anbieter des WLANs verbleibt zudem die Unsicherheit, wo die Grenze zu ziehen wäre. Mit der zunehmenden Nutzung von Videoportalen sind auch abseits von Filesharing eventuelle Volumengrenzen schnell erreicht. Bandbreitenbegrenzungen wiederum könnten dazu führen, dass bestimmte legale Internetangebote überhaupt nicht genutzt werden können, was wiederum ein Overblocking darstellen würde. WLANs werden schließlich als ein Weg angesehen, breitbandiges Internet flächendeckend zur Verfügung zu stellen.

Zudem sehen handelsübliche WLAN-Router auch einfache Datenmengenbegrenzungen nicht immer vor. Gerade bei Begrenzungen, die nur einzelne Nutzer betreffen sollen, also Volumengrenzen, wäre eine Art Ticketing-System z.B. anhand der MAC-Adresse des Nutzers erforderlich, die in dem für öffentliche WLANs erforderlichem Umfang nur bei professionellen, teuren WLAN-Systemen zur Verfügung stehen dürften.

---

[44] *Mantz/Sassenberg*, NJW 2014, 3537 (3542); *Grigorjew/Bile*, ZD-Aktuell 2017, 05621; vgl. auch Stellungnahme des Bundesrats BT-Drs. 18/12496, S. 2.

[45] Vgl. *Grigorjew/Bile*, ZD-Aktuell 2017, 05621.

[46] Ebenso Stellungnahme des Bundesrats BT-Drs. 18/12496, S. 2

Trotz all dieser Einwände erscheinen moderat eingesetzte und zeitlich begrenzte Datenmengenbegrenzungen insgesamt eher als eine mögliche Maßnahme zum Ausgleich der hier widerstreitenden Interessen, da ihnen insgesamt deutlich weniger Bedenken entgegenstehen als Websperren oder Portsperren. Nach Auftritt einer Rechtsverletzung gemäß § 7 Abs. 4 TMG durch Filesharing könnte beispielsweise eine zeitlich begrenzte Drosselung der Bandbreite Filesharing weniger attraktiv machen und dadurch Nutzer – wie es der EuGH verlangt – „von Rechtsverletzungen abgeschreckt werden".[47]

Für alle Sperrmaßnahmen kommt nach der Gesetzesbegründung eine **zeitliche Begrenzung** in Betracht. Diese sollte zwingend erfolgen. Einerseits dient die zeitliche Begrenzung dem Ausgleich der sich widerstreitenden Interessen von Rechteinhabern, Nutzern und Dritten. Unklar ist nach der derzeitigen Formulierung des Gesetzesentwurfs, ob der Anspruchsteller bei einer Forderung nach § 7 Abs. 4 TMG ggf. von Anfang an nur auf eine zeitlich begrenzte Sperrung dringen kann, oder ob es dem Anbieter des WLANs obliegt, quasi als Minus die Sperrung zeitlich zu begrenzen. Er trüge im letzteren Fall das Risiko, dass die zeitliche Begrenzung zu kurz bemessen wird oder gar nicht eingerichtet werden durfte.

Auch technisch und organisatorisch sind zeitliche Begrenzungen nicht trivial. Soweit ersichtlich, sehen selbst höherpreise handelsübliche WLAN-Router die Einstellung von zeitlich begrenzten Sperren nicht vor. Zwar gibt es in WLAN-Routern häufiger einen „Kindermodus", dieser muss aber in der Regel für jeden Nutzer konkret eingerichtet werden und sieht in der Regel weitere umfangreiche Beschränkungen vor, so dass hierauf nicht zurückgegriffen werden kann. Daher würde es dem Anbieter des WLANs selbst obliegen, zur Sicherung der Rechte seiner Nutzer und Dritter, die Sperrlisten regelmäßig zu prüfen und zu aktualisieren. So kann auf einer einmal gesperrten Webseite, die praktisch nur illegale Inhalte enthalten hatte und deren Sperrung das Argument des Overblocking nicht entgegenstand, zu einem späteren Zeitpunkt nur noch legaler Inhalt oder zumindest ein größerer legaler Anteil enthalten sein. Die Aufrechterhaltung der Sperre wäre dann möglicherweise nach § 7 Abs. 4 TMG nicht mehr rechtmäßig. Auch der Aufwand der Prüfung dieser Umstände dürfte dem Anbieter unzumutbar sein.

bb. Rechte der Betroffenen, Rechte Dritter und verfahrensrechtliche Ausgestaltung

Die obigen Ausführungen verdeutlichen die grundrechtliche Dimension, die nach dem Gesetzesentwurf in die Abwägung einfließen soll. Auf der einen Seite stehen die Rechte der Inhaber gewerblicher Schutzrechte, die jedenfalls als Ausfluss von Art. 14 GG geschützt sind. Auf der anderen Seite stehen die Rechte und Interessen der Betreiber von WLANs. Dies sind – bei gewerblich Tätigen – Rechte aus Art. 12 GG, bei privaten Anbietern aus Art. 2 Abs. 1 GG. Informationssuchende können sich auf ihr Recht auf Informationsfreiheit entsprechend Art. 5 Abs. 1 GG berufen. Auch der EuGH erkennt, dass Websperren einen

[47] EuGH EuZW 2016, 821 (Rn. 96) – McFadden.

Eingriff in das Recht auf Informationsfreiheit bedeuten.[48] Informationsanbieter wiederum können sich auf die Meinungs- und Äußerungsfreiheit nach Art. 5 Abs. 1 GG sowie ggf. Art. 12 Abs. 1 GG stützen. Hinzu kommen im Verhältnis von Nutzer zu Anbieter Bedenken hinsichtlich des Telekommunikationsgeheimnisses aus Art. 10 GG.

Wie oben dargestellt, können ausufernde Pflichten zur Einrichtung von Websperren das Angebot eines WLANs gerade bei kleineren Anbietern einschränken oder vollständig verhindern. Die Eingriffsintensität ist daher beachtlich. Informations- und Äußerungsfreiheit werden ebenfalls eingeschränkt, auch aus diesem Grunde ist ein Overblocking so weit wie möglich zu vermeiden. Auf der anderen Seite wird zu Recht darauf hingewiesen, dass Rechteinhaber nicht völlig rechtslos gestellt werden dürfen.[49]

Problematisch ist insoweit auch, dass die Rechte Dritter, insbesondere deren Äußerungsfreiheit, zwar eine Rolle bei der Abwägung spielen können, diese aber in der Regel gar nicht wahrgenommen werden können. Denn der Betreiber einer Webseite wird es im Zweifel kaum bemerken, wenn der Zugang zu seiner Webseite in einem einzelnen WLAN gesperrt wird. Er vermag sich entsprechend kaum Gehör zu verschaffen. Der EuGH hat in seiner Entscheidung „UPC/Telekabel“ darauf hingewiesen, dass durch verfahrensrechtliche Vorkehrungen die Rechte von Nutzern und Dritten gewahrt werden sollen.[50] Solche Verfahrensvorschriften, die z.B. die Einbindung repräsentativer Verbände als Vertreter der Interessen Dritten umfassen könnten,[51] sieht der Gesetzesentwurf bisher nicht vor.

Unklar ist letztlich auch, ob sich der Anbieter des WLANs, der einer Aufforderung nach § 7 Abs. 4 TMG Folge leistet, einem Anspruch des Dritten ausgesetzt sehen könnte. Gerade im Falle eines (möglicherweise unerkannten) Overblocking z.B. des Zugangs zu einer Firmenwebsite könnte der betroffene Dritte Ansprüche geltend machen.

cc. Gefahr des vorauseilenden Gehorsams und des Missbrauchs

Es besteht weiter die – berechtigte – Befürchtung, dass Anbieter, gerade von kleinen WLANs, einer Aufforderung zur Sperrung ohne weitere Prüfung nachkommen könnten, um ein eventuelles gerichtliches Verfahren nach § 7 Abs. 4 TMG zu vermeiden.[52] Für den Anbieter ist im Zweifel die Sperrung einfacher. Solches Verhalten ist bei der Löschung von Inhalten nach dem sog. „Notice-and-Takedown“-Verfahren in den USA vielfach bekannt

---

[48] EuGH EuZW 2016, 821 (Rn. 94) – McFadden; *Mantz*, EuZW 2016, 817; vgl. *Husovec*, Holey Cap! CJEU Drills (Yet) Another Hole in the E-Commerce Directive’s Safe Harbors, 10, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2843816.

[49] EuGH EuZW 2016, 821 (Rn. 96) – McFadden; *Spindler*, CR 2017, 262 (265).

[50] EuGH GRUR 2014, 468 (Rn. 57) – UPC Telekabel/Constantin Film.

[51] *Spindler*, CR 2017, 262 (265).

[52] Ebenso Stellungnahme des eco v. 9.3.2017 zum Referentenentwurf, S. 3, http://www.bmwi.de/Redaktion/DE/Downloads/Stellungnahmen/Stellungnahmen-WLAN-3/eco.pdf?__blob=publicationFile&v=2; *Grigorjew/Bile*, ZD-Aktuell 2017, 05621.

geworden, auch Missbrauchsfälle sind hier nicht unbekannt.[53] Weiter liegt die Gefahr eines Missbrauchs zur Verhinderung des Zugangs zu unliebsamen Inhalten auch bei WLANs auf der Hand.

Diese Problematik ließe sich lösen, indem die Anordnung nach § 7 Abs. 4 TMG von vorne herein unter einen Richtervorbehalt gestellt wird, z.B. ähnlich dem Verfahren nach § 101 Abs. 9 UrhG, aber anders als dort unter Beteiligung des Anbieters. Dies würde die nach dem Gesetzesentwurf gewünschte Einzelfallabwägung sicherstellen und gleichzeitig den Gefahren des vorauseilenden Gehorsams und des Missbrauchs entgegenwirken. An der Problematik der tatsächlichen und technischen Schwierigkeiten und daraus folgender Unzumutbarkeit der dargestellten Maßnahmen ändert allerdings auch der Richtervorbehalt nichts.

dd. Systematik

Systematisch ist § 7 Abs. 4 TMG falsch verortet. Der Anspruch auf Einrichtung von Websperren richtet sich nach der (mittlerweile) eindeutigen Formulierung nur gegen Anbieter von WLANs, die wiederum in § 8 Abs. 3 TMG genannt werden. Es ist daher nicht ersichtlich, warum der Anspruch auf Einrichtung von Websperren im „allgemeinen Teil" in § 7 TMG geregelt wird.[54] Dies eröffnet die Gefahr, dass mit systematischen Argumenten der Anwendungsbereich oder die Voraussetzungen von § 7 Abs. 4 TMG oder gar von § 8 Abs. 1 S. 2 TMG anders ausgelegt werden könnten, was wiederum dem Ziel der Rechtssicherheit zuwiderläuft.[55] § 7 Abs. 4 TMG sollte daher in § 8 Abs. 5 TMG verschoben werden.

ee. Streitwert

Zu Recht hat der Bundesrat darauf hingewiesen, dass eine Deckelung des Streitwerts für Verfahren nach § 7 Abs. 4 TMG sinnvoll ist.[56] Generell sollten Ansprüche nach § 7 Abs. 4 TMG mit einem deutlich niedrigeren Streitwert bemessen werden als Unterlassungsansprüche z.B. nach § 97 Abs. 1 UrhG. Denn das Ziel ist – wie der Gesetzesentwurf deutlich macht – im Umfang deutlich geringer. Dennoch steht zu befürchten, dass bei Verfahren nach § 7 Abs. 4 TMG ähnlich wie in bisherigen Verfahren bei Filesharing eher hohe Streitwerte angesetzt werden. Eine Deckelung dürfte daher dem Ziel der Rechtssicherheit förderlich sein.

III. Vereinbarkeit mit europarechtlichen Vorgaben

Es ist bezweifelt worden, ob der Gesetzesentwurf mit den europarechtlichen Vorgaben vereinbar ist.[57] Insoweit wird insbesondere der Einwand erhoben, dass dem betroffenen

---

[53] Vgl. *Seltzer*, Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment, Harvard Journal of Law & Technology, Vol. 24, 2010, 171.

[54] Vgl. *Grigorjew/Bile*, ZD-Aktuell 2017, 05621.

[55] Ebenso *Grigorjew/Bile*, ZD-Aktuell 2017, 05621.

[56] Stellungnahme des Bundesrats BT-Drs. 18/12496, S. 2.

Rechteinhaber nach § 8 Abs. 1 S. 2 TMG der Unterlassungsanspruch durch Ausweitung der Privilegierung genommen wird. Der „Ausgleich“ in Form des Anspruchs auf Einrichtung von Websperren nach § 7 Abs. 4 TMG sei insoweit möglicherweise nicht ausreichend wirksam, so dass der Rechteinhaber im Ergebnis schutzlos gestellt werden könnte. Da der tatsächliche Täter mangels Registrierung praktisch nie zu ermitteln sei, könne auch gegen diesen nicht vorgegangen werden.[58]

Wie der EuGH im Falle einer Vorlage des reformierten TMG entscheiden würde, lässt sich derzeit nicht absehen. Es ist auch festzuhalten, dass der Konflikt der sich widerstreitenden Interessen auf Grundlage der einschlägigen europäischen Richtlinien, namentlich Art. 8 Abs. 3 InfoSoc-Richtlinie, Art. 11 S. 3 Enforcement-Richtlinie und Art. 12 E-Commerce-Richtlinie, nur schwer oder gar nicht aufzulösen ist.[59]

Es ist allerdings im Rahmen dieses Konflikts auch einzustellen, dass nicht ersichtlich ist, dass von öffentlichen WLANs tatsächlich in erheblichem Umfang Rechtsverletzungen ausgehen. Soweit diesbezüglich auf die Möglichkeit der nichtverfolgbaren Nutzung von WLANs verwiesen wird, besteht diese Möglichkeit schon seit Jahren auch bei Internetverbindungen über Mobilfunk. Sowohl bei WLAN wie auch beim Mobilfunk teilen sich nämlich in der Regel eine Vielzahl von Nutzern eine öffentliche IP-Adresse. Die technische Lösung hierfür wird als „Network Address Translation“ (NAT) bezeichnet. Es ist bisher aber ebenfalls nicht ersichtlich, dass über Mobilfunkverbindungen in erheblichem Umfang Rechtsverletzungen begangen werden.

Weiter ist zu berücksichtigen, dass der nationale Gesetzgeber bei der Umsetzung von Richtlinien nach Art. 288 Abs. 3 AEUV einen gewissen Spielraum hat. Es ist Sache der Mitgliedsstaaten, bei der Umsetzung von Richtlinien auf ein angemessenes Gleichgewicht zwischen den verschiedenen Grundrechten zu achten.[60] Im Rahmen der Verhältnismäßigkeitsprüfung kann dabei auch der Grundsatz der praktischen Konkordanz eine Rolle spielen.[61] Nach dem Grundsatz der praktischen Konkordanz ist es Aufgabe des Gesetzgebers, sich widerstreitende grundrechtlich geschützte Interessen in Ausgleich zu bringen. Insoweit verbleibt dem Gesetzgeber in der Regel ein eher weiter Spielraum.

Diesen Spielraum nutzt der Gesetzesentwurf auch im Verhältnis zwischen § 8 Abs. 1 S. 2 und § 7 Abs. 4 TMG: Der betroffene Rechteinhaber kann vom Anbieter des WLAN nicht mehr Unterlassung verlangen, da dieser Anspruch im Ergebnis zu erheblicher rechtlicher Unsicherheit des Anbieters geführt hat und so dem erklärten politischen Ziel der breiten Verfügbarkeit von WLANs entgegensteht. Zum Ausgleich erhält der Rechteinhaber aber einen Anspruch auf Einrichtung von Websperren gegen den Anbieter des WLANs, wenn

---

[57] Vgl. nur *Spindler*, CR 2017, 262.

[58] *Spindler*, CR 2017, 262 (267).

[59] Vgl. insoweit auch *Spindler*, CR 2017, 262 (267).

[60] EuGH MMR 2008, 227 (Rn. 68) – Promusicae m.w.N.

[61] *Calliess/Ruffert*, EUV/AEUV, Art. 5 Rn. 57; *Schwarze/Stumpf*, EU-Kommentar, Art. 2 Rn. 18; *Ziegenhorn*, EuZW 2013, 351 (352).

Rechtsverletzungen auftreten. Es ist bereits nicht ausgemacht, ob der Anspruch auf Websperren tatsächlich in seiner Wirksamkeit begrenzter ist als der Unterlassungsanspruch, da bis zuletzt unklar war, wie denn der Anbieter eines WLANs im Rahmen der Störerhaftung seinen Prüfungs- und Überwachungspflichten nachkommen sollte.[62] Eine der zur Verfügung stehenden Möglichkeiten war stets die Sperrung von Inhalten, was auch das BGH-Urteil „Access Provider" zeigt.[63] Diese ist in Fällen von WLANs von den Gericht aber bisher nicht thematisiert worden. Darüber hinaus steht die möglicherweise begrenzte Wirksamkeit des Anspruchs nach § 7 Abs. 4 TMG dem Umstand gegenüber, dass eben nicht ersichtlich ist, dass von WLANs tatsächlich in nennenswertem Umfang Rechtsverletzungen ausgehen.

Soweit es um die Frage geht, ob ein Schadensersatzanspruch gegen den tatsächlichen Rechtsverletzer tatsächlich und wirksam durchgesetzt werden kann, unterscheidet sich die Situation nach dem Gesetzesentwurf und nach dem bisherigen Stand nicht wesentlich. Denn auch zuvor war dem Anbieter eines WLANs die Beauskunftung des tatsächlichen Rechtsverletzers unmöglich. Eine solche wäre überhaupt nur möglich, wenn der Anbieter des WLANs sämtlichen Datenverkehr seiner Nutzer überwachen würde, was – nicht nur – nach Art. 15 E-Commerce-Richtlinie untersagt ist. In der „McFadden"-Entscheidung des EuGH hat der EuGH letztlich zwar eine Registrierung der Nutzer und Sicherung des WLANs als eine mögliche (aber nicht zwingende) und zumutbare Maßnahme angesehen. Er hat dies aber nicht damit begründet, dass der betroffene Rechteinhaber dadurch einen Anspruch auf Schadensersatz gegen den Rechtsverletzer durchsetzen kann, sondern dass sich hierdurch Nutzer bereits von Rechtsverletzungen abschrecken ließen.[64]

Die gesetzgeberische Entscheidung, die in der Begründung ausdrücklich auf das „McFadden"-Urteil gestützt wird und einen Ausgleich der widerstreitenden Interessen sucht, dürfte daher im Wege der praktischen Konkordanz als verhältnismäßig und damit auch unter Berücksichtigung der europäischen Richtlinien zulässig sein.

***

[62] Vgl. *Sassenberg/Mantz*, (o. Fn. 3), Rn. 11 ff.

[63] BGH GRUR 2016, 268 – Access Provider II.

[64] EuGH EuZW 2016, 821 (Rn. 98) – McFadden; kritisch dazu *Mantz*, EuZW 2016, 817 (819).