# Kommunikation & Recht

## Betriebs-Berater für
## ● Medien ● Telekommunikation ● Multimedia

5
K&R



18. Jahrgang Mai 2015 Seiten 289 – 360

dfv Mediengruppe · Frankfurt am Main

Kommunikation & Recht

K&R 5/2015



RA Dr. Christian Volkmann, Berlin*

# Freies WLAN für einen Cappuccino

*Der aktuell diskutierte Referentenentwurf der Bundesregierung zum Zweiten Gesetz zur Änderung des Telemediengesetzes enthält erstmals Haftungsregelungen für die Betreiber von WLAN-Netzen sowie darüber hinaus Einschränkungen der Haftungsprivilegierungen für gefahrgeneigte Hosting-Dienste. Es gibt Verbesserungspotential.*

## I. Einleitung

Wer hätte das gedacht: Es sind die Wettbewerbsnachteile von Cafés oder Hotels, die ein freies WLAN unumgänglich machen. Wer geglaubt haben sollte, dass es in der digitalen Gesellschaft von wirtschaftlicher Bedeutung sei, dass möglichst viele Personen an möglichst vielen Orten einen Netzzugang haben, wird sich verwundert die Augen reiben. Ohne Cappuccino soll es kein freies WLAN geben. Nur wer neben einem WLAN-Zugang noch etwas Geschäftliches zu bieten hat, soll von Haftungserleichterungen profitieren können. Gleiches soll für öffentliche Einrichtungen gelten. Zu gefährlich sind die in den Privathaushalten bereitgehaltenen WLAN-Netzwerke. Zu gefährlich sollen wohl auch offene Netze sein, die ohne jedes Entgelt für Nutzer bereitgehalten werden. Wer freies WLAN möchte, muss ins Café oder in die Bibliothek.

Schon wer die ersten Sätze der Problemdarstellung des Referentenentwurfs der Bundesregierung liest, weiß, dass da kein besonders ausgewogener Vorschlag kommen kann. Wer ein freies WLAN nicht mit dem öffentlichen Bedürfnis privater und insbesondere auch geschäftlicher Netzsucher nach einem öffentlichen Zugang zum Internet begründet, sondern mit den geschäftlichen Interessen potentieller WLAN-Anbieter und deren Wettbewerbsnachteilen (gegenüber wem eigentlich?), wählt schon den falschen Ansatz. Wer Hotspots fördern will, indem er das Haftungsrisiko nur derjenigen einschränken möchte, die ihren Kunden neben einer anderen Leistung als Zusatz einen Hotspot bieten – die Bundesregierung nennt hier Cafés, Restaurants, Hotels, Einzelhändler, Touristeninformationen, Bürgerämter und Arztpraxen – fördert vielleicht die geschäftlichen Interessen dieser Anbieter, indem er für diese zusätzliche Kunden anlockt, aber wohl kaum in erster Linie die Interessen einer digitalen Gesellschaft.

Es bietet Trost, dass es sich bei dem hier besprochenen Entwurf um einen Referentenentwurf handelt, der noch nicht endgültig abgestimmt ist. Darüber hinaus soll für eine der vorgeschlagenen Regelungen ausdrücklich noch Diskussionsbedarf bestehen, nämlich gerade für den besonders heiklen § 8 Abs. 5 TMG-RefE. Dies soll keine Schwächen in der Formulierung des Referentenentwurfs und in der Begründung entschuldigen, lässt aber hoffen, dass Abstimmung und Diskussion noch etwas bewirken können.

## II. Die gesetzgeberische Intention

Da die Verbreitung von Breitband in Deutschland den Anforderungen der digitalen Gesellschaft seit Jahren hinterherhinkt, will die Bundesregierung eine möglichst weitreichende Versorgung mit öffentlichen WLANs sicherstellen. Dies ist begrüßenswert und überfällig. Mit dem Referentenentwurf wird die Bundesregierung dieses Ziel allerdings nicht erreichen.

Richtig ist die Annahme der Bundesregierung, dass für die Anbieter öffentlich zugänglicher WLAN-Netze in Deutschland Rechtsunsicherheit besteht. Die deutschen Gerichte einschließlich des BGH haben sich bislang lediglich mit der Haftung häuslich betriebener WLANs beschäftigt. Deren Haftung dürfte nicht zuletzt aufgrund der BGH-Entscheidung „Sommer unseres Lebens" zwar unbefriedigend, aber gleichwohl geklärt sein: Wer seinen WLAN-Zugang nicht verschlüsselt, kann zur Haftung herangezogen werden, wenn unberechtigte Dritte den Zugang für Rechtsverletzungen missbrauchen.[1] Zieht man die Rechtsprechung des BGH zur Haftung der Anschlussinhaber heran („Morpheus"[2] und „BearShare"[3]), ergibt sich ein recht klares Bild: Derjenige, der anderen den Zugang zum Internet ermöglicht, kann für von Dritten begangene Rechtsverletzungen haften, wenn damit zu rechnen ist, dass diese Dritten Rechtsverletzungen begehen könnten. Dies kann der Fall sein, wenn das Netz nicht vor dem Zugriff Unberechtigter geschützt ist („Sommer unseres Lebens"), wenn Minderjährige über das Netz auf das Internet zugreifen („Morpheus"), aber nicht, wenn der vom WLAN-Anbieter gestattete Netzzugang z. B. durch Volljährige erfolgt („BearShare"). Damit ist der private WLAN-Anbieter einigermaßen sicher, wenn er sein WLAN gegen den Zugriff Unberechtigter schützt.

Noch nicht von der höherinstanzlichen Rechtsprechung entschieden ist die Haftung der Anbieter, die gezielt offenes WLAN anbieten. Bei diesen sollte im Hinblick auf die Auferlegung von Pflichten zur Verhinderung von Rechtsverletzungen äußerste Zurückhaltung geboten sein.[4] Ob dies allerdings auch die Rechtsprechung so sieht und welche Pflichten diese den Anbietern offener WLAN-Netze auferlegen möchte, ist freilich offen. So ist bislang ungeklärt, ob auf WLAN-Anbieter die Haftungserleichterungen des TMG Anwendung finden. In der Rechtsprechung ungeklärt sind auch die Sicherungspflichten dieser Anbieter. Es fällt jedoch schwer, anzunehmen, dass der

* Mehr über den Autor erfahren Sie auf S. VIII.

1 BGH, 12. 5. 2010 – I ZR 121/08, K&R 2010, 492, Rn. 23 – Sommer unseres Lebens.

2 BGH, 15. 12. 2012 – I ZR 74/12, K&R 2013, 322 – Morpheus.

3 BGH, 8. 1. 2014 – I ZR 169/12, K&R 2014, 513 – BearShare.

4 *Spindler*, CR 2010, 592, 599; *Spindler/Volkmann*, in: Spindler/Schuster, Recht der elektronischen Medien, 3. Aufl. 2015, § 1004 BGB, Rn. 25.

BGH bei einem versehentlich offenen Netz („Sommer unseres Lebens“) einen strengeren Haftungsmaßstab anlegt, als bei einem gezielt offenen Netz, sei es betrieben von einem DEHOGA-Betrieb oder von einer Privatperson. Auch Auswüchse in der Rechtsprechung, die Anschlussinhaber mit Schadensersatz belasten, tragen nicht zur Rechtssicherheit bei.[5] Der Referentenentwurf möchte möglichen Haftungsrisiken durch die Rechtsprechung vorgreifen und Klarheit schaffen.

## III. Systematik und Regelungen

In einem ersten Schritt unterstellt die Bundesregierung in § 8 Abs. 3 TMG-RefE alle WLAN-Anbieter den Haftungsprivilegierungen der Access-Provider nach § 8 Abs. 1 TMG. In einem zweiten Schritt sieht die Bundesregierung im Fall von Rechtsverletzungen über den WLAN-Zugang ausdrücklich die Haftung der WLAN-Betreiber auf Unterlassen („Störerhaftung“) vor, wenn nicht bestimmte Voraussetzungen gegeben sind (§ 8 Abs. 4 a) und b) TMG-RefE: „Diensteanbieter (…) haften *nur* dann nicht als Störer auf Unterlassen, wenn (…)“). Liegen diese Voraussetzungen vor, scheidet die Störerhaftung auf Unterlassen aus. Um dies zu erreichen, müssen WLAN-Anbieter ihre Dienste angemessen gegen unberechtigten Zugriff sichern und eine Einwilligung der Nutzer einholen, dass diese keine Rechtsverletzungen begehen werden. Die Bundesregierung scheint damit – ein bemerkenswerter Ansatz für das haftungserleichternde TMG – eine haftungsbegründende Anspruchsnorm bzw. jedenfalls eine Zurechnungsnorm für die Haftung auf Unterlassen als Störer zu schaffen. Damit greift die Bundesregierung über das TMG in die allgemeinen Haftungsnormen und die dazu ergangene Rechtsprechung des UrhG, des MarkenG und des BGB ein, gar nicht zu denken an das Wettbewerbsrecht, in dem es gar keine Störerhaftung mehr gibt,[6] wohl aber natürlich eine Haftung auf Unterlassen.

### 1. WLANs unterfallen § 8 TMG

In § 8 Abs. 3 TMG-RefE werden die Anbieter von WLANs den Access-Providern gleichgestellt. Diese Klarstellung ist schon deshalb geboten, weil der BGH die Anwendung der Haftungsprivilegierungen des TMG jedenfalls bei privat betriebenen WLAN-Anschlüssen ausdrücklich abgelehnt hat,[7] diese nach dem Willen der Bundesregierung aber ausdrücklich von der Haftungserleichterung des § 8 Abs. 1 TMG profitieren sollen. Im Hinblick auf offene Netze ist die Rechtsprechung erst seit Kurzem und auf unterer Ebene zu der (richtigen) Erkenntnis gelangt, dass WLAN-Anbieter als Zugangsvermittler von den Haftungserleichterungen des TMG profitieren müssen.[8] Es ist aber zu erwarten, dass sich auch der EuGH – nach Vorlagebeschluss des LG München[9] – der Auffassung anschließen wird, dass der Betrieb eines WLANs die Vermittlung des Zugangs zu einem Kommunikationsnetz im Sinne von Art. 12 Abs. 1 der Richtlinie ist.[10]

Im weitesten Sinne ausgeschlossen sind nach § 8 Abs. 3 TMG-RefE Schadensersatzansprüche gegen die WLAN-Anbieter sowie eine strafrechtliche Verantwortlichkeit der WLAN-Anbieter.

### 2. Sicherungsmaßnahmen gewerblicher Nutzer und öffentlicher Einrichtungen

Nach § 8 Abs. 4 S. 1 TMG-RefE haftet der WLAN-Betreiber als Störer auf Unterlassen, wenn er nicht die ihm zumutbaren Maßnahmen ergreift, um eine Rechtsverletzung durch Dritte zu verhindern. In § 8 Abs. 4 S. 1 TMG-RefE sind Maßnahmen genannt, die die Bundesregierung „insbesondere“ erwartet, nämlich Verschlüsselung und die Abforderung einer Einwilligung durch den Nutzer, dass er keine Rechtsverletzungen über den Zugang begehen werde.

Gesetzestechnisch schafft die Bundesregierung dadurch zwei Voraussetzungen (a) und (b), die erfüllt sein müssen, damit der Anbieter nicht als Störer haftet. Leicht übersehen werden kann aber, dass sie darüber hinaus noch eine dritte Voraussetzung schafft, nämlich die generelle Pflicht, zumutbare Maßnahmen zur Verhinderung von Rechtsverletzungen zu ergreifen. Diese ist gewiss nicht durch das Wörtchen „insbesondere“ beschränkt. Es ist niemandem zu wünschen, eine Unterlassungserklärung mit einer „insbesondere“-Formulierung in dem Vertrauen darauf abzugeben, dass sich die Unterlassungserklärung dann auch nur auf den unter „insbesondere“ aufgeführten, konkreten Verstoß erstreckt. Jeder, der dies tut, wird spätestens bei der Geltendmachung der Vertragsstrafe durch den Gläubiger merken, dass „insbesondere“ gerade nicht das Vorstehende beschränkt, sondern lediglich ein konkretisiertes Beispiel ankündigt.

Im Ergebnis müssen WLAN-Anbieter daher „zumutbare Maßnahmen“ ergreifen, um Rechtsverletzungen durch Dritte über ihren Zugang zu verhindern; ansonsten haften sie als Störer auf Unterlassen. Diese zumutbaren Maßnahmen bedürfen der Ausgestaltung durch die Rechtsprechung, was auch der Bundesregierung klar ist, da sie die Einzelfallentscheidungen der Rechtsprechung zu den Pflichten der Anbieter als Grund für die bestehende Rechtsunsicherheit erkennt. Dieses Problem wird allerdings durch die Formulierung „zumutbare Maßnahmen“ und die Aufführung von nicht abschließenden Mindestmaßnahmen nicht beseitigt.

Die in § 8 Abs. 4 S. 2 a) und b) TMG-RefE aufgeführten Mindestmaßnahmen zeigen zudem, dass im Bundeswirtschaftsministerium wenig Verständnis von Internet-Nutzung vorzuherrschen scheint. Eine Verschlüsselung soll danach eine Voraussetzung sein, um die Störerhaftung auszuschließen. Allerdings ist nun gerade derjenige, der über das WLAN auf das Netz zugreift und dort Rechtsverletzungen begeht, bereits über das Stadium der Verschlüsselung hinaus. Vor diesem Hintergrund soll die Auflage der Verschlüsselung wohl gewährleisten, dass der Nutzer eingewilligt hat, keine Rechtsverletzungen zu begehen (was ihn davon allerdings nicht abhalten wird), oder dass der Nutzer seine Rechtsverletzung wenigstens mit einem Cappuccino finanziert, nachdem er sich beim Caféinhaber den WLAN-Schlüssel besorgt hat.

### 3. Sicherungsmaßnahmen privater Anbieter

Das Vorstehende gilt gleichermaßen für geschäftsmäßige Dienste und öffentliche Einrichtungen wie auch für private WLAN-Anbieter. Private Anbieter müssen für den Aus-

5 LG München, 19. 6. 2008 – 7 O 16 402/07, K&R 2008, 474, 476 zur Haftung wegen einer Verletzung der elterlichen Aufsichtspflicht.
6 St. Rspr. seit BGH, 12. 7. 2007 – I ZR 18/04, K&R 2007, 517 – Jugendgefährdende Medien bei eBay.
7 BGH, 12. 5. 2010 – I ZR 121/08, K&R 2010, 492, Rn. 24 – Sommer unseres Lebens.
8 AG Hamburg, 10. 6. 2014 – 25 b C 431/13, CR 2014, 536 m. Anm. *Mantz*; AG Charlottenburg, 17. 12. 2014 – 217 C 121/14, CR 2015, 192, Rn. 21.
9 LG München, 18. 9. 2014 – 7 O 14 719/12, K&R 2014, 827.
10 S. auch *Hoffmann*, in: Spindler/Schuster (Fn. 4), § 8 TMG, Rn. 1.

schluss der Störerhaftung darüber hinaus allerdings noch eine weitere Hürde nehmen (§ 8 Abs. 5 TMG-RefE): Sie müssen auch den Namen ihrer Nutzer kennen. Dies wirft mehrere Fragen auf:

*a) Differenzierung zwischen geschäftsmäßigen und nicht geschäftsmäßigen Anbietern*

Nach der Auffassung der Bundesregierung soll ein offenes Netz, das ohne wirtschaftlichen Hintergrund oder nicht von einer öffentlicher Einrichtung betrieben wird, haftungsrechtlich schlechter stehen, als ein offenes Netz, das von einem gewerblichen Anbieter zur Verfügung gestellt wird, § 8 Abs. 5 TMG-RefE. Anders formuliert: Wer zur Förderung geschäftlicher Zwecke eine Gefahr schafft, wird gegenüber demjenigen privilegiert, der privat eine Gefahr schafft.

Die Bundesregierung macht in ihrer Begründung zu § 8 Abs. 5 TMG-RefE ein Gefahrengefälle zwischen privaten WLAN-Anbietern und öffentlichen Anbietern aus. Warum aber gerade in Privathaushalten die Gefahr von Rechtsverletzungen höher sein soll als beispielsweise in Hotelzimmern, geht aus der Begründung nicht hervor. Die Auffassung, dass öffentliche Einrichtungen als Anbieter – gerade Universitäten – durch eine soziale (öffentliche) Kontrolle eher gewährleisten, dass Urheberrechtsverletzungen nicht stattfinden, als privat tätige Anbieter, ist eine reine Fiktion. Dass ein Straftäter sich im Café kaum kinderpornografische Inhalte ansieht, worauf der Gesetzgeber in der Begründung zur Störerhaftung verweist, dürfte klar sein. Er wird dies aber auch nicht bei einem Besuch in einem Privathaushalt tun. Die Annahme, dass sich jemand vom Kellner davon abhalten lässt, Filesharing zu betreiben, oder einen beleidigenden Forumsbeitrag zu schreiben, ist weltfremd. Außerdem: Wo ist die Kontrolle des Nutzers am Flughafen? Wo ist die Kontrolle des Nutzers im Hotelzimmer? Und was passiert, wenn der internet-affine Kellner durch einen Blick über die Schulter des Gastes entdeckt, dass dieser illegales Filesharing betreibt? Wird es einen Eklat im Café geben?

Ein weiterer Grund für die Differenzierung soll nach Auffassung der Bundesregierung die Möglichkeit des geschäftlich tätigen Anbieters sein, dem Nutzer die weitere Nutzung des WLAN zu untersagen. Es stellt sich allerdings die Frage, warum ein häuslicher, nicht geschäftlicher WLAN-Betreiber die Nutzung seines Zugangs nicht untersagen können soll. Dieser verliert bei einem Eklat vor unbeteiligten Dritten jedenfalls keine Cappuccino-trinkenden Stammkunden.

Es bleibt festzuhalten, dass es für die Differenzierung keine nachvollziehbare Begründung gibt, außer man will Gewerbebetriebe und öffentliche Einrichtungen gezielt fördern.

*b) Name des Nutzers*

Zum Ausgleich der nach Auffassung der Bundesregierung größeren Gefahr durch den Betrieb eines privaten WLAN, muss der Betreiber den Namen des Nutzers kennen. Ist dies der Fall, ist er haftungsmäßig dem geschäftlich Tätigen bzw. der öffentlichen Einrichtung gleichgestellt. Ist dies nicht der Fall, haftet er als Störer auf Unterlassen. Aber was passiert, wenn der WLAN-Betreiber die Namen aller potentiellen Nutzer kennt, wie dies in Haushalten und Büros regelmäßig der Fall ist? Wem soll das dann bei der Verfolgung von Rechtsverstößen nützen?

### 4. Haftung für Host-Provider

Nicht unerwähnt bleiben sollen die Regelungen, die die Bundesregierung zur Verschärfung der Haftung bestimmter Host-Provider vorsieht, § 10 Abs. 2 TMG-RefE. Es ist in der Rechtsprechung unbestritten, dass Dienste, die besonders gefahrgeneigt sind oder sogar Rechtsverletzungen fördern, höheren Aufwand betreiben müssen, um Rechtsverletzungen zu vermeiden.[11] Dies ist nichts Neues. § 10 Abs. 2 TMG-RefE verschärft aber nicht die Maßnahmen, die Host-Provider zur Verhinderung von Rechtsverletzungen ergreifen müssen. Die Regelung verschärft vielmehr per se die Haftung, indem bestimmte Host-Provider überhaupt nicht mehr von der Privilegierung des § 10 Abs. 1 TMG profitieren sollen.

Dieser weitreichende Ausschluss der Haftungsprivilegierung in den von der Bundesregierung vorgesehenen Fällen, dürfte kaum richtlinienkonform sein, sondern vielmehr Art. 14 Abs. 1 der RL 2000/31/EG in unzulässiger Weise einschränken. § 10 Abs. 2 TMG-RefE geht weit über die Maßnahmen hinaus, die die Mitgliedsstaaten den Anbietern nach Art. 14 Abs. 3 der RL 2000/31/EG zur bloßen „Rechtsverletzungsverhinderung“ (d. h. im Wesentlichen im Rahmen der Störerhaftung) auferlegen können. Sie erweitern die Verantwortlichkeit auch im Bereich der Sanktionen (Schadensersatz und Strafrecht) über den Geltungsbereich von Art. 14 Abs. 1 der RL 2000/31/EG hinaus.

Ganz davon abgesehen, ist es an der Zeit, den Fokus bei der Beurteilung der Frage, von wem die Gefahr für Rechtsgüter im Internet ausgeht, weniger auf die Dienste, die diese Inhalte verbreiten, zu richten. Dienste mögen ein Gefahrenpotential haben, wenn sie auch oder überwiegend oder gar ausschließlich rechtswidrige Inhalte speichern. Gefährlich ist aber vor allem der Nutzer, d. h. der eigentliche Täter einer Rechtsverletzung, der den Dienst für diese verwendet. Der eigentliche Gefahrentatbestand besteht daher wohl am ehesten darin, dass der Diensteanbieter den eigentlichen Täter durch die Ermöglichung der anonymen Nutzung seines Dienstes vor einer Rechtsdurchsetzung durch die Verletzten bewahrt.[12] Möglicherweise wäre dies ein Ansatz, den auch die Bundesregierung – jedenfalls im Rahmen der Haftung auf Unterlassen – im TMG verfolgen könnte.

## IV. Ergebnis

Positiv hervorzuheben ist der Ausschluss von Schadensersatzansprüchen gegen WLAN-Betreiber für Rechtsverletzungen, die über ihr WLAN begangen werden. Bei der Störerhaftung gibt es Nachbesserungsbedarf, insbesondere auch im Hinblick auf die privat tätigen Anbieter offener Netze. Das Ziel, mehr Rechtssicherheit für WLAN-Anbieter zu schaffen, erreicht die Bundesregierung mit ihrem Entwurf jedenfalls im Bereich der Störerhaftung nicht. Hier haben die Gerichte weiterhin Spielraum. Nicht gelungen ist die Verschärfung der Haftung bestimmter Host-Provider. Die im Entwurf vorgeschlagene Regelung verfolgt einen falschen Ansatz und dürfte zudem nicht europarechtskonform sein.

---

11 BGH, 15. 1. 2009 – I ZR 57/07, K&R 2009, 637, Rn. 21 f. – Cybersky; BGH, 15. 8. 2013 – I ZR 80/12, K&R 2013, 655, Rn. 36 – File-Hosting-Dienst, s. dazu *Spindler/Volkmann*, in: Spindler/Schuster (Fn. 4), § 1004 BGB, Rn. 24 f.

12 *Spindler/Volkmann*, in: Spindler/Schuster (Fn. 4), § 1004 BGB, Rn. 25.