Rechtsanwälte
LEHNER DÄNEKAMP & MAYER
Düsseldorf • Heidelberg

ERGÄNZUNGSGUTACHTEN
zur
RECHTSGUTACHTERLICHEN STELLUNGNAHME
vom 06. September 2016

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

Von RA Frank Joachim Mayer

Datum 13. Oktober 2016

Unser Zeichen: 023D/16

Betreff: Ergänzungsgutachten zur Rechtsgutachterlichen Stellungnahme zu Fragen der Zulässigkeit einer Kooperation der Stadt Heidelberg mit der Freifunk Rhein-Neckar e.V. im Hinblick auf die Bereitstellung öffentlich genutzter WLAN-Netze
hier: Störerhaftung nach dem WLAN-Urteil des Europäischen Gerichtshofs *(EuGH)* vom 15.09.2016, Konformität nach dem Telekommunikationsgesetz *(TKG)* und Telemediengesetz *(TMG)*.

Inhaltsverzeichnis

A. Ausgangssachverhalt des Erstgutachtens / Ausgangsprüfung

Dem zu prüfenden Ausgangssachverhalt lag 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 Freifunknetzwerke, die aus altruistischen Gründen öffentliche, entgeltfreie WLAN-Hotspots betreibt. Dabei ermöglicht Freifunk eine anonyme Nutzung des offenen WLANs. Weder erfolgt eine Erhebung oder Speicherung der Bestands- oder Verkehrsdaten noch eine Identifikation des jeweiligen Nutzers. Auch sonstige Sicherungsmaßnahmen gegen Rechtsverletzungen *(z.B. Urheberrechtsverletzungen)*, die Nutzer über das offene WLAN begehen, werden von Freifunk nicht getroffen.

Ausgehend von diesem Ausgangssachverhalt *(vgl. im Einzelnen unter A. des Erstgutachtens)* wurde eine rechtsgutachterliche Stellungnahme zu folgendem Prüfungsauftrag abgegeben:

- 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. Urheberrechtsverletzungen)*;
- Anbieterpflichten der Freifunk / Stadt Heidelberg nach dem Telekommunikationsgesetz *(TKG)*.

Die Stadt Heidelberg unterhält ihrerseits das Angebot und den Betrieb eines öffentlichen WLAN-Netzes unter der Bezeichnung *„Heidelberg4you“*. Der jeweilige Nutzer des öffentlichen WLAN-Netzes *„Heidelberg4you“* muss sich mit seiner Mobilfunkrufnummer zuvor registrieren, um das offene WLAN der Stadt Heidelberg nutzen zu können.

B. Zusammenfassung der Ausgangsfeststellungen des Erstgutachtens

1. Das Angebot eines öffentlich zugänglichen WLANs ist rechtlich zulässig und politisch erwünscht. Auch die anonyme Nutzung ohne vorherige Identifikation des Nutzers ist nicht per se unzulässig *(Erstgutachten, C. I., Seite 4 ff.)*.

2. Spätestens seit der am 27.07.2016 in Kraft getretenen Novelle des Telemediengesetzes *(TMG)* fallen alle Anbieter öffentlich zugänglicher WLANs, gleich ob gewerblicher, nichtgewerblicher, kommunaler oder altruistischer Natur, als Zugangsanbieter *(Access-Provider)* unter das Telemediengesetz und gelten damit als haftungsprivilegiert im Sinne von § 8 Abs. 1, 2 TMG, und zwar unabhängig davon, ob es sich um ein kommerzielles oder ein entgeltfreies Angebot handelt *(Ergänzungsgutachten, C. II. 5. lit. b), Seite 20)*.

3. In der höchstrichterlichen deutschen Rechtsprechung bislang nicht geklärt und damit umstritten war allerdings die Frage, ob das Haftungsprivileg des § 8 TMG den Anbieter öffentlich zugänglicher WLANs auch vor der Inanspruchnahme aus der sogenannten verschuldensunabhängigen Störerhaftung schützt, wenn Nutzer über den Netzzugang Rechtsverletzungen *(z.B. Urheberrechtsverletzungen)* begehen und der Rechteinhaber daraufhin den Access-Provider verschuldensunabhängig als *„Störer“* auf Unterlassung in Anspruch nimmt *(abmahnt)*. In der deutschen Rechtsprechung war bislang ebenfalls nicht geklärt, ob anlassbezogene Sicherungsmaßnahmen für Betreiber öffentlich zugänglicher Funknetze überhaupt in Betracht kommen, ohne das gewünschte Ergebnis frei zugänglicher Netze in Frage zu stellen. Diese Rechtsunsicherheit sollte eigentlich durch die am 27.07.2016 in Kraft getretene Novelle des Telemediengesetzes beseitigt werden, was allerdings missglückt ist. Die eigentliche Regelung in § 8 Abs. 4 TMG-Entwurf, mit der die Störerhaftung beseitigt werden sollte, wurde wieder gestrichen. Zur Begründung nahm der Gesetzgeber Bezug auf das beim EuGH anhängige Verfahren zur WLAN-Störerhaftung *(EuGH Rechtssache C-484/14)* nach Vorlage durch das Landgericht München I mit Beschluss vom 18.09.2014 – 7 O 14719/12. In diesem Vorlageverfahren hatte der Generalanwalt beim EuGH in seinem Schlussantrag vom 16.03.2015 die Auffassung vertreten, dass die derzeit geltenden Rechtsvorschriften der Artikel 12 Abs. 1 der Richtlinie 2000/31/EG *(und in deren Umsetzung § 8 TMG)* den Ausschluss der WLAN-Störerhaftung bereits mitumfasse und insbesondere keine weitergehenden Sicherungsmaßnahmen zulasse. Damit sei, so der Gesetzgeber in seiner Gesetzesbegründung, die zunächst im Gesetz vorgesehene Regelung zum Ausschluss der WLAN-Störerhaftung entbehrlich. Der Gesetzgeber übersah hierbei aber, dass längst nicht ausgemacht war, ob der EuGH tatsächlich der Auslegung im Schlussantrag des Generalanwaltes folgen oder

aber zu einer anderen Auslegung der bestehenden Rechtsvorschriften gelangen würde. Der Gesetzgeber versäumte es somit – ungewöhnlich genug – durch die zunächst vorgesehene Gesetzesänderung für endgültige Klarheit zu sorgen und überließ stattdessen die Klärung der Rechtsfrage zur WLAN-Störerhaftung einem laufenden Gerichtsverfahren, welches obendrein nur einen Einzelfall entscheidet.

Nachdem bereits im Erstgutachten als Fazit festgehalten wurde, dass zwecks weiterer Klärung der Rechtslage im Zusammenhang mit der WLAN-Störerhaftung nun die Entscheidung des EuGH abzuwarten sei *(Erstgutachten, Seite 21 unter C. II. 6.)*, und das WLAN-Urteil des EuGH nunmehr am 15.09.2016 ergangen ist, ist die vorliegende Neubewertung erforderlich.

4. Jeder Anbieter eines öffentlich zugänglichen lokalen WLAN-Hotspots gilt als Diensteanbieter nach § 3 Nr. 6 lit. b) TKG und unterliegt damit Anbieterpflichten nach dem TKG *(Erstgutachten, C. III., Seite 22 ff.)*.

5. Da nach § 3 Nr. 6 lit. b) TKG bereits Mitwirkungshandlungen an der Erbringung von TK-Diensten ausreichen, um die Diensteanbietereigenschaft nach dem TKG zu begründen, wurde im Rahmen der rechtlichen Beurteilung des Erstgutachtens kein Unterschied vorgenommen zwischen der Freifunk als dem unmittelbaren Betreiber des offenen WLAN und der Stadt Heidelberg, die gegebenenfalls *„nur“* daran mitwirkt. Soweit die Stadt Heidelberg ihrerseits das Heidelberg4you betreibt, begründet dies ohnehin die Diensteanbietereigenschaft im Sinne des TKG.

C. Prüfungsauftrag des Ergänzungsgutachtens

Anlass für die Erstellung des vorliegenden Ergänzungsgutachtens ist das am 15.09.2016 und damit nach Erstellung des Erstgutachtens vom 06.09.2016 ergangene WLAN-Urteil des Europäischen Gerichtshofes *(EuGH)* im Hinblick auf die urheberrechtliche Störerhaftung der Betreiber öffentlich zugänglicher WLAN-Netze *(EuGH, Urteil v. 15.09.2016, Rechtssache C-484/14)*. Die Urteilsgründe machen eine Neubewertung der in dem Erstgutachten hierzu getroffenen

Feststellungen notwendig. Im Zuge dieses Ergänzungsgutachtens sollen daher folgende ergänzende Fragestellungen rechtsgutachterlich beleuchtet werden:

- Welche Auswirkungen hat das WLAN-Urteil des EuGH auf das Geschäftsmodell der Freifunk und das Geschäftsmodell der Heidelberg4you?
- Welche Anbieterpflichten nach dem TKG sind – in Abhängigkeit von den konkret zu treffenden Schutzmaßnahmen – einzuhalten?

D. Ergänzendes Prüfungsergebnis

I. WLAN-Urteil des EuGH und seine Auswirkungen auf die WLAN-Störerhaftung

1. Feststellungen des EuGH-Urteils im Überblick

1.1 Allgemeine Feststellungen des EuGH zur Störerhaftung

Zunächst stellt der EuGH in seinem WLAN-Urteil fest, dass der Betrieb auch eines ungesicherten WLANs *„an sich“* keinen Anspruch auf Schadensersatz oder Ersatz der Abmahnkosten bzw. der Gerichtskosten begründet. Dies ergäbe sich aus der Vorschrift des Artikel 12 Abs. 1 der Richtlinie 2000/31/EG und – in dessen Umsetzung - § 8 Abs. 1 Telemediengesetz *(TMG)*, wonach Diensteanbieter unter den dort genannten Voraussetzungen für die Durchleitung fremder Informationen nicht verantwortlich sind. Allerdings, so der EuGH weiter, laufe es diesen Vorschriften nicht zuwider, wenn ein geschädigter Rechteinhaber im Verletzungsfall gegen den Betreiber eines schlecht gesicherten öffentlich zugänglichen WLANs die Unterlassung der Fortsetzung der Rechtsverletzung sowie die Zahlung der Abmahn- und Gerichtskosten verlangt und damit im Wege der Störerhaftung vorgeht. Damit hat der EuGH – wie zuvor der BGH im Zusammenhang mit Host-Providern nach § 10 TMG *(BGHZ 158, 343 = NJW 2004, 2158 – Schöner Wetten; BGHZ 158, 236 = NJW 2004, 3102 – Internet-Versteigerung I)* – im Ergeb-

nis festgestellt, dass die einschlägigen Rechtsvorschriften der Artikel 12 ECRL – und damit § 8 TMG – die Inanspruchnahme als Störer nicht ausschließen, wenn eine Rechtsverletzung über den Internetanschluss begangen und daraufhin der Anschluss nicht gesichert wird. Im Umkehrschluss bedeutet dies, dass keine Abmahnung erfolgen darf, wenn das öffentlich zugängliche WLAN von vornherein gesichert wird. Wenn – so im Ergebnis der EuGH – der öffentliche WLAN-Zugang allerdings ungesichert betrieben wird, droht bereits im ersten Verstoßfall eine Abmahnung, *„es zu unterlassen, weiterhin die Rechtsverletzung zu ermöglichen, ohne den Zugang geeignet zu sichern“*, wenn nach dem Verstoß nicht sofort eine Sicherung erfolgt

1.2 Feststellungen des EuGH zu geeigneten Sicherungsmaßnahmen

Vorab ist hierzu festzustellen, dass der EuGH in seinem WLAN-Urteil keine allgemeinverbindliche Regelung dazu treffen konnte, welche Sicherungsmaßnahmen geeignet sind, um die Fortsetzung einer Rechtsverletzung zu verhindern.

Dies liegt darin begründet, dass ein Gericht nur einen Einzelfall entscheidet. Insoweit weigerte sich der EuGH folgerichtig auch, sich mit anderen als den drei vom Landgericht München I vorgelegten Sicherheitsmaßnahmen zu beschäftigen. Allerdings lassen die Begleitausführungen eines höchstrichterlichen Gerichts Rückschlüsse darauf zu, welche Anforderungen nach Auffassung der Rechtsprechung Sicherungsmaßnahmen erfüllen müssen, um als geeignet zu erscheinen *(Obiter Dictum)*. Dazu führte der EuGH in seinem Urteil aus, dass nur solche Sicherungsmaßnahmen in Betracht kommen, die ein angemessenes Gleichgewicht zwischen den Grundrechten der Beteiligten sicherstellen *(EuGH, a.a.O., Rn. 89)*. Insoweit sei eine Abwägung zu treffen zwischen der unternehmerischen Freiheit des Anbieters eines öffentlich zugänglichen WLANs und dem Urheberrecht eines Rechteinhabers. Der EuGH stellte hierzu ausdrücklich fest, dass es dabei im Rahmen der Herstellung des

angemessenen Gleichgewichts zwischen den Grundrechten durchaus dem Anbieter des öffentlich zugänglichen WLANs überlassen bleiben kann, die konkreten Sicherungsmaßnahmen näher zu bestimmen *(EuGH a.a.O., Rn. 84)*. Insoweit muss die zu treffende Sicherungsmaßnahme nur hinreichend wirksam sein, um den Nutzer des Anschlusses zuverlässig davon abzuhalten bzw. davon abzuschrecken, über den Anschluss eine Rechtsverletzung zu begehen *(EuGH, a.a.O., Rn. 95, 96)*.

Der EuGH erkannte zwei der vom Landgericht München I vorgelegten drei Sicherungsmaßnahmen hiernach als ungeeignet an. Sowohl die vollständige Abschaltung des Internetanschlusses als auch die allgemeine Verpflichtung zur Überwachung der über den Anschluss übermittelten Informationen sei hiernach keine geeignete Maßnahme, um die Grundrechte der Beteiligten in Einklang zu bringen. Die vollständige Abschaltung des Internetanschlusses stelle einen nicht hinnehmbaren erheblichen Eingriff in die unternehmerische Freiheit des Anschlussbetreibers dar *(EuGH a.a.O., Rn. 88)*. Die allgemeine Verpflichtung zur Überwachung des Anschlusses scheide bereit aus Rechtsgründen aus, da sie Artikel 15 Abs. 1 der Richtlinie 2000/31 zuwiderlaufe, wonach Zugangsanbietern eine derartige Pflicht gerade nicht auferlegt werden dürfe *(EuGH a.a.O., Rn. 87)*.

Allein die vom Landgericht München I vorgelegte weitere Sicherungsmaßnahme, den Anschluss mit einem Passwort zu sichern, sah der EuGH als verhältnismäßig und geeignet an, den Nutzer des Anschlusses von einer Rechtsverletzung abzuhalten. Dies gelte aber nur dann, wenn die Nutzer zugleich ihre Identität offenbaren müssen, um das erforderliche Passwort zu erhalten *(EuGH, a.a.O., Rn. 95, 969)*.

Ob die vom EuGH als geeignet erkannte Sicherungsmaßnahme aber tatsächlich wirksam und rechtlich zulässig ist, erscheint dabei äußerst fraglich.

LDM Lehner Dänekamp & Mayer, Rechtsanwälte · Düsseldorf · Heidelberg
Büro Düsseldorf: Am Seestern 8· 40547 Düsseldorf · Tel.: (0211) 523964-0· Fax: (0211) 523964-9
E-Mail: frank.mayer@ldm-law.de · www.ldm-law.de

a) Tatsächliche Wirksamkeit der Passwortvergabe mit Identitätsfeststellung

Eine Passwortvergabe und Identitätsfeststellung des Nutzers ist nur dann wirksam, wenn im Verletzungsfall eine Rückverfolgung zu dem Nutzer möglich ist. Spätestens dann, wenn aber mehrere Nutzer parallel den Anschluss nutzen – was der Regelfall sein dürfte – kann ohne eine weitergehende Überwachung und Speicherung der Datenströme im Verletzungsfall der Verletzter nicht ermittelt werden. Obendrein kann selbst bei einer Überwachung und Speicherung der Datenströme die Zuordnung einer Rechtsverletzung zu einem zuvor bei der Passwortvergabe identifizierten Nutzer nur dann erfolgen, wenn im Zuge der vorherigen Offenbarung seiner Identität gleichzeitig eine Anschlusskennung *(Mobilfunkrufnummer oder Endgerätekennung)* mit registriert wird. Die Pflicht zur Offenbarung der Identität des Nutzers reicht für sich genommen damit nicht aus, um einen Nutzer wirksam von einer Rechtsverletzung abzuschrecken.

b) Rechtliche Zulässigkeit der Passwortvergabe mit Identitätsfeststellung

Die vom EuGH für wirksam erachtete Sicherungsmaßnahme der Offenbarung der Identität des Nutzers im Zuge der Passwortvergabe ist allerdings bereits für sich genommen mit den geltenden deutschen datenschutzrechtlichen Bestimmungen nur dann in Einklang zu bringen und rechtmäßig, wenn mit dem Nutzer – als gesetzlicher Erlaubnistatbestand für die Datenerhebung – vor Beginn des Nutzungsvorgangs ein Vertrag begründet wird, in dessen Rahmen der Nutzer über Art, Zweck und Umfang der Datenspeicherung unterrichtet wurde *(§§ 95, 3 Nr. 3, 96, 93 TKG, §§ 14, 15 Telemediengesetz, hierzu auch Sassen-*

berg/Mantz, WLAN und Recht, 2014, Rz. 234; Mantz/Sassenberg CR 5/2015, S. 298, 303).

Ob der Nutzer auch außerhalb eines Vertragsverhältnisses nach § 4 a BDSG seine ausdrückliche Einwilligung dazu erteilen kann, erscheint fraglich. Insoweit gehen die einschlägigen Vorschriften der §§ 91 ff. TKG bzw. §§ 14, 15 TMG nach § 1 Abs. 3 S. 1 BDSG als bereichsspezifische Regelungen dem BDSG vor. Lediglich soweit es an speziellen Regelungen im TKG/TMG zum Datenschutz fehlt, sind die Vorschriften des BDSG weiterhin ergänzend heranzuziehen *(Klesczewski, in: Franz Jürgen Säcker (Hrsg.) TKG Telekommunikationsgesetz, 3. Auflage, § 91 Rn. 16)*. Damit wäre eine Erhebung und Verarbeitung personenbezogener *(Bestands-)* Daten wie die Identitätsfeststellung nur im Rahmen eines zuvor begründeten Vertragsverhältnisses und nur zu den im TKG/TMG definierten Zwecken erlaubt, wobei der Nutzer bei Vertragsbegründung umfassend über Zweck und Umfang zu unterrichten wäre *(§ 93 TKG)*.

Einem solchen Vertragsschluss steht in der Praxis nichts im Wege. Denn ein sogenannter „*einseitig verpflichtender Vertrag*“ kann auch über ein kostenloses Angebot abgeschlossen werden kann, der mit Beendigung des Nutzungsvorgangs sein Ende findet.

c) Hilfserwägung: Zusätzliche Maßnahme der Protokollierung / Überwachung des Surfverhaltens des Nutzers zwecks Rückverfolgung

Wie zuvor festgestellt, ist die vom EuGH beurteilte Sicherungsmaßnahme der vorherigen Identitätsoffenbarung im Zuge einer Passwortvergabe an sich gar nicht wirksam. Als zusätzliche und tatsächlich wirksame Maßnahme käme also die Überwachung/Speicherung des

Datenverkehrs und einer Anschlusskennung *(Mobilfunkrufnummer)* des Nutzers zwecks späterer Zuordnung einer Rechtsverletzung zu dem konkreten Nutzer in Betracht. Dies dürfte aber in jedem Fall gesetzeswidrig sein.

aa) Keine allgemeine Überwachungspflicht

Die Registrierung einer Anschlusskennung *(Mobilfunkrufnummer)* des Nutzers und softwarebasierte Protokollierung und Speicherung des Datenverkehrs *(Verkehrsdaten)*, die – sei es auch nachträglich – eine Zuordnung der konkreten Nutzung zu einem bestimmten Nutzer ermöglicht, läuft bereits Artikel 15 Abs. 1 der Richtlinie 2000/31 zuwider. Der EuGH selbst gelangt unter Rn. 87 seines Urteils zu diesem Ergebnis, wonach eine Sicherungsmaßnahme von vornherein ausscheidet, die Zugangsanbietern entgegen Artikel 12 Abs. 1 der Richtlinie 2000/31 eine allgemeine Verpflichtung zur Überwachung des Datenverkehrs auferlegt. Auch der diese Vorschrift in das deutsche Recht umsetzende § 7 Abs. 2 Telemediengesetz schließt gerade die Verpflichtung des Diensteanbieters aus, die von ihnen übermittelten Informationen zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tat hinweisen.

bb) Verstoß gegen das deutsche Datenschutzrecht

Die weitergehende Möglichkeit einer Protokollierung des Surfverhaltens der Nutzer zwecks – sei es auch nachträglicher – Zuordnung zu dessen Anschlusskennung zur Verhinderung einer späteren Haftung sehen die einschlägigen datenschutzrechtlichen Vorschriften des TKG/TMG auch nicht vor.

So ist nach § 96 TKG, § 15 TMG die Speicherung von Verkehrsdaten *(Nutzungsdaten)* über den Nutzungsvorgang hinaus nur zu Abrechnungszwecken erlaubt *(hierzu auch Sassenberg/Mantz, WLAN und Recht, 2014, Rz. 234, Mantz/Sassenberg CR 5/2015, S. 303 unter 4. „Datenschutzrecht“).*

Ob WLAN-Anbieter hierbei datenschutzrechtlich unter das TMG oder das TKG fallen, was abschließend nicht geklärt ist *(zum Meinungsstand Klesczewski, a.a.O., Rn. 19),* kann bei der Beurteilung dahinstehen, da beide Gesetze insoweit eine übereinstimmende Regelung treffen.

Auch der Rückgriff auf eine ausdrücklich erteilte Einwilligung nach § 4 a BDSG hilft in diesem Fall nicht weiter, da das BDSG, wie zuvor dargelegt, nicht ergänzend anwendbar ist.

Damit ist die Überwachung des Datenverkehrs zwecks Rückverfolgung zum konkreten Nutzer in jedem Fall gesetzwidrig *(hierzu auch Mantz/Sassenberg, CR 5/2015, Seite 298, 303; Bergt, CR-Online vom 01.03.2015, http://www.cr-online.de/block/2015/03/01/gesetzesentwurf-zur-abschaffung-freier-wlans).*

1.3 Fazit

Ohne Protokollierung des Surfverhaltens des Nutzers mit anschließender Zuordnung des Datenverkehrs zur offenbarten Identität des Nutzers läuft die vom EuGH für wirksam erachtete Sicherungsmaßnahme der vorherigen

Passwortvergabe und Identitätsfeststellung ins Leere. Dies hat der EuGH in seinem WLAN-Urteil übersehen.

Aber auch datenschutzrechtlich ist das WLAN-Urteil des EuGH in diesem Punkt erheblichen Bedenken ausgesetzt. Nach den einschlägigen deutschen datenschutzrechtlichen Bestimmungen des TKG/TMG dürfen personenbezogene Daten wie die Identitätsfeststellung des Nutzers oder seiner Anschlusskennung *(Mobilfunkrufnummer)* nur im Zuge einer Vertragsbegründung und nur zu den im TKG/TMG genannten Zwecken erhoben *(verwendet)* werden, über die der Nutzer zuvor eingehend zu unterrichten ist.

Die eigentlich wirksame Sicherungsmaßnahme der Protokollierung des Surfverhaltens der Nutzer zwecks nachträglicher Rückverfolgung zur Identität/Anschlusskennung des Nutzers zwecks Verhinderung einer späteren Haftung wäre damit – jedenfalls ohne Vergabe einer eigenen IP-Adresse an den Nutzer, hierzu nachfolgend unter 3. - in jedem Fall als gesetzeswidrig zu beurteilen.

2. Auswirkungen des WLAN-Urteils des EuGH auf das Geschäftsmodell der Freifunk

Auch wenn sich das WLAN-Urteil des EuGH nur auf gewerbliche Anbieter bezieht, wird es künftig in der deutschen Rechtsprechung Berücksichtigung auch auf nicht-gewerbliche Anbieter wie z. B. die Freifunk-Initiativen oder Kommunen finden. Denn insoweit hat sich der deutsche Gesetzgeber mit der Einfügung des neuen § 8 Abs. 3 TMG im Zuge der am 27.07.2016 in Kraft getretenen TMG-Novelle für eine überschießende Umsetzung des europäischen Rechts entschieden, sodass auch kommunale WLANs oder rein altruistische Angebote wie die Freifunk-Initiative unter die Diensteanbietereigenschaft des TMG fallen.

Demnach dürften auch für nicht-gewerbliche Anbieter künftig die im WLAN-Urteil des EuGH niedergelegten Leitlinien zur WLAN-Störerhaftung Anwendung finden.

Folglich gilt auch für die Freifunk-Initiativen, dass die Inanspruchnahme als Störer künftig nicht ausgeschlossen ist, wenn eine Rechtsverletzung über den Internetanschluss begangen und daraufhin der Anschluss nicht gesichert wird.

3. Auswirkungen des WLAN-Urteils des EuGH auf das Geschäftsmodell der Stadt Heidelberg *(Heidelberg4you)*

3.1 Geeignetheit der Registrierung der Mobilfunkrufnummer als derzeit praktizierte Sicherungsmaßnahme

Nach den vom EuGH aufgestellten Rechtsgrundsätzen, unter welchen Voraussetzungen Sicherungsmaßnahmen geeignet sind, die Fortsetzung einer Rechtsverletzung zu verhindern, ist das von der Stadt Heidelberg derzeit praktizierte Modell der Registrierung der Mobilfunkrufnummer jedenfalls nicht ungeeigneter als eine Passwortvergabe und Identitätsfeststellung. Denn über eine sogenannte Inverssuche lässt sich der Anschlussinhaber auch bei Eingabe der Mobilfunkrufnummer leicht ermitteln.

3.2 Rechtliche Zulässigkeit der Registrierung der Mobilfunkrufnummer des Nutzers als Sicherungsmaßnahme

Wie zuvor bereits dargelegt *(vgl. D. I. 1.2 lit. b)*, hat der EuGH in seinem WLAN-Urteil übersehen, dass nach den einschlägigen deutschen datenschutzrechtlichen Bestimmungen des TKG/TMG personenbezogene *(Bestands-)* Daten wie die Identitätsfeststellung oder die Anschlusskennung des Nutzers nur im Zuge einer Vertragsbegründung – jedenfalls nicht ohne dessen ausdrückliche Einwilligung - und nur zu den im TKG/TMG genannten

Zwecken erhoben *(verwendet)* werden dürfen, wobei der Nutzer über den Zweck zuvor eingehend zu unterrichten ist.

Die eigentlich wirksame Sicherungsmaßnahme der Protokollierung des Surfverhaltens des Nutzers zwecks nachträglicher Rückverfolgung zu dessen Identität/Anschlusskennung zwecks Verhinderung einer späteren Haftung dürfte danach in jedem Falle gesetzeswidrig sein.

Soweit die von der „*Heidelberg4you*“ bereits jetzt verwendete Software eine Rückverfolgung des konkreten Datenverkehrs des Nutzers zu seiner Anschlusskennung zulässt, ist diese Funktion mit den einschlägigen deutschen datenschutzrechtlichen Bestimmungen daher nicht in Einklang zu bringen.

Im Ergebnis hat dies zur Folge, dass im Falle einer über den Internetanschluss begangenen Urheberrechtsverletzung eine Bestandsdatenauskunft gegenüber dem Rechteinhaber auf Grundlage dieser Datengewinnung unzulässig ist, solange nach außen hin nur eine einzige IP-Adresse des WLAN-Anbieters sichtbar ist. Dies dürfte derzeit noch der Regelfall sein, da angesichts der Knappheit von IPv4-Adressen und der noch äußerst geringen Verbreitung von IPv6-Adressen nach außen hin – im Regelfall – nur eine einzige IP-Adresse des WLAN-Anbieters sichtbar ist. Anders dürfte dies allerdings dann zu beurteilen sein, wenn der WLAN-Anbieter den Nutzer zunächst über die Offenbarung seiner Identität oder einer Anschlusskennung *(Mobilfunkrufnummer)* identifiziert und ihm sodann im Zuge der konkreten Nutzung eine auch nach außen hin sichtbare IPv6-Adresse vergibt. In diesem Falle dürfte eine Bestandsdatenabfrage nach den Regelungen des Telekommunikationsgesetzes und § 101 Abs. 9 Urheberrechtsgesetz zulässig sein, da die Zuordnung einer zu einem bestimmten Zeitpunkt benutzten dynamischen IP-Adresse zu einem *„Anschlussinhaber“* keine Aussage darüber enthält, mit wem der Betreffende worüber und wie lange kommuniziert hat *(BGHZ 185, 330 = NJW 2010, 2061 – Sommer unseres Lebens)*.

3.3 Handlungsempfehlung

Auch wenn die vom EuGH für wirksam erachtete Sicherungsmaßnahme der vorherigen Passwortvergabe und Identitätsfeststellung ohne Protokollierung des Surfverhaltens des Nutzers mit anschließender Zuordnung des Datenverkehrs zur offenbarten Identität des Nutzers ins Leere läuft, sollte sich die Praxis hieran orientieren.

Dies kann allerdings nur in Übereinstimmung mit den einschlägigen deutschen datenschutzrechtlichen Bestimmungen erfolgen.

Da der EuGH zudem ausdrücklich feststellt, dass es dem Diensteanbieter überlassen bleibt, die konkreten Sicherungsmaßnahmen zu bestimmen, dürfte die vorherige Identitätsfeststellung oder die vorherige Registrierung der Anschlusskennung *(Mobilfunkrufnummer)* als gleichwertige Sicherungsmaßnahme anzusehen sein, um den vom EuGH gewünschten Abschreckungseffekt zu erreichen und einer Inanspruchnahme aus Störerhaftung vorzubeugen.

Da die Protokollierung des Surfverhaltens des Nutzers selbst im Falle einer ausdrücklichen Einwilligung nicht protokolliert werden darf, ist allerdings darauf zu achten, dass sowohl bei einer Passwortvergabe und Identitätsfeststellung als auch bei der vorherigen Registrierung der Anschlusskennung *(Mobilfunkrufnummer)* dem Rechteinhaber im Verletzungsfall unter Verweis auf die datenschutzrechtlichen Bestimmungen keine Bestandsdatenauskunft über den konkreten Nutzer erteilt wird. Sollte ein Rechteinhaber aus diesem Grunde die Effektivität der getroffenen Sicherungsmaßnahe im Wege einer Abmahnung anzweifeln, wäre dieser Sachverhalt unter Verweis auf das WLAN-Urteil des EuGH gerichtlich zu klären.

Weiterhin wird angeregt, dass im Zuge der Registrierung entweder der Identität oder der Anschlusskennung *(Mobilfunkrufnummer)* vor Beginn des Nutzungsvorgangs – gegebenenfalls über eine Vorschaltseite – ein Nutzungsvertrag mit dem Nutzer abgeschlossen wird, den der Nutzer gegebenenfalls unter Setzen eines Häkchens bestätigt. In diesem Nutzungsvertrag sollten durchaus auch Regelungen dazu getroffen werden, wonach der Nutzer sich verpflichtet, über den Zugang keine Rechtsverletzungen zu begehen. In den Nutzungsvertrag sind auch die einschlägigen datenschutzrechtlichen Hinweise aufzunehmen.

Sollte die Stadt Heidelberg in der Lage sein, dem Nutzer im Zuge der konkreten Nutzung eine auch nach außen hin sichtbare eigene IPv6-Adresse zu verleihen, darf eine Bestandsdatenauskunft im Verletzungsfall erfolgen.

II. Anbieterpflichten nach dem TKG

Die den Anbieter offener WLANs treffenden Anbieterpflichten nach dem Telekommunikationsgesetz *(TKG)* wurden bereits in dem Erstgutachten ausführlich dargelegt *(Erstgutachten, C. 3.)*.

Auf diese Feststellungen wird verwiesen.

Soweit im Zuge der Diensterbringung personenbezogene Daten *(Bestands- und Verkehrsdaten)* wie z.B. die Identität des Nutzers oder dessen Anschlusskennung gespeichert und verwendet werden, ist ergänzend Nachfolgendes zu beachten:

1. Meldepflicht nach § 6 TKG

Im Hinblick auf die Meldepflicht nach § 6 TKG sind keine ergänzenden Feststellungen zum Erstgutachten zu treffen.

2. Technische Schutzmaßnahmen nach § 109 TKG

Soweit die Stadt Heidelberg *(oder Freifunk)* personenbezogene Daten erhebt, wie z. B. die Anschlusskennung *(Mobilfunkrufnummer)* oder die Identität des Nutzers, sind in dem nach § 109 TKG zu erstellenden Sicherheitskonzept gem. § 109 Abs. 1 Nr. 2 TKG ergänzende technische Vorkehrungen und Schutzmaßnahmen gegen die Verletzung des Schutzes personenbezogener Daten zu treffen. Dabei ist der Stand der Technik zu berücksichtigen. Insbesondere sind Maßnahmen zu treffen, um Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe zu sichern und die Auswirkungen von Sicherheitsverletzungen für Nutzer so gering wie möglich zu halten. In diesem Zusammenhang ist, wie bereits im Erstgutachten festgestellt, ein Sicherheitsbeauftragter zu benennen und ein Sicherheitskonzept zu erstellen, welches auf Verlangen der Bundesnetzagentur vorzulegen ist.

3. Datensicherheit nach § 109 a TKG

Im Zuge der Erhebung personenbezogener Daten, wozu auch die Identität des Nutzers oder dessen Anschlusskennung *(Mobilfunkrufnummer)* zählen, besteht im Fall der Verletzung des Schutzes personenbezogener Daten eine unverzügliche Mitteilungspflicht gegenüber der Bundesnetzagentur *(BNetzA)*, unabhängig von der Schwere der Verletzung. Zu den Einzelheiten wird auf die Feststellungen des Erstgutachtens verwiesen *(Erstgutachten, C. III. 2.3, Seite 25)*.

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

In Bezug auf die Einhaltung des Fernmeldegeheimnisses wird auf die Feststellungen des Erstgutachtens verwiesen *(Erstgutachten, C. III. 2.4, Seite 25)*.

Im Zuge der Erhebung von Bestandsdaten *(Identität des Nutzers oder dessen Anschlusskennung)* sind die entsprechenden gesetzlichen Löschungsfristen zu beachten.

Bestandsdaten sind gem. § 95 Abs. 3 TKG vom Diensteanbieter mit Ablauf des auf die Beendigung des Vertragsverhältnisses folgenden Kalenderjahres zu löschen. Wir gehen davon aus, dass mit Beendigung des Nutzungsvorgangs das Vertragsverhältnis endet.

Wie dargelegt, gehören zu den Bestandsdaten auch die Identität des Nutzers oder dessen Anschlusskennung *(Mobilfunkrufnummer)*. Diese dürfen innerhalb der Löschfristen vorgehalten werden. Sollte dem Nutzer im Zuge der konkreten Nutzung eine eigene IP-Adresse zugeteilt werden, dürfen als Bestandsdaten sowohl diese IP-Adresse, die der IP-Adresse zuzuordnende Identifikation / Anschlusskennung des Nutzers und die Zuordnung selbst gespeichert und im Wege der Bestandsdatenabfrage innerhalb der gesetzlichen Löschungsfristen an den Rechtinhaber auf richterliche Anordnung kommuniziert werden *(Regelung über die Bestandsdatenabfrage, hierzu LG Stuttgart MMR 2005, 624, 628; LG Hamburg MMR 2005, 711; LG Würzburg NStZ-RR 2006, 46; Sankol MMR 2006, 361, 365; hierzu ebenfalls eingehend BGHZ 185, 330 = NJW 2010, 2061 – Sommer unseres Lebens)*.

Wie zuvor dargelegt, ist allerdings aus datenschutzrechtlichen Gründen die Speicherung des Datenverkehrs zwecks Protokollierung des Surfverhaltens der Nutzer unzulässig. Verkehrsdaten *(Nutzungsdaten)* dürfen nach § 97 TKG, § 15 Telemediengesetz *(TMG)* über das Ende des Nutzungsvorgangs hinaus nur zu Abrechnungszwecken gespeichert werden und sind nach einer Frist von 6 Monaten nach Versand der Rechnung zu löschen. Da es sich vorliegend um ein kostenloses Angebot handelt, sind Verkehrsdaten daher unverzüglich nach Beendigung des Nutzungsvorgangs zu löschen.

5. Vorratsdatenspeicherung

Hierzu sind keine ergänzenden Feststellungen gegenüber dem Erstgutachten zu treffen.

6. Telekommunikations-Überwachung nach § 110 TKG

Hierzu kann auf die Ausführungen des Erstgutachtens verwiesen werden *(Erstgutachten, III. 2.6, Seite 29 ff.).*

Ergänzend ist hierzu festzustellen, dass selbst dann, wenn die Stadt Heidelberg zum Kreis der Verpflichteten gehören würde *(Überschreitung eines Nutzerkreises von 10.000 Teilnehmern)* im Rahmen einer konkret angeordneten Überwachungsmaßnahme nur die Bestandsdaten herauszugeben wären, die auch tatsächlich gespeichert wurden.

7. Manuelles Auskunftsersuchen

Sollte angedacht werden, dem Nutzer im Zuge der konkreten Nutzung tatsächlich eine eigene IP-Adresse zu vergeben, könnte dies zur Anwendbarkeit der Verpflichtung in § 111 Abs. 1 S. 1 Nr. 1 – 6 TKG führen, die 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 Auskunft zu erteilen.

Der damit verbundene Aufwand würde gegen ein mögliches Vorhaben sprechen, dem Nutzer im Zuge der konkreten Nutzung eine eigene IP-Adresse zu vergeben.

Düsseldorf, den 13.10.2016
(Mayer)
Rechtsanwalt