Stand: 5. November 2015

Teil 1 – NEU

Ausschussvorlage WVA/19/15 – öffentlich –

Stellungnahmen der Anzuhörenden

zu dem

Antrag
der Abg. Eckert, Frankenberger, Barth, Gremmels, Grüger, Weiß (SPD) und Fraktion betreffend WLAN-Hotspots in Hessen
– Drucks. 19/1900 –

Gemeinsames Konzept der Fraktionen der CDU, der SPD, BÜNDNIS 90/DIE GRÜNEN und der FDP für eine Anhörung im Hessischen Landtag zum Thema „Freie WLAN -Hotspots in Hessen“

1. Rechtliche Rahmenbedingungen

a) Was ist der rechtliche Unterschied zwischen Content-, Host- und Access-Providern und inwiefern ist diese Einordung für WLAN-Betreiber von Bedeutung?

Für die begriffliche Einordnung eines Diensteanbieters ist die Form maßgeblich, in welcher dieser im Internet in Erscheinung tritt: Der Content-Provider stellt eigene Informationen im Internet bereit. Der Host-Provider stellt Dritten Speicherplatz zur Verbreitung von Informationen zur Verfügung. Der Access-Provider ermöglicht den Netzzugang.

Die Unterscheidung zwischen Content-, Host- und Access-Providing ist für Bestehen und Voraussetzungen einer Haftungsprivilegierung nach den §§7 ff. TMG von Bedeutung. Für Content-Provider sieht das TMG keine Haftungsprivilegierung vor. Gemäß §7 Abs. 1 TMG haften diese nach den allgemeinen Gesetzen. Für Host-Provider gilt die Privilegierung gemäß §10 TMG, für Access-Provider die Privilegierung gemäß §8 TMG.

Provider	Zweck der Tätigkeit	Risiko	Privilegierung	Maßnahmen Provider
Content	Bereitstellung eigener Informationen	Content mit entsprechen Markenrecht-Risiken (Landing Page)	Keine Privilegierung	Überwachung durch Markenrechtspezialisten /Juristen
Host	Zur Verfügung Stellung von Speicherplatz	Rechtsverstöße von „Mieter“	Nicht mehr komplett privilegiert	Sorgfaltspflicht bei überprüfen von Neukunden/Kunden
Access	Nur zur Verfügung Stellung des Zugangs	Rechtsverstöße User	Privilegiert (Strafrecht, Schadensersatz, Störerhaftung)	Sorgfaltspflicht mittels Zugangsbeschränkungen oder Verschlüsselung

b) Wann erfahren Access-Provider eine Haftungsprivilegierung?

Die Haftungsprivilegierung für Access-Provider gemäß §8 TMG beruht darauf, dass sich die Tätigkeit des Diensteanbieters auf rein technische, nicht von ihm veranlasste, automatisch ablaufende Vorgänge beschränkt, bei denen er keine Kenntnis von den durchgeleiteten Informationen erlangen oder diese kontrollieren kann.

Gemäß §8 Satz 1 TMG sind Diensteanbieter deswegen nicht verantwortlich für fremde Informationen, die sie in einem Kommunikationsnetz übermitteln oder zu denen sie den Zugang zur Nutzung vermitteln, sofern sie

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

Wenn Diensteanbieter und Nutzer zur Begehung rechtswidriger Handlungen zusammenarbeiten, findet die Privilegierung keine Anwendung.

Die Privilegierung („nicht verantwortlich“) erfasst nach ständiger Rechtsprechung ausschließlich die Haftung des Access-Providers auf Schadensersatz und seine strafrechtliche Verantwortlichkeit. Für

Gemeinsames Konzept der Fraktionen der CDU, der SPD, BÜNDNIS 90/DIE GRÜNEN und der FDP für eine Anhörung im Hessischen Landtag zum Thema „Freie WLAN -Hotspots in Hessen“

Beseitigungs- und Unterlassungsansprüche gilt §8 TMG nicht. Selbst wenn die Voraussetzungen von §8 TMG vorliegen, kann der Access-Provider daher aufgrund einer rechtswidrigen Handlung des Nutzers auf Unterlassung in Anspruch genommen werden, wenn die Voraussetzungen der Störerhaftung erfüllt sind. Die Pflicht zu Beseitigung und Unterlassen kann die Ersatzpflicht des Access-Providers für (Rechtsanwalts-) Kosten einer berechtigten Abmahnung durch den Rechtsinhaber umfassen.

c) Welche Maßnahmen müssen Access-Provider ergreifen, wenn wiederholte Rechtsverletzungen auftreten?

Für Access-Provider besteht auch nach wiederholten Rechtsverletzungen über das bereitgestellte WLAN keine Rechtspflicht, Gegenmaßnahmen zu ergreifen. Zur Vermeidung der Störerhaftung muss der Access-Provider jedoch ihm zumutbare Prüf- und Kontrollmaßnahmen zur Verhinderung von Rechtsverletzungen durchführen, etwa eine Sicherung des WLAN durch Zugangsdaten und eine Belehrung der Nutzer. Die zumutbaren Maßnahmen richten sich nach den Umständen des Einzelfalls. Sind dem Access-Provider wiederholte Rechtsverletzungen über das von ihm bereitgestellte WLAN bekannt, dürften weitergehende Prüf- und Kontrollmaßnahmen zumutbar sein.

d) Welche Haftungsrisiken bestehen derzeit für WLAN-Betreiber, welche der TMG-Privilegierung nicht unterliegen?

Sind die Voraussetzungen des §8 TMG nicht erfüllt, haftet der Access -Provider – auch der Höhe nach – uneingeschränkt nach den allgemeinen Vorschriften. Neben einer Haftung des WLAN-Betreibers (Access-Providers) auf Beseitigung- und Unterlassung (vgl. lit. b)) haftet er dem Inhaber des verletzten Rechts auch auf Schadensersatz, wenn die Voraussetzungen einer gesetzlichen Haftungsnorm erfüllt sind. Die §§7 ff. TMG selbst sind keine Haftungsgrundlagen.

In der Regel setzt eine Haftung auf Schadensersatz zumindest Fahrlässigkeit des WLAN-Betreibers voraus. Fahrlässigkeit kommt etwa in Betracht, wenn dem WLAN-Betreiber Rechtsverletzungen über das von ihm betriebene WLAN bekannt sind, er aber für die Zukunft keine Gegenmaßnahmen ergreift.

e) Welche Haftungsprivilegierungen sind de lege ferenda denkbar?

Denkbar ist ein vollständiger Ausschluss jeglicher Haftung des Access-Providers (inklusive der Haftung auf Beseitigung und Unterlassen) für den Fall, dass sich seine Tätigkeit auf rein technische, nicht von ihm veranlasste, automatisch ablaufende Vorgänge beschränkt, bei denen er keine Kenntnis von den durchgeleiteten Informationen erlangen oder diese kontrollieren kann. Von diesem umfassenden Haftungsprivileg ausgenommen wären neben einem kollusiven Zusammenwirken mit dem Nutzer demnach nur Fälle, in denen der Diensteanbieter

1. die Übermittlung veranlasst;
2. den Adressaten der übermittelten Informationen ausgewählt oder ändert, oder
3. die übermittelten Informationen ausgewählt oder verändert hat.

Denkbar, aber rechtlich nicht zwingend erforderlich ist es, diese umfassende Haftungsprivilegierung an die Erfüllung bestimmter Voraussetzungen (z.B. Identifizierung einzelner Nutzer des WLAN oder Ausschluss einer unberechtigten Nutzung) zu knüpfen.

Gemeinsames Konzept der Fraktionen der CDU, der SPD, BÜNDNIS 90/DIE GRÜNEN und der FDP für eine Anhörung im Hessischen Landtag zum Thema „Freie WLAN -Hotspots in Hessen“

f) Existieren Gründe, zukünftig zwischen privaten und gewerblichen/institutionellen Betreibern zu unterscheiden?

Die Gefahr der Verletzung von Rechten Dritter ist im Bereich privater WLAN-Anbieter wohl höher einzuschätzen als bei gewerblich/institutionell betriebenen WLAN. Das gilt in besonderem Maße, wenn sich private Anbieter anonym für eine gemeinsame Nutzung organisieren können. Andererseits könnte gewerblichen WLAN-Betreibern aufgrund der – möglicherweise mittelbaren – Gewinnerzielungsabsicht wohl ein höheres Haftungsrisiko zugemutet werden. Zwingend erscheint eine differenzierende Behandlung auf dieser Grundlage allerdings nicht. Insgesamt bestehen daher wohl keine durchgreifenden Gründe für eine Unterscheidung von privaten und gewerblichen/institutionellen WLAN-Betreibern.

g) Bestehen neben den zivilrechtlichen Haftungsfragen sicherheitspolitische bzw. strafverfolgungserhebliche Bedenken?

Die Überwachung verdächtiger Personen sowie die Strafverfolgung sind erschwert, wenn sich Personen anonym über offene WLAN in das Internet einwählen können. Dies gilt jedoch bereits nach derzeitiger Rechtslage. Die Möglichkeit zur anonymen Internetnutzung besteht überdies auch außerhalb offener WLAN. Die Risiken sind dem Internet letztlich immanent. The Cloud sieht sich gleichgestellt mit Telekommunikations- und Mobilfunkanbieter und wird strafrechtlichen Behörden in gleichem Umfang wie diese unterstützen. Im Sinne der Strafverfolgung wäre die Identifizierung von Vorteil.

h) Wie ist die strafrechtliche Verantwortlichkeit von Betreibern offener WLAN-Netze einzuordnen im Hinblick auf Beihilfe, Mittäterschaft und (Eventual-)Vorsatz?

Im Rahmen der Privilegierung nach § 8 TMG ist die strafrechtliche Verantwortlichkeit von Betreibern offener WLAN ausgeschlossen. Darüber hinaus richtet sich die strafrechtliche Verantwortung nach allgemeinen strafrechtlichen Grundsätzen.

Eine strafbare Beihilfe des WLAN-Betreibers kommt dabei etwa in Betracht, wenn der WLAN-Betreiber von Straftaten Kenntnis hat, die über das von ihm betriebene WLAN begangen werden, dies jedoch billigend in Kauf nimmt. Mittäterschaft ist denkbar, wenn WLAN-Betreiber und Nutzer bei der Begehung von Straftaten über das WLAN bewusst zusammenwirken. Für den WLAN-Betreiber relevant sind zudem insbesondere Straftatbestände, die fahrlässig verwirklicht werden können.

2. Datenschutz und Datensicherheit

a) Aus welchen Gründen ist es sinnvoll/ nicht Sinnvoll Haftungsprivilegierungen nur für verschlüsselte Verbindungen vorzusehen?

Diese Differenzierung ist nach unserer Auffassung nicht zweckmäßig. Da der Access-Provider lediglich die Verbindung zwischen dem Nutzer und dem von ihm verwendeten Netzwerkgerät (Router) kontrollieren kann, nicht jedoch die Verbindungen des Nutzers „im Internet“, wäre eine solche Differenzierung sachlich wohl nicht zu rechtfertigen.

b) Bedarf es technischer Auflagen für den Betrieb zur Gewährung von Datenschutz- und Datensicherheit? Gibt es allgemeine Standards?

Hierfür gibt es bereits Grundlagen zur Einhaltung Datenschutz und Datensicherheit, die im

TKG § 113 d und g geregelt sind.(Sicherheit der Daten und Sicherheitskonzept)

Gemeinsames Konzept der Fraktionen der CDU, der SPD, BÜNDNIS 90/DIE GRÜNEN und der FDP für eine Anhörung im Hessischen Landtag zum Thema „Freie WLAN -Hotspots in Hessen“

3. Internationaler Vergleich

a) In welchem rechtlichen Rahmen im Hinblick auf zivil- und strafrechtliche Aspekte operieren WLAN-Betreiber im internationalen Vergleich?

In Deutschland gibt es im Verhältnis zum Ausland aktuell wohl sehr wenige offene WLAN Zugangspunkte. Eine Studie des Eco (https://www.eco.de/wp-content/blogs.dir/eco-microresearch_verbreitung-und-nutzung-von-wlan.pdf, dort Ziff. 5) zeigt auf, dass Deutschland im Vergleich zu anderen Ländern eine deutlich geringere WLAN-Verbreitung aufweist, und auf den hinteren Plätzen zu finden ist. Dies sei wohl auf die im Ausland nicht oder weniger verbreitete Störerhaftung zurückzuführen.

b) Welche Erkenntnisse lassen sich hieraus für Deutschland und Hessen ableiten?

Aufgrund der aktuellen Richtlinien die durch die EU hinsichtlich dieser Punkte gesetzt wurden, werden sich die länderspezifischen Gesetzgebungen an diese in Zukunft anlehnen. Dies hat zur Folge, dass voraussichtlich die Vorratsdatenspeicherung in allen EU Ländern gemäß den EU-Vorgaben umgesetzt werden und die Störerhaftung klarer definiert werden wird, oder entfällt.

4. Ausbau

a) Welche Gründe sprechen für und gegen öffentliche Förderung bei Aufbau und/oder Betrieb von WLAN-Netzen?

Für eine öffentliche Förderung spricht die Schaffung der notwendigen Infrastruktur als Voraussetzung einer dauerhaften Inbetriebnahme, da gerade anfängliche, einmalige Fixkosten oftmals als Hinderungsgrund angeführt werden. Weiter sehen wir eine Beratungsförderung von Providern als sinnvoll, da Städte und Kommunen Hilfestellung zu folgenden Fragen benötigen: Wo und in welchen Bereichen ist öffentliches WLAN sinnvoll; welche individuellen Lösungen sind denkbar; auf welche Weise kann WLAN als Marketing-, Kommunikations- und Informationskanal genutzt werden; wer betreibt das WLAN? Eine Förderung des laufenden Betriebs sollte zuvor geklärt werden. Ein langfristiger Betrieb könnte u.U. dadurch gefährdet werden, dass Betriebskosten nach Beendigung der Förderung nicht in Haushalten, bzw. Budgets eingeplant wurden und dennoch getragen werden müssen.

Wir empfehlen daher, die erstmalige Inbetriebnahme (Hardware und Installationsleistungen) zu fördern, da aus unserer Sicht dies die Eintrittshürde ist.

b) Welche Instrumente der Förderung existieren? Welche sind Ihnen bekannt? Welche Formen der Förderung wären denkbar?

Unserer Kenntnis nach existieren derzeit keine gezielten Förderungen für freie WLAN -Hotspots in Hessen. Finanzierungsinstrumente zur Implementierung freier digitaler Lösungen für den Innenbereich in Ladenlokalen, Hotels oder Gaststätten, bietet aktuell die KFW-Bank mit einem Innovations-Kredit für Unternehmen.

Denkbar wären Förderungen zur Implementierung einer flächendeckenden WLAN-Infrastruktur, sowie eine Unterstützung für den laufenden Betrieb.

Gemeinsames Konzept der Fraktionen der CDU, der SPD, BÜNDNIS 90/DIE GRÜNEN und der FDP für eine Anhörung im Hessischen Landtag zum Thema „Freie WLAN -Hotspots in Hessen“

c) Welche Betreibermodelle existieren? Welche Modelle werden am häufigsten gewählt und wie kann man dies erklären?

1. Das öffentliche WLAN betreibt die Stadt

2. Das öffentliche WLAN wird durch stadteigene / stadtnahe Gesellschaft wie z.B Marketing- oder Tourismusverbände gesponsort und von einem Provider betrieben

3. Das öffentliche WLAN betreibt ein Provider in Eigenregie an seinen vorhandenen Standorten (z.B. Verteilerkästen)

Aktuell trifft man vermehrt auf Punkt 3 – der Grund dafür liegt in der Tatsache, dass es grundsätzlich jedem Anbieter frei möglich ist, ein „City -Wifi“ zu eröffnen. Dieses Prinzip führt zu sogenannten „Insellösungen“, bei denen kein flächendeckendes Netz entsteht und damit ein durchweg uneingeschränkter, freier Online-Zugriff für Nutzer nicht möglich ist. Diese Modelle haben keinen echten Mehrwert für Städte, Kommunen und letztendlich auch den Endnutzer, da das Medium WLAN als Kommunikations- und Informationskanal für Städte verloren geht. Die Zusammenarbeit zwischen Provider und Stadt/Kommune muss in jedem Fall gegeben sein, um eine für alle Parteien sinnvolle und mehrwertige Lösung zu schaffen.

In den letzten Monaten setzt sich das Modell aus Punkt 2 eher durch. Dieses Modell folgt bereits etablierten Modellen aus den nordischen Ländern wie Schweden. Der Vorteil hier ist, dass ein klares, kommerzielles Geschäftsmodell mit Flächendeckung für die Bürger erreicht werden kann.

d) Welche Rolle kann das Modell „freifunk“ für den Ausbau des WLAN in Hessen spielen?

Das Modell „Freifunk“ kann für den professionellen Ausbau eines WLAN-Angebotes in Hessen aktuell keine Rolle spielen. Die (Rechts-)Unsicherheit und Umsetzung sind Gründe für diese Einschätzung. Das Modell „Freifunk“ bewegt sich in einer rechtlichen Grauzone, da der gesamte Traffic über Server im Ausland geleitet wird und somit im deutschen Recht keine Anwendung findet. (Umgehung der „Störerhaftung“)

Weiter sehen wir folgende Punkte kritisch:

- Schwankende Geschwindigkeiten
- Qualität der Hardware
- Sicherheit für die Nutzer
- Keine Kindersicherung oder Sperrung von Ports
- Zentrale Infrastruktur (VPN) ermöglicht gezielte Angriffe
- Keine Personenzuordnung durch Ausbleiben des Registrierungs-/Anmeldeverfahrens

Für den öffentlichen/wirtschaftlichen Raum ist es unabdingbar, ein dediziertes WLAN -Netz eines Providers aufzubauen, welches alle rechtlichen und sicherheitsrelevanten Aspekte wahrt, sowie zusammen mit auskunftssuchenden Behörden zukunftssicher arbeitet.

e) Welche Faktoren sind für eine leistungsfähige Versorgung öffentlicher Räume und Plätze mit WLAN von Relevanz?

Grundvoraussetzung stellt eine stabile und sichere Internetverbindung dar, welche im optimalen Fall über Glasfaserkabel gewährleitet wird. Darüber hinaus spielt der Einsatz professioneller Hardware eine wichtige Rolle, welche speziell für den Einsatz im öffentlichen -, respektive Outdoor-Bereich, konzipiert wurde. Weiterhin muss Nutzern und Betreibern ein Ansprechpartner (Support-Hotline) 24

Gemeinsames Konzept der Fraktionen der CDU, der SPD, BÜNDNIS 90/DIE GRÜNEN und der FDP für eine Anhörung im Hessischen Landtag zum Thema „Freie WLAN -Hotspots in Hessen“

Stunden, 365 Tagen im Jahr zur Seite gestellt werden, welcher sich in verschiedensten Sprachen professionell den Anliegen widmet. Zuletzt sollte ein zentrales Remote Management die Qualität sicherstellen.

f) Welche Gründe sprechen für eine Zusammenarbeit der Kommunen, der Städte, der Landkreise und des ÖPNV beim Aufbau eines öffentlichen WLANs? Welche Gründe sprechen dagegen?

Für eine Zusammenarbeit der genannten Stellen spricht, dass auf diese Weise zuvor erwähnte Insellösungen vermieden und ein flächendeckendes WLAN-Angebot bereitgestellt werden kann. Sämtliche Vorteile eines gemeinschaftlichen WLAN-Netzes können so von entsprechenden Stellen genutzt werden. Dieses Modell wird in London und anderen Großstädten bereits erfolgreich umgesetzt.

g) Wer trägt die Kosten für den Aufbau und den Betrieb von WLAN-Netzen?

Die Aufbaukosten können sowohl von der Stadt, vom Provider, als auch von stadtnahen Gesellschaften getragen werden. Ähnlich verhält es sich mit den Betriebskosten. Eine Einbindung der ansässigen Wirtschaft wäre denkbar, wenn eine Implementierung in das öffentliche WLAN-Netz seinesgleichen erfolgt. Zusätzlich wird zur Verdichtung des Netzes der lokale Handel mit einbezogen, der die Verdichtung ohne Einsatz zusätzlicher Mittel für die Stadt ermöglicht. Dieses Modell wird in London und Berlin verfolgt.

5. Wirtschaftliche Bedeutung und Effekte

a) Welche Nutzen haben Städte und Gemeinden durch freie öffentlich zugängliche WLAN-Netze?

- Aufwertung des Stadtzentrums durch eine neue Online-Erlebniszone
- Nutzung der bestehenden Infrastruktur für stadteigene Zwecke (z.B. Kameraüberwachung)
- Innovation und Modernisierung – Die digitale Mobilität der Bürger wird verbessert
- Erhöhung der Lebensqualität für Bürger und der Aufenthaltsqualität für Besucher
- Stärkung des stationären Handels/Gastronomie/Dienstleister durch Einbindung in ein flächendeckendes WLAN-Netz
- Steigerung der Attraktivität für Touristen und Besucher
    - Finanzieller Nutzen für ausländische Touristen, da Roaming-Kosten entfallen
- Registrierungs-/Anmeldefenster sollte durch zusätzliche Informationen (zu kulturellen Veranstaltungen, bevorstehende Events, digitale Stadtpläne, etc.) einen Mehrwert für Besucher darstellen.

b) Haben freie öffentlich zugängliche WLAN-Netze auch für die Tourismuswirtschaft eine Bedeutung?

Wir sehen einen zentralen Nutzen für die Tourismuswirtschaft. Internationale Besucher erwarten ein flächendeckendes WLAN-Angebot, welches im optimalen Falle mit einer mehrsprachigen Touristeninfo gekoppelt ist. Zusätzliche Informationen für Touristen (Stadtplan, Informationen zu Sehenswürdigkeiten, etc.) bilden darüber hinaus einen Mehrwert und steigern die Attraktivität.

Gemeinsames Konzept der Fraktionen der CDU, der SPD, BÜNDNIS 90/DIE GRÜNEN und der FDP für eine Anhörung im Hessischen Landtag zum Thema „Freie WLAN -Hotspots in Hessen“

Ein gutes Beispiel hierfür ist die Stadt Passau, die den Tourismusgedanken im Vordergrund hatte, und somit eine Kooperation zwischen Stadt, Stadtwerken und dem Provider eingeführt hat.

c) Welchen Nutzen haben andere Wirtschaftssektoren und Branchen durch frei öffentlich zugängliche WLAN-Netze?

Durch den Service „kostenfreies WLAN“ steigt die Attraktivität und Urbanität der Innenstädte. Somit profitieren alle Innenstadtrelevanten Akteure wie Handel, Gastronomie, Einkaufscenter, aber auch Unternehmen, bzw. deren Mitarbeiter vom Angebot.

Der Service sollte gleichermaßen „Outdoor“ (auf Straßen, Plätzen) wie auch „Indoor“ (innerhalb der Ladenlokale, Hotels, Restaurants) angeboten werden. Hierbei sollte der Ladeninhaber technologisch unabhängig von seinem Internetprovider die Möglichkeit haben, sich an das Stadtnetz mit anzuschließen und/oder zusätzlich seine lokalen POS zu vermarkten.

d) Sind Auswirkungen auf (lokale) Telekommunikationsbetreiber zu erwarten, die inzwischen Vergleichbare Leistungen (z.B. LTE) im Rahmen von Nutzerverträgen gegen Rechnung zur Verfügung stellen?

LTE stellt aus unserer Sicht keine vergleichbare Leistung dar und steht somit nicht in Konkurrenz zu einem flächendeckenden WLAN-Angebot. Öffentliches -WLAN sollte als Kommunikations- und Informationskanal der Städte angesehen werden, um hierdurch Besucher, Touristen und Bürger zu erreichen und zu informieren. Weiterhin stellt ein öffentliches WLAN als Service sicher, dass die Geschwindigkeit der Verbindung und die Datenvolumen für alle Nutzer in einem hohen Maße gegeben sind.

e) Was ist beim Aufbau eines öffentlich geförderten und/oder betriebenen WLAN -Netzes im Hinblick auf das Wirtschaftsverwaltungsrecht zu beachten, wenn bestehende WLAN-Angebote (z.B. durch die Telekom) bestehen?

Aus Providersicht keine Einschränkung, hinsichtlich des Wirtschaftsverwaltungsrecht ist uns keine Stellungnahme möglich.

6. Förderprojekte im Bundesvergleich

a) Welche staatlich geförderten Projekte existieren derzeit in Deutschland?

Uns sind nur Teilprojekte aus Berlin bekannt, die aber mediengetrieben sind/waren und somit nicht zur erwünschten WLAN-Abdeckung geführt haben.

Arbeitsgemeinschaft
Hessen

Arbeitsgemeinschaft hessischer Industrie- und Handelskammern | 60284 Frankfurt

Hessischer Landtag
Ausschuss für Wirtschaft, Energie,
Verkehr und Landesentwicklung
Herrn Clemens Reif
Postfach 3240
65022 Wiesbaden

Ihr Zeichen, Ihre Nachricht vom	Unser Zeichen, unsere Nachricht vom	Telefon	Frankfurt am Main
IA 2.2	ARGE-Ziff. 6	069 2197-1384	02.11.2015

Stellungnahme: Freie WLAN-Hotspots in Hessen

Sehr geehrter Herr Reif,

Zu Antrag Nr. 1
Dank Smartphones und Tablets ist es heutzutage normal geworden, mal kurz seine E-Mails zu checken oder im Internet zu surfen. Da aber bei den meisten Tarifen die Geschwindigkeit ab einem gewissen Daten-Volumen radikal gedrosselt wird, sind öffentliche WLAN-Hotspots zur Schonung des eigenen Daten-Volumens beliebt. Während in vielen europäischen Ländern der öffentliche Zugang zum Internet weit verbreitet ist, hapert es in Deutschland aber daran.

Von einem Ausbau würden indes alle profitieren, da immer mehr Lebensbereiche digitalisiert werden. Heute sind nicht nur die Jüngeren „always online", sondern zunehmend alle Teile der Bevölkerung. Daher steigt auch die Erwartungshaltung der Nutzer. Stehen sich zwei ansonsten gleichwertige Angebote gegenüber, zieht das Angebot ohne freies WLAN häufig den Kürzeren (v.a. im Beherbergungs-Gewerbe, Gaststätten oder Einkaufszentren). Daher bietet der Ausbau von öffentlichen WLAN-Hotspots in der Tat für die wirtschaftliche und touristische Entwicklung Potenziale.
Man sollte das Ausmaß von WLAN-Hotspots im Auge behalten, da diese nur eine geringe technische Reichweite haben, somit viele einzelne notwendig sind. Darüber hinaus ist es ökonomisch nur sinnvoll, wo viele Nutzer gleichzeitig im Netz sind.
Die Diskussion WLAN-Hotspots darf die oberste Priorität eines flächendeckenden kabelgebundenen Breitbandausbaus nicht behindern. Der Ausbau des WLAN-Netzes muss bedarfsorientiert erfolgen und dem Prinzip privater Anbieter vor kommunalem Betreiber erfolgen.

Geschäftsführung:
Industrie- und Handelskammer Frankfurt am Main
Börsenplatz 4
60313 Frankfurt

Telefon: 069 2197-1384
Telefax: 069 2197-1448
info@ihk-hessen.de
www.ihk-hessen.de

Zu Antrag Nr. 2
Aus Sicht der ARGE Hessen ist aber die Landesregierung der falsche Ansprechpartner für das Thema. Die wesentlichen Regeln trifft das Telemediengesetz (TMG). Die Vorschrift ist Bundesrecht, auf das die Landesregierung über den Bundesrat nur sehr geringen Einfluss hat.

Zu Antrag Nr. 3
Aktuell existiert bereits ein Novellierungs-Vorschlag zum TMG. Dieser wurde bereits durch das Bundeskabinett verabschiedet. Allerdings hapert es aus Sicht der gesamten IHK-Organisation an der angekündigten Rechtssicherheit.

Was z.B. sind die im Gesetz-Entwurf genannten "angemessene Sicherungsmaßnahmen"? Wann ist ein Verfahren nicht mehr als sicher einzustufen? Anfangs galten die Verschlüsselungs-Verfahren WPS und WPA als sicher. Schon lange weiß man, dass so gesicherte Netzwerke mit der heutigen Rechenleistung leicht zu knacken sind. Dennoch bietet jeder WLAN-Router diese Verfahren noch an und viele WLANs sind heute noch unzureichend gesichert. Ebenso ist höchst fraglich, wie die Zusicherung des Nutzers, keine Rechtsverletzung zu begehen, konkret auszusehen hat und wie sie zu dokumentieren ist.

Hier fordert die IHK-Organisation wie viele weitere Kritiker auch, diese wesentlichen Punkte im Gesetz-Entwurf selbst zu regeln statt sie der späteren Rechtsprechung zu überlassen.

Zielführend für eine größere WLAN-Abdeckung ist die Schaffung von Rechtssicherheit in den aufgeführten Fragen des Haftungsrisikos von WLAN-Betreibern. In allen Fällen muss die Einschränkung der Störerhaftung entfallen.

Zu Antrag Nr. 4
Im Gesetzgebungsverfahren wurde bereits die ursprünglich vorgesehene Differenzierung zwischen privaten und öffentlichen Anbietern fallengelassen. Eine einheitliche Regelung für öffentliche und private, kommerzielle und nicht-kommerzielle Anbieter ist damit noch nicht verbunden. Das ist aber nur auf dem Papier der Fall. Denn sieht man sich die konkreten Anforderungen des Gesetz-Entwurfs an, werden nur professionelle Anbieter technisch in der Lage sein, die angemessenen Sicherungsmaßnahmen und die Einwilligung des Nutzers ordnungsgemäß einzuholen und auch rechtssicher zu dokumentieren. Entsprechende Ticket-Systeme sind bereits heute im Einsatz, sind aber mit erheblichen Kosten und Installations- und Pflege-Aufwand verbunden. Daher ist nicht zu erwarten, dass private Anbieter aufgrund des neuen Gesetz-Entwurfs ihr privates WLAN bereitwilliger als bisher öffentlich machen werden. Zu groß ist nach wie vor die Gefahr, wegen einer (vermeintlichen) Urheberrechts-Verletzung abgemahnt zu werden.

Ganz abzulehnen ist schließlich die sogar vorgesehene Verschärfung der Haftung sog. „gefahrgeneigter Dienste“ (§ 10 TMG n.F.). Die Erfahrung zeigt, dass entsprechende

IHK Arbeitsgemeinschaft Hessen

Tauschbörsen zumeist im Ausland angesiedelt sind und sich dort dem Zugriff der Behörden zu entziehen versuchen. Gegenüber inländischen Anbietern bietet die aktuelle Rechtslage ausreichende Zugriffsmöglichkeiten.

Zu Antrag Nr. 5
Wenn der Hessische Landtag mit gutem Beispiel vorangeht, ist das aus Sicht der ARGE Hessen zu begrüßen. Denn das Anbieten von freiem WLAN ist auch ein Zeichen einer modernen, bürgernahen Verwaltung.

Mit freundlichen Grüßen

Arbeitsgemeinschaft hessischer
Industrie- und Handelskammern

Matthias Gräßle
Geschäftsführer

Industrie- und Handelskammer
Offenbach am Main
Geschäftsbereich Standortpolitik

Frank Achenbach
Federführer

Tobias Hachmer
Freifunk Wiesbaden
Blücherstraße 26
65195 Wiesbaden

Hessischer Landtag
Postfach 3240
z.H. Frau Claudia Lingelbach
65022 Wiesbaden

02.11.2015

Stellungnahme zum Antrag "Freie WLAN-Hotspots in Hessen" in der Drucksache 19/1900

Sehr geehrte Damen und Herren,

wir sind als Freifunk Wiesbaden angeschrieben und gebeten worden eine schriftliche Stellungnahme bzgl. des oben genannten Antrags abzugeben. Im vorliegenden Antrag geht es jedoch um WLAN-Hotspots in ganz Hessen. Aus diesem Grund haben wir auch die Freifunk Communities in Hessen gebeten, an dieser Stellungnahme mitzuwirken.

Freifunk Communities aus Hessen:

- **Butzbach** *(im Aufbau)* - https://www.freifunk-butzbach.de
- **Darmstadt** (unterstützt durch Chaos Darmstadt e.V.) - https://darmstadt.freifunk.net
- **Frankfurt** (unterstützt durch Freifunk Frankfurt am Main e.V.) http://www.wifi-frankfurt.de
- **Fulda** (unterstützt durch Magrathea Laboratories e.V.) https://fulda.freifunk.net
- **Gießen** Webseite: http://giessen.freifunk.net
- **Kassel** (unterstützt durch flipdot e.V.) - https://www.freifunk-kassel.de
- **Kelsterbach** (Freifunk Kelsterbach e.V. aktuell noch in Gründung) - http://www.freifunk-kelsterbach.de
- **Marburg** (unterstützt Rechenkraft.net e.V.) https://hsmr.cc/Wifi/Freifunk
- **Wiesbaden** (unterstützt durch Chaos Computer Club Mainz e.V. / Freifunk Mainz e.V.) http://wiesbaden.freifunk.net

Die Freifunk Communities in Hessen begrüßen den Antrag in der Drucksache 19/1900 der Abg. Eckert, Frankenberger, Barth, Gremmels, Grüger, Weiß (SPD) und Fraktion betreffend WLAN-Hotspots in Hessen in allen 5 Punkten. Wir würden uns freuen, zunehmend mit dem Land Hessen und auch den einzelnen Kommunen zusammenzuarbeiten, um eine größere Abdeckung von offenen WLAN-Zugängen in allen Regionen Hessens zu erreichen.

Die Arten der Zusammenarbeit und auch Unterstützung/Förderung durch Land und Kommunen können folgendermaßen aussehen:

- Ideelle Anerkennung von Freifunk als förderwürdige Initiative
- Schaffung freier WLAN-Netze in öffentlichen Gebäuden
- Förderung beim Ausbau des WLAN-Backbones durch Zugang zu Dächern öffentlicher Liegenschaften zwecks Installation von Richtfunk-Geräten
- Unterstützung durch die öffentliche Hand bei handwerklichen Arbeiten, z.B. elektrotechnischer Leitungsverlegung, Erfüllung von Brand-, Blitz- und Denkmalschutzauflagen
- Nicht-finanzielle Zuwendungen in Form von IP-Netzen

Vgl. 4 b) des Fragenkatalogs.

Im Folgenden werden wir zunächst unsere Initiative beschreiben und anschließend auf die Fragen im Fragenkatalog eingehen.

Was ist Freifunk und was zeichnet Freifunk aus?
Freifunk ist eine nicht-kommerzielle Bürgerinitiative für freie Funknetzwerke, die zum Ziel hat, ein freies Funknetzwerk aufzubauen, das für jeden gleichermaßen offen zugänglich und erweiterbar ist. In Deutschland existieren aktuell mehr als 200 Freifunk-Communities, die bereits über 22.000 offene WLAN-Zugänge aufgebaut haben. Davon befinden sich 9 Freifunk-Communities mit über 900 WLAN-Knoten in Hessen.

Freifunk ist sozial und hat einen Bildungsauftrag.
Es werden regelmäßige Treffen veranstaltet, auf denen Interessierten die Freifunk-Idee erläutert wird. Wir zeigen Möglichkeiten des Partizipierens auf und führen vor, wie einfach ein handelsüblicher Router zum Freifunk-Knoten werden kann. Wir erklären die Technik dahinter und bilden technische Laien und Experten.
So werden neue Kontakte geknüpft und Hilfe zur Selbsthilfe gegeben. Die Möglichkeiten zum Mitmachen sind vielseitig. Angefangen beim einfachen Nutzer des offenen WLANs über Betreiber eigener Freifunk-Knoten bis hin zum Engagement in der Entwickler-Community. Darüber hinaus sensibilisieren wir Menschen als mündige digitale Bürger im Umgang mit offenen WLAN-Netzwerken, insbesondere in Hinblick auf die digitale Sicherheit und informationelle Selbstbestimmung.

Freifunk hat Forschungscharakter.
Unter den Freifunkern sind Menschen aus den verschiedensten Berufen mit breitgefächertem und tiefgehendem sozio-technischem Knowhow. Die Technik hinter Freifunk, vor allem die verwendeten Netzwerk-Protokolle (Mesh-Protokolle), sowie die Software, die auf den Freifunk-Knoten läuft, wird stetig weiterentwickelt und verbessert. Oftmals werden auch gänzlich neue Wege eingeschlagen und mit neuen, teilweise selbst entwickelten Protokollen und Software-Bestandteilen experimentiert.

Freifunk fördert Innovation
Die in der Freifunk-Infrastruktur verwendeten Protokolle und Firmware werden unter freien Lizenzen entwickelt. Die Herausforderung eine alternative Netzwerkinfrastruktur von Bürgern für Bürger mit kostengünstiger Hardware zu erstellen, erfordert die Entwicklung neuer Technologien. Freifunk Netzwerke bieten eine Umgebung für die Entwicklung von resilienten und flexiblen Netzwerkprotokollen im Bereich des Routing und der sicheren Datenübertragung.
Stadtübergreifende Freifunk-Netze mit sicheren, quelloffenen Sicherheitsprotokollen und Firmware bieten eine Grundlage für die Entwicklung neuer Technologien z.B. im Bereich IoT (Internet of Things). Jede Kommune und Stadt können verbraucher- und bürgerfreundliche Smart Cities und Smart Villages werden, ohne sich an einzelne kommerzielle Unternehmen zu binden. Sensible Datenströme könnten zukünftig lokale Wege nutzen, ohne auf internationale Routen im Internet angewiesen zu sein.

Freifunk ist mehr als "nur" ein Zugang zum Internet.
Alle Freifunk-Knoten sind untereinander zu einem gemeinsamen Netzwerk verbunden. In diesem Netzwerk kann jeder Teilnehmer uneingeschränkt mit jedem anderen kommunizieren, z.B. einfach Daten austauschen, telefonieren, etc. Aus diesem Netzwerk steht auch ein Übergang zum Internet zur Verfügung. Das Internet wird als ein Dienst unter vielen angesehen. Es ist möglich im Freifunk-Netzwerk eigene Dienste bereitzustellen, z.B. Webseiten, Dateiablagen, Spiele-Server, Wissensdatenbanken, freie soziale Netzwerke, etc.

Freifunk ist nicht kommerziell.
Freifunk arbeitet nicht kommerziell. Demnach gibt es keine kommerzielle Firma hinter Freifunk. Alle aktiven Freifunker arbeiten ehrenamtlich. Die Freifunk Communities sind zunächst einfache Gruppierungen von Menschen/Bürgern, die zusammen an dem Freifunk-Netzwerk arbeiten. Viele dieser Gruppierungen haben einen Verein gegründet oder arbeiten mit einem bestehenden Verein zusammen, die oft als gemeinnützig anerkannt sind oder dies noch anstreben. Welche Community wie unterstützt wird, ist der obigen Liste zu entnehmen.
Das Gesamtnetz gehört der Gemeinschaft, jeder einzelne Knoten befindet sich in unterschiedlichem Besitz sowie individueller Betriebshoheit.

Freifunk praktiziert Netzneutralität und Datensparsamkeit.
Wir setzen uns stark für Datensparsamkeit und informationelle Selbstbestimmung ein. Aus diesen Gründen gibt es in Freifunk-Netzwerken z.B. keine Registrierungs- oder Anmeldepflichten.
Netzneutralität wird großgeschrieben, es findet keinerlei Eingriff in die über ein Freifunk-Netzwerk übertragenden Daten statt. Die Umleitung eines Freifunk Nutzers auf eine Anmelde- bzw. Einstiegsseite (genannt Splash-Page) unmittelbar nach der Herstellung der WLAN-Verbindung findet nicht statt.
Solche Manipulationen stellen einen technischen Eingriff in den Datenverkehr dar und verletzen die Netzneutralität. Im Einklang mit den Datenschutzgesetzen, speichert Freifunk keine Nutzer-Daten, weil diese für den Betrieb eines freien WLAN-Netzes nicht erforderlich sind.

Freifunk ist unabhängig.
Aller Anfang ist schwer. Zu Beginn eines Freifunk-Netzes existieren nur wenige freie Router. Sukzessive stellen andere Freifunker an verschiedenen Orten weitere Freifunk-Knoten auf. Zunächst stellen diese einzelne isolierte WLAN-Hotspots dar. Freifunk Router besitzen aber die Fähigkeit, sich automatisch zu sogenanneten Mesh-Netzen zusammenzuschließen. So entstehen anfänglich lokale Inseln, welche untereinander nicht in Funk-Reichweite zueinander stehen. Mit Hilfe des Internets und einer VPN-Technologie werden diese fragmentierten nachbarschaftlichen Netze zuerst über sogenannte Freifunk-Gateways im Internet untereinander verbunden.
Anfänglich ist dieses unscheinbare Funknetz stark abhängig vom Internet. Nach und nach, um so höher die Knoten-Dichte einer Stadt steigt, desto mehr wachsen die verteilten Inseln auch direkt per Funk zusammen.
Das Ziel ist es, alle Freifunk-Router unabhängig von Internet Service Providern über Mesh-Technologie miteinander zu verbinden. Dazu bauen wir insbesondere sogenannte WLAN-Backbones mit Richtfunk auf hohen Dächern und Türmen auf. Mit Hilfe dessen können wir die WLAN-Inseln über Richtfunk miteinander verbinden, die Abhängigkeit an das Internet fällt dann weg. Auch weit entfernte Regionen können über Richtfunk-Strecken an das WLAN-Backbone angeschlossen und somit mit freiem Netzwerk versorgt werden.

Weiterführende Links zum Thema Freifunk:

- **Freifunk Vision:** https://freifunk.net/worum-geht-es/vision/
- **Häufige Fragen:** https://freifunk.net/worum-geht-es/haufige-fragen/
- **Technik der Community Netzwerke** https://freifunk.net/worum-geht-es/technik-der-community-netzwerke/
- **Gemeinsames Grundverständnis:** http://blog.freifunk.net/2015/memorandum-understanding

Mit freundlichen Grüßen,
die Freifunk Communities in Hessen

Nachfolgend gehen wir im Einzelnen auf Ihre Fragen im Fragen-Katalog ein:

1. Rechtliche Rahmenbedingungen

a) Was ist der rechtliche Unterschied zwischen Content-, Host- und Access-Providern und inwiefern ist diese Einordung für WLAN-Betreiber von Bedeutung?

Die rechtlichen Unterschiede zwischen Content-, Host- und Access-Providern sind in §§ 8-10 TMG geregelt. Freifunker und Betreiber einzelner WLAN-Knoten sind als Access-Provider einzuordnen. Nach dem sog. Providerprivileg haften sie somit auch generell nicht für durchgeleiteten Datenverkehr. Vgl. 1. b).

b) Wann erfahren Access-Provider eine Haftungsprivilegierung?

Grundsätzlich durch die Art der tatsächlichen Tätigkeit, der Vermittlung zu Informationen in einem Kommunikationsnetz nach § 8 Abs. 1 TMG. Accessprovider sind haftungspriviligiert, sofern sie nicht in den Datenverkehr eingreifen und insgesamt eine neutrale Rolle einnehmen.

Wir weisen auch darauf hin, dass eine Meldepflicht bei der Bundesnetzagentur nicht zwangsläufig für alle TK-Anbieter gegeben ist (vgl. Amtsblattmitteilung 149/2015 der Bundesnetzagentur) und eine Meldung bei der BNetzA nur informativen Charakter hat. Die Bundesnetzagentur schreibt hierzu:

"Die Meldepflicht hat in erster Linie zum Ziel der Bundesnetzagentur eine Marktbeobachtung und die Beurteilung des Wettbewerbs zu ermöglichen. Die Aufnahme ins Melderegister ist weder eine Genehmigung noch ein (begünstigender) Verwaltungsakt. Einer Bescheinigung nach § 6 Abs. 3 TKG fehlt jeglicher eigenständiger Regelungsgehalt. Sie hat nur informatorischen Charakter und gibt lediglich die sich unmittelbar aus dem Gesetz ergebende Rechtslage wieder. Beispielsweise gilt ein Unternehmen durch Angabe einer Meldung nicht bereits als Internetserviceprovider. Insbesondere erlaubt eine Eintragung in das Melderegister nicht Rückschlüsse auf die tatsächlichen Rechte und Pflichten des gemeldeten Unternehmens. Diese ergeben sich aus der tatsächlichen Tätigkeit des gemeldeten Unternehmens."

c) Welche Maßnahmen müssen Access-Provider ergreifen, wenn wiederholte Rechtsverletzungen auftreten?
Die Haftungsprivilegierung für Access-Provider gilt nach unserem Kenntnisstand unabhängig von der Zahl der Nutzer und eventuellen Rechtsverletzungen. Es ist bisher nicht bekannt, dass Access Providern bestimmte Pflichten auferlegt worden sind.

d) Welche Haftungsrisiken bestehen derzeit für WLAN-Betreiber, welche der TMG-Privilegierung nicht unterliegen?
Es besteht die Gefahr, wegen möglicher Rechtsverletzungen der Nutzer auf Unterlassung in Anspruch genommen und abgemahnt zu werden. Dieses rechtliche, kaum sicher abschätzbare Risiko stellt ein häufig genanntes Hindernis für WLAN-Betreiber dar. Auch potentielle Freifunker die gerne mitmachen und einen Knoten aufbauen möchten, werden verunsichert, weshalb sich teilweise technische Lösungen etabliert haben, welche die Rechtsunsicherheit beseitigen.

e) Welche Haftungsprivilegierungen sind de lege ferenda denkbar?
*Jed*er Betreiber eines WLAN-Knotens sollte von der Haftung für Rechtsverletzungen durch seine Nutzer - unter den bisherigen Voraussetzungen von § 8 TMG - freigestellt werden.
Der bekannt gewordene Entwurf der Bundesregierung zur Änderung des TMG hat bereits jetzt für erhebliche Unsicherheit bei Freifunkern gesorgt. Die darin vorgesehenen zusätzlichen Pflichten (Verschlüsselung, Vorschaltseite) sind nicht geeignet, Rechtsverletzungen zu verhindern.

f) Existieren Gründe, zukünftig zwischen privaten und gewerblichen/institutionellen Betreibern zu unterscheiden?
Eine Unterscheidung ist nicht sinnvoll und nicht praktikabel, weil diese zu Unsicherheiten führt, welche die Verbreitung freier WLAN-Zugänge sehr stark hemmt.

g) Bestehen neben den zivilrechtlichen Haftungsfragen sicherheitspolitische bzw. strafverfolgungserhebliche Bedenken?
Spezielle sicherheitspolitische oder strafverfolgungserhebliche Bedenken bestehen aus unserer Sicht nicht. Eine anonyme/pseudonyme Internetnutzung ist auch bei anderen WLAN-Netzen möglich (z.B. DB Lounge von Telekom, mycloud in Einkaufszentren) oder durch VPN-Anbieter, die eine Anonymisierung im Netz bieten.
Man könnte anführen, dass Freifunk auch aus sicherheitspolitischer Perspektive zu befürworten sei. Schließlich sorgt Freifunk mit eigener Firmware für sichere und dezentrale Netze und stärkt damit im Einklang mit der Digitalen Agenda der Bundesregierung die technologische Souveränität.
Auch die kontinuierliche Open Source-Weiterentwicklung der Routerfirmware sorgt dafür, dass die Router gepflegt und mit Sicherheitsupdates versorgt werden, wodurch die IT-Sicherheit insgesamt gestärkt wird. Den Bedarf, die IT-Sicherheit von Heim-Routern zu verbessern, hat inzwischen auch das Bundesamt für Sicherheit in der Informationstechnik erkannt und entwickelt zurzeit ein Testkonzept: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Testkonzept-Breitbandrouter.pdf;jsessionid=95D96642D35DF474C87D5D22E2E871F0.2_cid359?__blob=publicationFile

h) Wie ist die strafrechtliche Verantwortlichkeit von Betreibern offener WLAN-Netze einzuordnen im Hinblick auf Beihilfe, Mittäterschaft und (Eventual-)Vorsatz?
Es sollten die gleichen Regeln wie in anderen Infrastrukturbereichen (z.B. bei Nutzungsangeboten des ÖPNV oder des Straßennetzes) gelten.

Der Betreiber eines Freifunk-Knotens hat keine Kenntnis von den Handlungen der Nutzer, genauso wenig wie z.B. die Telekom auch. Eine vorsätzliche Mitwirkung des Betreibers an möglicherweise rechtswidrigen Handlungen der Nutzer liegt nicht vor.

2. Datenschutz und Datensicherheit

a) Aus welchen Gründen ist es sinnvoll/ nicht Sinnvoll Haftungsprivilegierungen nur für verschlüsselte Verbindungen vorzusehen?
Eine Verschlüsselung öffentlicher WLANs ist nicht praktikabel, da sie Nutzer per se ausschließt. Öffentliche WLANs (z.B. Freifunk) sollen sich aber an jeden richten. Sichere "verschlüsselte Verbindungen" sind immer Ende-zu-Ende verschlüsselt (z.B. https): Also vom Endgerät des Nutzers, am WLAN-Access-Provider vorbei, bis zum Server des Content-Providers. Andere Arten von Verschlüsselung (z.B. WPA2) sind in öffentlichen WLANs angreifbar. Eine Verschlüsselung hindert Nutzer, die den Schlüssel kennen und im WLAN eingeloggt sind, nicht an der Begehung von Rechtsverletzungen. Eine diskriminierende Haftungspriviligierung halten wir daher nicht für sinnvoll.

b) Bedarf es technischer Auflagen für den Betrieb zur Gewährung von Datenschutz- und Datensicherheit? Gibt es allgemeine Standards?
Bereits heute gibt es Regelungen für Datenschutz und Datensicherheit, die sich aus dem TKG ergeben (§§ 91 ff. TKG und insbesondere § 109 TKG). Spezieller technischer Auflagen bedarf es daher nicht. In Freifunk-Netzen wird dem Datenschutz insbesondere durch die Beachtung des Grundsatzes der Datenvermeidung und Datensparsamkeit Rechnung getragen.

- §3a BDSG: Datenvermeidung und Datensparsamkeit

3. Internationaler Vergleich

a) In welchem rechtlichen Rahmen im Hinblick auf zivil- und strafrechtliche Aspekte operieren WLAN-Betreiber im internationalen Vergleich?

Die Störerhaftung ist eine weltweite Besonderheit die so in keinem anderen Land existiert und als deutscher Standort Nachteil angesehen werden muss. Die Abdeckung mit offenen WLAN-Zugängen in Ländern wie dem Vereinigten Königreich oder den USA, die keine Störerhaftung kennen, ist um ein Vielfaches höher als in Deutschland. Gleichwohl kommt es dort nicht zu massenhaften Urheberrechtsverstößen über offene Funknetze. Im Europäischen Vergleich können das freie Funknetz Guifi in Spanien mit über 46.000 Knoten oder Athens Wireless Metropolitan Network (AWMN) als vorbildhaft gesehen werden. Die digitale Agenda 2020 der EU Kommission meint: „Systeme, bei denen die Verbraucher ihr eigenes Wi-Fi-Netz mit anderen teilen, sind ein gutes Beispiel dafür, wie wir alle gemeinsam ein besseres Internet für alle erreichen können. Alle Menschen in Europa sollten die Möglichkeit haben, ins Internet zu gelangen, auch wenn sie gerade nicht zu Hause oder am Arbeitsplatz sind".

b) Welche Erkenntnisse lassen sich hieraus für Deutschland und Hessen ableiten?

- *Wirtschaftlicher Standortnachteil wenn nicht gefördert wird. Vgl. eco-Verbands Studie (2014): Verbreitung und Nutzung von WLAN, WLAN-Zugangspunkten sowie Öffentlicher Hotspots in Deutschland* https://www.eco.de/wp-content/blogs.dir/eco-microresearch_verbreitung-und-nutzung-von-wlan.pdf
- *USA Vergleich!* http://www.spiegel.de/netzwelt/web/keine-w-lan-stoererhaftung-in-den-usa-a-855563.html

4. Ausbau

a) Welche Gründe sprechen für und gegen öffentliche Förderung bei Aufbau und/oder Betrieb von WLAN-Netzen?

Chancen

- Die öffentliche Förderung des Aufbaus und Betriebs von freien WLAN-Netzen liegt im staatlichen Interesse. Bürgerschaftliche WLAN-Infrastrukturen mit barrierefreien, einfachen Zugängen zu Informationen sind förderwürdig, weil sie das Gemeinwohl mehren. Nur solche kostenfrei nutzbaren WLAN-Netze ohne aufwendiges Anmeldeverfahren sind ohne deutsche Sprachkenntnisse und mit geringem Einkommen zugänglich. Neben dem allgemein bekanntem touristischen und damit wirtschaftlichem Mehrwert für Geschäftsleute bietet sich so u.a. für Flüchtlinge und sozial benachteiligte Personen die Chance zur digitalen Teilhabe. Freies WLAN im Wartebereich von Ämtern kann z.B. helfen, um sich zu informieren und so behördliche Prozessabläufe zu verbessern.

- Besonders förderwürdig ist der Aufbau dezentraler stadtweiter WLAN-Netze (sog. "Mesh-Netze"), weil diese unabhängig vom Internet lokal funktionieren. Nicht nur im Katastrophenfall sind sie wertvolle resilente Ressourcen, die erforscht und erprobt werden sollten. Solche WLAN-Netze können unabhängig von internationalen Routen sichere und schnelle Kommunikation ermöglichen. Die Medienanstalt Berlin Brandenburg nutzt z.B. vorbildhaft freie Funknetze, um kostengünstig breitbandiges Bürgerfernsehen anzubieten.

- Der Breitbandausbau auf dem Land und außerhalb kommerziell interessanter Innenstadtbereiche bedarf einer gezielten öffentlichen Förderung, weil hier marktwirtschaftlich kaum Investitonsanreize bestehen. Gemeinnützige WLAN-Bürgernetze stellen hier eine kostengünstige Lösung dar, die digitale Spaltung zu verhindern.

Gefahren

- Gegen den Betrieb zentraler WLAN-Netze durch Behörden, oder die Subventionierung kommerzieller Hotspot-Monopolisten, spricht die Gefahr der Etablierung antidemokratischer Überwachungsstrukturen und verbraucherfeindlicher Geschäftsmodelle. Bestimmte WLAN-Netze sind in der Lage, individuelle Bewegungsprofile und komplexe Metadatenbanken zu erstellen. Daher ist bei der Ausgestaltung von WLAN-Förderung auf bürgerschaftlichen Betrieb, Datensparsamkeit, anonyme Nutzung und Netzneutralität zu achten, wie es z.B. im Freifunk praktiziert wird.

b) Welche Instrumente der Förderung existieren? Welche sind Ihnen bekannt? Welche Formen der Förderung wären denkbar?

- Liberalisierung der Gesetzgebung zu Gunsten privater WLAN-Betreiber (Ausdehnung der Providerprivilegierung, Schaffung von Rechtssicherheit)
- Förderung wissenschaftlicher Forschung (zu Mesh-Netzen, freier Router-Software und innovativer Netzwerkprotokolle)
- Staatliche Zusammenarbeit mit ehrenamtlichen Freifunk-Initiativen (Übernahme von Internet-Verträgen in Flüchtlingsunterkünften und sozialem Wohnungsbau)
- Wettbewerbspolitik und Regulierung zur Begrenzung von Quasi-Monopolen im Telekommunikationsbereich
- Pilotprojekte mit städtischen und kommunalen Freifunk-Netzen in Hessen
- Bereitstellung vorhandener IP-Subnetze staatlicher Unternehmen und Institutionen

c) Welche Betreibermodelle existieren? Welche Modelle werden am häufigsten gewählt und wie kann man dies erklären?

Betreiber ist, wer die Funktionsherrschaft über das WLAN ausübt, also rechtlich und tatsächlich die Kontrolle darüber hat. Häufigstes Betreibermodell ist der private Betrieb eines Freifunk-Knotens (z.B. Gastronom oder Privatperson), mit dahinterliegender Beratung und Serverweiterleitung durch gemeinnützige Technologievereine. Mit dem Freifunk Rheinland e.V. gibt es außerhalb Hessens auch einen Freifunk-Verein mit ISP-Status, der eine klassische Provider-Priviligierung und Eintragung im RIPE Register (Réseaux IP Européens) hat, ähnlich der Telekom.
Diese Konstruktion lässt sich u.a. durch die unklare Störerhaftung erklären, welche den rechtssichern Betrieb nur mittels VPN-Umleitung vertretbar erscheinen lässt. Durch eine rechtliche Priviligierung der Knoten Betreiber würde diese zentralistische Bündelung und der kryptografische Aufwand (Energie, Kosten, Komplexität) größtenteils eingespart.

d) Welche Rolle kann das Modell „freifunk" für den Ausbau des WLAN in Hessen spielen?

Freifunker haben in Hessen bereits große öffentlich zugängliche WLAN-Netze aufgebaut, die weiterhin stetig steigen. Freifunk kann daher beim Ausbau von WLANs in Hessen eine sehr große Rolle spielen. Insbesondere wird dadurch die Zivilgesellschaft in den Aufbau einbezogen.

e) Welche Gründe sprechen für eine Zusammenarbeit der Kommunen, der Städte, der Landkreise und des ÖPNV beim Aufbau eines öffentlichen WLANs? Welche Gründe sprechen dagegen?

Vgl. 4 a)

f) Wer trägt die Kosten für den Aufbau und den Betrieb von WLAN-Netzen?

Kosten werden bei Freifunk in der Regel von freiwilligen Einzelpersonen, Spendern, Vereinen, Organisationen und Firmen getragen. Teilweise hilft die Öffentliche Hand, Kosten zu tragen. Sie entstehen in folgenden Bereichen:

- Betriebskosten:
- Internetzugang
- Strom
- Wartung (Reparatur und Fahrtkosten)
- Serverbetrieb
- Anschaffungskosten:
- WLAN-Hardware vor Ort
- evtl. Server Hardware (Gateways, VPNs, Offloader)
- etwaige Verkabelungsmaßnahmen

Die Betriebskosten für die geteilte breitbandige Internet-Anbindung von WLAN-Netzen werden auf Seite der ISPs mit "Flatrate"-Modellen auf Wenignutzer umgelegt. WLAN-Netze ohne Internetanbindung sind sinnvoll möglich, aber bisher unüblich.

5. Wirtschaftliche Bedeutung und Effekte

a) Welche Nutzen haben Städte und Gemeinden durch freie öffentlich zugängliche WLAN-Netze?

- Informative Vorteile in Schulen, ÖPNV, Museen und Bibliotheken
- Mehrwert für öffentliche Schwimmbäder
- Tourismus / Standortwerbung, wenn Touristen Fotos von Orten via Social Media bewerben
- Mögliche Verfahrensvereinfachungen in Bürgerämtern
- Synergieeffekte (Nutzen von WLAN für Sensoren / Smart City von Umweltdaten)
- Nutzung lokaler Freifunk Mesh-Netze für TV Übertragungen Offener Kanäle und Freier Radios

b) Haben freie öffentlich zugängliche WLAN-Netze auch für die Tourismuswirtschaft eine Bedeutung?

Ja, Touristen können sich mit Smartphones kostenfrei ohne Sprachbarriere ins Internet begeben und dort z.B. nach Sehenswürdigkeiten, Hotels, Restaurants etc. suchen.

c) Welchen Nutzen haben andere Wirtschaftssektoren und Branchen durch frei öffentlich zugängliche WLAN-Netze?

Wachstum und Beschäftigung in folgenden Branchen sind denkbar.

- Branchen mit Wartezeiten
- Friseure
- Ärzte
- Wellness
- ÖPNV
- Schwimmbäder
- Ämter
- Bildungsinstitutionen
- Bibliotheken
- Schulen
- Museen
- Universitäten
- Branchen mit Gästebetrieb
- Gastronomie
- Hotellerie
- Bäckereien und Cafés
- Branchen mit ITK Bezug
- IT Startups
- Telekomunikationsbranche
- Hardware Hersteller/Reseller
- Unterhaltungs- und Werbeindustrie
- Branchen mit IoT Projekten
- Industrie 4.0
- Autoindustrie
- Smart City
- Branchen mit Außendienst
- Vertrieb
- Service
- Logistik

Arten der Nutzung:

- Gestaltung von Wartezeiten
- Ubiquitärer Zugang zu Informations- und Bildungsangeboten
- Anreiz zur Entwicklung innovativer mobiler Anwendungen (Smartphone Apps)
- VOIP und IP-TV Potentiale für Startups
- Router- und Antennen- & Smartphoneverkauf

- Ermöglicht die Auslieferung mobiler Werbung in werbefinanzierten Smartphone Apps
- Betriebskostensenkung durch kostenlose Internetanbindung mobiler Vertriebs- und Servicemitarbeiter
- Ermöglicht Smartcar Leitsysteme und andere Internet of Things Anwendungen (IoT)
- Anbindung an Liveübersetzungsdienste (google translate everywhere)

d) Sind Auswirkungen auf (lokale) Telekommunikationsbetreiber zu erwarten, die inzwischen Vergleichbare Leistungen (z.B. LTE) im Rahmen von Nutzerverträgen gegen Rechnung zur Verfügung stellen?
Nein: Telekommunikationsverträge enthalten Pakete von Leistungen, deren Nutzung nur teilweise mit der Verrechnung in Zusammenhang steht. Das Telefoniepaket von Mobilfunkverträgen und die Nutzung des Datennetzes hängen in der Abrechnung in der Regel unabhängig von der Nutzung zusammen.

WLANs dienen häufig der Ergänzung, so dass Auswirkungen nicht zu erwarten sind.

Zusätzlich stellen WLANs für Personen eine wichtige Alternative dar, die keinen Zugang zu Mobilfunkverträgen haben oder sich diese nicht leisten können (Obdachlose, Flüchtlinge etc.).

e) Was ist beim Aufbau eines öffentlich geförderten und/oder betriebenen WLAN-Netzes im Hinblick auf das Wirtschaftsverwaltungsrecht zu beachten, wenn bestehende WLAN-Angebote (z.B. durch die Telekom) bestehen?
Zu dieser Frage liegen uns keine Erkenntnisse vor. In uns bekannten Gemeinschaftsprojekten mit Städten und Kommunen sind solche Probleme uns gegenüber bisher nicht thematisiert worden.

6. Förderprojekte im Bundesvergleich
a) Welche staatlich geförderten WLAN-Projekte existieren derzeit in Deutschland?
Pilothaft gelten das Freifunk-Projekt der Medienanstalt Berlin Brandenburg (MABB) und die Zusammenarbeit von Freifunkern, lokaler Wirtschaft und städtischer IT in Arnsberg (NRW). In vielen Städten und Gemeinden helfen Freifunker aktuell ehrenamtlich bei der Bewältigung der Flüchtlingskrise. Dazu kooperieren sie direkt mit den Betreibern (auch staatlich) der Unterkünfte.

In mehreren Landtagen wurden überparteiliche Beschlüsse zur Freifunk-Förderung gefasst. Die Förderung reicht von der Bereitstellung von Standorten für Freifunk-Hardware in öffentlichen Gebäuden, bis hin zum gemeinsamen Ausbau digitaler Infrastrukturen im Bereich öffentlicher Bildungs- und Kultureinrichtungen. Viele Landesregierungen haben die Vorteile von Freifunk erkannt. Ihre politische Einflussnahme im Wirtschaftsausschuss des Bundesrats hat kürzlich dafür gesorgt, dass die Zwangs-Verschlüsselung und die Einholung einer Erklärung im Gesetzentwurf der Bundesregierung gestrichen werden soll (BR-Drs. 440/1/15).

Hessen
- Darmstadt http://www.darmstadt.de/nachrichten/darmstadt-aktuell/news/freifunk-initiative-darmstadt-versorgt-in-kooperation-mit-der-wissenschaftsstadt-darmstadt-fluechtlingsunterkuenfte-mit-freiem-wlan/index.htm?tx_news_pi1[controller]=News&tx_news_pi1[action]=detail&cHash=f0d9b7888e4c4c5c01a6eeeeb3599c97

Berlin/Brandenburg
- MABB Berlin Pilotprojekt: http://wiki.freifunk.net/MABB

Bremen
- Drs.18/1506 https://www.bremische-buergerschaft.de/drs_abo/2014-07-29_Drs-18-1506_e7c57.pdf (SPD/Grüne)
- Die Bürgerschaft (Landtag) fordert den Senat auf,
- Freifunk-Initiativen ideell zu unterstützen,
- insbesondere Standorte für Freifunk-Hardware in öffentlichen Gebäuden zu prüfen,
- die Einrichtung von für Benutzer kostenfreien WLAN-Zugängen an hochfrequentierten öffentlichen

Orten in Bremen und Bremerhaven zu unterstützen,
- dem Ausschuss für Wissenschaft, Medien, Datenschutz und Informationsfreiheit imersten Quartal 2015 einen Bericht zur Umsetzung vorzulegen.

NRW
- Landtagsbeschluss (SPD/Grüne/Piraten):
- http://landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument?Id=MMD16/8970&quelle=alle
- https://freifunk-rheinland.net/der-landtag-nordrhein-westfalen-unterstutzt-freifunk PR, Koordinierungsstelle in der Staatskanzlei.
- Dazu gehört neben Zuwendungen zur Förderung spezieller Projekte die mögliche Nutzung von Liegenschaften des Landes und deren Kartographierung.

Arnsberg
- http://www.arnsberg.de/baukultur/gute-beispiele/werkstatt_alter-markt/freifunk.php

Schleswig Holstein
- Landtagsbeschluss (SPD/Grüne/SSW/Piraten)
- Pilotprojekte in Kiel und Lübeck

Sachsen-Anhalt
- Landtagsbeschluss (Einstimmig! Eingebracht CDU/SPD, Zustimmung Linke und Grüne)
- Videos: http://www.landtag.sachsen-anhalt.de/plenarsitzungen/979899-landtagssitzung/#section-inner-32
- Alle Anträge: https://md.freifunk.net/2015/10/freifunk-thema-im-landtag/
- http://www.landtag.sachsen-anhalt.de/fileadmin/files/drs/wp6/drs/d4366ran.pdf
- Beschlusstext:
- (1) Der Landtag begrüßt den Auf- und Ausbau von freien Netzwerken (z. B. durch Freifunk-Initiativen) in Sachsen-Anhalt und dankt allen Freiwilligen, die in Sachsen-Anhalt ihren gesellschaftlichen Beitrag zur Internetgrundversorgung leisten.
- (2) Der Landtag unterstützt grundsätzlich das Vorhaben, eine Änderung des Telemediengesetzes auf Bundesebene anzustreben bzw. die Anwendung der Störerhaftung bei WLAN-Netzen neu zu regeln.
- (3) Der Landtag regt an, in der Medienanstalt Sachsen-Anhalt ein Pilotvorhaben im Bereich freier WLAN-Netzwerke zu starten. Für dieses Projekt soll auf die Erfahrungen des Landes Berlin mit der Medienanstalt Berlin-Brandenburg zurückgegriffen werden.
- (4) Die Landesregierung wird gebeten, sich dafür einzusetzen, dass Hürden für dieBereitstellung digitaler Infrastrukturen gesenkt werden, sowie darauf hinzuwirken,dass beim Ausbau digitaler Infrastrukturen im Bereich öffentlicher Bildungs- und Kultureinrichtungen (sowie insbesondere in Flüchtlingsunterkünften) ehrenamtliche Aktivitäten berücksichtigt und mit einbezogen werden.
- (5) Die Landesregierung wird gebeten, die rechtlichen und technischen Grundlagen für die Bereitstellung von Standorten für digitales bürgerschaftliches Engagement in öffentlichen Gebäuden zu prüfen.

Freie WLAN-Hotspots in Hessen

Schriftliche Stellungnahme im Vorgriff auf die öffentliche mündliche Anhörung des Ausschusses für Wirtschaft, Energie, Verkehr und Landesentwicklung des Hessischen Landtages

Schriftliche Stellungnahme der Verbraucherzentrale Hessen e.V.

Gemäß dem Beschlussantrag der SPD-Fraktion im Hessischen Landtag vom 28.04.2015 soll der Hessische Landtag beschließen, die Hessische Landesregierung aufzufordern, den Zugang zu öffentlichen drahtlosen lokalen Netzwerken in Hessen zu unterstützen und zu fördern (Ziff. 2) und sich in diesem Zusammenhang auf Bundesebene für eine rechtssichere Novellierung des Telemediengesetzes (TMG) einzusetzen, indem die Haftungsbeschränkung für Access-Provider nach § 8 TMG auf alle Betreiber, unabhängig von ihrem jeweiligen institutionellen und organisatorischen Hintergrund, erweitert wird (Ziff. 3).

Die Beschlussanträge stehen im unmittelbaren sachlichen und zeitlichen Zusammenhang mit einer am 16.09.2015 im Bundeskabinett getroffenen Entscheidung über einen Gesetzentwurf zur Änderung des bundesgesetzlichen TMG. Die Änderung betrifft im Kern zwei Normen (§§ 8, 10 TMG), die die Haftung von WLAN-Betreibern, insbesondere von Access- und Host-Providern, regeln. Mit den neuen Regelungen geht eine Verschärfung der Access- und Host-Provider-Haftung einher.

Die Verbraucherzentrale Hessen e.V. nimmt dazu wie folgt Stellung:

Der nämliche Gesetzentwurf der Bundesregierung zur Änderung des bundesgesetzlichen TMG steht der oben formulierten Intention der Beschlussanträge der SPD-Fraktion im Hessischen Landtag diametral entgegen. Die Verbraucherzentrale Hessen hält die Novellierung des TMG gerade nicht für rechtssicher. Die Novelle unterstützt und fördert gerade nicht den Zugang zu öffentlichen drahtlosen lokalen Netzwerken und sie erweitert nicht die Haftungsbeschränkung für Access-Provider auf alle Betreiber, unabhängig von ihrem jeweiligen institutionellen und organisatorischen Hintergrund. Die geplanten Regelungen greifen zu kurz und orientieren sich nicht an den Anforderungen des Verbraucherschutzes und des digitalen Zeitalters.

Schon heute unterscheiden sich die Haftungsregelungen von Internetprovidern: Zugangsanbieter, die einen Telekommunikationsanschluss bereitstellen, also Access-Provider, haften nicht für rechtswidrige Inhalte, weil sie die Kommunikation über ihre Leitungen nicht überwachen. Host-Provider, also Internet-Plattformen, auf denen Nutzer Inhalte einstellen, haften nur, wenn sie von rechtswidrig hochgeladenen Inhalten Kenntnis haben und nicht unverzüglich tätig werden.

Diese Differenzierung hält die Verbraucherzentrale Hessen für angemessen: Internetzugangsanbieter haften mit gutem Grund nicht für Inhalte, die von Nutzern über ihre Netze verbreitet werden, weil sie diese Verbreitung nicht kontrollieren und keinen Einfluss darauf nehmen. Im Übrigen müssten sie sonst den Datenverkehr kontrollieren.

Betreffs der nunmehr vorgeschlagenen neuen Verpflichtungen für **Access-Provider** ist nicht nachvollziehbar, warum Verbraucher, die anderen über ein WLAN den anonymen Zugang zum Internet ermöglichen, im Rahmen der Störerhaftung für von Dritten begangene Urheberrechtsverletzungen verantwortlich sein sollen. Der Gesetzentwurf sieht vor, dass derjenige, der sein WLAN für Dritte zur Mitnutzung freigibt, tatsächlich „angemessene Sicherungsmaßnahmen gegen den unberechtigten Zugriff auf das drahtlose lokale Netzwerk“ ergreifen muss, wenn er einer Haftung für Rechtsverletzungen auf der Rechtsgrundlage der Störerhaftung entgehen will.

Dies entspricht nicht der geltenden Rechtsprechung. So bezieht sich insbesondere das BGH-Urteil „Sommer Deines Lebens“ (BGH, Urteil vom 12.05.2010, Az. I ZR 121/08) gerade nicht auf bewusst an die Öffentlichkeit gerichtete WLANs und hierfür zumutbare Maßnahmen, sondern lediglich auf die Absicherung eines privaten Anschlusses gegen den unberechtigten Zugriff Dritter. Der BGH geht auch in seiner Urteilsbegründung mit keinem Wort auf die Haftungsfreistellung der Zugangsdiensteanbieter ein, sondern stellt lediglich fest, dass eine Haftungsfreistellung für Host-Provider nach § 10 TMG im strittigen Fall nicht in Frage komme. Einen privaten Anschlussinhaber trifft unstrittig eine sekundäre Darlegungslast, wenn er selbst als Täter nicht in Frage zu kommen behauptet – der BGH hat die entsprechenden Anforderungen in seinem BearShare-Urteil konkretisiert (Urteil vom 08.01.2014, Az. I ZR 169/12). Wenn hingegen Diensteanbieter einer unbestimmten und gegebenenfalls unbegrenzten Zahl von Dritten wissentlich und willentlich einen Zugang zum Internet eröffnen, handelt es sich um eine völlig andere Konstellation. Tatsächlich hatte der BGH bislang keinen

Fall zu entscheiden, bei dem etwa der Inhaber eines Cafés, das öffentliches WLAN anbietet, als Störer in Anspruch genommen worden wäre. Der Gesetzentwurf stellt in dieser Hinsicht also durchaus eine Verschärfung gegenüber der geltenden Rechtsprechung dar.

Anders als im Fall einer unzureichenden Absicherung eines privaten Internetzugangs ist auch fraglich, ob mit einer Anwendung der Störerhaftung auf Diensteanbieter überhaupt vorgebeugt zu werden braucht oder ob sich eine solche Anwendung nicht schon grundsätzlich verbietet. Denn man sollte sich in Erinnerung rufen, „dass die Versorgung mit einem Internetzugang letztlich eine Maßnahme der Daseinsvorsorge darstellt, ebenso wie die Versorgung mit Telefon oder dem Postdienst schon seit Jahrzehnten. Dass der Staat diese Leistung der Daseinsvorsorge heutzutage nicht mehr selbst erbringt, sondern dies von privaten Internet-Service-Providern erledigt wird, ist eine Folge der Privatisierung des Telekommunikationssektors. Würde nun der Staat selbst – in Erfüllung seiner Aufgabe der Daseinsvorsorge – einen flächendeckenden Internetzugang zur Verfügung stellen, so wäre dieser Zugang zwangsläufig für jedermann offen und frei und deshalb natürlich auch mit der Gefahr von Urheberrechtsverletzungen durch Nutzer verbunden. Man würde bei einer solchen Ausgestaltung allerdings wohl kaum die Frage stellen, ob der Staat als Störer einer Urheberrechtsverletzung anzusehen ist“ (aus: Stadler, AnwZert ITR 9/2010, Anm. 3).

Darüber hinaus sei darauf hingewiesen, dass die vorgeschlagene Regelung gleichfalls nicht vereinbar ist mit Art. 12 der E-Commerce-Richtlinie (Reine Durchleitung), der eine ausdrückliche Haftungsbefreiung der Access-Provider zwingend vorschreibt, sofern bestimmte Voraussetzungen erfüllt sind (Übermittlung nicht veranlasst, Adressat nicht ausgewählt, übermittelte Informationen nicht ausgewählt oder verändert). Auch die Vereinbarkeit mit Art. 15 der E-Commerce-Richtlinie, demzufolge keine allgemeinen Maßnahmen auferlegt werden dürfen, erscheint zumindest fragwürdig.

Die Verbraucherzentrale Hessen plädiert stattdessen dafür, dass durch den Gesetzgeber klargestellt wird, dass auch Verbraucherinnen und Verbraucher, die ihr WLAN für Mitnutzer unverschlüsselt offen lassen, im Sinne des TMG als Access-Provider gelten und somit von einer uneingeschränkten Haftungsfreistellung profitieren. Auch die Unsicherheit darüber verhindert derzeit noch die von der Politik geforderte flächendeckende, allgemein verfügbare Versorgung mit mobilem Internet für alle - anders als in vielen anderen europäischen Ländern, wo es viel mehr freies, nicht-kommerzielles WLAN gibt, welches man ohne Registrierungsformalitäten nutzen kann.

Ebenso verfehlt erscheint die Verschärfung der Voraussetzungen für eine Haftung der **Host-Provider**. Dass in Zukunft statt des Nachweises tatsächlicher Kenntnis von Rechtsverletzungen eine gesetzliche Vermutung solcher Kenntnis ausreichen soll, um Host-Provider haftbar zu machen, erscheint als eilfertige Reaktion zum Schutz der Rechte an geistigem Eigentum, ohne dabei die Auswirkungen auf die gesellschaftliche und wirtschaftliche Bedeutung des Internets abzuwägen. Der Schaden dieser Regelung wird vorhersehbar darin bestehen, dass Host-Provider vermeintlich freiwillig diverse Inhalte löschen, deren rechtliche Bewertung sich ihrer Kenntnis entzieht, um von vornherein keine Angriffsfläche für Haftungsklagen zu bieten. Hier drohen eine freiwillige Selbstzensur und damit eine Privatisierung der Rechtsdurchsetzung.

Von diesen Einwand ganz abgesehen, hält die Verbraucherzentrale Hessen eine Haftungsverschärfung für Hostprovider ohnehin nicht für sachgerecht. Es ist insbesondere nicht richtig, wie es die Begründung zur Novelle des TMG darlegt, „dass bei Urheberrechtsverletzungen im Internet ein Vorgehen der betroffenen Inhaber des Rechts auf geistiges Eigentum gegen Diensteanbieter, deren Geschäftsmodelle im Wesentlichen auf Rechtsverletzungen beruht vielfach schwierig, wenn nicht unmöglich ist.“ Nicht nur ist unklar, welche Art von Diensteanbieter im Bereich der Hostprovider hier gemeint ist, nachdem der BGH in einem Grundsatzurteil („Rapidshare“) ausdrücklich klargestellt hat, dass jedenfalls das Geschäftsmodell von Filehostern „nicht von vornherein auf Rechtsverletzungen angelegt“ ist. Sondern es ist auch darauf hinzuweisen, dass die Bundesregierung bereits 2008 mit dem „Gesetz zur Verbesserung der Durchsetzung der Rechte des geistigen Eigentums“ einen Auskunftsanspruch gegenüber den Providern eingeführt hat, der es Rechteinhabern jederzeit ermöglicht, direkt gegen Rechtsverletzer vorzugehen. Voraussetzung dafür ist ein „gewerbliches Ausmaß“ der Rechtsverletzungen, was unstrittig gegeben sein dürfte, sofern es sich um „Geschäftsmodelle“ handelt, wie in der Begründung angegeben. Das erwähnte Gesetz hat sich nicht nur als effektiv im Sinne der Rechteinhaber erwiesen, sondern es ist daraus sogar eine Abmahnindustrie entstanden, bei der Verbraucher mit standardisierten Mahnschreiben und einschüchternden Klageandrohungen zu oftmals ungerechtfertigt überhöhten Zahlungen an die Rechteinhaber gedrängt werden. Jedenfalls hat sich die Bundesregierung aufgrund des anhaltenden Missbrauchs der den „Inhabern des Rechts auf geistiges Eigentum“ eingeräumten Durchsetzungsregeln erst 2013 genötigt gesehen, ein „Gesetz gegen unseriöse Geschäftspraktiken“ zu verabschieden, das leider bis heute weitgehend wirkungslos geblieben ist.

Bekanntlich überziehen die Rechteinhaber heute bereits die Host-Provider mit automatisierten Löschansprüchen, die häufig ebenso automatisiert zu einer Sperrung bzw. Löschung der entsprechenden Inhalte führen. Es ist offenkundig unbefriedigend, dass es zum Teil noch immer keine für beide Seiten befriedigenden Lösungen zur Vergütung der Nutzung urheberrechtlich geschützter Inhalte auf Plattformen gibt. Dieses Problem dadurch lösen zu wollen, dass man die Haftungspflichten nach und nach über die **Content-Provider** hinaus auf die Host-Provider ausdehnt, hält die Verbraucherzentrale Hessen für unsachgemäß. Der vorliegende Regelungsvorschlag ist insofern ein Schritt in die falsche Richtung.

Nach alledem bezweifelt die Verbraucherzentrale Hessen, dass Verschärfungen der Haftungsregelungen für Access- und Host-Provider ein geeignetes Mittel sind, um gegen Urheberrechtsverstöße im Internet wirksam vorzugehen. Die Haftungsregelungen für Access- und Host-Provider zu verschärfen führt vielmehr zu einer eingeschränkten Verfügbarkeit von Internetzugängen sowie zu einer Erschwerung der Tätigkeit von Host-Providern. Die vorgeschlagenen Regelungen sind zudem unvereinbar mit der Richtlinie über den Elektronischen Geschäftsverkehr (RL 2000/31/EG, E-Commerce-Richtlinie), stehen im Widerspruch zu Regelungen des TMG und des Telekommunikationsgesetzes (TKG) und laufen den aktuellen Entwürfen der Europäischen Kommission für eine Verordnung über Maßnahmen zum europäischen Binnenmarkt der elektronischen Kommunikation und zur Verwirklichung des vernetzten Kontinents zuwider (2013/0309 (COD), Telecom Single Market Act).

Der freie Zugang zu offenen WLAN-Netzen und Cloud-Diensten, bei denen die Inhalte der Nutzer nicht kontrolliert werden, sind zwei Grundvoraussetzungen für digitale Teilhabe von Verbrauchern im 21. Jahrhundert. Sie müssen erhalten und ausgebaut werden und dürfen nicht durch überzogene Haftungsregeln im Keim erstickt werden.

Demzufolge begrüßt die Verbraucherzentrale Hessen die Beschlussanträge der SPD-Fraktion im Hessischen Landtag, darauf hinzuwirken, im Landtag zu beschließen, dass sich die Landesregierung dafür einsetze,

a) die Haftungsbeschränkung für Access-Provider nach § 8 TMG auf alle Betreiber unabhängig von ihrem jeweiligen institutionellen und organisatorischen Hintergrund zu erweitern (Ziff. 3) und
b) den Zugang zu öffentlichen drahtlosen lokalen Netzwerken in Hessen zu unterstützen und zu fördern (Ziff. 2)

sowie darauf hinzuwirken, im Landtag zu beschließen, dass die Gefahr für mögliche Rechtsverletzungen der Nutzer bei jeder Betreiberform (kommerziell, öffentlich oder privat) gleichermaßen gegeben gesehen wird und dies demnach einheitlich geregelt sein muss.

Frankfurt, 30.10.2015

Wall

An den
Hessischen Landtag
z.Hd. Herrn Clemens Reif, MdL, Vorsitzender
des Ausschusses für Wirtschaft, Energie,
Verkehr und Landesentwicklung
Schlossplatz 1-3
65183 Wiesbaden

Wall Aktiengesellschaft

Niederlassung Frankfurt am Main
Börsenplatz 1
60313 Frankfurt am Main

Tel. (+49/69) 219 36 58-0
Fax (+49/69) 219 36 58-19

Unternehmenszentrale
Friedrichstraße 118
10117 Berlin

Tel. (+49/30) 33 8 99-0
Fax (+49/30) 33 8 99-295

info@wall.de
www.wall.de

2. November 2015

Öffentliche mündliche Anhörung des Ausschusses für Wirtschaft, Energie, Verkehr und Landesentwicklung zum Thema „Freie WLAN-Hotspots in Hessen",

Sehr geehrter Herr Vorsitzender,
sehr geehrte Damen und Herren Mitglieder des Landestages,

vielen Dank für die Einladung zu der oben genannten Anhörung und für die Möglichkeit zur Abgabe einer Stellungnahme.

Dieser Einladung kommen wir sehr gerne nach und übersenden Ihnen in der Anlage vorab die schriftliche Stellungnahme unseres Unternehmens.

Mit freundlichen Grüßen

Cristian Kohut

Cristian Kohut
Regionalmanager

ANLAGE

Stellungnahme der Wall AG:

Öffentliche mündliche Anhörung „Freie WLAN- Hotspots in Hessen“

Vorgelegt von: Cristian Kohut, Regionalmanager

Vorgelegt bei: Hessische Landtag; Ausschuss für Wirtschaft, Energie, Verkehr und Landesentwicklung

Vorgelegt am: 2. November 2015

Einführung

Mobiles Internet ist zu einer Selbstverständlichkeit des Alltags geworden. Mobile Endgeräte wie Smartphones und Tablets sind ständige Begleiter der Menschen und haben das Surfverhalten stark verändert. Die Nutzung von Social Media-Kanälen und von Videotelefonie ist heute Teil der alltäglichen Kommunikation und hat zu einer starken Erhöhung des Datenverkehrs geführt.

Insbesondere in urbanen Ballungsgebieten stößt das Mobilfunknetz an seine Grenzen und das Angebot eines öffentlichen kostenfreien WLANs ist von hoher Bedeutung. In Städten, die ein hohes Aufkommen an Geschäftsreisenden und Touristen aufweisen, wird dieses als selbstverständlich vorausgesetzt. Für Besucher aus anderen Ländern ist es oft nur schwer verständlich, dass selbst in vielen erstklassigen Hotels kostenfreies Internet bis heute eine Seltenheit ist. Und ebenso stellen sie verwundert fest, dass WiFi auf der Straße nicht gratis verfügbar ist, und wenn doch, dann meist nur als zeitlich begrenztes Angebot von Café- oder Restaurantbetreibern. Dies entspricht nicht einer modernen öffentlichen Infrastruktur im Zeitalter der weltweiten Digitalisierung.

Die Wall AG als international tätiges Unternehmen trägt durch ihre innovativen Stadtmöblierungsprodukte erfolgreich dazu bei, städtische Räume für Bürger und Touristen noch attraktiver zu gestalten und für das digitale Zeitalter zu rüsten. Getreu unserem Leitgedanken „Für Städte. Für Menschen.“ bieten wir mit dem von uns entwickelten WLAN-Angebot „bluespot Free WiFi“ eine schnelle, kostenlose, unbegrenzte und einfach zu bedienende Möglichkeit zur digitalen Vernetzung des städtischen Raums.

Die Wall AG – Für Städte. Für Menschen.

Seit bald 40 Jahren steht der Name Wall für Stadtmöblierung und Außenwerbung in Premium-Qualität. Im Einklang mit den Bedürfnissen einer Stadt gestaltet, fertigt und pflegt Wall Stadtmöbel, vermarktet Werbeflächen und beteiligt die Städte direkt am Erfolg.

Die Wall AG wurde 1976 im badischen Ettlingen durch Hans Wall gegründet. Seit 1984 hat das Unternehmen seinen Sitz in Berlin. Heute wird das Unternehmen in zweiter Generation vom Sohn des Firmengründers, Daniel Wall, geführt. Seit 2009 gehört die Wall AG zur internationalen JCDecaux-Gruppe, der Nummer Eins für Stadtmöblierung und Außenwerbung weltweit. Wall ist in Deutschland und der Türkei tätig.

Das Markenzeichen der Wall AG sind innovative Stadtmöbelkonzepte in höchster Designqualität. In Velten/ Brandenburg unterhalten wir ein eigenes Forschungs- und Entwicklungszentrum sowie eine eigene Produktionsstätte mit über 10.000qm Produktionsfläche. Hier entstehen maßgeschneiderte Lösungen für städtische Räume. Unser Angebot wird komplettiert durch einen eigenen Wartungs- und Reinigungsservice, für den wir in allen Partnerstädten in Deutschland wie in der Türkei eigene, festangestellte Mitarbeiter einsetzen.

bluespot Free WiFi – Intelligente Stadtmöbel für Smart Cities

Schon vor über zehn Jahren begann die Wall AG damit, ihre Stadtmöblierung intelligent und digital zu vernetzen und ging so den ersten Schritt in Richtung „Smart Cities". Im April 2005 wurde das selbst entwickelte bluespot-System, ein digitales Kunden- und Stadtinformationsnetz, in Berlin eingeführt. Bluespot kombinierte dabei klassische Plakatwerbung mit Internet und Handy. An 46 innerstädtischen Wall-Terminals konnten Nutzer kostenlos Stadtinformationen, Veranstaltungstipps und Angebote des Einzelhandels auf ihr Handy laden. Touristen konnten sich kostenfrei über die Internetterminals wichtige Stadtinformationen besorgen. Und eingebaute Telefone machten auch Nicht-Handybesitzern das kostenfreie Telefonieren im lokalen Netz möglich. Weitere Städte wie Freiburg im Breisgau, Dortmund, Düsseldorf, Karlsruhe und andere folgten.

Zehn Jahre später hat sich die Technik entscheidend weiterentwickelt. Starre Internet-Terminals gehören der Vergangenheit an. Sie sind für ein öffentliches WLAN-Angebot nicht mehr erforderlich. Mobiles Internet ist eine Selbstverständlichkeit geworden.

Entsprechend hat die Wall AG auch ihr bluespot-Produkte weiterentwickelt. Die Marke bluespot umfasst heute kostenlose Zusatzdienste für Bürger und Touristen einer Stadt und beliefert mit dem Produkt bluespot Free WiFi den öffentlichen Raum mit kostenfreiem, zeitlich unbegrenztem WLAN.

Die Refinanzierung von bluespot Free WiFi als kostenloser Connectivity-Service der Städte erfolgt, wie für alle Produkte des Unternehmens, durch die Vermarktung der Außenwerbeflächen, die dem Unternehmen durch die Stadt im Rahmen eines Konzessionsvertrages gestattet werden. Bluespot Free WiFi bedeutet somit keine zusätzliche Belastung des städtischen Haushalts.

Die Projektkoordination, den Aufbau von Hotspots, die Wartung und den dauerhaften Service gewährleistet die Wall AG durch eigene Mitarbeiter. Alles bleibt in einer Hand. Die WLAN-Technik wird dezent, aber dennoch für jeden Nutzer gut erkennbar in die Stadtmöblierung des Unternehmens integriert. Ein Fahrgastunterstand an einer Tram-Haltestelle wird so zum Beispiel zum WiFi-Hotspot für die Nutzer des Öffentlichen Personennahverkehrs (ÖPNV). Eine Stadtinformationsanlage präsentiert dann nicht nur einen gedruckten Stadtplan, sondern liefert über das kostenfreie WiFi gleich wertvolle Umgebungsinformationen dazu. Die Stadtmöbel werden durch gut sichtbare, aber elegant gestaltete Aufsätze als WiFi-Standorte gekennzeichnet.

Pressestimmen

Mai 2012 – Pilotprojekt in Berlin

Endlich freies Surfen in Berlins Wartehäuschen

Kostenloses WLAN für alle zwischen Kudamm und Alexanderplatz

Berlin – **Trotz großer Senatspläne, die im Zuge der „Innovationsinitiative Berlin" kostenlosen Zugang zum Internet in der Stadt vorsahen, warten die Berliner Internet-Junkies seit Jahren vergeblich auf WLAN für alle. Bis jetzt.**

Bevor der Bus kommt schnell noch Mails checken. In der Kneipenrunde dem Besserwisser mit Fakten Paroli bieten. Unterwegs im Internet surfen ist dank Smartphone und Co. für viele Alltag. Doch „drin sein" kostet. Bisher. Denn nun macht der Plakat- und Stadtmöbel-Riese Wall den Berlinern und ihren Gästen ein neues Angebot. Ab sofort gibt's an 20 Orten in der Innenstadt kostenlosen Internetzugang für alle. Die Technik steckt in Bushaltestellen, knallblaue Plakate weisen auf den neuen Service hin. Mit einer eigens entwickelten App soll das Surfen hier sicher wie zu Hause sein.

„Wir wollen das Thema vorantreiben, wir glauben, dass kostenloses Internet in den Städten in Zukunft selbstverständlich wird", erklärt Geschäftsführer Daniel Wall zum Start des Projekts. In einer Testphase bis Ende August will Wall testen, wie das Angebot angenommen wird.

Und so funktioniert's: An der Bushaltestelle die Wall-Wifi-App herunterladen, mit Mail-Adresse und Passwort registrieren und kostenlos lossurfen. Die App zeigt außerdem an, wo sich der nächste der über 20 Standorte in der Innenstadt befindet.

Fortsetzung

September 2013 – bluespot Free WiFi in Düsseldorf

Kostenloses Internet an der Königsallee

In der Düsseldorfer Innenstadt können Besitzer von Smartphones und Tablet PCs jetzt gratis ins Internet. Möglich ist das durch zehn drahtlose Internet-Hotspots. Bis 2014 soll die Zahl auf 50 ausgeweitet werden.

KOMMENTAR

Eine gelungene Werbemaßnahme

Das sagen die Kö-Besucher zum WLAN-Angebot

Oktober 2015 – bluespot Free WiFi in Freiburg

FREIBURGER ZEITUNG

Innenstadt-WLAN ist da

Wall AG integriert Internet-Hotspots in Werbetafel– kostenlos Surfen in der Innenstadt

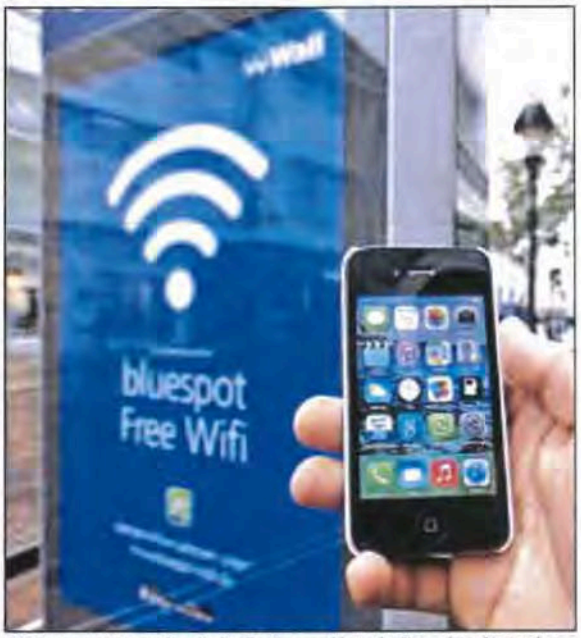
Von Merlin Gröber

Kostenfrei und zeitlich unbegrenzt ist das neue WLAN-Netz in der Freiburger Innenstadt. Die Berliner Wall AG integrierte insgesamt 17 Hotspots in bestehende Werbetafeln, um ein möglichst flächendeckendes Internet für Bürger und Touristen in der Innenstadt bieten zu können. Oberbürgermeister Dieter Salomon weihte den ersten öffentlichen WLAN- Zugangspunkten in der Kaiser-Joseph-Straße ein.

Seit einigen Tagen sind sie auf Werbetafeln in der Innenstadt zu sehen– dunkelblaue Aufsätze mit weißem „Free Wifi"-Schriftzug. Sie kennzeichnen Hotspots an denen man kostenfrei und zeitlich unbegrenzt auf Smartphones, Tablets oder Notebooks im Internet surfen kann. Bei der einmaligen Registrierung werden Vor- und Zuname, E-Mail und Passwort abgefragt. Mit diesen Daten kann man sich dann wiederkehrend anmelden und losurfen. Die Anmeldung erfolgt sowohl über die Startseite am Hotspot, als auch über die Website www.bluespot-wifi.de, wo's auch eine Übersicht über alle 17 Standorte gibt. Diese reichen vom ZOB bis zum Schlossbergring und der Kaiserbrücke bis zum Friedrichring. Jeder Hotspot hat– je nach Umgebung– 150 bis 200 Meter Reichweite. Im Praxistest war in der Innenstadt nicht überall eine gute Abdeckung. In einigen Seitenstraßen der Kajo brach das Signal ab. Die Kosten für den WLAN-Ausbau lagen im niedrigen fünfstelligen Bereich und wurden von der Berliner Wall AG übernommen.

Bei der Einweihung wurde vor allem die Nützlichkeit des Services für die Bürger und Touristen hervorgehoben. Ein kostenfreies und unbegrenztes WLAN orientiere sich „an den Wünschen und Bedürfnissen von Bürgern und Touristen" betonte Daniel Wall, Vorstandsvorsitzender der Wall AG. Auch Oberbürgermeister Dieter Salomon lobte das öffentliche WLAN als wichtigen Teil der urbanen Infrastruktur. Ein Ausbau der bestehenden Hotspots hängt laut Salomon von der Nachfrage und der Funktionalität des Internets ab. Bei der Wall AG gibt man sich zuversichtlich und freut sich auf weitere Kooperationen. „Wenn der Wunsch der Stadt da ist, bauen wir das Netz gerne weiter aus" betont Frauke Bank, Pressesprecherin der Wall AG.

Kritik an dem neuen WLAN-Netz kommt von Freifunk Freiburg. Durch bürgerschaftliches Engagement organisiert man hier ein wachsendes Netzt von freien WLAN-Routern, auf die kostenfrei zugegriffen werden kann. Gegenüber dem WLAN-Netz der Wall AG hat man vor allem datenschutzrechtliche Bedenken bezüglich des Trackings. Auch verstehe man nicht, warum die Wall AG für die Werberechte in der Innestadt 2004 noch 4,2 Millionen Euro bezahlte, zehn Jahre später hingegen nur 2,5 Millionen. Der Preisverfall erklärt sich laut OB Salomon durch den sinkenden Marktwert von Außenwerbeanlagen und der zunehmenden Konkurrenz der Internetwerbung. Es hätten sich nur wenige Interessenten bei der Ausschreibung gemeldet – ein Zeichen, dass Außenwerbung an Attraktivität verliere.



Einloggen und losurfen: In der Freiburger Altstadt gibt es jetzt kostenloses WLAN an den Werbetafeln der Wall AG. FOTO: THOMAS KUNZ

Wie das WLAN funktioniert, zeigt ein Video: **http://fudc.fr/freiburgwlan**

bluespot Free WiFi in der Praxis

Bereits in drei Großstädten Deutschlands hat die Wall AG ihr WLAN-Angebot erfolgreich getestet und etabliert: Berlin, Düsseldorf und Freiburg im Breisgau.

Berlin

Im Mai 2012 sorgte Wall als erster Anbieter für ein kostenfreies WLAN-Angebot im öffentlichen Raum in der deutschen Hauptstadt.

In Eigeninitiative und im Rahmen eines Pilotprojekts stattete die Wall AG rund 30 Standorte in der Berliner Innenstadt mit WiFi-Hotspots aus und bot diese von Ende Mai bis Ende August den Berlinern und Touristen zur freien Nutzung an. Dabei konnte das Internetangebot wahlweise per kostenfreier bluespot App oder via Landing Page genutzt werden. Der Service wurde in Deutsch wie in Englisch bereitgestellt.

Die Nutzer mussten sich bei erstmaliger Nutzung mit ihrer E-Mail-Adresse sowie einem selbstgewählten Passwort registrieren.

Das Pilotprojekt erbrachte den erstrebten Nachweis, dass das bluespot Free WiFiSystem nicht nur eine sehr einfache Handhabung von WiFi ermöglichte, sondern insbesondere einen Mehrwert für Besucher der Stadt Berlin bot. Pro Tag nutzten rund 600 User das neue Angebot. Insbesondere das hohe, positive Feedback von ausländischen Touristen auf den neuen Service bestätigte die Überzeugung, dass kostenfreies WLAN im öffentlichen Raum ein wichtiger Wettbewerbsfaktor für Städte ist, die ein hohes touristisches Aufkommen aufweisen. Die Projektauswertung zeigte, dass rund 50 Prozent der Wall-WiFi-Nutzer aus dem europäischen Ausland (Spanien, Italien, Frankreich, Niederlande) und Russland kamen, die restlichen Nutzer aus Deutschland.

Düsseldorf

In der Landeshauptstadt Nordrhein-Westfalens ist kostenfreies WLAN dank Wall bereits etablierte Realität.

Seit September 2013 bietet die Wall AG in der Innenstadt das bluespot Free WiFi mit inzwischen 55 Standorten an. Durch die Installation der Hotspots in die bestehende Stadtmöblierung der Wall AG, zum Beispiel entlang der pulsierenden, berühmten Königsallee, der „Kö", oder im modernen Medienhafen wurde eine hochmoderne, digitale Netzinfrastruktur geschaffen. Trotz ihrer dezenten Integration in die bereits bestehenden Stadtmöbel sind die bluespot-Hotspots dennoch leicht zu erkennen. Die markanten, aber elegant gehaltenen blauen Aufsätze sind weithin sichtbar und wiedererkennbar.

In rund zwei Jahren, bis September 2015, verzeichnete Wall über 580.000 Zugriffe auf das bluespot WiFi-Angebot in Düsseldorf. Pro Tag wird bluespot bis zu 3500 Mal genutzt. Das belegt die hohe Akzeptanz des Service. Dabei hat mehr als jeder zweite WiFi-Nutzer eine andere Sprache als Deutsch auf seinem Telefon eingestellt. Das WiFi wird also auch hier, analog zum Pilotprojekt in Berlin, gern von Touristen genutzt.

Freiburg im Breisgau

Vor Kurzem konnte die Wall AG bluespot Free WiFi in der dritten deutschen Großstadt etablieren. Am 15. Oktober 2015 weihte sie gemeinsam mit dem Freiburger Oberbürgermeister Dr. Salomon 17 WLAN-Hotspots an den am stärksten frequentierten Standorten der Freiburger Innenstadt ein. Wie auch in Berlin und Düsseldorf wurden die Hotspots in die bestehende Stadtmöblierung von Wall integriert und durch die blauen Aufsätze sichtbar gekennzeichnet. Auch hier wird der Service auf Deutsch und Englisch angeboten, sodass er auch für Touristen einen hohen Mehrwert bietet. Aufgrund der Nähe zu Frankreich sowie zur Schweiz wird Französisch als drittes Sprachangebot in Kürze folgen.

Einweihung des ersten von insgesamt 17 bluespot Free WiFi-Hotspots am 15. Oktober 2015 in Freiburg im Breisgau, in Anwesenheit des Oberbügermeisters Dr. Salomon (2. von links)

Einfache Nutzung – Sichere Daten

Bluespot Free WiFi kann mit allen WLAN-fähigen Endgeräten wie Smartphones, Tablets, Note- oder Netbooks genutzt werden. Wahlweise können Nutzer sich die kostenfreie bluespot-App auf ihrem Endgerät installieren oder sie wählen sich über die Landing-Page am Hotspot ein.

Jeder Nutzer muss sich vor der ersten Nutzung einmalig mit Vor- und Zunamen, E-Mail und selbstgewählten Passwort registrieren. Mit diesen Daten ist eine wiederkehrende Anmeldung an jedem WLAN-Hotspot möglich.

Die Angabe des Nutzernamens wird zur Identifizierung des Nutzers am Standort genutzt (Nutzerdaten). Eine Verarbeitung dieser Information über die Dauer der Nutzung hinaus findet nicht statt. Zur Verbesserung des Angebotes werden auf einem gesonderten System anonymisierte Verkehrsdaten zur Nutzung aggregiert. Durch die hier gespeicherten Daten kann die Wall AG keine Rückschlüsse auf die tatsächliche Identität des Nutzers ziehen. Es sind lediglich Rückschlüsse auf das Benutzungsverhalten der Nutzer möglich (Zahl der Zugriffe, Zuordnung zu örtlichem Hotspot etc.). Die Wall AG speichert keine Nutzerdaten für Werbe- oder ähnliche Zwecke.

Die Erstregistrierung ist angesichts der noch unklaren Gesetzeslage zur Störerhaftung erforderlich.

Das bluespot Free WiFi wurde vom Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) geprüft und als empfehlenswert eingestuft.

Allgemeine Informationen und Anleitungen zur Nutzung des bluespot Free WiFi können online unter www.bluespot-wifi.de abgerufen werden.

Rechtliche Rahmenbedingungen

Die Wall AG hat erstmals im Jahre 2012 ein öffentliches WLAN in Berlin angeboten. Das Projekt hat sich vor allem aufgrund der teilweise unklaren und oft für WLAN-Anbieter ungeeigneten rechtlichen Rahmenbedingungen als sehr aufwändig erwiesen. Dies betraf nicht nur Fragen der Haftung des Anbieters, sondern auch umfassende Informationspflichten und Abstimmungen mit unterschiedlichen Behörden. Da diese Themen von dem Fragenkatalog des Landtages nicht abgedeckt sind, möchten wir hierzu kurz vorab Stellung nehmen.

Nach umfassender anwaltlicher Beratung und Auswertung der Rechtsprechung zu den telekommunikationsrechtlichen Pflichten ist die Wall AG zu dem Ergebnis gekommen, dass sie für das Angebot eines kostenlosen WLAN-Hotspots nicht verpflichtet ist, die in § 111 Abs. 1 TKG genannten Daten der Nutzer (u.a. Name, Abschrift, Geburtsdatum) zu erheben (LG München I, Urt. v. 12.1.2012 – 17 HKO 1398/11, ZD 2012, 281). Unter Berücksichtigung der damals aktuellen Rechtsprechung zur Störerhaftung von Access Providern stellte sich dann jedoch die Frage, ob die anonyme Nutzungsmöglichkeit der geplanten WLAN-Hotspots zu einer Gefahrgeneigtheit des Angebotes und damit zu einer möglichen Haftung der Wall AG für rechtswidrige Downloads der Nutzer führen würde. Es wurde daher eine Registrierungspflicht der Nutzer (Name und E-Mail-Adresse) aufgenommen und in Nutzungsbedingungen geregelt, dass die Nutzung zu rechtswidrigen Zwecken untersagt ist. Zusätzlich wurden technische Einschränkungen des Hotspots implementiert, die die Nutzung für rechtwidrige Handlungen erschweren sollten (u.a. Portsperren, URL-Blacklists).

Nach Inbetriebnahme der Hotspots erfolgte umgehend eine behördliche Anhörung durch den Berliner Beauftragten für Datenschutz und Informationsfreiheit, der die in der Datenschutzerklärung des Hotspots beschriebene Datenerhebung als übermäßig ansah. Nach Stellungnahme der Wall AG und kleineren Anpassungen am Dienst wurde das Verfahren zuständigkeitshalber an den für Telekommunikationsanbieter zuständigen Bundesbeauftragten für den Datenschutz und die Informationsfreiheit abgegeben. Nach eingehender Prüfung des Angebots und wiederholter rechtlicher und technischer Stellungnahme der Wall AG wurde der Hotspot von der Aufsichtsbehörde am Ende als „datenschutzfreundlich" eingestuft.

Die von der Wall AG vorgenommene physikalische Trennung der Nutzerdaten von den Verkehrsdaten führt allerdings dazu, dass nun Maßnahmen nach § 110 TKG (Überwachung, Auskünfte) für die Wall AG mit erhöhtem personellem und technischem Aufwand verbunden sind.

Die Anforderungen der Datenschutzbehörden, der Strafverfolgungsbehörden und der Rechteinhaber sind für Anbieter von WLAN-Hotspots aufgrund der unklaren Rechtslage faktisch nicht in Einklang zu bringen. Die damit verbundenen Haftungsrisiken belasten im Besonderen die Anbieter kostenloser WLAN-Hotspots wie die Wall AG.

Zu den einzelnen Fragen:

Zu a)

Content-Provider haften für eigene Inhalte nach den üblichen gesetzlichen Regelungen. Für Host- und Access-Provider sehen die § 7-10 TMG eigentlich ein Haftungsprivileg vor, welches jedoch nach der bisherigen Rechtsprechung des BGH auf Unterlassungspflichten nach der sog. Störerhaftung nicht anwendbar ist.

Zu b) und c)

Wann die Haftung des Access-Providers einsetzt und wann er sich auf ein Haftungsprivileg stützen kann, ist unklar und in Politik, Literatur und Rechtsprechung umstritten. Der aktuell diskutierte Entwurf eines Änderungsgesetzes zum TMG soll zwar nach politischen Willensbekundungen eine klarere Privilegierung der Access-Provider herbeiführen, das Privileg soll jedoch nur greifen, wenn „angemessenes Schutzmaßnahmen" durch den Provider getroffen wurden. Welche das sind, bleibt völlig im Unklaren. Nach erster Einschätzung wird die geplante Änderung daher weder zu einer Klärung der Rechtslage, noch zu einer Verbesserung der Haftungssituation der Hotspot-Betreiber führen.

Der EuGH hat mit seinem Urteil vom 27.3.2014 (C-314/12) faktisch die Forderung aufgestellt, dass Access-Provider die Inanspruchnahme ihrer Leistungen für rechtswidrige Zwecke zwar wirksam unterbinden müssen, dadurch aber die Nutzung der Dienste für rechtmäßige Zwecke nicht beeinträchtigt werden darf. Wie ein solches technisches Wunder zu erreichen ist, hat der EuGH jedoch nicht verraten und damit ebenfalls keinen Beitrag zur Klärung der unklaren Rechtslage geleistet.

Zu d)

Im Rahmen der Störerhaftung kann der WLAN-Betreiber vor allem mit Unterlassungsverlangen konfrontiert werden, die aufgrund der von den Gerichten relativ hoch angesetzten Streitwerte erhebliche Kostenrisiken für die WLAN-Betreiber bedeuten. Im Falle einer möglichen einstweiligen Verfügung, kann der WLAN-Betreiber zu kostenintensiven Ad-hoc-Maßnahmen gezwungen werden, die bis zur faktischen Aufgabe des Dienstes reichen können.

Die von einem WLAN-Betreiber zur Vermeidung einer möglichen Inanspruchnahme vorab getroffenen Schutzmaßnahmen (Registrierung der Nutzer, technische Einschränkungen des Dienstes) schränken die Nutzer ein und machen die WLAN-Angebote auch für rechtmäßig handelnde Nutzer weniger attraktiv.

Zu e)

Die umfassende und klare Haftungsprivilegierung in § 8 TMG sollte uneingeschränkt auch für WLAN-Betreiber und auch für Ansprüche aus der sog. Störerhaftung gelten. Die Vorschrift sieht zudem bereits vor, dass ein vorsätzliches Mitwirken an Rechtsverletzungen das Haftungsprivileg entfallen lässt.

Zu f)

Nach unserer Einschätzung bestehen bei privaten wie bei gewerblichen/institutionellen Betreibern die gleichen Risiken. Eine unterschiedliche Behandlung erscheint daher nicht zweckmäßig.

Zu g)

Das TKG sieht klare Regelungen vor, wann und unter welchen Voraussetzungen Behörden Maßnahmen ergreifen dürfen, die von Telekommunikationsanbietern umzusetzen sind.

Zu h)

Nein. S.o. e)

2. Datensicherheit und Datenschutz

Zu a)

Da unverschlüsselte Kommunikation im Internet sehr leicht von jedermann mitgelesen werden kann, erscheint der Wunsch der Nutzer, im Internet nur verschlüsselt zu kommunizieren, nachvollziehbar. Aktivisten für den Datenschutz und Datenschutzbehörden fordern Anbieter seit Jahren auf, den Nutzern verschlüsselte Kommunikation zu ermöglichen. Vor diesem Hintergrund darf nach unserer Einschätzung das Haftungsprivileg des WLAN-Betreibers nicht davon abhängig gemacht werden, ob er nur verschlüsselte oder nur unverschlüsselte Kommunikation ermöglicht.

b)

Nach unserer Auffassung bestehen bereits ausreichende Auflagen für Datenschutz und Datensicherheit.

Fazit

Öffentliche drahtlose lokale Netzwerke (WLAN-Hotspots) sind ein wichtiger Beitrag für die wirtschaftliche, touristische und gesellschaftliche Entwicklung Hessens.

In der digitalen Hauptstadt Europas, der Europastadt Frankfurt, im gesamten Rhein-Main-Gebiet aber auch in der touristisch immer stärker frequentierten Documenta-Stadt Kassel ist der Bedarf besonderes deutlich zu erkennen. In anderen Teilen Hessens besteht dieser jedoch gleichermaßen.

Nur durch das Zusammenwirken unterschiedlicher Technologien und Modelle und dem weiteren Ausbau der bestehenden Angebote kann sichergestellt werden, dass mittelfristig eine optimale und tatsächlich zukunftsorientierte Netzinfrastruktur in hessischen Kommunen entsteht.

Obwohl bereits heute bewährte PPP-Modelle existieren, die einen Aufbau von WLAN Netzen ohne eine Belastung öffentlicher Haushalte ermöglichen, überwiegt bei den zuständigen politischen Entscheidern eine Zurückhaltung, die auf rechtliche Bedenken zurückzuführen ist. Diese Zurückhaltung verhindert wiederum vielerorts die so dringend benötigten Investitionen in den weiteren Netzausbau.

Die mangelhafte Netzinfrastruktur droht mittel- und langfristig zu einem ernsthaften Standortnachteil für Hessen zu werden. Um dies zu verhindern, ist es erforderlich, dass sich der Hessische Landtag und die Hessische Landesregierung auf Bundesebene dafür einsetzen, dass

- klare rechtlichen Grundlagen geschaffen werden, die die Anforderungen von Datenschutzbehörden, Strafverfolgungsbehörden und Rechteinhabern an Betreiber von WLAN-Netzen in Einklang bringen. Hierbei müssen die tatsächlichen Möglichkeiten der Anbieter von WLAN-Hotspots berücksichtigt werden.

- die Störerhaftung neu definiert und das Providerprivileg ausdrücklich auf alle Anbieter von öffentlichen WLAN Netzen ausgedehnt wird.

Diese zwingend erforderlichen Klarstellungen durch den Gesetzgeber werden in Hessen und bundesweit dazu beitragen, dass

- Bedenken und Befürchtungen von kommunalen Entscheidern entgegengewirkt wird und diese sich verstärkt bereit erklären, im Rahmen von PPP-Projekten (und anderen Modellen) den Netzausbau zu befürworten und voranzutreiben;
- Unternehmen verstärkt bereit sind, in diesen Bereich zu investieren.

Damit kann das Land Hessen einen wichtigen Impuls für eine zukunftssichere Infrastruktur in ganz Deutschland geben und seine Wettbewerbsfähigkeit im europäischen Maßstab dauerhaft verbessern.

bitkom

Stellungnahme

Anhörung im Hessischen Landtag zum Thema "Freie WLAN-Hotspots in Hessen"

2. November 2015
Seite 1

Bitkom vertritt mehr als 2.300 Unternehmen der digitalen Wirtschaft, davon gut 1.500 Direktmitglieder. Sie erzielen mit 700.000 Beschäftigten jährlich Inlands-umsätze von 140 Milliarden Euro und stehen für Exporte von weiteren 50 Milliarden Euro. Zu den Mitgliedern zählen 1.000 Mittelständler, 300 Start-ups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Hardware oder Consumer Electronics her, sind im Bereich der digitalen Medien oder der Netzwirtschaft tätig oder in anderer Weise Teil der digitalen Wirtschaft. 78 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, 9 Prozent kommen aus Europa, 9 Prozent aus den USA und 4 Prozent aus anderen Regionen. Bitkom setzt sich insbesondere für eine innovative Wirtschaftspolitik, eine Modernisierung des Bildungssystems und eine zukunftsorientierte Netzpolitik ein.

Wir begrüßen es sehr, mit dem von dem Hessischen Landtag vorgegebenen Fragenkatalog zum Thema „Freie WLAN-Hotspots in Hessen“ unsere Position dazu und zu dem aktuell im Bundesrat diskutierten Regierungsentwurf zur Änderung des Telemediengesetzes vermitteln zu können.

1. Rechtliche Rahmenbedingungen

a) Was ist der rechtliche Unterschied zwischen Content-, Host- und Access Providern und inwiefern ist diese Einordnung für WLAN-Betreiber von Bedeutung?

Die E-Commerce-Richtlinie und so auch das deutsche Telemediengesetz (TMG), das die E-Commerce-Richtlinie umsetzt, unterscheiden zwischen Content-, Host- und Access-Providern. Damit wird zwischen unterschiedlichen Wertschöpfungsebenen im Internet und anhand der Nähe zu und Einwirkungsmöglichkeit auf eine etwaige Gefahrenquelle (bspw. rechtswidriger Inhalt) differenziert. Danach ausgerichtet werden unterschiedliche Haftungskategorien geschaffen, die darauf abstellen, ob es sich um eigene oder fremde Inhalte handelt, und darauf, ob fremde Inhalte gespeichert oder zum Konsumenten nur durchgeleitet werden. Für Access- und Hostprovider schafft die E-Commerce-Richtlinie eine Haftungsprivilegierung (ins nationale

Bundesverband
Informationswirtschaft,
Telekommunikation
und Neue Medien e.V.

Nick Kriegeskotte
Bereichsleiter
Telekommunikationspolitik
T +49 30 27576-224
n.kriegeskotte@bitkom.org

Judith Steinbrecher, LL.M.
Bereichsleiterin Gewerblicher
Rechtsschutz & Urheberrecht
T +49 30 27576-155
j.steinbrecher@bitkom.org

Albrechtstraße 10
10117 Berlin

Präsident
Thorsten Dirks

Hauptgeschäftsführer
Dr. Bernhard Rohleder

www.bitkom.org

Recht umgesetzt in §§ 8 bis 10 TMG), d.h. Accessprovider, die ausschließlich fremde Inhalte durchleiten und nur den Zugang zum Internet gewährleisten, haften für fremde Inhalte gar nicht. Hostprovider, die fremde Inhalte speichern, haften nur, wenn sie Kenntnis von einem Rechtsverstoß haben und nicht sodann, im Rahmen ihrer Möglichkeiten, für Abhilfemaßnahmen bereitstehen.

Für die Einordnung von WLAN-Betreibern ist die Differenzierung zwischen Content-, Host- und Access-Providern allerdings irrelevant. WLAN-Betreiber bieten nicht mehr als einen Internetzugang an, d.h. sie haben auf fremde Inhalte keinerlei Einfluss. Sie sollten deshalb hinsichtlich der Haftungsrisiken genauso behandelt werden wie Access-Provider.

b) Wann erfahren Access-Provider eine Haftungsprivilegierung?

Access-Provider, die fremde Inhalte ausschließlich in einem Kommunikationsnetz übermitteln oder nur den Zugang zur Nutzung vermitteln, haften dann nicht für die illegale Inhalte, wenn sie (1) die Übermittlung der illegalen Inhalte nicht veranlasst haben, (2) den Adressaten der übermittelten Information nicht ausgewählt haben und (3) die illegalen Inhalte nicht ausgewählt oder verändert haben. Darüber hinaus verweist Bitkom auf die einschlägige Rechtsprechung zu § 8 TMG.

c) Welche Maßnahmen müssen Access-Provider ergreifen, wenn wiederholte Rechtsverletzungen auftreten?

Access-Provider müssen, könnten aber auch keine Maßnahmen treffen, wenn wiederholte Rechtsverletzungen auftreten. Aus fernmelde- und datenschutzrechtlichen Gründen werden beim Access-Provider keine Daten gespeichert, die die Zuordnung von wiederholten Rechtsverletzungen zu einzelnen Nutzern ermöglichen würden. Darüber hinaus verweist Bitkom auf die einschlägige Rechtsprechung zu § 8 TMG.

d) Welche Haftungsrisiken bestehen derzeit für WLAN-Betreiber, welche der TMG Privilegierung nicht unterliegen?

Nach der aktuellen deutschen Rechtsprechung kann der Betreiber eines WLAN als Störer für Rechtsverletzungen Dritter auf Beseitigung und Unterlassung in Anspruch genommen werden. Der BGH hat dem Betreiber eines *privaten* WLAN auferlegt, dieses durch Verschlüsselungstechniken gegenüber Zugriffen von außen zu schützen, will er eine Haftung für fremde Rechtsverstöße ausschließen. Damit besteht für WLAN-Betreiber, die es gerade bezwecken Internetzugang für Dritte anzubieten, ein Haftungsrisiko. Die von verschiedenen Landgerichten definierten Pflichten, die daraus resultieren könnten,

reichen von Sperrungen bis hin zu Hinweisen auf die Einhaltung gesetzlicher Vorschriften.

e) Welche Haftungsprivilegierungen *de lege ferenda* sind denkbar?

Zwischen WLAN-Betreibern im privaten, gewerblichen Bereich und Access-Providern sollten keine unterschiedlichen Haftungsregeln gelten. Sie sollten weder auf Beseitigung noch auf Unterlassung haften. Haftungsprivilegierungen sollten nicht an Sicherungsmaßnahmen geknüpft werden, die der Zielsetzung einer Verbesserung des Zugangs zu WLAN-Angeboten widersprechen. Die von den Gerichten für private WLAN-Zugänge präzisierten Obliegenheiten dürfen hierbei nicht undifferenziert auf gewerbliche Angebote übertragen werden.

f) Existieren Gründe, zukünftig zwischen privaten und gewerblichen/institutionellen Betreibern zu unterscheiden?

Erfahrungswerte zeigen, dass WLAN-Hotspots gewerblicher Access-Provider nahezu ausschließlich zum Zwecke der Information und Kommunikation genutzt werden. Wenn überhaupt, spielen sich Rechtsverletzungen im Bereich von privaten WLAN-Zugängen ab.

Daher gilt es aus Sicht des BITKOM, die durch die Rechtsprechung präzisierten Haftungsmaßstäbe und die sich daraus ergebenden Anforderungen für WLAN-Betreiber zu berücksichtigen, aus denen sich insofern unterschiedliche Obliegenheiten für gewerbliche WLAN-Betreiber einerseits und private WLAN-Zugänge andererseits ergeben. Letztere sind nicht auf die besonderen Gegebenheiten von gewerblichen Betreibern großer Hotspot-Angebote übertragbar. Letztlich sind es gewerbliche WLAN-Betreiber, die schon heute ein rechtssicheres Angebot für alle Beteiligten (insbesondere die Nutzer), einschließlich einer Durchsetzbarkeit bei Rechtsverletzungen, schaffen und maßgeblich zu dem Ziel einer möglichst großflächigen Verfügbarkeit von freien WLAN-Angeboten beitragen. Diese bieten darüber hinaus am Markt eine breite Palette an Lösungen an, bei denen sie für Betreiber von privatwirtschaftlichen Einrichtungen (Hotels, Cafés, Restaurants, Freizeitparks, Schwimmbäder etc.), aber insbesondere auch für Behörden und Gemeinden in Räumlichkeiten mit Publikumsverkehr sowie im öffentlichen Raum WLAN-Angebote realisieren und sich um Maßnahmen zur Vermeidung von Haftungsrisiken bemühen.

g) Bestehen neben den zivilrechtlichen Haftungsfragen sicherheitspolitische bzw. strafverfolgungserhebliche Bedenken?

Die Bedeutung der WLAN-Betreiberhaftung für die Sicherheitspolitik und die Strafverfolgung wird in der politischen Debatte zu den gewerblichen WLAN-Zugängen regelmäßig überschätzt.

Urheberrechtsverletzungen (in Form von illegalem File-Sharing) über geschäftliche offene WLAN-Zugänge kommen nicht vor. Dies gilt insbesondere für die gewerblichen Hotspots. Hinsichtlich der strafrechtlichen Verfolgung von Urheberrechtsverletzungen dürften demnach keine Bedenken bestehen.

Aus Sicht des Bitkom wirft lediglich eine etwaige Ausweitung des Angebotes privater WLAN-Zugänge sicherheitspolitische bzw. strafverfolgungserhebliche Fragen auf.

So unterliegen gewerbliche Anbieter bzw. Telekommunikationsnetzbetreiber, die WLAN-bezogene Internetzugangsdienste anbieten, gemäß den Vorgaben des Telekommunikationsgesetzes (TKG) sowie der Bundesnetzagentur der Verpflichtung zur Umsetzung von Anordnungen zur Überwachung der Telekommunikation. Sie treffen dazu umfangreiche technische Vorkehrungen, um im Einzelfall entsprechenden richterlichen Beschlüssen für Strafverfolgungszwecke nachzukommen.

Bitkom geht davon aus, dass grundsätzlich auch alle natürlichen und juristischen Personen (z.B. Städte und Gemeinden, aber auch Unternehmen und Vereine), die WLAN-basiert Zugänge zum Internet für die Öffentlichkeit (z.B. auch durch Aggregation von WLAN-Zugangspunkten an Endnutzerstandorten) anbieten, zum Kreis der Verpflichteten gehören müssten.[1]

Dies ist zum einen schon aus Gründen der Gleichbehandlung und zur Vermeidung von Wettbewerbsverzerrungen geboten. Zum anderen aber auch deshalb, um das Entstehen eines nicht unerheblichen Angebotes an öffentlichen WLAN-Zugängen zu vermeiden, das im Ernstfall für Strafverfolgungsbehörden nicht greifbar ist.

Angesichts unklarer Abgrenzungsfragen hinsichtlich der Eigenschaft als gewerblicher Erbringer öffentlich zugänglicher Telekommunikationsdienste im Kontext von WLAN-Angeboten sowie unter Berücksichtigung von auf der Nutzung privater Internetzugänge basierenden Modellen, bei denen der gesamte Datenverkehr aus dem offenen WLAN per VPN ins Ausland getunnelt wird, muss eine Öffnung privater WLAN-Zugänge für Dritte

[1] Siehe dazu im Detail die Bitkom-Stellungnahme Umsetzung von Überwachungsmaßnahmen gem. § 110 TKG - Überwachung von WLAN-bezogenen Internetzugangsdiensten vom 04. März 2015

aus Sicht des Bitkom erheblichen sicherheitspolitischen und strafverfolgungserheblichen Bedenken begegnen.

h) Wie ist die strafrechtliche Verantwortlichkeit von Betreibern offener WLAN-Netze einzuordnen in Hinblick auf Beihilfe, Mittäterschaft und (Eventual-)Vorsatz?

WLAN-Betreiber können als Vermittler von Internetzugängen nicht als Teilnehmer geschweige denn als Täter verantwortlich gemacht werden. Allein aus fernmelde- wie auch datenschutzrechtlichen Gründen können sie die Nutzung des Internet-Zugangs nicht kontrollieren und damit auch nicht zur Verantwortung gezogen werden. Darüber hinaus verweist Bitkom auf die einschlägige Rechtsprechung.

2. Datensicherheit und Datenschutz

a) Aus welchen Gründen ist es nicht sinnvoll Haftungsprivilegierungen nur für verschlüsselte Verbindungen vorzusehen?

Es widerspricht der Zielsetzung einer Verbesserung des Zugangs zu WLAN-Angeboten, eine Haftungsprivilegierung für die Betreiber von offenen WLAN-Zugängen unter die Pflicht zu Sicherungsmaßnahmen zu stellen.

Mit einer Verknüpfung von Haftungsprivilegierung und Verschlüsselungspflicht würde man unreflektiert die für private WLAN Zugänge in der deutschen Rechtsprechung entwickelten Obliegenheiten auf alle Anbieter übertragen. Dabei wird aber übersehen, dass die für private WLAN-Zugänge entwickelten Grundsätze maßgeblich davon getrieben waren, prozessuale Schutzbehauptungen des Anschlussinhabers im Sinn einer nicht identifizierbaren Drittnutzung durch unberechtigten Zugriff haftungsrechtlich einen Riegel vorzuschieben. Diese Anforderungen sind aber nicht auf die besonderen Gegebenheiten von Betreibern großer geschäftlicher Hotspots übertragbar, bei denen die Drittnutzung gemäß der politischen Motivation explizit gewünscht ist.

Sofern in der aktuellen Diskussion um eine TMG-Novelle beispielhaft auf die Verschlüsselung von WLAN-Routern bzw. eine „WPA2-Verschlüsselung“ verwiesen wird, ist damit jedenfalls keine Verschlüsselung von Verbindungen gemeint, sondern diese wird beispielhaft im Sinne einer Zugangsbeschränkung als Sicherungsmaßnahme diskutiert.

Eine Verschlüsselung dient dem Schutz des Anschlussinhabers vor Datenklau, nicht aber dem Schutz vor illegalen Up- oder Downloads. Diese ist aber regelmäßig gerade nicht Sache des Access-Providers, sondern desjenigen, der ein Angebot im Internet bereitstellt (beispielsweise einer Bank beim Internetbanking) und dazu automatisch eine verschlüsselte Verbindung initiiert.

Darüber hinaus würde mit der Verknüpfung der Haftungsbefreiung an die Verpflichtung zum Einsatz von Sicherungsmaßnahmen gegen europäisches Recht verstoßen. Denn die in Vollharmonisierung festgelegten Regelungen zur Access-Provider-Haftung werden damit unterlaufen.

b) Bedarf es technischer Auflagen für Betreiber zur Gewährung von Datenschutz und Datensicherheit? Gibt es allgemeine Standards?

Dem Bitkom liegen – jedenfalls in Bezug auf gewerbliche WLAN-Betreiber –keine Erkenntnisse über Vorkommnisse in der Praxis vor, die in Bezug auf das Angebot von WLAN-Zugangsdiensten besondere Anforderungen hinsichtlich Datensicherheit und Datenschutz rechtfertigen würden. Die einschlägigen, etwa durch Vorschriften des TKG vorgegebenen Anforderungen an Datenschutz und Datensicherheit sollten selbstverständlich für alle WLAN-Betreiber gelten.

3. Internationaler Vergleich

a) In welchem rechtlichen Rahmen im Hinblick auf zivil- und strafrechtliche Aspekte operieren WLAN-Betreiber im internationalen Vergleich?

In Österreich beispielsweise werden WLAN-Betreiber haftungsrechtlich wie Access-Provider behandelt. Dies spiegelt sich unmittelbar im WLAN-Angebot wieder. Im Verhältnis zur Einwohnerzahl ist Österreich mit seinem WLAN-Angebot führend in Europa.

Das Konstrukt der Störerhaftung ist insbesondere eine deutsche Besonderheit, weshalb in vielen anderen Ländern die Haftungsproblematik wie hier in Deutschland gar nicht erst aufkommt.

b) Welche Erkenntnisse lassen sich hieraus für Deutschland und Hessen ableiten?

Auch Deutschland sollte das Telemediengesetz dahingehend anpassen, dass zwischen WLAN-Betreibern im privaten, gewerblichen Bereich und Access-Providern keine unterschiedlichen Haftungsregeln gelten, so dass in Ländern wie Hessen die offene WLAN-Abdeckung gefördert werden kann.

4. Ausbau

Deutschland verfügt insgesamt bereits über eine gute Breitbandversorgung – sowohl im Festnetz-, insbesondere aber auch im Mobilfunkbereich. Ziel muss es zunächst sein, so viel wie möglich an privaten, eigenwirtschaftlichen Investitionen in einen zukunftsfähigen weiteren Breitbandausbau auszulösen. Zu berücksichtigen ist insoweit auch, dass WLAN-Zugänge oder WLAN-Netze kein Ersatz sein können für die Verfügbarkeit leistungsfähiger Breitbandinfrastrukturen, sondern diese lediglich ergänzen können. Zudem bedarf jeder WLAN-Hotspot immer auch einer festnetzbasierten Anbindung.

Wir halten freies WLAN dort für sinnvoll und angemessen, wo Unternehmen oder Kommunen öffentliche Orte attraktiver machen möchten und wo der Bedarf für eine kabellose Datennutzung vorhanden ist. Dort kann öffentliches WLAN eine sinnvolle Ergänzung zu bestehenden Telekommunikationsinfrastrukturen sein.

a) Welche Gründe sprechen für und gegen öffentliche Förderungen bei Aufbau und/oder Betrieb von WLAN-Netzen?

Grundsätzlich kann eine öffentliche Förderung aus Sicht des Bitkom immer nur als ergänzendes, nachrangiges Instrument eines privatwirtschaftlichen Ausbaus in Betracht kommen, auch weil Verzögerungs-, Mitnahme- und langfristige wettbewerbliche Verzerrungseffekte unvermeidlich sind. Förderungen, seien sie von öffentlicher oder privater Seite erbracht, können in Fällen des Marktversagens einen Beitrag zum beschleunigten Aufbau einer öffentlich zugänglichen WLAN- Infrastruktur leisten, insbesondere, soweit es sich um substanzielle Unterstützungsleistungen handelt. Handlungsspielräume der Gebietskörperschaften und Träger öffentlicher Einrichtungen können im Einzelfall genutzt werden, um mittels öffentlicher Förderung die Realisierungschance des Aufbaus und/oder Betriebs von öffentlich zugänglichen WLAN-Zugängen dort zu erhöhen, wo ein Marktversagen festgestellt wurde. Der privatwirtschaftlichen Erschließung mit TK-Dienstleistungen ist nach dem europäischen Telekommunikations- und Beihilferecht

Vorrang einzuräumen. Nur dort, wo mittelfristig über den Markt ein konkret festgestellter Bedarf nicht gedeckt wird, kann eine Förderung mit öffentlichen Mitteln erfolgen.

Öffentlich zugängliche WLAN-Zugänge werden allerdings sowohl im öffentlichen Raum und/oder öffentlichen Einrichtungen, als auch in vorwiegend zur privaten Nutzung vorgesehenen Gebäuden und Flächen realisiert. Den Erfahrungen von BITKOM-Mitgliedsunternehmen nach sind solche Modelle vorzugswürdig und erfolgreich, bei denen Gemeinden, die Bedarf für freies WLAN an einem öffentlichen Ort sehen, dies mit einem Telekommunikationsnetzbetreiber bzw. einem gewerblichen Anbieter von WLAN-Diensten als Partner realisieren. Diese halten entsprechende Angebote vor, bei denen nicht nur ein leistungsfähiger Internetz-Zugang geboten, sondern auch für die Umsetzung der erforderlichen Sicherungsmaßnahmen zur Vermeidung von Haftungs- und Datensicherheitsrisiken gesorgt wird. Dabei können die Gemeinden, die (anteilig durch den Bezug entsprechender Angebote aus dem Markt die Kosten für Aufbau und Betrieb tragen) u.a. entscheiden, zu welchen Bedingungen für den Nutzer ein WLAN-Zugang bereitgestellt wird, ob dieser zeitlich begrenzt sein oder unbegrenzt kostenfreies Surfen möglich sein soll. Auf diese Weise werden bereits heute rechtssichere Angebote für die Beteiligten geschaffen. Bei diesen Lösungen stehen kommerzielle Vereinbarungen als Basis einer Versorgung klar im Vordergrund, also eine Realisierung aufgrund privater Initiative mit durchweg beeindruckenden Ergebnissen. Zudem bieten die Telekommunikationsanbieter – über ihren vorbestehenden Kundenstamm hinausreichend – zahlreiche Möglichkeiten für Verbraucherinnen und Verbraucher, WLAN-Zugänge oder andere Formen des Zugangs zu einer mobilen Breitbandversorgung zu nutzen. Angesichts eines in wenigen Jahren erreichten Versorgungsgrades von mindestens 95 % (Fläche, städtischer Bereich höher) mit schnellen breitbandigen Internetzugängen mittels LTE wird eine mobil und standortungebunden nutzbare Breitbandinfrastruktur zur Verfügung stehen.

Insgesamt betrachtet sollte der Einsatz von Förderungen den Ausbau derartiger Ansätze nicht behindern, sondern lediglich im Einzelfall zur Ergänzung herangezogen werden, etwa dort, wo die Errichtung einer zusätzlichen Versorgung nicht in einer dem Modell geschäftlicher Initiativen folgenden Art und Weise erfolgen kann. Insofern stellt sich bereits die Frage, ob mittelfristig überhaupt eine Unterversorgung feststellbar ist. Zumal es nicht darum gehen kann, eine konkrete technische Lösung (WLAN) zu fördern, wenn die mittels dieser Lösung zu deckenden Bedarfe (hier: nach mobiler Nutzung eines Breitbandzugangs) bereits über andere technische Lösungen – wie z. B. LTE – gedeckt werden können.

b) Welche Instrumente der Förderung existieren? Welche sind Ihnen bekannt?

Soweit uns bekannt, gelangen bislang im Wesentlichen Investitionszuschüsse, Gestattungsrechte sowie die operative Unterstützung bei der Realisierung als Förderungsinstrumente zum Einsatz. In der Regel werden an eine Förderung die Voraussetzungen gestellt werden müssen, dass diese einerseits substanziell und der vorliegend angestrebten Versorgungssituation angemessen ist und andererseits durch die Nutzung verschiedener Instrumente insgesamt ein relevanter Grad an Unterstützung erzielt werden kann. Soweit eine allgemeine Förderung des Breitbandausbaus als Grundlage für WLAN-Netzwerke erfolgen soll, sind aus Sicht des Bitkom eine Förderung durch den Ausgleich von Wirtschaftlichkeitslücken und die Förderung von Betreibermodellen Bausteine eines flächendeckenden Breitbandausbaus und kommen daher grundsätzlich auch als Instrumente für den Ausbau von WLAN in Betracht.

Welche weiteren Formen der Förderung wären denkbar?

Nach hiesiger Einschätzung würde insbesondere ein Verzicht auf die Erhebung von Entgelten zur Abgeltung von Sondernutzungsrechten bei Outdoor-Standorten eine weitere ergänzende Maßnahme darstellen.

c) Welche Betreibermodelle existieren? Welche Modelle werden am häufigsten gewählt und wie kann man dies erklären?

Viele Unternehmen bieten hier Lösungen sowohl im B2C Geschäft als auch im B2B2C Bereich an.

d) Welche Rolle kann das Modell "Freifunk" für den Ausbau des WLAN in Hessen spielen?

Zunächst erlauben wir uns darauf hinzuweisen, dass eine WLAN-Versorgung über den sog. „Freifunk“ zunächst eine Versorgung von (Ausgangs-)Standorten der entsprechenden Anbieter des Modells voraussetzt, die in aller Regel durch Internetzugangsanbieter realisiert wird. Das Modell „Freifunk“ selbst stellt gerade nicht den für ein attraktives WLAN-Angebot stets erforderlichen Netzzugang bereit. Vielmehr basieren auf die Nutzung privater Internet-Zugänge ausgelegte WLAN-Angebote immer auf der Infrastruktur, die erst im Wege des Breitbandausbaus der deutschen Telekommunikationsnetzbetreiber geschaffen wurde und geschaffen wird. Das Modell „Freifunk“ muss aus Sicht des Bitkom u.a. wegen unklaren Abgrenzungsfragen hinsichtlich der Eigenschaft als gewerblicher Erbringer öffentlich zugänglicher Telekommunikationsdienste im Kontext von

WLAN-Angeboten sowie mit Blick auf sicherheitspolitische und strafverfolgungserhebliche Fragen beantworten, die bisher offen geblieben sind.

Ein im Zweifel von vornherein auf Umgehung einschlägiger Anforderungen angelegtes (sowie ggf. auf der AGB-widrigen Nutzung privater Breitbandanschlüsse basierendes) Modell, dass letztlich die Verfolgung von Rechtsverletzungen – gerade auch im Bereich des Urheberrechts – erschwert, sollte daher nach Einschätzung des Bitkom für den Ausbau des WLAN in Hessen keine staatlich unterstützte Rolle spielen.

e) Welche Faktoren sind für eine leistungsfähige Versorgung öffentlicher Räume und Plätze mit WLAN von Relevanz?

In erster Linie sind Faktoren performanter Versorgung öffentlicher Räume und Plätze die Verfügbarkeit geeigneter Standorte für WLAN Access Points und der darüber hinaus benötigten Infrastruktur. Grundvoraussetzung ist, dass eine breitbandige Anbindung dieser Standorte realisiert werden kann. Eine solche Anbindung ist an öffentlichen Plätzen, zum Beispiel in Parks, häufig nicht verfügbar und muss erst kostenintensiv erstellt werden. Zusätzlich müssen WLAN-Hotspots entweder an privaten, öffentlichen oder auch architektonisch besonders schützenswerten Gebäuden und Orten installiert werden. Hierbei müssen die Interessen der Eigentümer gewahrt und Auflagen zu Denkmal- und Ensemble-Schutz berücksichtigt werden. Außerdem müssen mit den Gebäudeeigentümern Regelungen über die Stromversorgung getroffen werden.

f) Welche Gründe sprechen für eine Zusammenarbeit, der Kommunen, der Städte, der Landkreise und des ÖPNV beim Aufbau eines öffentlichen WLAN? Welche Gründe sprechen dagegen?

Siehe bitte zunächst die Antwort auf Frage 4. a), was den klaren Vorrang privatwirtschaftlicher Aktivitäten anbelangt: Handlungsspielräume für Gebietskörperschaften und von kommunalen Betrieben wie ÖPNV-Unternehmen können im Einzelfall genutzt werden, um die Realisierungschance des Aufbaus und/oder Betriebs von öffentlich zugänglichen WLAN-Zugängen zu erhöhen. Und zwar dort, wo ein Marktversagen festgestellt wurde. Der privatwirtschaftlichen Erschließung mit TK-Dienstleistungen ist nach dem europäischen Telekommunikations- und Beihilferecht stets Vorrang einzuräumen. Nur so fern, wie mittelfristig über den Markt ein konkret festgestellter Bedarf nicht gedeckt wird, kann eine Förderung mit öffentlichen Mitteln erfolgen. (In diesem Kontext sei darauf hingewiesen, dass auch der Ausbau eines WLAN-Netzes aus Mitteln einer Gebietskörperschaft oder eines kommunalen Unternehmens eine Beihilfe darstellt.)

Insofern stellt sich bereits die Frage, ob mittelfristig überhaupt eine Unterversorgung feststellbar ist. Zumal es nicht darum gehen kann, *eine konkrete technische Lösung (WLAN) zu fördern*, wenn die mittels dieser Lösung zu deckenden *Bedarfe* von den Verbrauchern bereits über andere technische Lösungen gedeckt werden können.

Davon zu unterscheiden sind Lösungen, wo Gebietskörperschaften oder ÖPNV-Unternehmen nicht selbst WLANs errichten, sondern entsprechende Dienstleistungen bei TK-Netzbetreibern und –Zugangsdiensteanbietern einkaufen. Diese Lösungen sind auf jeden Fall vorzuziehen.

Je nach verfolgtem Modell und der Tiefe eines eigenen Engagements seitens der öffentlichen Hand im (Ausnahme-)Einzelfall kann die Nutzung möglicher Synergieeffekte einer gemeinsam angeschafften Hardware einen Vorteil darstellen: des Weiteren dürfte gelten, dass je größer der abgedeckte Bereich, desto attraktiver das Angebot für die Nutzer derartiger WLAN-Zugänge. Eher problematisch dürften sich dagegen u.a. der erforderliche Koordinationsaufwand sowie der Prüfaufwand im Hinblick auf geeignete Rechtsinstrumente für diese Form von (Körperschafts-übergreifender) Zusammenarbeit darstellen. Aus allgemeinen ordnungspolitischen Erwägungen heraus ist die Errichtung einer von der öffentlichen Hand zu tragenden Infrastruktur für öffentlich zugängliche WLAN Hot Spots besonders zu hinterfragen.

g) Wer trägt die Kosten für den Aufbau und Betrieb von WLAN-Netzen?

Die Entscheidung über die Kostentragung/-aufteilung ist grundsätzlich abhängig vom Geschäftsmodell, das bei der Errichtung von WLAN-Netzen zur Anwendung gelangt.

5. Wirtschaftliche Bedeutung und Effekte

a) Welchen Nutzen haben Städte und Gemeinden durch frei öffentlich zugängliche WLAN-Netze?

Wie bereits dargestellt, ist aus Sicht des Bitkom freies WLAN dort sinnvoll und angemessen, wo Unternehmen oder Kommunen öffentliche Orte attraktiver machen möchten und wo der Bedarf für eine kabellose Datennutzung vorhanden ist. Dort kann öffentliches WLAN eine sinnvolle Ergänzung zu bestehenden Telekommunikationsinfrastrukturen sein. Öffentliches WLAN ist daher als komplementär im Rahmen einer zunehmend konvergenten Nutzung und nicht als Substitut in Bezug auf das bereits nahezu flächendeckende, umfangreiche und zu attraktiven Konditionen für die Nutzer bestehende Angebot an mobilfunkbasierten Internetzugangsdiensten zu sehen.

b) Haben frei öffentlich zugängliche WLAN-Netze auch für die Tourismuswirtschaft eine Bedeutung?

Für Städte und Gemeinden sowie auch für Unternehmen kann ein mit einem Telekommunikationsnetzbetreiber bzw. einem gewerblichen Anbieter von WLAN-Diensten als Partner realisiertes offenes WLAN-Angebot ein zusätzlicher Faktor sein, um an – insbesondere touristisch relevanten – Orten mit Publikumsverkehr die eigene Attraktivität zu erhöhen. Allerdings ist zu bedenken, dass die Tourismuswirtschaft ihrerseits zumindest in bestimmten Bereichen eigene Anstrengungen unternimmt, um Besucherinnen und Besuchern eine (häufig für diese kostenfreie) Nutzung von WLAN-Zugängen zu ermöglichen (Hotels, Restaurants, Cafés etc.).

c) Welchen Nutzen haben andere Wirtschaftssektoren und Branchen durch frei öffentlich zugängliche WLAN-Netze?

Neben dem Bereich Touristik können wirtschaftlich positive Effekte dort entstehen, wo aufgrund einer längeren Verweildauer oder durch Angebot und Nutzung standortbezogener Dienste zusätzliche Umsätze generiert werden. Gewerbliche Anbieter von WLAN-Diensten stehen aber auch hier als Partner für die Tourismuswirtschaft zur Verfügung, teils auch mit speziell auf diese zugeschnittenen Landing-Pages bei der Einwahl in das WLAN-Netz, auf der ortsbezogene Informationen und Angebote bereitgestellt werden können.

d) Sind Auswirkungen auf (lokale) Telekommunikationsbetreiber zu erwarten, die inzwischen vergleichbare Leistungen (z. B. LTE) im Rahmen von Nutzerverträgen gegen Rechnung zur Verfügung stellen?

Eine pauschale Antwort auf diese Fragestellung erscheint schwierig, nicht zuletzt, weil diesseits keine umfassende Beurteilung vorbestehender oder geplanter Versorgungen und zugehöriger Geschäftsmodelle möglich ist. Die Bestimmung von konkreten Auswirkungen wird also auch Einzelfall-bezogen zu erfolgen haben.

Wie bereits in der Antwort auf Frage 4. a) hervorgehoben, bieten privatwirtschaftlich organisierte Unternehmen der TK-Wirtschaft eine Vielzahl von Modellen an, die den Nutzerinnen und Nutzern einen mobilen und performanten, häufig gerade Standort-übergreifenden Internetzugang ermöglichen. Dabei ist für die WLAN-Nutzung weder durchweg Voraussetzung, dass eine Kundenbeziehung vorbesteht, noch, dass die Kosten von den Nutzerinnen und Nutzern getragen werden müssen (teilweise zeitlich begrenzte Gratisnutzung, teilweise Kostentragung durch Dritte im B2B2C-Modell).

Mögliche Wechselwirkungen auf Telefonie- und Breitbandangebote der TK-Unternehmen durch kostenfreie WLAN-Angebote können nicht ausgeschlossen werden.

e) Was ist beim Ausbau eines öffentlich geförderten und/oder betriebenen WLAN Netzes im Hinblick auf das Wirtschaftsverwaltungsrecht zu beachten, wenn bestehende WLAN-Angebote (z.B. durch die Telekom) bestehen?

Siehe hierzu bitte insbesondere die Antworten auf die Fragen 4. a) und f). In einem weit verstandenen Sinne gehört zum Wirtschaftsverwaltungsrecht auch der Grundsatz nur subsidiären Tätigwerdens der öffentlichen Hand. Eine konkrete Ausprägung erfährt dieses Prinzip in Artikel 87f des Grundgesetzes. Ferner gilt, dass beim Ausbau eines öffentlich geförderten und/oder betriebenen WLAN-Netzes selbstverständlich insbesondere die einschlägigen EU-beihilferechtlichen Vorgaben zu beachten sind. Danach kann ein öffentlich gefördertes Angebot allenfalls dann in Betracht kommen, wenn durch private Anbieter eigenwirtschaftlich eine bedarfsgerechte Versorgung nicht gegeben ist. Auch (kommunal-)verfassungsrechtlich dürften einer Betätigung der öffentlichen Hand im Bereich des Aufbaus von WLAN-Netzen enge Grenzen gesetzt sein.

6. Förderprojekte im Bundesvergleich

a) Welche staatlich geförderten WLAN-Projekte existieren derzeit in Deutschland?

Hierzu liegen Bitkom keine detaillierten Kenntnisse vor. Bekannt ist aber, dass Berlin im Rahmen eines zweijährigen Pilotprojektes 170.000 € Fördergeld für den Aufbau von 650 Hotspots an öffentlichen Gebäuden bereit stellt. Die Fürther Marketingagentur *„abl Social Federation“* will zusätzlich Eigenmittel i.H.v. 500.000€ in das Projekt einbringen.

Digitale Gesellschaft e. V.
Sophienstraße 5
D - 10178 Berlin

+49 30 689 16 575

info@digitalegesellschaft.de
www.digitalegesellschaft.de
@digiges

Berlin, den 2. November 2015

Stellungnahme des Digitale Gesellschaft e.V. zum Thema „Freie WLAN-Hotspots in Hessen“

Hessischer Landtag, Anhörung im Ausschuss für Wirtschaft, Energie, Verkehr und Landesentwicklung, 12. November 2015

Die rasanten Fortschritte im Bereich der Informationstechnologie bieten ein breites Spektrum neuer Möglichkeiten, gerade auch für demokratische Teilhabe, zivilgesellschaftlichen Diskurs, lebenslanges Lernen und innovative Geschäftsmodelle. Wesentliche Voraussetzung einer funktionsfähigen Informationsgesellschaft ist jedoch ein möglichst leichter und kostengünstiger Zugang zum Internet, unabhängig vom konkreten Aufenthaltsort.

Über ortsgebundene Breitband-Anschlüsse und mobile Datenkommunikation stehen zwar relativ leicht zugängliche und leistungsfähige Wege für einen Zugang zum Internet zur Verfügung. Gerade mobile Netzzugänge sind jedoch in der Regel volumenbeschränkt, so dass der Datenfluss nach Ausschöpfen des jeweiligen Kontingents auf äußerst niedrige Geschwindigkeiten gedrosselt wird. Datenintensive Dienste wie Videostreaming sind mobil daher kaum bis gar nicht nutzbar. Viele Netzbetreiber verbieten in ihren AGB außerdem die Verwendung bestimmter Online-Dienste wie etwa Voice-over-IP (z.B. Skype), Instant Messaging (z.B. Threema oder WhatsApp) oder Virtual Private Networks (VPN). Schließlich kann die Nutzung mobiler Datenkommunikation in Deutschland aufgrund der anfallenden Roaming-Gebühren insbesondere für Touristen verhältnismäßig teuer ausfallen, so dass sie im Zweifel nur zögerlich darauf zurückgreifen werden.

Diese Beschränkungen und Nachteile der mobilen Datennutzung lassen sich umgehen, indem der Zugang zum Internet über offene Funknetze, auch WLAN-Hotspots genannt, erfolgt. Hier ist der Kreis der verfügbaren Anwendungen und Online-Dienste in der Regel nicht eingeschränkt und auch die Bandbreite wird für gewöhnlich nicht nach Erreichen einer Volumengrenze gedrosselt. In einer zunehmend digitalisierten Gesellschaft kann die flächendeckende Versorgung mit leistungsstarken Internetzugängen daher durchaus als Teil der öffentlichen Daseinsvorsorge begriffen werden. Naturgemäß sind die staatlichen Möglichkeiten begrenzt, etwa durch den Aufbau von kostenfreien „Bürgernetzen" einen leichteren Zugang zum Netz zu schaffen. Allerdings werden in der Bundesrepublik mehrere Millionen privater und öffentlicher Funknetze (sog. WLANs) betrieben, die grundsätzlich von jedermann in der näheren Umgebung für den Zugang zum Internet genutzt werden könnten. Damit wäre im Grundsatz bereits heute jedenfalls in dichter besiedelten Gebieten nahezu flächendeckend ein Internetzugang für jedermann verfügbar.

Gleichwohl haben freie WLAN-Hotspots und offene Funknetze in Deutschland noch immer Seltenheitswert. Der Gründe dafür liegen weder in einer zu geringen Nachfrage seitens der Nutzerinnen und Nutzer, noch in einem mangelnden Interesse bei potentiellen Anbietern, noch in Gefahren für Datensicherheit und Datenschutz bei unverschlüsselten Netzwerken. Die Mangelsituation wird vielmehr allein durch die gegenwärtige Rechtslage und die damit verbundenen Haftungsrisiken beim Betrieb offener Drahtloszugänge zum Internet verursacht.

1. Rechtliche Rahmenbedingungen

a. Einschlägige Vorschriften

Der Rechtsrahmen für die Haftung beim Betrieb offener Funknetze in Deutschland wird bestimmt durch die EU-Richtlinie 2000/31/EG („Richtlinie über den elektronischen Geschäftsverkehr" oder „E-Commerce-Richtlinie") und ihre einfachgesetzliche Umsetzung im Telemediengesetz (TMG).

Diese Vorschriften kennen unterschiedliche Anbieter von Diensten der Informationsgesellschaft, für die jeweils spezifische Haftungsmaßstäbe gelten. Anbieter, die lediglich fremde Informationen in einem Kommunikationsnetz durchleiten oder den Zugang zu einem Kommunikationsnetz vermitteln, werden als Access-Provider bezeichnet. Für diese gelten nach Artikel 12 der E-Commerce-Richtlinie sowie § 8 TMG Haftungserleichterungen („Providerprivileg"):

Art. 12 Abs. 1 E-Commerce-Richtlinie lautet:

„Die Mitgliedstaaten stellen sicher, daß im Fall eines Dienstes der Informationsgesellschaft, der darin besteht, von einem Nutzer eingegebene Informationen in einem Kommunikationsnetz zu übermitteln oder Zugang zu einem Kommunikationsnetz zu vermitteln, der Diensteanbieter nicht für die übermittelten Informationen verantwortlich ist, sofern er
a) die Übermittlung nicht veranlaßt,
b) den Adressaten der übermittelten Informationen nicht auswählt und
c) die übermittelten Informationen nicht auswählt oder verändert."

§ 8 Abs. 1 TMG lautet:

„Diensteanbieter sind für fremde Informationen, die sie in einem Kommunikationsnetz übermitteln oder zu denen sie den Zugang zur Nutzung vermitteln, nicht verantwortlich, sofern sie
1. die Übermittlung nicht veranlasst,
2. den Adressaten der übermittelten Informationen nicht ausgewählt und
3. die übermittelten Informationen nicht ausgewählt oder verändert haben.
Satz 1 findet keine Anwendung, wenn der Diensteanbieter absichtlich mit einem Nutzer seines Dienstes zusammenarbeitet, um rechtswidrige Handlungen zu begehen."

Vereinfacht besagen beide Vorschriften, dass Anbieter, die lediglich den Zugang zum Netz anbieten, nicht für die Inhalte und Daten verantwortlich sind, welche Nutzerinnen, Nutzer und Online-Dienste über dieses Netz transportieren. Diese Haftungsprivilegierung gilt sowohl für das Zivil- wie für das Strafrecht.

<u>b. WLAN-Störerhaftung</u>

Trotz dieser grundsätzlich klaren Regelungen ist bislang nicht abschließend geklärt, für welche Anbieter die Haftungsfreistellung gilt und unter welchen Voraussetzungen sie greift. Während die Rechtsprechung die Privilegierung bei gewerblichen Anbietern, deren Geschäftsschwerpunkt in der Vermarktung von Internetzugängen liegt („klassische" Provider wie Deutsche Telekom, Vodafone, Unitymedia etc), ohne Weiteres für anwendbar hält, bestehen Unsicherheiten vor allem bei gewerblichen, nichtkommerziellen und rein privaten „Nebenbei-Providern". Darunter fallen etwa Hotels und Cafés, die ihren Gästen offene WLAN-Zugänge anbieten, aber auch Schulen, Jugendeinrichtungen, Initiativen wie die „Freifunker" sowie Privatleute, die ihre Drahtlosnetze für die Allgemeinheit öffnen. Für diese Gruppe von Betreibern nimmt die höchstrichterliche Rechtsprechung eine verschuldensunabhängige Störerhaftung für rechtswidrige

Handlungen Dritter an, die über ein nicht ausreichend gegen Missbrauch gesichertes Netzwerk begangen werden (vgl. BGH, Urteil vom 12. Mai 2010, I ZR 121/08 - „Sommer unseres Lebens").

Die Störerhaftung erstreckt sich dabei zwar nur auf Unterlassungsansprüche, jedoch können auch diese kostenpflichtig abgemahnt werden. Besondere Gefahren gehen sind in diesem Zusammenhang von Abmahnungen wegen vermeintlicher Urheberrechtsverletzungen aus, deren Kosten durchaus vierstellige Beträge erreichen. Die vom Gesetzgeber in § 97a Abs. 3 UrhG vorgesehene Begrenzung der Anwaltskosten für eine erste Abmahnung auf einen Gegenstandswert von 1.000€, mithin Gebühren von rund 150€, bleibt in der Praxis weitgehend wirkungslos: sie gilt nur für natürliche Personen, die weder gewerblich noch in Ausübung einer selbständigen beruflichen Tätigkeit handeln. In Wiederholungsfällen und bei Unbilligkeit greift die Beschränkung ebenfalls nicht. Um diesem Haftungsrisiko zu entgehen, müssen die Betreiber ihre Netze nach Ansicht der Rechtsprechung gegen Missbrauch schützen, indem sie ausreichend sichere Passworte verwenden und ihre Router verschlüsseln. Ob es in diesem Zusammenhang ausreicht, für sämtliche Nutzerinnen und Nutzer dasselbe Passwort zu verwenden, oder ob in jedem Einzelfall ein individuelles Passwort vergeben werden muss, ist dabei ebenso ungeklärt wie die Frage, ob und gegebenfalls wie häufig die Passwörter geändert werden müssen.

2. Auswirkungen

Im Ergebnis führt insbesondere die Rechtsprechung des Bundesgerichtshofs dazu, dass Funknetzwerke der „Nebenbei-Provider" regelmäßig verschlüsselt werden und für die kostenfreie Mitnutzung nicht zur Verfügung stehen.

Offene Netze, auf die Nutzerinnen und Nutzer ohne Zugangshürden zugreifen können, sind in Deutschland daher immer noch sehr selten. Während in den USA gut fünf, im Vereinigten Königreich über 28 und in Südkorea mehr als 37 WLAN-Hotspots auf 10.000 Einwohner kommen, sind es in Deutschland noch nicht einmal zwei.[1]

3. Erwägungen für eine flächendeckende Versorgung mit offenen WLAN-Zugängen

Diese Auswirkungen erscheinen umso nachteiliger, da es eine Reihe guter Gründe gibt, eine möglichst flächendeckende Versorgung mit offenen Netzzugängen zu gewährleisten:

- Bei internationalen Gästen sorgt die hiesige geringe Abdeckung mit offenen WLAN-Zugängen immer wieder für Verwunderung und Verärgerung. Zwar verfügen die meisten Menschen über

1 https://www.eco.de/wp-content/blogs.dir/eco-microresearch_verbreitung-und-nutzung-von-wlan.pdf

einen eigenen, bezahlten mobilen Zugang zum Internet. Ausländische Gäste müssen für dessen Nutzung in Deutschland jedoch häufig hohe Roaming-Gebühren entrichten. Zudem sind mobile Netzzugänge zumeist volumenbeschränkt, so dass die Nutzer nach Ausschöpfen des Kontingents auf Zugänge von dritter Seite angewiesen sind. Die bestehende WLAN-Störerhaftung wirkt sich daher nachteilig auf Tourismus und Fremdenverkehr aus.

- Eine vollständige Haftungsprivilegierung allein für „klassische" Access-Provider verhindert wichtige wirtschaftliche Impulse. Würden hingegen auch nebengewerbliche, nichtkommerzielle und private Funknetzbetreiber von der Haftung freigestellt und in der Folge mehr offene WLAN-Zugänge verfügbar sein, so würde dies auch die Telekommunikationsunternehmen unter Druck setzen, wettbewerbsfähiger zu werden, stärker verbraucherorientiert zu denken und zu handeln und einen deutlichen Mehrwert für kostenpflichtige Zugänge zu schaffen.

- Daneben würden auch Anbieter von Apps und anderen, für mobile Geräte optimierten Anwendungen von einer flächendeckenden Versorgung mit offenen WLANs profitieren: die Häufigkeit und Intensität der Nutzung mobiler Anwendungen würde insgesamt zunehmen, zugleich würde speziell die Nachfrage nach Apps mit lokalem Bezug (etwa Informationen über Geschäfte, Sehenswürdigkeiten etc.) ansteigen und das Marktgeschehen in diesem Bereich befördern. Vorteilhaft könnte sich dies auch für Einzelhandelsgeschäfte auswirken, die auf diese Weise einem „Abwandern" der Kundschaft zu Online-Händlern etwas entgegensetzen könnten.

- Ihre starke IT-Wirtschaft verdanken die USA vor allem einem innovations- und investitionsfreundlichen Klima. Um hier einen wichtigen Impuls in Deutschland zu setzen, brauchen wir eine legislative Kultur, die zunächst einmal Experimente ermöglicht, statt Neues mit präventiven Bedenken zu ersticken. Eventuelle negative Effekte einer bedingungslosen Abschaffung der WLAN-Störerhaftung könnten durch entsprechende gesetzgeberische Vorkehrungen, beispielsweise eine regelmäßige parlamentarische Evaluation der Folgen, abgefedert werden.

- Die digitale Gesellschaft braucht junge Menschen, die gelernt haben, sich über das Internet fortzubilden und medienkompetent damit umzugehen, und nicht Konsumenten, deren Nutzungserfahrung sich auf Facebook, Whatsapp und Youtube beschränkt. Die WLAN-Störerhaftung hält Schulen und Jugendeinrichtungen bislang davon ab, die neuen digitalen Möglichkeiten zur Unterrichtsgestaltung und zur Vertiefung des Gelernten in nennenswertem Umfang zu nutzen.

- Eine nur auf kommerzielle Anbieter beschränkte Abschaffung der Störerhaftung würde es für private WLAN-Betreiber weiterhin unmöglich machen, ihren Zugang bedenkenlos mit anderen Menschen zu teilen. Statt altruistisches, solidarisches Verhalten in einer Art "digitaler Nachbarschaftshilfe" zu fördern, würden damit insbesondere Menschen mit geringem Einkommen von den neuen digitalen Möglichkeiten zur Kommunikation, zur gesellschaftlichen und politischen Teilhabe, zur Fortbildung und zur persönlichen Entfaltung ausgeschlossen.

- Deutschland belegt nicht nur bei der Abdeckung mit offenen Funknetzen im internationalen Vergleich einen der hinteren Plätze; auch beim Breitbandausbau hinkt man hierzulande anderen europäischen Staaten weit hinterher. Offene WLAN-Netze können einen wichtigen Beitrag zur flächendeckenden Versorgung mit Internetzugängen leisten. Dies entspricht sogar den Plänen der Bundesregierung, die laut Digitaler Agenda eine möglichst lückenlose Abdeckung mit Netzzugängen durch einen Technologiemix aus Glasfaser, LTE und Funknetzen sicherstellen will.

- Routerverschlüsselung und Passwortschutz sind für die Sicherheit des Netzwerks und des darüber laufenden Datenverkehrs nicht erforderlich. Der Zugriff fremder Mitnutzer auf private Daten lässt sich mittels allgemein verfügbarer Techniken wie Verschlüsselung der Inhalte oder VLANs (logisch getrennter „privater" und „öffentlicher" Netze innerhalb eines physikalischen WLANs) problemlos ausschließen. Der Hersteller AMV bietet etwa in seinen bekannten Routern der Marke „FRITZ!Box" eine Funktion „WLAN-Gastzugang" an, der nur einen Zugriff auf das Internet bietet, aber keinen Zugriff auf das übrige private Netzwerk. Zusätzliche Kosten für die Nutzung des Zugangs durch Dritte würden für die WLAN-Betreiber in aller Regel nicht anfallen, da WLAN-Router praktisch ausschließlich mit Flatrate-Tarifen, also Pauschaltarifen, genutzt werden. Ob die vertraglichen Beziehungen zum Provider eine Mitnutzung zulassen, ist eine Frage des Einzelfalls. Eine derartige Mitnutzung ist zivilrechtlich jedenfalls nicht a priori unzulässig.

4. Reform der WLAN-Störerhaftung

Verschiedene Vorschläge für eine Reform der WLAN-Störerhaftung liegen auf dem Tisch. Während der Digitale Gesellschaft e.V. bereits im Jahr 2012 einen konkreten Gesetzentwurf für eine bedingungslose Abschaffung der WLAN-Störerhaftung vorgelegt hat, beschloss die Bundesregierung am 16. September 2015 einen Kabinettsentwurf für eine Neuregelung, der jedoch erheblichen europarechtlichen Bedenken begegnet.

a. Kabinettsentwurf zur WLAN-Störerhaftung

Der Kabinettsentwurf (im Folgenden TMG-E) sieht eine Ergänzung des § 8 TMG vor. Diesem sollen zwei Absätze mit folgendem Wortlaut hinzugefügt werden:

„(3) Die Absätze 1 und 2 gelten auch für Diensteanbieter nach Absatz 1, die Nutzern einen Internetzugang über ein drahtloses lokales Netzwerk zur Verfügung stellen.
(4) Diensteanbieter nach Absatz 3 können wegen einer rechtswidrigen Handlung eines Nutzers nicht auf Beseitigung oder Unterlassung in Anspruch genommen werden, wenn sie zumutbare Maßnahmen ergriffen haben, um eine Rechtsverletzung durch Nutzer zu verhindern. Dies ist insbesondere der Fall, wenn der Diensteanbieter angemessene Sicherungsmaßnahmen gegen den unberechtigten Zugriff auf das drahtlose lokale Netzwerk ergriffen hat und Zugang zum Internet nur dem Nutzer gewährt, der erklärt hat, im Rahmen der Nutzung keine Rechtsverletzungen zu begehen."

Während die Ausdehnung des Providerprivilegs in § 8 Abs. 3 TMG-E keinen Bedenken unterliegt, verstoßen die Einschränkungen des § 8 Abs. 4 TMG-E gegen EU-Recht.

aa. Verstoß gegen Artikel 12 E-Commerce-Richtlinie

§ 8 Abs. 4 TMG-E ist nicht mit Art. 12 Abs. 1 der E-Commerce-Richtlinie (s.o.) vereinbar. Art. 12 Abs. 1 E-Commerce Richtlinie zählt abschließend die Bedingungen auf, unter denen Access-Provider nicht für die über ihr Netzwerk übermittelten Informationen verantwortlich sind. Demgegenüber postuliert § 8 Abs. 4 TMG-E speziell für Diensteanbieter von Drahtlosnetzwerken weitere Voraussetzungen für die Haftungsfreistellung („zumutbare Maßnahmen [...], um eine Rechtsverletzung durch Nutzer zu verhindern."). Bereits damit überschreitet die geplante Regelung des § 8 Abs. 4 TMG-E den durch Art. 12 Abs. 1 E-Commerce-Richtlinie gesteckten Regulierungsrahmen.

Hinzu kommt, dass § 8 Abs. 4 Satz 1 TMG-E mit dem unbestimmten Rechtsbegriff der „zumutbaren Maßnahmen" keine klare Eingrenzung der Voraussetzungen vornimmt, unter denen ein Diensteanbieter sich auf die Haftungsfreistellung berufen kann. Auch der nachfolgende Satz, in dem beispielhaft („insbesondere") zwei „zumutbare Maßnahmen" benannt werden, gibt keine erschöpfende Antwort auf die Frage, welche Bedingungen ein Diensteanbieter zu erfüllen hat, um in den Genuss der Privilegierung zu kommen. Entgegen der Vorgabe von Art. 12 Abs. 1 E-Commerce-Richtlinie stellt § 8 Abs. 4 TMG-E daher keineswegs sicher, dass der Diensteanbieter nicht für die übermittelten Informationen verantwortlich ist. Vielmehr entsteht durch die unvollständige Regelung eine neue Rechtsunsicherheit für Diensteanbieter von Drahtlosnetzwerken.

bb. Verstoß gegen Art. 16 EU-Grundrechte-Charta

Die Regelung des § 8 Abs. 4 TMG-E verstößt des Weiteren gegen das EU-Grundrecht auf unternehmerische Freiheit aus Art. 16 EU-Grundrechte-Charta.

Das Recht auf unternehmerische Freiheit umfasst unter anderem das Recht jedes Unternehmens, in den Grenzen seiner Verantwortlichkeit für seine eigenen Handlungen frei über seine wirtschaftlichen, technischen und finanziellen Ressourcen verfügen zu können. § 8 Abs. 4 TMG-E verlangt von einem Unternehmen, das als Diensteanbieter im Sinne der Vorschrift agiert, einen Teil seiner Ressourcen für die geforderten „zumutbaren Maßnahmen" einzusetzen. Daher verkürzt § 8 Abs. 4 TMG-E die in Art. 16 EU-Grundrechte-Charta garantierte unternehmerische Freiheit.

Wie der Wortlaut des § 8 Abs. 4 Satz 1 TMG-E erkennen lässt, sollen die „zumutbaren Maßnahmen" dazu dienen, Rechtsverletzungen durch Nutzer zu verhindern. In Betracht kommen dabei etwa Verletzungen des Urheberrechts, welches als Teil des geistigen Eigentumsrechts dem Schutz des Art. 17 Abs. 2 EU-Grundrechte-Charta unterliegt. Der Europäische Gerichtshof hat bereits entschieden, dass es im Fall mehrerer kollidierender Grundrechte Sache der Mitgliedstaaten ist, bei der Umsetzung einer Richtlinie (hier: E-Commerce-Richtlinie) darauf zu achten, dass sie sich auf eine Auslegung dieser Richtlinie stützen, die es ihnen erlaubt, ein angemessenes Gleichgewicht zwischen den durch die Unionsrechtsordnung geschützten anwendbaren Grundrechten sicherzustellen (vgl. in diesem Sinne Urteil vom 29. Januar 2008, Promusicae, C-275/06, Slg. 2008, I-271, Rn. 68). Ordnet ein Mitgliedstaat zu diesem Zweck bestimmte Maßnahmen an, so müssen diese nach Ansicht des EuGH „hinreichend wirksam sein, um einen wirkungsvollen Schutz des betreffenden Grundrechts sicherzustellen, d.h., sie müssen bewirken, dass unerlaubte Zugriffe auf die Schutzgegenstände verhindert oder zumindest erschwert werden und dass die Internetnutzer, die die Dienste [...] in Anspruch nehmen, zuverlässig davon abgehalten werden, auf die ihnen unter Verletzung des genannten Grundrechts zugänglich gemachten Schutzgegenstände zuzugreifen" (vgl. Urt. v. 27. 03. 2014, C-314/12, Rn 62).

§ 8 Abs. 4 TMG-E erfüllt diese Voraussetzungen nicht. Die in § 8 Abs. 4 Satz 2 TMG-E beispielhaft aufgeführten Maßnahmen sind offensichtlich ungeeignet, Urheberrechtsverletzungen oder andere Rechtsverstöße durch die Nutzer eines Diensteanbieters im Sinne der Vorschrift zu verhindern. Weder die dort vorgesehenen Sicherungsmaßnahmen gegen unberechtigten Zugriff noch die Rechtstreueerklärung verhindern oder erschweren für die Nutzer unerlaubte Zugriffe auf Schutzgegenstände. Faktisch bedeuten diese Maßnahmen nämlich nur, dass die Nutzer sich mit einem öffentlich ausliegenden Passwort einloggen und durch einem bloßen weiteren Mausklick eine Rechtstreueerklärung abgeben müssen, um Zugang zu dem Drahtlosnetzwerk zu erhalten. Auf das, was

die Nutzer anschließend über diesen Zugang im Netz machen, haben die Maßnahmen keinerlei Einfluss.

b. Bedingungslose Abschaffung der WLAN-Störerhaftung

Bereits in der letzten Legislaturperiode hat der Digitale Gesellschaft e.V. eine Gesetzesänderung vorgeschlagen, um die bestehenden Hindernisse zu beheben und eine flächendeckende Versorgung mit offenen Funknetzzugängen effektiv zu fördern.

Aus den bereits oben unter 3. angeführten Gründen sowie den unter 4. a. skizzierten unionsrechtlichen Vorgaben muss das Providerprivileg unserer Ansicht nach unterschiedslos auf sämtliche Personen ausgeweitet werden, die Dritten Zugang zum Internet vermitteln. Die Haftungsfreistellung darf ferner nicht von der Erfüllung besonderer Pflichten oder dem Ergreifen bestimmter Maßnahmen abhängig gemacht werden. Zudem sollte klargestellt werden, dass sich die Haftungsfreistellung auch auf Unterlassungsansprüche erstreckt.

Konkret schlagen wir deshalb vor, § 8 TMG um zwei Absätze mit folgendem Wortlaut zu ergänzen:

„(3) Der Ausschluss der Verantwortlichkeit (Absatz 1) umfasst auch gewerbliche und nichtgewerbliche Betreiberinnen und Betreiber von Funknetzwerken, die sich an einen nicht im Voraus namentlich bestimmten Nutzerkreis richten (öffentliche Funknetzwerke).

(4) Der Ausschluss der Verantwortlichkeit (Absatz 1) umfasst auch Ansprüche auf Unterlassung."

STELLUNGNAHME

An: Ausschuss für Wirtschaft, Verkehr und Landesentwicklung des Hessischen Landtags

Kontakt: Dr. Thomas Sassenberg
M: +49 152 31083281
E: thomas@sassenberg.info

Von: Dr. jur. Reto Mantz, Dipl.-Inf.,
Richter am Landgericht Frankfurt am Main

Dr. Thomas Sassenberg, LL.M.
Rechtsanwalt
Fachanwalt für Medien- und Urheberrecht

Dr. Reto Mantz
M: rm@wlan-recht.de

Datum: 02. November 2015

FREIE WLAN-HOTSPOTS IN HESSEN

A. EINFÜHRENDE ZUSAMMENFASSUNG

I. Derzeitige Rechtslage

(1) Der im internationalen Vergleich geringe Ausbau von öffentlichen WLAN-Hotspots lässt sich damit erklären, dass eine große Unsicherheit potentieller Hotspot-Betreiber hinsichtlich einer möglichen Inanspruchnahme aufgrund von Nutzern des Hotspots über das Internet begangener Rechtsverletzungen besteht. Teilweise wird zudem angeführt, dass kleinere Anbieter mit der Umsetzung der telekommunikationsrechtlichen Anforderungen überfordert sind.

(2) Es besteht Einigkeit dahingehend, dass der Betreiber eines öffentlichen WLAN-Hotspots als sog. Access-Provider der ***telemedienrechtlichen Haftungsprivilegierung*** unterfällt und – vereinfacht – im Rahmen seines typischen Verhaltens als Provider nicht in Anspruch genommen werden kann. Nach der bisherigen Rechtsprechung des Bundesgerichtshof (BGH) gilt diese Privilegierung jedoch nicht für Ansprüche, welche darauf gerichtet sind, dass ein bestimmtes rechtswidriges Verhalten zukünftig zu unterbinden ist (sog. Unterlassungsansprüche). Für diese Unterlassungsansprüche gilt im Grundsatz, dass der Betreiber eines WLAN-Hotspots verpflichtet ist, die ihm zumutbaren Maßnahmen zu ergreifen, um zukünftige Rechtsverletzungen zu verhindern, ohne dass ihm hierbei sein Geschäftsmodell unmöglich gemacht wird. Kommt er den ihm zumutbaren Maßnahmen nach, kann er nicht als sog. ***Störer*** in Anspruch genommen werden. Welche Maßnahmen dies sind, wurde in der höchstrichterlichen Rechtsprechung bisher noch nicht konkretisiert. Die Instanzgerichte gehen bislang zutreffend davon aus, dass keine Maßnahmen zu ergreifen sind.

(3) Als ***Maßnahmen*** werden in diesem Zusammenhang insb. die Verschlüsselung und die Nutzeridentifikation sowie das Sperren und Filtern diskutiert. Die insoweit diskutierten Optionen tragen jedoch nicht zur Rechtssicherheit bei, laufen dem Interesse der Möglichkeit einer einfachen Nutzung entgegen und stellen zudem das Geschäftsmodell des offenen und entgeltfreien WLANs in Frage. Dies hat zur Folge, dass der Betreiber eines offenen WLAN-Hotspots auch dann nicht in Anspruch genommen werden kann, wenn er keine der genannten Maßnahmen ergriffen hat.

II. Aktuelle Entwicklungen

(4) Derzeit sind Verfahren vor dem Europäischen Gerichtshof (EuGH) und dem BGH anhängig, welche zu einer Klärung der offenen Rechtsfragen führen könnten. Der BGH befasst sich in zwei Verfahren mit der Frage, welche Maßnahmen einem Access-Provider zugemutet werden können. Das Landgericht München I hat dem EuGH die Frage vorgelegt, ob die Haftungsprivilegierung des § 8 TMG auch für Unterlassungsansprüche zur Anwendung kommt – dann würde sich die Frage einer möglichen Inanspruchnahme als Störer erst gar nicht stellen – und welche Maßnahmen andernfalls dem Provider zugemutet werden können.

(5) Gleichzeitig hat die Bundesregierung einen Gesetzesentwurf verabschiedet, der eine Änderung des Telemediengesetzes (TMG) vorsieht, und der die Frage der Haftungsprivilegierung für WLANs klären soll. Zu Recht ist dieser Gesetzesentwurf auf Kritik gestoßen. Es ist nicht damit zu rechnen, dass er das Ziel der Förderung des Aufbaus von öffentlichen WLANs erreichen wird, da er insbesondere das (zulässige) Geschäftsmodell öffentlich zugänglicher WLANs in Frage stellt.

(6) Am 16.10.2015 hat der Bundestag zudem das „*Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten*“ verabschiedet (BT-Drs. 18/6391). Die Verpflichtung zur sog. Vorratsdatenspeicherung ist von allen Erbringern von öffentlichen Telekommunikationsdienstleistungen umzusetzen. Auch dieser führt zu einer Unsicherheit bei bestehenden und potentiellen Betreibern von öffentlich zugänglichen WLAN-Hotspots.

III. Förderung durch die öffentliche Hand

(7) Der Vergleich mit anderen Ländern zeigt, dass eine öffentliche Förderung des Ausbaus von öffentlichen WLANs geboten ist und u.a. der Wirtschaft zugute kommen würde. Es ist nicht davon auszugehen, dass dies Mobilfunk- oder Festnetznetzanbieter beeinträchtigen würde. Eine Förderung muss dabei nicht per se finanzieller Art sein. In der Regel verfügen Städte, Kreise und Länder aufgrund ihrer innerstädtischen Gebäude über eine Infrastruktur, welche Anbietern den Aufbau eines öffentlichen WLANs erheblich erleichtert.

B. BEANTWORTUNG DER FRAGEN DES HESSISCHEN LANDTAGS

I. RECHTLICHE RAHMENBEDINGUNGEN

1. WAS IST DER RECHTLICHE UNTERSCHIED ZWISCHEN CONTENT-, HOST- UND ACCESS-PROVIDERN UND INWIEFERN IST DIESE EINORDUNG FÜR WLAN-BETREIBER VON BEDEUTUNG?

(8) Das TMG und die E-Commerce-Richtlinie, deren Umsetzung das TMG dient, unterscheiden allgemein zwischen verschiedenen Diensteanbietern. Die Unterscheidung zwischen den verschiedenen Anbietern ist für alle Diensteanbieter von Bedeutung, da an diese Einordnung jeweils unterschiedliche Folgen geknüpft werden. Diensteanbieter sind u.a. der Content Provider (§ 7 Abs. 1 TMG), der Access Provider (§ 8 TMG) und der Host Provider (§ 10 TMG):

- **Content Provider** ist jeder Diensteanbieter der selbst (eigene) Inhalte bereitstellt, beispielsweise der Betreiber einer redaktionell betreuten Zeitungswebseite oder der Inhaber eines privaten Blogs, auf dem über den letzten Urlaub berichtet wird. Content Provider sind gemäß § 7 Abs. 1 TMG für ihre Inhalte nach den allgemeinen Gesetzen verantwortlich. Für sie greift keine Haftungsprivilegierung.

- **Access Provider** ist nach § 8 Abs. 1 TMG ein Diensteanbieter, der fremde Informationen in einem Kommunikationsnetz übermittelt oder den Zugang zur Nutzung von fremden Informationen vermittelt. Nach der Definition gehört hierzu insbesondere jeder, der den Zugang ins Internet vermittelt.

- **Host Provider** ist gemäß § 10 TMG, wer fremde Informationen für Nutzer speichert. Hierzu gehören insbesondere Plattformbetreiber, die ihren Nutzern die Möglichkeit geben, Informationen zum Abruf im Internet bereitzustellen, beispielsweise eBay, Blog-Portale, E-Mail-Dienste und sogenannte Filehoster.

2. WANN ERFAHREN ACCESS-PROVIDER EINE HAFTUNGSPRIVILEGIERUNG?

(9) Nach § 8 TMG ist eine Verantwortlichkeit des Access Providers ausgeschlossen, wenn es sich bei der von ihm übermittelten Information um (i.) eine fremde Information handelt, der Access Provider (ii.) die Übermittlung nicht veranlasst, (iii.) den Adressaten nicht ausgewählt, (iv.) die übermittelten Informationen nicht ausgewählt oder verändert und (v.) nicht mit dem rechtsverletzenden Nutzer absichtlich zusammengearbeitet hat. Zusammenfassen lässt sich dies dahingehend, dass Access Provider im Hinblick auf die von ihnen über das Netzwerk übermittelten Informationen eine streng neutrale Stellung einnehmen müssen. Weitere Anforderungen sieht § 8 TMG – nach derzeitigem Stand – nicht vor.

(10) Zur Bedeutung der Haftungsprivilegierung für WLAN-Betreiber und insb. zur Anwendbarkeit auf Unterlassungsansprüche siehe auch die Antwort zu Frage I.4 (Rn. 14).

3. Welche Maßnahmen müssen Access-Provider ergreifen, wenn wiederholte Rechtsverletzungen auftreten?

(11) Es ist noch nicht abschließend geklärt, welche Maßnahmen Access Provider ergreifen müssen, nachdem eine Rechtsverletzung auftritt. In diesem Zusammenhang werden verschiedene Maßnahmen diskutiert. Einerseits geht es dabei im weiteren Sinne um „*Sperren und Filtern*“, namentlich durch DNS-Sperren, IP-Sperren, URL-Sperren und Verkehrsfilter. Im Falle wiederholter Rechtsverletzungen eines Nutzers wurde vor einigen Jahren die Aussprache von Verwarnungen verlangt – meist unter den Bezeichnungen „*Three-Strikes-Modell*“ oder „*abgestufte Erwiderung*“. Umsetzungen in anderen Ländern haben sich jedoch als unpraktikabel und unverhältnismäßig erwiesen (näher *Sassenberg*/*Mantz*, WLAN und Recht, 2014, Rn. 236 m.w.N.). Im Hinblick auf WLANs werden derzeit teilweise Verschlüsselung, Registrierung und Belehrung der Nutzer diskutiert (vgl. BT-Drs. 18/5088).

(12) In der Rechtsprechung sind Pflichten für Access Provider auch bei mehrfachem Auftreten von Rechtsverletzungen bisher als gesetzeswidrig oder unverhältnismäßig abgelehnt worden. So haben das OLG Hamburg und das OLG Köln DNS-Sperren, IP-Sperren, URL-Sperren und Verkehrsfilter als unzumutbare Maßnahmen angesehen (OLG Köln GRUR 2014, 1081 – Goldesel; OLG Hamburg GRUR-RR 2014, 140 – 3dl.am; die Entscheidungen sind derzeit als Revision beim BGH anhängig, Entscheidungen werden für den 26.11.2015 erwartet), wobei nach Auffassung von OLG Köln und OLG Hamburg insbesondere URL-Sperren und Verkehrsfilter Eingriffe in das Fernmeldegeheimnis darstellen. Verschlüsselung, Registrierung und Belehrung sind von Access Providern bisher nicht verlangt worden.

(13) Es hat sich herausgestellt, dass diese Maßnahmen praktisch unwirksam und leicht zu umgehen sind. Gegen DNS-Sperren wird insbesondere angeführt, dass sie zum einen durch Verwendung alternativer DNS-Server leicht zu umgehen sind (OLG Hamburg, MMR 2009, 631 – Usenet), und dass sie dazu führen, dass nicht nur rechtswidrige Inhalte blockiert werden, sondern auch andere, legale Inhalte, was als „Overblocking“ bezeichnet wird (OLG Hamburg MMR 2009, 631 – Usenet; OLG Hamburg GRUR-RR 2014, 140 (147) – 3dl.am; OLG Köln GRUR 2014, 1081 – Goldesel). Gleiches gilt für URL-Sperren. Filter, die auf den Datenverkehr selbst abstellen, sind vor allem problematisch, weil die Inhalte zur Kenntnis genommen werden, was einen Verstoß gegen das Fernmeldegeheimnis bedeutet. Darüber hinaus können auch solche Filter Rechtsverletzungen nicht sicher erkennen und zum Overblocking führen.

4. Welche Haftungsrisiken bestehen derzeit für WLAN-Betreiber, welche der TMG-Privilegierung nicht unterliegen?

(14) Nach §§ 7 ff. TMG und in Umsetzung von Art. 12 bis 15 E-Commerce-Richtlinie sollen Internet Service Provider für Rechtsverletzungen ihrer Nutzer nicht haften. Insbesondere sollen ihnen keine proaktiven Überwachungspflichten obliegen. Daher schließen diese – unter den jeweiligen Voraussetzungen – eine Verantwortlichkeit der Internet Service Provider für die rechtswidrigen Handlungen ihrer Nutzer aus. Für

Access Provider greift hierbei die Privilegierung in § 8 TMG, nach dem eine Verantwortlichkeit unter den oben genannten Voraussetzungen ausgeschlossen ist.

(15) Es besteht derzeit kein ernsthafter Zweifel daran, dass auch der Betreiber eines WLANs die Voraussetzungen des § 8 TMG erfüllt (LG München I GRURInt 2014, 1166 – Bring mich nach Hause; AG Berlin-Charlottenburg CR 2015, 192; AG Hamburg CR 2014, 536; AG Hamburg, Urt. v. 24.6.2014 – 25b C 924/13; *Sassenberg*/*Mantz*, WLAN und Recht, 2014, Rn. 211; *Röhrborn*/*Katko*, CR 2002, 882; *Hoffmann*, in: *Spindler*/*Schuster*, Recht der elektronischen Medien, 3. Aufl. 2015, § 8 TMG Rn. 17; *Spindler*, CR 2010, 592 (595); *Altenhain*, in: MünchKommStGB, 2. Aufl. 2010, vor § 7 TMG, Rn. 43; *Kaeding*, CR 2010, 164 (168); *Mantz*, Rechtsfragen offener Netze, 2008, 48).

(16) Danach besteht kein Risiko des Betreibers eines WLANs, für Rechtsverletzungen seiner Nutzer strafrechtlich in Anspruch genommen zu werden oder Schadensersatz leisten zu müssen.

(17) Die Privilegierung findet nach ständiger Rechtsprechung des BGH aber keine Anwendung auf Unterlassungsansprüche, also auf Ansprüche aus Störerhaftung (BGH GRUR 2004, 693 (694) – Schöner Wetten; BGH GRUR 2004, 860 (862 f.) – Internetversteigerung I; auf die Haftung aufgrund Verkehrspflichten soll hier nicht näher eingegangen werden, für sie gilt im Ergebnis dasselbe wie für die Störerhaftung, vgl. *Mantz*/*Sassenberg*, NJW 2014, 3537 (3541)). Dies ist zwar in der juristischen Literatur mit Blick auf eine Vereinbarkeit Art. 15 E-Commerce-Richtlinie wiederholt kritisiert worden, der EuGH hat jedoch im Rahmen der Entscheidung UPC Telekabel trotz Art. 12 bis 15 E-Commerce-Richtlinie Prüfpflichten nicht rundheraus abgelehnt (EuGH GRUR 2014, 468 – UPC Telekabel/Constantin Film). Auf der anderen Seite greift der BGH die Privilegierung mittlerweile auch bei der Störerhaftung ausdrücklich auf und integriert die Vorgaben der E-Commerce-Richtlinie, des TMG und der Rechtsprechung des EuGH in die Bewertung der Prüfungs- und Überwachungspflichten im Rahmen der Störerhaftung (OLG Hamburg GRUR-RR 2014, 140 – 3dl.am; KG Berlin MMR 2014, 46; *Volkmann*, K&R 2013, 257 (258)). Die Frage der Zulässigkeit der Einschränkung der Privilegierung liegt mittlerweile als Vorlagefrage dem EuGH vor. Das LG München I hat Ende 2014 einen Fall eines WLAN-Betreibers zum Anlass genommen, diese und andere Fragen zu § 8 TMG dem EuGH vorzulegen (LG München I GRUR Int. 2014, 1166 – Bring mich nach Haus).

(18) Als Haftungsrisiko verbleibt beim Betreiber eines WLANs daher die Haftung auf Unterlassung nach den Grundsätzen der sog. Störerhaftung. Dies bedeutet, dass der Betreiber verpflichtet sein kann, bestimmte Maßnahmen zur Verhinderung von Rechtsverletzungen zu ergreifen. Als Störer kann dabei grundsätzlich derjenige in Anspruch genommen werden, der (i.) adäquat-kausal an einer Rechtsverletzung mitwirkt und (ii.) hierbei seine so genannten Prüfungs- und Überwachungspflichten verletzt hat. Ein Verschulden ist hierfür nicht erforderlich. Die erste Voraussetzung der Störerhaftung, eine adäquat-kausale Mitwirkung an der Rechtsverletzung des Nutzers, liegt jedenfalls in der Vermittlung des Zugangs zum Internet – auch über WLAN – vor

(BGH NJW 2010, 2062 – Sommer unseres Lebens; LG Frankfurt a.M., MMR 2011, 401; LG Frankfurt a.M. GRUR-RR 2013, 507 – Ferienwohnung; a.A. noch OLG Frankfurt a.M., MMR 2008, 603.) Insofern stellt sich die Frage, ob und gegebenenfalls wann durch den WLAN-Betreiber Prüfungs- und Überwachungspflichten verletzt werden. Hierunter werden bestimmte – nicht genau konkretisierte – Maßnahmen verstanden, die ein Betreiber zur Verhinderung von Rechtsverletzungen ergreifen soll. Die konkreten Pflichten sind (bisher) nicht gesetzlich geregelt, sondern werden maßgeblich von der Rechtsprechung in Einzelfallentscheidungen herausgebildet. Ein anschauliches Beispiel für eine auf Grund von Prüfungs- und Überwachungspflichten zu ergreifende Maßnahme kann die Pflicht von Eltern sein, ihre minderjährigen Kinder vor der Erlaubnis der Nutzung des familiären Internetzugangs darauf hinzuweisen, dass der Internetanschluss nicht für rechtswidrige Handlungen genutzt werden soll (BGH NJW 2013, 1441 – Morpheus).

(19) Welche Prüfungs- und Überwachungspflichten jeweils verlangt werden können, ist eine Frage des Einzelfalls. Dafür haben sich in der Rechtsprechung in unzähligen Entscheidungen bestimmte Kriterien herausgebildet. Zu unterscheiden ist zwischen denjenigen Kriterien, die den Anbieter und das Angebot auf der einen Seite und die zur Verhinderung von Rechtsverletzungen möglicherweise zu ergreifenden Maßnahmen auf der anderen Seite betreffen. Stark verkürzt lässt sich festhalten, dass jedenfalls bei rechtmäßigen Geschäftsmodellen zu entscheiden ist, welche Maßnahmen dem Betroffenen möglich und zumutbar sind. Dabei ist im Rahmen der Zumutbarkeit für jede konkrete Maßnahme eine Abwägung der Interessen des Geschädigten, des vermittelnden Anbieters und der Allgemeinheit durchzuführen (BGH NJW 2004, 2158 (2159) – Schöner Wetten; BGH MMR 2004, 668 – Internet-Versteigerung I; BGH MMR 2007, 634 (637) – Jugendgefährdende Medien bei Ebay; BGH NJW 2013, 784 Rn. 31 – Alone in the Dark), wobei beim Angebot rechtmäßiger und von der Rechtsordnung gebilligter Geschäftsmodelle – dazu gehört das Angebot des Zugangs zum Internet und auch WLAN – die Grenze der Zumutbarkeit überschritten ist, wenn das Geschäftsmodell erheblich beeinträchtigt wird (BGH MMR 2011, 172 (173) – Kinderhochstühle im Internet; BGH MMR 2007, 634 (637) – Jugendgefährdende Medien bei Ebay; BGH NJW 2013, 784 Rn. 22 – Alone in the Dark).

(20) Wird der Betreiber eines WLANs als Störer in Anspruch genommen, kann zusätzlich ein Anspruch auf Ersatz von Abmahnkosten bestehen. Da bisher unklar ist, ob überhaupt und welche Pflichten Access Provider (und damit WLAN-Betreiber) ergreifen müssten, besteht insoweit zusätzlich ein Risiko.

5. WELCHE HAFTUNGSPRIVILEGIERUNGEN SIND DE LEGE FERENDA DENKBAR?

(21) Denkbar – und aufgrund der bestehenden Unsicherheiten auch sinnvoll – ist eine Klarstellung, wonach die Privilegierung des § 8 Abs. 1 TMG auch für Unterlassungsansprüche Anwendung findet (vgl. BT-Drs. 18/3047 sowie § 8 Abs. 3 Entwurf eines Zweiten Gesetzes zur Änderung des Telemediengesetzes, zu diesem Entwurf eingehend *Mantz*/*Sassenberg*, CR 2015, 298; BR-Drs. 440/1/15).

(22) Der von der Bundesregierung verabschiedete Gesetzesentwurf zur Änderung des TMG (BR-Drs. 440/15) sieht eine solche Klarstellung vor. Nach § 8 Abs. 4 TMG-E soll die Privilegierung für Unterlassungsansprüche jedoch nur greifen, wenn die Betreiber „*zumutbare Maßnahmen ergriffen haben, um eine Rechtsverletzung durch Nutzer zu verhindern*“ Dabei konkretisiert § 8 Abs. 4 S. 2 TMG-E diese Maßnahmen, nämlich (i.) angemessene Sicherungsmaßnahmen gegen den unberechtigten Zugriff auf das WLAN und (ii.) Einholung einer Erklärung des Nutzers, dass dieser im Rahmen der Nutzung keine Rechtsverletzungen begehen wird. Diese Anforderungen müssen dabei kumulativ erfüllt sein, wie schon der Gesetzeswortlaut („*und*“) deutlich macht.

(23) Nach der Gesetzesbegründung sollen als zumutbare Maßnahmen insbesondere die Verschlüsselung des WLANs oder die freiwillige Registrierung der Nutzer dienen. Die Verschlüsselung ist problematisch, da sie für das gesteckte Ziel nutzlos und sogar kontraproduktiv ist. Sie verhindert, dass der Nutzer einfach und unkompliziert den Zugang zum WLAN und damit zum Internet erhält, da immer zunächst ein Schlüssel ausgetauscht werden muss (*Mantz*/*Sassenberg*, CR 2015, 298). Diese Einschränkung gefährdet das Geschäftsmodell von öffentlichen WLANs erheblich. Denn rund 20% der Nutzer von WLANs lassen sich bereits von einfachen Hürden wie einer Vorschaltseite oder Registrierung von der Nutzung eines WLANs abhalten (Befragung Kabel Deutschland, Pressemitteilung v. 6.3.2014, https://www.kabeldeutschland.com/de/presse/pressemitteilung/produktnachrichten/632014.html). Es stellt ein großes Hindernis dar, dass der Nutzer zunächst an den Schlüssel kommen muss. In Restaurants und Cafés mag man den Schlüssel in die Speisekarte drucken können. In einer Vielzahl von Situationen steht dem Betreiber eine solche Möglichkeit aber nicht offen. Unklar ist z.B., wie bei WLAN-Hotspots an Bahnhöfen oder Flughäfen den Nutzern das Passwort mitgeteilt werden soll. Insbesondere ist die Verschlüsselung des WLANs nicht geeignet, Rechtsverletzungen zu verhindern. Denn jeder Nutzer, der den WPA2-Schlüssel erhält, z.B. aus der Speisekarte des Restaurants, ist in der Lage, aus dem WLAN heraus Rechtsverletzungen zu begehen. Darüber hinaus ist die Verschlüsselung auch nicht geeignet, im Falle einer Rechtsverletzung den Täter ausfindig zu machen. Eine Verschlüsselungspflicht wird zusätzlich dazu führen, dass der Großteil der in Deutschland betriebenen öffentlichen WLAN-Hotspots umgerüstet werden muss. Denn bisher war selbst bei der Mehrzahl der WLAN-Hotspots mit Registrierung der Zugang zum WLAN selbst zunächst ohne Passwort möglich. Die Anmeldung erfolgte dann (innerhalb des WLANs) auf einer sog. Splash-Page. Dementsprechend kommen auf Betreiber von WLANs Kosten für die Umrüstung sowie höhere Kosten bei der Neueinrichtung zu. Beispielsweise das von Verkehrsminister Dobrindt (CSU) erst im März 2015 vorgestellte öffentliche und barrierefreie WLAN in 100 Behördengebäuden in Bonn müsste umgerüstet werden. Wie die Benutzung anschließend wieder barrierefrei gewährleistet sein soll, bleibt ebenfalls unklar.

(24) Als Alternative soll der Anbieter eine „*freiwillige Registrierung*“ vornehmen. Dies ist wohl so zu verstehen, dass der Nutzer gebeten werden soll, seine Daten einzugeben, wobei deutlich zu machen ist, dass diese Eingabe freiwillig erfolgt. Es ist davon

auszugehen, dass kaum Nutzer von dieser freiwilligen Möglichkeit Gebrauch machen werden, so dass auch insoweit unklar bleibt, wie diese Maßnahme Rechtsverletzungen verhindern soll.

(25) Auch die Erklärung des Nutzers, dass er keine Rechtsverletzungen begehen werde, ist dem Ziel des Gesetzes nicht förderlich. Dabei soll das Einverständnis in eine entsprechende Klausel in AGB ausreichen. Es ist nicht zu ersehen, wie durch eine solche Erklärung Rechtsverletzungen tatsächlich verhindert werden können (*Mantz*/*Sassenberg*, CR 2015, 298). Es ist zweifelhaft, ob sich Nutzer, die sich zur Vornahme von Rechtsverletzungen entschlossen haben, von einem solchen – konsequenzlosen – Versprechen tatsächlich abhalten lassen werden (*Hullen*, jurisPR-ITR 7/2015, Anm. 2: „Placebo“; *Bergt*, CR-Online v. 1.3.2015, http://www.cr-online.de/blog/2015/03/01/gesetzentwurf-zur-abschaffung-freier-wlans.). Dem folgend geht die Rechtsprechung bezüglich der Störerhaftung von jeher davon aus, dass der Täter eigenverantwortlich handelt und der Anbieter von dessen rechtskonformem Verhalten ausgehen darf (vgl. BGH GRUR 2003, 969 – Ausschreibung von Vermessungsleistungen; *Mantz*, GRUR-RR 2013, 497). Eine entsprechende Erklärung in AGB wird generell für untauglich gehalten (OLG Hamburg, Urt. v. 28.1.2009 – 5 U 255/07, NJOZ 2009, 1595 (1619) – alphaload). Darüber hinaus sind Vorschaltseiten zwar eine praktikable Lösung, technisch aber schwierig zu realisieren. In der Regel wird der Nutzer beim Aufruf irgendeiner Webseite im WWW durch einen „*Trick*“ zwangsweise auf die Splash-Page umgeleitet. Erst nachdem er dort die Erklärung erteilt hat, kann er weitersurfen. Problematisch ist dies bspw., wenn der Nutzer gar kein WWW nutzt, sondern nur am Mobiltelefon die E-Mails über eine Applikation nutzen will. Er erhält keine Fehlermeldung und wird kaum verstehen, warum der Zugang zum Internet „*nicht funktioniert*“.

(26) Dem folgend ist gegen den Gesetzesentwurf heftige Kritik erhoben worden (Nachweise bei *Mantz*/*Sassenberg*, CR 2015, 298, 305). Daraufhin hat auch der Wirtschaftsausschuss des Bundesrats eine Änderung des Gesetzesentwurfs vorgeschlagen (BR-Drs. 440/1/2015), wonach Verschlüsselung, Registrierung und Einholung einer Erklärung nicht mehr erforderlich sein sollen. Der Wirtschaftsausschuss sieht diese als hinderlich bei der Förderung und Verbreitung von WLANs an. Die von der Bundesregierung in ihrem Gesetzesentwurf herausgestellte Gefahr von Rechtsverletzungen erkennt der Wirtschaftsausschuss des Bundesrats nicht. Auch Thüringen plant einen entsprechenden Vorstoß zur Änderung des Gesetzesentwurfs im Bundesrat (Meldung bei Heise-Online v. 27.10.2015, http://www.heise.de/newsticker/meldung/Thueringen-will-WLAN-Anbieter-ganz-von-der-Stoererhaftung-befreien-2860225.html).

6. Existieren Gründe, zukünftig zwischen privaten und gewerblichen/institutionellen Betreibern zu unterscheiden?

(27) Es bestehen keine Gründe, zukünftig zwischen privaten und gewerblichen/institutionellen Betreibern zu unterscheiden. Bisher war eine solche Entscheidung durch die Gerichte auch nicht thematisiert worden. Die Bundesregierung

hatte im ersten Entwurf zur Änderung des TMG noch eine Unterscheidung zwischen gewerblichen/institutionellen („*geschäftsmäßigen*“) und privaten („*nicht geschäftsmäßigen*“) Betreibern vorgesehen (dazu *Mantz*/*Sassenberg*, CR 2015, 298, 300 ff.), hat diese Unterscheidung jedoch auf die erhebliche Kritik daran fallen gelassen. Insbesondere kann von privaten Betreibern nicht mehr verlangt werden als von gewerblichen/institutionellen Betreibern. Dies hat auch der BGH in seiner Entscheidung „*Sommer unseres Lebens*“ herausgestellt (BGH MMR 2010, 565 Rn. 23 – Sommer unseres Lebens). Denn private Betreiber haben meist weniger Sachkenntnis und weniger wirtschaftliche Möglichkeiten.

7. BESTEHEN NEBEN DEN ZIVILRECHTLICHEN HAFTUNGSFRAGEN SICHERHEITSPOLITISCHE BZW. STRAFVERFOLGUNGSERHEBLICHE BEDENKEN?

(28) E-Commerce-Richtlinie und TMG haben eine klare Haftungsregelung für Access Provider getroffen: Wer sich als Diensteanbieter neutral verhält, soll nicht für die Handlungen seiner Nutzer haften. Hierbei wird nicht zwischen „*klassischen*“ Telekommunikationsanbietern und Betreibern von offenen WLANs differenziert.

(29) Im aktuellen Entwurf eines Zweiten Gesetzes zur Änderung des Telemediengesetzes geht die Bundesregierung – ohne nähere Begründung – davon aus, dass mit der weiteren Verbreitung von WLANs die Gefahr von Rechtsverletzungen steigen würde, weil Nutzer darin anonym handeln könnten. Diese Auffassung verkennt, dass sich WLANs im Ergebnis nicht von anderen Mitteln zur Kommunikation unterscheiden und dass es bisher keine nennenswerten Vorfälle von Rechtsverletzungen über öffentliche WLANs gegeben hat (mabb-Stellungnahme v. 7.4.2015,http://www.mabb.de/files/content/document/Stellungnahmen/mabb_Stellungnahme_BMWi_TMGAendG.pdf, S. 3; hierauf stellt auch der Wirtschaftsausschuss des Bundesrates ab, BR-Drs. 440/1/2015, S. 4 f.). Auch bei der Nutzung von „*klassischen*“ Telekommunikationsanbietern ist eine Identifikation möglicher Rechtsverletzer nicht gewährleistet. Einige dieser Anbieter speicherten (im Einklang mit den bisherigen Bestimmungen vor Einführung der Vorratsdatenspeicherung) IP-Adressen ihrer Nutzer nicht. Nach Ende der Verbindung konnte ein bestimmter Nutzer daher nicht mehr identifiziert werden. Auch beim mobilen Internetzugang über das Mobilfunknetz (UMTS oder LTE) konnte der Täter nicht identifiziert werden. Nach Kenntnis der Verfasser hat dies bisher weder zu Problemen noch zu gesetzgeberischer Tätigkeit geführt. Es kann aber keinen Unterschied machen, ob man ein WLAN über einen Mobilfunkanschluss anbindet (sog. Tethering) oder über einen „*klassischen*“ Telekommunikationsanbieter.

(30) Darüber hinaus hat die Bundesregierung auch im „*Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten*“ (Vorratsdatenspeicherungsgesetz, BT-Drs. 18/5088) den Großteil der Betreiber von WLAN-Hotspots von der Speicherpflicht ausgenommen. So bezieht sich die Gesetzesbegründung ausdrücklich (BT-Drs. 18/5088, S. 37) auf eine Einschränkung des Verpflichtetenkreises aufgrund einer neuen Auslegung der Bundesnetzagentur des Begriffs des „Erbringens“ in ihrer Mitteilung Nr. 149/15 (hierzu auch unter B.II.2;

eingehend *Sassenberg*/*Mantz*, MMR 2015, 428). Danach sind insbesondere kleinere WLAN-Hotspots, bei denen zur Erbringung ein vorhandene DSL-Anschluss genutzt sowie den Nutzern nur für kurze Zeit und nicht dauerhaft und mittels einer festen IP-Adresse der Zugang zum Internet gewährt wird, nicht als Erbringer von Telekommunikationsdiensten anzusehen. In der Gesetzesbegründung heißt es (BT-Drs. 18/5088, S. 37):

„Nicht verpflichtet sind demnach Anbieter, die ihren Kunden nur eine kurzzeitige Nutzung des Telekommunikationsanschlusses ermöglichen, zum Beispiel Betreiber von Hotels, Restaurants und Cafés, die ihren Kunden eine Telefon- oder Internetnutzung zur Verfügung stellen....“

(31) Weiter sind insbesondere Verletzungen von gewerblichen Schutzrechten nach dem neu gefassten § 100g Abs. 2 StPO nicht als „*besonders schwere Rechtsverletzungen*“ anzusehen, die eine Beauskunftung der durch die Vorratsdatenspeicherung erhobenen und gespeicherten Daten erlauben würde.

8. WIE IST DIE STRAFRECHTLICHE VERANTWORTLICHKEIT VON BETREIBERN OFFENER WLAN-NETZE EINZUORDNEN IM HINBLICK AUF BEIHILFE, MITTÄTERSCHAFT UND (EVENTUAL-)VORSATZ?

(32) Wie oben dargestellt, sind Betreiber von WLAN-Hotspots nach § 8 Abs. 1 TMG privilegiert. Unter den Voraussetzungen der Norm ist eine strafrechtliche Verantwortlichkeit ausgeschlossen. Solange sich der WLAN-Betreiber daher im Hinblick auf die übermittelten Informationen neutral verhält und diese lediglich durchleitet, handelt er weder als Mittäter noch als Beihelfer.

(33) Darüber hinaus hat der WLAN-Betreiber aufgrund seiner neutralen Stellung auch keinen Vorsatz hinsichtlich eventueller rechtswidriger Taten seiner Nutzer. Dies gilt auch im Hinblick auf die Annahme eines Eventualvorsatzes. Solange der Betreiber keine konkrete Kenntnis von konkreten rechtswidrigen Handlungen seiner Nutzer hat oder mit diesen im Sinne von § 8 Abs. 1 S. 2 TMG kollusiv zusammenwirkt, liegt ein Eventualvorsatz nicht vor. Ein solcher ist auch dann nicht anzunehmen, wenn der Betreiber sich grundsätzlich bewusst ist, dass über das Netzwerk rechtswidrige Handlungen begangen werden können. Im Hinblick auf Host Provider ist in der Rechtsprechung bei der hartnäckigen Weigerung der Löschung rechtsverletzender Inhalte teilweise eine Gehilfenhaftung angenommen worden (OLG Hamburg GRUR-RR 2013, 382; LG Frankfurt, Urt. v. 05.02.2014 - 2-06 O 319/13, BeckRS 2014, 03623). Diese Rechtsprechung soll – für Host Provider – nach dem Entwurf eines Zweiten Gesetzes zur Änderung des Telemediengesetzes (BR-Drs. 440/15) in § 10 TMG-E kodifiziert werden. Auf den Access Provider oder den WLAN-Betreiber ist dies aus den oben aufgeführten Gründen nicht übertragbar, was auch die im Entwurf eines Zweiten Gesetzes zur Änderung des Telemediengesetzes klare Unterscheidung zwischen dem Access Provider und dem Host Provider erneut deutlich macht.

II. Datenschutz und Datensicherheit

1. Aus welchen Gründen ist es sinnvoll/nicht sinnvoll Haftungsprivilegierungen nur für verschlüsselte Verbindungen vorzusehen?

(34) Die Verschlüsselung einer Verbindung darf nicht mit dem Erfordernis einer Nutzeridentifikation gleichgesetzt werden. Einer solchen Nutzeridentifikation bedarf es gerade nicht, um eine Verschlüsselung des Verkehrs zu erreichen. Durch eine Verschlüsselung der Verbindung soll und kann vielmehr alleine verhindert werden, dass Dritte den Verkehr ohne größere technische Anstrengung „*mitlesen*“ können. Es steht zu befürchten, dass eine Verschlüsselung eine unnötige zusätzliche Hürde für Nutzer und Betreiber darstellt, diese zudem nur geringfügig zur Absicherung gegenüber dem Zugriff Dritter beitragen würde und für die Betreiber zusätzliche Kosten entstehen (hierzu auch unter B.I.4, ausführlich: *Mantz*/*Sassenberg*, CR 2015, 298 (301 f.)). Insofern läuft eine Verschlüsselung dem Interesse der Förderung von freien WLAN-Hotspots entgegen. Ein Zusammenhang mit der Frage einer Haftungsprivilegierung ist nicht zu erkennen.

2. Bedarf es technischer Auflagen für den Betrieb zur Gewährung von Datenschutz- und Datensicherheit? Gibt es allgemeine Standards?

(35) De lege lata sind gesetzliche Regelungen für Datenschutz- und Datensicherheit vorgesehen, welche von einem Betreiber eines offenen WLANs zu berücksichtigen sind. Ausschlaggebend sind insofern die telekommunikationsrechtlichen Bestimmungen, nicht einschlägig sind hingegen die Vorgaben des TMG. Die regulatorischen Bestimmungen des Telekommunikationsgesetzes (TKG) unterscheiden hierbei zwischen verschiedenen Adressaten, an die sich die jeweiligen Regelungen wenden. Auf der einen Seite ist die Bejahung der Diensteanbietereigenschaft, auf der anderen Seite der Eigenschaft als Anbieter von öffentlich zugänglichen Telekommunikationsdiensten und Betreiber öffentlicher Telekommunikationsnetze entscheidend.

a. Diensteanbieter

(36) Alle Anbieter von offenen bzw. öffentlichen WLANs sind als Diensteanbieter nach § 3 Nr. 6 TKG anzusehen (*Redeker*, ITRB 2011, 186 (186 f.); zu Hotels vgl. *Ricke* in *Spindler*/*Schuster*, Recht der elektronischen Medien, 3. Aufl. 2015, § 3 TKG Rn. 9; *Sassenberg*/*Mantz*, WLAN und Recht, 2014, Rn. 34 ff. m.w.N.). Diensteanbieter ist „*jeder, der ganz oder teilweise geschäftsmäßig a) Telekommunikationsdienste erbringt oder b) an der Erbringung solcher Dienste mitwirkt*“. Bereits das Mitwirken an der Erbringung eines Dienstes ist damit ausreichend, wobei das Mitwirken Aufgaben betreffen muss, die mit der charakteristischen Signalübertragung und deren insbesondere datenschutzrechtlichen Gefahren in Zusammenhang stehen (vgl. *Sassenberg*/*Franke*, CR 2013, 772 (775)). Unter dem Merkmal des geschäftsmäßigen Erbringens von Telekommunikationsdiensten wird gemäß § 3 Nr. 10 TKG das „*nachhaltige Angebot von Telekommunikation für Dritte mit oder ohne*

Gewinnerzielungsabsicht“ verstanden. Die Bejahung der Eigenschaft als Diensteanbieter hat zur Folge, dass die Regelungen zum Fernmeldegeheimnis (§§ 88 ff. TKG), zum telekommunikationsrechtlichen Datenschutz (§§ 91 ff. TKG) sowie ein Teil der Regelungen zur öffentlichen Sicherheit (§§ 108 ff. TKG) zur Anwendung kommen.

(37) Der Diensteanbieter unterliegt dem Fernmeldegeheimnis nach § 88 TKG, wobei Verstöße nach § 206 StGB strafbewehrt sind. Die datenschutzrechtlichen Regelungen ergeben sich aus den §§ 91 ff. TKG, die den Umgang mit personenbezogenen Daten, insbesondere also mit Bestands- und Verkehrsdaten, regeln. Hinsichtlich des (restriktiven) Umgangs mit Verkehrsdaten haben die Bundesbeauftragte für Datenschutz und Informationssicherheit (BfDI) und die Bundesnetzagentur (BNetzA) am 19.12.2012 einen Leitfaden herausgegeben, in den sich auch die einzelnen Betreibermodelle einordnen lassen.

(38) Der Diensteanbieter unterliegt jedoch nicht nur dem Fernmeldegeheimnis und muss die Bestimmungen des telekommunikationsrechtlichen Datenschutzes einhalten. Er muss nach § 109 Abs. 1 TKG auch die erforderlichen technischen Vorkehrungen und sonstigen Maßnahmen treffen, die zum Schutz des Fernmeldegeheimnisses und gegen die Verletzung des Schutzes personenbezogener Daten erforderlich sind. So sollen Fernmeldegeheimnis und Datenschutz sowie der Betrieb im Katastrophenfall sichergestellt werden. Konkrete Anforderungen, welche technischen Vorkehrungen und Maßnahmen zu ergreifen sind, hat der Gesetzgeber nicht vorgesehen, so dass der Diensteanbieter die im konkreten Fall erforderlichen technischen Vorkehrungen und sonstige Maßnahmen ermitteln muss. Die BNetzA hat zudem im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und der BfDI einen Katalog von Sicherheitsanforderungen gem. § 109 Abs. 6 TKG erstellt, der Anbietern als Grundlage zur Erfüllung der gesetzlichen Verpflichtung dienen soll. Der Entwurf einer aktualisierten Fassung wurde gerade im Amtsblatt der Bundesnetzagentur (ABl. Nr. 19/2015 unter der Mitteilungs-Nr. 1213/2015) veröffentlicht. Welche Maßnahmen im Einzelfall zu treffen sind, hängt vom jeweiligen Betreibermodell ab. Ausschlaggebend ist hierbei auch, ob Bestandsdaten erhoben werden. Hinsichtlich der technischen Vorkehrungen liefern die IT-Grundschutzkataloge des BSI einen Anhaltspunkt.

b. Anbieter von öffentlich zugänglichen Telekommunikationsdiensten und Betreiber öffentlicher Telekommunikationsnetze

(39) Zudem ist der Betreiber eines offenen WLANs als Anbieter von öffentlich zugänglichen Telekommunikationsdiensten anzusehen (vgl. *Sassenberg*/*Mantz*, WLAN und Recht, 2014, Rn. 22 ff. m.w.N.). Seitens der BNetzA wird entgegen der bisher einhelligen Literaturauffassung danach differenziert, ob durch den Anbieter ein eigener, in der Regel auf eine bestimmte Dauer angelegter Telekommunikationsanschluss überlassen wird oder lediglich die Nutzung eines vorhandenen TK-Anschlusses erfolgt (vgl. Mitteilung 149/2015 der Bundesnetzagentur, ABl. 4/2015 vom 04.03.2015, S. 1140). Nur wenn ein eigener Telekommunikationsanschluss überlassen wird, liegt

danach ein Fall des „*Erbringens*“ von Telekommunikationsdiensten vor. Wird jedoch ein vorhandener DSL-Anschluss genutzt, so liegt kein Fall des „*Erbringens*“ sondern lediglich ein „*Mitwirken*“ vor, das für die Anbietereigenschaft nicht ausreichend sei. Die Auffassung der Bundesnetzagentur reduziert die regulatorischen Anforderungen für kleinere Hotspot-Betreiber und ist insoweit hinsichtlich des Ergebnisses zu begrüßen, gleichwohl vermag die Ungleichbehandlung der Anbieter jedoch dogmatisch nicht zu überzeugen und lässt zudem unberücksichtigt, dass auch das Betreiben von öffentlichen Telekommunikationsnetzen die regulatorischen Pflichten auslöst (hierzu im Einzelnen *Sassenberg*/*Mantz*, MMR 2015, 428 ff.).

(40) Wird für den jeweiligen WLAN-Hotspot die Anbieter- und/oder Betreibereigenschaft angenommen, so ist die Folge, dass nicht nur die Kundenschutzvorschriften in §§ 43 a ff. TKG grundsätzlich anwendbar sind, sondern dass auch weitere Anforderungen der öffentlichen Sicherheit (§§ 108 ff. TKG) zur Anwendung kommen, nämlich insbesondere ein Sicherheitsbeauftragter zu benennen und ein Sicherheitskonzept zu erstellen ist. Bei Datenschutzverstößen besteht – unabhängig von deren Schweregrad – eine Meldepflicht nach § 109a TKG bzw. der EU-Verordnung 611/2013 „über die Maßnahmen für die Benachrichtigung von Verletzungen des Schutzes personenbezogener Daten gemäß der Richtlinie 2002/58/EG.“

c. Keine (weiteren) technischen Auflagen erforderlich

(41) Die obigen Ausführungen zeigen, dass durch die bestehenden rechtlichen Rahmenbedingungen die Gewährung von Datenschutz- und Datensicherheit bereits hinreichend sichergestellt ist. Die Bandbreite unterschiedlicher Betreibermodelle trägt dazu bei, dass eine konkretere Regelung nur wenig erfolgversprechend wäre. Die Frage, ob es zusätzlicher technischer Auflagen für Betreiber von „öffentlichen WLAN-Hotspots“ bedarf, ist daher zu verneinen. Vielmehr stellen bereits die existierenden Regelungen Datenschutz- und Datensicherheit in einem ausreichenden Maße sicher. Aufgrund der abstrakten gesetzlichen Reglungen besteht die Gefahr, dass gerade kleinere Anbieter mit der Umsetzung der diesbezüglichen Anforderungen überfordert sind und diese daher der Verbreitung von freien WLAN-Hotspots entgegenstehen. Werden jedoch keine Bestandsdaten erhoben und die Verbindungsdaten unmittelbar mit der Beendigung der Verbindung gelöscht, so ergeben sich aus den Regelungen zur öffentlichen Sicherheit de facto nur geringe Anforderungen. Dem Stellenwert des Fernmeldegeheimnisses sowie des Datenschutzes wird insoweit in Abhängigkeit vom jeweiligen Betreibermodell Rechnung getragen, so dass von einem ausgewogenen rechtlichen Rahmen auszugehen ist.

III. INTERNATIONALER VERGLEICH

1. IN WELCHEM RECHTLICHEN RAHMEN IM HINBLICK AUF ZIVIL- UND STRAFRECHTLICHE ASPEKTE OPERIEREN WLAN-BETREIBER IM INTERNATIONALEN VERGLEICH?

(42) Seitens des eco – Verbands der deutschen Internetwirtschaft e.V. (eco) wurde im November 2014 eine Studie zur „*Verbreitung und Nutzung von WLAN, WLAN-Zugangspunkten sowie öffentlichen Hotspots in Deutschland*“ durchgeführt. Im Rahmen der Studie wird vom eco aufgezeigt, dass die Verbreitung von freien öffentlichen WLAN-Hotspots im internationalen Vergleich gering ist und Länder wie Südkorea, Großbritannien, Taiwan, Schweden, Frankreich und die USA über eine erheblich größere Reichweite verfügen. Auch in Estland können fast überall freie WLAN-Hotspots genutzt werden (*Grüner*, golem.de Beitrag „WLAN-Paradies Estland“ vom 16.07.2012).

(43) Die Frage der Verantwortlichkeit speziell des WLAN-Betreibers ist innerhalb Europas nicht harmonisiert. Die Mitgliedsstaaten sind – im Rahmen der Vorgaben der E-Commerce-Richtlinie – in der Ausgestaltung der Haftung von Intermediären frei (Erwägungsgrund 59 der E-Commerce-Richtlinie). Die in den Mitgliedsstaaten anzutreffenden Regelungsmodelle zur Verantwortlichkeit sind sehr unterschiedlich und abweichend zur deutschen Störerhaftung geregelt, wenngleich es Ähnlichkeiten in der Rechtsprechung gibt (vgl. *Ohly*, ZUM 2013, 308 (311 m.w.N.); *Lensing-Kramer*, GRUR 2009, 722 (724)). Die Frage der Haftung des Betreibers öffentlicher WLANs wird – soweit ersichtlich – hauptsächlich in Deutschland diskutiert.

2. WELCHE ERKENNTNISSE LASSEN SICH HIERAUS FÜR DEUTSCHLAND UND HESSEN ABLEITEN?

(44) Für den im Vergleich zögerlichen Ausbau in Deutschland werden regelmäßig die regulatorischen Bestimmungen des Telekommunikationsrechts sowie die Gefahr der Verantwortlichkeit des Hotspot-Betreibers für ein Handeln Dritter angeführt, wobei der letzte Punkt klar die Diskussion beherrscht. Die anhaltende Unsicherheit über den Rechtsrahmen und die daraus resultierende zögerliche Herangehensweise werden dabei inzwischen kurz als „*German Angst*“ zusammengefasst und führten zu der (überzogenen bzw. plakativen) Forderung, die Störerhaftung generell „abzuschaffen“. Die international bestehenden unterschiedlichen Regelungsmodelle sollten nicht dazu führen, dass die Störerhaftung bzw. Täterhaftung wegen Verkehrspflichtverletzung grundsätzlich in Frage gestellt wird. Diese hat sich vielmehr als effektiv und flexibel erwiesen (*Ohly*, ZUM 2013, 308 (312 f.)). Unabhängig von der Frage, ob langfristig eine europäische Vollharmonisierung wünschenswert wäre, geht es derzeit darum, national zu klären, ob und wenn ja, welche Prüfungs- und Verkehrspflichten für Betreiber von WLAN-Hotspots bestehen. Diese Konkretisierung kann dabei – natürlich nur unter Berücksichtigung des europäischen Rechtsrahmens – sowohl durch den Gesetzgeber als auch durch die Rechtsprechung erfolgen. Richtigerweise haben CDU, CSU und SPD im Koalitionsvertrag vom 16.12.2013 daher auch „nur“ davon

gesprochen, dass für offene WLANs eine „Klarstellung der Haftungsregelungen“ erfolgen soll. Der internationale Vergleich bestätigt, dass es aus dem Gesichtspunkt der Rechtssicherheit nicht erforderlich ist, dem Hotspot-Betreiber Prüfungs- und Verkehrspflichten aufzuerlegen.

IV. AUSBAU

1. WELCHE GRÜNDE SPRECHEN FÜR UND GEGEN ÖFFENTLICHE FÖRDERUNG BEI AUFBAU UND/ODER BETRIEB VON WLAN-NETZEN?

(45) Die im internationalen Vergleich geringe Verbreitung (siehe hierzu unter B.III.1) spricht für eine Förderung von öffentlichen WLANs. Die Förderung könnte – auch wenn der geringe Ausbaustand primär auf die Rechtsunsicherheit und regulatorischen Anforderungen zurückzuführen ist – dazu beitragen, dass der im Vergleich zu anderen Ländern bestehende Rückstand so schnell wie möglich aufgeholt wird. Hiervon würde nicht nur die Wirtschaft, beispielsweise in Form der Förderung des Tourismus oder der Möglichkeit des mobilen Arbeitens, profitieren. Vielfach würde auch der mobile Informationsaustausch gefördert. Es ist nicht davon auszugehen, dass sich eine solche Förderung auf Anbieter von Festnetz- oder Mobilfunkprodukten negativ auswirken würde (siehe hierzu unter B.IV.5). Bei der Förderung ist allerdings unter Berücksichtigung des Grundsatzes der Gleichbehandlung darauf zu achten, dass keine negativen Effekte für Geschäftsmodelle von entgeltpflichtigen WLAN-Betreibern entstehen.

2. WELCHE INSTRUMENTE DER FÖRDERUNG EXISTIEREN? WELCHE SIND IHNEN BEKANNT? WELCHE FORMEN DER FÖRDERUNG WÄREN DENKBAR?

(46) Gerade beim Aufbau von städtischen WLANs hat sich gezeigt, dass der Verfügbarkeit von zentralen Standpunkten für den Aufbau der Router sowie der Infrastruktur (Strom, Anbindung ans Internet) an sich eine wesentliche Bedeutung zukommt. Die öffentliche Hand verfügt in der Regel über innerstädtische Gebäude, die für den Aufbau eines innerstädtischen Netzes genutzt werden können. Der Ausbau kann insofern nicht nur mit finanziellen Mitteln zur Verfügung gefördert werden, sondern auch mit der Bereitstellung der vorhandenen Infrastruktur. Teilweise wird die Förderung davon abhängig gemacht, dass der Anbieter zumindest für einen bestimmten Zeitraum– z.B. 30 Minuten am Tag – einen kostenlosen Zugang für Jedermann gewährleistet.

(47) Theoretisch wäre auch ein eigener Betrieb durch die öffentliche Hand zur Förderung der Verbreitung von WLANs denkbar, wobei hier zu berücksichtigen ist, dass die Erbringung von Telekommunikationsdienstleistungen aufgrund der landes- und verfassungsrechtlichen Rahmenbedingungen nur in einem engen Rahmen zulässig ist (*Sassenberg*/*Mantz*, WLAN und Recht, 2014, Rn. 345 ff.).

3. Welche Betreibermodelle existieren? Welche Modelle werden am häufigsten gewählt und wie kann man dies erklären?

(48) Die nachfolgende Übersicht zeigt die gängigen Betreibermodelle für offene WLANs auf und beschreibt diese summarisch, eine ausführliche Darstellung der Betreibermodelle findet sich bei *Sassenberg*/*Mantz*, WLAN und Recht, 2014, Rn. 11 ff.:

Betreibermodell	Beschreibung
WLAN zur Absatzförderung	Der Aufbau und Betreib eines WLANs wird zur Förderung des Absatzes der eigenen Leistungen genutzt (z.B. Café, Hotel oder Kaufhaus).
Werbefinanziertes WLAN	Der Aufbau und Betrieb eines WLANs wird durch Werbung finanziert.
Kommunales WLAN	Der Aufbau und Betrieb eines WLANs erfolgt durch die öffentliche Hand.
Freies WLAN	Der Aufbau und Betrieb eines WLANs erfolgt aus altruistischen Gründen.
Entgeltpflichtiges WLAN	Die Nutzung des WLANs ist entgeltpflichtig.
Kommerzielles WLAN-Sharing	Ein Anbieter nutzt vorhandene – in der Regel eigene – Infrastruktur (z.B. in Form eines DSL oder Kabelanschlusses) um nicht nur einen Kunden anzubinden, sondern mit den nicht benötigten Kapazitäten ein WLAN-Netzwerk aufzubauen. Betreiber des Hotspots ist der Anbieter.

(49) Auch sind Abweichungen von den vorgestellten Betreibermodellen zu finden bzw. diese werden zum Teil kombiniert (z.B. entgeltfreie Nutzung nur für 30 Minuten). Allgemein lässt sich sagen, dass sämtliche Betreibermodelle anzutreffen sind. Die weiteste Verbreitung dürften hierbei WLANs zur Absatzförderung haben. Dies lässt sich damit begründen, dass Kunden den kostenlosen Internetzugang inzwischen zum Gegenstand für ihre Auswahlentscheidung machen (hierzu bereits unter B.V.2). Darauf dürften entgeltliche WLANs folgen.

4. Welche Rolle kann das Modell „Freifunk“ für den Ausbau des WLAN in Hessen spielen?

(50) Verteilt über Deutschland existieren viele WLAN-Hotspots, die nach dem sog. Freifunk-Modell von Privaten angeboten werden. Die Freifunk-Communities in Hessen waren in den letzten Jahren sehr aktiv und zeichnen sich durch ein stetes Wachstum aus. Nach Kenntnis der Verfasser bestehen u.a. Kontakte zur Stadt Frankfurt am Main. Freifunk-Communities in Deutschland und speziell auch in Hessen und Frankfurt statten zudem bereits aktiv neu eingerichtete Flüchtlingsunterkünfte mit WLAN aus, wo dies aufgrund der jeweiligen Gegebenheiten möglich ist.

(51) Freifunk kann für den Aufbau von öffentlichen Hotspots daher verschiedene Rollen einnehmen. Zum einen stellen diese bereits heute, wenn auch teils noch weit verteilt oder nicht großflächig, öffentlich zugängliche, freie WLAN-Hotspots zur Verfügung. Es gibt eine Vielzahl an Beispielen der Zusammenarbeit von Gemeinden mit Freifunk-Communities, die zum kostengünstigen Aufbau von WLAN-Hotspots und WLAN-Infrastruktur geführt haben. Eine Zusammenarbeit mit Freifunk kann daher den einfachen, günstigen und zudem besonders schnellen Aufbau von WLAN-Hotspots fördern. Die Umsetzung ist dabei sehr von den einzelnen Beteiligten abhängig, erfolgt in der Regel aber deutlich schneller als durch Unternehmen. Dabei bedarf es nicht zwingend einer finanziellen Förderung. Bereits die Gewährung von Zugang zu öffentlichen Gebäuden, die Übernahme von (eher geringen) Stromkosten für WLAN-Router und ggf. die Bereitstellung von Uplinks sind für den Aufbau von Freifunk-Knoten hilfreich. Des Weiteren können Mitglieder der Freifunk-Community aufgrund ihrer jahrelangen Erfahrungen Ansprechpartner darstellen.

(52) Alternativ können vom Land Hessen oder Städten und Gemeinden aufgebaute WLAN-Hotspots auch unabhängig von Freifunk betrieben werden, wobei sich die Angebote dann – jedenfalls in der Fläche – ergänzen. Nach Kenntnis der Verfasser ist bei verschiedenen WLAN-Projekten eine Zusammenarbeit mit Freifunk auch allein dadurch erfolgt, dass eine Verbindung mit Freifunk-Knoten erfolgte. Über die Infrastruktur des öffentlichen WLANs konnten dann verteilte Freifunk-Standorte verbunden werden. Dies fördert das Zusammenwachsen der Freifunk-Netze und befördert dadurch den Aufbau neuer Knoten.

5. WELCHE GRÜNDE SPRECHEN FÜR EINE ZUSAMMENARBEIT DER KOMMUNEN, DER STÄDTE, DER LANDKREISE UND DES ÖPNV BEIM AUFBAU EINES ÖFFENTLICHEN WLANS? WELCHE GRÜNDE SPRECHEN DAGEGEN?

(53) Verschiedene Studien zeigen, dass die mobil abgerufenen Datenmengen – auch aufgrund deren rapider Zunahme – noch nicht alleine über die Mobilfunknetze übertragen werden können (vgl. Goldmedia Trendmonitor 2013, www.goldmedia.com/aktuelles/trendmonitor-2013/data-offloading.html; Cisco, www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.html). Auch wenn die Frage der verfügbaren Bandbreite im Fokus steht, ist die WLAN-Nutzung auch aufgrund mangelnder Netzabdeckung von Interesse. Daher sollen aus Sicht der Telekommunikationsunternehmen Datenströme stattdessen über lokale WLANs übertragen werden (sog. „*Data Offloading*“). Auch die EU-Kommission hat dieses Potential erkannt (Entwurf der Digital Single Market-VO, COM (2013) 627 final, ErwGr. 26 f.; dazu eingehend Mantz/Sassenberg, CR 2014, 370). So wirbt bspw. der Anbieter *Telefónica* derzeit mit einem neuen Angebot, welches das Führen von Mobilfunkgesprächen über einen beliebigen WLAN-Hotspot ermöglicht und so gerade bei eingeschränktem Mobilfunkempfang eine Alternative darstellt. Neben der grundsätzlichen Frage des Netzausbaus können auch die äußeren Rahmenbedingungen – bspw. im Zug – für die Nutzung eines WLAN-Hotspots sprechen. WLAN-Angebote sind jedoch nicht nur erforderlich, um ein mobiles Arbeiten

zu ermöglichen, sondern stellen gerade in den Städten auch einen Mehrwert für Touristen und Einwohner dar.

(54) Offene WLAN-Hotspots sind weder ein Surrogat für den Internetzugang über den klassischen Telefonanschluss noch den mobilen Datentarif, so dass nicht davon auszugehen ist, dass der diesbezügliche Wettbewerb negativ beeinträchtigt werden könnte. Dies zeigen auch die derzeit über das Mobilfunknetz übertragenen Datenmengen. So hat das pro SIM-Karte übertragene Datenvolumen im letzten Jahr zwar um 30,4% zugenommen, beläuft sich derzeit aber dennoch nur auf 377 MB pro Monat (vgl. DIALOG Consult / VATM 17 TK-Marktstudie 2015, 28). Gleichzeitig sprechen die o.g. Gründe für einen kurzfristigen Ausbau von freien WLAN-Hotspots. Hierzu kann die öffentliche Hand insbesondere auch mit den in Innenstadtlagen vorhandenen Standorten beitragen.

6. WER TRÄGT DIE KOSTEN FÜR DEN AUFBAU UND DEN BETRIEB VON WLAN-NETZEN?

(55) Der Aufbau und Betrieb von WLAN-Netzen erfolgt aus gänzlich unterschiedlichen Gründen (vgl. zu den Betreibermodellen *Sassenberg*/*Mantz*, WLAN und Recht, 2014, Rn. 11 ff.). Allgemein lässt sich sagen, dass der Aufbau und Betrieb in der Regel vom Betreiber des jeweiligen Netzes getragen wird. Bei entgeltfreien Angeboten geschehen Aufbau und Betrieb häufig zum Zwecke der Absatzförderung (z.B. in einem Café, Hotel oder Kaufhaus). Gerade größere Unternehmen treten hierbei jedoch aus den unter B.II.3 ausgeführten Gründen häufig nur als „*Sponsor*“ auf und der Betrieb erfolgt durch einen klassischen Telekommunikationsanbieter.

V. WIRTSCHAFTLICHE BEDEUTUNG UND EFFEKTE

1. WELCHEN NUTZEN HABEN STÄDTE UND GEMEINDEN DURCH FREIE ÖFFENTLICH ZUGÄNGLICHE WLAN-NETZE?

(56) Für Städte und Gemeinden bieten WLAN-Hotspots verschiedene Vorteile. So können WLAN-Hotspots u.a. in öffentlichen Gebäuden zum Beispiel zur Versorgung von Wartenden dienen. Weiter können öffentliche Dienstleistungen und Echtzeitinformationen über WLANs angeboten werden, wie z. B. im öffentlichen Verkehr oder im Verkehrsmanagement. Dies hebt beispielsweise die EU-Kommission hervor. Sie hat im Entwurf zur Digital Single Market ausgeführt (COM (2013) 627 final, ErwGr 28):

> *„Behörden und Anbieter öffentlicher Dienste nutzen Funk-LAN-Zugangspunkte zunehmend in ihren Räumlichkeiten für eigene Zwecke, z. B. für ihre Mitarbeiter oder um Bürgerinnen und Bürgern vor Ort einen kostengünstigen Zugang zu elektronischen Behördendiensten zu bieten, um intelligente öffentliche Dienstleistungen zu unterstützen, die die Übermittlung von Informationen in Echtzeit beinhalten, wie z. B. im öffentlichen Verkehr oder im Verkehrsmanagement. Solche Einrichtungen könnten Bürgerinnen und Bürgern*

als Nebenleistung zu den in den betreffenden Räumlichkeiten angebotenen Diensten auch generell Zugang zu solchen Zugangspunkten gewähren (...)“

2. HABEN FREIE ÖFFENTLICH ZUGÄNGLICHE WLAN-NETZE AUCH FÜR DIE TOURISMUSWIRTSCHAFT EINE BEDEUTUNG?

(57) Öffentlich zugängliche WLANs haben für die Tourismuswirtschaft einen positiven Effekt. Für Hotelgäste ist die Verfügbarkeit eines WLAN mittlerweile sogar eines der wichtigsten Kriterien bei der Hotelwahl (vgl. Stellungnahme der DeHoGa/IHA zur Anhörung im Landtag Nordrhein-Westfalen v. 3.7.2013, http://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument?Id=MMST16/933; Pressemitteilung HRS v. 3.4.2014, http://hrs.de/presse/pressemitteilungen/mit-gratis-wlan-auf-dem-zimmer-punkten-hotels.html).

(58) Verschiedene Städte nutzen öffentliche WLANs auch als Informationsplattform für Touristen, durch die Nutzern Hinweise zu Sehenswürdigkeiten, Aktionen etc. an die Hand gegeben werden.

(59) Weiter werden Städte, die mit öffentlichen WLANs ausgestattet sind, als weltoffener und moderner wahrgenommen. Öffentliche WLANs steigern daher generell die Attraktivität von Städten und Regionen. Aus diesem Grunde werben auch Touristeninformationen mit der Verfügbarkeit von öffentlichen WLANs (so z.B. die Hamburg Tourismus GmbH, http://www.hamburg-tourism.de/infos/mobile-angebote/w-lan-hotspots). Teilweise wird WLAN auch als Teil einer Gesamtstrategie angesehen. So schreibt der Tourismusverband Sächsisches Elbland e.V. in seiner „Destinationsstrategie“ (2. Aufl. 2014, http://www.elbland.de/fileadmin/userfiles/TVSE/Downloads/Destinationsstrategie_ab_2014_Internet.pdf):

„2.1.5 Digitale Versorgung

Die gesellschaftliche Bedeutung des Internets wächst zunehmend. Immer mehr Menschen greifen mehrmals täglich auf das World Wide Web zu. Um auch das vielfältige touristische Online-Angebot optimal zu nutzen braucht es eine schnelle Verbindung. (..)

WLAN-Verbindungen an touristischen Einrichtungen sollen die Ansprüche und den Bedarf der Besucher des Freistaats aus dem In- und Ausland erfüllen. Sachsen ist Kulturreiseland Nr. 1 und soll sich z.B. durch die Einrichtung von Hot Spots und WLAN an den entsprechenden Orten als modernes Reiseziel präsentieren. (...)

Vor allem internationale Besucher erwarten permanent verfügbares Internet, für viele stellt dies eine Buchungsvoraussetzung dar. Der Ausbau und die Weiterentwicklung des (teilweise vorhandenen) Angebotes sind für die touristischen Leistungsträger wünschenswert. So könnten z. B. (kostenfreies) WLAN in den Beherbergungen, gastronomischen Betrieben, Museen etc. noch

mehr Gäste anziehen. Auch andere elektronische Dienste vor Ort, wie z. B. Apps zu Museumsrundgängen und Stadtführungen oder GPS-gestützte Fahrradtouren hätten somit größeres Potenzial der Gästeakzeptanz (kürzere Ladezeiten etc.) (...)“

(60) Die Wahrnehmung von Städten und Touristenregionen wird maßgeblich auch durch die Touristen selbst geprägt. Das zeitnahe Versenden oder Posten von Fotos von Sehenswürdigkeiten oder sog. „*Selfies*“ ist heutzutage üblich. Besucher, die ihre Fotos unmittelbar mit Freunden oder öffentlich teilen (können), bewirken dementsprechend einen Werbeeffekt (teilweise bezeichnet als „virales Marketing“). Insbesondere Skigebiete haben WLAN als Werbeplattform schon vor Jahren entdeckt (vgl. http://stadt-bremerhaven.de/wie-man-kostenloses-wlan-fuer-den-tourismus-nutzt/). Da insbesondere ausländische Touristen sehr häufig keine Mobilfunkanbindung haben werden, sind diese auf WLANs angewiesen. So schreibt z.B. das Reiseunternehmen Thomas Cook (Eintrag v. 11.12.2014, http://www.thomascook.de/unternehmen/newsroom/braggie-neuer-tourismus-trend-im-social-web):

„Mit welchen Fotos machen die Urlauber die Daheimgebliebenen am liebsten neidisch?

Martin Widenka: `Mit Fotos vom Hotelbett mit direktem Blick aufs Meer, mit Cocktails beim Sonnenuntergang und tollen Bildern am Pool. Weil am liebsten sofort gepostet wird, ist besonders jungen Urlaubern kostenloses WLAN in der Hotelanlage sehr wichtig.' “

3. Welchen Nutzen haben andere Wirtschaftssektoren und Branchen durch frei öffentlich zugängliche WLAN-Netze?

(61) Einen bekanntermaßen enormen Nutzen haben **Telekommunikationsunternehmen**. Diese begreifen WLAN-Hotspots als Möglichkeit zur Entlastung ihrer Mobilfunknetze. Aufgrund des ständig wachsenden Übertragungsvolumens werden auch in der näheren Zukunft die Mobilfunknetze nicht in der Lage sein, für alle Nutzer ausreichend Bandbreite zur Verfügung zu stellen (siehe oben Rn. 56).

(62) Kostenlose WLANs haben darüber hinaus für praktisch alle Branchen einen starken Kundenbindungseffekt. Dies hat insbesondere die **Gastronomie** früh erkannt und bietet seit Jahren lokale WLANs an. Dadurch können neue Kunden angelockt und die Verweildauer der Kunden erhöht werden.

(63) **Fernbusse** bieten bereits seit längerer Zeit kostenloses WLAN an und stellen damit gegenüber dem – derzeit noch kostenpflichtigen – nur wenig verbreiteten WLAN in der Bahn ein Unterscheidungsmerkmal und damit einen Wettbewerbsvorteil dar.

(64) Für den **Einzelhandel** bieten WLAN-Hotspots ebenfalls die Möglichkeit, das Geschäft oder den Einkaufsbereich attraktiver zu gestalten. Über WLANs können Unternehmen auch Zusatzangebote machen. So bietet seit einigen Monaten eine deutsche

Drogeriekette kostenlose WLANs an. Zusätzlich können Kunden über dieses WLAN unmittelbar Dienste des Unternehmens (z.B. Foto-Entwicklung) in Anspruch nehmen.

(65) Das Angebot eines kostenlosen WLANs führt darüber hinaus generell zu Werbeeffekten. Wer ein kostenloses WLAN anbietet, zeigt dem Kunden, dass er mit der Zeit zu gehen weiß. Über im WLAN verfügbare Webseiten oder Apps können Kunden aktuelle Angebote vorgeschlagen werden.

(66) Durch das Angebot von kostenlosen WLAN-Hotspots können Anbieter zudem – unter Beachtung der entsprechenden (auch telekommunikationsrechtlichen) Datenschutzvorschriften – Daten erheben und auswerten (dazu *Sassenberg*/*Mantz*, WLAN und Recht, 2014, Rn. 126 ff., 141), die bei der weiteren Verbesserung ihrer Produkte oder ihres Angebots helfen. So können über WLANs beispielsweise Kundenströme und Laufwege in Supermärkten erhoben und genutzt werden.

(67) Die Verbreitung von kostenlosen WLAN-Hotspots hat auch positive Auswirkungen auf den (lokalen) **IT-Handel** und die Anbieter von IT-Dienstleistungen. Denn für den Aufbau müssen entsprechende Anlagen und Dienstleistungen hierfür erworben werden. Bereits seit Jahren haben sich verschiedene (teils nur lokal tätige) Unternehmen darauf spezialisiert, z.B. Hotels mit WLANs auszustatten und deren WLANs zu betreuen.

(68) Im Übrigen erkennen mittlerweile auch **Schulen**, dass die Integration von WLAN an der Schule und im Unterricht vorteilhaft sein kann (vgl. z.B. http://www-de.scoyo.com/eltern/aktuelles-zu-scoyo/wlan-projekt-in-hamburg).

(69) WLAN-Hotspots können auch der Integration dienen. So werden derzeit insbesondere auf Betreiben verschiedener lokaler Freifunk-Initiativen eine Vielzahl von **Flüchtlingsunterkünften** mit WLAN versorgt.

4. SIND AUSWIRKUNGEN AUF (LOKALE) TELEKOMMUNIKATIONSBETREIBER ZU ERWARTEN, DIE INZWISCHEN VERGLEICHBARE LEISTUNGEN (Z.B. LTE) IM RAHMEN VON NUTZERVERTRÄGEN GEGEN RECHNUNG ZUR VERFÜGUNG STELLEN?

(70) Wie oben dargestellt, geht ein Teil der Bestrebungen zum Ausbau öffentlicher WLAN-Hotspots von Telekommunikationsbetreibern aus. Für diese bieten sich beim Aufbau von WLAN-Hotspots neue Geschäftsfelder mit möglicherweise anderen/neuen Kunden. Darüber hinaus können die Betreiber positive Effekte durch die Entlastung der eigenen Netze über WLAN-Hotspots erzielen.

(71) Bisher sind den Verfassern negative Auswirkungen insbesondere auf Mobilfunkbetreiber nicht bekannt geworden. Aufgrund der unterschiedlichen Technologie und insbesondere der sich deutlich unterscheidenden Reichweite von WLAN-Hotspots gegenüber Mobilfunknetzen findet eine Substitution von Mobilfunk aufgrund der Nutzung von WLAN bisher nicht statt. Gleiches gilt für den eigenen heimischen Internetanschluss bspw. per DSL oder Kabel.

(72) Praktisch alle Mobilfunkverträge mit Internetzugang enthalten derzeit eine Drosselung ab einem bestimmten pro Monat verbrauchten Datenvolumen, d.h. nach Überschreiten des vertraglich vereinbarten Datenvolumens wird die Geschwindigkeit der Datenübertragung reduziert. Für das weiter übertragene Datenvolumen fallen jedoch in der Regel keine zusätzlichen Gebühren an. Teilweise bieten Telekommunikationsbetreiber in solchen Fällen gegen Aufpreis ein weiteres Datenvolumenkontingent an. Bei einer weiteren Verbreitung von kostenlosen WLAN-Hotspots könnten weniger Nutzer diese Option nutzen. Den Verfassern liegen Erfahrungen hierzu jedoch nicht vor.

5. Was ist beim Aufbau eines öffentlich geförderten und/oder betriebenen WLAN-Netzes im Hinblick auf das Wirtschaftsverwaltungsrecht zu beachten, wenn bestehende WLAN-Angebote (z.B. durch die Telekom) bestehen?

(73) Grundsätzlich ist Voraussetzung einer wirtschaftlichen Tätigkeit von Gemeinden, dass es sich (i.) um die Betätigung eines öffentlichen Zwecks handelt, (ii.) die Leistungsfähigkeit der Gemeinde nicht überstiegen werden darf und (iii.) die Aufgabe nicht besser bzw. ebenso gut durch Private erbracht werden kann (näher dazu *Sassenberg*/*Mantz*, WLAN und Recht, 2014, Rn. 346 ff.). Die ersten beiden Voraussetzungen liegen bei WLAN-Hotspots jedenfalls vor. Denn diese sind als Teil der Daseinsvorsorge anzusehen (vgl. *Haack*, VerwArch 2008, 197 (205); *Pünder*, DVBl. 1997, 1553 (1558 f.)). Die obigen Ausführungen belegen den öffentlichen Zweck. Darüber hinaus ist der Aufbau von WLAN-Hotspots mit relativ geringen Kosten möglich.

(74) Ob WLAN-Hotspots besser oder nicht ebenso gut von Privaten aufgebaut und betrieben werden können, wird vom konkreten Einzelfall abhängen. Den Verfassern sind keine Gerichtsverfahren oder -entscheidungen zu dieser Thematik bekannt.

(75) Im Übrigen hat sich auch die EU-Kommission im Entwurf zur Digital Single Market-Verordnung dafür ausgesprochen, dass Gemeinden öffentliche WLAN-Hotspots aufbauen und betreiben können sollten (COM (2013) 627 final, ErwGr 28):

> *„Solche Einrichtungen könnten Bürgerinnen und Bürgern als Nebenleistung zu den in den betreffenden Räumlichkeiten angebotenen Diensten auch generell Zugang zu solchen Zugangspunkten gewähren; sie sollten diese Möglichkeit unter Einhaltung des Wettbewerbsrechts und der Vorschriften für die öffentliche Auftragsvergabe erhalten.“*

VI. FÖRDERPROJEKTE IM BUNDESVERGLEICH

1. WELCHE STAATLICH GEFÖRDERTEN WLAN-PROJEKTE EXISTIEREN DERZEIT IN DEUTSCHLAND?

(76) Nach Kenntnis der Verfasser gibt es mittlerweile mehrere durch staatliche Institutionen geförderte WLAN-Projekte. Insbesondere Städte, Kommunen und Länder erkennen immer mehr, dass die Förderung solcher Projekte bei geringen Kosten einen positiven Effekt hat. Die folgende Aufzählung gibt nur einen unvollständigen Ausschnitt wieder, die Links finden sich aus Gründen der Übersichtlichkeit im Anhang.

(77) Seit dem Jahr 2012 fördert die Medienanstalt Berlin-Brandenburg (mabb) WLAN-Hotspots der Firma Kabel Deutschland. Zunächst wurden 44 Hotspots in Berlin betrieben (mabb, PM v. 19.10.2012 – [Link 1]). Mittlerweile werden in Berlin und Potsdam 100 Hotspots gefördert (mabb, PM v. 18.03.2015, [Link 2].

(78) Seit 2013 fördert die mabb die Berliner Freifunk-Initiative. Die mabb schreibt hierzu auf ihrer Webseite (mabb, PM v. 13.01.2015, [Link 3]):

> *„Die mabb fördert damit gezielt einen Ansatz zur WLAN-Versorgung des öffentlichen Raums, der nicht-kommerziell angelegt ist und als Ergänzung bereits bestehender kommerzieller Angebote weiterentwickelt werden soll. „WLAN-Netze nehmen eine Schlüsselfunktion ein, wenn es um zeitgemäße Formen der Mediennutzung geht“, so Dr. Hans Hege, Direktor der mabb.“*

Zur Förderung der mabb und der Stadt Berlin gehört auch, dass Freifunk-Knoten auf öffentlichen Gebäuden aufgebaut werden (s. Sitzungsprotokoll des Abgeordnetenhauses Berlin v. 15.06.2015, [Link 4]).

(79) Der Landtag Sachsen-Anhalt hat kürzlich angeregt, dass die Medienanstalt Sachsen-Anhalt ein „*Pilotvorhaben im Bereich freier WLAN-Netzwerke*“ starte (Beschl. v. 15.10.2015, [Link 5]).

(80) Verschiedene Städte, Kommunen und Länder haben sich in den letzten Jahren entschieden, Freifunk-Projekte zu fördern. Die Förderung erfolgt dabei teilweise durch Bereitstellung von finanziellen Mitteln, durch Gewährung von Zugang zu kommunalen Gebäuden und Bereitstellung von Strom für dort aufgebaute WLAN-Router oder den Anschluss von WLAN-Routern an das Internet als Uplink, so z.B. in:

- Berlin-Friedrichshain [Link 6]
- Berlin-Neukölln [Link 7]
- Technikmuseum Berlin [Link 8]
- Potsdam [Link 9]

- Münster [Link 10]
- Gera (Pilotprojekt des Landes Thüringen [Link 11]
- Arnsberg [Link 12]
- Heidelberg [Link 13]
- Digitale Offensive Sachsen [Link 14]
- Thüringen [Link 15]
- Nordrhein-Westfalen [Link 16]
- Schleswig-Holstein [Link 17]
- Halle, Amtsblatt 18/2015 der Stadt Halle/Saale v. 14.10.2015 [Link 18]
- Linnich [Link 19]
- Aachen [Link 20]
- Dueren [Link 21]

Anhang – Linkliste staatlich geförderter WLAN-Projekte

[1] http://www.mabb.de/presse/pressemitteilungen/details/kabel-deutschland-und-medienanstalt-berlin-brandenburg-starten-pilotprojekt-fuer-oeffentliches-wlan-netz-in-berlin.html
[2] http://www.mabb.de/presse/pressemitteilungen/details/wlan-zugang-ohne-barrieren.html
[3] http://mabb.de/presse/pressemitteilungen/details/wlan-fuer-alle-freie-funknetze-in-der-praxis.html
[4] http://www.parlament-berlin.de/ados/17/BuergEn/protokoll/bge17-018-ip.pdf
[5] http://www.landtag.sachsen-anhalt.de/fileadmin/files/drs/wp6/drs/d4366ran.pdf
[6] http://www.berlin.de/ba-friedrichshain-kreuzberg/politik-und-verwaltung/bezirksverordnetenversammlung/online/vo020.asp?VOLFDNR=5324&options=4
[7] http://www.neukoellner.net/verbrauch-verzehr/neukoellner-freifunk/
[8] http://netzblog.sdtb.de/ueber-den-daechern-von-berlin/
[9] http://www.pnn.de/potsdam/717144/
[10] https://freifunk-muensterland.de/stadt-muenster-beschliesst-unterstuetzung-von-freifunk/
[11] https://www.freifunk-gera-greiz.de/web/joergd/home/-/blogs/stadt-gera-erhalt-zuschlag-fur-freifunk-forderung
[12] http://www.arnsberg-info.de/arnsberg/freizeitangebote/freifunk/
[13] https://www.heidelberg.de/hd,Lde/02_06_2014+Kostenloses+WLAN+in+Heidelberg.html
[14] http://www.digitale.offensive.sachsen.de/9893.html
[15] http://www.mdr.de/thueringen/breitband_ausbau100.html
[16] http://www.aachener-zeitung.de/lokales/region/kostenloses-wlan-nrw-will-ausbau-foerdern-1.1122086
[17] http://www.shz.de/schleswig-holstein/politik/sh-will-kostenlose-wlan-hotspots-foerdern-id9116656.html
[18] www.halle.de/Publications/6293/amtsblatt18_141015.pdf
[19] http://www.aachener-zeitung.de/lokales/juelich/die-freifunk-idee-faellt-in-linnich-auf-fruchtbaren-boden-1.1084663
[20] http://aachen.de/DE/stadt_buerger/politik_verwaltung/pressemitteilungen/Fluechtlingssituation.html
[21] http://www.dueren.de/stadtinfo/freies-wlan/

Per E-Mail an:
c.lingelbach@ltg.hessen.de, m.eisert@ltg.hessen.de

Hessischer Landtag
Ausschuss für Wirtschaft, Energie,
Verkehr und Landesentwicklung
Schlossplatz 1-3
65183 Wiesbaden

Berlin, den 03.11.2015

Stellungnahme des Verbands unabhängiger Musikunternehmen e.V. (VUT) zum Entwurf (im Folgenden „Referentenentwurf" genannt) eines Zweiten Gesetzes zur Änderung des Telemediengesetzes in seiner Version vom 25.9.2015 (Zweites Telemedienänderungsgesetz – 2. TMGÄndG)

1. HAFTUNG DER WLAN-BETREIBER

Es ist richtig, WLAN-Anbieter von der Haftung für das Verhalten ihrer Nutzer freizustellen, wenn sie die zum Schutz der Rechtsgüter Dritter notwendigen, zumutbaren Verkehrs- und Sorgfaltspflichten erfüllen.

Solange jedoch die Registrierung der Nutzer immer freiwillig bleibt, vielmehr allein eine Verschlüsselung des Zugangs gegen Zugriff von Unberechtigten sowie eine Hinweispflicht gegen missbräuchliche Nutzung zur Enthaftung des WLAN-Betreibers ausreichen, bleibt ein Hauptproblem der Betroffenen von Cyberkriminalität bestehen. Ob berechtigte oder unberechtigte Nutzer von WLAN-Zugängen Dritter, die notwendigen Bestandsdaten für eine Rechtsverfolgung von rechtwidrigen Taten der Nutzer stehen nicht zur Verfügung.

2. HAFTUNGSPRIVILEGIERUNG DER HOSTPROVIDER

Der Referentenentwurf formuliert unserer Ansicht nach im Kern gute Unterscheidungskriterien zwischen rein passiven Hostprovidern, deren Haftung für Rechtsverletzungen Dritter zu Recht weitgehend eingeschränkt ist sowie solchen Hostprovidern, die ganz überwiegend aus eigenem wirtschaftlichen Interesse bewusst durch ihr Tun oder Unterlassen Rechtsverletzungen im Internet den Weg bereiten. Wir halten es für einen guten Ansatz, den von der Rechtsprechung entwickelten Begriff eines „besonders gefahrgeneigten Dienstes" gesetzlich zu übernehmen. Die Regelbeispiele könnten jedoch noch klarer sein und ausführlicher erläutert werden.

§ 10 Abs. 2 Nr. 1 RefE-TMG (wenn die Speicherung oder Verwendung der weit überwiegenden Zahl der gespeicherten Informationen rechtswidrig erfolgt)

Es sollte der Begriff „weit“ gestrichen und der Begriff der gespeicherten Informationen als gespeicherte „nutzerrelevante“ Informationen präzisiert werden. Es ist verständlich, dass eine rein quantitative Konkretisierung rechtwidrig gespeicherter Informationen nur ein grobes Raster sein kann. Dass jedoch das Haftungsprivileg erst bei deutlich über 50 Prozent rechtwidriger Nutzungen verloren gehen soll, ist unverständlich. Wer ein Geschäftsmodell betreibt, das große Kollateralschäden bei Dritten verursacht und wer diese Kollateralschäden billigend in Kauf nimmt, wird ohne großen Aufwand und Kosten eine ausreichende, ergänzende auch rechtmäßige Nutzung seines Dienstes ermöglichen können, ausschließlich mit dem Ziel, den Folgen des § 10 Abs. 2 Nr. 1 RefE-TMG entgegenzuwirken.

Zu berücksichtigen ist weiter, dass die Verhältnismäßigkeit der Nutzungen nichts über tatsächliche Nutzungszahlen aussagt und damit über die Angriffshöhe eines Dienstes gegen ein geschütztes Rechtsgut. Der verursachte Kollateralschaden an Rechtsverletzungen eines Dienstes, der 50:50 rechtswidrige und rechtmäßige Nutzungen nachweisen kann, aber trotzdem massenhafte rechtswidrige Nutzungen ermöglicht, darf bei der Beurteilung der Frage, ob ein Dienst besonders Gefahr geneigt ist, nicht unberücksichtigt bleiben. Wir empfehlen, das Tatbestandsmerkmal einer massenhaften Verletzung als Alternative einzufügen. Der Begriff Informationen sollte um „nutzerrelevant“ präzisiert werden, denn nicht alle Informationen sind im Sinne dieser Vorschrift relevant (zum Beispiel technische Informationen zur Funktionalität).

§ 10 Abs. 2 Nr. 2 RefE-TMG (wenn der Diensteanbieter durch eigene Maßnahmen vorsätzlich die Gefahr einer rechtsverletzenden Nutzung fördert)

Die Erläuterungen zu diesem Teil des Entwurfes sind sehr kurz. Der Gesetzgeber sollte dieses Regelbeispiel in den Anmerkungen ausführlicher erläutern. Die Rechtsprechung sieht zum Beispiel in der Möglichkeit des anonymen Uploads ein Kriterium, das die Gefahr von rechtsverletzender Nutzung fördert.

3. OFFENE FRAGEN

Im Referentenentwurf wurde unverständlicherweise versäumt, in weiteren Bereichen des TMG Regelungsvorschläge zu machen, die seit vielen Jahren aufgrund unsicherer Rechtslage Gegenstand zahlreicher Rechtsstreitigkeiten sind und unmittelbar mit den zu beurteilenden Änderungsvorschlägen des RefE-TMG zusammenhängen.

Nur der Zugangsprovider kann akute Maßnahmen gegen rechtswidrige Live-Streaming-Angebote ergreifen oder gegen rechtswidrige Dienste, die sich vorsätzlich ihrer Verantwortung entziehen. Der EuGH hat mit der Entscheidung vom 27.03.2014 (C-314/12) zur Auslegung von Art. 8 Abs. 3 RL 2001/29/EG (kino.to) Stellung genommen, dass Rechteinhaber wegen urheberrechtsverletzender Inhalte im Internet gegen Zugangsprovider Sperransprüche stellen können.

Das Telemediengesetz sieht vor, dass ein Hostprovider von der Haftung für fremde Inhalte freigestellt wird, wenn er auf Hinweis den Zugang zu dem betroffenen Inhalt unterbindet. Noch weitestgehend ungeklärt ist der Umfang seiner Pflicht dafür zu sorgen, dass der betroffene

Inhalt nicht erneut über seinen Service öffentlich zugänglich gemacht wird und ab wann sich ein Hostprovider unter Umständen sogar schadensersatzpflichtig macht.

Zu eigen machen fremder Inhalte, § 7 TMG

§ 7 TMG unterscheidet grundsätzlich zwischen eigenen und fremden Informationen. Die Norm § 7 TMG findet keine Entsprechung in der E-Commerce-Richtlinie, denn dort wird unterstellt, dass Diensteanbieter für eigene Inhalte nach den allgemeinen Rechtsvorschriften haften. Dies ergibt sich daraus, dass Art. 12–14 der E-Commerce-Richtlinie jeweils die Begrifflichkeit „von einem Nutzer eingegebene Informationen“ in Abgrenzung zu denjenigen Informationen verwenden, die der Diensteanbieter selbst erstellt und eingegeben hat[1].

Für eigene Informationen, § 7 Abs. 1 TMG, trifft den Diensteanbieter auch ohne konkreten Hinweis auf eine Rechtsverletzung die volle Verantwortung nach den allgemeinen Gesetzen (als Täter oder Teilnehmer). Im Falle von Rechtsverletzungen können die Betroffenen sämtliche Ansprüche gegen den jeweiligen Dienst geltend machen, die bei schuldhaftem Handeln auch Schadensersatz umfassen. Nach dem Prinzip der Lizenzanalogie entspricht der Schadensersatzanspruch im Hinblick auf die widerrechtlichen Nutzungen der vorenthaltenen Lizenzzahlung. Dieser Lizenz- bzw. Schadensersatzanspruch steht für die Mitglieder des VUT im Vordergrund, denn entscheidend ist nach wie vor, dass sie für alle Nutzungen angemessen vergütet werden.

Der BGH hat in seiner Entscheidung *„Marions Kochbuch“* (BGH MMR 2010, 556) festgestellt, dass hohe Sorgfaltspflichten gelten, wenn ein Diensteanbieter fremde Informationen als eigene übernimmt. Wer fremde Inhalte als eigene Inhalte übernimmt, handelt widerrechtlich und schuldhaft, wenn er nicht zuvor die erforderlichen Rechte eingeholt hat. Er wird dann behandelt, als hätte er selbst diese Inhalte öffentlich zugänglich gemacht und haftet gleich einem Täter einer Rechtsverletzung nicht nur auf Unterlassung, sondern auch auf Auskunft und Schadensersatz.

Wir halten es daher für konsequent, geboten und in der Rechtsfolge für richtig, in § 7 Abs. 2 TMG klarzustellen, dass durch aktives Verwalten von Inhalten, zum Beispiel durch Gruppierung, Auswahl und Umgestaltung, sei sie auch nur rein technisch und automatisiert durchgeführt, fremde Inhalte übernommen und damit zu eigenen Informationen gem. § 7 Abs. 1 TMG werden. Das muss jedenfalls dann gelten, wenn das aktive Verwalten der Inhalte nicht nur im Interesse desjenigen geschieht, der die fremden Inhalte dem Dienst zur Verfügung gestellt hat. Gleiches muss gelten, wenn der Diensteanbieter Nutzungsrechte an den Informationen vom Bereitsteller erwirbt.

Besonders gefahrgeneigte Geschäftsmodelle und § 8 TMG

Aus Art. 8 Abs. 3 Richtlinie 2001/29/EG (Urheberrichtlinie) folgt, konkretisiert durch das Urteil des EuGH, Az. C 314/12, vom 27. März 2014, dass auch Zugangsprovider unter bestimmten Umständen Maßnahmen gegen besonders gefahrgeneigte Geschäftsmodelle ergreifen müssen. Er muss dann Maßnahmen ergreifen, wenn diese Maßnahmen zumutbar sind und vor

[1] aaO., Rn. 6

allem wenn er der einzige Teilnehmer der Kommunikationskette ist, dem überhaupt Maßnahmen möglich sind.

Dies dürfte insbesondere der Fall sein, wenn eine Inanspruchnahme der Betreiber von gefahrgeneigten Geschäftsmodellen scheitert oder sofortiges Handeln (zum Beispiel bei illegalen Liveübertragungen) geboten ist. Klarstellend halten wir fest, dass den Zugangsprovider ausdrücklich keine Pflicht treffen soll und darf, die Nutzung seiner Kunden zu überwachen oder das Nutzungsverhalten aufzuzeichnen. Wenn der Zugangsprovider jedoch von Dritten konkrete Kenntnis von rechtswidriger Nutzung erhält, zum Beispiel einen rechtswidrigen Livestream, dann ist erforderlich und zumutbar, dass er sofortige Maßnahmen ergreift, den Zugang zu unterbinden.

Allerdings ist sehr umstritten, ob die Rechtsfigur der Störerhaftung Anspruchsgrundlage für die bezeichneten Ansprüche sein kann und ob sie die vom EuGH geforderte Verhältnismäßigkeitsprüfung im Hinblick auf die Sperrmaßnahmen leisten kann. Im Referentenentwurf des TMG hätte der Gesetzgeber Klarheit durch eine Anspruchsgrundlage schaffen können. In Österreich, Frankreich und Großbritannien werden auf Access-Provider-Ebene inzwischen Maßnahmen gegen besonders gefahrgeneigte Dienste ergriffen (zum Beispiel Blacklisting).

Stay Down - § 10 TMG

Diensteanbieter sind für fremde Informationen, die sie für einen Nutzer speichern, nicht verantwortlich, sofern sie unverzüglich tätig geworden sind, um die Informationen zu entfernen oder den Zugang zu ihnen zu sperren, sobald sie diese Kenntnis erlangt haben (§ 10 S.1 Nr.2 TMG). Hinter dieser Formulierung verbirgt sich das praktizierte „Notice-and-Take-Down“-Verfahren. Allerdings ist der Diensteanbieter nicht nur zur Beseitigung der rechtsverletzenden Informationen verpflichtet, sondern muss auch im Rahmen des Zumutbaren Vorkehrungen dagegen treffen, dass diese Informationen erneut unter rechtwidrigen Umständen zur Verfügung gestellt werden (BGH ZUM 2013, 288 Rn. 32 – Alone in the Dark), sog. „Notice, Take Down and Stay Down“-Verfahren. Diese Pflicht sollte in § 10 S.1 Nr.2 TMG rechtlich kodifiziert werden.

Reinher Karl

Justiziar des VUT e.V.

Fachanwalt für Urheber- und Medienrecht

Gemeinsame

Stellungnahme

des Hotelverband Deutschland e.V. (IHA) und des
Hotel- und Gastronomieverband DEHOGA Hessen e.V.

zum
Antrag der SPD-Landtagsfraktion sowie zum
Fragenkatalog des Ausschusses für Wirtschaft, Energie, Verkehr und Landesentwicklung des Hessischen Landtages
hier:

Freie WLAN-Hotspots in Hessen

Stand: 3. November 2015

Ansprechpartner:
Julius Wagner (Hauptgeschäftsführer)
| wagner@dehoga-hessen.de | Tel.: 0611 ¯ 99201-15 |
Markus Danuser (pers. Referent Grundsatzfragen)
| danuser@dehoga-hessen.de | Tel.: 0611 ¯ 99201-16 |

I. Vorbemerkung

Der Hotelverband Deutschland (IHA) ist der Branchenverband der Hotellerie. Ihm gehören rund 1.400 führende Hotels aller Kategorien aus Individual-, Kooperations- und Kettenhotellerie an. Der Hotelverband vertritt die Interessen der Hotellerie auf nationaler und internationaler Ebene gegenüber Politik und Öffentlichkeit und unterstützt seine Mitglieder exklusiv mit professionellen und spezialisierten Dienstleistungen.

Der Hotel- und Gastronomieverband DEHOGA Hessen ist der Branchenverband der Hoteliers und Gastronomen in Hessen. Der DEHOGA Hessen vertritt als Berufs- und Wirtschaftsverband das hessische Gastgewerbe, den Hauptleistungsträger des Tourismus in Hessen. Mit über 18.000 Hoteliers und Gastronomen, 180.000 Erwerbstätigen und 4.500 Auszubildenden ist das Gastgewerbe ein starkes Stück hessische Wirtschaft und das Rückgrat der heimischen Tourismusindustrie.

Die Stellungnahme beschränkt sich auf die für den Hotelverband Deutschland e.V. (IHA) und den DEHOGA Hessen e.V. besonders relevanten Fragestellungen und orientiert sich dabei an der Gliederung des überfraktionellen Anhörungskonzeptes.

1. Rechtliche Rahmenbedingungen

d) Welche Haftungsrisiken bestehen derzeit für WLAN-Betreiber, welche der TMG-Privilegierung nicht unterliegen?

Die Frage, ob Hoteliers und Gastwirte, die ihren Gästen Internetzugang über ihr betriebliches WLAN gewähren, bereits de lege lata vom Haftungsprivileg des § 8 Abs. 1 TMG erfasst werden, wird in Rechtsprechung und Literatur unterschiedlich beantwortet und ist derzeit u.a. Gegenstand eines Vorlageverfahrens zum Europäischen Gerichtshof gem. Art. 267 AEUV, welches durch einen Beschluss des Landgerichts München veranlasst wurde (LG München, Beschluss vom 18.09.2014 zum AZ 7 O 14719/12.

Wir halten den Ausgang dieses Verfahrens zwar durchaus relevant für zukünftige Novellierungen des TMG, verzichten jedoch auf eine inhaltliche Positionierung, da es uns in erster Linie um eine möglichst kurzfristige und praxiswirksame Lösung im Interesse unserer Mitglieder geht.

Denn aktuell gehört es in der vorwiegend von kleineren und mittleren Betrieben geprägten hessischen Hotellerie zu den sich immer wieder realisierenden alltäglichen Risiken, für offenbar von Gästen begangenen Urheberrechtsverletzungen durch illegale Downloads abgemahnt zu werden.
Häufig gelingt es zwar, diese Abmahnungen abzuwehren, indem den anwaltlichen Vertretern der Rechteinhaber dargestellt wird, dass das WLAN des jeweiligen Betriebes ausreichend verschlüsselt war und unsere Mitglieder ihre Gäste vor der Ermöglichung des Internetzugangs zur rechtmäßigen Nutzung ermahnt haben.

Dies setzt jedoch voraus, dass sich der betroffene Hotelier, der durch die scharf formulierten Anwaltsschreiben mit kurzen Reaktionsfristen erheblich unter Druck steht, an die DEHOGA-Rechtsberatung oder einen Anwalt wendet, anstatt die geforderte Unterlassungs- und Verpflichtungserklärung abzugeben und den verlangten Schadenersatz zu leisten.

Noch schwieriger in tatsächlicher und rechtlicher Hinsicht wird es dann, wenn unsere Mitglieder auch nicht erfassten Gästen z.B. im Bereich der Hotel-Lobby oder einer Außengastronomie, Internetzugang per WLAN als touristischen bzw. gastronomischen Service anbieten wollen oder ein registrierter ausländischer Hotelgast rein sprachlich nicht in der Lage ist, die standardmäßig nur in deutscher und englischer Sprache vorgehaltene Aufklärung über die rechtmäßige Internetnutzung zu verstehen und damit auch wirksam zu akzeptieren.

Das Risiko, als gastronomischer WLAN-Anbieter für ein potentielles Fehlverhalten seiner Gäste in Haftung genommen zu werden, ist derzeit sehr real und stellt insbesondere für kleinere und mittlere Unternehmen, die tendenziell eher über wenig rechtliches und technisches Know-how verfügen, eine durchaus erhebliche Belastung ihrer wirtschaftlichen Betätigung dar.

e) Welche Haftungsprivilegien de lege ferenda sind denkbar?

Für Hoteliers und Gastronomen gilt wir für alle Unternehmer der Grundsatz, dass die besten Lösungen diejenigen sind, die bei größtmöglicher Rechtssicherheit einfach umsetzbar und kostengünstig sind sowie sich im besten Falle sogar förderlich auf das eigene Geschäftsmodell auswirken.

Insofern wäre die radikale Beseitigung sämtlicher Haftungsrisiken für die Bereitsteller von WLAN-Zugängen zur Internetnutzung ohne Etablierung von Sicherungspflichten sicherlich diejenige Variante, die den hessischen Gastgebern die spürbarste Entlastung bringen und zugleich den Serviceansprüchen vieler Gäste entsprechen würde.

In diesem Sinne verstehen wir auch die Empfehlungen der zuständigen Ausschüsse vom 23.10.2015 (BR Drucksache 440/1/15) für die Stellungnahme des Bundesrates zur TMG-Novelle.

Hiernach verfehle die im Regierungsentwurf enthaltene Regelung, wonach eine Haftung des WLAN-Anbieters als Störer nur dann nicht in Betracht komme, wenn der Dienstanbieter angemessene Sicherungsmaßnahmen ergriffen habe, das mit dem Gesetzentwurf verfolgte Ziel, Kdie Verbreitung von WLAN im öffentlichen Raum zu stärken und diesbezügliche Rechtssicherheit zu schaffen.` Dieses Ziel könne Knicht erreicht werden, wenn lediglich versucht wird, die jetzige durch Einzelfallrechtsprechung geschaffene Rechtslage in Gesetzesform zu gießen. Es sind vielmehr Regelungen erforderlich, die sich klar hiervon abgrenzen und klarstellen, dass die Grundsätze der Störerhaftung von WLAN-Anbietern künftig in Deutschland ¯ wie auch derzeit bereits in zahlreichen anderen europäischen Ländern ¯ nicht mehr gelten sollen.`

Sollte diese rigorose und politisch ambitionierte Lösung wegen der ebenso legitimen Interessen der Rechteinhaber am Ende nicht durchsetzbar sein, , stünden die Mitglieder des IHA und des DEHOGA Hessen e.V. daher auch allen Gestaltungsinitiativen aufgeschlossen gegenüber, die zu einer Beseitigung bzw. Reduzierung der bestehenden Haftungsrisiken führen würden und in der Praxis leicht handhabbar wären.

5. Wirtschaftliche Bedeutung und Effekte

b) Haben frei öffentlich zugängliche WLAN-Netze auch für die Tourismuswirtschaft eine Bedeutung?

Die Bedeutung der Bereitstellung von niedrigschwelligen und leistungsstarken Internetzugängen in der Öffentlichkeit für den Tourismus ist kaum zu überschätzen.

Studien und Gästebefragungen belegen immer wieder, dass ein flächendeckender und kostenloser Internetzugang nahezu ein Grundbedürfnis vieler Touristen ist.

Da das Smartphone für immer mehr Menschen das Hauptinstrument ist, um sich über verschiedene internetbasierte Informationsdienste eine neue Umgebung zu erschließen und diese touristisch zu nutzen, wird es immer wichtiger, diesem Gästeverhalten Rechnung zu tragen, um als leistungsstarke und attraktive touristische Destination wahrgenommen zu werden.

Mitglieder sowohl des IHA als auch des DEHOGA Hessen e.V. berichten zunehmend, dass die Frage nach den Zugangsmöglichkeiten zum Internet immer häufiger bereits vor einer Buchung abgefragt werden, es also vielfach schon so ist, dass eine Reiseentscheidung vom leichten Internetzugang abhängig gemacht wird.

Auch in touristischen Bewertungsportalen, die sowohl für die einzelnen Betriebe, als auch für die gesamte Gastronomiebranche zunehmend an Bedeutung gewinnen, finden sich vermehrt Kommentare, die der Bereitstellung und der Leistungsstärke von WLAN-Netzen große Bedeutung beimessen.

Gerade der starke Anstieg der Besucher aus dem asiatischen Raum, namentlich aus China, verstärkt die von den hessischen Gastgebern wahrgenommene Anspruchshaltung, weil diese Gäste es aus ihren Heimatländern gewohnt sind,

nahezu überall im öffentlichen Raum einfach und kostenlos ins Internet zu gelangen. Schaut man sich die Gruppe der chinesischen Gäste genauer an, wird jedoch auch deutlich, welche Herausforderungen sich für mögliche gesetzgeberische Maßnahmen stellen. Zum einen wird es schwierig sein, diese Gäste wirksam über die rechtlichen Nutzungsbedingungen aufzuklären und eine verantwortete und informierte Zustimmung zu entsprechenden Regularien zu erhalten. Zum anderen sind die urheberrechtlichen Standards, die in Deutschland und Europa herrschen, in China und vielen anderen Ländern nicht nur unbekannt, sondern unterliegen auch einem Akzeptanzproblem, weil geistiges Eigentum in anderen Rechts- und Kulturkreisen nicht den gleichen Stellenwert genießt und auch nicht so stark mit wirtschaftlichem Wert verknüpft wird.

Zwar wird man einwenden können, dass die Befriedigung touristischer Bedürfnisse nicht den Stellenwert des Schutzes von geistigem Eigentum erodieren lassen darf. Zu berücksichtigen ist jedoch auch, dass nach bisherigen Erfahrungen im In- und Ausland mit der Ausweitung von öffentlichen WLAN-Angeboten keine erhebliche Zunahme von Urheberrechtsverletzungen verbunden ist.

Es ist daher notwendig, sich den skizzierten Herausforderungen zu stellen und die Möglichkeiten zur risikofreien Bereitstellung von öffentlichen WLAN-Netzen auch im Interesse der touristischen Attraktivität des Reiselandes Hessen zu verbessern.