- **Zuerst veröffentlicht in EuZW 2016, 817 –**
-

Rechtssicherheit für WLAN? Die Haftung des WLAN-Betreibers und das McFadden-Urteil des EuGH

Dr. Reto Mantz*

Mit der Sache „McFadden" hatte der EuGH Gelegenheit, zur Vereinbarkeit der deutschen Störerhaftung mit europäischen Vorgaben sowie zu den haftungsrechtlichen Anforderungen an den Betreiber eines öffentlichen WLANs Stellung zu nehmen. Den Schlussanträgen des Generalanwalts ist er dabei nur teilweise gefolgt. Zwar sind Fragen der grundsätzlichen Anwendbarkeit der Störerhaftung nun geklärt. Rechtssicherheit vermag auch dieses Urteil aber nicht zu schaffen. Stattdessen eröffnet der EuGH eine ganze Reihe von Folgefragen.

With „McFadden", the ECJ had the opportunity to address questions regarding the compatibility of the German intermediary liability with European Directives as well as the reasonability of certain measures for providers of public WiFi hotspots. All in all, the ECJ followed the recommendations of the Advocate General only partially. On the one hand, the general applicability of intermediary liability is now clear. However, legal certainty for public WiFi has not been obtained. Instead, with its decision the ECJ poses a set of new questions.

I. Einleitung

Seit Jahren wird über die Verantwortlichkeit des Betreibers eines öffentlichen WLAN diskutiert. Dabei hat die Debatte eine rechtliche und eine politische Seite, die beide eng miteinander verwoben sind. Auf der rechtlichen Seite konnte (und kann) man u.a. über die Anwendbarkeit und Reichweite der Privilegierung in Art. 12 der E-Commerce-Richtlinie 2000/31/EG (ECRL), deren Verhältnis zur deutschen Regelung in § 8 TMG und die Zumutbarkeit von einzelnen Maßnahmen wie Verschlüsselung, Identifizierung und Überwachung streiten. Auf der anderen, politischen Seite wurde und wird sowohl von der EU-Kommission als auch der deutschen Bundesregierung die Verbreitung öffentlicher WLANs auch unter Einbindung von Privatpersonen gefordert und gefördert. Nur einen Tag vor der Verkündung der EuGH-Entscheidung hatte die EU-Kommission das Projekt „WiFi4EU" vorgestellt, eine Schlüsselinitiative zur Förderung öffentlich zugänglicher WLANs.[1] Die Förderung von WLANs tat und tut auch Not, denn Deutschland ist mit unter zwei WLAN-Hotspots auf 100.000 Einwohner praktisch auf dem Stand eines Entwicklungslandes.[2] Grund ist u.a., dass die seit vielen Jahren bestehende Rechtsunsicherheit, ob und wann der Betreiber als Störer haftet, den Ausbau massiv behinderte. Denn welcher Betreiber wollte mit ungewisser Aussicht ein WLAN aufbauen und am Ende für – praktisch nicht verhinderbare – Rechtsverletzungen der eigenen Nutzer haften?
Vor diesem Hintergrund hatte sich der deutsche Gesetzgeber im Sommer 2016 nach jahrelanger Diskussion und unter dem Eindruck der Schlussanträge des EuGH-Generalanwalts, zu einer Anpassung von § 8 TMG durchgerungen.[3]

---

* Der Autor ist Richter am Landgericht Frankfurt am Main und Dipl.-Informatiker.

[1] EU-Kommission, Pressemitteilung IP/16/3008 v. 14.9.2016, http://europa.eu/rapid/press-release_IP-16-3008_de.htm.

[2] eco MicroResearch, Verbreitung und Nutzbarkeit von WLAN in Deutschland, 11/2014, https://www.eco.de/wp-content/blogs.dir/eco-microresearch_verbreitung-und-nutzung-von-wlan1.pdf.

[3] Dazu *Spindler*, NJW 2016, 2449; *Sesing*, MMR 2016, 507; *Franz/Sakowski*, CR 2016, 524; zur Entwicklung und den Vorentwürfen *Mantz/Sassenberg*, CR 2015, 298; *Sesing*, MMR 2015, 423.

Die Entscheidung „McFadden“ des EuGH[4] stellt in der rechtlichen Diskussion nun den bisherigen Höhepunkt dar. Den großen Erwartungen, die nicht zuletzt aufgrund der politischen Dimension an den EuGH gestellt worden sind, wird das Urteil aber leider in keiner Weise gerecht.

II. Die Rechtssache McFadden

1. Sachverhalt

Im Jahr 2014 hatte das LG München I über die negative Feststellungsklage eines WLAN-Betreibers zu entscheiden.[5] Der Betreiber, Herr McFadden, hatte sein WLAN zu Werbezwecken kostenfrei und ohne weitere Sicherheitsvorkehrungen der Öffentlichkeit angeboten. Einer seiner Nutzer hatte darüber ein urheberrechtlich geschütztes Werk mittels Filesharing heruntergeladen und gleichzeitig angeboten. McFadden war daraufhin abgemahnt worden. Der Rechteinhaber verlangte die Abgabe einer Unterlassungserklärung, Schadensersatz und Abmahnkosten.
Das LG München I wollte vom EuGH u.a. wissen, ob Art. 12 ECRL auf das unentgeltlich angebotene WLAN von McFadden überhaupt Anwendung findet, ob Art. 12 ECRL Unterlassungsansprüche erfasst und was vom WLAN-Betreiber an Schutzmaßnahmen verlangt werden kann.

2. Schlussanträge

Der zuständige Generalanwalt beim EuGH hat im März 2016 seine Schlussanträge[6] vorgelegt. Er bejahte die Frage der persönlichen Anwendbarkeit von Art. 12 ECRL. Es sei auch grundsätzlich zulässig, wenn gegen den WLAN-Betreiber gerichtliche oder behördliche Anordnungen ergingen. Schadensersatz oder Abmahnkosten könnten jedoch nicht verlangt werden. Auch die Auferlegung von Kosten des Anordnungsverfahrens sei unzulässig, da diese eine ähnlich abschreckende Wirkung wie Schadensersatzforderungen hätten.[7] Darüber hinaus sei es dem WLAN-Betreiber unzumutbar, den Datenverkehr seiner Nutzer zu überwachen, das WLAN durch Verschlüsselung zu sichern oder den Betrieb zur Vermeidung von Rechtsverletzungen gänzlich einzustellen.

3. Entscheidung des EuGH

Der EuGH ist dem Generalanwalt nur teilweise gefolgt. Er hat – in Übereinstimmung mit der allgemeinen Auffassung in der Literatur[8] – die Anwendung von Art. 12 ECRL auf WLANs angenommen.[9] Der persönliche Anwendungsbereich, der für „in der Regel gegen Entgelt“ erbrachte Dienste gilt, ist danach auch dann eröffnet, wenn ein Dienst zu Werbezwecken erbracht wird.[10] Weitere Voraussetzungen, wie z.B. ein Vertrag mit dem Nutzer, bestehen nicht.[11] Damit hat der EuGH implizit auch die Frage – negativ – beantwortet, ob Art. 12 ECRL auf die WLANs privater Personen Anwendung findet. Der Generalanwalt hatte dies noch offen gelassen.
Inhaltlich obliegen dem WLAN-Betreiber, anders als dem Host Provider, auch nach einer Aufforderung keine Lösch- oder Sperrpflichten entsprechend Art. 14 ECRL, da aufgrund der reinen Durchleitung von Informationen keine Kontrollmöglichkeiten über Inhalte bestehen.[12]

---

[4] EuGH, Urt. v. 15.9.2016 – C-484/14, EuZW 2016, 821 (in diesem Heft).
[5] LG München I, GRUR Int. 2014, 1166 – Bring mich nach Haus; eingehend dazu *Mantz/Sassenberg*, MMR 2015, 85.
[6] EuGH-Generalanwalt, Schlussanträge vom 16.3.2016 – C-484/14, BeckRS 2016, 80483.
[7] EuGH-Generalanwalt, Schlussanträge vom 16.3.2016 – C-484/14, BeckRS 2016, 80483 Rn. 77.
[8] *Sassenberg/Mantz*, WLAN und Recht, 2014, Rn. 216; *Stang/Hühner*, GRUR-RR 2008, 273 (275); *Gietl*, MMR 2007, 630 (631); *Hornung*, CR 2007, 88 (93).
[9] EuGH, EuZW 2016, 821 Rn. 34 ff. – McFadden.
[10] EuGH, EuZW 2016, 821 Rn. 43. – McFadden; vgl. in diese Richtung schon EuGH, Urt. v. 11.9.2014 - C‑291/13 Rn. 28 f. – Papasavvas.
[11] EuGH, EuZW 2016, 821 Rn. 45 ff. – McFadden.
[12] EuGH, EuZW 2016, 821 Rn. 63 – McFadden.

Auch zu der lange strittigen Frage, welche Ansprüche Art. 12 ECRL sachlich umfasst, hat der EuGH Stellung genommen und hier seine bisherige Linie[13] bestätigt. Art. 12 ECRL schließt danach insbesondere Ansprüche auf Schadensersatz aus.[14] Allerdings sei es nach Art. 12 Abs. 3 ECRL zulässig, wenn „gerichtliche oder behördliche Anordnungen" ergehen, die es dem Betreiber untersagen, die Fortsetzung der Rechtsverletzung zu ermöglichen.[15] Damit schließt Art. 12 ECRL Unterlassungsansprüche – in Übereinstimmung mit der langjährigen Rechtsprechung des BGH[16] - nicht aus.
Auf die Fragen des LG München I nach den dem WLAN-Betreiber zumutbaren Maßnahmen, nämlich, ob es dem Betreiber zuzumuten ist, den Betrieb einzustellen, seine Nutzer zu überwachen oder den Zugang mit einem Passwortschutz zu versehen, erachtet der EuGH zunächst die Einstellung des Betriebs als unverhältnismäßig.[17] Die Überwachung der Nutzer wiederum stelle einen evidenten Verstoß gegen Art. 15 ECRL dar.[18] Allerdings sei es verhältnismäßig, wenn der Betreiber auf gerichtliche Anordnung hin verpflichtet werde, seinen Anschluss durch ein Passwort zu sichern. Denn es sei davon auszugehen, dass diese Sicherung eine Abschreckung der Nutzer von der Begehung von Rechtsverletzungen bewirke, wenn die Nutzer zuvor ihre Identität offenbaren müssten, um das erforderliche Passwort zu erhalten und damit nicht anonym handeln könnten.[19]

III. Bewertung und Folgen

Es ist begrüßenswert, dass der EuGH mit dem vorliegenden Urteil eine Reihe von bisher strittigen oder wenigstens unklaren Fragen insbesondere zum persönlichen und sachlichen Anwendungsbereich der ECRL beantwortet hat. Auf der anderen Seite lässt das Urteil aber eminent wichtige Probleme weiterhin offen und eröffnet insbesondere mit der Postulierung einer Sicherungs- und Identifizierungspflicht erhebliche neue tatsächliche und rechtliche Unsicherheiten. Unklar bleibt letztlich das Verhältnis zur – teilweise überschießenden – neu gefassten deutschen Regelung in § 8 TMG. Hierzu hat der EuGH selbstverständlich nicht Stellung genommen.

1. Schadensersatz, Unterlassungsansprüche und Abmahnkosten

Mit dem Urteil des EuGH ist nun geklärt, dass den WLAN-Betreiber keine Schadensersatzansprüche für die rechtswidrigen Handlungen seiner Nutzer treffen. Dies stellt allerdings keine Neuerung dar. Wird mit einer Abmahnung dieser Schadensersatz ebenfalls verlangt, sind insoweit auch keine Abmahnkosten zu erstatten. Im Ergebnis ist auch dies jedoch unbedeutend, da zum einen Abmahnkosten in der Regel allein auf Basis des Werts des Unterlassungsanspruchs geltend gemacht werden und andererseits der Schadensersatzanspruch in seiner Höhe meist nicht ins Gewicht fällt.
Andererseits können Unterlassungsansprüche sowie hierauf gestützte Abmahnkosten gegen den WLAN-Betreiber geltend gemacht werden. Dabei ist der Unterlassungsanspruch darauf zu richten,

---

[13] EuGH, GRUR 2014, 468 – UPC Telekabel/Constantin Film; vgl. auch schon EuGH, GRUR 2012, 265 – Scarlet Extended.
[14] EuGH, EuZW 2016, 821 Rn. 74 f. – McFadden.
[15] EuGH, EuZW 2016, 821 Rn. 77 – McFadden.
[16] BGH, GRUR 2004, 693 – Schöner Wetten; BGH, GRUR 2004, 860 – Internetversteigerung I; kritisch dazu *Spindler*, GRUR 2011, 101 (102); *Leible/Sosnitza*, NJW 2007, 3324.
[17] EuGH, EuZW 2016, 821 Rn. 88 – McFadden.
[18] EuGH, EuZW 2016, 821 Rn. 87 – McFadden.
[19] EuGH, EuZW 2016, 821 Rn. 96 – McFadden.

dass der WLAN-Betreiber es unterlässt, die Fortsetzung der Rechtsverletzung zu ermöglichen.[20] Das EuGH-Urteil steht damit letztlich auch massenhaften Abmahnungen von Anschlussinhabern nicht entgegen.

2. Zumutbare Sicherungsmaßnahmen

Als problematisch wird sich das EuGH-Urteil mit Blick auf die dem Betreiber zumutbaren Maßnahmen erweisen. Insoweit hat der EuGH ausdrücklich allein diejenigen Maßnahmen bewertet, die das LG München I in der Vorlagefrage angeführt hatte.[21] Er hat damit insbesondere offen gelassen, ob andere Maßnahmen in Betracht kommen. Die entsprechenden Diskussionen werden dementsprechend weitergehen.[22]

a. Abwägung betroffener Rechte

Der EuGH betont erneut, dass insoweit eine Abwägung zwischen den betroffenen Grundrechten zu treffen ist. Angeführt hat der EuGH hier die Rechte auf Schutz des geistigen Eigentums nach Art. 17 Abs. 2 der Grundrechte-Charta (GRCh), der unternehmerischen Freiheit nach Art. 16 GRCh und der Informationsfreiheit nach Art. 11 GRCh. Wieder unberücksichtigt hat der EuGH leider das Recht auf Achtung der Kommunikation nach Art. 7 GRCh und Art. 8 EMRK gelassen, die im deutschen Recht dem Schutz des Fernmeldegeheimnisses nach Art. 10 GG entsprechen.[23] Dies mag daran liegen, dass die Einstellung des Betriebs und die Einrichtung einer Zugangssicherung dieses Recht nicht beeinträchtigen dürften. Bei der Abwägung anderer Maßnahmen wird das Fernmeldegeheimnis aber durchaus eine Rolle spielen.[24] Zu berücksichtigen wird weiter sein, dass der EuGH anerkannt hat, dass der Anbieter eines Kommunikationsnetzes nur durchfließende Daten transportiert und dementsprechend praktisch keine Kontrollmöglichkeiten hat.[25]

Wenig überraschend hat der EuGH jedenfalls Überwachungspflichten abgelehnt, da diese Art. 15 ECRL widersprechen würden.[26] Ebenso ist ohne Weiteres verständlich, dass der EuGH es als unzumutbar erachtet hat, den WLAN-Anbieter zur vollständigen Einstellung seines Angebots zu zwingen, weil dies einen massiven Eingriff in die unternehmerische Freiheit darstellen würde.

b. Sicherung durch Passwort und Identifizierung

Als zumutbar angesehen hat der EuGH hingegen, dass der Anbieter sein WLAN durch ein Passwort sichert. Technisch kann eine solche Sicherung durch eine Verschlüsselung (z.B. nach dem Standard WPA2) oder durch eine Vorschaltseite mit Anmeldemaske realisiert werden.

aa. Sicherung ...

---

[20] EuGH, EuZW 2016, 821 Rn. 77 – McFadden; zur Antragsfassung vgl. auch BGH, MMR 2010, 565 – Sommer unseres Lebens m. Anm. Mantz.
[21] EuGH, EuZW 2016, 821 Rn. 86 – McFadden.
[22] Zur Zumutbarkeit der einzelnen, denkbaren Maßnahmen eingehend *Sassenberg/Mantz*, (o. Fn. 8), Rn. 227 ff.
[23] *Baldus*, in: Epping/Hillgruber, BeckOK-GG, 29. Ed. 2015, Art. 10 Rn. 76 f.
[24] Vgl. zu Websperren *Heidrich/Heymann*, MMR 2016, 370 (374); s. auch OLG Köln, GRUR 2014, 1081 – Goldesel; OLG Hamburg, GRUR-RR 2014, 140 – 3dl.am; anders im Ergebnis aber BGH, GRUR 2016, 268 – Störerhaftung des Access Providers II.
[25] EuGH, EuZW 2016, 821 Rn. 63 – McFadden.
[26] So auch schon EuGH, GRUR 2012, 265 – Scarlet Extended.

Die Pflicht zur Sicherung des WLAN hat der EuGH als eine lediglich „technische Modalität" bezeichnet, die nur in „marginaler Weise" die Ausübung der Tätigkeit des Anbieters beeinflusse.[27] Leider bleibt der EuGH hier jegliche tatsächliche Grundlage seiner Entscheidung schuldig.
Selbstverständlich ist die Verschlüsselung eines WLAN für den Anbieter im Kern eine einfach einzurichtende „technische Modalität". Der EuGH verkennt jedoch, dass diese „Modalität" die Reichweite des Angebots ganz erheblich einschränkt. Nutzer, die erst ein Passwort (analog) erfragen oder sich in einer Anmeldemaske anmelden müssen, werden in nicht unbeachtlichem Umfang von der Nutzung des WLAN ganz absehen, was – bezogen auf den Fall McFadden – die Werbewirkung für sein Unternehmen massiv reduzieren würde.[28] Diese Problematik hatte der Generalanwalt beim EuGH erkannt und konstatiert, dass bei der Einrichtung einer Verschlüsselung damit zu rechnen sei, dass manche Unternehmen nicht mehr bereit seien, WLAN anzubieten.[29]
Eine Vorschaltseite mit Anmeldung wiederum würde – neben der Abschreckung potentieller Nutzer – die Einrichtung und den Betrieb einer erheblichen technischen Infrastruktur erfordern. Zusätzlich sind Vorschaltseiten, auch Captive Portals genannt, technisch problematisch. Sie nutzen nämlich einen technischen Trick, um Nutzer auf eine bestimmte Seite zu lenken. Dieser Trick hat aber zur Folge, dass Nutzer, die nicht das WWW nutzen wollen, sondern z.B. nur E-Mail, Whatsapp etc., überhaupt keinen Zugang zum Netz erlangen können, da schon die Weiterleitung auf die Anmeldemaske nicht funktioniert.[30]

bb. ... und Offenlegung der Identität

Weiter nimmt der EuGH – erneut ohne Darlegung einer faktischen Grundlage – an, dass die Einrichtung einer Sicherung des WLAN, bei der die Nutzer ihre Identität offenbaren müssen,[31] Nutzer von Rechtsverletzungen abschrecken könne.[32] Diese Annahme ist jedoch fragwürdig. Der EuGH-Generalanwalt hat eine solche Maßnahme folgerichtig als zur Abschreckung unwirksam und unverhältnismäßig bezeichnet.[33] Schon im Rahmen der Diskussion um den Klarnamenzwang in Internetforen hat sich gezeigt, dass der Zwang zur Offenlegung der Identität Rechtsverletzungen nicht zu verhindern vermag.[34] Gerade in Universitätsnetzwerken, bei denen die Studenten zwingend mit vollem Namen angemeldet sind, dürfte Filesharing häufig betrieben werden. Zudem können Nutzer im WLAN ohne Weiteres auch selbst Maßnahmen zur Verschleierung ihres Handelns ergreifen und so einer Inanspruchnahme entgehen.[35]

---

[27] EuGH, EuZW 2016, 821 Rn. 91 – McFadden.
[28] Ebenso EuGH-Generalanwalt, Schlussanträge vom 16.3.2016 – C-484/14, BeckRS 2016, 80483 Rn. 139; vgl. auch Befragung *Kabel Deutschland*, PM v. 6.3.2014, abrufbar unter: https://www.kabeldeutschland.com/de/presse/pressemitteilung/produktnachrichten/632014.html; *Mantz/Sassenberg*, MMR 2015, 85 (90); vgl. auch AG Hamburg, CR 2014, 536.
[29] EuGH-Generalanwalt, Schlussanträge vom 16.3.2016 – C-484/14, BeckRS 2016, 80483 Rn. 139.
[30] *Mantz/Sassenberg*, NJW 2014, 3537 (3542); dies verkennen *Franz/Sakowski*, CR 2016, 524 (530).
[31] Eine Sicherung ohne Identitätsoffenbarung sieht der EuGH offenbar nicht als abschreckend an, vgl. *Husovec*, Holey Cap! CJEU Drills (Yet) Another Hole in the E-Commerce Directive's Safe Harbors, 10, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2843816.
[32] EuGH, EuZW 2016, 821 Rn. 96 – McFadden.
[33] EuGH-Generalanwalt, Schlussanträge vom 16.3.2016 – C-484/14, BeckRS 2016, 80483 Rn. 142.
[34] *Caspar*, ZRP 2015, 233 (235 f.).
[35] Zu Anonymisierungslösungen eingehend *Scheder-Bieschin*, Modernes Filesharing, 2014, 71 ff.

Darüber hinaus übersieht der EuGH, dass die Offenbarung der Identität des Nutzers eine Verfolgbarkeit – und damit die angebliche Abschreckung – nur erreichen kann, wenn der Anbieter gleichzeitig das gesamte Verhalten seiner Nutzer überwacht und speichert.[36] Ohne Überwachung können innerhalb eines WLAN rechtsverletzende Handlungen nämlich nicht auf einen Nutzer zurückgeführt werden. Die Überwachung ist aber wiederum nach Art. 15 ECRL ausgeschlossen, zudem dürfte die Speicherung des Datenverkehrs grund- und datenschutzrechtlich unzulässig sein. Der EuGH-Generalanwalt hat sie daher zu Recht als unverhältnismäßig abgelehnt.[37]
Weiter ist bedenklich, dass der EuGH Fragen des Datenschutzes und deren Einfluss auf die Abwägung überhaupt nicht beachtet hat.[38] ErwGr 14 ECRL verweist ausdrücklich auf das Verhältnis zur Datenschutzrichtlinie 95/46/EG und statuiert, dass die anonyme Nutzung des Internet durch die ECRL nicht unterbunden werde. Ebenso verweist ErwGr 9 der E-Privacy-Richtlinie 2002/58/EG den Anbieter nach Möglichkeit auf die Verwendung anonymer oder pseudonymer Daten. Diese Vorgaben entsprechen zudem der nationalen Regelung in § 13 Abs. 6 TMG.[39] Es hätte angesichts der Erwägungsgründe daher für den EuGH sogar nahe gelegen, datenschutzrechtliche Grundsätze in die Abwägung einzubeziehen. Dies gilt insbesondere auch mit Blick auf die Entscheidung des EuGH, die europäische Richtlinie zur Vorratsdatenspeicherung für ungültig zu erklären,[40] was der vorliegenden Entscheidung klar entgegen zu stehen scheint.
Grundsätzlich kann der WLAN-Betreiber nach § 95 TKG Bestandsdaten, also z.B. Namen und Anschrift, erheben, soweit dies für das Vertragsverhältnis erforderlich ist.[41] Auch unentgeltliche Gefälligkeitsverträge – wie wohl beim WLAN zu Werbezwecken – können hierunter fallen. An die Erforderlichkeit sind auch grundsätzlich keine hohen Anforderungen zu stellen, so dass es ausreicht, wenn die Daten dem Vertragszweck förderlich sind. Es ist jedoch fraglich, ob die Erhebung allein zum Zwecke der „Abschreckung von Rechtsverletzungen" dem Verhältnis zum Betreiber förderlich ist, da dieser ja den transportierten Daten gerade neutral gegenübersteht und aufgrund der sein Angebot erheblich einschränkenden Zugangshürden und der erforderlichen Infrastruktur möglicherweise gerne auf die Datenerhebung verzichten würde.[42] Zudem würde es dem vom EuGH postulierten Abschreckungseffekt genügen, wenn der Betreiber beim Erheben der Daten lediglich behauptet, diese auch speichern zu wollen, die Daten aber unverzüglich wieder löscht. Überhaupt ist unklar, ob der Betreiber zur Speicherung über den Nutzungsvorgang hinaus verpflichtet sein soll und ggf. wie lange, was auch die Möglichkeit einer späteren Herausgabe dieser Daten nach § 101 UrhG eröffnen würde.

Aus all diesen Gründen war eine Identifizierungspflicht bisher zu Recht abgelehnt worden.[43]

Unklar bleibt auch die praktische Durchführung der „Offenlegung der Identität". Reicht es z.B. aus, wenn der Betreiber über eine Anmeldemaske Namen und E-Mail-Adresse abfragt? Muss der

---

[36] Ebenso EuGH-Generalanwalt, Schlussanträge vom 16.3.2016 – C-484/14, BeckRS 2016, 80483 Rn. 141.
[37] EuGH-Generalanwalt, Schlussanträge vom 16.3.2016 – C-484/14, BeckRS 2016, 80483 Rn. 142, 146.
[38] Ebenso *Husovec*, (o. Fn. 31), 12.
[39] Dazu *Caspar*, ZRP 2015, 233; allerdings findet § 13 Abs. 6 TMG auf Access Provider keine unmittelbare Anwendung, BR-Drs. 556/06, S. 22.
[40] EuGH, EuZW 2014, 459 – Digital Rights Ireland.
[41] Eingehend zu den Anforderungen *Sassenberg/Mantz*, (o. Fn. 8), Rn. 128.
[42] Vgl. auch *Scheder-Bieschin*, (o. Fn. 30), 211.
[43] OLG Hamburg, MMR 2009, 631 – Usenet I; LG München I, CR 2012, 605; *Breyer*, MMR 2010, 55; *Mantz*, Rechtsfragen offener Netze, 2008, 262; *Hornung*, CR 2007, 88 (91).

Personalausweis kontrolliert und ggf. kopiert werden?[44] Kann eine Identifizierung über die Mobilfunknummer erfolgen? Ist die Identität „offenbart" bzw. der nötige Abschreckungseffekt erreicht, wenn das WLAN-Passwort nur den Kunden eines Cafés mitgeteilt wird, ohne dass die Nennung eines Namens oder die Vorlage von Ausweisdokumenten verlangt werden, weil der Nutzer als Kunde der optischen Kontrolle durch den Kellner unterliegt?[45]
Teilweise sind die hier mit Fragezeichen zu versehenden Vorgaben auch schlicht nicht erfüllbar. Man stelle sich die Nutzung des WLAN im Zug vor. Bevor die Nutzung beginnen kann, müsste der potentielle Nutzer auf den Schaffner warten und dieser müsste nach Identifizierung des Passagiers den Zugang freischalten oder das Passwort herausgeben.
Bereits diese Fragen verdeutlichen, dass der EuGH dem WLAN-Betreiber unüberbrückbare praktische Hürden in den Weg legt, um einen nicht belegten Abschreckungseffekt herbeizuführen. Wie hierbei die Förderung der Verbreitung von öffetnlichen WLANs erreicht werden soll, bleibt ebenfalls offen.

c. Websperren

Nicht geklärt ist übrigens auch, ob dem WLAN-Betreiber Websperren auferlegt werden können.[46] Der EuGH hat Websperren bei „klassischen" Access Providern bisher als Ergebnis einer Einzelfallabwägung grundsätzlich für zulässig erklärt.[47] Ob dies auch für WLANs gilt, hat das Gericht nicht explizit geprüft. Im Rahmen der Abwägung betont der EuGH jedoch, dass das Recht auf Informationsfreiheit nicht beeinträchtigt sei, weil die Sicherung des WLAN keine Sperrung der Webseite bewirke.[48] Websperren können sich daher bei WLANs durchaus als unzumutbar erweisen.[49] Dies gilt insbesondere im Hinblick darauf, dass Websperren bei einzelnen WLANs praktisch sogar noch unwirksamer sein dürften als bei „klassischen" Access Providern.

3. Ansprüche außerhalb des Urheberrechts

Das Urteil des EuGH verfestigt darüber hinaus eine Divergenz des Rechtsschutzes. Der WLAN-Betreiber, der das WLAN nicht entsprechend den – unklaren – Vorgaben des EuGH sichert, läuft Gefahr, bei Urheberrechtsverletzungen seiner Nutzer auf Unterlassung in Anspruch genommen zu werden. Anders ist dies jedoch bei allen Rechtsgebieten, die nicht unter Art. 8 Abs. 3 der InfoSoc-Richtlinie fallen,[50] insbesondere also Persönlichkeits- oder Wettbewerbsrechtsverletzungen.[51] Gegenüber solchen Rechtsverletzungen ist der Betreiber wohl ohne Weiteres privilegiert.

IV. Folgen für private Anbieter von WLANs

Offen bleibt nach dem Urteil des EuGH auch, wie die Haftungssituation bei rein privaten Anbietern von WLANs ist. Da diese nicht unter die Vorgaben der ECRL fallen, greift die insoweit überschießende nationale Regelung in § 8 TMG, die erst im Sommer 2016 novelliert wurde. Der Gesetzgeber hat insoweit ausdrücklich beabsichtigt, die Privilegierung auch auf

---

[44] Dazu *Sassenberg/Mantz*, (o. Fn. 8), Rn. 128.
[45] Vgl. kritisch zur Durchführung der Identifizierung auch Scheder-Bieschin, Modernes Filesharing: Störerhaftung und Auskunftspflicht von Anonymisierungsdiensten, 2014, 212 f.
[46] Zu Websperren bei „klassischen" Access Providern BGH, GRUR 2016, 268 – Störerhaftung des Access Providers II; krit. dazu *Heidrich/Heymann*, MMR 2016, 370.
[47] S. nur EuGH, GRUR 2014, 468 – UPC Telekabel/Constantin Film; dem folgend BGH, GRUR 2016, 268 – Störerhaftung des Access Providers II.
[48] EuGH, EuZW 2016, 821 Rn. 94 – McFadden.
[49] Ebenso *Husovec*, (o. Fn. 31), 10; vgl. auch *Sesing*, MMR 2016, 507 (511); *Sassenberg/Mantz*, (o. Fn. 8), Rn. 231 ff.
[50] Die Norm erwähnt der EuGH in seiner Entscheidung interessanterweise überhaupt nicht.
[51] *Spindler*, GRUR 2016, 451 (460).

Unterlassungsansprüche auszuweiten. Dies ergibt sich jedoch allein aus der Gesetzesbegründung.[52] Dem Wortlaut von § 8 Abs. 3 TMG ist diese Auffassung, anders als noch im gestrichenen § 8 Abs. 4 des TMG-Entwurfs nicht zu entnehmen.[53] Es ist daher abzuwarten, ob die Absichtserklärung Wirkung entfalten wird.[54] Es verbleibt dementsprechend auch hier immer noch Rechtsunsicherheit.
Nimmt man den von der Bundesregierung immer wieder geäußerten Willen ernst, Rechtssicherheit bei WLANs herzustellen, und sollen die Verlautbarungen der EU-Kommission zur Förderung von öffentlichen WLANs nicht nur leere Worte bleiben, kann man nur hoffen, dass unter dem Eindruck des EuGH-Urteils ein neuer Anlauf einer gesetzlichen Regelung unternommen wird, entweder auf nationaler oder auf europäischer Ebene. Gerade bei Privaten könnte der nationale Gesetzgeber eine Abwägungsentscheidung treffen, an der sich die Gerichte orientieren können (vgl. Rn 70).[55] Fraglich ist jedoch bereits, ob der nationale Gesetzgeber Unterlassungsansprüche überhaupt vollständig ausschließen kann.[56] Allerdings wäre es durchaus möglich, z.B. den Anspruch auf Ersatz von Abmahnkosten gegenüber dem WLAN-Anbieter auszuschließen, ähnlich wie bei der Begrenzung nach § 97a Abs. 3 S. 2 UrhG. Dies würde die privaten Anbieter von WLANs teilweise schützen, die bisher primär Adressat von urheberrechtlichen Abmahnungen waren.

V. Fazit

Das Urteil des EuGH ist in vielerlei Hinsicht unbefriedigend. Gerade bei der Durchführung von wichtigen grundrechtlichen Abwägungsentscheidungen wäre es hilfreich, wenn das Gericht zunächst eine solide Tatsachengrundlage schaffen würde. Das McFadden-Urteil entbehrt dieser Grundlage und ruft im Ergebnis mehr Probleme hervor als es löst. Nicht nur sind die Voraussetzungen und Folgen der Sicherung des WLANs mit einer Identifizierungspflicht völlig offen, vielmehr werden die Diskussionen darum weitergehen, ob andere Sicherungsmaßnahmen nach den Vorgaben des EuGH hinreichend sind oder nicht.
Folge des Urteils könnte – neben der Behinderung öffentlicher WLANs – sein, dass die Anbieter von WLANs den Datenverkehr erneut über VPN-Lösungen ins (ggf. außereuropäische) Ausland leiten, um so wenigstens faktisch Rechtssicherheit herzustellen.

***

[52] BT-Drs. 18/8645, S. 10.
[53] BT-Drs. 18/6745.
[54] Kritisch auch *Sesing*, MMR 2016, 507 (509 f.); *Franz/Sakowski*, CR 2016, 524 (527).
[55] Vgl. EuGH, EuZW 2016, 821 Rn. 70 – McFadden.
[56] *Spindler*, NJW 2016, 2449 (2452 f.).