Einführung in das Medienrecht

Zivilrechtliche Grundlagen

Skript 3

Einführung in die Störerhaftung

Die Haftung der Access Provider

Dr. Mischa Dippelhofer

Fall 6

Herr Frank Frey, Inhaber des Internetcafés „Surf & Sauf“ in der Innenstadt von Saarbrücken, kommt in Ihre Kanzlei.

Er betreibt in seinem Café ein offenes WLAN, das jeder kostenlos nutzen kann. Die Nutzung ist nicht auf die Gäste seines Cafés beschränkt, es ist auch keine Anmeldung erforderlich. Jedem Nutzer wird lediglich als Startseite eine Seite mit Informationen über sein Café angezeigt.

Herr Frey berichtet Ihnen, dass sein WLAN-Router eine Reichweite von etwa 500 Metern habe und außer seinem Café auch weite Teile der Nachbarschaft abdecke. Er erhofft sich dadurch eine größere Bekanntheit seines Cafés. Dieses Konzept sei auch erfolgreich, er habe einige Stammkunden hinzugewonnen, die in der Nachbarschaft wohnen und dort sein WLAN-Netzwerk gefunden haben. Nun würden sie ihren Kaffee regelmäßig in seinem Café trinken.

Nun hat er eine Abmahnung erhalten, in der er für eine Urheberrechtsverletzung eines Benutzers verantwortlich gemacht wird.

Herr Frey versteht „die Welt nicht mehr“. Er stelle doch lediglich einen Internet-Zugang zur Verfügung, da könne er doch für die Rechtsverletzungen der Benutzer genauso wenig verantwortlich sein „wie die Post für Briefbomben“.

Sollte die Abmahnung berechtigt sein, müsse er sein WLAN-Netz und sein Internet-Café schließen, denn die dort genannten Anforderungen könne er niemals erfüllen. Seine Kunden würden es sehr schätzen, anonym zu surfen. Er sei auch nicht bereit, für die Rechteverwerter „Stasi zu spielen“.

Was raten Sie Herrn Frey?

Wie funktioniert ein WLAN-Netzwerk?

WLAN-Netzwerke funktionieren normalerweise im „Infrastruktur-Modus“:

Ein Router fungiert als zentrale Vermittlungsstelle. Er sendet ständig Datenpakete („Beacons“), die Geräten mit WLAN-Ausstattung signalisieren, dass ein WLAN-Netzwerk vorhanden ist. Die Beacons enthalten gewöhnlich auch den Namen des Netzwerks und ggf. die verwendete Verschlüsselung.

Empfängt ein Endgerät im Übertragungsbereich des Routers die Beacons, kann es sich mit dem Netzwerk verbinden, indem es seinerseits Datenpakete mit einer Verbindungsanfrage an den Router sendet.

Der Router lässt die Verbindung dann entweder unmittelbar zu (offenes WLAN) oder fragt zunächst ein Kennwort ab (geschlossenes WLAN).

Ist die Verbindung hergestellt, besteht ein lokales Netzwerk mit der Möglichkeit, zwischen allen Endgeräten, die eine Verbindung aufgebaut haben, miteinander zu kommunizieren.

WLAN-Netzwerke im Infrastrukturmodus sind damit technisch gesehen Telekommunikationsnetzwerke.

WLAN-Netzwerke vermitteln häufig den Zugang ins Internet:

Die meisten WLAN-Router bieten Anschlussmöglichkeiten für Ethernet-Kabel, mit denen eine Verbindung ins Internet hergestellt werden kann

Verbinden sich die angeschlossenen Endgeräte auf diese Weise ins Internet, übernimmt der WLAN-Router für diese Geräte die Funktion der Verbindung des WLAN-Netzwerkes mit dem Internet

Technisch gesehen sind Anbieter von WLAN-Netzwerken daher zugleich auch Zugangsvermittler ins Internet.

Das Urhebergesetz

§ 1 UrhG - Allgemeines

Die Urheber von Werken der Literatur, Wissenschaft und Kunst genießen für ihre Werke Schutz nach Maßgabe dieses Gesetzes.

Urheberrechte bestehen somit an schutzfähigen Werken.

Gesetzliche Übersicht über die geschützten Werke

§ 2 UrhG - Geschützte Werke

(1) Zu den geschützten Werken der Literatur, Wissenschaft und Kunst gehören insbesondere:

1. *Sprachwerke, wie Schriftwerke, Reden und Computerprogramme;*
2. *Werke der Musik;*
3. *pantomimische Werke einschließlich der Werke der Tanzkunst;*
4. *Werke der bildenden Künste einschließlich der Werke der Baukunst und der angewandten Kunst und Entwürfe solcher Werke;*
5. *Lichtbildwerke einschließlich der Werke, die ähnlich wie Lichtbildwerke geschaffen werden;*
6. *Filmwerke einschließlich der Werke, die ähnlich wie Filmwerke geschaffen werden;*
7. *Darstellungen wissenschaftlicher oder technischer Art, wie Zeichnungen, Pläne, Karten, Skizzen, Tabellen und plastische Darstellungen.*

Diese Aufzählung ist nicht abschließend (Wandke/Bullinger-Bullinger § 2 RN 153).

Das schutzfähige Werk

§ 2 UrhG - Geschützte Werke

(2) Werke im Sinne dieses Gesetzes sind nur persönliche geistige Schöpfungen.

Voraussetzung ist somit das Vorliegen einer persönlichen geistigen Schöpfung.

An die Schöpfungshöhe werden aber nur geringe Anforderungen gestellt, auch die „kleine Münze“ ist geschützt (Ahlberg/Götting-Ahlberg § 2 RN 95).

Bei Musikwerken genügt eine individuelle Komposition, auf die künstlerische Bedeutung oder die Länge des Werkes kommt es nicht an (Wandtke/Bullinger-Bullinger § 2 RN 70). Es genügt ein geringer Eigentümlichkeitsgrad der Komposition. Nur wenn jede Eigentümlichkeit fehlt, ist die Werksqualität zu verneinen (Ahlberg/Götting-Ahlberg § 2 RN 95 f).

Selbst der Schutz von Handyklingeltönen kommt wegen ihrer zunehmenden Länge und Komplexität in Betracht (Wandtke/Bullinger-Bullinger § 2 RN 73).

Bei einem gesamten Album kann von einer Schutzfähigkeit ausgegangen werden.

In Fall 6 handelt es sich um ein schutzfähiges Werk der Musik

Die Rechte des Urhebers

§ 7 Urheber

Urheber ist der Schöpfer des Werkes.

In Fall 6 ist Troubardix der alleinige Urheber.

Übersicht über die Rechte des Urhebers

1. **Verwertungsrechte (§ 15 UrhG):**
   - Vervielfältigungsrecht (§ 16 UrhG)
   - Verbreitungsrecht (§ 17 UrhG)
   - Ausstellungsrecht (§ 18 UrhG)
   - Vortrags-, Aufführungs- und Vorführungsrecht (§ 19 UrhG)
   - Recht der öffentlichen Zugänglichmachung (§ 19a UrhG)
   - Sende- und Wiedergaberechte (§§ 20 ff UrhG)

2. **Urheberpersönlichkeitsrechte:**
   - Recht, über Veröffentlichung zu bestimmen (§ 12 UrhG)
   - Recht der Benennung als Urheber (§ 13 UrhG)
   - Abwehrrecht gegen Entstellung des Werkes (§ 14 UrhG)

Der ausübende Künstler

§ 73 Ausübender Künstler
Ausübender Künstler im Sinne dieses Gesetzes ist, wer ein Werk oder eine Ausdrucksform der Volkskunst aufführt, singt, spielt oder auf eine andere Weise darbietet oder an einer solchen Darbietung künstlerisch mitwirkt.

In Fall 6 ist Troubardix alleiniger Interpret.

Übersicht über die Rechte des ausübenden Künstlers:

1. **Leistungsschutzrechte:**
    - Aufnahme- Vervielfältigungs- und Verbreitungsrecht (§ 77 UrhG)
    - Recht der öffentlichen Wiedergabe (§ 78 UrhG)
2. **Urheberpersönlichkeitsrechte**
    - Recht auf Anerkennung als ausübender Künstler(§ 74 UrhG)
    - Recht auf Verbietung von Beeinträchtigungen (§ 75 UrhG)

Verletzung von Rechten des Urhebers?

§ 19a Recht der öffentlichen Zugänglichmachung

Das Recht der öffentlichen Zugänglichmachung ist das Recht, das Werk drahtgebunden oder drahtlos der Öffentlichkeit in einer Weise zugänglich zu machen, dass es Mitgliedern der Öffentlichkeit von Orten und zu Zeiten ihrer Wahl zugänglich ist.

Werden Daten auf einem Computer bereitgestellt mit dem Angebot an Nutzer einer Filesharingbörse, sie jederzeit herunterladen zu können, liegt eine öffentliche Zugänglichmachung vor (Wandtke/Bulllinger-Bullinger § 19a RN 23).

Das ist bei Filesharing-Tauschbörsen regelmäßig der Fall, selbst wenn der Benutzer nur Dateien herunterladen will, da alle Dateien, die heruntergeladen werden, zugleich allen anderen Benutzern der Tauschbörse freigegeben werden.

Das Recht der öffentlichen Zugänglichmachung ist verletzt.

Verletzung von Rechten des ausübenden Künstlers?

§ 78 UrhG Öffentliche Wiedergabe

(1) Der ausübende Künstler hat das ausschließliche Recht, seine Darbietung

1. öffentlich zugänglich zu machen (§ 19a),
2. zu senden, es sei denn, dass die Darbietung erlaubterweise auf Bild- oder Tonträger aufgenommen worden ist, die erschienen oder erlaubterweise öffentlich zugänglich gemacht worden sind,
3. außerhalb des Raumes, in dem sie stattfindet, durch Bildschirm, Lautsprecher oder ähnliche technische Einrichtungen öffentlich wahrnehmbar zu machen.

Durch den Verweis in § 78 Ab. 1 UrhG gilt das Recht der öffentlichen Zugänglichmachung auch für den ausübenden Künstler (Wandtke/Bullinger § 78 RN 3).

In Fall 6 wurde das Rechts der öffentlichen Zugänglichmachung durch den Benutzer verletzt. Dies verletzt die Rechte von Troubardix als Urheber und ausübender Künstler

Gewerbliche Schutzrechte (z. B. Urheberrechte) sind Ausschließlichkeitsrechte, d. h. nur der Berechtigte darf sie ausüben. Berechtigung der MGB Media AG?

Gewährung von Nutzungsrechten an Dritte

Der Urheber kann nach § 31 UrhG Dritten die Berechtigung erteilen, bestimmte Verwertungsrechte auszuüben, man bezeichnet dies als **Nutzungsrecht** oder **Lizenz.**

§ 31 Einräumung von Nutzungsrechten

(1) Der Urheber kann einem anderen das Recht einräumen, das Werk auf einzelne oder alle Nutzungsarten zu nutzen (Nutzungsrecht). Das Nutzungsrecht kann als einfaches oder ausschließliches Recht sowie räumlich, zeitlich oder inhaltlich beschränkt eingeräumt werden.

(2) Das einfache Nutzungsrecht berechtigt den Inhaber, das Werk auf die erlaubte Art zu nutzen, ohne dass eine Nutzung durch andere ausgeschlossen ist.

(3) Das ausschließliche Nutzungsrecht berechtigt den Inhaber, das Werk unter Ausschluss aller anderen Personen auf die ihm erlaubte Art zu nutzen und Nutzungsrechte einzuräumen. Es kann bestimmt werden, dass die Nutzung durch den Urheber vorbehalten bleibt. § 35 bleibt unberührt.

Erteilt der Urheber das **ausschließliche Nutzungsrecht** an einen Dritten, ist nur dieser allein berechtigt, das Verwertungsrecht auszuüben.

Das ausschließliche Nutzungsrecht umfasst auch das Recht, einem Dritten die Nutzung zu verbieten (negatives Verbietungsrecht; Wandke/Bullinger – Wandtke/Grunert, § 31 RN 29).

In Fall 6 behauptet die Gegenseite, Inhaberin der ausschließlichen Nutzungsrechte zu sein. Das wird sie ggf. vor Gericht beweisen müssen.

§ 79 Nutzungsrechte

(1) *Der ausübende Künstler kann seine Rechte und Ansprüche aus den §§ 77 und 78 übertragen. § 78 Abs. 3 und 4 bleibt unberührt.*

(2) *Der ausübende Künstler kann einem anderen das Recht einräumen, die Darbietung auf einzelne oder alle der ihm vorbehaltenen Nutzungsarten zu nutzen.*

(2a) Auf Übertragungen nach Absatz 1 und Rechtseinräumungen nach Absatz 2 sind die §§ 31, 32 bis 32b, 32d bis 40, 41, 42 und 43 entsprechend anzuwenden.

Auch der ausübende Künstler kann seine Nutzungsrechte an Dritte übertragen.

In Fall 6 ist daher davon auszugehen, dass alle Rechte an die Gegnerin übertragen wurden.

Ansprüche der Gegnerin gegen den Benutzer?

§ 97 Anspruch auf Unterlassung und Schadensersatz

(1) *Wer das Urheberrecht oder ein anderes nach diesem Gesetz geschütztes Recht widerrechtlich verletzt, kann von dem Verletzten auf Beseitigung der Beeinträchtigung, bei Wiederholungsgefahr auf Unterlassung in Anspruch genommen werden. Der Anspruch auf Unterlassung besteht auch dann, wenn eine Zuwiderhandlung erstmalig droht.*

(2) *Wer die Handlung vorsätzlich oder fahrlässig vornimmt, ist dem Verletzten zum Ersatz des daraus entstehenden Schadens verpflichtet. Bei der Bemessung des Schadensersatzes kann auch der Gewinn, den der Verletzer durch die Verletzung des Rechts erzielt hat, berücksichtigt werden. Der Schadensersatzanspruch kann auch auf der Grundlage des Betrages berechnet werden, den der Verletzer als angemessene Vergütung hätte entrichten müssen, wenn er die Erlaubnis zur Nutzung des verletzten Rechts eingeholt hätte. Urheber, Verfasser wissenschaftlicher Ausgaben (§ 70), Lichtbildner (§ 72) und ausübende Künstler (§ 73) können auch wegen des Schadens, der nicht Vermögensschaden ist, eine Entschädigung in Geld verlangen, wenn und soweit dies der Billigkeit entspricht.*

Unterlassungs- und Schadenersatzansprüche setzen Widerrechtlichkeit voraus.

Eine Berechtigung ergibt sich entweder aus einer Genehmigung des Rechteinhabers oder einer Schrankenbestimmung.

Eine Genehmigung der Rechteinhaberin liegt offensichtlich nicht vor.

Eine Schranke für das Recht der öffentlichen Zugänglichmachung existiert mit § 52a UrhG nur für Unterricht und Forschung. Eine Schrankenbestimmung greift nicht ein.

Die Gegnerin in Fall 6 hat gegen den Benutzer Ansprüche auf Unterlassung und Schadenersatz.

Haftung des WLAN-Betreibers als Täter für Rechtsverletzungen der Benutzer?

Der Mandant könnte nach § 97 Abs. 1 UrhG als Täter auf Unterlassung und Schadenersatz haften.

§ 97 Anspruch auf Unterlassung und Schadensersatz

(1) Wer das Urheberrecht oder ein anderes nach diesem Gesetz geschütztes Recht widerrechtlich verletzt, kann von dem Verletzten auf Beseitigung der Beeinträchtigung, bei Wiederholungsgefahr auf Unterlassung in Anspruch genommen werden. Der Anspruch auf Unterlassung besteht auch dann, wenn eine Zuwiderhandlung erstmalig droht.

(2) *Wer die Handlung vorsätzlich oder fahrlässig vornimmt, ist dem Verletzten zum Ersatz des daraus entstehenden Schadens verpflichtet. Bei der Bemessung des Schadensersatzes kann auch der Gewinn, den der Verletzer durch die Verletzung des Rechts erzielt hat, berücksichtigt werden. Der Schadensersatzanspruch kann auch auf der Grundlage des Betrages berechnet werden, den der Verletzer als angemessene Vergütung hätte entrichten müssen, wenn er die Erlaubnis zur Nutzung des verletzten Rechts eingeholt hätte. Urheber, Verfasser wissenschaftlicher Ausgaben (§ 70), Lichtbildner (§ 72) und ausübende Künstler (§ 73) können auch wegen des Schadens, der nicht Vermögensschaden ist, eine Entschädigung in Geld verlangen, wenn und soweit dies der Billigkeit entspricht.*

Ob und unter welchen Umständen ein WLAN Anbieter als Täter einer Urheberrechtsverletzung seines Benutzers haften kann, ist umstritten

Stang und Hühner haben die Ansicht vertreten, der WLAN-Betreiber hafte als Täter eines Unterlassungsdeliktes aufgrund einer Verkehrspflichtverletzung. Wie im Wettbewerbsrecht könne auch im Urheberrecht eine täterschaftliche Haftung bei Unterlassung zumutbarer Maßnahmen zur Gefahrenabwehr in Betracht kommen (GRUR 2010, 633).

Der BGH hat den Ansätzen von Hühner und Stang eine klare Absage erteilt. Im Gegensatz zum Wettbewerbsrecht, wo die Eröffnung einer Gefahr für die Interessen anderer Marktteilnehmer als unlautere Handlung angesehen werden könne, setzte eine täterschaftliche Haftung im Urheberrecht voraus, dass die Merkmale des Verletzungstatbestandes in der Person des Täters erfüllt seien. Das Bereithalten eines nicht gesicherten WLAN-Zugangs erfülle jedoch nicht den Tatbestand der öffentlichen Zugänglichmachung (GRUR 2010, 633 – „Sommer unseres Lebens“).

Die Ansicht von Stang und Hühner wird jedoch noch heute von Hofmann vertreten: Alle Intermediären, auch WLAN-Betreiber, sollen nach dieser Auffassung haften, wenn sie Verkehrspflichten verletzen. Dieser Grundsatz sei der Störerhaftung überlegen, an der der BGH nur festhalte, um die Haftung nicht auf Schadenersatz ausdehnen zu müssen. Die Schadenersatzhaftung lasse sich aber auch über die Verkehrspflichtverletzung begrenzen oder durch § 8 TMG explizit ausschließen (Hofmann JUS 2017, 713).

Der BGH hingegen bejaht bei Urheberrechtsverletzungen im WLAN (vom Sonderfall einer Aufsichtspflichtverletzung für minderjährige Kinder abgesehen (GRUR 2016, 184 – „Tauschbörse II“, RN 29 ff)) keine täterschaftliche Haftung des Anschlussinhabers als solchem, sondern

lediglich eine sekundäre Darlegungslast des Anschlussinhabers, dass auch andere den Anschluss benutzt haben können (BGH GRUR 2010, 633 – „Sommer unseres Lebens“, RN 12).

Er hat zunächst ausgeführt, es bestehe eine tatsächliche Vermutung für die Täterschaft des Anschlussinhabers. Diese sei widerlegt, wenn der sekundären Darlegungslast Genüge getan würde (BGH ZUM 2014, 707 – „Bearshare“, RN 15); da sie hierdurch erschüttert werde (BGH ZUM 2013, 493 – „Morpheus“, RN 34; GRUR 2010, 633 – „Sommer unseres Lebens“, RN 12). In der Entscheidung „Bearshare“ hat der BGH aber auch festgestellt, diese sogenannte sekundäre Darlegungslast des Anschlussinhabers führe nicht zu einer Umkehr der Beweislast (ZUM 2014, 707 RN 18).

In der Entscheidung „Afterlife“ hat der BGH die Reichweite der tatsächlichen Vermutung aber deutlich eingeschränkt. Diese bestehe nicht allein aufgrund der Anschlussinhaberschaft, sondern nur beim Vorliegen von typischen Geschehensabläufen, die bei einem naheliegenden Zugriff Dritter auf den Anschluss nicht gegeben seien (GRUR 217, 386 – „Afterlife“, RN 18 ff).

Wie weit die sekundäre Darlegungslast reicht, war zunächst unter den Instanzgerichten umstritten (siehe dazu Solmecke/Rüther/Büring MMR 2016, 153 m. w. N.). Der BGH hat daraufhin festgestellt, der Anschlussinhaber genüge der sekundären Darlegungslast mit der pauschalen Behauptung der bloß theoretischen Möglichkeit des Zugriffs Dritter nicht (GRUR 2016, 191 – „Tauschbörse III“, RN 42). Komme der Anschlussinhaber der sekundären Darlegungslast nicht nach, fehle der Feststellung, ein Dritter komme als Täter in Betracht, die tatsächliche Grundlage (GRUR 2016, 191 – „Tauschbörse III“, RN 48). Dagegen genüge der Anschlussinhaber der sekundären Darlegungslast durchaus mit der Angabe, auch seine Ehefrau habe Zugriff zum WLAN gehabt. Nähere Angaben zum Nutzungsverhalten der Ehefrau seien nicht erforderlich (GRUR 217, 386 – „Afterlife“, RN 26). Es sei auch durchaus zu verlangen, dass der Anschlussinhaber den Namen seines Kindes nennt, dass ihm die Filesharing-Nutzung gestanden hat (BGH BeckRS 2017, 108569 „Loud“, RN 24 ff).

Die Reichweite der sekundären Darlegungslast wird in der Literatur kritisiert. Wenn man fordere, den Namen eines Familienmitglieds zu nennen, fordere man, einen „Verrat“ an der Familie zu begehen (Köhler ZUM 2017, 507). Damit wird aber verkannt, dass Beklagte im Zivilprozess keine Zeugen sind, denen Aussageverweigerungsrechte zustehen. Durch die Pflicht der Namensnennung wird letztlich nur einer Prozessstrategie der Boden entzogen, die die Verletzten rechtlos stellen würde.

In der Literatur wird teilweise angenommen, die tatsächliche Vermutung laufe regelmäßig ins Leere, da sie nur begründet sei, wenn nur der Anschlussinhaber den Anschluss benutze, und dies sei von dem Verletzten zu beweisen (Köhler ZUM 2017, 507; Hofmann ZUM 2014, 654). Dies lässt sich der BGH-Rechtsprechung jedoch nicht entnehmen. Vielmehr muss die tatsächliche Vermutung vom Anschlussinhaber entkräftet werden, indem er vorträgt, nicht der einzige Nutzer zu sein (ebenso Weber ZUM 2014, 710).

Der überwiegende Teil der Literatur jedoch unterstützt die Ansicht des BGH vorbehaltlos (Sesing/Baumann MMR 2017, 583; Specht GRUR 2017, 42, Forch GRUR-Prax 2017, 152).

Stellungnahme

Bezüglich der Ansicht von Hühner/Stang und Hofmann ist dem BGH zuzustimmen.

Eine Urheberrechtsverletzung setzt voraus, dass eine Verwertungshandlung vorgenommen wurde, ohne dass eine Genehmigung vorlag oder eine Schrankenbestimmung eingriff. Der Access Provider macht die Datei jedoch nicht selbst öffentlich zugänglich nach § 19a UrhG, sondern vermittelt nur den Zugang zu einer bereits zugänglichen Datei.

Damit ist der Ansicht des BGH zu folgen, nach der eine täterschaftliche Haftung des WLAN-Betreibers nur in Betracht kommt, wenn er der Täter ist. Ob die tatsächliche Vermutung der Täterschaft die richtige Begrifflichkeit für Zweifelsfälle ist, steht allerdings seit „Afterlife“ in Frage. Es handelst sich nämlich gerade nicht um eine widerlegliche Vermutung, sondern lediglich um einen Anscheinsbeweis, für den die Anschlussinhaberschaft alleine nicht genügt.

Folgen der BGH-Rechtsprechung für Fall 6

Die Rechtsprechung des BGH zur sekundären Darlegungslast bezieht sich jedoch auf Betreiber von privaten WLAN im eigenen Haushalt.

Es erscheint durchaus fraglich, ob diese Rechtsprechung auf kommerzielle Betreiber offener WLANs übertragbar ist. Nach der Entscheidung „Afterlife“ soll die tatsächliche Vermutung ja nur solche Fälle betreffen, in dem es ein typischer Geschehensablauf ist, dass der WLAN-Inhaber selbst der Täter sein könnte. Das ist jedoch bei einem offenen WLAN in einem Internet-Café gerade nicht zu erwarten, da das WLAN primär den Gästen zur Verfügung steht (ähnlich Sesing MMR 2017, 473). Denkt man „Afterlife“ zu Ende, sollte es daher eine tatsächliche Vermutung bei kommerziellen WLANs nicht geben.

Allerdings existiert bisher keine Rechtsprechung des BGH zur Frage der Haftung kommerzieller WLAN-Betreiber.

Der WLAN Betreiber vermittelt technisch gesehen den Benutzern den Zugang zum Internet. Dieser Zugang ist somit für die vom Benutzer begangene Urheberrechtsverletzung kausal. Zugleich ist seine Funktion mit der von Internet-Zugangsprovidern vergleichbar wie Innexio oder der deutschen Telekom vergleichbar.

Dies gilt insbesondere für öffentliche WLAN Betreiber, die in der Praxis bei mobilen Endgeräten den Mobilfunk-Zugangsanbieter ersetzen. Daher sollte noch ein Blick auf die Rechtsprechung und Literatur zur Haftung von Internet-Zugangsanbietern geworfen werden.

Haftung eines Internet-Zugangsanbieters als Täter für Rechtsverletzungen der Benutzer?

Ob und unter welchen Umständen ein Internet-Zugangsanbieter als Täter einer Urheberrechtsverletzung seines Benutzers haften kann, ist umstritten.

Czychowski und Nordemann sind der Meinung, § 97 Abs. 1 UrhG sei im Lichte von Art. 8 Abs. 3 InfoSoc-Richtlinie und Art. 11 Satz 3 Enforcement-Richtlinie richtlinienkonform dahingehend auszulegen, dass jeder, der in der Lage sei, die Rechtsverletzung zu verhindern, einer entsprechenden Hilfeleistungspflicht unterliege. Dabei komme es nicht darauf an, ob sein Beitrag für die Verletzung adäquat kausal sei (GRUR 2013, 986). Daran anknüpfend ist Hofmann der Ansicht, Access Provider müssten „in analoger Anwendung der Auskunftspflichten nach § 101 Abs. 9 UrhG“ durch richterliche Anordnung zu Sperren verpflichtet werden können, da sie als einzige in der Lage seien, den Rechtinhabern zu helfen (GRUR 2015, 123; NJW 2016, 769). Die Störerhaftung sei hingegen als Haftungsgrundlage ungeeignet, da es an einer Kausalität fehle. Denke man einen Zugangsprovider hinweg, sei der Inhalt immer noch über andere Anbieter erreichbar (Hofmann NJW 2016, 769).

Heid ist der Meinung, jeder, der auch nur adäquat kausal zu einer Urheberrechtsverletzung beigetragen habe, sei Täter einer Urheberrechtsverletzung nach § 97 Abs. 1 UrhG. Dieser Verstoß sei widerrechtlich, wenn eine Verkehrspflicht verletzt werde (Heid, Haftung bei Urheberrechtsverletzungen im Netz, S. 56ff). Auch die Tätigkeit der Access Provider sei für Urheberrechtsverletzungen im Netz adäquat kausal, da sie durch den Zugang zum Netz eine Gefahrenquelle für Verletzungen schaffen (S. 102ff). Access Provider könnten daher im Einzelfall nach einer Güterabwägung verpflichtet sein, urheberrechtsverletzende Inhalte mit einer DNS-Sperre zu belegen (S. 113 ff).

Der BGH lehnt dagegen eine Haftung des Internetzugangsanbieters als Täter mit dem Argument ab, die Tathandlung einer öffentlichen Zugänglichmachung nach § 19 UrhG werde nicht von dem Access Provider selbst begangen. Auch eine Beteiligung als Gehilfe scheide aus (ZUM-RD 2016, 156, - „3dl.am“, RN 18; GRUR 2016, 268 – „goldesel.to“, RN 19). Jedoch sei eine Haftung als Störer denkbar, da der Access-Provider einen adäquat-kausalen Tatbeitrag leiste (ZUM-RD 2016, 156, - „3dl.am“, RN 24; GRUR 2016, 268 – „goldesel.to“, RN 25). Teile der Literatur unterstützen diese Ansicht des BGH (Spindler GRUR 2016, 451; Sesing/Putzki MMR 2016, 660; Finger MMR 2016, 180).

Dagegen lehnen Teile der Literatur sowohl eine Haftung als Täter, als auch als Störer ab. Da sowohl Grundrechte des Providers, also auch seiner Nutzer und der durch „Overblocking“ zu Unrecht gesperrten Drittinhalte betroffen seien, bedürfe ein Eingriff in Form einer gerichtlichen Verfügung zur Sperrung von Inhalten einer gesetzlichen Grundlage (Frey/Nohr GRUR-Prax 2016, 164; Heydrich/Heymann MMR 2016, 370).

Stellungnahme

Die Ansicht von Czychowski/Nordemann und Hofmann ist abzulehnen, da sie dem europäischen Recht widerspricht.

Artikel 8 Richtlinie 2001/29/EG (Infosoc-Richtlinie) Sanktionen und Rechtsbehelfe

(3) Die Mitgliedstaaten stellen sicher, dass die Rechtsinhaber gerichtliche Anordnungen gegen Vermittler beantragen können, deren Dienste von einem Dritten zur Verletzung eines Urheberrechts oder verwandter Schutzrechte genutzt werden.

Artikel 11 Richtlinie 2004/48/EG (Enforcement-Richtlinie) Gerichtliche Anordnungen

[…] Unbeschadet des Artikels 8 Absatz 3 der Richtlinie 2001/29/EG stellen die Mitgliedstaaten ferner sicher, dass die Rechtsinhaber eine Anordnung gegen Mittelspersonen beantragen können, deren Dienste von einem Dritten zwecks Verletzung eines Rechts des geistigen Eigentums in Anspruch genommen werden.

In Erwägungsgrund 23 der Enforcement-Richtlinie heißt es:

(23) Unbeschadet anderer verfügbarer Maßnahmen, Verfahren und Rechtsbehelfe sollten Rechtsinhaber die Möglichkeit haben, eine gerichtliche Anordnung gegen eine Mittelsperson zu beantragen, deren Dienste von einem Dritten dazu genutzt werden, das gewerbliche Schutzrecht des Rechtsinhabers zu verletzen. Die Voraussetzungen und Verfahren für derartige Anordnungen sollten Gegenstand der einzelstaatlichen Rechtsvorschriften der Mitgliedstaaten bleiben.

Es ist somit Sache der deutschen Rechtsvorschriften, den Rechteinhabern einen Anspruch gegen „Mittelspersonen" wie Provider zu gewähren. Sieht § 97 UrhG oder § 101 UrhG einen solchen Anspruch nicht vor, zwingen die Richtlinien damit auch nicht zu einer erweiterten Auslegung der Vorschrift. Das deutsche Recht sieht in § 101 Abs. 2 Nr. 3 , Abs. 3 und 9 UrhG lediglich einen Auskunftsanspruch vor, der auch gegen Access-Provider eingesetzt werden kann, um Namen und Anschrift des Verletzers zu erfahren. Dem Gesetzgeber stand es frei, die Ansprüche gegen Provider hierauf zu beschränken.

Auch die Ansicht von Heid ist abzulehnen. Das Konzept Heids würde zu einer grenzenlosen Ausweitung der Haftung ohne gesetzliche Grundlage führen. So wäre danach etwa ein Hersteller eines Fotokopierers, der für eine rechtswidrige Kopie benutzt wird, ein Täter einer Urheberrechtsverletzung.

Eine Urheberrechtsverletzung setzt voraus, dass eine Verwertungshandlung vorgenommen wurde, ohne dass eine Genehmigung vorlag oder eine Schrankenbestimmung eingriff. Der Access Provider macht die Datei jedoch nicht selbst öffentlich zugänglich nach § 19a UrhG, sondern vermittelt nur den Zugang zu einer bereits zugänglichen Datei.

Die Ansicht von Frey/Nohr und Heydrich/Heymann übersieht, dass die Störerhaftung durchaus auf einer gesetzlichen Grundlage basiert (vgl. GRUR 2016, 268 – „goldesel.to", RN 74) – mehr dazu unten.

Es ist also auch hier der Ansicht des BGH zu folgen. Die Handlung des Zugangsanbieters ist jedenfalls dann adäquat kausal für die Rechtsverletzung, wenn man die Zugangsanbieter insgesamt betrachtet. Ohne Internet-Zugangsanbieter gäbe es keine Benutzer im Internet und damit auch keine Öffentlichkeit, der im Internet im Sinne von § 19 UrhG etwas zugänglich gemacht werden könnte (vgl. Sesing/Putzki MMR 2016, 660).

Folgen der BGH-Rechtsprechung für Fall 6

Nach der Rechtsprechung des BGH sowohl zu den privaten WLAN-Betreibern, also auch zu den Internet-Zugangsanbietern haftet der Mandant als Anschlussinhaber nicht unmittelbar als Täter, er kann jedoch als Störer haften.

Haftung des WLAN-Betreibers als Störer?

Der Mandant könnte als Störer auf Unterlassung haften.

Wer – ohne Täter oder Teilnehmer zu sein – in irgendeiner Weise willentlich und adäquat kausal zur Verletzung des geschützten Guts beiträgt, kann jedenfalls bei der Verletzung absoluter Rechte als Störer auf Unterlassung in Anspruch genommen werden (ständige Rechtsprechung des BGH JurPC Web-Dok. 265/2004 – Internetversteigerung I; K&R 2013, 655 – File-Hosting-Dienst, RN 30).

Nach herrschender Meinung kann ein WLAN-Betreiber grundsätzlich als Störer für eine Rechtsverletzung eines Benutzers in Betracht kommen (BGH GRUR 2010, 633 – „Sommer unseres Lebens“; Ahlberg/Götting-Reber § 97 RN 80; Ungern-Sternberg GRUR 2015, 205; Leistner/Grisse GRUR 2015, 19; Mantz/Sassenberg NJW 2014, 3537). Der BGH sieht den Betrieb eines nicht ausreichend gesicherten WLAN-Anschlusses als adäquat kausal für Urheberrechtsverletzungen, die unbekannte Dritte unter Einsatz dieses Anschlusses begehen, an (GRUR 2010, 633 – Sommer unseres Lebens, RN 20).

Lediglich vereinzelt wird bezweifelt, ob in der bloßen Ermöglichung des Zugriffs auf Internetinhalte überhaupt eine hinreichende Mitwirkung liegt (Spindler GRUR 2014, 826 m. w. N.).

Umstritten ist ferner, auf welcher Rechtsgrundlage die Störerhaftung im Urheberrecht beruht:

Teilweise wird die Rechtsgrundlage unmittelbar in § 97 UrhG gesehen (KG NJOZ 2005, 1094).

Dagegen sieht die überwiegende Ansicht die Grundlage der Störerhaftung auch im Urheberrecht in einer analogen Anwendung von § 1004 BGB (OLG Hamburg GRUR-RR 2014, 140 – 3dl.am; LG Köln CR 2008, 184; LG Düsseldorf ZUM 2007, 553; Wandtke/Bullinger – von Wolff § 97 RN 14).

Letztere Ansicht überzeugt, da § 97 UrhG die Verwirklichung eines Verwertungstatbestandes voraussetzt, woran es beim Störer regelmäßig fehlt.

Dagegen ist die Ansicht von Spindler abzulehnen. Der Beitrag des WLAN Betreibers ist adäquat kausal, ohne den Internetzugang kein Zugang zur Tauschbörse.

Folgen für Fall 6

Der Beitrag des Mandanten ist für die Rechtsverletzung adäquat kausal, ohne den Internetzugang wäre die Rechtsverletzung nicht möglich. Der Mandant hat zumindest theoretisch die Möglichkeit, die Rechtsverletzung zu unterbinden.

Eine Haftung des Mandanten als Störer kommt grundsätzlich in Betracht.

Prüfungspflichten

Die Haftung als Störer setzt die Verletzung zumutbarer Verhaltenspflichten, insbesondere von Prüfungspflichten voraus (BGH ZUM 2014, 707 – „Bearshare“, RN 22). Prüfungspflichten sind das Korrektiv zur Vermeidung einer ausufernden Haftung. Sie bestimmen sich danach, wieweit

der als Störer in Anspruch genommenen Partei billigerweise ein Tun zur Unterbindung der jeweiligen Rechtsverletzung zugemutet werden kann (OLG Hamburg GRUR-RR 2014, 140 – 3dl.am). Wie weit diese Prüfungspflichten reichen, ist umstritten. Grundsätzlich kommen als Prüfungspflichten Überwachungspflichten, Informationspflichten, Aufklärungspflichten und Sicherungspflichten in Betracht (Apel/Stolz ZUM 2017, 674).

Prüfungspflichten von klassischen Internetzugangsanbietern

Umstritten war bisher, inwieweit klassischen Internetzugangsanbietern Prüfungspflichten zuzumuten sind.

Das OLG Hamburg hat hierzu ausgeführt, jede denkbare Sperrmöglichkeit greife letztlich in Rechte Dritter ein, so dass eine Zumutbarkeit fehle (GRUR-RR 2014, 140 – 3dl.am). Das OLG Köln führt aus, DNS Sperren seien leicht zu umgehen und daher unzumutbar. IP-Sperren würden auch andere Angebote betreffen und seinen daher ebenfalls unzumutbar. Wegen des Eingriffs in die wirtschaftlichen Belange der Provider seien Prüfungspflichten insgesamt unzumutbar, da kein entgegenstehender wirtschaftlicher Vorteil der Rechteinhaber vorgetragen sei (ZUM-RD 2014, 603 – goldesel.to). Ein Teil der Literatur hat sich dieser Ansicht angeschlossen (Heydrich/Heymann MMR 2016, 370).

Nazari-Khanachayi vertritt die Ansicht, die Tatsache, dass die deutschen Instanzgerichte eine Zumutbarkeit von Prüfungspflichten verneinen, belege die Europarechtswidrigkeit des deutschen Rechts. Der Gesetzgeber müsse daher eine neue Rechtsgrundlage für Sperrverfügungen gegen Internetzugangsanbieter schaffen (GRUR-Prax 2014, 513).

Weisser und Färber sind der Ansicht, DNS-Sperren seine nicht wirksam und IP-Sperren seien allenfalls in wenigen Härtefällen zumutbar. Inzwischen seien Sperrverpflichtungen auf der Grundlage der Störerhaftung allerdings nicht mehr zulässig, da diese nach Art. 3 Abs. 3 Unterabsatz 3 der Netzneutralitätsverordnung 2015/2120 einer ausdrücklichen gesetzlichen Grundlage oder einer gerichtlichen Verfügung bedürfe. Weder die Störerhaftung, noch die Infosoc-Richtlinie stelle eine hinreichende Grundlage dar und eine gerichtliche Verfügung dürfe ohne eine solche Grundlage nicht ergehen (BB 2016, 776).

Leistner/Grisse hingegen haben die Ansicht vertreten, „allenfalls punktuell“ seinen DNS- und IP-Sperren zumutbar, die Inanspruchnahme der Zugangsanbieter sei aber immer subsidiär hinter der Inanspruchnahme der Anbieter der rechtsverletzenden Inhalte und der Betreiber der Server, auf denen sie gespeichert sind (GRUR 2015, 105).

Der BGH geht über diese Ansicht noch hinaus. Eine Sperranordnung stelle allerdings einen Eingriff in die Berufsfreiheit des Providers dar, die gegen die Rechte der Verletzen aus der Infosoc-Richtlinie, die auf dem Grundrecht auf Eigentum beruhen, abgewogen werden müssten (ZUM-RD 2016, 156, - „3dl.am“, RN 30 ff; GRUR 2016, 268 – „goldesel.to“, RN 31 ff). Vor diesem Hintergrund seien Sperrmaßnahmen nur zumutbar, wenn sie den Zugang zu rechtsverletzenden Inhalten zumindest erschweren (GRUR 2016, 268 – „goldesel.to“, RN 47). Allerdings stehe die Möglichkeit, Sperren zu umgehen, ihrer Zumutbarkeit grundsätzlich nicht entgegen (GRUR 2016, 268 – „goldesel.to“, RN 48). Daher seien DNS- und IP-Sperren grundsätzlich hinreichend effektiv (GRUR 2016, 268 – „goldesel.to“, RN 50), die gleichzeitige Mitsperrung legaler Websites unter

der gleichen Adresse könne allerdings gegen die Zumutbarkeit sprechen (GRUR 2016, 268 – „goldesel.to“, RN 53f), wobei ein Anteil von 4 % legaler Angebote allerdings nicht genüge (GRUR 2016, 268 – „goldesel.to“, RN 56). Der Zumutbarkeit stehe auch das Recht der Internetnutzer auf Informationsfreiheit nicht entgegen, dieses könnten sie auf vertraglicher Ebene gegen den Internet-Zugangsanbieter durchsetzen, wenn dieser legale Inhalte sperre (GRUR 2016, 268 – „goldesel.to“, RN 57; ZUM-RD 2016, 156, - „3dl.am“, RN 46). Auch wenn die Störerhaftung grundsätzlich nicht subsidiär sei, sei sie jedoch im Fall der Internet-Zugangsanbieter erst dann zumutbar, wenn zuerst gegen den Betreiber der Website mit den beanstandeten Inhalten vorgegangen worden ist, da dieser wesentlich näher an der Rechtsverletzung sei als der Access Provider. Eine direkte Inanspruchnahme des Access Providers komme nur in Betracht, wenn eine Inanspruchnahme des Content Provider nicht erfolgversprechend ist (GRUR 2016, 268 – „goldesel.to“, RN 81 ff; ZUM-RD 2016, 156, - „3dl.am“, RN 68 ff). Dafür genüge nicht, dass Name und Anschrift nicht aus der Website hervorgehen, es müssten weitergehende Ermittlungen angestellt werden (GRUR 2016, 268 – „goldesel.to“, RN 87). Auch genüge es nicht, eine einstweilige Verfügung zu erwirken, die dann wegen Verschleierung der wahren Anschrift nicht zugestellt werden kann, erst wenn auch eine Strafanzeige oder die Einschaltung eines Detektivs nicht zur Ermittlung der Anschrift führt, sei die Inanspruchnahme des Access Provider zumutbar (ZUM-RD 2016, 156, - „3dl.am“, RN 73 ff).

Ein Teil der Literatur hat sich der Ansicht des BGH angeschlossen (Spindler GRUR 2016, 451, Finger MMR 2016, 180).

Prüfungspflichten privater WLAN-Betreiber

Für Betreiber privater WLAN-Zugänge wurden früher die folgenden Ansichten vertreten:

Ein Teil der Teil der Rechtsprechung ging davon aus, dass Prüfungspflichten verletzt werden, wenn „zumutbare Sicherungsmaßnahmen“ für den WLAN-Zugang unterlassen werden. Diese bestünden in der Verschlüsselung des Zugangs und der Vergabe von Benutzerkonten (OLG Düsseldorf ZUM-RD 2008, 170). Es sei auch zumutbar, zur Sicherung fachkundige Hilfe in Anspruch zu nehmen (LG Hamburg JurPC Web-Dok 6/2008, bestätigt durch OLG Hamburg, Beschluss vom 21. 11. 2006, AZ 5 W 171/06). Ein Teil der Literatur unterstützt diese Ansicht (Stang/Hühner GRUR-RR 2008, 273; Mühlberger GRUR 2009, 1022).

Das OLG Frankfurt sah hingegen eine Störerhaftung privater WLAN-Betreiber nicht als gegeben an, so lange keine konkreten Hinweise auf einen Missbrauch den Zugangs bestünden, ansonsten würde die Prüfungspflichten ins Unzumutbare überspannt (ZUM-RD 2009, 68). Dies entspricht der Literaturmeinung von Ernst (MMR 2007, 538).

Der BGH hat das Urteil des OLG Frankfurt aufgehoben. Auch privaten WLAN-Betreibern sei es zuzumuten zu prüfen, ob der Zugang durch angemessene Sicherheitsmaßnahmen dagegen geschützt ist, dass Dritte ihn für Schutzrechtsverletzungen missbrauchen. Es seien daher die beim Kauf des Routers marktüblichen Sicherungen zu aktivieren und ein persönliches Kennwort zu verwenden (GRUR 2010, 633 – „Sommer unseres Lebens“).

Das OLG Frankfurt ist dem BGH nach Zurückverweisung gefolgt (MMR 2011, 420).

Inzwischen hat der BGH die Anforderung, es müsse ein Passwort verwendet werden, nochmals bestätigt, zugleich aber festgehalten, dass ein werksseitiges Passwort genügt, wenn es nicht bei allen gelieferten Geräten identisch vorgegeben ist, sondern für jedes Gerät ein individuelles Passwort vergeben wurde (ZUM 2017, 672 – „WLAN-Schlüssel“, RN 15). Als Verschlüsselungsstandard genüge WPA2 (ZUM 2017, 672 – „WLAN-Schlüssel“, RN 18).

Im Rahmen der Prüfungspflichten ist es nach Ansicht des BGH jedoch nicht erforderlich, Gästen der Wohnung oder volljährigen Mitbewohnern den Zugang zu verwehren oder sie auch nur über die Rechtswidrigkeit von Internettauschbörsen zu belehren (ZUM 2016, 1043 – „Silver Linings Playbook“, RN 20 ff).

Prüfungspflichten professioneller WLAN-Betreiber

Zu den Prüfungspflichten der Betreiber professionell betriebene WLANs wurden bisher folgende Ansichten vertreten:

Das LG Hamburg hat in einer einstweiligen Verfügung ausgeführt, der Betreiber eines Internetcafés mit WLAN hafte als Störer, wenn er keine Maßnahmen wie etwa Portsperren ergreift, um Filesharing zu verhindern (K&R 2011, 215). Auch Nordemann hält Portsperren für ein geeignetes Mittel, um Filesharing vorzubeugen (GRUR 2016, 1097).

Das LG Frankfurt hat die Ansicht vertreten, jedenfalls bei einer Verschlüsselung des WLAN hafte ein Hotelier nicht für Urheberrechtsverletzungen seiner Gäste (ZUM-RD 2011, 371). Diese Ansicht findet auch in der Literatur Zustimmung (Füglein Lagadère MMR-Aktuell 2013, 341464; Schmidt-Bens/Suhren K&R 2013, 1). Auch das LG München hat sich in seinem Vorlagebeschluss an den EuGH der Ansicht angeschlossen, da die Anforderungen aus der BGH-Entscheidung „Sommer unseres Lebens“ erst recht für gewerbliche WLAN-Anbieter gelten würden (GRUR-RR 2014, 1166). Auch das AG Koblenz vertrat diese Ansicht (MMR-Aktuell 2014, 361339). Noch im März 2017 hat sich das OLG Düsseldorf dieser Ansicht angeschlossen (GRUR 2017, 811, RN 13).

Kaeding vertrat die Ansicht, bereits vor Kenntnis von Rechtsverletzungen sei eine Registrierungspflicht für die Nutzer zumutbar und geeignet, um Missbrauch einzudämmen. Ferner sei es angezeigt, in den Nutzungsbedingungen missbräuchliche Nutzung zu untersagen. Nach Kenntnis von Rechtsverletzungen müssten diese künftig verhindert werden, etwa durch Sperren von IP-Adressen oder Filter (CR 2010, 164). Auch der EuGH vertritt die Ansicht, die Sicherung des Internetanschlusses durch ein Passwort sei für einen wirksamen Schutz des Urheberrechts erforderlich (GRUR 2016, 1146 – „McFadden ./. Sony Music“, RN 99).

Gietl vertrat die Ansicht, eine Haftung komme erst nach Kenntnis von Rechtsverletzungen in Betracht. Auch dann seien Maßnahmen zur Verhinderung von Rechtsverletzungen zumeist unzumutbar. Sperrungen seien wegen Verstoßes gegen das Fernmeldegeheimnis nach § 88 TKG unzulässig (MMR 2007, 630) Das AG Hamburg hat sich dem angeschlossen (ZUM-RD, 2015, 207).

Dagegen halten das AG Charlottenburg sowie die meisten Autoren Handlungspflichten für kommerzielle WLAN-Betreiber in jedem Fall für unzumutbar. Der Ausschluss von Benutzern sei unzumutbar, da diese zu Wettbewerbern abwandern würden. Filterpflichten seien ungeeignet, da jeweils nur bestimmte Ports gesperrt werden könnten, Filesharing aber über alle Ports möglich sei (Breyer, NJOZ 2010, 1085; Manz, JurPCWeb-Dok 95/2010; Feldmann K&R 2011, 225;

Mantz/Sassenberg NJW 2014, 3537). Darüber hinaus dürften bei einem von der Rechtsordnung gebilligten Geschäftsmodell dem Diensteanbieter keine Kontrollmaßnahmen auferlegt werden, die sein Geschäftsmodell gefährden (AG Charlottenburg GRURRS 2015, 02858; Ungern-Sternberg GRUR 2012, 321; Kirchberg ZUM 2012, 544).

Haftungsbegrenzung durch § 7 ff TMG?

Haftungsbegrenzung durch § 8 TMG?

§ 8 TMG Durchleitung von Informationen

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

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

Sofern diese Diensteanbieter nicht verantwortlich sind, können sie insbesondere nicht wegen einer rechtswidrigen Handlung eines Nutzers auf Schadensersatz oder Beseitigung oder Unterlassung einer Rechtsverletzung in Anspruch genommen werden; dasselbe gilt hinsichtlich aller Kosten für die Geltendmachung und Durchsetzung dieser Ansprüche. Die Sätze 1 und 2 finden keine Anwendung, wenn der Diensteanbieter absichtlich mit einem Nutzer seines Dienstes zusammenarbeitet, um rechtswidrige Handlungen zu begehen.

(3) *Die Absätze 1 und 2 gelten auch für Diensteanbieter nach Absatz 1, die Nutzern einen Internetzugang über ein drahtloses lokales Netzwerk zur Verfügung stellen.*

(4) *Diensteanbieter nach § 8 Absatz 3 dürfen von einer Behörde nicht verpflichtet werden,*

1. *vor Gewährung des Zugangs*
   a) *die persönlichen Daten von Nutzern zu erheben und zu speichern (Registrierung) oder*
   b) *die Eingabe eines Passworts zu verlangen oder*
2. *das Anbieten des Dienstes dauerhaft einzustellen*

Davon unberührt bleibt, wenn ein Diensteanbieter auf freiwilliger Basis die Nutzer identifiziert, eine Passworteingabe verlangt oder andere freiwillige Maßnahmen ergreift.

Absatz 3 wurde 2016 neu in das Gesetz eingefügt. Damit fallen WLAN – Betreiber grundsätzlich unter § 8 TMG, wenn die Voraussetzungen von Abs. 1 vorliegen.

Absatz 1 Satz 2 wurde mit Wirkung zum 13. Oktober2017 geändert. Damit könnte die Haftung für Unterlassungsansprüche beschränkt sein.

Begrenzung oder Erweiterung der Prüfungspflichten durch § 7 TMG?

§ 7 TMG- Allgemeine Grundsätze

(1) *Diensteanbieter sind für eigene Informationen, die sie zur Nutzung bereithalten, nach den allgemeinen Gesetzen verantwortlich.*

(2) *Diensteanbieter im Sinne der §§ 8 bis 10 sind nicht verpflichtet, die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen.*

(3) *Verpflichtungen zur Entfernung von Informationen oder zur Sperrung der Nutzung von Informationen nach den allgemeinen Gesetzen aufgrund von gerichtlichen oder behördlichen Anordnungen bleiben auch im Falle der Nichtverantwortlichkeit des Diensteanbieters nach den §§ 8 bis 10 unberührt. Das Fernmeldegeheimnis nach § 88 des Telekommunikationsgesetzes ist zu wahren.*

(4) *Wurde ein Telemediendienst von einem Nutzer in Anspruch genommen, um das Recht am geistigen Eigentum eines anderen zu verletzen und besteht für den Inhaber dieses Rechts keine andere Möglichkeit, der Verletzung seines Rechts abzuhelfen, so kann der Inhaber des Rechts von dem betroffenen Diensteanbieter nach § 8 Absatz 3 die Sperrung der Nutzung von Informationen verlangen, um die Wiederholung der Rechtsverletzung zu verhindern. Die Sperrung muss zumutbar und verhältnismäßig sein. Ein Anspruch gegen den Diensteanbieter auf Erstattung der vor- und außergerichtlichen Kosten für die Geltendmachung und Durchsetzung des Anspruchs nach Satz 1 besteht außer in den Fällen des § 8 Absatz 1 Satz 3 nicht.*

Aus § 7 Abs. 3 oder 4 TMG könnten sich neue gesetzliche Prüfungspflichten ergeben.

Internet-Café-Betreiber als Diensteanbieter im Sinne des TMG

Dies ergibt sich auch aus den übrigen Vorschriften des TMG:

§ 2 Begriffsbestimmungen

Im Sinne dieses Gesetzes

1. *ist Diensteanbieter jede natürliche oder juristische Person, die eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt; bei audiovisuellen Mediendiensten auf Abruf ist Diensteanbieter jede natürliche oder juristische Person, die die Auswahl und Gestaltung der angebotenen Inhalte wirksam kontrolliert, […]*

§ 1 TMG Anwendungsbereich

(1) […] Dieses Gesetz gilt für alle Anbieter einschließlich der öffentlichen Stellen unabhängig davon, ob für die Nutzung ein Entgelt erhoben wird.

Ein Anbieter eines WLAN-Netzes vermittelt lediglich den Zugang zum Internet, wenn über das drahtlose Netz eine Verbindung zum Internet besteht (AG Charlottenburg BeckRS 2015, 2858; Hoeren/Sieber-Sieber/Hoefinger, Teil 18.1 RN 64; Roßnagel – Jandt, § 8 TMG RN 12). Gleiches gilt auch für den Betreiber eines Internetcafés. Dass dort in der Regel auch Hardware zur Verfügung gestellt wird, ändert daran nichts (Hoeren/Sieber-Sieber/Hoefinger, Teil 18.1 RN 64; Jandt aaO. RN 13).

Dabei werden weder Adressaten noch Informationen ausgewählt, dies erfolgt ausschließlich durch die Endnutzer (Redeker ITRB 2011, 186).

Haftungsbegrenzung auch für private WLAN-Betreiber?

§ 8 TMG Durchleitung von Informationen

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

4. die Übermittlung nicht veranlasst,

5. den Adressaten der übermittelten Informationen nicht ausgewählt und

6. die übermittelten Informationen nicht ausgewählt oder verändert haben.

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

§ 2 Begriffsbestimmungen

Im Sinne dieses Gesetzes

2. ist Diensteanbieter jede natürliche oder juristische Person, die eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt; bei audiovisuellen Mediendiensten auf Abruf ist Diensteanbieter jede natürliche oder juristische Person, die die Auswahl und Gestaltung der angebotenen Inhalte wirksam kontrolliert, […]

§ 1 TMG Anwendungsbereich

(2) […] Dieses Gesetz gilt für alle Anbieter einschließlich der öffentlichen Stellen unabhängig davon, ob für die Nutzung ein Entgelt erhoben wird.

Bisher war streitig, ob § 8 TMG auch auf private WLAN-Anbieter angewendet werden kann.

Borges wollte § 8 TMG bei Privaten teleologisch reduzieren, da ein Haftungsausschluss nicht angemessen erscheine (NJW 2014, 2305).

Dagegen vertreten andere Autoren die Ansicht, der Anwendungsbereich sei nach § 1 Abs. 1 Satz 2 TMG nicht auf kommerzielle WLAN-Betreiber beschränkt (Mantz/Sassenberg, NJW 2014, 3537; Hoeren/Sieber/Holznagel-Sieber/Höfinger, Teil 18.1., RN 64; Hoeren/Jakopp ZRP 2014, 72).

Die Ansicht von Borges überzeugt nicht, da der Gesetzeswortlaut eindeutig ist. „Alle Anbieter“ schließt eindeutig auch Private ein. Nach der Beschlussempfehlung des Ausschusses für Wirtschaft und Energie war es die ausdrückliche Absicht des Gesetzgebers, mit § 8 Abs. 3 TMG klarzustellen, dass „auch Anbieter von WLAN-Internetzugängen ohne jede Einschränkung Diensteanbieter im Sinne des § 8 TMG sind“ (Bundestags-Drucksache 18/8645, S. 10).

Damit dürfte sich die Diskussion erübrigt haben. § 8 TMG gilt auch für private WLAN-Betreiber (Spindler NJW 2017, 2305).

Eigene oder fremde Informationen ?

§ 7 TMG- Allgemeine Grundsätze

(1) *Diensteanbieter sind für eigene Informationen, die sie zur Nutzung bereithalten, nach den allgemeinen Gesetzen verantwortlich.*

§ 8 Durchleitung von Informationen

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

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

Sofern diese Diensteanbieter nicht verantwortlich sind, können sie insbesondere nicht wegen einer rechtswidrigen Handlung eines Nutzers auf Schadensersatz oder Beseitigung oder Unterlassung einer Rechtsverletzung in Anspruch genommen werden; dasselbe gilt hinsichtlich aller Kosten für die Geltendmachung und Durchsetzung dieser Ansprüche. Die Sätze 1 und 2 finden keine Anwendung, wenn der Diensteanbieter absichtlich mit einem Nutzer seines Dienstes zusammenarbeitet, um rechtswidrige Handlungen zu begehen.

Informationen, die Benutzer über das WLAN übertragen, sind aus Sicht des Betreibers fremde Informationen.

§ 8 TMG ist grundsätzlich anwendbar.

§ 8 TMG auf Unterlassungsansprüche anwendbar?

Bisher war umstritten, ob § 8 TMG auf Unterlassungsansprüche anwendbar ist. Dagegen könnte § 7 Abs. 2 TMG sprechen:

§ 7 Allgemeine Grundsätze

(2) *Diensteanbieter im Sinne der §§ 8 bis 10 sind nicht verpflichtet, die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen. Verpflichtungen zur Entfernung oder Sperrung der Nutzung von Informationen nach den allgemeinen Gesetzen bleiben auch im Falle der Nichtverantwortlichkeit des Diensteanbieters nach den §§ 8 bis 10 unberührt.*

Ein Teil von Rechtsprechung und Literatur vertraten die Ansicht, die Haftungsprivilegierung der Access Provider finde wegen § 7 Abs. 2 Satz 2 TMG keine Anwendung auf Unterlassungsansprüche (OLG Köln ZUM-RD 2014, 693; LG Frankfurt MMR 2008, 344; LG Kiel Jur-PC Web-Dok. 24/2008; LG Hamburg K&R 2009, 272; AG Charlottenburg BeckRS 2015, 2858; Redeker ITRB 2011, 186; Ahlberg/Götting-Reber, § 97 RN 80; Leistner/Grisse GRUR 2015, 19; Sesing MMR 2015, 423).

Das OLG Hamburg wollte zwar § 8 TMG auf Unterlassungsansprüche nicht unmittelbar anwenden, aber die Prüfungspflichten im Hinblick auf die gesetzgeberische Wertung in § 8 TMG stark reduzieren (ZUM-RD 2009, 246; BeckRS 2011, 22463; GRUR-RR 2014; 140; ähnlich Feldmann K&R 2011, 225; Roßnagel-Jandt § 7 RN 51).

Gietl vertrat die Auffassung, die Haftungsprivilegien fänden zwar auf Unterlassungsansprüche nicht unmittelbar Anwendung, wegen § 7 Abs. 2 Satz 1 TMG setze die Haftung aber erst ab Kenntnis ein (MMR 2007, 630 und ZUM 2008, 249). Das AG Charlottenburg hat sich dieser Auffassung offenbar angeschlossen (BeckRS 2015, 2858), ebenso Nordemann (GRUR 2016, 1097).

Ein anderer Teil der Rechtsprechung und Literatur forderte die volle Anwendbarkeit der Haftungsprivilegien auf Unterlassungsansprüche. Das Entfernen und Sperren im Sinne des § 7 Abs. 2 S. 1 seien Handlungen, die der Beseitigung einer bereits bestehenden Rechtsverletzung dienten. Eine Erstreckung auf Unterlassungsansprüche, die auf die Zukunft gerichtet sind, gebe die Norm nicht her, da es sich um eine abschließende Ausnahmeregelung zur grundsätzlichen Haftungsbefreiung handele (AG Hamburg ZUM-RD 2015, 207; Härting, Internetrecht, Kapitel H RN 1354 ff; Breyer MMR 2009, 14 und NJOZ 2010, 1085; Nolte Wimmers GRUR-Beilage 2014, 58, 62). Diese Regelung ordne lediglich an, dass anderweitige Ansprüche zur Entfernung und Sperrung unberührt bleiben (VG Düsseldorf ZUM-RD 2012, 362; VG Köln BeckRS 2012, 46096).

Der BGH hat sich in seinem Urteil vom 12. Mai 2010 nicht mit der Frage einer Anwendbarkeit von § 8 TMG auseinandergesetzt, was von Nenninger zu Recht kritisiert wurde (BGH NJW 2010, 2061 mit Anm. Nenninger).

In seinen beiden Urteilen vom 26. November 2015, in denen es um Unterlassungsansprüche gegen Internetzugangsanbieter ging hat der BGH hat ausgeführt, Internet-Zugangsanbieter seien Diensteanbieter nach § 8 Abs. 1 TMG (GRUR 2016, 268 – „goldesel.to“, RN 24; ZUM-RD 2016, 156, - „3dl.am“, RN 23). Die Haftungsprivilegierungen hat er allerdings nicht angewandt, möglicherweise weil es aus seiner Sicht nicht darauf ankam.

Mit Wirkung zum 13. Oktober 2017 hat der Gesetzgeber in § 8 TMG einen neuen Satz 2 eingefügt:

> ***§ 8 Durchleitung von Informationen***
>
> (1) *Diensteanbieter sind für fremde Informationen, die sie in einem Kommunikationsnetz übermitteln oder zu denen sie den Zugang zur Nutzung vermitteln, nicht verantwortlich, sofern sie [..]*
>
> *Sofern diese Diensteanbieter nicht verantwortlich sind, können sie insbesondere nicht wegen einer rechtswidrigen Handlung eines Nutzers auf Schadensersatz oder Beseitigung oder Unterlassung einer Rechtsverletzung in Anspruch genommen werden; dasselbe gilt hinsichtlich aller Kosten für die Geltendmachung und Durchsetzung dieser Ansprüche. Die Sätze 1 und 2 finden keine Anwendung, wenn der Diensteanbieter absichtlich mit einem Nutzer seines Dienstes zusammenarbeitet, um rechtswidrige Handlungen zu begehen.*

§ 8 Abs. 2 Satz 2 stellt nun klar, dass § 8 TMG auf Unterlassungsansprüche anwendbar ist.

Sind §§ 7, 8 TMG in ihrer neuen Fassung europarechtswidrig?

Conraths und Peintinger vertreten die Auffassung, das 3. TMG-Änderungsgesetz insgesamt verstoße „möglicherweise“ gegen (EU-)Sekundärrecht. Aufgrund Art. 8 Abs. 3 InfoSoc-Richtlinie und Art. 11 Enforcement-Richtlinie müssten Rechteinhaber die Möglichkeit haben, wirkungsvolle Schutzmaßnahmen geltend zu machen. Dies sei nun durch § 8 IV TMG nicht mehr gegeben. Jedenfalls finde kein ausreichender Ausgleich zwischen Rechteinhabern und Diensteanbietern mehr statt (GRUR-Prax 2017, 206). Apel und Stolz schließen sich der Kritik mit dem Argument an, eine praktisch unbegrenzte Anzahl der WLAN-Netze sei ohne das Damoklesschwert der Störerhaftung eine Einladung zu massenhaften Urheberrechtsverletzungen (ZUM 2017, 674).

Spindler hält hingegen ausschließlich § 7 Abs. 4 Satz 3 TMG für europarechtswidrig, da er mit Art. 14 der Enforcement-Richtlinie nicht vereinbar sei, wonach die Mitgliedsstaaten sicherstellen müssen, dass die unterliegende Partei die Rechtsverfolgungskosten zu tragen hat. Er hält allerdings darüber hinaus § 7 Abs. 4 Satz 1 TMG für verfassungswidrig, da es gegen den Gleichheitsgrundsatz verstoße, Sperrmaßnahmen nur bei der Verletzung geistigen Eigentums vorzusehen und nicht bei der Verletzung anderer Rechte (NJW 2017, 2305).

Nach Ansicht von Sesing und Baumann ist § 7 Abs. 4 TMG europarechtswidrig, da gegen WLAN-Anbieter ausschließlich Sperranordnungen möglich seien, was zur Erfüllung der Anforderungen von InfoSoc- und Enforcementrichtlinie nicht ausreiche. Dazu bedürfe es der Verhinderung anonymer Nutzung und der Abschreckung durch drohende Anwaltskosten. Allerdings sei der Mangel durch eine europarechtskonforme Auslegung heilbar, die auch eine Verschlüsselung von WLANs vorsehen müsse (MMR 2017, 583). Dem schließt sich Grisse an, die zusätzlich auch § 7 Abs. 3 für unionsrechtswidrig hält, wenn man ihn so auslegt, wie vom Gesetzgeber vorgesehen. Auch sie geht allerdings davon aus, dass eine richtlinienkonforme Auslegung die vermeintlichen Mängel heilen könnte (GRUR 2017, 1073).

Demgegenüber hält Mantz die Reform des TMG insgesamt für europarechts- und verfassungskonform. Der Gesetzgeber habe die Anforderungen der EuGH-Entscheidung „McFadden beachtet und schaffe einen Ausgleich zwischen den widersprechenden Richtlinien E-Commerce-Richtlinie auf der einen bzw. Enforcement- und InfoSoc-Richtlinie auf der anderen Seite. Er habe bei der Umsetzung von EU-Richtlinien einen gewissen Spielraum, den er genutzt habe. Es liege auch keine Ungleichbehandlung von WLAN- und klassischen Access-Providern vor. Bei Access-Providern sei der Name des Anschlussinhabers bekannt und könne von den Rechteinhabern über § 101 UrhG auch ermittelt werden. Daher sei deren Lage nicht mit den WLAN-Anbietern vergleichbar (GRUR 2017, 969; ähnlich Grigorjew/Bile ZD-Aktuell 2017, 05621).

Die europarechtlichen Wurzeln von § 8 TMG

Um zu der Diskussion fundiert Stellung nehmen zu können, sollten zunächst die europarechtlichen Grundlagen der Debatte und die europarechtlichen Wurzeln der §§ 7 ff TMG betrachtet werden.

§ 8 TMG basiert auf Art. 12 der Richtlinie 2000/31/EG („E-Commerce-Richtlinie“)

Artikel 12 E-Commerce-RL - Reine Durchleitung

(1) Die Mitgliedstaaten stellen sicher, daß im Fall eines Dienstes der Informationsgesellschaft, der darin besteht, von einem Nutzer eingegebene Informationen in einem Kommunikationsnetz zu übermitteln oder Zugang zu einem Kommunikationsnetz zu vermitteln, der Diensteanbieter nicht für die übermittelten Informationen verantwortlich ist, sofern er

a) die Übermittlung nicht veranlaßt,

b) den Adressaten der übermittelten Informationen nicht auswählt und

c) die übermittelten Informationen nicht auswählt oder verändert.

(2) Die Übermittlung von Informationen und die Vermittlung des Zugangs im Sinne von Absatz 1 umfassen auch die automatische kurzzeitige Zwischenspeicherung der übermittelten Informationen, soweit dies nur zur Durchführung der Übermittlung im Kommunikationsnetz geschieht und die Information nicht länger gespeichert wird, als es für die Übermittlung üblicherweise erforderlich ist.

(3) Dieser Artikel läßt die Möglichkeit unberührt, daß ein Gericht oder eine Verwaltungsbehörde nach den Rechtssystemen der Mitgliedstaaten vom Diensteanbieter verlangt, die Rechtsverletzung abzustellen oder zu verhindern.

Die Auslegung von Art. 12 der E-Commerce-RL durch den EuGH

„Scarlet extended“

Der EuGH verweist in seinem Urteil „Scarlet extended“ zunächst darauf, dass nach Art. 12 Abs. 3 der Richtlinie 2000/31/EG und Art. 11 Satz 3 der Richtlinie 2004/48/EG (Enforcement-Richtlinie) gerichtliche Anordnungen gegen Access Provider beantragt werden können, deren Dienste für Urheberrechtsverletzungen benutzt werden (MMR 2012, 174 – Scarlet extended ./. SABAM RN 30).

Artikel 11 Enforcement –RL - Gerichtliche Anordnungen (Richtlinie 2004/48/EG)

Die Mitgliedstaaten stellen sicher, dass die zuständigen Gerichte bei Feststellung einer Verletzung eines Rechts des geistigen Eigentums eine Anordnung gegen den Verletzer erlassen können, die ihm die weitere Verletzung des betreffenden Rechts untersagt. Sofern dies nach dem Recht eines Mitgliedstaats vorgesehen ist, werden im Falle einer Missachtung dieser Anordnung in geeigneten Fällen Zwangsgelder verhängt, um die Einhaltung der Anordnung zu gewährleisten. Unbeschadet des Artikels 8 Absatz 3 der Richtlinie 2001/29/EG stellen die Mitgliedstaaten ferner sicher, dass die Rechtsinhaber eine Anordnung gegen Mittelspersonen beantragen können, deren Dienste von einem Dritten zwecks Verletzung eines Rechts des geistigen Eigentums in Anspruch genommen werden.

Nach Ansicht des EuGH sind zwar die Anspruchsgrundlagen für solchen Anordnungen gegen Access Provider Sache des Rechts des jeweiligen Mitgliedsstaates, allerdings haben dabei das Recht der Mitgliedsstaaten wie auch die Auslegung durch die Gerichte die Beschränkungen der Richtlinien 2000/31/EG und 2004/48/EG zu beachten. Die Beschränkungen der Art. 12 bis 15 der

Richtlinie 2000/31/EG würden dabei nach Art. 2 Abs. 3 der Richtlinie 2004/48/EG durch die Enforcement-Richtlinie nicht eingeschränkt (MMR 2012, 174 – Scarlet extended ./. SABAM RN 32ff).

Artikel 2 Enforcement –RL - Anwendungsbereich (Richtlinie 2004/48/EG)

(3) Diese Richtlinie berührt nicht:

a) die gemeinschaftlichen Bestimmungen zum materiellen Recht auf dem Gebiet des geistigen Eigentums, die Richtlinie 95/46/EG, die Richtlinie 1999/93/EG und die Richtlinie 2000/31/EG im Allgemeinen und insbesondere deren Artikel 12 bis 15;

Daher sei durch die Gerichte auch Art. 15 Abs. 1 der Richtlinie 2000/31/EG zu beachten, der Anordnungen verbiete, die einen Diensteanbieter zur Überwachung der übermittelten Informationen verpflichten würde. Dieses Verbot erstrecke sich auf eine Verpflichtung eines Providers, sämtliche Daten seiner Kunden aktiv und präventiv zu überwachen. Eine solche Verpflichtung würde ferner in die unternehmerische Freiheit des Providers eingreifen und gegen Art. 3 Abs. 1 der Richtlinie 2004/48/EG verstoßen, wonach Enforcement-Maßnahmen nicht unnötig kostspielig sein dürfen. Zwischen den Grundrechten der Rechteinhaber und denen des Providers und seiner Kunden sei ein Gleichgewicht herzustellen (MMR 2012, 174 – Scarlet extended ./. SABAM RN 35ff).

Artikel 3 Enforcement –RL - Allgemeine Verpflichtung (Richtlinie 2004/48/EG)

(1) Die Mitgliedstaaten sehen die Maßnahmen, Verfahren und Rechtsbehelfe vor, die zur Durchsetzung der Rechte des geistigen Eigentums, auf die diese Richtlinie abstellt, erforderlich sind. Diese Maßnahmen, Verfahren und Rechtsbehelfe müssen fair und gerecht sein, außerdem dürfen sie nicht unnötig kompliziert oder kostspielig sein und keine unangemessenen Fristen oder ungerechtfertigten Verzögerungen mit sich bringen.

„UPC Telekabel“

In einem weiteren Urteil hat der EuGH klargestellt, dass nach Art. 8 Abs. 3 der Infosoc-Richtlinie 2001/29/EG Verfügungen zur Sperrung bestimmter Internetadressen grundsätzlich zulässig sind und dass das Grundrecht der Benutzer auf Informationsfreiheit dem nicht grundsätzlich entgegensteht. Es sein eine Abwägung der Rechte im Einzelfall vorzunehmen und der Provider können die Sperrmethode selbst wählen (GRUR Int. 2014, 469 – Constantin ./.UPC Telekabel, RN 42).

Der EuGH hat im Fall Constantin ./. UPC Telekabel klargestellt, dass Gerichte Verfügungen gegen Access-Provider erlassen können, den Zugang zu bestimmten Servern zu sperren.

Auch in Deutschland hat es derartige Sperrverfügungen bereits gegeben. Bereits 2010 hat das LG Hamburg einem Access-Provider per einstweiliger Verfügung untersagt, der in den Niederlanden gehosteten Website „Pirate Bay“ weiterhin eine Zugangsleitung ins Internet bereitzustellen (Beschluss vom 6. Mai 2010, AZ 310 O 154/10). Die Rechtsmäßigkeit bleibt jedoch umstritten. Während in der Literatur gefordert wird, jede im Ausland gehostete Seite mit urheberrechtswidrigen Inhalten per einstweiliger Verfügung bei den Access-Providern zu

sperren (Nordemann/Schäfer GRUR 2009, 579), hat das OLG Köln eine Sperrverfügung als unzumutbar abgelehnt (GRUR 2014, 1081).

„McFadden“

Das LG München hat daher dem EuGH die Frage vorgelegt, ob Art. 12 der E-Commerce-Richtlinie so auszulegen ist, dass mit „nicht für die übermittelten Informationen verantwortlich“ bedeutet, dass etwaige Ansprüche auf Unterlassung, Schadensersatz, Zahlung der Abmahnkosten und Gerichtsgebühren des aufgrund einer Urheberrechtsverletzung Betroffenen gegen den Zugangs-Provider grundsätzlich oder jedenfalls in Bezug auf eine erste festgestellte Urheberrechtsverletzung ausgeschlossen sind“ (GRUR-RR 2014, 1166).

Der EuGH hat in seinem Urteil „McFadden“ auf die Frage geantwortet, wenn die drei Voraussetzungen des Art. 12 Abs. 1 vorliegen, bestehe keine Haftung des Diensteanbieters und es sei daher jedenfalls ausgeschlossen, dass der Rechteinhaber von dem Anbieter Schadenersatz verlange (GRUR 2016, 1146 – „McFadden ./. Sony Music“, RN 74).

Folglich sei auch die Erstattung der für den Schadenersatzanspruch aufgewendeten Abmahn- und Gerichtskosten ausgeschlossen (GRUR 2016, 1146 – „McFadden ./. Sony Music“, RN 75).

Wegen Art. 12 Abs. 3 stehe Art. 12 Abs. 1 aber einem Antrag bei einem Gericht nicht entgegen, es dem Anbieter zu untersagen, die Fortsetzung der Rechtsverletzung zu ermöglichen (GRUR 2016, 1146 – „McFadden ./. Sony Music“, RN 77).

Art. 12 Abs. 1 schließe es daher für sich genommen nicht aus, dass der Geschädigte die Erstattung der Gerichts- und Abmahnkosten verlangt, die für den vorstehenden Antrag aufgewendet worden sind (GRUR 2016, 1146 – „McFadden ./. Sony Music“, RN 78).

Zusammenfassend stellt das Gericht fest, es laufe Art. 12 Abs. 1 entgegen, wenn der Rechteinhaber Schadenersatzansprüche geltend mache, es laufe der Bestimmung aber nicht zuwider, wenn er von dem Zugangsanbieter Unterlassung der Rechtsverletzung und Zahlung der damit zusammenhängenden Anwalts- und Gerichtskosten verlangt, wenn die Ansprüche auf eine Gerichtsanordnung abzielen (GRUR 2016, 1146 – „McFadden ./. Sony Music“, RN 79).

Der EuGH hat auf eine weitere Frage des LG München festgehalten, dass die Ausnahmebestimmung des Art. 14 Abs. 1 Buchstabe b) der E-Commerce-Richtlinie (das „notice and take down“ bei Host Providern) nicht analog auf Access Provider anzuwenden ist (GRUR 2016, 1146 – „McFadden ./. Sony Music“, RN 65).

Auf eine weitere Frage hat der EuGH geantwortet, die Sicherung des Internetanschlusses durch ein Passwort sei für einen wirksamen Schutz des Urheberrechts erforderlich (GRUR 2016, 1146 – „McFadden ./. Sony Music“, RN 99). Eine solche Maßnahme schrecke Nutzer davon ab, über den WLAN-Zugang Urheberrechtsverletzungen zu begehen, wenn die Benutzer ihre Identität preisgeben müssen, um das Passwort zu erhalten, und damit nicht anonym handeln können (GRUR 2016, 1146 – „McFadden ./. Sony Music“, RN 96).

Stellungnahme zur Vereinbarkeit von §§ 7, 8 TMG mit dem EU-Recht

Die Ansicht des EuGH in „Scarlet Extended“ läuft auf eine Vollharmonisierung hinaus, die es dem nationalen Gesetzgeber und den nationalen Gerichten verbietet, die Haftungsprivilegien der Art. 12-15 ECRL abzuschwächen.

Zugleich lässt der EuGH in „UPC Telekabel“ zwar grundsätzlich gerichtliche Anordnungen gegen Provider zu, diese müssen jedoch vor dem Hintergrund der unternehmerischen Freiheit des Providers und der Grundrechte der Kunden verhältnismäßig sein.

Vor dem Hintergrund dieser Rechtsprechung und auch der Stellungnahme des Generalanwalts war die Entscheidung des EUG in „McFadden“ eher eine Überraschung. Der EuGH stellt fest, wenn die drei Voraussetzungen vorliegen, bestehe keine Haftung des Diensteanbieters. Zugleich soll es Art. 12 Abs. 1 nicht entgegenstehen, wenn der Rechteinhaber vom Diensteanbieter die Unterlassung der Rechtsverletzung fordert und vor Gericht beantragt, diesen zu verurteilen, es ihm zu untersagen, die Fortsetzung der Rechtsverletzung zu ermöglichen.

Diese Argumentation erscheint widersprüchlich. Wenn keine Haftung des Diensteanbieters besteht, kann der Diensteanbieter jedenfalls nach deutscher Rechtsbegrifflichkeit auch nicht auf Unterlassung haften. Die Begrifflichkeiten des EuGH sind jedoch offenbar andere. Unter „Haftung“ scheint er ausschließlich finanzielle Ansprüche zu verstehen.

Dennoch geht aus dem Urteil klar hervor, dass Art. 12 der E-Commerce-Richtlinie die Geltendmachung von Unterlassungsansprüchen nicht hindert.

Diese Ansicht ist abzulehnen, da sie im Ergebnis Art. 15 Abs. 1 der Richtlinie widerspricht. Muss der Access-Provider Unterlassungsansprüche auch für Verstöße fürchten, die ihm nicht bekannt sind, so muss er letztlich doch sein Angebot auf illegale Aktivitäten seiner Nutzer überwachen, schon um die Kosten von Abmahnungen zu vermeiden. Dies widerspricht aber dem klaren Wortlaut von Art. 15 abs. 1, umgesetzt in § 7 Abs. 2 TMG.

Im Gegensatz zur Ansicht von Nordemann (GRUR 2016, 1097) muss der WLAN-Anbieter nach dem Urteil des EuGH nämlich auch die Kosten der ersten Abmahnung tragen. Auch die erste Abmahnung dient nämlich der Vorbereitung der gerichtlichen Unterlassungsverfügung, die bei einer Zurückweisung der Abmahnung ohne Kostenrisiko eines sofortigen Anerkenntnisses beantragt werden kann. Nordemann übersieht ferner, dass der EuGH die analoge Anwendung des „notice and take down“ Prinzips, das Art. 14 der Richtlinie für Host Provider vorsieht, auf WLAN-Betreiber ausdrücklich abgelehnt hat (GRUR 2016, 1146 – „McFadden ./. Sony Music“, RN 65).

Der Anspruch von Art. 11 Enforcement-Richtlinie und Ar. 8 InfoSoc-Richtlinie, gerichtliche Anordnungen gegen Provider zuzulassen, steht also in einem Spannungsverhältnis zum Anspruch von Art. 12 E-Commerce-Richtlinie, von der Verantwortung freigestellt zu werden und zum Anspruch von Art. 15 E-Commerce-Richtlinie, nicht proaktiv tätig werden zu müssen.

Nach dem EuGH-Urteil „Scarlet Extended“ ist ein Gleichgewicht zwischen den Grundrechten der Rechteinhaber, des Providers und seiner Kunden herzustellen.

Es war erklärte Intention des deutschen Gesetzgebers, Rechtssicherheit für WLAN-Anbieter zu schaffen, indem diese von Prüf- und Verschlüsselungspflichten und vor der Pflicht zur Tragung von Anwaltskosten befreit werden (Gesetzentwurf der Bundesregierung, BT-DS 18/12202, S. 9). Zugleich sollte ein Verfahren geschaffen werden, um den Rechteinhabern außerhalb der Störerhaftung zu ihrem Recht zu verhelfen (Gesetzentwurf der Bundesregierung, BT-DS 18/12202, S. 9). Der Gesetzgeber hat also versucht, die Rechte beider Akteure im Sinne von „Scarlet Extended“ in Einklang zu bringen. Ob ihm das gelungen ist, soll ein Blick auf die betroffenen Grundrechte der Akteure zeigen.

Greifen Prüfungspflichten der WLAN-Anbieter in Grundrechte ein?

Alle von Rechtsprechung und Literatur im Rahmen der Prüfungspflichten der Störerhaftung diskutierten Maßnahmen bedeuten einen Konflikt mit den Grundrechten des Betreibers und seiner Kunden:

Eine Verschlüsselung des Zugangs beschneidet für Internetcafé-Betreiber bereits die Werbefunktion, da nur Personen das WLAN benutzen können, die bereits Kunden sind. Eine Weitergabe des Kennwortes an die Kunden ermöglicht jedoch Urheberrechtsverletzungen

Eine Kennungsvergabe an die Benutzer ergibt damit nur Sinn, wenn die Benutzer auch überwacht und bei Verstößen die Kennungen gesperrt werden.

Auch eine Portsperre, wie vom LG Hamburg vorgeschlagen, ergibt nur Sinn, wenn der Betreiber weiß, über welche Ports die Kunden Filesharing betreiben. Für Filesharing lassen sich nämlich prinzipiell alle Ports nutzen. Der Betreiber müsste also das Netz überwachen und prüfen, welche Ports für Filesharing genutzt werden.

Ohne eine solche Benutzerüberwachung wären weder eine Verschlüsselung, noch eine Portsperre wirkungsvoll. Wirkungslose Eingriffe können jedoch im Rahmen der Störerhaftung niemals zumutbar sein (so ausdrücklich LG Hamburg ZUM 2010, 902).

Es stellt sich daher die Frage, ob eine solche Überwachung der Benutzer nicht in die Rechte oder die Grundrechte der Benutzer eingreifen würde.

Access Provider und das Fernmeldegeheimnis

Art 10 Grundgesetz

(1) Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich.

§ 88 TKG - Fernmeldegeheimnis

(1) Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

(2) Zur Wahrung des Fernmeldegeheimnisses ist jeder Diensteanbieter verpflichtet. Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist.

(3) Den nach Absatz 2 Verpflichteten ist es untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. Sie dürfen Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, nur für den in Satz 1 genannten Zweck verwenden. Eine Verwendung dieser Kenntnisse für andere Zwecke, insbesondere die Weitergabe an andere, ist nur zulässig, soweit dieses Gesetz oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht. Die Anzeigepflicht nach § 138 des Strafgesetzbuches hat Vorrang.

Ob das Fernmeldegeheimnis einer Haftung der Access Provider entgegensteht, ist umstritten:

Nazari-Khanachayi ist der Ansicht, das Fernmeldegeheimnis sei vorliegend gar nicht einschlägig. Die Störerhaftung diene insoweit der Umsetzung von Art. 8 Abs. 3 der Infosoc-Richtlinie. Daher sei die Störerhaftung in dieser Frage nicht dem Grundgesetz, sondern der EU-Grundrechtecharta unterworfen (Nazari-Khanachayi GRU 2015, 115).

Eine andere Ansicht ist der Meinung, § 88 TKG schütze nur die Individuelle Kommunikation, nicht Angebote an jedermann auf Web-Servern. Auch die Verhinderung von Kommunikation greife nicht in den Schutzbereich des Art. 10 GG ein. Für eine DNS-Blockade sei auch keine Kenntnisnahme von Nutzerverhalten nötig (Durner ZUM 2010, 833)

Das OLG Köln sieht dagegen einen Eingriff in das Fernmeldegeheimnis als gegeben an. Da Fernmeldegeheimnis schütze allerdings nicht vor einer staatlichen Blockade der Kommunikation (GRUR 2014, 1081).

Nach einer weiteren Ansicht in Literatur und Rechtsprechung stand § 88 TKG bisher einer Verpflichtung zur Sperrung urheberrechtsverletzender Quellen entgegen. Sperrungen seien nur durchführbar, wenn sich der Provider Kenntnisse über Umstände der Telekommunikation zu Nutze macht, um aufgrund dieser Umstände als illegal identifizierte Websites zu sperren. Dies greife in das Fernmeldegeheimnis ein, was einer gesetzliche Beschränkung von Art. 10 GG bedürfe (LG Hamburg ZUM 2010, 902; Frey/Rudolph/Oster MMR-Beilage 2012, 1; OLG Hamburg GRUR 2014, 140; ebenso zur TMG-Reform Mantz GRUR 2017, 969). Übertragen auf die TMG-Reform, schafft § 7 Abs. 4 TMG nach dieser Ansicht erst die gesetzliche Rechtsgrundlage für einen solchen Eingriff in das Fernmeldegeheimnis.

Der BGH hat sich in seinen Entscheidungen vom 26. November 2015 der Ansicht von Durner angeschlossen, allerdings mit einer Einschränkung. Er führt aus, das Fernmeldegeheimnis gelte nicht für Kommunikation, die an die Allgemeinheit gerichtet ist. Solange keine weitergehende Sichtung der Daten erfolge und dies lediglich technikbedingt und anonym erfasst werden, werde nicht in den Schutzbereich des Fernmeldegeheimnisses eingegriffen TMG (GRUR 2016, 268 – „goldesel.to“, RN 69; ZUM-RD 2016, 156, - „3dl.am“, RN 56). Spindler hat sich inzwischen der Ansicht des BGH angeschlossen (GRUR 2016, 451; NJW 2017, 2305).

Stellungnahme zur Auslegung von §§ 7, 8 TMG vor dem Hintergrund des Fernmeldegeheimnisses

Es spricht in der Tat einiges dafür, neben der EU-Grundrechtecharta auch das Grundgesetz anzuwenden, und damit auch Art. 10, der durch § 88 TKG konkretisiert wird.

Nach § 88 Abs. 3 TKG ist es WLAN-Betreibern ausdrücklich untersagt, sich Kenntnisse von Inhalt der Kommunikation zu verschaffen, wenn das nicht für den Betrieb des Netzes erforderlich ist. Die Überwachung der Benutzer auf die Verwendung von Filesharing-Programmen ist damit ausdrücklich verboten. Ebenso untersagt ist die Prüfung, welche Ports für Filesharing benutzt werden, denn auch dies setzt eine Kenntnisnahme vom Inhalt der Kommunikation voraus.

Entgegen der Ansicht von Durner, dem BGH und dem OLG Köln greift auch die Sperrung von bestimmten IP-Adressen in das Fernmeldegeheimnis ein. Eine IP-Sperre wird technisch dadurch umgesetzt, dass die von den Benutzerrechnern abgesendeten IP-Anforderungen von einem Router umgeleitet werden, so dass eine Fehlermeldung oder eine andere Website ausgegeben wird. Dieser Eingriff in den Kommunikationsprozess betrifft auch das in Art 10 GG geschützte Fernmeldegeheimnis (Frey/Rudolf MMR-Beilage 2012,1; OLG Hamburg GRUR 2014, 104).

Auch die Sperre von DNS-Einträgen stellt technisch eine Manipulation der DNS-Auflösung in IP-Adressen dar, indem anstelle der tatsächlichen IP-Adresse durch einen manipulierten DNS-Server eine falsche IP-Adresse ausgegeben wird. Da diese Ausgabe des DNS-Servers letztlich durch Anfragen des Benutzers ausgelöst wird, findet auch bei der DNS-Sperre ein Eingriff in die Individualkommunikation statt, die in das Fernmeldegeheimnis eingreift. Das hat auch der Gesetzgeber so gesehen, der in dem inzwischen aufgehobenen Zugangserschwerungsgesetz in § 11 ausdrücklich das Fernmeldegeheimnis als eingeschränktes Grundrecht zitiert hat (Frey/Rudolf MMR-Beilage 2012,1; OLG Hamburg GRUR 2014, 140; Heidrich/Heymann MMR 20016, 370; Frey/Nohr GRUR-Prax 2016, 164).

Damit bedarf jede Verpflichtung eines Access-Providers oder WLAN-Anbieters zur Sperrung bestimmter Adressen oder Ports einer gesetzlichen Grundlage. Eine solche Grundlage schafft § 7 Abs. 4 TMG nun erstmals und ausschließlich für WLAN-Betreiber. Sperrverpflichtungen gegen sonstige Access-Provider würden damit nach wie vor gegen das Fernmeldegeheimnis verstoßen.

Kommerzielle WLAN-Betreiber und die EU-Grundrechtecharta

Einer Haftung der Access Provider könnte auch die EU-Grundrechtecharta entgegenstehen:

Artikel 7 Achtung des Privat- und Familienlebens

Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation.

Artikel 8 Schutz personenbezogener Daten

Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

Artikel 11 Freiheit der Meinungsäußerung und Informationsfreiheit

(1) Jede Person hat das Recht auf freie Meinungsäußerung. Dieses Recht schließt die Meinungsfreiheit und die Freiheit ein, Informationen und Ideen ohne behördliche Eingriffe und ohne Rücksicht auf Staatsgrenzen zu empfangen und weiterzugeben.

In seinem Urteil Scarlet extended ./. SABAM hat der EuGH festgestellt, dass zwar auch das Recht der am geistigen Eigentum dem Schutz des Art. 17Abs. 2 der EU-Grundrechtecharta unterliegt. Das Recht sei jedoch nicht schrankenlos. Vielmehr hätten die nationalen Gerichte dieses Recht in ein Gleichgewicht mit anderen Grundrechten zu bringen. Der EuGH nennt in diesem Zusammenhang das nach Art. 16 der Charta geschützte Recht des Providers auf seine unternehmerische Freiheit, aber auch die Rechte der Benutzer auf den Schutz ihrer personenbezogenen Daten (Art. 8) und den freien Empfang und die freie Sendung von Informationen (Art. 11 Abs. 1). Bei einer Identifikation der Benutzer oder der Prüfung aller Kommunikationseinhalte werde in Art. 8, bei einer Sperrung in Art. 11 eingegriffen (MMR 2012, 174 – Scarlet extended ./. SABAM RN 43ff).

In der Entscheidung „McFadden“ hat der EuGH ferner darauf hingewiesen, dass die Prüfung aller übermittelten Informationen auch gegen Art. 15 der E-Commerce-Richtlinie verstoßen würde (GRUR 2016, 1146 – „McFadden ./. Sony Music“, RN 87), er hat zugleich aber die Identifikation des Benutzer für erforderlich angesehen, ohne auf den noch im Urteil „Scarlet extended“ bejahten Eingriff in das Recht auf Datenschutz einzugehen (GRUR 2016, 1146 – „McFadden ./. Sony Music“, RN 99).

Stellungnahme zur Wirkung der EU-Grundrechtecharta

Der EuGH widerspricht sich auch in dieser Frage selbst. Wenn die Identifikation des Benutzers einen Eingriff in das Recht auf Datenschutz bedeutet, dann bedarf dieser Eingriff einer Rechtfertigung und damit auch einer ausdrücklichen gesetzlichen Grundlage.

Bei Diensteanbietern im Internet wäre ein Zwang zur Identifikation jedoch sogar ein Verstoß gegen eine gesetzliche Vorschrift:

§ 13 Pflichten des Diensteanbieters

(6) Der Diensteanbieter hat die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren.

Nach dem gesetzlichen Leitbild soll somit eine anonyme Nutzung ausdrücklich zulässig sein. Dem widerspricht es, wenn der WLAN-Betreiber dafür haften soll, wenn er anonyme Nutzung zulässt. Es fehlt somit nicht nur an einer gesetzlichen Grundlage für den Eingriff in den Datenschutz, das Gesetz steht dem Eingriff sogar ausdrücklich entgegen.

Entgegen der Ansicht von Sesing und Baumann scheidet es daher aus, WLAN-Anbieter im Rahmen einer „richtlinienkonformen Auslegung“ ohne gesetzliche Grundlage zu einer Registrierung der Benutzer zu verpflichten.

Stellungnahme zur Vereinbarkeit von §§ 7 und 8 TMG mit EU-Recht und dem Grundgesetz

Wie gesehen, enthält das EU-Recht einige Widersprüche. Zugleich sind alle Beteiligten, WLAN-Anbieter, Rechteinhaber und Benutzer, Grundrechtsträger.

Wie Mantz zutreffend feststellt, hat der Gesetzgeber bei der Umsetzung der EU-Richtlinien Spielräume. Diese konnte er bei der TMG-Reform nutzen.

Art. 8 InfoSoc-Richtlinie und Art. 11 Enforcement-Richtlinie besagen ausschließlich, dass gerichtliche Anordnungen zulässig sein müssen. Dies hat der Gesetzgeber mit Art. 7 Abs. 4 TMG für WLAN-Anbieter ausdrücklich vorgesehen. Ferner lässt auch Art. 7 Abs. 3 TMG gerichtliche Anordnungen weiterhin zu. Damit ist den Rechtsinhabern das Recht eingeräumt, die ihnen nach den Richtlinien zusteht, ein Folgenbeseitigungsanspruch.

Fraglich ist aber, ob die Sperrung von Informationen in einem WLAN ein taugliches Mittel darstellt. Der Gesetzentwurf erwähnt als Sperrmaßnahme die Sperrung bestimmter Ports am Router, um Filesharing zu unterbinden (Gesetzentwurf der Bundesregierung, BT-DS 18/12202, S. 12). Portsperren sind jedoch zu diesem Zweck untauglich, da Filesharing grundsätzlich auf allen Ports möglich ist. Sie dürften daher unverhältnismäßig sein (Mantz GRUR 2017, 969). Ferner erwähnt der Gesetzentwurf die Sperre bestimmter Websites (Gesetzentwurf der Bundesregierung, BT-DS 18/12202, S. 12). Dabei besteht jedoch das Problem des Overblockings, wenn die Sperre auf IP-Basis erfolgt, da unter einer IP meist mehrere Webserver abrufbar sind. Ein Overblocking würde die Maßnahme unverhältnismäßig werden lassen (Mantz GRUR 2017, 969). Es stellt sich daher die Frage, ob sich im Einzelfall Sperrmaßnahmen finden lassen, die zumutbar und verhältnismäßig sind.

Eine Verletzung von Art. 3 GG liegt nicht vor, da die Rechteinhaber bei den Access Providern über § 101 UrhG die Möglichkeit haben, gegen die Rechtsverletzer vorzugehen. Ihre Rechte sind daher anderweitig gesichert. Art. 3 GG fordert jedoch nur, gleiches gleich zu behandeln, nicht, Access Provider und WLAN Anbieter trotz der unterschiedlichen Kenntnisse über die Benutzer gleich zu behandeln (ähnlich Mantz GRUR 2017, 969).

§ 8 TMG kann damit wieder die Funktion erfüllen, die ihm von Beginn an zugedacht war: Access Provider von jeder Haftung für Rechtsverletzungen der Benutzer befreien.

Folgerungen für Fall 6

§ 8 Durchleitung von Informationen

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

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

Sofern diese Diensteanbieter nicht verantwortlich sind, können sie insbesondere nicht wegen einer rechtswidrigen Handlung eines Nutzers auf Schadensersatz oder Beseitigung oder Unterlassung einer Rechtsverletzung in Anspruch genommen werden; dasselbe gilt hinsichtlich aller Kosten für die Geltendmachung und Durchsetzung dieser Ansprüche. Die Sätze 1 und 2 finden keine Anwendung, wenn der Diensteanbieter absichtlich mit einem Nutzer seines Dienstes zusammenarbeitet, um rechtswidrige Handlungen zu begehen. […]

(3) Die Absätze 1 und 2 gelten auch für Diensteanbieter nach Absatz 1, die Nutzern einen Internetzugang über ein drahtloses lokales Netzwerk zur Verfügung stellen.

(4) *Diensteanbieter nach § 8 Absatz 3 dürfen von einer Behörde nicht verpflichtet werden,*

a. *vor Gewährung des Zugangs*
   a) *die persönlichen Daten von Nutzern zu erheben und zu speichern (Registrierung) oder*
   b) *die Eingabe eines Passworts zu verlangen oder*
b. *das Anbieten des Dienstes dauerhaft einzustellen*

Davon unberührt bleibt, wenn ein Diensteanbieter auf freiwilliger Basis die Nutzer identifiziert, eine Passworteingabe verlangt oder andere freiwillige Maßnahmen ergreift.

Nach § 8 Abs. 1 Satz 2 und Abs. 3 unterliegt der Mandant keiner Unterlassungspflicht.

Nach § 8 Abs. 1 Satz 2 braucht der Mandant auch die Anwaltskosten nicht zu zahlen.

§ 8 Abs. 4 ist nicht anwendbar, da die Gegenseite keine Behörde ist. Das bedeutet aber nicht im Umkehrschluss, dass die Gegenseite die Vergabe von Passwörtern fordern könnte, denn der Mandant unterliegt schon nach § 8 Abs. 1 keiner Haftung. Daher unterliegt er auch keinen entsprechenden Prüfungspflichten der Störerhaftung. Eine andere Rechtsgrundlage für den Anspruch liegt nicht vor. Im Übrigen würde eine Pflicht zur Vergabe von Benutzerkennungen dem Recht der Nutzer auf anonyme Nutzung nach § 13 Abs. 6 TMG widersprechen.

Taktisches Vorgehen

1. Die Abmahnung unter Verweis auf § 8 Abs. 1 und 3 TMG zurückweisen
2. Keine Unterlassungserklärung abgeben
3. Die Forderung auf Zahlung der Kosten der Abmahnung zurückweisen
4. Die Forderung auf Einrichtung von Benutzerkonten zurückweisen
5. Den Mandanten darauf hinweisen, dass der Gegner Ansprüche nach § 7 Abs. 4 TMG stellen könnte

§ 7 TMG- Allgemeine Grundsätze

(4) *Wurde ein Telemediendienst von einem Nutzer in Anspruch genommen, um das Recht am geistigen Eigentum eines anderen zu verletzen und besteht für den Inhaber dieses Rechts keine andere Möglichkeit, der Verletzung seines Rechts abzuhelfen, so kann der Inhaber des Rechts von dem betroffenen Diensteanbieter nach § 8 Absatz 3 die Sperrung der Nutzung von Informationen verlangen, um die Wiederholung der Rechtsverletzung zu verhindern. Die Sperrung muss zumutbar und verhältnismäßig sein. Ein Anspruch gegen den Diensteanbieter auf Erstattung der vor- und außergerichtlichen Kosten für die Geltendmachung und Durchsetzung des Anspruchs nach Satz 1 besteht außer in den Fällen des § 8 Absatz 1 Satz 3 nicht.*