- veröffentlicht in CR 2015, 298 –

Reto Mantz / Thomas Sassenberg[*]

Die Neuregelung der Störerhaftung für öffentliche WLANs – Eine Analyse des TMG-RefE v. 11.3.2015

Warum der Referentenentwurf die Verbreitung von WLANs nicht fördern wird

Die Verbreitung von breitbandigen Internetzugängen und deren Verfügbarkeit haben nach den Verlautbarungen der Bundesregierung höchste Priorität. Die Anzahl der öffentlichen WLAN-Hotspots nimmt jedoch nur schleppend zu und Deutschland hängt im internationalen Vergleich weit hinterher. Als Ursache hierfür wird neben den regulatorischen Anforderungen seit langer Zeit eine bestehende Rechtsunsicherheit beim Betrieb öffentlicher WLANs identifiziert. Dies veranlasste die große Koalition schon bei den Koalitionsverhandlungen dazu, die Notwendigkeit einer Regelung festzuschreiben. Inzwischen liegt der endabgestimmte Referentenentwurf der Bundesregierung zur Änderung des Telemediengesetzes (TMG-RefE) vor, der kurz darauf vielfach und teilweise heftig kritisiert worden ist. Der folgende Beitrag stellt zunächst kursorisch den Hintergrund dar (I.), analysiert anschließend den Referentenentwurf und dessen Folgen (II.), beleuchtet die europarechtliche Dimension (III.) und zuletzt die Reaktionen auf den Referentenentwurf (IV.). Auf die im Referentenentwurf enthaltenen Änderungen der Haftung für Host Provider nach § 10 TMG geht der vorliegende Beitrag nicht ein.

I. Hintergrund

Es ist bereits vielfach darüber berichtet worden, dass Deutschland bei der Verbreitung von Breitband allgemein und speziell von öffentlichen WLANs im internationalen Vergleich deutlich hinterherhinkt.[1] Gerade einmal rund 15.000 freie, öffentliche WLAN-Hotspots stehen in Deutschland zur Verfügung, das entspricht einer Quote von rund 1,9 Hotspots pro 10.000 Einwohner. Südkorea weist bspw. eine Quote von über 37 WLAN-Hotspots pro 10.000 Einwohner auf.[2] Die wesentliche Ursache hierfür ist bereits häufig dargestellt worden: Die

---

[*] Dr. iur. Reto Mantz, Dipl.-Inf., Richter, Landgericht Frankfurt am Main; Dr. iur. Thomas Sassenberg, LL.M., Rechtsanwalt und Fachanwalt für Urheber- und Medienrecht, Frankfurt am Main.

[1] Vgl. *Mantz/Sassenberg*, NJW 2014, 3537 m.w.N.

[2] eco Microresearch, November 2014, https://www.eco.de/wp-content/blogs.dir/eco-microresearch_verbreitung-und-nutzung-von-wlan.pdf; alle angegebenen Links wurden zuletzt am 21.04.2015 abgerufen.

bestehende Rechtsunsicherheit im Hinblick auf die Haftung des Betreibers für die Handlungen seiner Nutzer, zurückgehend auf verschiedene Gerichtsurteile.[3] Keine Rolle spielte allerdings bei diesen Entscheidungen jeweils die Haftungsprivilegierung in § 8 TMG, wonach derjenige, der Nutzern den Zugang zum Internet ermöglicht, für Handlungen seiner Nutzer nicht haften soll. Dass § 8 TMG dem Grunde nach Anwendung auch auf WLANs findet, war in der Literatur nie umstritten.[4] Problematisch ist aber, welche Prüfungs- und Überwachungspflichten der Betreiber zu erfüllen hat.[5]

1. Die Diskussion um Haftung bei und Förderung von öffentlichen WLANs

Die juristische Diskussion um die Frage der Verantwortlichkeit des Betreibers eines WLAN-Hotspots begann mit der ersten Entscheidung des LG Hamburg aus dem Jahr 2006.[6] Die Politik griff die Thematik auf, nachdem der *Digitale Gesellschaft e.V.* 2012/2013 einen konkreten Gesetzesentwurf veröffentlichte und den Parteien vorlegte. Der Entwurf sah – ähnlich § 8 Abs. 3 TMG-RefE – eine Klarstellung zur Anwendbarkeit von § 8 TMG auf WLANs vor und erklärte eine Privilegierung auch gegenüber Unterlassungsansprüchen. Die LINKE griff diesen Entwurf letztlich auf und brachte ihn in den Bundestag ein,[7] wo er allerdings abgelehnt wurde. Praktisch gleichzeitig legte die *SPD* einen Prüf- und Handlungsauftrag an den *Bundestag* vor, um zu prüfen, welche Maßnahmen zur Lösung der Problematik zu ergreifen seien.[8] Im November 2013 brachten *Piraten, SPD* und *Grüne* im Düsseldorfer Landtag einen weiteren Entwurf mit Aufforderung zur gesetzlichen Regelung ein.[9] Ende 2013 vereinbarten dann *CDU/CSU* und *SPD* im Rahmen ihres Koalitionsvertrages, dass in der folgenden Legislaturperiode ein Gesetzesentwurf angestrebt werden solle.[10] Im Juli 2014 wurde ein solcher Entwurf angekündigt, aber – wohl aufgrund von Abstimmungsproblemen innerhalb der *Bundesregierung* – doch nicht vorgelegt. Stattdessen griff die *Bundesregierung* die Thematik im Rahmen ihrer Digitalen Agenda auf.[11] *Grüne* und *LINKE* legten anschließend den 2013

---

[3] LG Hamburg, Urt. v. 26.7.2006 – 308 O 407/06, MMR 2006, 763; BGH, Urt. v. 12.5.2010 – I ZR 121/08, MMR 2010, 565 – Sommer unseres Lebens m. Anm. *Mantz*; a.A. OLG Frankfurt, Urt. v. 1.7.2008 – 11 U 52/07, MMR 2008, 603 m. Anm. *Mantz/Gietl*.

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

[5] Eingehend und ablehnend zu verschiedenen Maßnahmen OLG Köln, Urt. v. 18.7.2014 – 6 U 192/11, GRUR 2014, 1081 – Goldesel; OLG Hamburg, Urt. v. 21.11.2013 – 5 U 68/10, GRUR-RR 2014, 140 – 3dl.am; LG München I, Beschl. v. 18.9.2014 – 7 O 14719/12, GRUR Int. 2014, 1166; näher *Sassenberg/Mantz*, WLAN und Recht, 2014, Rn. 227 ff.

[6] O. Fn. 3.

[7] BT-Drs. 17/11137.

[8] BT-Drs. 17/11145.

[9] LT NRW-Drs. 16/4427; s. zuvor Antrag der Piraten v. 12.3.2013 LT NRW-Drs. 16/2284.

[10] Koalitionsvertrag 2013 zwischen CDU, CSU und SPD, S. 35.

[11] https://netzpolitik.org/2014/gier-nach-informationen-wir-veroeffentlichen-die-endgueltige-version-der-digitalen-agenda-der-bundesregierung/.

gescheiterten Gesetzesentwurf des *Digitale Gesellschaft e.V.* mit ergänzter Begründung erneut dem *Bundestag* vor,[12] konnten diesen jedoch erneut nicht durchsetzen. Zuletzt sprach sich die CDU im Dezember 2014 auf ihrem Parteitag erneut für eine Förderung öffentlicher WLANs aus.[13]

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*".[14] Als Folge enthielt der 2013 vorgelegte Entwurf für eine Verordnung zur Schaffung eines einheitlichen europäischen Binnentelekommunikationsmarktes („Digital Single Market-Verordnung", DSM-VO) in Art. 14 explizite Vorschriften zur Förderung der Verbreitung von WLANs, die insb. auch das WLAN-Sharing betreffen.[15]

2. Die Entwicklung in der Rechtsprechung

Die Rechtsprechung hatte sich zunächst ausschließlich mit der Haftung der privaten Inhaber von WLANs beschäftigt. Die Frage, ob § 8 TMG hier Anwendung finden sollte, wurde allein in der Literatur diskutiert.[16] Erstmals 2010 wandte das LG Frankfurt die bekannten Kriterien zur Haftung der privaten Anschlussinhaber für einen gewerblichen WLAN-Betreiber, einem Hotel, an und lehnte eine Haftung ab, allerdings wieder ohne auf § 8 TMG einzugehen.[17] Ganz ähnlich urteilte das LG Frankfurt 2013.[18]

Im Jahr 2014 - also acht Jahre nach der ersten Entscheidung des LG Hamburg – prüfte und bejahte das AG Hamburg bei Hotel- und Ferienwohnungsvermietern die Anwendbarkeit von § 8 TMG.[19] Dem folgte das AG Charlottenburg zum Fall eines öffentlichen, entgeltfreien WLAN-Hotspots, der aus altruistischen Gründen betrieben wurde.[20] Auch nach dem LG München I ist § 8 TMG auf WLANs und zudem auf Unterlassungsansprüche anwendbar. In der Folge legte

---

[12] BT-Drs. 18/3047.
[13] Beschlüsse abrufbar unter http://www.koeln2014.cdu.de/antraege-beschluesse. Dort „Beschluss D1", S. 2 und „Sonstige Beschlüsse", S. 12.
[14] Pressemitteilung der Europäischen Kommission vom 1.8.2013.
[15] COM (2013), 627 final; dazu *Mantz/Sassenberg*, CR 2014, 370.
[16] Vgl. *Gietl*, MMR 2007, 630; *Mantz*, Rechtsfragen offener Netze, 2008, 291 m.w.N.
[17] LG Frankfurt MMR 2011, 401 m. Anm. *Mantz*.
[18] LG Frankfurt, Urt. v. 28.6.2013 – 2-06 O 304/12, GRUR-RR 2013, 507 – Ferienwohnung; dazu *Mantz*, GRUR-RR 2013, 497.
[19] AG Hamburg, Urt. v. 10.6.2014 – 25b C 431/13, CR 2014, 536 m. Anm. *Mantz*; AG Hamburg, Urt. v. 24.6.2014 – 25b C 924/13.
[20] AG Berlin-Charlottenburg, Beschl. v. 17.12.2014 – 217 C 121/14, CR 2015, 192 m. Anm. *Bergt*.

das LG München I dem EuGH verschiedene Fragen zur Anwendbarkeit und zu den Rechtsfolgen von § 8 TMG für WLAN-Betreiber vor.[21]

II. Der Referentenentwurf der Bundesregierung

Ende Februar 2015 – und offiziell vorgestellt am 11.3.2015 – wurde der RefE eines Zweiten Gesetzes zur Änderung des Telemediengesetzes bekannt.[22] Auf die teils heftigen Reaktionen[23] reagierte das *Bundeswirtschaftsministerium* (*BMWi*) im April 2015 – mit einer für ein Gesetzgebungsvorhaben bisher neuen Vorgehensweise – und stellte eine ausführliche Liste häufiger Fragen und Antworten mit Erläuterungen und Klarstellungen online (FAQ *BMWi*).[24]

1. Zielsetzung und Definition „drahtloses Funknetz“

Im Hinblick auf die Störerhaftung bei WLAN-Hotspots ist es das Ziel des TMG-RefE, die Anwendbarkeit der Haftungsprivilegierung für die Betreiber von WLANs klarzustellen und zu präzisieren. Hierdurch soll der einfache und rechtssichere Aufbau und Betrieb von WLANs ermöglicht und somit die Verbreitung von WLANs gefördert werden.[25] Hierzu wird mit dem Entwurf zunächst in § 2 S. 1 TMG die Definition des „*drahtlosen lokalen Funknetzes*“ eingeführt und als „*ein Drahtloszugangssystem mit geringer Leistung und geringer Reichweite sowie mit geringem Störungsrisiko für weitere, von anderen Nutzern in unmittelbarer Nähe installierte Systeme dieser Art, welches nicht-exklusive Grundfrequenzen nutzt*“ legaldefiniert. Dies entspricht dem Wortlaut von Art. 2 Abs. 2 Nr. 10 des Entwurfs der europäischen DSM-VO,[26] der in Art. 14 spezielle Regelungen zur Förderung der Verbreitung von öffentlichen WLANs enthält. Hiervon werden insbesondere WLAN-Hotspots erfasst.[27]

2. Klarstellung des Anwendungsbereichs von § 8 TMG

a. Erfassung von WLANs, § 8 TMG-RefE

---

[21] LG München I, Beschl. v. 18.9.2014 – 7 O 14719/12, GRUR Int. 2014, 1166; dazu *Mantz/Sassenberg*, MMR 2015, 85; das Verfahren wird vor dem EuGH unter dem Az. C-484/14 geführt, jeweils aktualisierte Dokumente finden sich unter http://www.wlan-recht.de/urls/lgmuceugh.

[22] http://www.bmwi.de/BMWi/Redaktion/PDF/S-T/telemedienaenderungsgesetz,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf; Gesetzgebungsreport unter http://www.cr-online.de/29748.htm.

[23] Dazu unter IV.

[24] http://www.bmwi.de/DE/Themen/Digitale-Welt/Netzpolitik/rechtssicherheit-wlan,did=695728.html.

[25] RefE, S. 2 f.; PM des BMWi v. 12.3.2015: “Schub für kostenloses WLAN”, http://www.bmwi.de/DE/Presse/pressemitteilungen,did=695502.html.

[26] COM (2013) 627 final.

[27] ErwGr 25 DSM-VO; *Mantz/Sassenberg*, CR 2014, 370 (371).

Nach § 8 Abs. 3 TMG-RefE soll die Haftungsprivilegierung gemäß § 8 Abs. 1 TMG auch für Diensteanbieter gelten, die Nutzern einen Internetzugang über ein drahtloses Netzwerk zur Verfügung stellen. Auch wenn dies – wie dargestellt – der Auffassung in Literatur und Rechtsprechung entspricht, ist die Klarstellung zu begrüßen. Rechtsfolge der Haftungsprivilegierung ist, dass Anbieter von WLANs unter den Voraussetzungen des § 8 Abs. 1 TMG (Übermittlung nicht veranlasst, Adressat der Information nicht ausgewählt, Information weder ausgewählt noch verändert, kein kollusives Zusammenwirken mit dem Rechtsverletzer[28]) und unabhängig von den weiteren Voraussetzungen nach § 8 Abs. 3 und 4 TMG-RefE gegenüber allen Ansprüchen mit Ausnahme des Unterlassungsanspruch privilegiert sind und daher für entsprechende Handlungen ihrer Nutzer nicht haften.[29] Damit sind insbesondere Schadensersatzansprüche, aber auch die strafrechtliche Verfolgung des Betreibers ausgeschlossen.

b. Haftungsprivilegierung auch für private WLANs

Im Übrigen hält der TMG-RefE eine gewisse Überraschung bereit. Bisher war vor dem Hintergrund der Rechtsprechung unklar, ob von § 8 TMG auch Privatpersonen profitieren.[30] Schon nach dem bisherigen Wortlaut waren jedenfalls Privatpersonen erfasst, die ihr WLAN der Öffentlichkeit angeboten haben. In Auslegung von Wortlaut und Gesetzessystematik sollen sich künftig auch Betreiber privater geschlossener WLANs auf § 8 TMG-RefE berufen können. § 2 S. 1 Nr. 2 lit. a) TMG-RefE definiert den Begriff des drahtlosen Funknetzes rein technisch und damit weit. Insbesondere sieht er – an dieser Stelle – eine Unterscheidung zwischen geschäftsmäßigem und nicht geschäftsmäßigem Angebot nicht vor. Auch die Klarstellung in § 8 Abs. 3 TMG-RefE unterscheidet insoweit nicht, obwohl sich die *Bundesregierung* in § 8 Abs. 4 und 5 TMG-RefE intensiv mit dieser Differenzierung auseinander gesetzt hat. Zusätzlich war bereits zuvor anerkannt, dass es auf die Rechtsform des Betreibers nicht ankommt.[31] Auch die Erläuterungen des *BMWi* unterstützen diese Auslegung.[32]

3. Haftungsfreistellung auch für Unterlassungsansprüche

---

[28] Näher *Hoffmann*, in: Spindler/Schuster, Recht der elektronischen Medien, 3. Aufl. 2015, § 8 TMG Rn. 15 ff.
[29] *Sassenberg/Mantz*, WLAN und Recht, 2014, Rn. 212 f. m.w.N.*; Hoffmann*, in: Spindler/Schuster, Recht der elektronischen Medien, 3. Aufl. 2015, vor § 7 TMG Rn. 2, 25 ff.; zu Unterlassungsansprüchen s.u. 3.
[30] *Sassenberg/Mantz*, WLAN und Recht, 2014, Rn. 216 m.w.N.
[31] *Sassenberg/Mantz*, WLAN und Recht, 2014, Rn. 216; *Jandt*, in: *Roßnagel*, Beck'scher Kommentar zum Recht der Telemediendienste, 2013, § 7 TMG Rn. 3.
[32] FAQ BMWi, Fragen 2, 8, 12, 13.

Nach der Rechtsprechung des BGH finden die Haftungsprivilegierungen der §§ 8 – 10 TMG nicht auf Unterlassungs- und Beseitigungsansprüche Anwendung.[33] Die Frage der Vereinbarkeit mit Europarecht hat das LG München I gerade dem EuGH vorgelegt.[34] Die Regelung in § 8 Abs. 4 und 5 TMG-RefE sieht nun vor, dass der WLAN-Anbieter unter bestimmten Voraussetzungen auch gegenüber Unterlassungsansprüchen aufgrund Rechtsverletzungen seiner Nutzer privilegiert wird. Auch insoweit kann also ein Haftungsausschluss greifen. In der öffentlichen Wahrnehmung war insoweit stets praktisch nur von der (u.a.) auf §§ 97 Abs. 1 UrhG, 1004 BGB begründeten Störerhaftung die Rede. Von der Privilegierung erfasst werden aber Unterlassungsansprüche generell, so dass auch die insbesondere im Wettbewerbsrecht relevanten Ansprüche auf Unterlassung aus Verletzung von Verkehrspflichten[35] ausgeschlossen werden.

a. Persönlicher Anwendungsbereich, geschäftsmäßig betriebene WLANs

Die konkreten Anforderungen an WLAN-Anbieter unterscheiden sich in Abhängigkeit davon, ob der Diensteanbieter das WLAN „*anlässlich einer geschäftsmäßigen Tätigkeit oder als öffentliche Einrichtung*“ anbietet. Geschäftsmäßig ist ausweislich der Begründung „*jede nachhaltige Tätigkeit mit oder ohne Gewinnerzielungsabsicht.*“ Der Gesetzgeber hat hier die Legaldefinition des § 3 Nr. 10 TKG übernommen und insoweit einen Gleichklang mit den Regelungen des TKG hergestellt. Der TMG-RefE bzw. die Berichterstattung darüber[36] hatte zunächst für Verwirrung gesorgt, da teilweise ein Gegensatz zwischen dem „geschäftsmäßigen“ und allen „privaten“ WLANs angenommen wurde,[37] auf der anderen Seite aber nur die „*gelegentliche*, private Tätigkeit“ ausgenommen werden sollte.[38] Das *BMWi* hat in seiner FAQ auf die Kritik hin eindeutig klargestellt, dass z.B. auch Freifunker,[39] die ihr WLAN dauerhaft und unentgeltlich der Öffentlichkeit zur Verfügung stellen, „geschäftsmäßig“ i.S.d. des TMG-RefE handeln.[40] Als geschäftsmäßig anzusehen sind damit jedenfalls Internet-Cafés und

---

[33] BGH, Urt. v. 30.4.2008 – I ZR 73/05 MMR 2008, 531 ff. – Internet-Versteigerung III; BGH MMR 2007, 634, Urt. v. 12.7.2007 – I ZR 18/04 – Jugendgefährdende Medien bei eBay; BGH MMR 2007, 507 ff. – Internet-Versteigerung II; BGH, Urt. v. 27.3.2007 – VI ZR 101/06, ZUM 2007, 533 ff. – Meinungsforum; BGHZ 158, 236, Urt. v. 11.3.2004 – I ZR 304/01 = MMR 2004, 668 ff. – Internet-Versteigerung I.
[34] O. Fn. 21.
[35] Dazu BGH, Urt. v. 22.7.2010 – I ZR 139/08, GRUR 2011, 152 – Kinderhochstühle im Internet; BGH, Urt. v. 12.5.2010 – I ZR 121/08, MMR 2010, 565 – Sommer unseres Lebens; zur Haftung aus Verkehrspflichten eingehend *Sassenberg/Mantz*, WLAN und Recht, 2014, Rn. 243; *Köhler*, GRUR 2008, 1.
[36] Spiegel Online v. 20.2.2015, http://www.spiegel.de/netzwelt/netzpolitik/w-lan-bundesregierung-will-offenen-zugang-foerdern-a-1019668.html.
[37] *Bergt*, CR-Online v. 1.3.2015, http://www.cr-online.de/blog/2015/03/01/gesetzentwurf-zur-abschaffung-freier-wlans; vgl. auch *Hullen*, jurisPR-ITR 7/2015, Anm. 2.
[38] RefE, S. 12.
[39] Also Mitglieder der nichtstaatlichen Initiative Freifunk, http://freifunk.net.
[40] FAQ BMWi, (o. Fn. 24), Frage 2; vgl. auch FAQ BMWi, Fragen 8, 9.

Sportvereine,[41] aber auch Geschäfte, die das WLAN zur Absatzförderung dauerhaft und nachhaltig betreiben.[42] Ausgenommen ist lediglich die gelegentliche private Betätigung[43] und damit i.E. nur das rein private WLAN, das gelegentlich anderen Personen als den Haushaltsmitgliedern zur Verfügung gestellt wird.

b. Zusätzliche Pflichten für Betreiber (§ 8 Abs. 4 TMG-RefE)

Nach § 8 Abs. 4 und 5 TMG-RefE wird die Freistellung im Fall eines Unterlassungsanspruchs nur dann gewährt, wenn weitere Voraussetzungen erfüllt sind. Den Betreibern obliegt es, „*zumutbare Maßnahmen [zu ergreifen], um eine Rechtsverletzung durch Dritte zu verhindern*". Die Maßnahmen müssen nach dem Wortlaut zwingend ergriffen werden („*haften nur dann nicht ...*"), damit der Betreiber von der Privilegierung profitiert.

Nach Postulierung dieser Pflicht stellt der TMG-RefE ein Regelbeispiel auf, wonach dies der Fall sein soll, wenn der Anbieter sein WLAN „*durch Verschlüsselung oder vergleichbare Maßnahmen gegen den unberechtigten Zugriff durch außenstehende Dritte*" sichert und die Erklärung des Nutzers einholt, dass dieser keine Rechtsverletzungen begehen werde. Diese Anforderungen müssen dabei kumulativ erfüllt sein, wie schon der Gesetzeswortlaut („*und*") deutlich macht.[44] Bei Ergreifen dieser konkreten Maßnahmen erfolgt zwingend die Haftungsbefreiung des Diensteanbieters. Die Konstruktion der offenen Formulierung („*zumutbare Maßnahmen*") mit Regelbeispiel soll die Technologieneutralität sicherstellen,[45] es bleibt dem Anbieter daher die Möglichkeit, das WLAN gegen Rechtsverletzungen durch Dritte mittels anderer zumutbarer Maßnahmen zu sichern. Welche Maßnahmen dies sein könnten, erläutert der Entwurf nicht. Ergreift der Anbieter solche alternativen Maßnahmen, trägt er das Risiko, dass diese von der Rechtsprechung als nicht ausreichend erachtet werden. *De facto* wird daher wohl nur mit den im TMG-RefE konkret dargestellten Maßnahmen die beabsichtigte Rechtssicherheit erreicht werden.

aa. Verschlüsselung

Der RefE fordert somit i.E. für die Privilegierung im Hinblick auf Unterlassungsansprüche die Einrichtung der Verschlüsselung von WLANs. Nach der Begründung soll dadurch gewährleistet werden, dass die Daten des Anbieters und der übrigen Nutzer gegen den Zugriff durch Unbefugte gesichert und das Kommunikationsgeheimnis geschützt werden. Orientiert hat

---

[41] RefE, S. 11.
[42] Zu den verschiedenen Modellen beim WLAN *Sassenberg/Mantz*, WLAN und Recht, 2014, Rn. 11 ff.
[43] RefE, S. 12.
[44] Klarstellend auch FAQ BMWi, Frage 3.
[45] RefE, S. 12.

sich die *Bundesregierung* dabei an der BGH-Rechtsprechung „Sommer unseres Lebens“.[46] Dabei verkennt sie aber, dass die Verschlüsselung des WLANs für das gesteckte Ziel weitgehend nutzlos und sogar kontraproduktiv ist.

(1) Zusätzliche Hürden, Verteilung des Schlüssels

Zunächst widerspricht die Verschlüsselung dem Ziel der Förderung und weiteren Verbreitung von WLANs. Sie verhindert, dass der Nutzer einfach und unkompliziert den Zugang zum WLAN und damit zum Internet erhält, da immer zunächst ein Schlüssel ausgetauscht werden muss. Diese Einschränkung gefährdet das Geschäftsmodell von öffentlichen WLANs erheblich. Denn rund 20% der Nutzer von WLANs lassen sich bereits von einfachen Hürden wie einer Vorschaltseite oder Registrierung von der Nutzung eines WLANs abhalten.[47] Zusätzlich schafft die *Bundesregierung* für Anbieter die kaum zu überwindende Problematik, wie der Nutzer an den Schlüssel kommen soll. In Restaurants und Cafés mag man den Schlüssel in die Speisekarte drucken können.[48] In einer Vielzahl von Situationen steht dem Betreiber eine solche Möglichkeit aber nicht offen. Unklar ist z.B., wie bei WLAN-Hotspots in Zügen, an Bahnhöfen oder Flughäfen den Nutzern das Passwort mitgeteilt werden soll.

(2) Eigeninteresse an der Sicherung

Der zweite Punkt, den die *Bundesregierung* anspricht ist der Schutz der Sicherheit der Anlagen und Daten des Betreibers. Auf ein solches „Eigeninteresse“ hatte auch der BGH abgestellt,[49] was in der Literatur bereits kritisiert wurde.[50] Denn die Verschlüsselung des WLANs dient nicht dem Schutz der Daten und Anlagen des Betreibers, sondern der Begrenzung des Zugangs auf einen ausgewählten Personenkreis. Ein öffentliches WLAN soll aber jedem potenziellen Nutzer zur Verfügung stehen. Die Sicherung des Betreibers erfolgt vielmehr durch sichere Konfiguration der Anlagen, so dass Nutzer des WLANs nur auf das Internet, nicht aber auf die Server des Betreibers zugreifen können. Insofern ist auch unklar, warum die Gesetzesbegründung vom Ausschluss des „Zugriffs durch Unbefugte“ spricht.[51] In einem

---

[46] BGH, Urt. v. 12.5.2010 – I ZR 121/08, MMR 2010, 565 – Sommer unseres Lebens; s. FAQ BMWi, Frage 4; auch in der Literatur ist vereinzelt die Verschlüsselung gefordert worden, vgl. *Eichelberger*, in: Hoeren/Bensinger, Haftung Im Internet, 2014, Kap. 4 Rn. 122.

[47] Befragung Kabel Deutschland, PM v. 6.3.2014, https://www.kabeldeutschland.com/de/presse/pressemitteilung/produktnachrichten/632014.html.

[48] RefE, S. 13.

[49] BGH, Urt. v. 12.5.2010 – I ZR 121/08, MMR 2010, 565 (Rn. 22) – Sommer unseres Lebens.

[50] *Mantz*, MMR 2010, 568.

[51] RefE, S. 12; kritisch dazu auch DIHK-Stellungnahme v. 8.4.2015, http://www.ihk-nuernberg.de/blogs/it-region-nuernberg/files/2015/04/Stellungnahme-DIHK-TMG.pdf.

öffentlichen WLAN, das sich an jedermann richtet, gibt es definitionsgemäß keine unbefugten Nutzer.

Aber auch der Schutz der Daten der Nutzer und des Kommunikationsgeheimnisses werden durch die im RefE angedachte Verschlüsselung nicht gewährleistet. Die Gesetzesbegründung sieht hier die die weit verbreitete Verschlüsselung z.B. mittels WPA2 vor.[52] Bei dieser teilen sich alle Nutzer einen Schlüssel („*shared key*"). Bei der Anmeldung am WLAN-Router mittels dieses *shared key* handeln Router und Nutzergerät für die Dauer der Nutzung einen persönlichen Schlüssel aus („*session key*"). Dieser Aushandlungsprozess kann jedoch von allen anderen bereits eingeloggten Nutzern des WLANs beobachtet werden, so dass ihnen der *session key* bekannt sein kann. In der Folge können sie die Kommunikation des anderen Nutzers entschlüsseln und belauschen. Zusätzlich können Nutzer, die sich später einloggen, mittels einer sog. „*Deauthentication Attack*" dafür sorgen, dass ein anderer Nutzer kurzzeitig die Verbindung mit dem Router abbricht. Bei der neuerlichen Verbindung kann anschließend die Aushandlung des neuen *session key* abgehört werden. Es ist daher für Nutzer auch im WPA2-verschlüsselten WLAN unabdinglich, selbst für Verschlüsselung des Datenstroms zu sorgen. Eine Lösung für dieses Problem stellen komplexe Authentifizierungsmechanismen wie etwa WPA2-Enterprise/802.1X dar.[53] Diese erfordern jedoch enormen Aufwand, da spezielle Server eingerichtet und bereitgehalten werden müssen. Zudem muss jeder Nutzer registriert und mit einem persönlichen Passwort versehen werden.

(3) IT-Sicherheit ≠ Verantwortlichkeit

Ein weiterer schwerwiegender Mangel des TMG-RefE ist, dass er IT-Sicherheit und Verantwortlichkeit miteinander vermischt. Das eine hat *per se* aber mit dem anderen nichts zu tun. Insbesondere ist die Verschlüsselung des WLANs nicht geeignet, Rechtsverletzungen zu verhindern. Denn jeder Nutzer, der den WPA2-Schlüssel erhält, z.B. aus der Speisekarte des Restaurants, ist in der Lage, aus dem WLAN heraus Rechtsverletzungen zu begehen. Dabei verkennt die *Bundesregierung* auch das Gefahrenpotenzial für Rechtsverletzungen über WLANs. Wie die *Medienanstalt Berlin-Brandenburg* (*mabb*) berichtet, die zusammen mit *Kabel Deutschland* u.a. in Berlin viele WLAN-Hotspots seit 2012 betreibt, ist es seit dem Start des Projekts nicht zu Urheberrechtsverletzungen gekommen.[54]

---

[52] RefE, S. 12.

[53] *Tanenbaum/Wetherall*, Computer Networks, 5. Aufl. 2010, 824; eingehend zu Verschlüsselung in WLANs *Sassenberg/Mantz*, WLAN und Recht, 2014, Rn. 8.

[54] mabb-Stellungnahme v. 7.4.2015, (u. Fn. 103), S. 3. Kabel Deutschland hat in Deutschland inzwischen 750.000 Hotspots aufgebaut, vgl. http://www.heise.de/netze/meldung/Hotspot-Ausbau-Kabel-Deutschland-meldet-750-000-oeffentliche-Internet-Zugaenge-2592129.html.

Darüber hinaus ist die Verschlüsselung auch nicht geeignet, im Falle einer Rechtsverletzung den Täter ausfindig zu machen. Hierfür wäre es vielmehr zwingend erforderlich, Kommunikationsdaten zu erheben und zu speichern, wozu keine Pflicht besteht und was bei IP-Adressen über sieben Tage hinaus unzulässig wäre, solange keine Abrechnung erfolgt,[55] und in Bezug auf andere Daten dem Fernmeldegeheimnis zuwiderlaufen kann.[56] Aus diesem Grunde verzichtet der TMG-RefE auch ausdrücklich darauf, den Anbieter zur Erhebung und Speicherung von Daten zu verpflichten.[57]

(4) Kosten

Die Verschlüsselungspflicht wird zusätzlich dazu führen, dass der Großteil der in Deutschland betriebenen öffentlichen WLAN-Hotspots umgerüstet werden muss. Denn bisher war selbst bei der Mehrzahl der WLAN-Hotspots mit Registrierung der Zugang zum WLAN selbst zunächst ohne Passwort möglich. Die Anmeldung erfolgte dann (innerhalb des WLANs) auf einer sog. *Splash-Page*. Dementsprechend kommen auf Betreiber von WLANs erhebliche Kosten für die Umrüstung sowie höhere Kosten bei der Neueinrichtung zu. Beispielsweise das von Verkehrsminister *Dobrindt* (CSU) erst im März 2015 vorgestellte öffentliche und barrierefreie WLAN in 100 Behördengebäuden in Bonn müsste umgerüstet werden.[58] Dennoch geht der TMG-RefE davon aus, dass keine Kosten für Wirtschaft und Verwaltung entstehen werden.[59]

(5) Außendarstellung

Die Außendarstellung des „Digitalen Deutschlands“ wird jedenfalls weiter erheblich leiden. Es ist im Ausland üblich, dass praktisch an jedem Ort ohne Probleme ein öffentliches (oder auch privates) WLAN genutzt werden kann. Insbesondere Touristen werden durch Verschlüsselung vom schnellen, unkomplizierten und kostengünstigen Zugang zum Internet abgehalten. Die verschlüsselten WLANs werden gerade auf diese wie verschlossene Türen wirken.

(6) Verschlüsselungsstandard

Nicht ganz klar ist, welchen Verschlüsselungsstandard der Betreiber wird einhalten müssen. Der TMG-RefE spricht von „sicheren“ Verfahren, allerdings soll „in der Regel“ die vom Hersteller vorgesehene Verschlüsselung, z.B. WPA2, genügen. Der BGH hatte jedenfalls bei

---

[55] BGH, Urt. v. 3.7.2014 – III ZR 391/13, NJW 2014, 2500 = ZD 2014, 461 (m. Anm. Eckhardt); OVG NRW, Urt. v. 10.11.2014 – 13 A 1973/13, MMR 2015, 209.
[56] Vgl. BVerfG, Urt. v. 2.3.2010 – 1 BvR 256/08 u.a., NJW 2010, 833 – Vorratsdatenspeicherung.
[57] FAQ BMWi, Frage 1.
[58] BMVI-PM v. 23.3.2015, http://www.bmvi.de/SharedDocs/DE/Artikel/DG/offenes-wlan-am-bmvi.html.
[59] RefE, S. 2.

privaten Betreibern denjenigen Verschlüsselungsstandard als ausreichend angesehen, der beim Erwerb des WLAN-Routers aktuell war.[60] Möglicherweise will die *Bundesregierung* dies auch für den geschäftsmäßigen Anbieter beibehalten.

bb. Erklärung, keine Rechtsverletzungen zu begehen

Zweite Voraussetzung der Haftungsprivilegierung auch gegenüber Unterlassungsansprüchen ist, dass der Diensteanbieter die Erklärung des Nutzers einholt, keine Rechtsverletzungen zu begehen. Dabei überlässt es die *Bundesregierung* dem Anbieter, wie er diese Erklärung einholt. So soll das Einverständnis in eine entsprechende Klausel in AGB ausreichen, wobei nach der Vorstellung der *Bundesregierung* diese AGB wohl auch – zusammen mit dem Passwort – in der Speisekarte abgedruckt werden könnten.[61] Ähnlich dazu sieht § 45o TKG für die Rufnummernzuteilung vor, dass der Anbieter darauf hinweisen muss, dass die zugeteilte Rufnummer nicht missbräuchlich verwendet werden darf.

Auch mit dieser Anforderung orientiert sich die *Bundesregierung* teilweise an der Rechtsprechung, die immer wieder eine Belehrung der Nutzer diskutiert hatte.[62] Der BGH hat eine solche Belehrung bei volljährigen Nutzern jedoch zumindest im Familienbereich ohne vorherigen Anlass gerade nicht verlangt.[63] Bei der Störerhaftung geht die Rechtsprechung von jeher auch davon aus, dass der Täter eigenverantwortlich handelt und daher der Anbieter von dessen rechtskonformem Verhalten ausgehen darf.[64] Eine entsprechende Erklärung in AGB wird generell für untauglich gehalten.[65] Es ist zudem sehr zweifelhaft, ob sich Nutzer, die sich zur Vornahme von Rechtsverletzungen entschlossen haben, von einem solchen – konsequenzlosen – Versprechen tatsächlich davon abhalten lassen werden.[66] Darüber hinaus sind Vorschaltseiten zwar eine praktikable Lösung, technisch aber schwierig zu realisieren. In der Regel wird der Nutzer beim Aufruf irgendeiner Webseite im WWW durch einen „Trick“ zwangsweise auf die *Splash-Page* umgeleitet. Erst nachdem er dort die Erklärung erteilt hat, kann er weitersurfen. Problematisch ist dies bspw., wenn der Nutzer gar kein WWW nutzt, sondern nur am Mobiltelefon die E-Mail-App nutzen will. Er erhält keine Fehlermeldung und wird kaum verstehen, warum der Zugang zum Internet „nicht funktioniert“.

---

[60] BGH, Urt. v. 12.5.2010 – I ZR 121/08, MMR 2010, 565 (Rn. 33) – Sommer unseres Lebens.
[61] RefE, S. 13.
[62] Z.B. LG Frankfurt, Urt. v. 28.6.2013 – 2-06 O 304/12, GRUR-RR 2013, 507 – Ferienwohnung.
[63] BGH, Urt. v. 8.1.2014 – I ZR 169/12, GRUR 2014, 657 – BearShare.
[64] Vgl. BGH, Urt. v. 15.5.2003 – I ZR 292/00, GRUR 2003, 969 – Ausschreibung von Vermessungsleistungen; *Mantz*, GRUR-RR 2013, 497.
[65] OLG Hamburg, Urt. v. 28.1.2009 – 5 U 255/07, NJOZ 2009, 1595 (1619) – alphaload.
[66] *Hullen*, jurisPR-ITR 7/2015, Anm. 2: „Placebo“; *Bergt*, CR-Online v. 1.3.2015, http://www.cr-online.de/blog/2015/03/01/gesetzentwurf-zur-abschaffung-freier-wlans.

Ein satirischer, aber dennoch überraschend guter Ansatz wurde im Internet vorgeschlagen: Das WLAN solle so eingerichtet werden, dass es den Namen (SSID) „Ich werde keine Rechtsverletzungen begehen“ trägt und das Passwort „Einverstanden“ lautet.[67] Dem Gesetzeswortlaut dürfte diese Lösung jedenfalls entsprechen.

cc. Alternative Maßnahmen

Offen lässt der TMG-RefE, welche alternativen zumutbaren Maßnahmen Betreiber ergreifen können, um der Haftung zu entgehen. Für Access Provider haben OLG Hamburg und OLG Köln jedenfalls DNS-, IP-, URL- und hybride Sperren als unzumutbar abgelehnt, auch weil sie teilweise in das Fernmeldegeheimnis eingreifen und weitgehend ineffektiv sind.[68] Würde man an den TMG-RefE dieselben Maßstäbe anlegen wie die OLGe Köln und Hamburg, wären wohl auch Verschlüsselung und Belehrung als unzumutbar anzusehen. Stellt man auf die Wirksamkeit ab, müsste man auch konstatieren, dass das völlig offene und ungesicherte WLAN Rechtsverletzungen ebenso gut entgegen wirkt wie die vom TMG-RefE geforderte Verschlüsselung und Erklärung.

c. Private WLANs (§ 8 Abs. 5 TMG-RefE)

Die Betreiber nicht geschäftsmäßiger, nur gelegentlich öffentlicher WLANs müssen zusätzlich zu den zumutbaren Maßnahmen nach § 8 Abs. 4 TMG-RefE noch „*die Namen der Nutzer kennen, denen sie den Zugang gewährt haben*.“ Auch dies hatte zunächst zu Unsicherheiten geführt. So wurde vermutet, dass der Inhaber des WLANs die Namen der Nutzer erfragen und aufzeichnen,[69] sich ggf. sogar den Personalausweis zeigen lassen müsse.[70] Die *Bundesregierung* hat mit ihrer Formulierung aber wohl nur beabsichtigt, den Nutzerkreis einzuschränken:[71] Nicht geschäftsmäßige Anbieter sollen ihnen unbekannten Personen schlicht keinen Zugang gewähren. Allerdings dürfte es ausreichen, wenn der Nutzer nur einem der Familien- oder Haushaltsmitglieder persönlich bekannt ist. Das Haushaltsmitglied des Anschlussinhabers wird daher einem Freund das Passwort des verschlüsselten Heim-WLANs mitteilen dürfen – wenn sichergestellt ist, dass der Freund erklärt, keine Rechtsverletzungen zu begehen.

---

[67] https://plus.google.com/106108666832471430646/posts/CsZhdEyJC4m.
[68] OLG Köln, Urt. v. 18.7.2014 – 6 U 192/11, GRUR 2014, 1081 – Goldesel; OLG Hamburg, Urt. v. 21.11.2013 – 5 U 68/10, GRUR-RR 2014, 140 – 3dl.am.
[69] *Härting*, LTO-Online v. 12.3.2015, http://www.lto.de/recht/hintergruende/h/referentenentwurf-stoererhaftung-wlan-hotspot.
[70] *Hullen*, jurisPR-ITR 7/2015 Anm. 2.
[71] FAQ BMWi, Frage 1 („im privaten Umfeld regelmäßig der Fall“).

Fraglich bleibt allerdings, wie der WLAN-Inhaber im Streitfall darlegen und beweisen soll, dass er die Anforderungen von § 8 Abs. 5 TMG-RefE eingehalten hat. Grundsätzlich trifft den Betreiber die Beweislast für die Anforderungen der Privilegierung,[72] was sich auch aus der Gesetzessystematik ergibt. Hierbei wird jedenfalls für die zusätzliche Anforderung in § 8 Abs. 5 TMG-RefE aber zu berücksichtigen sein, dass die *Bundesregierung* eine Registrierung oder Protokollierung der Nutzer ausdrücklich ausschließen will.[73] Nimmt man die *Bundesregierung* und das Ziel des Entwurfs, Rechtssicherheit zu schaffen, insoweit ernst, wird es wohl ausreichen müssen, wenn der private Betreiber generell vorträgt, dass nur er und seine Haushaltsmitglieder Zugang zum WLAN haben (belegt z.B. durch Zeugenbeweis) und dass jedes der Haushaltsmitglieder angewiesen ist, nur namentlich bekannten Personen den Zugang zu gewähren. Angesichts des Umstandes, dass gerade im Privatbereich Ansprüche häufig erst Jahre nach dem eigentlichen Vorfall geltend gemacht werden, wäre für den Betreiber ansonsten zwingend eine Protokollierung aller Nutzer erforderlich, denen jemals Zugang gewährt wurde. Mit dem Begriff des „namentlichen Kennens“ eröffnet die *Bundesregierung* jedenfalls Diskussionsstoff und trägt damit kaum zur Rechtssicherheit bei.

d. Keine Registrierungs- oder Speicherpflichten

Festzuhalten und hervorzuheben ist, dass der TMG-RefE keine Identifizierungs-, Registrierungs- oder Speicherpflichten beinhaltet oder bezweckt.[74] Daher bleibt es dabei, dass derzeit keinerlei Registrierungspflichten im Zusammenhang mit dem Betrieb eines WLANs bestehen.[75] Der Betreiber muss daher insbesondere nicht die Erklärung des Nutzers, keine Rechtsverletzungen zu begehen, protokollieren. Für den späteren Nachweis der Erfüllung der Voraussetzungen des § 8 Abs. 4 TMG-RefE ist es daher nur erforderlich darzulegen, dass eine solche Erklärung überhaupt stets eingeholt wird.

Durch die begrüßenswerte Klarstellung des *BMWi* sollte jedenfalls endlich mit der immer wieder (insbesondere aus dem Bereich kommunaler Entscheider) zu hörenden Mär aufgeräumt sein, dass ein WLAN nur mit Registrierung und Identifizierung rechtssicher zu betreiben sei.

e. Login (doch) bei jedem Hotspot erforderlich

---

[72] *Hoffmann*, in: Spindler/Schuster, Recht der elektronischen Medien, 3. Aufl. 2015, § 8 TMG Rn. 42 f.; *Sassenberg/Mantz*, WLAN und Recht, 2014, Rn. 249 m.w.N.

[73] FAQ BMWi, Frage 1.

[74] Ausdrücklich FAQ BMWi, Frage 1.

[75] So schon LG München I, Urt. v. 1.12.2012 – 7 HK O 1398/11, CR 2012, 605; *Sassenberg/Mantz*, WLAN und Recht, 2014, Rn. 234.

Problematisch ist wie unter II.3.b.aa. angesprochen, dass bei der Verschlüsselung von Hotspots der Nutzer für jeden der vielen tausend Hotspots ein separates Passwort benötigt. Wenn das Passwort zusätzlich nicht am Schaufenster angebracht ist oder in der Speisekarte steht, muss der Nutzer ggf. zuvor mit jedem Anbieter einen separaten Login vereinbaren. Dem tritt die *Bundesregierung* entgegen und verweist auf die Initiative „eduroam", bei der sich insbesondere Universitäten zusammengeschlossen haben und es so ermöglichen, dass eine Anmeldung an verschiedenen Institutionen genutzt werden kann.[76] Die *Bundesregierung* stellt sich vor, dass sich Händler in Fußgängerzonen zu solchen „Roaming-Zonen" zusammentun und Nutzer sich daher für eine Fußgängerzone nur einmal anmelden müssen.[77]

Zum einen löst dies nicht das Problem, dass sich Nutzer in jeder einzelnen Fußgängerzone anmelden müssen. Insbesondere Touristen werden auch weiterhin größtenteils ausgeschlossen. Zum anderen macht sich die *Bundesregierung* nicht klar, welcher (personelle und finanzielle) Aufwand für eine solche „eduroam"-ähnliche Infrastruktur erforderlich ist, den daher im Grunde nur Universitäten betreiben können. Mit dem einfachen und unkomplizierten Einrichten eines WLAN-Hotspots für Betreiber hat dies nichts mehr zu tun. Auch ist kaum damit zu rechnen, dass die Verfasser des TMG-RefE jemals selbst ein „eduroam"-Zertifikat installiert haben. An der *Universität Frankfurt* bspw. muss hierfür (unter Windows 8) eine .exe-Datei heruntergeladen und – unter „Zurkenntnisnahme der Sicherheitswarnung" – ausgeführt werden.[78] Auf mobilen Geräten oder anderen Betriebssystemen erfordert die Installation von solchen Zertifikaten in der Regel händische Eingriffe. Die Fußgängerzonen-Netze dürften daher im Ergebnis praktisch nicht genutzt werden, wenn nicht ein erheblicher zusätzlicher und dauerhafter Werbe- und Aufklärungsaufwand durch die Anbieter betrieben wird.

4. Datenschutzrecht

Datenschutzrechtlich dürfte der TMG-RefE kaum Probleme aufwerfen.[79] Nach der klaren Aussage des *BMWi* sollen *keine* zusätzlichen Daten erhoben und gespeichert werden, insbesondere nicht Namen, Nutzungszeitpunkte etc. § 8 Abs. 4 und 5 TMG-RefE enthalten daher auch keine entsprechende Erhebungs- und Speicherungsbefugnis i.S.v. § 4 Abs. 1 BDSG. Die Zulässigkeit der Erhebung und Nutzung von Daten richtet sich wie bisher nach §§ 91 ff. TKG, nicht nach §§ 11 ff. TMG.[80] Gerade bei kostenlosen Angeboten dürfte daher eine

[76] Ähnlich *Eichelberger*, in: Hoeren/Bensinger, Haftung Im Internet, 2014, Kap. 4 Rn. 122.
[77] FAQ BMWi, Frage 14.
[78] http://www.rz.uni-frankfurt.de/51139054/10_Windows8.
[79] A.A. (aber vor Veröffentlichung der FAQ BMWi) *Hullen*, jurisPR-ITR 7/2015 Anm. 2.
[80] Eingehend zum Datenschutz beim Betrieb von WLANs *Sassenberg/Mantz*, WLAN und Recht, 2014, Rn. 123 ff.

Erhebung und Speicherung von Daten – mit Ausnahme der gem. § 100 TKG zur Störungserkennung und -beseitigung erforderlichen Daten – nach wie vor nur mit ausdrücklicher Einwilligung des Nutzers zulässig sein.[81] Die Protokollierung des Surfverhaltens der Nutzer, die Betreiber möglicherweise zur Verhinderung einer späteren Haftung einrichten könnten,[82] ist in jedem Fall gesetzeswidrig. Dementsprechend dürfen – sofern für die Entgeltabrechnung nicht erforderlich – weder der geschäftsmäßige noch der nicht-geschäftsmäßige Anbieter Namen und Nutzungszeitpunkt z.B. zum Zwecke einer späteren Verwendung in einem Gerichtsverfahren erheben und speichern, so dass entsprechende Protokolle in der Regel unzulässig sein werden. Auch die Leitlinien des Bundesministeriums der Justiz und Verbraucherschutz für die erneute Einführung der Vorratsdatenspeicherung führen zu keinem anderen Ergebnis.[83] Zwar sehen diese vor, dass die zugewiesene IP-Adresse, Kennung eines Anschlusses „sowie die zugewiesene Benutzerkennung“ bei Internetzugangsdiensten zu speichern sind. Es ist jedoch davon auszugehen, dass tatsächlich nur die erzeugten und verarbeiteten Daten gespeichert werden müssen und damit keine Pflicht zu einer zusätzlichen Erhebung oder Vergabe einer Benutzerkennung besteht. Ob und welcher Form die Leitlinien letztlich verabschiedet werden, ist zudem noch unklar.

III. Der Referentenentwurf und das europäische Recht

Der TMG-RefE selbst nimmt Stellung zur Vereinbarkeit mit der E-Commerce-Richtlinie (ECRL): Da lediglich die bestehenden Regelungen im TMG und die Rechtsprechung zur Störerhaftung präzisiert würden, widerspreche der Entwurf dem europäischen Recht nicht.[84] Im Kontrast dazu ist der TMG-RefE nach seiner Veröffentlichung wiederholt als europarechtswidrig kritisiert worden.[85]

1. Vereinbarkeit mit der E-Commerce-Richtlinie

Auf europäischer Ebene ist die Privilegierung von Internet Service Providern in Art. 12 - 15 ECRL geregelt, deren Umsetzung §§ 7 - 10 TMG dienen. Hier von Relevanz sind insbesondere Art. 12 ECRL, der die Voraussetzungen der Privilegierung für Access Provider regelt

---

[81] *Sassenberg/Mantz*, WLAN und Recht, 2014, Rn. 234.
[82] *Bergt*, CR-Online v. 1.3.2015, http://www.cr-online.de/blog/2015/03/01/gesetzentwurf-zur-abschaffung-freier-wlans.
[83] BMJV, Leitlinien zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten v. 15.04.2015, S. 9.
[84] RefE, S. 9.
[85] *Hoeren*, Beck-Blog v. 15.3.2015, http://blog.beck.de/2015/03/15/eine-unversch-mtheit-der-regierungsentwurf-zur-wlan-haftung; s. auch die Stellungnahmen unter IV.

(entspricht § 8 TMG), und Art. 15 ECRL, der jedenfalls proaktive allgemeine Überwachungspflichten vollständig ausschließen soll (entspricht § 7 TMG), aber auch die Enforcement-RL 2004/48/EG sowie allgemeine verfassungsrechtliche Grundsätze. Dabei können § 8 Abs. 4 und 5 TMG-RefE grundsätzlich als gesetzgeberisches Abwägungsergebnis im Wege der praktischen Konkordanz angesehen werden.[86]

Unproblematisch ist in diesem Zusammenhang die Formulierung in § 8 Abs. 3 TMG-RefE. Denn dort wird lediglich klargestellt, dass WLANs auch unter die Privilegierung fallen. Mit Blick auf andere Ansprüche als solche auf Unterlassung sind auch § 8 Abs. 4 und 5 TMG-RefE nicht zu beanstanden, da die zusätzlichen Voraussetzungen ausdrücklich nur die Haftung auf Unterlassung berühren.

§ 8 Abs. 4 und 5 TMG-RefE regeln den Ausschluss der Haftung auf Unterlassung. Wer die jeweiligen Voraussetzungen erfüllt, haftet nicht als Unterlassungsschuldner. Im praktischen Umkehrschluss wird aber derjenige, der die jeweiligen Anforderungen nicht erfüllt, wohl auf Unterlassung haften, jedenfalls wird dies voraussichtlich die Handhabung der Praxis sein, zumal der Gesetzesentwurf Klarheit über die Privilegierung schaffen sollte.

In Deutschland herrschte lange Zeit Streit darum, wie weit das Verbot von Überwachungspflichten in Art. 15 ECRL reicht, insbesondere, ob die Anwendung der (in die Zukunft gerichteten) Störerhaftung einen Verstoß gegen Art. 15 ECRL darstellt.[87] Das LG München I hat diese Frage 2014 explizit an den EuGH gerichtet.[88] Allerdings hat der *EuGH* in der Entscheidung *UPC/Constantin* Pflichten des Access Providers zur Verhinderung von Rechtsverletzungen nicht *per se* als unzulässig angesehen,[89] so dass die Verurteilung eines Access Providers zur Unterlassung auch nicht *per se* einen Verstoß gegen Art. 15 ECRL darstellen dürfte.[90] Stellte man dies apodiktisch fest, wäre nur noch zu überprüfen, ob die im TMG-RefE vorgesehenen Pflichten zu einer allgemeinen Überwachungspflicht führen würden, was tatsächlich nicht der Fall ist. Denn Verschlüsselung, Erklärung, keine Rechtsverletzungen zu begehen, und Kenntnis des Namens betreffen allein den Zugang des Nutzers zum WLAN, nicht aber den übertragenen Datenstrom. Dementsprechend enthalten § 8 Abs. 4 und 5 TMG-RefE im Grundsatz keine auf eine Überwachung gerichteten Pflichten.

---

[86] BVerfG, 27.11.1990 – 1 BvR 402/87, NJW 1991, 1471 (1472) – Josefine Mutzenbacher; BVerfG, 7.3.1990 – 1 BvR 266/86, 1 BvR 913/87, NJW 1990, 1982; zum Ausgleich bei Intermediären unter Berücksichtigung der Rechtsprechung des EuGH und des BGH *Nolte/Wimmers*, GRUR 2014, 16 (22).

[87] Vgl. zur Problematik der Vorlagepflicht des BGH *Leible/Sosnitza*, NJW 2007, 3324; *Spindler*, JZ 2012, 311; *Spindler*, GRUR 2011, 101 (102).

[88] O. Fn. 21.

[89] EuGH, Urt. v. 27.3.2014 – C-314/12, GRUR 2014, 468 – UPC Telekabel/Constantin Film = K&R 2014, 329 m. Anm. *Assion*; dazu auch *Spindler*, GRUR 2014, 826; unklar zuvor EuGH GRUR 2011, 1025 – L'Oréal/Ebay.

[90] *Spindler*, GRUR 2014, 826 (827); *Brinkel/Osthaus*, CR 2014, 642 (646); *Mantz/Sassenberg*, MMR 2015, 85 (89).

Allerdings hat der EuGH in *UPC/Constantin* gefordert, dass bei jeder einzelnen Maßnahme, die einem Provider auferlegt werden soll, im konkreten Einzelfall die jeweils betroffenen Rechte gegeneinander abzuwägen sind. Namentlich sind daher bei jeder Maßnahme die jeweils durch den Nutzer verletzten Rechte auf der einen Seite, häufig Rechte des geistigen Eigentums (Art. 17 Abs. 2 EU-Grundrechtecharta (GRC)), die unternehmerische Freiheit des Access Providers (Art. 16 GRC), das Fernmeldegeheimnis (Art. 7 GRC[91]), der Schutz personenbezogener Daten (Art. 8 GRC[92]) sowie die Informationsfreiheit der Nutzer (Art. 11 GRC) auf der anderen Seite gegeneinander abzuwägen. Zusätzlich ist – auch mit Blick auf Art. 3 Abs. 1 der Enforcement-RL 2004/48/EG – zu überprüfen, ob die Maßnahmen geeignet, erforderlich und angemessen sind.[93] Diese Abwägung hat dazu geführt, dass jedenfalls im Rahmen der deutschen Rechtsprechung Filter- und Sperrpflichten als unzulässig angesehen wurden.[94]

Vor diesem Hintergrund sind nun die Maßnahmen in § 8 Abs. 4 und 5 TMG-RefE zu betrachten: Insbesondere die Verschlüsselung stellt hier einen massiven Eingriff in das Geschäftsmodell dar, das auf der einen Seite Kosten und Aufwand für ein WLAN erheblich steigert und andererseits die potenzielle Kundenbasis massiv beeinträchtigt. Es ist zu daher befürchten, dass die Wirtschaftlichkeit von WLANs praktisch entfällt. Auch an Geeignetheit, Erforderlichkeit und Angemessenheit bestehen Zweifel. Wie unter II.3.b.aa. und bb. dargestellt, verfehlen insbesondere Verschlüsselung und Erklärungserfordernis ihr Ziel. Sie sind daher ungeeignet oder wenigstens nicht angemessen. Die lapidare Erklärung der *Bundesregierung*, dass der Entwurf mit dem europäischen Recht konform sei, steht daher zumindest auf tönernen Füßen.

2. Vereinbarkeit mit den Plänen der EU-Kommission

Ein Problem könnte für die *Bundesregierung* auch aus Europa erwachsen. Der TMG-RefE sieht selbst vor, dass das Notifizierungsverfahren nach Richtlinie 98/34/EG (sog. „TRIS-Notifizierung“) durchgeführt werden soll.[95] Bisher ist diese Notifizierung noch nicht erfolgt, vermutlich soll dies nach Verabschiedung im Kabinett geschehen. Die *EU-Kommission* und die übrigen EU-Mitgliedsstaaten haben nach der Notifizierung drei Monate Zeit, um Bemerkungen vorzubringen (Art. 8 Abs. 2, 9 Abs. 1 RL 98/34/EG).

---

[91] *Mantz/Sassenberg*, MMR 2015, 85 (89); vgl. auch OLG Köln, Urt. v. 18.7.2014 – 6 U 192/11, GRUR 2014, 1081 – Goldesel.
[92] Vgl. EuGH, Urt. v. 24.11.2011 – C-70/10, GRUR 2012, 265 Rn. 50 – Scarlet Extended.
[93] EuGH, Urt. v. 24.11.2011 – C-70/10, GRUR 2012, 265 Rn. 48 – Scarlet Extended.
[94] OLG Köln, Urt. v. 18.7.2014 – 6 U 192/11, GRUR 2014, 1081 – Goldesel; vgl. auch *Brinkel/Osthaus*, CR 2014, 642; *Assion*, K&R 2014, 333.
[95] RefE, S. 9.

Es ist nicht auszuschließen, dass die *EU-Kommission* Einwände gegen den TMG-RefE erheben wird. Denn der TMG-RefE wird nicht nur das selbst gesteckte Ziel der Förderung von WLANs voraussichtlich verfehlen, er läuft auch den entsprechenden Zielen der *EU-Kommission* zuwider, die sich die Verbreitung und Förderung von WLANs im Europäischen Digitalen Binnenmarkt zum Ziel gesetzt hat. Insbesondere Art. 14 des Entwurf der DSM-VO zeugt davon, dass die Hürden beim Aufbau von flächendeckendem WLAN erheblich abgebaut werden sollen.[96] Wie unter II.3.b.aa.(1) dargestellt wird die erzwungene Verschlüsselung hier das Gegenteil bewirken. Die *EU-Kommission* könnte den TMG-RefE daher nach Art. 9 Abs. 3, 4 RL 98/34/EG sogar für 12 bzw. 18 Monate blockieren.

IV. Reaktionen

Die Reaktionen auf den Gesetzesentwurf waren – wie zu erwarten – weit überwiegend kritisch bis vernichtend. Bemerkenswert ist dabei, dass die Kritik nicht nur vom politischen Gegner oder von den betroffenen Gruppen, sondern sowohl aus den Reihen der Großen Koalition als auch durch große Verbände erfolgte.[97]

Bspw. der *eco*-Wirtschaftsverband kritisiert den Entwurf als zu unbestimmt, nicht praktikabel, da bestehende Anlagen umgerüstet werden müssten, und europarechtswidrig.[98] Der *vzbv* hält den Entwurf für „grundsätzlich verfehlt“ und europarechtswidrig, die Verschlüsselung für unzumutbar und rät von der Verabschiedung des Gesetzesentwurfs ab.[99] Nach dem Einzelhandelsverband *HDE* verhindere der Entwurf den schnellen und einfachen Zugang zum Internet, insbesondere Verschlüsselung und Anmeldeprozeduren seien hinderlich. Die vorgeschlagenen Lösungen seien nicht praktikabel.[100] Der *Deutsche Industrie- und Handelskammertag* (*DIHK*) bemängelt, dass durch die Neuregelung neue Infrastruktur geschaffen werden müsse, was erhebliche Kosten verursache. Fehlende Definitionen würden erneute Rechtsunsicherheit bringen. Es sei nicht gerechtfertigt, private gelegentliche Betreiber zu benachteiligen. Daher sei vor einer Regelung die Entscheidung des EuGH abzuwarten.[101]

---

[96] COM(2013), 627 final; eingehend *Mantz/Sassenberg*, CR 2014, 370.
[97] Eine Übersicht der an das BMWi gerichteten, öffentlichen Stellungnahmen (Stand 21.4.2015: 29) findet sich unter http://www.bmwi.de/DE/Themen/Digitale-Welt/Netzpolitik/Rechtssicherheit-WLAN/stellungnahmen.html.
[98] eco-Stellungnahme v. 8.4.2015, https://www.eco.de/wp-content/blogs.dir/20150408-eco-stellungnahme-2.telemedienaendg.pdf.
[99] vzbv-Stellungnahme v. 7.4.2015, http://zap.vzbv.de/e52a031a-62ff-4b6e-b51c-b793171d8d94/Haftungsbefreiung_WLAN_Stellungnahme-vzbv-2015-04-07.pdf.
[100] HDE-Stellungnahme v. 8.4.2015, http://www.einzelhandel.de/images/E-Commerce/Positionspapiere__Stellungsnahmen/20150408_Stellungnahme_-_Entwurf_eines_Zweiten_Gesetzes_zur_Anderung_des_Telemediengesetzes_Handelsverband_Deutschland.pdf.
[101] DIHK-Stellungnahme v. 8.4.2015, http://www.ihk-nuernberg.de/blogs/it-region-nuernberg/files/2015/04/Stellungnahme-DIHK-TMG.pdf.

Auch der *VATM* sieht die Verschlüsselungsverpflichtung als unverhältnismäßig an. Viele Anbieter von WLANs würden ihr Angebot einstellen oder einschränken. Der Gesetzesentwurf stehe in Widerspruch zur ECRL.[102] Nach der *Medienanstalt Berlin-Brandenburg* (*mabb*) gefährdet der Entwurf den dringend nötigen einfachen und unkomplizierten Zugang zu WLANs. Sie kritisiert weiter die Ungleichbehandlung von WLAN-Betreibern.[103] Das Ende eines zivilgesellschaftlichen Engagements bei freien WLANs sei zu befürchten.[104] Der *Digitale Gesellschaft e.V.* erklärte, dass der TMG-RefE das fehlende Verständnis des Gesetzgebers offenbare.[105]

Auch aus der Politik kam Kritik. Neben kritischen Stimmen der Opposition lehnte auch die *Medien- und Netzpolitische Kommission* der *SPD* den TMG-RefE ab.[106] *Markus Söder* (CSU) twitterte, dass „Freies WLAN keine Störerhaftung brauche".[107]

V. Fazit und Ausblick

Die Folgen einer Verabschiedung des Gesetzesentwurfs lassen sich nur schwer vorhersagen. Das Ziel einer Förderung und weiteren Verbreitung von WLANs wird er aber voraussichtlich verfehlen. Wer die Voraussetzungen des Gesetzesentwurfs umsetzen will, muss mit deutlich erhöhten Kosten bei Einrichtung und Betrieb sowie der Umrüstung bisheriger Systeme rechnen. Auch verschlechtert sich durch den RefE die Rechtslage gegenüber der Ist-Situation, da die Gerichte (richtigerweise) Verschlüsselung und Erklärung gerade nicht fordern. Aufgrund der zukünftig zu erwartenden höheren Komplexität von WLAN-Systemen ist damit zu rechnen, dass entweder WLAN-Hotspots abgebaut oder alternativ – mit entsprechenden Kosten – Fertigpakete von kommerziellen Anbietern erworben werden. Zusätzlich werden die Nutzerzahlen umgerüsteter Hotspots wohl drastisch sinken, da der Zugang zum WLAN mittels Verschlüsselung erheblich erschwert wird und Nutzer durch Anmelde- und Registrierungsprozeduren zusätzlich abgeschreckt werden.

Reaktion auf die kontraproduktiven und überspitzten Anforderungen könnte daher sein, dass der Entwurf entweder weitgehend ignoriert wird, oder die Betroffenen Umgehungslösungen einrichten. So kann insbesondere durch eine Umleitung des Verkehrs mittels Virtual Private

---

[102] VATM-Stellungnahme vom 8.4.2015.
[103] mabb-Stellungnahme v. 7.4.2015, http://www.mabb.de/files/content/document/Stellungnahmen/mabb_Stellungnahme_BMWi_TMGAendG.pdf
[104] mabb-Stellungnahme v. 18.03.2015, http://www.mabb.de/presse/pressemitteilungen/details/wlan-zugang-ohne-barrieren.html.
[105] Stellungnahme v. 9.4.2015, https://digitalegesellschaft.de/2015/04/stoererhaftung-sie-koennen-es-nicht.
[106] Stellungnahme v. 27.2.2015, https://www.spd.de/presse/Pressemitteilungen/127562/20150227_netzwerkpolitiker_stoererhaftung.html.
[107] Tweet v. 15.4.2015, https://twitter.com/Markus_Soeder/status/588311851848572928.

Networks (VPN) die Identität des eigentlichen Anbieters verschleiert und damit die Geltendmachung von Ansprüchen (rein faktisch) verhindert werden.[108] Nach außen tritt dann ein traditionelles Telekommunikationsunternehmen oder sogar ein VPN-Dienst im Ausland auf, die mit dem Server, der nach außen sichtbar ist („*Exit Node*"), einer Verschlüsselungspflicht nach § 8 TMG nicht unterliegen.

Obwohl es sich bei dem TMG-RefE um ein Thema handelt, das die *Bundesregierung* für ihre Digitale Agenda als wesentlich ansieht, ist mit einer Verabschiedung jedenfalls im Sommer diesen Jahres nicht mehr zu rechnen. Insbesondere das Notifizierungsverfahren bei der *EU-Kommission* kann längere Zeit in Anspruch nehmen. Die *Bundesregierung* sollte zudem überlegen, ob und wie sie auf die harsche Kritik am RefE reagieren will.

Angesichts der oben dargestellten Probleme sollte der TMG-RefE in dieser Form nicht in den *Bundestag* eingebracht werden. Die Kritik aus praktisch allen Bereichen (Verbände der Wirtschaft und Verbraucher, digitaler Gesellschaft und Politik) sollte nicht ungehört verhallen. Es ist der *Bundesregierung* daher insgesamt anzuraten, zunächst die Entscheidung des EuGH im oben angesprochenen Vorlageverfahren abzuwarten.

***

[108] Vgl. *Mattke*, Technology Review v. 25.3.2015, http://m.heise.de/tr/artikel/Tricks-fuer-offene-WLANs-ohne-Haftungsrisiko-2583166.html.