Rechtsanwälte
LEHNER DÄNEKAMP & MAYER
Düsseldorf • Heidelberg

RECHTSGUTACHTERLICHE STELLUNGNAHME

An Stadt Heidelberg, Herrn Alexander Krohn *(Referat des Oberbürgermeisters, Bereichsleiter digitale Zukunft)*

Von RA Frank Joachim Mayer

Datum 6. September 2016

Unser Zeichen: 023D/16

Betreff: Rechtsgutachterliche Stellungnahme zu Fragen der Zulässigkeit einer Kooperation der Stadt Heidelberg mit dem Freifunk Rhein-Neckar e.V. im Hinblick auf die Bereitstellung öffentlich genutzter WLAN-Netze

hier: Konformität nach dem Telekommunikationsgesetz *(TKG)* und Telemediengesetz *(TMG)*, Störerhaftung

Inhaltsverzeichnis

A. Sachverhalt

Dem zu prüfenden Sachverhalt liegt die Anfrage des Vereins Freifunk Rhein-Neckar e.V. *(nachfolgend „Freifunk“)* zugrunde, ob auf Seiten der Stadt Heidelberg die Bereitschaft besteht, eine Mitnutzung der öffentlichen Infrastruktur zuzulassen, um die Stadt mit sogenanntem Freifunk versorgen zu können.

Freifunk ist eine nicht-kommerzielle Initiative für freie Funknetzwerke, die aus altruistischen Gründen öffentliche, entgeltfreie WLAN-Hotspots betreibt.

Dem Angebot liegt dabei das Konzept zugrunde, dass jeder *„Teilnehmer“* über einen eigenen, überall im Handel erhältlichen WLAN-Router einen sogenannten Freifunkknoten installiert, auf den die Freifunkfirmware installiert wird. Der jeweilige Teilnehmer *(Betreiber)* behält dabei die volle Kontrolle über den von ihm bereitgestellten Freifunkknoten. Der durch eine Firmware vorkonfigurierte Freifunkknoten *(WLAN-Hotspot)* ermöglicht es jedem beliebigen Nutzer, sich

über sein Smartphone, Laptop, Tablet usw. in das offene WLAN-Netz ohne Registrierung einwählen zu können.

Die Freifunkknoten wiederum sind untereinander über eine MeshLink-Verbindung verbunden und bilden damit ein öffentliches WLAN-Netzwerk. Die auf dem Freifunkknoten installierte Firmware baut dabei eine verschlüsselte VPN-Verbindung *(Virtual Private Network)* zu den Gateway-Servern der Freifunk auf, die sich in diversen deutschen Rechenzentren befinden. Hierdurch erfolgt die Trennung zwischen dem privaten Netz des Teilnehmers und dem öffentlichen Netz der Freifunk.

Sobald sich ein Nutzer mit dem Freifunk WLAN verbindet, erhält er von dem Freifunk-Gateway-Server eine IP-Adresse. Damit kann der jeweilige Nutzer über das Freifunk-Gateway auf das Internet zugreifen. Erst auf dem Freifunk-Gateway erfolgt die Einwahl in das Internet. Aufgrund dieser Netz-Architektur ist stets der Verein Freifunk Absender der Daten. Hierbei wird keinerlei Information über die Einwahlverbindungen der jeweiligen Nutzer gespeichert. Auch können einzelne Datenströme nicht einem bestimmten Freifunkknoten zugeordnet werden. Eine Identifikation des jeweiligen Nutzers erfolgt somit nicht. Im Rahmen dieser anonymen Nutzung des offenen WLANs werden somit weder Bestands- noch Verkehrsdaten des jeweiligen Nutzers erhoben oder gespeichert.

Aufgrund der zuvor beschriebenen Netzwerk-Architektur möchte die Freifunk nunmehr die existierende Infrastruktur der Stadt Heidelberg zur Erweiterung des WLAN-Netzes mitnutzen. Dabei soll die Stadt Heidelberg zum einen in öffentlichen Gebäuden den Zugang zum Internet über bestehende Anschlüsse/Leitungen ermöglichen, an die ein WLAN-Router angeschlossen wird. Zusätzlich benötigen die WLAN-Router an diesen Standorten den Anschluss an das Stromnetz über eine Steckdose. Aufgrund der Mesh-Technologie reicht an einzelnen Standorten auch nur ein Stromanschluss aus, da dieses Gerät sodann die nächstgelegenen internetangebundenen WLAN-Router *„sucht“*. Zum anderen besteht Interesse, Gebäude der Stadt Heidelberg als Standort für WLAN-Richtfunk zu nutzen, um weit auseinanderliegende Punkte über das Netzwerk verbinden zu können. An den insoweit genutzten Standorten bedarf es auch keines Internetzuganges, sondern nur eines Stromanschlusses.

B. Prüfungsauftrag

Die Stadt Heidelberg hat uns im Zusammenhang mit dem zuvor unter A. dargelegten Sachverhalt um eine rechtsgutachterliche Stellungnahme zu Fragen der Zulässigkeit einer Kooperation mit der Freifunk Rhein-Neckar e.V. im Hinblick auf die Bereitstellung öffentlich genutzter WLAN-Netze gebeten. Aus Sicht der Stadt Heidelberg stellt sich dabei die Frage, ob es sich bei dem Freifunk um ein rechtlich zulässiges, insbesondere TKG/TMG-konformes, Konzept handelt, sodass die angestrebte Kooperation keine Angriffsfläche bietet.

Im Rahmen der nachfolgenden rechtsgutachterlichen Stellungnahme sollen daher nachfolgende Fragen geklärt werden:

- Allgemeine Zulässigkeit des Konzeptes Freifunk/Politische Einordnung;
- Haftungsrisiko der Freifunk als Betreiber eines offenen WLANs als sogenannter Störer bzw. (Mit-)Störerhaftung der Stadt Heidelberg aufgrund der Bereitstellung öffentlicher Infrastruktur wegen von Nutzern begangener Rechtsverletzungen *(z.B. Urheberrechtsverletzung)*;
- Anbieterpflichten der Freifunk/Stadt Heidelberg nach dem Telekommunikationsgesetz *(TKG).*

C. Prüfungsergebnis

I. Allgemeine Zulässigkeit des Freifunk Konzeptes/Politische Einordnung

Das von der Freifunk Rhein-Neckar e.V. verfolgte Freifunk Konzept ist allgemein zulässig und obendrein politisch erwünscht.

Die Koalitionsfraktion von CDU, CSU und der SPD hatten sich bereits im Koalitionsvertrag der 18. Legislaturperiode *„Deutschlands Zukunft gestalten“* darauf verständigt, in deutschen Städten die Voraussetzungen für mehr WLAN-Angebote zu schaffen. Ziel soll-

te hiernach sein, das mobile Internet über WLAN-Hotspots für jeden verfügbar zu machen.

Zu diesem Zwecke brachte die Bundesregierung am 18.11.2015 einen Gesetzesentwurf zur Änderung des Telemediengesetzes in den Bundestag ein *(Drucksache 18/6745 vom 18.11.2015)*. Nach der Gesetzesbegründung war es die ausdrückliche Zielsetzung des Gesetzentwurfes, den Betreibern offener WLANs die nötige Rechtssicherheit insbesondere vor urheberrechtlichen Abmahnungen von Rechteinhabern zu verschaffen und damit das aufgrund der unklaren Rechtslage bestehende Haftungsrisiko aus der sogenannten Störerhaftung zu beseitigen *(dazu, und ob dies aufgrund der Gesetzesänderung tatsächlich gelungen ist, nachstehend unter C. II. WLAN-Störerhaftung)*.

Auch die anonyme Nutzung offener WLAN-Netze ohne vorherige Identifikation der Nutzer ist vom europäischen und nationalen Gesetzgeber gerade gewollt. So heißt es bereits in dem Erwägungsgrund 14 der unionsrechtlichen Richtlinie 2000/31/EG vom 08.06.2000 *(E-Commerce-Richtlinie-ECRL)* ausdrücklich: *„die anonyme Nutzung offener Netze wie des Internets kann diese Richtlinie nicht unterbinden."* Auch § 13 Abs. 6 Telemediengesetz *(TMG)* sieht vor, dass der Diensteanbieter die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen hat, soweit dies technisch möglich ist.

Allerdings ist zu beachten, dass der Anbieter eines offenen WLANs – jedenfalls bislang – Haftungsrisiken durch eine unklare Rechtslage im Zusammenhang mit der sogenannten Störerhaftung ausgesetzt ist, wenn Nutzer Rechtsverletzungen *(z.B. Urheberrechtsverletzungen)* über das offene WLAN begehen. Diese Rechtsunsicherheit sollte eigentlich durch die am 27.07.2016 in Kraft getretene Änderung des Telemediengesetzes *(TMG)* beseitigt werden, was dem Gesetzgeber allerdings missglückt ist *(dazu nachstehend unter C. II, 4. und 5.)*. Mit dem jüngst geänderten Telemediengesetz ist aber immerhin klargestellt, dass nun alle Anbieter offener WLANs unter die Anwendbarkeit des Telemediengesetzes fallen und damit haftungsprivilegiert sind, jedenfalls was Schadensersatz und die strafrechtliche Verantwortlichkeit angeht. Ferner ist zu beachten, dass jeder Anbieter von

offenen WLANs als Diensteanbieter im Sinne des Telekommunikationsgesetzes *(TKG)* anzusehen ist und hiernach bestimmten Anbieterpflichten nach dem TKG unterliegt *(Regelungen zum Fernmeldegeheimnis nach §§ 88 ff. TKG, zum telekommunikationsrechtlichen Datenschutz nach §§ 91 ff. TKG sowie einen Teil der Regelungen zur öffentlichen Sicherheit nach §§ 108 ff. TKG – dazu nachfolgend unter C. III.).*

Im Zusammenhang mit unseren nachfolgenden Ausführungen ist ebenfalls zu beachten, dass wir im Rahmen unserer rechtlichen Beurteilung keinen Unterschied vornehmen werden zwischen der Freifunk als dem unmittelbaren Betreiber des offenen WLAN und der Stadt Heidelberg, die gegebenenfalls *„nur“* daran mitwirkt. Denn die Stadt Heidelberg kommt zum einen nach den vom Bundesgerichtshof aufgestellten Kriterien der Störerhaftung gegebenenfalls als *„Mitstörer“* in Betracht. Zum anderen kann bereits derjenige als Diensteanbieter nach dem TKG gelten, der ganz oder teilweise an der Erbringung von Telekommunikationsdiensten *„mitwirkt“ (§ 3 Nr. 6 lit. b) TKG)*, sodass die nachfolgend unter C. III. aufgeführten Anbieterpflichten bereits den *„Mitwirkenden“* treffen können.

Im Hinblick auf diesen – vorweggenommenen – Befund wird daher vorgeschlagen, dass im Falle einer Bejahung der Kooperation zwischen der Stadt Heidelberg und Freifunk ein Kooperationsvertrag abgeschlossen wird, der zum einen eine Freistellung der Statdt Heidelberg von Haftungsrisiken aus der Störerhaftung vorsieht und andererseits regelt, dass die Anbieterpflichten nach dem TKG im Verhältnis der Parteien untereinander die Freifunk zu erfüllen hat.

II. WLAN-Störerhaftung

1. Vorbemerkung

Mit der immer weiter fortschreitenden Digitalisierung ist auch das Bedürfnis nach einem öffentlichen Zugang zum Internet unter Nutzung drahtloser lokaler Netzwerke *(Wireless Local Area Network-WLAN)* gestiegen. Der Verbreitung von breitbandigen Internetzugängen und speziell von öffentlichen WLANs und deren

Verfügbarkeit soll nach den Verlautbarungen der Bundesregierung höchste Priorität zukommen *(Koalitionsvertrag 2013 zwischen CDU, CSU und SPD, Seite 35)*. Die Anzahl der öffentlichen WLAN-Hotspots nimmt jedoch nur schleppend zu und Deutschland hinkt bei der Verbreitung von öffentlichem WLAN im internationalen Vergleich deutlich hinterher. Gerade einmal rund 15.000 freie, öffentliche WLAN-Hotspots stehen in Deutschland zur Verfügung, das entspricht einer Quote von rund 1,9 Hotspots pro 10.000 Einwohner. Südkorea weist beispielweise eine Quote von über 37 WLAN-Hotspots pro 10.000 Einwohner auf *(Eco Microresearch, November 2014, Stand 21.04.2015).* Als Ursache hierfür wird neben den regulatorischen Anforderungen seit Langem die bestehende Rechtsunsicherheit der Betreiber öffentlicher WLANs identifiziert, von Rechteinhabern als Störer wegen der über den Internetzugang durch die Nutzer begangenen Verletzung urheberrechtlich geschützter Werke in Anspruch genommen zu werden *(so genannte urheberrechtliche WLAN-Störerhaftung im Zusammenhang mit dem kostenfreien Herunterladen urheberrechtlich geschützter Werke durch die Zugangsnutzer)*. Dies veranlasste die große Koalition schon bei den Koalitionsverhandlungen dazu, die Notwendigkeit einer Regelung festzuschreiben *(ebd.)*. Inzwischen ist am 27.07.2016 das zweite Gesetz zur Änderung des Telemediengesetzes in Kraft getreten *(BGBl. Teil I Nr. 36 vom 26.07.2016)*. Die Regierungskoalition feiert die Gesetzesänderung als Durchbruch, der endlich den Weg für offenes WLAN in Deutschland freimacht und ruft die Kommunen und Landkreise dazu auf, WLAN-Netze einzurichten und anzubieten *(Plenarprotokoll 18/173 der 173. Sitzung des Deutschen Bundestages vom 02.06.2016 betreffend die Lesung (Aussprache) zum zweiten Gesetz zur Änderung des Telemediengesetzes – Störerhaftung)*. Die Opposition *(ebd.)*, weite Teile der öffentlichen Berichterstattung und zwischenzeitlich veröffentlichte einschlägige Meinungen in der juristischen Literatur hingegen halten die Gesetzesänderung für verfehlt. Das eigentliche Ziel, die Störerhaftung für öffentliche WLAN-Anbieter auszuschließen, sei in das Gesetz nicht hineingeschrieben bzw. wieder gestrichen worden. Die im Gesetz allein vorgenommene – und nun gültige - Klarstellung, dass auch Anbieter offener WLANs als Access-Provider *(Zugangsanbieter)* im Sinne des § 8 TMG gelten, bewirke keinerlei Änderung am Status quo. Die Gesetzesän-

derung sei damit nicht geeignet, die Rechtsunsicherheit im Zusammenhang mit der WLAN-Störerhaftung wirklich zu beseitigen.

Trotz der jüngsten Gesetzesänderung zum TMG ist die Frage der Störerhaftung in der Tat weiterhin nicht geklärt. Es gilt daher, nachfolgend den derzeitigen – kontroversen - Diskussionsstand rund um die Frage der Sörerhaftung in der deutschen Rechtsprechung des BGH und der europäischen Rechtsprechung des Europäischen Gerichtshofes *(EuGH)* zu skizieren.

2. Entwicklung und aktueller Stand der WLAN-Störerhaftung in der deutschen Rechtsprechung

2.1 Ausgangslage

Nach § 8 Absatz 1 und 2 Telemediengesetzes *(TMG)* genießen Access-Provider *(Zugangsanbieter)* ein Haftungsprivileg. Hiernach haften Access-Provider in Umsetzung der E-Commerce-Richtlinie *(ECRL)* 2000/31/EG als Anbieter von Diensten der reinen Durchleitung nicht, wenn Dritte *(Nutzer)* über den Netzzugang Rechtsverletzungen *(z.B. Urheberrechtsverletzungen)* begehen; auch können Ihnen keine proaktiven Überwachungspflichten auferlegt werden. Die Verantwortlichkeit des Access-Providers ist damit nach der Privilegierung in § 8 TMG ausgeschlossen, sofern er – verkürzt – bis auf seine neutrale Vermittlerposition durch den Transport von Daten des Nutzers an der Rechtsverletzung des Nutzers nicht mitgewirkt hat *(Mantz/Sassenberg, NJW 2014, S. 3537 ff.)*.

Höchstrichterlich nicht geklärt und damit umstritten war allerdings bis zu einer Leitentscheidung des BGH vom 26.11.2015 (*BGH, Urteil vom 26.11.2015 – I ZR 174/14, in CR 2016, S. 408 ff.)* die Frage, ob das für Access-Provider geltende Haftungsprivileg des § 8 TMG „*nur*“ die strafrechtliche Verantwortlichkeit sowie Schadensersatzansprüche betrifft oder aber

auch den Fall der sogenannten verschuldensunabhängigen Störerhaftung erfasst. Konkret geht es bei der auf Unterlassung, nicht aber auf Schadensersatz gerichteten Störerhaftung um die Frage, ob der Rechteinhaber den Access-Provider verschuldensunabhängig als *„Störer“* auf Unterlassung in Anspruch nehmen – also abmahnen – kann, wenn der Nutzer über den Netzzugang Rechtsverletzungen *(z.B. Urheberrechtsverletzungen)* begeht. Haftpflichtiger Störer kann nach der hierzu ergangenen Rechtsprechung jeder sein, der – ohne Täter oder Teilnehmer zu sein - in irgendeiner Weise willentlich und adäquat-kausal zur Verletzung eines geschützten Rechtsguts beiträgt, sofern er zumutbare Prüfpflichten verletzt hat *(BGH, Urt. V. 18.10.2001 – I ZR 22/99, GRUR 2002, 618, 619 = WRP 2002, 532 – Meißner Dekor I; BGH, Urt. V. 30.4.2008 – I ZR 73/05, GRUR 2008, 702 Tz. 50 = WRP 2008, 1104 = CR 2008, 579 – Internet-Versteigerung III).*

Nach der bislang hierzu ergangenen Rechtsprechung des BGH schloss das Haftungsprivileg des TMG nicht die *(urheberrechtliche)* Störerhaftung aus, sodass ein Anbieter trotz der Haftungsprivilegierung in § 8 TMG weiterhin als Störer urheberrechtlichen Unterlassungsansprüchen ausgesetzt blieb. Der BGH leitete dies aus der Vorschrift des § 7 Abs. 2 Satz 2 TMG ab, wonach Verpflichtungen nach den allgemeinen Gesetzen unberührt bleiben. Entschieden hatte dies der BGH bis zu der jüngst ergangenen Leitentscheidung aber nur im Zusammenhang mit den sogenannten Host-Providern nach § 10 TMG, die Informationen für Nutzer speichern *(BGHZ 158, 343 = NJW 2004, 2158 – Schöner Wetten; BGHZ 158, 236 = NJW 2004, 3102 – Internet-Versteigerung I).*

2.2. Netzsperren-Entscheidung des BGH vom 26.11.2015

In gleich zwei Urteilen hat der BGH nun am 26.11.2015 entschieden, dass auch Access-Provider, die ihren Kunden den Zugang zum Internet bereitstellen und dabei lediglich einen Datenstrom vermitteln, grundsätzlich von Rechteinhabern als Störer trotz des Haftungsprivilegs in § 8 TMG in An-

spruch genommen werden können (*BGH, Urteil vom 26.11.2015 – I ZR 174/14, in CR 2016, S. 408 ff., MMR 2016, S. 180 mit Anm. Finger, ferner Parallelentscheidung BGH, Urteil vom 26.11.2015 – I ZR 3/14*; vgl. *zum bisherigen Meinungsstand Mantz/Sassenberg, NJW 2014, 3537, zur Entwicklung der Störerhaftung Köhler, GRUR 2008, 1 (2) m.w.N.).*

Nach den Urteilen des BGH steht den Rechteinhabern dabei ein Anspruch gegen den Access-Provider dahingehend zu, von diesem die Sperrung des Zugangs zu bestimmten Webseiten, auf denen urheberrechtlich geschützte Werke rechtswidrig veröffentlicht werden, zu verlangen. Im ersten der beiden Verfahren klagte die Verwertungsgesellschaft GEMA gegen die Deutsche Telekom, im zweiten die Musiklabels Warner Universal Sony gemeinsam gegen Telefonica. Gegenstand der Streitigkeiten waren jeweils Webseiten mit Linksammlungen, über die sich urheberrechtlich geschützte Werke kostenfrei herunterladen ließen.

Ein Vorgehen des Rechteinhabers gegen den Access-Provider im Wege der urheberrechtlichen Störerhaftung kommt nach dem BGH aber nur dann in Betracht, wenn eine vorangegangene Inanspruchnahme des die Webseite tatsächlich betreibenden Content-Providers und des den virtuellen Speicherplatz zur Verfügung stellenden Hosting-Providers gescheitert ist oder von vornherein keine Erfolgsaussichten bestünden. Damit ist die Hürde, als Access-Provider für urheberrechtliche Rechtsverstöße der Nutzer in Anspruch genommen zu werden, vom BGH recht hoch angesetzt worden.

Liegen diese Voraussetzungen allerdings vor, kann der Access-Provider zu weitergehenden Maßnahmen verpflichtet werden, um dem Begehren des Rechteinhabers zu entsprechen.

a) Blockaden: Insofern stellte der BGH zunächst abschließend klar, dass die Anwendung von DNS-IP-Adress- und URL-Blockaden keinen

Eingriff in das Telekommunikationsgeheimnis darstellen und für den Access-Provider somit rechtlich zumutbar sind.

b) Effektivität: Ferner wies der BGH darauf hin, dass es auf die Effektivität der konkreten Sperrmaßnahmen nicht ankomme, solange durch die Sperrung der Zugriff auf die rechtverletzenden Inhalte verhindert oder zumindest erschwert werde.

Die Rechtsprechung des BGH ist auch im Lichte der zuvor bereits ergangenen EuGH-Entscheidung *„UPC/Constantin“* zu sehen, die ebenfalls bereits die Auferlegung von Sperrpflichten gegenüber Access-Providern für zulässig erachtet hat *(EuGH v. 27.03.2014 – Rs. C-314/12, MMR 2014, 397 m. Anm. Roth-UPC/Constantin-kino.to).*

2.3. Übertragbarkeit der Netzsperren-Entscheidung des BGH auf Anbieter offener WLANs/Zumutbarkeit von Schutzmaßnahmen

Fraglich ist allerdings, ob diese sogenannte Netzsperren-Entscheidung des BGH auf WLAN-Betreiber – als Access-Provider - übertragbar ist und somit überhaupt ein – wenn auch bereits erheblich reduziertes - Haftungsrisiko für diese begründet (*Finger, in: MMR 2016, S. 511).* Denn ob anlassbezogene Maßnahmen für Betreiber offener Funknetze in Betracht kommen, ohne das erwünschte Ergebnis frei zugänglicher Netze in Frage zu stellen, ist bislang ungeklärt.

Knackpunkt dabei ist, dass Freifunk dem Nutzer *„anonym“* eine IP-Adresse vergibt, deren Nutzung nicht konkret zurückverfolgt werden kann. Da im Wege des Unterlassungsanspruchs vom Schuldner aber nichts tatsächlich oder rechtlich unmögliches verlangt werden kann, und entsprechende Maßnahmen für WLAN-Betreiber derzeit nicht ersichtlich sind *(Spindler, GRUR 2016, 451, 459 f.)* ist bereits zweifelhaft, ob dem WLAN Betreiber überhaupt zumutbare Maßnahmen zur Verhinderung von Rechtsverstößen abverlangt

werden können *(Finger, a.a.O., S. 511, in diese Richtung auch OLG Köln, MMR 2014, S. 832, 824)*. Wenn aber überhaupt nicht irgendeine technische Maßnahme zur Verfügung steht, deren Einsatz zumutbar ist, steht die generelle Zumutbarkeit einer Erfolgsabwendungspflicht im Raum *(BGH GRUR 2011, 152 = MMR 2011, 172 mit Anm. Engels - Kinderhochstühle im Internet, BGH MMR 2014, 55 – Kinderhochstühle im Internet II)*.

Auch die im Jahre 2010 ergangene Entscheidung des BGH zur generellen anlasslosen Verschlüsselungspflicht eines WLAN-Betreibers für ein schlecht gesichertes WLAN, über welches dann Urheberrechtsverletzungen begangen werden *(BGHZ 185, 330 = NJW 2010, 2061 – Sommer unseres Lebens)*, hilft nicht weiter, da dieses Urteil ausschließlich ein rein privat genutztes WLAN zum Gegenstand hatte, wohingegen der *„gewerbliche“* Anbieter eines offenen WLANs unter die Diensteanbietereigenschaft des TMG fällt und bereits deshalb im Rahmen der dann vorzunehmenden Grundrechtsabwägung mit seinem *„Geschäftsmodell“* entsprechend geschützt ist.

Damit ist derzeit die Frage einer anlasslosen Verschlüsselungspflicht für Anbieter offener Funknetzwerke bzw. sonstiger zu treffender Schutzmaßnahmen *(Passwortvergabe etc.)* zur Vermeidung einer Inanspruchnahme als Störer in der höchstrichterlichen Rechtsprechung unbeantwortet. Tendenziell zeichnet sich aber aufgrund der bisherigen Rechtsprechung das Bild ab, dass im Spannungsfeld des Verbots allgemeiner Überwachungspflichten *(§ 7 Abs. 2 Satz 1 TMG)* einerseits und der Ausnahme von Verpflichtungen zur Entfernung oder Sperrung nach Bekanntwerden einer Rechtsverletzung andererseits *(§ 7 Abs. 2 Satz 2 TMG)* die Haftungsrisiken für Anbieter offener WLANs eingrenzbar erscheinen.

Dies gilt umso mehr, als nach dem bisherigen Meinungsstand in der Literatur und der Instanzrechtsprechung Schutzpflichten, die eine dauerhafte Überwachung des Verhaltens der Nutzer erfordern, überwiegend als unzu-

mutbar eingestuft werden, da sie massiv in die Rechte auch der Nutzer eingreifen, die sich völlig legal verhalten (zum Meinungsstand Mantz/Sassenberg, NJW 2014, S. 3537 f.). Eine Pflicht zur Registrierung wird überwiegend abgelehnt *(LG München IZD 2012, 281 mit Anmerkung Bertermann; Scheder-Bieschin, modernes Filesharing, 2014, S. 214; vgl. auch LG Frankfurt/Main, MMR 2004, 344, AG Hamburg, CR 2014, 536;)*. In Bezug auf eine Registrierungspflicht ist ohnehin zu berücksichtigen, dass diese ohne Überwachung des kompletten Datenverkehrs der Nutzer absolut wirkungslos ist, da ohne Überwachung die Zuordnung einer Rechtsverletzung zum Nutzer unmöglich ist *(Mantz/Sassenberg, NJW 2014, 3537, 3542; Spindler, GRUR 2014, 826, 831)*. Nach dem von Freifunk verfolgten Konzept erfolgt aber gerade keine Speicherung des Datenverkehrs der Nutzer. Auch die Pflicht, öffentliche WLANs mit einem *(Verschlüsselungs-)* Passwort zu sichern, wird hiernach als unzumutbar eingeschätzt. Die Verschlüsselung eines an die Öffentlichkeit gerichteten WLAN hat den zwangsläufigen Effekt, dass Nutzer aus dem WLAN ausgeschlossen oder jedenfalls durch eine weitere Hürde an der Nutzung gehindert werden. Immerhin rund 20% der Nutzer lassen sich nämlich von einer Registrierung vollständig von der Nutzung eines WLAN abhalten *(Befragung Kabel Deutschland, PM v. 06.03.2014, abrufbar unter https://www.kabeldeutschland.com/de/presse/pressemitteilung/produktnachrichten/632014.html.)*. Damit wäre das legale Geschäftsmodell des Anbieters in ganz erheblicher Weise beeinträchtigt.

Damit erscheint bereits nach derzeitiger Rechtslage zweifelhaft, ob einem Anbieter eines offenen WLANs überhaupt technische Maßnahmen zugemutet werden können, deren Unterlassung eine Störerhaftung begründen kann. Eine höchstrichterliche Entscheidung dazu steht in der deutschen Rechtsprechung noch aus.

3. Vorlageverfahren EuGH

Im Hinblick auf die zuvor aufgezeigten Rechtsunsicherheiten und die höchstrichterlich nicht geklärten Fragen der Haftung beim Betrieb eines offenen WLAN legte das Landgericht München I einen von ihm zu entscheidenden Fall mit Beschluss vom 18.09.2014 – 7 O 14719/12 dem EuGH zur Vorabentscheidung vor *(EuGH Rechtssache C-484/14)*.

Diesem Verfahren kommt grundlegende Bedeutung zu, weil der Generalanwalt beim Europäischen Gerichtshof in seinem Schlussantrag vom 16.03.2015 Leitlinien zur Auslegung der Bestimmungen des Artikels 12 der Richtlinie 2000/31/EG *(und damit des § 8 TMG)* zur Zumutbarkeit der Störerhaftung aufstellte, die von den zuvor vom BGH in seinen Leitentscheidungen vom 26.11.2015 aufgestellten Haftungsvoraussetzungen des Access-Providers grundlegend abwichen und unmittelbar Eingang in die Erwägungen des Gesetzgebers zu dem am 27.07.2016 in Kraft getretenen geänderten Telemediengesetzes fanden, obwohl der Schlussantrag für den EuGH selbst noch gar nicht bindend ist.

Gegenstand des Ausgangsfalls war, dass ein gewerblicher Anbieter eines offenen WLANs *(Verkäufer von Licht- und Tontechnik)* im Rahmen seines Gewerbes ein für jedermann zugängliches WLAN-Netz betrieb, welches Dritten *(Kunden)* den unentgeltlichen und nicht passwortgeschützten Zugang zum Internet ermöglichte. Über diesen Internetanschluss wurde am 04.09.2010 ein musikalisches Werk rechtswidrig zum Herunterladen angeboten, woraufhin der Rechteinhaber *(Sony Music)* den Anschlussinhaber *(Herrn Mc Fadden)* wegen dieser Rechtsverletzung abmahnte. Das Landgericht München I legte dem EuGH 9 Fragen zur Auslegung der sogenannten E-Commerce-Richtlinie 2000/31/EG vom 08.06.2000, ABl. L 178, S. 1 *(ECRL)* vor. Insbesondere solle geklärt werden, ob die in Artikel 12 Abs. 1 der Richtlinie 2000/31/EG *(und in deren Umsetzung § 8 TMG)* enthaltene Haftungsprivilegierung des Access-Providers nicht nur die strafrechtliche Verantwortlichkeit und die Verantwortlichkeit für Schadenssatzansprüche, sondern sämtliche

Ansprüche und damit auch die Ansprüche aus Störerhaftung *(Unterlassung, Zahlung der Abmahnkosten und Gerichtsgebühren)* ausschließe. Ferner solle geklärt werden, ob auch der Betreiber eines gewerblich betriebenen WLANs in Nebentätigkeit als Access-Provider im Sinne von Artikel 12 Abs. 1 der Richtlinie 2000/31/EG gilt und welche Maßnahmen dieser Betreiber im Falle des Bestehens einer Störerhaftung gegebenenfalls ergreifen müsse *(Stilllegen des Internetanschlusses, Vergabe von Passwörtern, Registrierung der Nutzer oder Analyse des Datenverkehrs, näher dazu Mantz/Sassenberg MMR 2015, S. 85 ff.)*. In seinem Schlussantrag vom 16.03.2016 stellte der Generalanwalt beim Europäischen Gerichtshof Leitlinien zur Auslegung der Bestimmungen des Artikels 12 der Richtlinie 2000/31/EG *(und damit des § 8 TMG)* auf, die für den EuGH allerdings noch nicht bindend sind.

Der Generalanwalt stellt hierbei zunächst fest, dass ein *(gewerblicher)* Anbieter eines entgeltfrei angebotenen offenen WLAN - auch ohne Vertragsbeziehung zum Nutzer - als Access-Provider unter die Haftungsprivilegierung des Artikel 12 Abs. 1 der Richtlinie 2000/31/EG *(und damit des § 8 TMG)* fällt. Weiterhin umfasse nach den Feststellungen des Generalanwalts die Haftungsprivilegierung des Access-Providers nach Artikel 12 Abs. 1 der Richtlinie 2000/31/EG *(und damit des § 8 TMG)* uneingeschränkt auch die verschuldensunabhängige Störerhaftung. Die Haftungsprivilegierung stehe daher nicht nur einer Verurteilung des Access-Providers zur Zahlung von Schadensersatz, sondern auch seiner Verurteilung zur Tragung der Abmahnkosten und der Gerichtskosten im Zusammenhang mit der von einem Dritten durch die Übermittlung von Informationen begangenen Rechtsverletzung entgegen. Damit könne der Anbieter von Diensten der reinen Durchleitung *(Access-Provider)* nach Artikel 12 Abs. 1 der Richtlinie 2000/31/EG nicht für eine durch die Übermittlung von Informationen begangenen Urheberrechtsverletzung verantwortlich gemacht und ihm daher auch nicht die außergerichtlichen oder die gerichtlichen Kosten im Zusammenhang mit einer solchen Rechtsverletzung auferlegt werden *(siehe. Rn. 76 ff. des Schlussantrages)*. Weiterhin formulierte der Generalanwalt in seinem Schlussantrag, dass die Haftungsprivilegierung zwar nicht

dem Erlass einer gerichtlichen Anordnung gegen einen Access-Provider auf einer entsprechenden gesetzlichen Grundlage entgegenstünde. Eine solche gerichtliche Anordnung darf jedoch – insoweit abweichend vom BGH - nicht die Haftung des Access-Providers für eine durch die reine Durchleitung von Informationen begangenen Rechtsverletzung beinhalten und keine allgemeinen Überwachungspflichten anordnen. Insbesondere sei nach Artikel 12 Abs. 3 der Richtlinie 2000/31/EG jede gerichtliche Anordnung gegen den Access-Provider unzulässig, wenn der Access-Provider dieser nur dadurch nachkommen könne, dass er den Internetzugang stilllegt, mit einem Passwortschutz oder einer Verschlüsselung sichert oder sämtliche über den Anschluss laufende Kommunikation auf Rechtsverletzungen hin untersucht *(ebd. Rn. 105 ff., 151)*.

Mit diesem Ansatz erteilte der Generalanwalt auch der immer wieder in der deutschen Rechtsprechung verfolgten Tendenz eine Absage, die Grundsätze der Haftung bei Host-Providern nach Artikel 14 der Richtlinie 2000/31/EG auf den Access-Provider entsprechend anzuwenden und diesen nach Kenntniserlangung eines Rechtsverstoßes in Haftung zu nehmen *(ebd. Rn. 99)*.

Damit nimmt der Generalanwalt im Ergebnis die bei der Bewertung von Prüfungs- und Überwachungspflichten im Rahmen der Störerhaftung vorzunehmende Grundrechtsabwägung vor, wonach ein zulässiges Geschäftsmodell durch Auferlegung präventiver Prüfungspflichten nicht gefährdet werden darf *(siehe hierzu auch BGHZ 158, 236, 251 f. – Internet-Versteigerung I)*.

Sollte der EuGH in dem noch nicht rechtskräftig entschiedenen Fall der Auffassung des Generalanwaltes folgen, würde die in Artikel 12 Abs. 1 der Richtlinie 2000/31/EG *(und in § 8 TMG)* enthaltene Haftungsprivilegierung den Anbieter eines offenen WLANs als Access-Provider erfassen und – entgegen dem BGH - von der Störerhaftung freistellen.

4. Zweites Gesetz zur Änderung des Telemediengesetzes *(TMG)*

Mit dem von der Bundesregierung am 18.11.2015 in den deutschen Bundestag eingebrachten Gesetzentwurf zur Änderung des Telemediengesetzes *(Drucksache 18/6745 vom 18.11.2015)* wurde die ausdrückliche Zielsetzung verfolgt, den Betreibern offener WLANs die nötige Rechtssicherheit insbesondere vor urheberrechtlichen Abmahnungen von Rechteinhabern zu verschaffen und damit das aufgrund der zuvor aufgezeigten unklaren Rechtslage bestehende Haftungsrisiko aus der sogenannten urheberrechtlichen Störerhaftung endgültig zu beseitigen.

Mit dem Gesetzesentwurf wurde zunächst durch die Neueinfügung eines § 8 Abs. 3 ausdrücklich eine Gleichstellung von Anbietern offener WLANs mit Zugangsvermittlern *(Access-Providern)* im Sinne des § 8 TMG vorgenommen und somit das Haftungsprivileg des § 8 Abs. 1 und 2 TMG ausdrücklich auf Anbieter offener WLANs erstreckt. Da die Haftungsprivilegierung des § 8 Abs. 1 und 2 TMG nach der zuvor bereits skizierten Rechtsprechung des BGH aber *„nur“* die strafrechtliche Verantwortlichkeit sowie Schadensersatzansprüche betrifft, sah der Regierungsentwurf ferner die Einfügung eines neuen § 8 Abs. 4 TMG vor, wonach WLAN-Anschlussinhaber ausdrücklich nicht als Störer haften sollten, wenn sie zumutbare Pflichten erfüllten, um Rechtsverletzungen zu verhindern. In den Nrn. 1 und 2 des neuen § 8 Abs. 4 TMG wurden Regelbeispiele für Sicherungsmaßnahmen angeführt, deren Erfüllung die Störerhaftung ausschließen sollte *(angemessene Sicherungsmaßnahmen gegen den unberechtigten Zugriff bzw. Einholung einer Nutzererklärung, keine Rechtsverletzung zu begehen)*.

Ausweislich der Gesetzesbegründung sollten unter diese neue Regelung weiterhin alle Anbieter eines offenen WLANs fallen, und zwar unabhängig davon, ob es sich um gewerbliche oder private Anbieter oder um eine öffentliche Einrichtung handelte *(Drs., ebd., S. 10 zu § 8 Abs. 4 TMG)*.

In der abschließenden Beratung des federführenden Ausschusses für Wirtschaft und Energie am 01.06.2016 einigten sich die Koalitionsfraktionen sodann auf einen geänderten Gesetzentwurf *(Drucksache 18/8645 zu dem Gesetzentwurf der Bundesregierung Drucksache 18/6745 vom 01.06.2016)*. Der Änderungsantrag sah die Streichung des zuvor eingefügten § 8 Abs. 4 des Regierungsentwurfs zur Störerhaftung vor. Zur Begründung wurde Bezug genommen auf den zwischenzeitlich gestellten Schlussantrag des Generalanwaltes vom 16.03.2016 in der beim EuGH anhängigen Rechtssache C-484/14 *(Vorlageverfahren Landgericht München I)*, mit welchem der Generalanwalt festgestellt hatte, dass Artikel 12 Abs. 1 der Richtlinie 2000/31/EG und damit auch der diesen Artikel ins deutsche Recht umsetzende § 8 TMG so auszulegen sei, dass das darin enthaltene Haftungsprivileg uneingeschränkt – entgegen dem BGH - auch die Störerhaftung ausschlösse. Dieser Auffassung folgend, so die Gesetzesbegründung zum Neuentwurf, sei § 8 Abs. 4 des Ursprungsentwurfs, wonach ein WLAN-Anschlussinhaber nicht als Störer hafte, entbehrlich. Auch dürfe nach den weiteren Ausführungen des Generalanwaltes in seinem Schlussantrag das in Artikel 12 Abs. 1 der Richtlinie 2000/31/EG und § 8 TMG enthaltene Haftungsprivileg nicht von zusätzlichen Voraussetzungen abhängig gemacht werden. Damit seien aber die in den Nrn. 1 und 2 des § 8 Abs. 4 TMG des ursprünglichen Regierungsentwurfs als Regelbeispiele vorgesehenen Schutzmaßnahmen nunmehr mit den unionsrechtlichen Vorgaben nicht mehr zu vereinbaren und daher ebenfalls zu streichen.

5. Kontroverse Rechtslage nach Inkrafttreten der Änderung des Telemediengesetzes *(TMG)*

Die in der 173. Sitzung des deutschen Bundestages vom 02.06.2016 beschlossene und am 27.07.2016 in Kraft getretene Änderung des Telemediengesetzes – Störerhaftung – ist noch in der parlamentarischen Aussprache – zu Recht – auf heftige Kritik der Opposition gestoßen *(siehe stenografischer Bericht (Auszug) des Plenarprotokolls 18/173 der 173. Sitzung des deutschen Bundestages vom 02.06.2016)*. Denn die Zielsetzung, die unklare Rechtslage für Anbieter offener

WLANs im Hinblick auf die Haftungsrisiken der Störerhaftung zu beseitigen und den WLAN-Betreibern die nötige Rechtssicherheit zu verschaffen, findet sich nur in der Gesetzesbegründung, nicht aber im Wortlaut des Gesetzes selbst.

Mit der Neuregelung in § 8 Abs. 3 TMG wurde hingegen nur klargestellt, dass Anbieter offener WLANs mit Access-Providern *(Zugangsanbietern)* im Sinne des § 8 TMG gleichzusetzen sind. Die Neuregelung des § 8 Abs. 4 TMG, wonach Anbieter offener WLANs nicht als Störer haften, wurde wieder gestrichen.

a) Der Wille des Gesetzgebers, die Haftung des WLAN Betreibers auf Abmahn- und Gerichtskosten nach den Grundsätzen der Störerhaftung auszuschließen, kommt im Wortlaut des Gesetzes mithin in keiner Weise zum Ausdruck. Subjektive Ansichten des Gesetzgebers, die allein in der Gesetzesbegründung mitgeteilt werden, sind aber nach ständiger Rechtsprechung des BGH und des BVerfG unbeachtlich *(zuletzt BGH v. 21.04.2016 – IZR 198/13 = GRUR 2016, 596; BVerfG v. 3.6.1992 – 2 BvR 1041/88)*. Insoweit beachtlich ist nur der sich im Gesetzeswortlaut selbst manifestierende Wille des Gesetzgebers. Im Gesetz selbst wurde aber die Abschaffung der Störerhaftung wieder gestrichen. Folglich wurde durch die TMG-Novelle das Ziel des Gesetzgerbers, die Störerhaftung für Anbieter offener WLANs abzuschaffen, verfehlt *(so auch Franz/Sakowski: Die Haftung des WLAN-Betreibers nach der TMG-Novelle und den Schlussanträgen des Generalanwalts beim EuGH – Handelnden- und Störerhaftung nach dem Stand der deutschen Rechtsprechung, der TMG-Novelle und den Schlussanträgen des Generalanwaltes in Rs. C-484/14 Mc Fadden/Sony Music, in: CR 8/2016, S. 524 ff., ferner Sesing, Verantwortlichkeit für offenes WLAN, in: MMR 8/2016. S. 507 f.)*.

Soweit sich der Gesetzgeber, wenn auch nur in der Gesetzesbegründung, auf die vom Generalanwalt beim Europäischen Gerichtshof in seinem Schlussantrag vom 16.03.2016 vorgenommene Auslegung des Artikel 12 Abs. 1 der

Richtlinie 2000/31/EG und des § 8 TMG bezogen hat, die – angeblich – bereits jetzt die Störerhaftung ausschließt, ist auch längst nicht ausgemacht, ob der EuGH in dem noch nicht rechtskräftig entschiedenen Fall dieser Auffassung überhaupt folgen wird.
Bis zur Klärung dieser Frage durch den EuGH besteht daher nach wie vor die bereits skizierte Rechtsunsicherheit, ob und inwieweit der Anbieter offener WLANs - trotz der Gesetzesänderung - vor kostenträchtigen Abmahnungen wirksam geschützt ist und ob und gegebenenfalls welche Sicherungsmaßnahmen dem Anbieter offener WLANs auferlegt werden können.

b) Festzuhalten ist aber, dass mit der Einfügung des neuen § 8 Abs. 3 TMG nun immerhin klargestellt ist, dass sowohl gewerbliche als auch private Anbieter offener WLANs als auch Kommunen als Access-Provider im Sinne dieser Vorschrift gelten und damit unter das Haftungsprivileg des § 8 Abs. 1 und 2 TMG fallen, und zwar unabhängig davon, ob es sich um ein kommerzielles oder ein entgeltfreies Angebot handelt. Dies ergibt sich sowohl aus dem Wortlaut und der Gesetzessystematik des geänderten TMG. Der ebenfalls neu eingefügte § 2 S. 1 Nr. 2 lit. a) TMG definiert den Begriff des drahtlosen Funknetzes rein technisch und damit weit. Insbesondere sieht er – an dieser Stelle – keine Unterscheidung zwischen geschäftsmäßigem und nicht geschäftsmäßigem Angebot vor. Auch die Klarstellung in § 8 Abs. 3 TMG unterscheidet insoweit nicht, sondern umfasst jeden Diensteanbieter, der einen Internetzugang über ein drahtloses lokales Netzwerk zur Verfügung stellt. Obendrein findet dieser Ansatz seine Stütze in der Vorschrift des § 1 Abs. 1 Satz 2 TMG, der bestimmt, dass das TMG für alle Anbieter einschließlich der öffentlichen Stellen unabhängig davon gilt, ob für die Nutzung ein Entgelt erhoben wird. Dieser Auslegung steht auch Art. 2 lit. a) der Richtlinie 2000/31/EG nicht entgegen, der unter Verweis auf Art. 1 Nr. 2 EG-Normen-Info-RL nur einen „*in der Regel gegen Entgelt*“ erbrachten Dienst von der Anwendbarkeit der Richtlinie erfasst. Denn der nationale Gesetzgeber hat sich insoweit für eine überschießende Umsetzung entschieden, die europa-

rechtlich nicht zu beanstanden ist *(Hoffmann, in: Spindler/Schuster, § 7 TMG Rdnr. 12 m.w.Nw.)*.

6. Fazit

Mit der am 27.07.2016 in Kraft getretenen Änderung des TMG ist die bestehende Rechtsunsicherheit beim Betrieb öffentlicher WLANs nicht endgültig beseitigt worden. Um diese Rechtssicherheit im Zusammenhang mit der Störerhaftung zu schaffen, hätte der Gesetzgeber in der Tat ausdrücklich in das Gesetz hineinschreiben müssen, dass WLAN-Anschlussinhaber nicht als Störer haften. Dies ist nicht erfolgt. Nun bleibt abzuwarten, wie der EuGH in der anhängigen Rechtssache entscheidet.

Die Entscheidung des EuGHs darf also mit großer Spannung erwartet werden. Folgt der EuGH dem Schlussantrag des Generalanwaltes, wird sich auch die deutsche Rechtsprechung nicht davor verschließen können, dass das Haftungsprivileg des Artikels 12 ECRL und des § 8 TMG auch die Störerhaftung ausschließt. Bleibt der EuGH aber hinter dem Schlussantrag des Generalanwaltes in den Vorabentscheidungsersuchen des LG München I zurück, bleibt abzuwarten, wie die Frage der Störerhaftung und der Bewertung der Zumutbarkeit der von einem WLAN-Anbieter zu treffenden technischen Schutzmaßnahmen, um dieser zu entgehen, künftig zu beurteilen ist.

Soweit die Stadt Heidelberg durch Bereitstellung von Infrastruktur willentlich und adäquat-kausal an der Nutzung eines offenen WLANs ohne Sicherungsmaßnahmen mitwirkt, erscheint damit auch eine *(Mit-)*Haftung als Störer nicht völlig ausgeschlossen. Allerdings dürfte aufgrund der von Freifunk gewählten Netztopologie und der zuvor unter 2. skizierten aktuellen Rechtslage das Risiko einer Inanspruchnahme eher als gering zu bewerten sein, da – wenn überhaupt - im Regelfall der Anschlussinhaber *(Freifunk)* Adressat einer gerichtlichen Verfügung ist.

III. Anbieterpflichten nach dem Telekommunikationsgesetz *(TKG)*

1. Zusammengefasste rechtliche Einordnung des Anbieters eines öffentlich zugänglichen lokalen WLAN-Hotspots

Alle Anbieter von öffentlich zugänglichen lokalen WLAN-Hotspots sind als Diensteanbieter nach § 3 Nr. 6 TKG einzuordnen *((Mantz/Sassenberg, NJW 49/2014, S. 537 ff.; Redeker, ITRB 2011, 186 ff.; zu Hotels Holznagel/Ricke in Spindler/Schuster, Recht der elektronischen Medien, 2. Aufl. 2011, § 3 TKG Rn. 8)*. Diensteanbieter ist danach *„jeder, der ganz oder teilweise geschäftsmäßig a) Telekommunikationsdienste erbringt oder b) an der Erbringung solcher Dienste mitwirkt."* Durch die Bezugnahme auf die Begriffsbestimmung des geschäftsmäßigen Erbringens von Telekommunikationsdiensten *(§ 3 Nr. 10 TKG)* wird klargestellt, dass der Tatbestand der Geschäftsmäßigkeit keine Gewinnerzielungsabsicht voraussetzt *(Säcker, in: Franz Jürgen Säcker (Hrsg.) TKG Kommentar, 3. Auflage zu § 3 Rn. 14, 26)*. Für das Merkmal der Geschäftsmäßigkeit genügt eine gewisse Dauerhaftigkeit und Nachhaltigkeit des Angebots, was vorliegend der Fall ist *(a.a.O., Rn. 26)*.

Da sich das Angebot nicht nur an einen begrenzten Personenkreis, sondern an die Öffentlichkeit richtet, erbringt die Freifunk mit dem Geschäftsmodell eines lokalen W-LAN-Hotspots zudem einen öffentlich zugänglichen Telekommunikationsdienst im Sinne von § 3 Nr. 17 a TKG und ist damit als Diensteanbieter eines öffentlich zugänglichen Telekommunikationsdienstes einzuordnen *(Sassenberg/ Mantz a.a.O., Tornow, in: Säcker, a.a.O., § 6 Rn 27 ff.)*

Im Übrigen ist der Anbieter offener WLANs auch Betreiber von öffentlichen Telekommunikationsnetzen i.S.d. § 3 Nr. 16 a TKG. Ein Telekommunikationsnetz wird definiert als Netz, das ganz oder überwiegend der Bereitstellung öffentlich zugänglicher Telekommunikationsdienste dient, die die Übertragung von Informationen zwischen Netzabschlusspunkten ermöglichen.

Was ein Netzabschlusspunkt ist, wird wiederum in § 3 Nr. 12 a TKG definiert als der physische Punkt, an dem einem Teilnehmer der Zugang zu einem Telekommunikationsnetz bereitgestellt wird *(Säcker, a.a.O., § 3 Rn. 48, 35; Sassenberg/Mantz, a.a.O.)*.

Die den Anbieter offener WLANs hiernach treffenden Anbieterpflichten nach dem Telekommunikationsgesetz *(TKG)* werden nachfolgend und 2. dargelegt.

2. Einzelne Pflichten des Anbieters eines öffentlich zugänglichen lokalen WLAN-Hotspots

2.1 Meldepflicht nach § 6 TKG

Nach § 6 TKG besteht für gewerbliche Betreiber öffentlicher Telekommunikationsnetze oder gewerbliche Anbieter öffentlicher Telekommunikationsdienste eine Meldepflicht bei der BNetzA. Freie oder kommunale WLANs handeln hingegen nicht gewerblich, sodass für diese Anbieter keine Meldepflicht nach § 6 TKG besteht. Anders verhält es sich aber bei WLANs zur Absatzförderung, werbefinanzierten WLANs und entgeltpflichtigen WLANs. Gewerblich ist hiernach – abweichend vom Merkmal der Gewerblichkeit nach § 14 GewO – jede Tätigkeit, die zumindest mit der Absicht der Kostendeckung angeboten wird *(BT-Drs. 15/2316, 60)*. Ausreichend ist, wenn lediglich eine mittelbare Kostendeckung, beispielsweise aus dem Verkauf von Getränken in einem Café, angestrebt wird. Solange Freifunk oder die Stadt Heidelberg das offene WLAN also nicht in der Absicht der Kostendeckung betreiben, scheidet eine Meldepflicht nach § 6 TKG aus.

2.2 Technische Schutzmaßnahmen nach § 109 TKG

Der Diensteanbieter ist verpflichtet, nach § 109 TKG technische Schutzmaßnahmen zu treffen, um die Telekommunikationsdienste gegen unerlaubte Zugriffe zu sichern. In diesem Zusammenhang ist ein Sicherheitsbeauftragter zu benennen und ein Sicherheitskonzept zu erstellen. Auf Verlangen ist dies der Bundesnetzagentur vorzulegen.

Die technischen Schutzmaßnahmen dienen zum einen dem Schutz des Fernmeldegeheimnisses und zum anderen dem Schutz personenbezogener Daten. Solange Freifunk oder die Stadt Heidelberg personenbezogene Daten nicht erhebt, geht es nur um die Einhaltung des Fernmeldegeheimnisses *(nachfolgend unter Punkt 2.4.)*.

Die nicht rechtzeitige Vorlage stellt eine Ordnungswidrigkeit nach § 149 I Nr. 21 iVm § 149 II TKG dar, die mit bis zu € 100.000,00 geahndet werden kann.

Das TKG sieht zudem verschiedene Mitteilungs- und Meldepflichten vor. Insbesondere sind Sicherheitsverletzungen nach § 109 V TKG der BNetzA mitzuteilen, sofern hierdurch beträchtliche Auswirkungen auf den Betrieb der Telekommunikationsnetze oder das Erbringen von Telekommunikationsdiensten entstehen. Dies sieht die BNetzA aber erst bei einem Grenzwert von über 1 Mio. betroffenen Nutzerstunden *(Teilnehmerstunden)* als eindeutig gegeben an *(BNetzA, Umsetzung des § 109 V TKG zur Mitteilung einer Sicherheitsverletzung (Umsetzungskonzept), abrufbar über www.bundesnetzagentur.de – Telekommunikation – öffentliche Sicherheit – Mitteilungen Sicherheitsverletzung – Betroffene Teilnehmerstunden werden ermittelt vom Eintritt bis zur Behebung der Beeinträchtigung)*. Entsprechen-

de Schwellenwerte werden typische WLAN-Angebote in der Regel nicht erreichen.

2.3 Datensicherheit nach § 109 a TKG

Als Anbieter öffentlich zugänglicher Telekommunikationsdienste hat die Freifunk bzw. die Stadt Heidelberg die Bundesnetzagentur im Falle einer Verletzung des Schutzes personenbezogener Daten unverzüglich zu benachrichtigen.

Solange bei dem in Rede stehenden Dienst allerdings keine personenbezogenen Daten erhoben werden, hat die Vorschrift vorliegend keinen Anwendungsbereich.

Sollte aber die Erhebung personenbezogener Daten erwogen werden, gilt Folgendes:

Eine unverzügliche Mitteilungspflicht besteht dann im Fall der Verletzung des Schutzes personenbezogener Daten, unabhängig von der Schwere der Verletzung. Die Leitlinien der BNetzA gehen von einer Meldung binnen 24 Stunden aus, so dass es für den Anbieter unbedingt erforderlich ist, vorab entsprechende Prozesse zu etablieren. Eine nahezu identische Meldepflicht ergibt sich aus der Verordnung *(EU)* Nr. 611/2013 über die Maßnahmen für die Benachrichtigung von Verletzungen des Schutzes personenbezogener Daten gem. RL 2002/58/EG.

2.4 Fernmeldegeheimnis nach § 88 TKG und Datenschutz nach § 91 f. TKG

Als Anbieter öffentlich zugänglicher Telekommunikationsdienste unterliegt der Anbieter offener WLANs dem Fernmeldegeheimnis nach § 88 TKG sowie den datenschutzrechtlichen Bestimmungen *(§§ 91 – 107 TKG)*. Das

Fernmeldegeheimnis schützt Inhalt und nähere Umstände der Telekommunikation, wobei es sowohl natürliche als auch juristische Personen umfasst *(Klesczewski, in: Säcker, a.a.O., § 88 Rn. 10)*. Hieran ändert sich auch für den Fall nichts, dass der Nutzer seine Daten über ein unverschlüsseltes WLAN überträgt. Der Verstoß gegen die Verpflichtung zur Wahrung des Fernmeldegeheimnisses ist nicht nur eine Ordnungswidrigkeit, die mit einer Geldbuße von bis zu € 300.000,00 geahndet werden kann *(§ 149 Nr. 16 TKG)*, sondern bei unbefugter Weitergabe an Dritte auch strafbewehrt *(3 206 StGB)*.

Nach § 88 Abs. 3 TKG ist es den Verpflichteten untersagt, sich oder anderen über das für die Erbringung der Telekommunikationsdienste erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. Insoweit sind Schutzmaßnahmen zu treffen, damit sich ein Unbefugter nicht Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation durch die individuellen Nutzer verschaffen kann. Was Art und Umfang derartiger Schutzmaßnahmen vor unberechtigten Zugriffen angeht, muss dies in technischer Hinsicht im Sicherheitskonzept festgelegt und deren Umsetzung und Einhaltung durch den zu bestimmenden Sicherheitsbeauftragten überwacht werden.

Weiter regeln die §§ 91 ff. TKG den Umgang mit personenbezogenen Daten spezialgesetzlich, sodass die Regelungen des BDSG weitgehend verdrängt werden *(hierzu Beck TKG/Braun, § 96 Rn. 7 f.)*. Im TKG wird primär zwischen Bestands- und Verkehrsdaten unterschieden.

Die spezialgesetzlichen Datenschutzvorschriften finden allerdings nur Anwendung, sofern überhaupt personenbezogene Daten *(Bestands- oder Verkehrsdaten)* im Zuge der Nutzung des Dienstes vom Nutzer erhoben werden, was nicht unbedingt erforderlich ist.

aa) Bestandsdaten

Bestandsdaten sind nach § 3 Nr. 3 TKG die *„Daten eines Teilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden."*

bb) Verkehrsdaten

Verkehrsdaten sind nach § 3 Nr. 30 TKG hingegen *„Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden."*

cc) Anonyme Nutzung/keine Pflicht des Anbieters offener WLANs zur Speicherung von Bestands- oder Verkehrsdaten.

Die Nutzung eines WLAN-Hotspots muss nicht per se zu einer Vertragsbeziehung zwischen dem Anbieter und dem Nutzer und/oder zu einer Speicherung von Bestands- oder Verkehrsdaten führen. Vielmehr wird aus Erwägungsgrund 42 der Richtlinie 2000/31/EG *(ECRL)* deutlich, dass allein auf den technischen Vorgang der sogenannten *„reinen Durchleitung"* abzustellen ist. Hiernach wird die Tätigkeit des Access Providers als *„rein technischer, automatischer und passiver Art"* charakterisiert *(siehe auch Hoffmann, in: Spindler/Schuster, § 8 TMG Rn. 12 m.w.N.)*. Folglich ist eine solche anonyme Nutzung vom europäischen und nationalen Gesetzgeber gerade gewollt. Dies ergibt sich auch aus dem Erwägungsgrund 14 der ECRL ausdrücklich: *„die anonyme Nutzung offener Netze wie des Internets kann diese Richtlinie nicht unterbinden."* Auch § 13 Abs. 6 TMG sieht vor, dass der Diensteanbieter die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen hat, soweit dies technisch möglich ist. Damit besteht aus Sicht des TK-Rechts für den Anbieter keine Pflicht zur Speicherung von Verkehrs- und Bestandsda-

ten, die für eine Identifikation des Nutzers zwingend erforderlich wären oder dessen Rückverfolgung ermöglichen *(hierzu auch OVG, NRW, Beschluss vom 10.11.2014 – 13 A 1973/13; Sassenberg/Mantz, WLAN & Recht, 2014, Rn. 233; zur „Speicherung auf Zuruf" OLG München MMR 2012, 764; OLG Düsseldorf MMR 2013, 392, siehe auch Braun, in: Geppert/Schütz, Beck TKG, 4. Aufl. 2013, § 96 TKG Rn. 8, 13, 17).*

Damit ist der Anbieter offener WLANs zwar im Rahmen der §§ 91 ff. TKG berechtigt, aber nicht verpflichtet, Verkehrs- und Bestandsdaten zu erheben und zu speichern oder aber den Dienst auch völlig anonym anzubieten. Sollte angedacht sein, in den Vermittlungsknoten die IP-Adresse des Nutzers als Bestandsdaten zu speichern, sind ebenso wie bei eventueller Speicherung von Verkehrsdaten die entsprechenden gesetzlichen Löschungsfristen zu beachten.

2.5 Vorratsdatenspeicherung

Nachdem zunächst aufgrund des Urteils des Bundesverfassungsgerichts vom 02.03.2010 – 1 WvR 256/08 die Vorschriften zur Vorratsdatenspeicherung für nichtig erklärt wurden, hat der Gesetzgeber zwischenzeitlich in den §§ 113 a – g TKG eine Speicherpflicht und Höchstspeicherpflicht für Verkehrsdaten eingefügt. Dabei beschreibt die Vorschrift des § 113 a TKG den Kreis der zur Speicherung Verpflichteten. Nicht verpflichtet sind hiernach Anbieter, die ihren Kunden nur eine kurzzeitige Nutzung des Telekommunikationsanschlusses ermöglichen, z. B. Betreiber von Hotels, Restaurants und Cafés, die ihren Kunden eine Telefon- oder Internetnutzung zur Verfügung stellen *(zur näheren Bestimmung des Begriffs des „Erbringens" vgl. die Mitteilung Nr. 149/2015 im Amtsblatt der Bundesnetzagentur)*. Dabei sieht die Bundesnetzagentur die Betreiber von WLAN-Hotspots in Cafés, Hotels etc., die lediglich ihren Internetanschluss mit anderen teilen und dem Nutzer nicht

einen eigenen Telekommunikationsanschluss zur Verfügung stellen, nicht als *„Erbringer“* im Sinne der Vorschrift des § 113 a Abs. 1 S. 1 TKG an, sondern lediglich als *„Mitwirkende“* an einem Telekommunikationsdienst *(vgl. Mitteilung Nr. 149/2015 im Amtsblatt der Bundesnetzagentur)*. Folgt man der Auslegung der Bundesnetzagentur, findet die gesamte Pflicht zur Vorratsdatenspeicherung auf offene WLANs keine Anwendung. Diese Auslegung ist auch europarechtskonform, da, wie zuvor bereits ausgeführt, nach der Richtlinie 2000/31/EG eine anonyme Nutzung eines offenen WLANs vom europäischen Gesetzgeber gerade gewollt ist. Dem würde eine Pflicht zur Vorratsdatenspeicherung von Verkehrsdaten aber gerade entgegenstehen.

2.6 Telekommunikations-Überwachung nach § 110 TKG

Für Betreiber eines offenen Internetzugangs über lokale WLAN-Hotspots ist die Vorschrift des § 110 TKG zur Telekommunikations-Überwachung anwendbar.

Hiernach muss auf Ersuchen einer auskunftsberechtigten Stelle *(Sicherheitsbehörden)* als Datensatz eine Überwachungskopie *(Ereignis- und Nutzdaten)* des Telekommunikationsvorganges übermittelt werden.

Näheres regelt die Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation *(Telekommunikations-Überwachungsverordnung-TKÜV)* und die in Umsetzung der Verordnung ergangene technische Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation *(TR TKÜV Ausgabe 6.3 April 2016* - Bekanntmachung im Amtsblatt der Bundesnetzagentur Amtsblatt Nr. 6/2016 vom 06.04.2016, Vfg-Nr. 18, Seite 716).

Im Sinne der vorgenannten Rechtsvorschriften gilt ein lokaler WLAN-Hotspot als Internetzugangsweg *(Übertragungsweg)*, der dem unmittelbaren

teilnehmerbezogenen Zugang zum Internet dient, da mit diesem Angebot eine der Individualkommunikation dienende Nutzung des Internets ermöglicht wird.

Als Anbieter wäre die Freifunk bzw. die Stadt Heidelberg daher grundsätzlich verpflichtet, Vorkehrungen zur Überwachung des gesamten IP-Verkehrs zu treffen. Technisch geschieht dies in der Weise, dass durch Installation eines zusätzlichen Routers eine vollständige Überwachungskopie der zu überwachenden Telekommunikation verschlüsselt über IPsec an die auskunftsersuchende Stelle übermittelt wird. Das zu übermittelnde Doppel der zu überwachenden Telekommunikation besteht in den Ereignisdaten *(Login/Logout)* und der Übermittlung der Nutzkopie *(Nutzerinformationen)*. Ist bei einem Zugang über ein öffentliches WLAN die nach der TR TKÜV vorgesehene Kennung nicht verfügbar, so ist eine Kennung des Endgerätes zu verwenden *(z.B. MAC-Adresse, IMEI)*.

<u>Rechtliche Einordnung</u>

aa) Allerdings gehören Betreiber öffentlicher Internetzugänge *(beispielsweise über W-LAN)* dann **nicht** zum Kreis der Verpflichteten, wenn nicht mehr als 10.000 Teilnehmer angeschlossen sind *(vgl. § 3 Abs. 2 Nr. 5 TKÜV)*. Soweit es sich bei der Nutzung öffentlicher WLANs nicht um registrierte Kunden handelt, ist bei der Ermittlung der relevanten Teilnehmerzahl die Anzahl gleichzeitig an der gesamten TK-Anlage angeschlossenen Endgeräte maßgeblich *(TR TKÜV, Teil A, S. 13)*. Aus diesem Grund wären die vorgenannten Vorschriften auf die Freifunk bzw. die Stadt Heidelberg als Betreiber nicht anwendbar, wenn man unterstellt, dass der Nutzerkreis 10.000 Teilnehmer nicht überschreitet. Die Vorschriften richten sich somit nur an größere Betreiber.

bb) Aber selbst für den Fall der Anwendbarkeit bei mehr als 10.000 Teilnehmern besteht im Hinblick auf den Grundsatz, dass es keine Verpflichtung des Betreibers zur vorherigen Identifikation des Nutzers gibt *(also wenn die Einwahl nur unter einer IP-Adresse erfolgt)*, keine weitergehende Verpflichtung auf eine vorherige Individualisierung bzw. Identifikation des Nutzers. Wird im Rahmen des öffentlichen Zugangs zum WLAN für den jeweiligen Nutzer nur eine User-ID und ein Passwort vergeben oder erfolgt nur die Vergabe einer IP-Adresse, ohne dass der Nutzer zuvor identifiziert wird, käme allenfalls eine Speicherung individueller Kennungen wie z.B. der Endgerätekennung in Betracht. Wenn im Rahmen einer konkret angeordneten Überwachungsmaßnahme aus technischen Gründen die Endgerätekennung aber nicht ermittelt werden kann, besteht, wie zuvor dargelegt, keine Verpflichtung, eine individuelle Kennung zu vergeben. Gegenüber der Sicherheitsbehörde ginge die Überwachungsmaßnahme sodann ins Leere.

2.7 Manuelles Auskunftsersuchen

Wer geschäftsmäßig Telekommunikationsdienste erbringt oder hieran mitwirkt und dabei Rufnummern oder Anschlusskennungen vergibt, hat die in § 111 Abs. 1 S. 1 Nr. 1 - 6 TKG aufgeführten Bestandsdaten des Anschlussinhabers zu speichern und den zuständigen Behörden hierüber im Wege des manuellen Auskunftsverfahrens nach § 113 TKG oder *(ab 100.000 Kunden)* im Wege des automatisierten Auskunftsverfahrens durch Einrichtung einer elektronischen Schnittstelle nach § 113 Abs. 5 S. 1, § 112 TKG Auskunft zu erteilen. Wenn vorliegend jedoch die anonyme Nutzung des Netzes durch jeden Nutzer ohne Registrierung vorgesehen ist, lässt sich auch im Hinblick auf die dem Nutzer im Zuge der Einwahl vergebene IP-Adresse kein Rückschluss auf eine Endgerätekennung entnehmen; auch taucht dann die IP-Adresse konkret in der Verbindungskette nicht auf. Dann wird aber im Zuge

der Einwahl in das Internet bereits tatbestandlich keine dauerhafte Anschlusskennung vergeben, sodass die Vorschriften betreffend das Auskunftsersuchen nach §§ 111 - 113 TKG nicht einschlägig sind. Sollte die Freifunk bzw. die Stadt Heidelberg daher mit der Anfrage einer zuständigen Stelle konfrontiert werden, ist es ausreichend, auf diesen Umstand hinzuweisen.

Bei all diesen Vorgängen sollten auch keinerlei Informationen über die Verbindungen der Nutzer gespeichert werden.

Düsseldorf, den 06.09.2016
(Mayer)
Rechtsanwalt