Stand: 11. November 2015

Teil 2

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 –

11.	Handelsverband Hessen e. V.	S. 98
12.	Förderverein freie Netzwerke e. V., Christian Heise	S. 104
13.	Dr. Ulf Buermeyer, Landgericht Berlin	S. 106
14.	Stadtwerke Marburg GmbH, CityNet, Stefan Koch	S. 116
15.	Unitymedia	S. 122
16.	Mindbase Strategic Consulting	S. 126
17.	Staatskanzlei des Landes Nordrhein-Westfalen, Kordula Attermeyer	S. 139
18.	Hessischer Städtetag	S. 141
19.	Hessischer Landkreistag	S. 143
20.	Medienanstalt Berlin-Brandenburg (mabb)	S. 145

HANDELSVERBAND HESSEN

Stellungnahme zur mündlichen Anhörung des Ausschuss für Wirtschaft, Energie, Verkehr und Landesentwicklung „Freie WLAN-Hotspots in Hessen"

Donnerstag, 12. November 2015

Der Handelsverband Hessen ist ein Landesverband des Handelsverbandes Deutschland (HDE) der Spitzenorganisation des deutschen Einzelhandels. Insgesamt erwirtschaften in Deutschland rund 300.000 Einzelhandelsunternehmen mit drei Millionen Beschäftigten an 450.000 Standorten einen Umsatz von über 450 Milliarden Euro im Jahr. Im Bundesland Hessen liegt der Branchenumsatz bei über 40 Milliarden Euro. 160.000 Beschäftigten sind in Hessen im Einzelhandel beschäftigt. In 17.000 Arbeitsstätten auf einer Verkaufsfläche von 22 Millionen qm.

Etwa ein Drittel der Einzelhändler nutzt auch das Internet als Vertriebskanal. Die fortschreitende Digitalisierung stellt den Einzelhandel vor große Herausforderungen. Die Möglichkeit für Kunden, Waren und Dienstleistungen über das Internet zu bestellen, führt zu einer nachhaltigen Veränderung der Handelsstrukturen. Für die Unternehmen ergeben sich neue Vertriebsoptionen etwa im Rahmen von Multi-Channel-Strategien. Gleichzeitig übernehmen auch Akteure wie Hersteller oder Dienstleister verstärkt Handelsfunktionen und beleben den Wettbewerb. Die mit dem Internet verbundene Transparenz von Angeboten und Preisen hat auch Folgen für das Verhältnis zwischen Verbraucher, Handel und Industrie. Mobile Kommunikation beschleunigt diesen Prozess. Zusätzlich agiert der Einzelhandel immer häufiger in einem internationalen Wettbewerb. In einem wettbewerbsintensiven Umfeld gilt es für den stationären Handel, seine Kernkompetenzen konsequent weiter zu entwickeln. Kaum etwas wirkt stärker auf die Kundenbindung, als ein kundenspezifisches attraktives Sortiment und eine kompetente Beratung. Dabei können digitale Services auf der Fläche zu wichtigen Erfolgsfaktoren werden. Und auch im Zusammenspiel mit dem Online - Kanal bieten sich neue attraktive Chancen für den stationären Handel. Um diese Potenziale zu nutzen, muss der Handel seine Strategien überdenken und seine Geschäftsmodelle vor Ort anpassen. Die Händler brauchen geeignet Rahmenbedingungen, um sich mit innovativen Ideen und Geschäftsmodellen in einem intensiven Wettbewerb profilieren zu können. Dazu gehört auch der Einsatz von öffentlichen WLAN – Angeboten.

Handelsverband Hessen e.V.
Rheinstraße 36
65185 Wiesbaden

Telefon: 0611-372685
Telefax: 0611-302547
E-Mail: service@einzelhandelsverband.de
Website: www.einzelhandelsverband.de

Vereinsregisternummer: VR 6696
Präsident: Friedrich J. Wagner
Hauptgeschäftsführer: Michael Kullmann
Sitz des Vereins: Wiesbaden

Generelle Erwägungen

Ein wichtiger definitorischer Hinweis vorab: Der Handelsverband Hessen definiert einen „freien WLAN-Hotspot" als Sender eines WLAN-Signals, auf das jeder Nutzer eines WLAN-fähigen Devices zugreifen kann. Dabei dürfen im ersten Schritt keine direkten Kosten für den Nutzer entstehen. Ob sich der Hotspot innerhalb eines Gebäudes befindet oder im öffentlichen Raum, ist hierbei unerheblich.

Der Handelsverband Hessen begrüßt ausdrücklich, öffentliche WLAN Angebote zu fördern. Der Einzelhandel misst entsprechenden Services eine hohe Bedeutung bei. In einer breit angelegten HDE-Umfrage gaben fast die Hälfte (48%) der befragten Unternehmen an, dass Sie ihren Kunden gerne WLAN in ihren Geschäften anbieten würden.

Ein solches Angebot ist zentrale Voraussetzung für den Einsatz neuer Technologien im Ladengeschäft. Es wird als Instrument gesehen, die Kundenbindung zu erhöhen, mobile Geräte in Beratung und Kauf einzubeziehen und mobiles Bezahlen zu unterstützen. Auch zur Nutzung von Anwendungen der Beacon - Technologie wie z.B. die Innen- oder Innenstadtnavigation (siehe Amsterdam) kann WLAN einen Beitrag leisten. Überdies gibt es Händlern die Möglichkeit, ihren Kunden zusätzliche Produktinformationen anzubieten oder eine Verknüpfung zum Online – Shop bereitzustellen.

Ein flankierendes öffentliches WLAN Angebot im öffentlichen Raum in Städten und Gemeinden ist ein wichtiger Baustein, für die Attraktivität der Innenstädte. Von diesem Mehrwert profitieren alle in einer Stadt und internationale Gäste setzen diesen Service zunehmend voraus.

Handelsverband Hessen e.V.
Rheinstraße 36
65185 Wiesbaden

Telefon: 0611-372685
Telefax: 0611-302547
E-Mail: service@einzelhandelsverband.de
Website: www.einzelhandelsverband.de

Vereinsregisternummer: VR 6696
Präsident: Friedrich J. Wagner
Hauptgeschäftsführer: Michael Kullmann
Sitz des Vereins: Wiesbaden

Stellungnahme zu den Fragen 4 – 6.

4a) Die Schaffung der notwendigen Infrastruktur ist die Voraussetzung einer dauerhaften Inbetriebnahme eines öffentlichen WLAN-Angebotes. Gerade diese anfänglichen Fixkosten werden oftmals als Hinderungsgrund der Implementierung angeführt. Eine öffentliche Förderung würde diese Hemmnisse abschwächen. Darüber hinaus kann eine Beratungsförderung als sinnvoll erachtet werden. Die Beratung von Städten und Kommen sollte folgende Punkte beinhalten:

- In welchen Bereichen
- ist ein WLAN-Angebot sinnvoll?
- Auf welche Weise kann ein WLAN als Marketing- und Kommunikationskanal genutzt werden?
- Wer ist Betreiber des WLAN?

Eine Förderung des laufenden Betriebs sollte genau abgewogen werden. Ein langfristiger Betrieb kann dadurch gefährdet werden, da die Betriebskosten auch nach der Förderung getragen werden und entsprechend in den Haushalten resp. Budgets verankert sein müssen.

b) Ein flächendeckender Breitbandausbau und die Versorgung - auch ländlicher Regionen - mit Glasfaserkabeln ist Voraussetzung für ein stabiles WLAN-Netz. Für das Bundeland Hessen finden sich die unter www.breitband-in-hessen.de Finanzierungs, Förderungs- und Beratungsangebote. Finanzierung- und Förderinstrumente zur Implementierung eine freier WLAN-Hotspots für den Innenbereich in Ladenlokalen, Hotels oder Gaststätten bieten die KFW-Bank über ihr allgemeines Angebot.

c) Folgende Modelle sind dem Handelsverband bekannt:
1. Die Stadt betreibt das WLAN
2. Eine stadteigene/ stadtnahe Gesellschaft betreibt das WLAN
3. Ein Provider betreibt das WLAN

Aktuell trifft man vermehrt auf Variante 3 – der Grund dafür liegt in der Tatsache, dass es grundsätzlich jedem Anbieter möglich ist, ein „City-Wifi" zu eröffnen und dieses auch zu benennen. Das führt zu den sogenannten „Insellösungen". Diese Modelle haben allerdings keinen echten Mehrwert für die Städte und Kommunen, da das WLAN als Kommunikationskanal für Städte verloren geht. Ein nachhaltiger und langfristiger Betrieb ist nicht sichergestellt. Flächendeckende WLAN-Angebote, mit der Stadt als Betreiber finden sich selten, das liegt aus unserer Sicht, an fehlenden klaren Zuständigkeiten und Verantwortungsbereichen in den Verwaltungen-

Handelsverband Hessen e.V.
Rheinstraße 36
65185 Wiesbaden

Telefon: 0611-372685
Telefax: 0611-302547
E-Mail: service@einzelhandelsverband.de
Website: www.einzelhandelsverband.de

Vereinsregisternummer: VR 6696
Präsident: Friedrich J. Wagner
Hauptgeschäftsführer: Michael Kullmann
Sitz des Vereins: Wiesbaden

d) Der Handelsverband begrüßt den Gedanken, dem das Modell „Freifunk" zu Grunde liegt und auch das bürgerschaftliche Engagement der Betreiber.
Aus unserer Sicht, kann das Modell „Freifunk" für den professionellen Ausbau eines WLAN-Angebotes in Hessen aktuell allerdings keine Rolle spielen. Die (Rechts-)unsicherheit ist der Grund für diese Einschätzung. Das Modell „Freifunk" bewegt sich in einer rechtlichen Grauzone, da der Traffic über Server im Ausland geleitet wird und somit nicht das deutsche Recht Anwendung findet.

Weiter müssen folgende Punkte beim Modell „Freifunk" kritisch gesehen werden:

- Schwankende Geschwindigkeiten durch fehlendes Loadbalancing
- Qualität der Hardware
- Sicherheit für die Nutzer
- Keine Kindersicherung oder Sperrung von Ports
- Zentrale Infrastruktur (VPN) ermöglicht gezielte Angriffe

e) Als Voraussetzung für die stabile Versorgung des öffentlichen Raumes mit WLAN sind folgende Punkte zu nennen:

- Stabile und sichere Internetverbindung, im optimalen Fall über ein Glasfaserkabel
- Professionelle Hardware, die speziell für den Einsatz im öffentlichen- respektive outdoor- Bereich vorgesehen ist.
  Professionellen und unabhängigen WLAN-Provider als Partner
- Support für Nutzer und Betreiber 24 Stunden, 7 Tage die Woche auf verschiedenen Sprachen
- Zentrales Remote Management

f) Für eine Zusammenarbeit der genannten Stellen spricht, dass auf diese Weise die sogenannten Insellösungen vermieden und ein flächendeckendes WLAN-Angebot bereitgestellt werden kann. Sämtliche Vorteile eines WLAN Netzes können so von einer Stadt genutzt werden. Gleichzeitig ist zu befürchten, dass durch die Einbindung verschiedener Stellen, die Entscheidungsprozesse verlangsamt werden.

g) Hier sind verschiedene Optionen denkbar. Die Aufbaukosten können sowohl von der Stadt, vom Provider als auch von stadtnahen Gesellschaften getragen werden. Ähnlich verhält es sich mit den Betriebskosten. Eine weitere Möglichkeit ist, dass Aufbau und Betreib von Immobilieneigentümern finanziell unterstützt werden kann.

Handelsverband Hessen e.V.
Rheinstraße 36
65185 Wiesbaden

Telefon: 0611-372685
Telefax: 0611-302547
E-Mail: service@einzelhandelsverband.de
Website: www.einzelhandelsverband.de

Vereinsregisternummer: VR 6696
Präsident: Friedrich J. Wagner
Hauptgeschäftsführer: Michael Kullmann
Sitz des Vereins: Wiesbaden

5.a)

- Hebung der innerstädtischen Aufenthaltsqualität.
- Schaffung eines zusätzlichen Marketing- und Kommunikationskanal. Informationen zu Veranstaltungen, Behörden und Stadtpläne können veröffentlich werden.
- Stärkung des stationären Handels/Gastronomie/Dienstleister durch Einbindung in ein flächendeckendes WLAN-Netzes.
- Steigerung der Attraktivität für Touristen und Besucher.
- Finanzieller Nutzen für ausländische Touristen, da Roaming-Kosten entfallen.

b) Wir sehen einen zentralen Nutzen für die Tourismuswirtschaft. Internationale Besucher erwarten ein flächendeckendes WLAN-Angebot, welches im optimalen Falle mit der mehrsprachigen Touristeninfo gekoppelt ist.

c) Durch den Service „kostenfreies WLAN" steigt die Attraktivität und Urbanität der Innenstädte. Somit profitieren alle innenstadtrelevanten Akteure von Angebot. Aus Sicht des Handels ist der Ausbau des WLAN-Angebotes in den Innenstädten im Zuge der Digitalisierung zwingend notwendig. Die nachfolge Grafik des Handelsverbandes Deutschland illustriert die die Einsatzmöglichkeiten von WLAN im Handel.

Diese Nutzung setzt einen öffentlichen WLAN-Zugang „instore" voraus. Hier ist es wichtig, dass der Internetanschluss (in diesem Fall der Anschluss des Händlers) nicht vertraglich in Verbindung mit dem WLAN-Angebot stehen sollte. Der Händler seinen WLAN-Provider frei wählen und im besten Falle, sich an das City-Wifi anschließen kann. Dies hätte zur Folge, dass sich der Nutzer sowohl auf der Straße, als auch im Laden (im Hotel, oder im Restaurant) im gleichen Netz befindet.

d) LTE ist aus Sicht des Handels keine vergleichbare Leistung und steht somit nicht in Konkurrenz zu einem flächendeckenden WLAN-Angebot. Öffentliches-WLAN sollte als Kommunikationskanal der Städte angesehen werden, um hierdurch Besucher, Touristen und Bürger zu erreichen und zu informieren. Weiter stellt ein öffentliches WLAN sicher, dass die Geschwindigkeit der Verbindung und die Datenvolumen für alle Nutzer in einem hohen Maße gegeben sind.

e) Diese Frage ist uns nicht verständlich und müsste konkretisiert werden.
Grundsätzlich ist jedem privatwirtschaftlichen Anbieter freigesellt ein WLAN-Signal auszustrahlen und somit seine Dienstleistung Dritten anzubieten.

6. a) Die Möglichkeit der Förderung über den Ausbau des Breitbandnetzes wurde bereits angeführt. Im Bundesland Thüringen ist diese Förderung jüngst explizit auf den Ausbau eines öffentlichen WLAN-Angebotes ausgeweitet worden.

Handelsverband Hessen e.V.
Rheinstraße 36
65185 Wiesbaden

Telefon: 0611-372685
Telefax: 0611-302547
E-Mail: service@einzelhandelsverband.de
Website: www.einzelhandelsverband.de

Vereinsregisternummer: VR 6696
Präsident: Friedrich J. Wagner
Hauptgeschäftsführer: Michael Kullmann
Sitz des Vereins: Wiesbaden

Eisert, Martina (HLT)

Betreff: WG: Anhörung des Ausschusses für Wirtschaft, Energie, Verkehr und Landesentwicklung

Von: christian.heise@gmail.com [mailto:christian.heise@gmail.com] **Im Auftrag von** Christian Heise
Gesendet: Mittwoch, 4. November 2015 09:34
An: Eisert, Martina (HLT)
Cc: verein@foerderverein.freie-netzwerke.de
Betreff: Re: Anhörung des Ausschusses für Wirtschaft, Energie, Verkehr und Landesentwicklung

Liebe Frau Eisert,

leider haben wir es auf Grund der vielseitigen ehrenamtlichen Aktivitäten des Fördervereins freie Netzwerke e.V. und deren Mitgliedern nicht rechtzeitig geschafft eine Stellungnahme für das Land Hessen abzugeben und können leider auch nicht persönlich nach Wiesbaden kommen.

Wir schließen uns aber ausdrücklich der Stellungnahme von Freifunk Wiesbaden an und sehen unsere Bedenken auch in der Stellungnahme des Digitale Gesellschaft e.V. (https://digitalegesellschaft.de/wp-content/uploads/2015/11/DigiGes-Stellungnahme-WLAN-Hessen.pdf) und der Stellungnahme von Reto Mantz umfassend berücksichtigt.

Folgende 5 Punkte stehen (aus Sicht Fördervereins freie Netzwerke e.V.) dabei auch weiterhin im Zentrum der Kritik am TMG-Entwurf:

1. Mittels § 8 Abs. 4 TMG-E werden kommerzielle Anbieter aufgefordert, verschlüsselte Netzwerke aufzubauen. **Verschlüsselung ist** aber genau **das Gegenteil von öffentlichen WLANs**. Verschlüsselung behindert die Verbreitung öffentlicher WLANs! Wir fragen uns, wie das bei öffentlichen Hotspot-Lösungen technisch und praktisch umgesetzt werden soll? Wie sollen Nutzer_Innen einen Hotspot (beispielsweise bei der Bahn oder in einem Flüchtlingsheim) nutzen, wenn der Nutzer auf ein verschlüsseltes WLAN gar nicht zugreifen kann, um sich anzumelden. Darüber hinaus ist die Verschlüsselung des Netzzugangs derzeit technisch mit lediglich einem Schlüssel möglich, der doch wieder allen potentiellen Nutzern bekannt gemacht werden müsste. Damit ist sie wirkungslos. Entscheidend im Sinne der IT-Sicherheit ist allein die Sicherung der Einstellungen des Routers mittels Passwort und die Verschlüsselung seitens der Nutzer.
2. Auch mit §8 Abs. 5 TMG-E wird lediglich ein Placeboeffekt erzeugt. Die Nutzer_Innen sollen einen beliebigen Namen eingeben und versichern, keine rechtswidrigen Handlungen vorzunehmen. Diese **Maßnahmen im Rahmen des Entwurfs sind weder zur Abschreckung noch zur Aufklärung möglicher Straftaten geeignet und werfen rechtsmethodisch ungewollte datenschutzrechtliche Herausforderungen auf**. Dieser Absatz würde für weitere Unsicherheit (auch bei der Bereitstellung von WLANs z.B. in Flüchtlingsheimen) sorgen, da weder der Umfang dieser Erhebung, noch die rechtliche Absicherung im Entwurf er- oder geklärt wird. Abgesehen davon ist auch unklar, ob die Erhebung des Namens überhaupt stattfinden darf? § 12 Abs. 1 TMG sieht vor, dass personenbezogene Daten (wie der Name!) nur erhoben werden dürfen, wenn dieses Gesetz es erlaubt. Es stellt sich aber die Frage, ob § 8 Abs. 5 TMG-E diesem Erfordernis gerecht wird.
3. Im Entwurf wird der **Erfüllungsaufwand und die wirtschaftliche Auswirkungen** mit **"keine"** bewertet. Das **ist nachweislich falsch**, denn Betreiber von WLANs müssten nach dem vorliegenden Gesetzesentwurf ihre WLANs komplett neu konfigurieren. Gerade kleinere Betreiber haben derzeit auch gar nicht die Möglichkeit, die Einwilligung einzuholen. Sie müssten sich also neue Anlagen kaufen. Das ist ein erheblicher wirtschaftlicher Faktor, der möglicherweise sogar zum WLAN-Sterben führen könnte. Das gilt darüber hinaus auch für WLANs der öffentlichen Hand.
4. Der Gesetzesentwurf geht in seiner Begründung auch von einem **sinkenden Beratungsbedarf** bei WLANs aus (unter „Weitere Kosten"). Im Rahmen der bisher genannten Punkte ist diese Begründung **ebenfalls falsch**.

5. **Keine Vereinbarkeit mit Art. 12 der EU E-Commerce-Richtlinie**: Hier könnte die neue Regelung des § 8 TMG vor dem EuGH landen, bevor tatsächlich Rechtssicherheit eintritt. Es ist davon auszugehen, dass die im Entwurf genannten Regelungen durch Art. 12 ECRL verboten sind.

Wir würden uns freuen, wenn sie diese Nachricht an die Abgeordneten weiterleiten können. Bei weiteren Rückfragen stehe ich Ihnen jederzeit unter 01711430774 zur Verfügung.

Mit freundlichen Grüßen,
Christian Heise

Vorstand Förderverein freie Netzwerke e.V.

Gutachterliche Stellungnahme

zur Anhörung

Freie WLAN-Hotspots in Hessen

im Hessischen Landtag in Wiesbaden
am 12. November 2015

von

Dr. iur. Ulf Buermeyer, LL.M. (Columbia)

Richter am Landgericht Berlin

ulf@buermeyer.de

Berlin, den 4. November 2015

Meine Stellungnahme orientiert sich an dem seitens der Verwaltung des Landtages übermittelten Fragenkatalog. Sie konzentriert sich dabei auf die Ziffern 1 bis 3 des Fragenkataloges, da diese genuin juristische Fragen betreffen.

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 Begriffe beschreiben unterschiedliche Dienste „rund um das Internet", die jedoch nicht legaldefiniert sind. Phänomenologisch lassen sich folgende Dienste unterscheiden:

- ein **Access-Provider** bietet Kunden den Zugang zum Internet

- ein **Host-Provider** stellt Speicherplatz für Informationen und Services zum Zugriff hierauf zur Verfügung (WWW-Provider, eMail-Provider)

- ein **Content-Provider** bietet Informationen im Netz zum Abruf durch Dritte an, wobei diese Informationen nicht selten von den Nutzern des Dienstes hochgeladen werden, sodass der Content-Provider letztlich vor allem die Plattform bereitstellt, auf der Nutzer sich austauschen (wie etwa Facebook)

Das Telemediengesetz enthält Haftungsprivilegierungen für Access-Provider (in § 8 TMG) und Host-Provider (in § 10 TMG).

WLAN-Betreiber bieten einen Zugang zum Internet an, sind also Access-Provider; ihre Tätigkeit ist zugleich jedenfalls dem Wortlaut nach unter § 8 Abs. 1 TMG zu subsumieren.

Über die Frage, ob die Privilegierung des § 8 Abs. 1 TMG auf sie tatsächlich anwendbar ist, ist gleichwohl Verwirrung entstanden. Denn der BGH hat in seiner Entscheidung

„Sommer unseres Lebens“[1] nur den – offensichtlich nicht einschlägigen, da nur auf Host-Provider anwendbaren – § 10 TMG geprüft und (insoweit zutreffend) dessen Anwendbarkeit verneint, während er § 8 Abs. 1 TMG nicht einmal geprüft hat. Diese Nicht-Anwendung einer offenkundig einschlägigen Norm ist rational nur schwer nachzuvollziehen und lässt besorgen, der Senat habe die Anwendung der Norm um jeden Preis vermeiden wollen.

b) Wann erfahren Access-Provider eine Haftungsprivilegierung?

Gem. § 8 Abs. 1 TMG sind sie *„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.“*

Diese Definition beschreibt – wie die Überschrift des § 8 TMG bereits andeutet – die bloße „Durchleitung von Informationen“, ohne auf deren Inhalt Einfluss zu nehmen, und umfasst damit die Tätigkeit der Internet-Zugangsanbieter / Access-Provider. Damit sind auch die Betreiber von WLAN-Zugängen zum Internet umfasst, solange sie auf die übertragenen Inhalte keinen Einfluss nehmen. Wesentlich ist, dass weder gewerbliches Handeln noch gar die Registrierung eines Anbieters als Provider beispielsweise bei der Bundesnetzagentur Voraussetzung dieses sog. „Provider-Privilegs“ ist. Die gesetzliche Haftungsprivilegierung stellt allein auf die Natur der erbrachten Dienstleistung ab.

Die Haftungsprivilegierung gilt jedoch nicht, wenn Zugangs-Anbieter absichtlich mit einem Nutzer ihres Dienstes zusammenarbeiten, um rechtswidrige Handlungen zu begehen (§ 8 Abs. 1 Satz 2 TMG).

---

[1] BGH, Urteil vom 12. Mai 2010, I ZR 121/08.

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

Keine, sofern sie nicht absichtlich mit einem Nutzer ihres Dienstes zusammenarbeiten, um rechtswidrige Handlungen zu begehen (§ 8 Abs. 1 Satz 2 TMG). Hintergrund dieser gesetzlichen Wertentscheidung in § 8 Abs. 1 TMG ist die Erkenntnis, dass ein bloßer Zugang zum Internet wertneutral ist und alle etwaigen Netz-Sperren technisch leicht zu umgehen wären. Daher würde es keinen Sinn machen, Zugangs-Anbieter zu irgendwelchen Sperren oder Filterungen zu verpflichten.

Im Übrigen setzt § 8 TMG die Vorgabe des Art. 12 der e-Commerce-Richtlinie[2] über die „Reine Durchleitung" von Inhalten um, der eine „automatische" Verantwortlichkeit von Zugangsanbietern selbst im Falle positiver Kenntnis von einer über seine Infrastruktur vorgenommene Rechtsverletzung nicht zulässt. Die Richtlinie enthält in Art. 12 Abs. 3 lediglich eine Öffnungsklausel dafür, dass „ein Gericht oder eine Verwaltungsbehörde ... vom Diensteanbieter verlangt, die Rechtsverletzung abzustellen oder zu verhindern". Von dieser Möglichkeit hat der Bundesgesetzgeber jedoch in § 8 TMG keinen Gebrauch gemacht.

[2] Richtlinie des 2000/31/EG des Europäischen Parlaments und des Rates über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt, Abl. EG L 178/1 vom 17. Juli 2000.

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

Nach hier vertretener Auffassung fallen alle Betreiber von Internet-Zugangsdiensten – somit auch die Betreiber von WLAN-Hotspots – unter die Haftungsprivilegierung des § 8 Abs. 1 TMG. Sie haften damit zumindest nicht auf Schadensersatz.

Fraglich ist indes, ob sie auf Unterlassen der Mitwirkung an einer fremden Rechtsverletzung in Anspruch genommen werden können (sog. Störerhaftung). Nach hier vertretener Auffassung lässt die e-Commerce-Richtlinie es aber nur unter den Voraussetzungen ihres Art. 12 Abs. 3 zu, von einem Diensteanbieter zu verlangen, eine Rechtsverletzung abzustellen. Dies lässt wie gezeigt allein Unterlassungsverlangen durch eine Gericht oder eine Verwaltungsbehörde zu, nicht aber durch Private. Auch wenn § 8 TMG keine ausdrückliche Regelung für die Haftung auf Unterlassen enthält, so ist die Norm zumindest europarechtskonform so auszulegen, dass alleine gerichtliche Unterlassungsanordnungen oder Unterlassungsverfügungen durch die Exekutive zulässig sind. Privatrechtlichen Unterlassens-Verlangen sind hingegen von der Öffnungsklausel des Art. 12 Abs. 3 ECRL nicht gedeckt und dürfen daher auch vom nationalen Recht nicht vorgesehen werden – und demnach auch keine kostenpflichtigen Unterlassens-Aufforderungen (Abmahnungen). In diesem Sinne ist folglich auch § 8 TMG auszulegen, der Art. 12 ECRL in nationales Recht umsetzt.

Diese Rechtsauffassung, die sich eindeutig erst aus dem Rückgriff auf Art. 12 der ECRL ergibt, ist indes noch nicht allgemeine Auffassung der Instanzgerichte, sodass sich Betreiber von WLAN-Internetzugängen de facto, wenn auch contra legem, durchaus der Gefahr aussetzen, im Falle von Rechtsverletzungen auf Unterlassung in Anspruch genommen zu werden.

e) Welche Haftungsprivilegierungen de lege ferenda sind denkbar?

Die Haftungsfreistellung des § 8 Abs. 1 TMG kann – und sollte – dahingehend klargestellt werden, dass zum einen auch die Anbieter von drahtlosen Internet-Zugängen eindeutig erfasst sind und zum anderen eindeutig auch die Haftung auf Unterlassen

ausgeschlossen ist. Dies entspricht zwar nach hiesiger Auffassung bereits der heutigen Rechtslage. Doch zeigt die Vielzahl von Abmahnungen auch von WLAN-Anbietern, dass die Rechtslage jedenfalls in der gerichtlichen Praxis nicht hinreichend eindeutig ist. Dies wiederum wird von interessierten Kreise für das Geschäft mit Abmahnungen ausgenutzt.

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

Eine solche Differenzierung ist abzulehnen, da sie bereits mit der e-Commerce-Richtlinie, der diese Unterscheidung fremd ist, nicht zu vereinbaren wäre. Aber auch sachlich ist nicht zu erkennen, warum Private gegenüber gewerblichen Betreibern von Internet-Zugängen privilegiert oder benachteiligt werden sollten: Sie alle haben aus technischer Sicht gleichermaßen keine realistische Möglichkeit, die Nutzung des Internet über den von ihnen betriebenen Zugang zu kontrollieren. Demnach wäre eine solche Unterscheidung im Lichte des Art. 3 Abs. 1 GG (allgemeiner Gleichheitssatz) nicht zu rechtfertigen.

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

Aus kriminalistischer Sicht spielen öffentliche WLAN-Zugänge keine Rolle. Zwar bieten sie einen de facto anonymen Zugang zum Internet, da die Zuordnung einer konkreten Nutzerin bzw. eines konkreten Nutzers zu einer IP-Adresse in aller Regel nicht möglich ist. Doch gibt es auch abgesehen von öffentlichen WLAN-Diensten eine Vielzahl von einfachen Möglichkeiten, das Internet anonym zu nutzen, sodass diese Möglichkeit in der Praxis der Strafverfolgung nicht relevant wird. Dies zeigen auch die empirischen Erfahrungen mit öffentlichen WLAN-Netzen: Die Medienanstalt Berlin-Brandenburg, die in Berlin gemeinsam mit der Firma Kabel Deutschland ein Pilotprojekt eines öffentlichen

WLAN-Netzes betrieb[3] und auch mit verschiedenen Freifunk-Initiativen kooperiert, berichtet, dass nach ihren Erfahrungen offene Internet-Zugänge gerade nicht zu rechtswidrigen Handlungen missbraucht worden seien[4].

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

Hierzu lässt sich keine pauschale Aussage treffen. In aller Regel werden Betreiber eines WLAN keinerlei Veranlassung haben, davon auszugehen, dass ihre Nutzer Straftaten begehen werden. Und selbst wenn Betreiber darüber nachdenken sollten, ob möglicherweise über ihren Zugang etwa beleidigende Kommentaren in Online-Foren hinterlassen werden könnten, so würde es jedenfalls an der für eine Strafbarkeit wegen Beihilfe notwendigen hinreichenden Konkretisierung der für möglich gehaltenen Straftaten – etwa: Person des Täters, konkrete strafbare Äußerung – fehlen.

2. Datensicherheit und Datenschutz

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

Es gibt keinen Grund, eine Haftungsprivilegierung auf verschlüsselte Internet-Zugänge zu beschränken. Im Gegenteil ist eine Verschlüsselung entweder unter dem Aspekt der Datensicherheit wirkungslos – nämlich wenn das Passwort allgemein bekannt ist –, oder sie stellt eine erhebliche Hürde für die bequeme Nutzung eines WLANs dar, wenn nämlich erst ein individuelles Passwort vergeben werden muss (auf welchem Wege?).

Im Übrigen haben es Nutzerinnen und Nutzer in der Hand, durch die Nutzung von verschlüsselten Internet-Verbindungen (z.B. via SSL, HTTPS) auch in offenen WLANs die

[3] http://mabb.de/presse/pressemitteilungen/details/pilotprojekt-public-wifi-von-mabb-und-kabel-deutschland-erfolgreich-abgeschlossen-734.html

[4] http://www.mabb.de/presse/pressemitteilungen/details/wlan-zugang-ohne-barrieren.html

Sicherheit ihrer Daten zu gewährleisten. Solche Verfahren sind bei allen sicherheitskritischen Inhalten ohnehin Standard (etwa bei WWW-Seiten von Banken oder eMail-Anbietern).

Technisch etwas versiertere Nutzerinnen und Nutzer können außerdem einen VPN-Zugang zum Internet nutzen, sodass der komplette Datenverkehr über das WLAN verschlüsselt wird.

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

Nein. Auf die Antwort zu Frage 2 a) wird verwiesen.

3. Internationaler Vergleich

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

Nach meiner Kenntnis existieren der Störerhaftung vergleichbare Haftungsrisiken für WLAN-Betreiber nirgendwo auf der Welt. In den Vereinigten Staaten beispielsweise gilt eine dem § 8 Abs. 1 TMG vergleichbare generelle Haftungsfreistellung für Access Provider unter dem Aspekt der reinen Durchleitung von Informationen („mere conduit"), vgl. 17 U.S.C. § 512 (a)[5], der teilweise fast wörtlich Art. 12 Abs. 1 der ECRL und

[5] A service provider shall not be liable … if
(1) the transmission of the material was initiated by or at the direction of a person other than the service provider;
(2) the transmission, routing, provision of connections, or storage is carried out through an automatic technical process without selection of the material by the service provider;
(3) the service provider does not select the recipients of the material except as an automatic response to the request of another person;

§ 8 Abs. 1 TMG entspricht. Diese Regelung ist in den USA – soweit ersichtlich – rechtspolitisch nicht umstritten, selbst seitens der Content-Industrie wird keine Verantwortlichkeit von Internet-Zugangsanbietern für übertragene Inhalte angestrebt.

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

Die nicht eindeutige und rechtssichere Anwendung der Privilegierung des § 8 Abs. 1 TMG auf WLANs ist ein deutscher Sonderweg, der die Nutzung des Internet unterwegs behindert, ohne dass dem gesellschaftliche Vorteile gegenüberstünden.

Das Land Hessen sollte sich im Bundesrat dafür einsetzen, dass die Störerhaftung für Betreiber öffentlicher WLANs in rechtssicherer Weise abgeschafft wird. Dies leistet etwa der Gesetzentwurf der Fraktionen der Grünen und der Linken im Deutschen Bundestag[6]. Der Gesetzentwurf der Bundesregierung zur Änderung des TMG[7] hingegen sieht vor, unklar definierte „Maßnahmen", um „eine Rechtsverletzung durch Nutzer zu verhindern", zur Bedingung einer Haftungsprivilegierung für WLAN-Zugangsanbieter zu machen. Er würde damit lediglich die bestehende **Rechtsunsicherheit** durch eine neue, diesmal im Gesetz selbst angelegte Rechtsunsicherheit ersetzen. Zudem stellt der Regierungsentwurf eine **Verschlechterung** der Rechtslage dar, weil – zutreffend, insbesondere europarechtskonform ausgelegt – bereits der geltende § 8 Abs. 1 TMG eine unbedingte Haftungsfreistellung für WLAN-Provider vorsieht. Schließlich wäre der Regierungsentwurf aus den oben näher dargelegten Gründen mit der Vorgabe des Art. 12 ECRL nicht vereinbar und daher **europarechtswidrig**. Nicht umsonst hat auch die Europäische Kommission in ihrer Stellungnahme zum Regierungsentwurf im Rahmen

---

(4) no copy of the material made by the service provider in the course of such intermediate or transient storage is maintained on the system or network in a manner ordinarily accessible to anyone other than anticipated recipients, and no such copy is maintained on the system or network in a manner ordinarily accessible to such anticipated recipients for a longer period than is reasonably necessary for the transmission, routing, or provision of connections; and

(5) the material is transmitted through the system or network without modification of its content.

[6] BT-Drucks. 18/3047.

[7] BR-Drucks. 440/15.

des Notifizierungs-Verfahrens gem. Richtlinie 98/34/EG darauf hingewiesen, dass Access-Providern nach dem eindeutigen Wortlaut des Art. 12 ECRL sowie des Erwägungsgrundes 48 der ECRL keine Sorgfaltspflichten auferlegt werden dürfen. Damit wäre § 8 Abs. 4 TMG in der Fassung des Regierungsentwurfs nicht zu vereinbaren, ggf. wäre ein Vertragsverletzungsverfahren zu besorgen.

Die geltende Regelung des § 8 TMG bedarf vielmehr lediglich der gesetzlichen **Klarstellung**, um der bestehenden Rechtsunsicherheit zu begegnen. Dies leistet etwa der Gesetzentwurf der Oppositionsfraktionen im Deutschen Bundestag[8]. Der Regierungsentwurf hingegen kann dieses Ziel nur in der Fassung des Änderungsantrages des Landes Nordrhein-Westfalen erreichen, der von den Ausschüssen des Bundesrats mehrheitlich zur Annahme empfohlen wurde[9]. Die Abstimmung im Plenum des Bundesrats ist für den 6. November 2015 vorgesehen.

Berlin, den 4. November 2015

Dr. Ulf Buermeyer, LL.M. (Columbia)

[8] BT-Drucks. 18/3047.

[9] BR-Drucksache 440/1/15.

Stadtwerke Marburg GmbH · Postfach 2180 · 35009 Marburg

Hessischer Landtag
Frau Claudia Lingelbach
Postfach 3240
65022 Wiesbaden

STADTWERKE MARBURG

Netze
Planung / Dokumentation
Ansprechpartner:
Markus Scholz
Tel.: 06421 205714
Fax: 06421 205300
markus.scholz@swmr.de

5. November 2015 / IHa

Öffentliche Anhörung des Ausschusses für Wirtschaft, Energie, Verkehr und Landesentwicklung zum Thema Freie WLAN-Hotspots in Hessen
Stellungnahme der Stadtwerke Marburg GmbH zu „Freie WLAN-Hotspots in Hessen"

Sehr geehrte Damen und Herren,
sehr geehrte Frau Lingelbach,

wir bedanken uns für die Möglichkeit, im Rahmen der öffentlichen Anhörung des Ausschusses für Wirtschaft, Energie, Verkehr und Landesentwicklung zum Thema „Freie WLAN-Hotspots in Hessen" Stellung zu nehmen.

Zunächst einige Sätze zu den Stadtwerken Marburg:

Die Stadtwerke Marburg GmbH als 100% kommunales Unternehmen ist seit 2003 im Telekommunikationsmarkt aktiv. Neben der Erschließung von Geschäftskunden in Gewerbegebieten mit eigenen Glasfasernetzen wurde ab 2005 im Landkreis Marburg-Biedenkopf ein kreisweites Funknetz zur Versorgung der sogenannten „weißen Flecken" aufgebaut. Mehrt als 2/3 dieser nicht oder schlecht versorgten Gebiete wurden bereits 2010 - übrigens ohne einen Euro Fördergeld - mit Internetanbindungen versorgt.

Seit 2013 erschließen die Stadtwerke Stadtteile der Stadt Marburg flächendeckend mit einem neuen Glasfasernetz, basierend auf dem modernsten FTTH-Standard (Glasfaser bis in die Wohnung). Hier werden garantierte Bandbreiten von 200 Mbit/s angeboten, das Netz ist Gigabit-Ready. Bei entsprechender Nachfrage könnten bereits heute Bandbreiten von 1.000 Mbit/s angeboten werden. Die Stadtwerke treten als Anbieter für Internet und Telefonie auf, stellen das Netz - ohne rechtliche Verpflichtung - aber auch für andere Netzbetreiber bereit.

Seit Frühjahr 2015 bieten die Stadtwerke Marburg im Stadtgebiet von Marburg auch freies öffentliches Internet per WLAN („CityWiFi") an.

...

Beginnend mit dem Marktplatz, Bahnhofsvorplatz, Stadion und Großsporthalle sollen bis 2016 alle für Bürger und Tourismus wichtigen öffentlichen Aufenthalts- und Veranstaltungsbereiche in der Stadt mit einem leistungsfähigen freien Internetzugang per WLAN ausgestattet sein. Wichtig sind für uns eine einfache Nutzbarkeit für den Bürger sowie ein Schutz der persönlichen Daten der Nutzer. Nach einmaliger Registrierung der E-Mail-Adresse wird ein Endgerät des Nutzers (Smartphone, Tablet) stadtweit wiedererkannt, der Nutzer kann bis zu 1 Jahr stadtweit, ohne dass er sich irgendwo erneut anmelden muss, den Zugang nutzen. Ergänzend werden auch Hotels, Gaststätten und Geschäften der Anschluss an das CityWiFi angeboten. Das Ziel ist: Eine Stadt - ein WLAN-Zugang.

Seit Juni 2015 versorgen die Stadtwerke auch die neue Marburger Erstaufnahmeeinrichtung für ca. 800 Flüchtlinge (Zeltdorf) mit einem freien Internetzugang per WLAN. Es gibt Ihnen die Möglichkeit, sich nicht nur als betreutes Objekt zu erfahren, sondern aktiv Informationen über ein für sie fremdes Land einzuholen, Online-Sprachkurse zu nutzen oder einfach den Kontakt zu Familienangehörigen und Freunden im Heimatland oder in Europa aufzunehmen.

Im Folgenden möchten wir zum Thema Ihrer Anhörung Stellung nehmen:

Grundsätzliches:

Wir halten, wie auch der Bundesverband der Verbraucherzentralen[1], die gegenwärtige Rechtslage für grundsätzlich verfehlt. Sie steht mit zentralen Prinzipien eines demokratischen Rechtsstaats in Konflikt und verstößt gegen Art. 12.1 der E-Commerce-Richtlinie der EU.

Anbietern von öffentlichen Internetzugängen per WLAN wird mittels eines gesetzlich nicht kodifizierten Richterrechts (die europaweit wohl einmalige sogenannte Störerhaftung) eine Haftung für rechtswidriges Verhalten von Nutzern auferlegt.

Zur Begründung wird ausgeführt, wer einen Zugang zum Internet ermögliche, eröffne eine Gefahrenquelle für rechtswidrige Taten im Zuge der Nutzung des Internets und müsse sich daher grundsätzlich diese Taten zurechnen lassen, sofern er nicht Vorgaben zur Beschränkung und Überwachung des Zugangs erfülle.

Der Geist einer solchen Argumentation wird vielleicht greifbar, wenn man dieses Argument auf andere Bereiche oder Dienste überträgt:

Wer einen Zugang zum Briefversandt oder Paketversand eröffnet, indem er einen Briefkasten aufstellt, schafft eine Gefahrenquelle für rechtswidrige Taten durch die Beförderung (Beleidigungen, Handel mit urheberechtsverletzenden Werken, Briefbomben etc.) und haftet daher für diese, sofern er nicht den Versender vorher erfasst hat und dieser vorher bestätigt, bei dem Versand keine Straftaten zu begehen?

Wer einen öffentlichen Platz oder Park zum Aufenthalt bereitstellt, eröffnet eine Gefahrenquelle (Körperverletzungen, Drogenhandel, Handel mit urheberechtsverletzenden Werken) und haftet dafür, wenn nicht den Zugang kontrolliert und die Nutzer vorher bestätigen lässt, dass sie auf dem Platz keine Straftaten begehen?

Eine solche Bewertung nimmt einen unbeteiligten Infrastrukturanbieter für Handeln Dritter in Sippenhaft.

---

[1] http://www.bmwi.de/BMWi/Redaktion/PDF/Stellungnahmen/Stellungnahmen-WLAN/verbraucherzentrale-bund,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf

Verschärft wird die Lage dadurch, dass die Voraussetzungen dafür, wie man eben diese gesetzlich nicht geregelte Haftung vermeiden kann, unklar, unbestimmt, wechselnd und bisher gesetzlich ebenfalls nicht kodifiziert sind

Diese sich daraus ergebende aktuelle Rechtslage ist weder mit dem Wesentlichkeitsgrundsatz (wesentliche Dinge sind vom Gesetzgeber zu regeln) noch mit dem Bestimmtheitsgrundsatz des Rechtsstaatsprinzips vereinbar.

Diese Rechtslage hat in der Summe dazu geführt, dass wie allgemein beklagt öffentliche, frei zugängliche WLAN-Netze in Deutschland kaum vorhanden sind. Für Hotels, Gaststätten oder Ähnliches hat sich hierdurch ein Markt für WLAN-Hotspot-Anbieter gebildet, die den armen Hoteliers & Co. vor allem Rechtsicherheit und Haftungsfreistellung gegen Entgelt anbieten, indem sie selber die Anbieterrolle übernehmen.

Der bisher vorliegende Gesetzentwurf zur Änderung des TMG führt leider zu keiner durchgreifenden Änderung. Erneut werden in § 8 Abs. 4 E-TMG Voraussetzungen an eine Haftungsfreistellung geknüpft. Es bleibt auch das Geheimnis der Entwurfsverfasser, wie mit den zahlreichen neuen unbestimmten Rechtsbegriffen (zumutbare Maßnahmen, angemessene Sicherungsmaßnahmen, unberechtigte Nutzer) Rechtssicherhaft bei der Haftung geschaffen werden soll.

Wer sind bei einem freien öffentlichen WLAN unberechnete Nutzer, wo doch der Dienst gerade der Öffentlichkeit, d.h. grundsätzlich allen zur Verfügung stehen soll? Was für Maßnahmen gegen einen Zugang muss ich dabei treffen, wo ich doch bei einem freien öffentlichen WLAN den Zugang möglichst einfach allen ermöglichen will?

Dabei wäre eine rechtsichere gesetzliche Lösung ganz einfach möglich, wenn man § 8 Abs. 4 E-TMG auf den ersten Halbsatz beschränkt:

(4) Diensteanbieter nach Absatz 3 können wegen einer rechtswidrigen Handlung eines Nutzers nicht auf Beseitigung oder Unterlassung in Anspruch genommen werden.

Zusammenfassend lässt sich sagen, dass die Stadtwerke nicht wegen, sondern trotz der rechtlichen Regelung öffentliche WLAN-Netze ausbauen.

Zur Ihren Fragen im Einzelnen:

1. Rechtliche Rahmenbedingungen

Wir möchten hier in Gänze auf die aktuelle Stellungnahme des Wirtschaftsausschuss des Bundesrates vom 23.10.2015 zum Änderungsentwurf des TMG[2] verweisen. Dieser können wir uns nur anschließen.

2. Datensicherheit und Datenschutz

a) Nach dem ursprünglichen Entwurf des § 8 Abs. 4 TMG wurde die Verschlüsselung nicht zur Datensicherheit oder dem Datenschutz vorgeschrieben, sondern als Mittel der Zugangskontrolle. Eine Verschlüsselung für öffentlich allgemein zugängliche WLAN-Zugänge als Zugangskontrolle führt sich aber ad absurdum. Ein Schlüssel, der auf Anfrage jedem sofort elektronisch mitgeteilt wird, hat keinen Effekt, es erhöht nur die Komplexität des Zugangs.

Er kann auch nicht der Datensicherheit dienen, weil jeder Interessierte ihn jederzeit bekommt und damit die Daten anderer entschlüsseln kann.

[2] http://www.bundesrat.de/drs.html?id=440-1-15

Aus diesem Grunde arbeiten nahezu alle öffentlichen WLAN-Netze unverschlüsselt.

Es würde daher eine Abschaffung öffentlicher frei zugänglicher WLAN-Netze bedeuten, eine Haftungsfreistellung an Verschlüsselung zu koppeln.

Eine Verschlüsselung auf Netzebene ist auch nicht erforderlich. Benutzer werden vom Endgerät auf die Gefahren unverschlüsselter Verbindungen hingewiesen, die Datensicherheit muss und kann durch sichere Verschlüsselung auf Anwendungsebene (E-Mail-Programm etc.) sichergestellt werden. Hier sind gesetzliche Vorgaben für Anbieter wie Whatsup etc. sinnvoll.

b) Erforderlich sind Vorgaben, die für jeden Telekommunikationsanbieter selbstverständlich sind: Schutz der Daten und des Fernmeldegeheimnisses jedes Nutzers vor einer Aufzeichnung und Auswertung durch den Anbieter.

3. Internationaler Vergleich

a) An dieser Stelle soll auf die Eco-Studie aus dem November 2014 zur Verbreitung von WLAN Zugängen in Deutschland mit internationalem Vergleich verwiesen werden[3].

b) Eine klare gesetzliche Regelung ohne unangemessene Haftungsregeln wie eine Störerhaftung fördert massiv das Angebot öffentlich zugänglicher WLAN-Netze. Länder mit entsprechenden Regelungen haben 10-30mal mehr öffentliche Zugangspunkte.

4. Ausbau

a) Ein Förderung-Programm hat eine Signal- und Initialwirkung und kann daher den Ausbau von freien öffentlichen WLAN erheblich beschleunigen. Es entstehen überwiegend einmalige Kosten, die aufgrund der entgeltfreien Nutzung nicht durch die Nutzung erlöst, aber gut über Förderprogramme gedeckt werden können.

b) Förderprogramme für den Ausbau kommunaler Infrastruktur wären für Kommunen nutzbar, stehen aber im Wettbewerb zu anderen wichtigen kommunalen Aufgaben und sind daher wenig geeignet für ein explizites Vorantreiben von öffentlichen WLAN-Angeboten in Hessen.

Hessen könnte jedoch aus den 46 Mio. €, die es aus der sogenannten Digitalen Dividende erhält, einen Teil für ein spezielles Förderprogramm für öffentliche freie WLAN-Netze verwenden. Hier sollte eine uneingeschränkte freie Nutzung ohne Kundenverhältnis und ohne persönliche Anmeldung zur Voraussetzung gemacht werden. Kommerzielle Anbieter, die nur Ihren Kunden einen uneingeschränkten Zugang bieten, der Öffentlichkeit aber nur einem limitierten, sollten von der Förderung ausgeschlossen werden.

c) Aus Gründen der oben skizzierten Rechtslage werden in aller Regel kommerzielle Anbieter mit der WLAN-Versorgung beauftragt, um nicht in die Gefahr von Haftungsfällen zu kommen. Das führt dazu, dass die eigentlichen „Anbieter" wie Hoteliers, Kneipiers oder auch Kommunen sich nicht in der Anbieterrolle wiederfinden und auf zum Teil zweifelhafte Geschäftsmodelle bezüglich der Datenverwendung der Nutzer angewiesen sind.

d) Das Modell „Freifunk" gewährleistet zwar auf technischer Ebene die Aushebelung der aktuellen Haftungsproblematik. Die Zielrichtung von „Freifunk" ist zu begrüßen. Eine leistungsfähige Versorgung der gewünschten öffentlichen Räume kann auf dieser Basis (zufälliges Engagement einzelner) nicht

[3] https://www.eco.de/wp-content/blogs.dir/eco-microresearch_verbreitung-und-nutzung-von-wlan1.pdf

gewährleistet werden. Wir sind der Auffassung, dass eine WLAN-Versorgung auf öffentlichen Plätzen und Räumen auch eine gewisse Zuverlässigkeit und Leistungsfähigkeit haben sollte.

e) Für eine leistungsfähige Versorgung ist neben der Bereitstellung der nötigen Standorte vor allem eine tragfähige und dauerhafte Finanzierung dieser Vorhaben notwendig, da von den Nutzern typischerweise keine Erlöse fließen.

f) Wir erkennen nur Gründe für eine Zusammenarbeit. Die teilweise schwierigen technischen und rechtlichen Fragen bei Aufbau eines stadtweiten Netzes lassen sich in Kooperation effektiver klären. Zudem verfügen Kommunen und der ÖPNV über viele geeignete Standorte.

In Marburg wurden beispielsweise neue elektronische Fahrgastinformationssysteme zur Aufnahme von leistungsfähiger WLAN-Technik mit direkter Glasfaseranbindung genutzt.

City-WiFi am Bahnhofsvorplatz in Marburg

g) Die Kosten kann nur der mittelbare Nutznießer tragen, da der direkte Nutzer für den Service nichts zahlt. Das ist regelmäßig der Eigentümer oder der Betreiber der entsprechenden Lokation, die mit dem öffentlichen WLAN aufgewertet wird (beispielsweise der Besitzer einer Kneipe oder eines Hotels, aber auch die Kommune bei einer Steigerung der Aufenthaltsqualität öffentlicher Plätze oder der Förderung des Tourismus oder der ÖPNV für WLAN-Angebote im öffentlichen Nahverkehr).

5. Wirtschaftliche Bedeutung

a) Die Aufenthaltsqualität öffentlicher Plätze oder Veranstaltungsorte oder auch des ÖPNV nimmt zu. WLAN lässt sich zur Steuerung gewünschter Aufenthaltsorte verwenden.

b) Touristen, die häufig keine Mobilfunktarife für Deutschland gebucht haben, finden ein Vorhandensein solcher Angebote sehr attraktiv. Daneben lassen sich über solche Netze zielgerichtet Informationen an Touristen übermitteln, bis hin zu modernen beacon-gesteuerten Stadtführungen.

c) Ein öffentliches WLAN-Netz kann die Basis für weitere intelligente Plattformen sein, die die Kommune für die lokalen Anbieter von Waren und Produkten bereitstellt bzw. koordiniert. Beispielsweise könnte eine „Lokal Amazon" Plattform mit einer zugehörigen App implementiert werden, auf der lokale Anbieter von Waren und Produkten diese bewerben und verkaufen und, beacon-gesteuert, beim Passieren des Ladenlokal weitere Informationen wie aktuelle Angebote an den Kunden übermittelt

werden. Die Kommune unterstützt hierbei lokale Händler mit Ladengeschäftigen im Wettbewerb mit dem Onlinehandel.

d) WLAN-Angebote werden nie eine komplette Flächendeckung und vollständige Mobilität bieten, Angebote wie LTE werden durch öffentliche WLAN-Netze daher nicht obsolet.

Im Übrigen sind Mobilfunkangebote wie LTE gerade dort, wo sich viele Menschen aufhalten, häufig chronisch überlastet und kaum nutzbar.

e) Bestehende WLAN-Angebote gegen Entgelt leisten nicht, was als Ziel öffentlicher WLAN-Netze erreicht werden soll: Eine unkomplizierte Versorgung öffentlicher Plätze mit Internet und Informationen für alle Bürger und Touristen. Dieser öffentliche Zweck wird und kann nicht ebenso gut durch punktuelle WLAN-Angebote kommerzieller Anbieter erreicht werden, eine Betätigung gemäß § 121 HGO ist daher zulässig.

Die öffentliche Straßenbeleuchtung kann auch nicht durch aufstellen von privaten Laternen mit Münzeinwurf erreicht werden.

6. Förderprojekte im Bundesvergleich

Fraglich ist, ob damit jede von der Kommune beauftragte WLAN-Versorgung einer ihrer Liegenschaften und Plätze oder eher flächendeckende Vorhaben wie in Marburg gemeint sind.

In erstem Falle dürfte es zahlreiche Fälle geben, im letzteren Falle sind uns keine bekannt.

Mit freundlichen Grüßen
Stadtwerke Marburg GmbH

Rainer Kühne
Geschäftsführer

ppa. Alexander Schurz
Prokurist

unitymedia

„Freie WLAN-Hotspots in Hessen“

Stellungnahme von Unitymedia

Unitymedia mit Hauptsitz in Köln ist der führende Kabelnetzbetreiber in Deutschland und eine Tochter von Liberty Global, dem größten internationalen Kabelunternehmen mit Niederlassungen in 14 Ländern. Unitymedia erreicht mit seinem Glasfaser-Koax-Netz 12,7 Millionen Haushalte mit Breitbandkabeldiensten. Neben klassischen Kabel-TV-Dienstleistungen bietet Unitymedia seinen Kunden auch die Versorgung mit Telefonie sowie Highspeed- Internet mit Bandbreiten bis 200 MBit/s und ist so zum wichtigen Infrastrukturwettbewerber im Telekommunikations- und Breitbandmarkt geworden. Ende 2014 hatte Unitymedia 7,1 Mio. Kunden, die 6,6 Mio. TV-Abonnements und 2,9 Mio. Internet- sowie 2,7 Mio. Telefonie-Abonnements bezogen haben. Weitere Informationen zu Unitymedia finden Sie unter www.unitymedia.de.

Unitymedia hat Anfang des Jahres mit dem Aufbau eines freien WLAN-Netzes begonnen und hat im Rahmen dieser Wifi-Initiative in 100 Städten innerhalb unseres Verbreitungsgebiets ein öffentliches WLAN-Netz errichtet. Insgesamt wurden dabei bisher rund 1.000 Hotspots in Betrieb genommen. Die nächste Ausbaustufe mit einem noch attraktiveren Angebot für Endkonsumenten ist bereits für 2016 in Planung. Ergänzt wird dieses Angebot bereits heute durch unser B2B-Produkt „Powerspot“, welches Geschäftskunden wie z.B. Restaurants oder Cafés die Möglichkeit bietet, öffentliche und für ihre Kunden kostenloste WLAN-Hotspots einzurichten und dabei sogar eine eigene Landingpage zu gestalten. Diese wird dem Nutzer bei der Einwahl in das WLAN angezeigt und kann seitens unseres „Powerspot“-Partners beispielsweise mit aktuellen Informationen und Angeboten gestaltet werden.
Zur Nutzung unseres WLANs können sich Nutzer auf einfachstem Weg mittels einer SMS registrieren und erhalten dann – ebenfalls per SMS – einen Zugangscode, mit dem sie sich – wahlweise auch über eine verschlüsselte Verbindung – mit dem Internet verbinden können. Unseren Breitbandkunden steht dieser Service ohne die sonst übliche Volumenbegrenzung zur Verfügung; zeitlich unbefristet ist die Nutzung sogar für alle Kunden.

Fragenkomplex 1 – Rechtliche Rahmenbedingungen

1. a) bis 1. e), 1. h)

Hinsichtlich der rechtlichen Rahmenbedingungen, die in den Fragen 1. a) bis 1. e) sowie 1. h) abgefragt werden, verweisen wir auf die Stellungnahme unseres Verbandes BITKOM vom 2. November 2015. Zu den Fragen 1. f) und 1. g) siehe nachfolgend.

1. f) und 1. g)

Für die schnelle Verbreitung öffentlicher WLAN-Netze ist es unabdingbar, den jeweiligen Betreibern die notwendige Rechtssicherheit zu geben und hierfür die rechtlichen Voraussetzungen zu schaffen. Dabei gilt es,

einen angemessen Ausgleich zwischen den Interessen der Rechteinhaber und Sicherheitsinteressen auf der einen Seite und der Verbreitung von öffentlich zugänglichem WLAN auf der anderen Seite zu ermöglichen. Die notwendige Abwägung muss berücksichtigen, dass es sich auf beiden Seiten um legitime Interessen handelt.

Sowohl hinsichtlich der von öffentlich zugänglichen WLAN-Netzen ausgehenden Gefahren als auch in Bezug auf die rechtlichen Rahmenbedingungen gibt es Unterschiede zwischen von kommerziellen Anbietern und von Privaten betriebenen Angeboten. Die bisherigen Erfahrung mit offenem WLAN-Netzen zeigen, dass die öffentlichen Hotspots gewerblicher Access-Provider nahezu ausschließlich zum Zweck der Kommunikation und der Information genutzt werden, nicht hingegen zur Begehung von Rechtsverletzung, gleich ob urheberrechtlicher oder sicherheitsrelevanter Art. So bezieht sich nahezu die gesamte Rechtsprechung zur Störerhaftung ausschließlich auf private Hotspots, welche meist unzureichend gesichert waren und sodann zu Rechtsverletzungen genutzt wurden.

Hierbei besteht möglicherweise ein Zusammenhang mit den unterschiedlichen rechtlichen Rahmenbedingungen, denen gewerbliche und private WLAN-Betreiber unterliegen. Gerade gewerbliche WLAN-Betreiber sind bereits heute verpflichtet, entsprechend hohe Sicherheitsstandards aufrecht zu erhalten und beispielsweise auf Anordnung auch sicherheitspolitisch wünschenswerte TKÜ-Überwachungsmaßnahmen zu ermöglichen, wohingegen private WLAN-Betreiber von diesen Pflichten bisher nicht erfasst sind. Die technisch komplexen Voraussetzungen hierfür wären von ihnen auch nur schwer zu gewährleisten. Im Gegensatz zu gewerblichen Anbietern unterliegen sie insoweit nicht den Vorgaben des Telekommunikationsgesetzes sowie Anordnungen der Bundesnetzagentur und könnten auch im Falle von richterlichen Beschlüssen den geforderten Aufklärungsmaßnahmen im Bereich der Strafverfolgung nur schwerlich nachkommen.

Neben den selbst im Aufbau befindlichen öffentlichen WLAN-Netzen bietet Unitymedia mit dem B2B-Produkt „Power-Spot“ zudem Geschäftskunden die Möglichkeit, öffentliche und für ihre Kunden kostenloste WLAN-Hotspots einzurichten, ohne dabei dem Risiko der Störerhaftung zu unterliegen – diese übernimmt im Fall des Falles Unitymedia. Auch in diesem Sinne leisten wir einen Beitrag zur schnellen Verbreitung von öffentlichem WLAN, und das in Übereinstimmung mit höchsten Sicherheitsstandards.

Fragenkomplex 2 – Datensicherheit und Datenschutz

Hinsichtlich Datensicherheit und Datenschutz ist zwischen den Themen einer verschlüsselten Kommunikation und einer Zugangskontrolle zu einem geschützten WLAN-Netz zu unterscheiden. Die Verknüpfung von Haftungsprivilegierungen mit einer Verschlüsselung der Kommunikation erscheint nicht sinnvoll, da die Verschlüsselung einer anderen Zielsetzung dient, nämlich der Sicherung des Datentransfers gegen einen unberechtigten Zugriff von Dritten auf diese Daten. Sie ermöglicht aber selbst keine Verfolgung von Rechtverletzungen, die eine Haftungsprivilegierung rechtfertigen würde. Anders sieht es hingegen im Hinblick auf eine Zugangskontrolle aus, die die unberechtigte Einwahl in ein WLAN-Netz unterbindet.

Gleichwohl unterstützen wir den Ansatz, den Einsatz von Verschlüsselungsmethoden aus Gründen der Datensicherheit zu fördern. Aus diesem Grund bieten wir allen Nutzern neben einem unverschlüsselten Zugang

zum WLAN die Möglichkeit, ohne zusätzliche Kosten auch eine dem Stand der Technik entsprechende verschlüsselte Verbindung (nach Standard WPA2-Enterprise) zu nutzen und somit sicher im Internet zu surfen. Der Nutzer kann bei jeder Einwahl selbst entscheiden, ob er die unverschlüsselte Verbindung nutzen möchte, oder ob er lieber auf eine verschlüsselte Kommunikation zurückgreift, weil er beispielsweise sensible Bankgeschäfte erledigen möchte.

Fragenkomplex 3 – Internationaler Vergleich

Hinsichtlich des internationalen Vergleichs verweisen wir auf die Stellungnahme unseres Verbandes BITKOM vom 2. November 2015.

Fragenkomplex 4 – Ausbau

Im Markt herrschen zurzeit großer Wettbewerb und eine enorme Dynamik, was den Ausbau frei zugänglicher WLAN-Netze angeht. So ist Unitymedia dabei, bis Ende 2015 ein öffentliches WLAN-Netz in 100 Städten mit insgesamt über 1.000 „Wifispots“ innerhalb unseres Verbreitungsgebiets aufzubauen. Zudem bietet Unitymedia mit dem B2B-Produkt „Power-Spot“ Geschäftskunden – z.B. Cafés, Restaurants, Hotels, etc. – die Möglichkeit, öffentliche WLAN-Hotspots für ihre Kunden einzurichten – und das völlig risikolos im Hinblick auf die Störerhaftung. Wir bieten damit unseren B2B-Kunden eine einfache Möglichkeit zur Einrichtung eines Kunden-WLANs und verdichten so gleichzeitig unser eigenes WLAN-Netz, auch über die 100 unmittelbar ausgebauten Städte hinaus.

Ähnliche Initiativen zum Ausbau öffentlicher WLAN-Netze gibt es auch seitens unserer Wettbewerber. Dort, wo der Ausbau bereits ohne öffentliche Fördermaßnahmen wie aufgezeigt voranschreitet, dürfen getätigte privatwirtschaftliche Investitionen durch die öffentliche Förderung oder gar den öffentlich betriebenen Ausbau von konkurrierenden WLAN-Angeboten nicht entwertet werden. Gerade in Innenstadtbereichen und an öffentlichen Plätzen oder in Parks kann es jedoch notwendig und hilfreich sein, potentiellen Betreibern den Aufbau der notwendigen Hardware zu ermöglichen und die notwendigen rechtlichen Voraussetzungen, z.B. etwaige Wegerechte, unbürokratisch zu einzuräumen.

Fragekomplex 5 – Wirtschaftliche Bedeutung und Effekte

Die Einrichtung öffentlicher WLAN-Netze ist auch ein Beitrag zur Erhöhung der touristischen Attraktivität von Innenstädten. Sie laden erfahrungsgemäß zu einer längeren Verweildauer an öffentlichen Plätzen oder z.B. auch in Geschäften, Restaurants und Cafés ein. Insbesondere ausländische Touristen, die ansonsten nicht ohne weiteres auf einen mobilen Internetzugang im Rahmen eines Mobilfunkvertrages zurückgreifen können, profitieren besonders von den Möglichkeiten durch ein öffentliches WLAN-Netz.

Städten und Gemeinden bietet Unitymedia besondere Kooperationen an, durch die sie ebenso wie unsere Powerspot-Kunden eine individuelle und auf Wunsch von ihnen redaktionell betreute Startseite erstellen können, die jeder Nutzer beim Einloggen in das WLAN-Netz zu sehen bekommt. Auf dieser sog. Landing-Page können dann beispielsweise touristische Informationen zu der jeweiligen Kommune angezeigt werden,

Restaurants haben die Möglichkeit ihre Speisekarte zu hinterlegen und Geschäfte können z.B. auf besondere Angebote hinweisen. Dies stellt zum einen einen deutlichen touristischen Mehrwehrt für den jeweiligen Anbieter dar und gibt zum anderen dem Nutzer des Hotspots die Möglichkeit, Zugang zu für ihn wertvolle Informationen einfach und ohne lange Suche im Internet zu erhalten. Gerade dieses Alleinstellungsmerkmal des Angebots von Unitymedia bietet über den generellen Nutzen öffentlicher WLAN-Netze hinaus einen zusätzlichen besonderen touristischen oder auch geschäftlichen Mehrwert.

Angesichts der großen Herausforderung, die sich in vielen deutschen Städten und Gemeinden im Rahmen der aktuellen Flüchtlingskrise stellt, hat sich Unitymedia zudem entschlossen, überall dort, wo dies für uns möglich und von den Betreibern gewünscht ist, WLAN-Hotspots für Flüchtlingsunterkünfte einzurichten. Damit soll den Flüchtlingen ermöglicht werden, mit ihrer Familie in der Heimat in Kontakt zu bleiben und Zugang zu im Internet verfügbaren Informationen zu erhalten. Unitymedia arbeitet so in partnerschaftlicher Abstimmung mit Kommunen und Hilfsorganisationen daran, die Situation für die Flüchtlinge zu verbessern. Auch in Hessen konnten erste Unterkünfte bereits mit WLAN ausgestattet werden.

Aus unserer Sicht gibt es durch öffentliche WLAN-Netze auch keine größeren negativen Auswirkungen auf (lokale) Telekommunikationsbetreiber, da WLAN zwar komplementär beispielsweise zu LTE genutzt werden könnte, es sich gleichwohl um andere Nutzungsszenarien handelt und WLAN zudem auch zusätzlich (ausländische) Touristen adressiert, die ggf. keinen Zugang zu einer mobilen Datenverbindung haben. Hingegen sehen wir eher positive Auswirkungen, da gerade an Orten, an denen viele Menschen auf einmal zusammenkommen (Innenstädte, Veranstaltungsorte, Stadien, etc.), ein gut funktionierendes WLAN-Netz die überlasteten Funkzellen von Mobilfunkanbietern entlastet und zudem zahlreiche Zusatzangebote ermöglicht.

Berlin, den 6. November 2015

Mindbase Strategic Consulting
Stefan Herwig
Horster Straße 31
45897 Gelsenkirchen
Tel: 0209 38 650 670
Fax: 0209 38 650 668

Hessischer Landtag

Öffentliche mündliche Anhörung des Ausschuss für Wirtschaft, Energie, Verkehr und Landesentwicklung zum Thema:

Freie WLAN-Hotspots in Hessen

Anhörung am Donnerstag 12. November 2015

Stellungnahme Stefan HERWIG / Mindbase Strategic Consulting

A. Vorbemerkung

Mindbase ist ein netzpolitischer Thinktank und eine Beratungsagentur. Ihr Geschäftsführer Stefan Herwig befasste sich im Rahmen seines kommunikationswissenschaftlichen Studiums seit 2007 wissenschaftlich mit netzpolitischen Problemstellungen wie Datenschutz, Providerhaftung, Netzökonomie und Urheberrecht. Er publizierte Ende 2012 wissenschaftlich zu dem Anhörungsthema: Zur Austarierung von Anonymität und Verantwortung im Netz (Zeitung für Datenschutz (ZD) 12/2012, C.H. Beck Verlag). Die Erkenntnisse aus seiner wissenschaftlichen Arbeit sind Grundlage dieser Stellungname.

Bei der Ausarbeitung dieser Eingabe wurde Mindbase juristisch durch Dr. Christian Volkmann beraten. Dr. Volkmann ist Rechtsanwalt mit Sitz in Berlin. Er ist Fachanwalt für Gewerblichen Rechtschutz, E-Commerce, Recht der neuen Medien (Internetrecht) und Urheberrecht. Er veröffentlichte seit 2002 über 40 Fachaufsätze zum Thema Providerhaftung. Curriculum Vitae: http://www.advokat.de/anwaelte/dr-christian-volkmann/

Darüber hinaus wurde Mindbase in IT-Sicherheitsfragen durch die Firma Forensik.it, Florian Rothenaicher beraten.

(Stellungnahme Mindbase, Landtag Hessen Seite 2)

B. Executive Summary

Grundlage für die Anhörung ist ein Antrag des hessischen Landtags „den Zugang zu öffentlichen drahtlosen lokalen Netzwerk in Hessen zu unterstützen und zu fördern." Zusätzlich soll die im bisherigen Referentenentwurf für die sog. Telemediengesetz(hiernach: TMG)-Novelle vorgeschlagene Ungleichbehandlung von privaten und öffentlichen WLAN zurückgenommen werden. WLAN Betreiber sollen „unabhängig von ihrem jeweiligen institutionellen und organisatorischen Hintergrund" wie Access Provider nach §8 TMG eine Haftungsprivilegierung erfahren.

Obwohl der Vorstoß des hessischen Landtags generell unterstützenswert ist – insbesondere was die Gleichstellung des Status' privater und öffentlicher WLANs angeht – sehen wir eine Ausdehnung der Haftungsprivilegierung von WLAN-Betreibern parallel zur momentanen Haftungsprivilegierung von Accessprovidern, also Internet Service Providern wie der Telekom, Unitymedia, Vodafone etc. kritisch. Das Problem ist, dass hiermit auf ein bereits weitgehend dysfunktionales Haftungssystem im TMG eine weitere dysfunktionale Ebene aufgesattelt würde.

Die Haftung im TMG – und auf der europäischen Ebene in der E-Commerce Richtlinie (hiernach: EC-RL) ist Gegenstand einer langanhaltenden und äußerst komplexen Rechtsfortschreibung durch die Judikative. Auf allen Ebenen bemühen sich die Gerichte die Regelungen des TMG bzw. der EC-RL konform zu anderen Rechtsgütern und insbesondere Ansprüchen Dritter zu gestalten. Eine Rechtssicherheit findet hier momentan aber weder auf der Hostproviderebene noch auf der Accessprovider Ebene statt. Das liegt nicht zuletzt an dem veralteten TMG-Rechtsrahmen der vornehmlich aus den Jahren 1995 – 1999 stammt, damals noch als „Informations- und Kommunikationsdienstegesetz" (IuKDG) bekannt.

1. Problemaufriss

Grund für die unbefriedigende Entwicklung sind die widerstreitenden Abwägungskriterien im Koordinatensystem der auf die Providerhaftung anwendbaren Regelungen. Da sind einerseits die schützenswerten Interessen der Inhaber von Rechten, die in den allgemeinen nationalen Gesetzen (UrhG, MarkenG, BGB) aber auch in der Urheberrechtsrichtlinie sowie der Enforcementrichtlinie der EU geregelt sind. Andererseits sind da die ebenfalls schützenswerten Interessen der Provider, die nach der E-Commerce-Richtlinie und dem TMG zu berücksichtigen sind.

Die abzuwägenden Interessen stehen sich seit Jahren nahezu unverändert gegenüber und haben in der deutschen und internationalen Rechtsprechung eine Einzelfallkasuistik hervorgebracht, die weit von einem rechtssicheren Haftungsrahmen bzw. einer den rechtsstaatlichen Anforderungen genügenden Rechtsdurchsetzung entfernt ist. Dies gilt insbesondere für Provider, die Inhalte für Dritte speichern („Host-Provider"), aber ebenso für Provider, die ihren Kunden den Zugang zum Netz vermitteln („Access-Provider") sowie für Rechteinhaber, aber auch andere Dritte durch Online-kommunikation geschädigte Parteien. Bei den Access-Providern zeigt sich exemplarisch die ganze Hilflosigkeit der Rechtsprechung, wenn der EuGH in der Entscheidung vom 27.03.2014 - C-314/12 - UPC Telekabel Wien / Constantin Film Verleih im Leitsatz Folgendes formuliert:

(Stellungnahme Mindbase, Landtag Hessen Seite 3)

„Die durch das Unionsrecht anerkannten Grundrechte sind dahin auszulegen, dass sie einer gerichtlichen Anordnung nicht entgegenstehen, mit der einem Anbieter von Internetzugangsdiensten verboten wird, seinen Kunden den Zugang zu einer Website zu ermöglichen, auf der ohne Zustimmung der Rechtsinhaber Schutzgegenstände online zugänglich gemacht werden, wenn die Anordnung keine Angaben dazu enthält, welche Maßnahmen dieser Anbieter ergreifen muss, und wenn er Beugestrafen wegen eines Verstoßes gegen die Anordnung durch den Nachweis abwenden kann, dass er alle zumutbaren Maßnahmen ergriffen hat; dies setzt allerdings voraus, dass die ergriffenen Maßnahmen zum einen den Internetnutzern nicht unnötig die Möglichkeit vorenthalten, in rechtmäßiger Weise Zugang zu den verfügbaren Informationen zu erlangen, und zum anderen bewirken, dass unerlaubte Zugriffe auf die Schutzgegenstände verhindert oder zumindest erschwert werden und dass die Internetnutzer, die die Dienste des Adressaten der Anordnung in Anspruch nehmen, zuverlässig davon abgehalten werden, auf die ihnen unter Verletzung des Rechts des geistigen Eigentums zugänglich gemachten Schutzgegenstände zuzugreifen, was die nationalen Behörden und Gerichte zu prüfen haben.“

Der EuGH schreibt in diesem Leitsatz nur auf, was die Gesetzeslage ihm vorgibt, und versucht diese mit einer Austarierung der Interessen in Einklang zu bringen. Weniger präzise und rechtssicher geht es allerdings kaum mehr. Im Rahmen einer Liberalisierung des Zugangs freier W-Lans, in dem WLAN-Betreiber wie Accessprovider haften sollen, werden WLAN-Betreiber und eventuelle Geschädigte nun in dieses dysfunktionale Haftungsregime hereingezogen.

2. Widersprüchliche Rechtsprechung

Wer welche Pflichten bei welcher Art der Rechtsverletzung und welcher Art der konkreten Ausgestaltung eines Dienste, der alle möglichen entscheidungsrelevanten Facetten aufweisen kann, haben soll, entscheiden die Gerichte über mehrere Instanzen zumeist anhand von allgemeinen Gerechtigkeitserwägungen.

Rechteinhaber und Provider streiten in jedem Einzelfall erbittert, wessen Interessen überwiegen. Überwiegen die Interessen des Rechteinhabers, ist die Folge in aller Regel eine ganz erhebliche Belastung der haftenden Provider. Denn diese müssen die Rechtsverletzung nicht nur abstellen, sondern sie auch in der Zukunft verhindern, d. h. sie müssen Inhalte zwangsläufig filtern. Überwiegen demgegenüber die Interessen des Providers, bleibt der Inhalt online; die Rechtsverletzung wird zementiert. Dies bedeutet im Ergebnis, dass die gerichtliche Entscheidung für eine der beiden Parteien untragbar ist.

3. Zielvision

Abschließend ist es insofern vorrangig, der Liberalisierung freier WLAN Hotspots eine ausgewogene und funktionale Haftungslogik voranzustellen. Im Rahmen der TMG-Novelle wird dies jedoch nur für Urheberrechtsverletzungen versucht, andere Haftungslücken verbleiben.

(Stellungnahme Mindbase, Landtag Hessen Seite 4)

Eine funktionale Austarierung des Haftungssystems für Host- und Accessprovider sollte idealerweise auf der Providerebene sinnvoll ineinandergreifen, keine Schutzlücken offenlassen und alle gegenständlichen Rechtsgüter, wie Persönlichkeitsrechtsverletzungen, Jugendmedienschutz sicherstellen, aber auch vor Cybercrime-Tatbeständen wie Phishing, Abofallen, Scam- und Scareware und der Ausspähung von Rechnern entgegenwirken, dies bei angemessener Berücksichtigung der Zumutbarkeit für die verschiedenen Providerklassen. Insbesondere der Punkt Cyberkriminalität ist bei der Ausgestaltung von WLAN-Haftung von besonderer Bedeutung, denn durch eine Liberalisierung der Haftung ergäben sich weitere Schutzlücken auf gleich mehreren Ebenen, wie wir unten (siehe 1.g) ausführen werden.

Darüber hinaus ist es sinnvoll darauf hinzuweisen, dass innerhalb der Europäischen Kommission für diese Legislaturperiode eine Überarbeitung der E-Commerce-Richtlinie geplant ist, in der das gesamte Haftungsregime möglicherweise nochmal überarbeitet wird. Auch vor diesem Hintergrund ist eine entsprechende bundesweite Justierung der WLAN-Haftung zu bedenken. Sie könnte durch eine Öffnung der EC-RL sehr schnell obsolet werden.

C. Fragen

1. Rechtliche Rahmenbedingungen

a) Was ist der rechtliche Unterschied zwischen Content-, Host- und Accessprovidern und inwiefern ist diese Einordnung für W-Lan-Betreiber von Bedeutung?

Contentprovider bieten eigene Inhalte an, vgl. § 7 I TMG (vgl. auch Erwägungsgrund 42 der ECRL). Dazu zählen in der Regel Webseitenbetreiber wie Blogs, oder auch E-Commerce Anbieter, die ihr Angebot ausschließlich selbst betreiben.

Accessprovider vermitteln den Zugang zu einem Telekommunikationsnetz (bzw. fremden Informationen),vgl. § 8 TMG, Art. 12 ECRL dazu zählen momentan vor allem Internet Service Provider.

Hostprovider speichern fremde Inhalte im Auftrag Dritter, vgl. § 10 TMG, Art. 14 ECRL. Dazu zählen eine große Anzahl von Diensten, sowohl Speicherdienste für Dritte (sog. Cyberlocker oder Cloudservices), als auch Webseiten, die Inhalte anderer zugänglich machen (Social Media Netzwerke, Internetforen, Handelsplätze wie eBay oder Amazon), Kundenbewertungsportale, etc., aber auch Rechenzentren, die Speicherplatz anbieten.

Die abstrakte Kategorisierung dieser unterschiedlichen Diensteklassen macht eine Einarbeitung der Politik in die Haftungssystematik deutlich schwieriger als sie theoretisch sein müsste. Auch ist es problematisch, verschiedene Diensteebenen (z.B. Rechenzentren/Serverbetreiber, Clouddienste und Webseitenbetreiber, etc. als die Diensteklasse Hostprovider) zusammen zu fassen.

(Stellungnahme Mindbase, Landtag Hessen Seite 5)

Momentane Rechtsprechung:

Der Betreiber eines WLAN kann insofern allenfalls als Accessprovider i.S.d. § 8 TMG, Art. 12 ECRL angesehen werden. Es steht aber zu beachten, dass möglicherweise keine der drei Diensteklassen für diese Einteilung sinnvoll ist und, dass für WLAN-Betreiber ggf. eine eigene Diensteklasse definiert werden könnte, um das Haftungsregime sinnvoll auszutarieren.

Nach geltender Rechtsprechung jedoch dürfte für kommerzielle Anbieter von WLAN (z.B. Telekom-Hotspot) die Anwendung des § 8 TMG, Art. 12 ECRL weitgehend unstreitig sein.

Bei nichtkommerziellen privaten Anbietern und öffentlichen Anbietern (z.B. der Landtag Hessen) ist zu differenzieren:

Diese fallen nicht in den Anwendungsbereich der EC-RL, da das Europarecht im Grundsatz nur gewerbliche Tätigkeiten regeln kann (ggf. ergeben sich hier im Rahmen der EuGH - McFadden - Vorlagefrage neue Erkenntnisse, mündliche Verhandlung am 09.12.2015).

Unter Umständen können sich diese jedoch gleichwohl auf § 8 TMG berufen, da das nationale TMG über §§ 1, 2 TMG ausdrücklich auch unentgeltliche und öffentliche Diensteanbieter erfassen will.

Der Grundsatz der Vollharmonisierung der EC-RL steht hier nicht per se entgegen, da die EC-RL für nichtkommerzielle private und öffentliche Anbieter keine Regelungen trifft.

b) Wann erfahren Access-Provider eine Haftungsprivilegierung?

Accessprovider haften weder **strafrechtlich** noch **zivilrechtlich auf Schadenersatz**, sofern die Voraussetzungen des § 8 Abs. 1 TMG erfüllt sind:

- Bloße Zugangsvermittlung zu fremden Informationen, d.h. Übermittlung der Informationen werden nicht selbst nicht veranlasst, ein Adressat wird nicht ausgewählt, die Information selbst wird nicht ausgewählt oder verändert.

- Kein kollusives Zusammenwirken mit dem Nutzer des Dienstes, um rechtswidrige Handlungen zu begehen.

Keine Haftungsprivilegierung i.e.S. erfahren Accessprovider jedoch, soweit es um **Ansprüche auf Beseitigung und Unterlassung (Verhinderung)** von Rechtsverletzungen Dritter geht (§ 7 Abs. 2 Satz 2 TMG). Siehe hierzu auch die komplexe Austarierung des EUGH (s. UPC Telekabel im Rahmen unseres Executive Summary). Speziell ist zu berücksichtigen, dass §8 TMG damit generell gerade keine Privilegierung für Ansprüche aus der Störerhaftung liefert, was in der politischen Diskussion gerne übersehen wird).

Im Rahmen der Störerhaftung werden die Rechtsgedanken der §§ 8 bis 10 TMG lediglich "wertend" bei der Bemessung der zumutbaren Prüf- und Überwachungspflichten herangezogen. Auch hier versucht der BGH eine entsprechende Austarierung der Rechtsinteressen der Beteiligten vorzunehmen, mit ähnlich inkohärentem Ergebnis.

Dass eine Ausnahme der Haftungsprivilegierung für Ansprüche auf Beseitigung und Unterlassung bestehen muss, entspricht auch den europarechtlichen Vorgaben in Art. 12 Abs. 3 EC-RL, Art. 8 Abs. 3 der sogenannten Information Society Richtlinie (Hiernach: InfoSoc) (der jedenfalls für gewerbliche Anbieter im Wege einer Vollharmonisierung anzuwenden ist).

Diese Ausnahme vom Haftungsprivileg ist zum Schutz der berechtigten Interessen Dritter auch zwingend, da in vielen Fällen nur der Accessprovider eine Rechtsverletzung abstellen bzw. verhindern kann.

(Stellungnahme Mindbase, Landtag Hessen Seite 6)

Wichtig: Soweit der neue TMG-Entwurf der Bundesregierung in § 8 Abs. 4 TMG-E nunmehr offenbar (systemwidrig) auch ein Haftungsprivileg für Unterlassungsansprüche normieren will, widerspricht dies nicht nur der gegenteiligen Regelung des § 7 Abs. 2 S. 2 TMG sondern v.a. auch den Vorgaben des Art. 12 Abs. 3 EC-RL.

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

Access-Provider sind aufgrund der europarechtlichen Vorgaben grundsätzlich verpflichtet, Rechtsverletzungen zu beseitigen und zu verhindern (insb. Art. 12 Abs. 3 EC-RL, Erwägungsgrund 45 EC-RL; Art. 8 Abs. 3 InfoSoc, Erwägungsgrund 59 InfoSoc, Art. 11 Enforcement-RL).

In welchem konkreten Umfang Access-Provider als Störer Maßnahmen zu ergreifen haben, um Rechtsverletzungen zu verhindern, ist u.a. Gegenstand zweier aktueller BGH-Verfahren (Goldesel und 3dl.am). Dort geht es um die (ultima ratio-)Verpflichtung **zur Sperrung bestimmter Webseiten durch den Accessprovider**.

Auf europäischer Ebene hat der **EuGH** im Verfahren UPC Telekabel (kino.to) entschieden, dass Access-Provider jedenfalls grundsätzlich zur Sperrung von Webseiten wie kino.to verpflichtet werden können. Die Sperrung ist aber nicht (zwingend) Unterlassung im Sinne eines Unterlassungsanspruchs nach dem deutschen Recht.

An weitergehenden Pflichten lässt sich die BGH-Entscheidung (Sommer unseres Lebens) und die Instanzrechtsprechung dahingehend verstehen, dass ein (öffentliches) WLAN wohl zumindest **gegen unberechtigte Zugriffe von Dritten abgesichert** sein muss (z.B. WPA2-Verschlüsselung) und die **Nutzer vom WLAN-Betreiber belehrt** sein müssen, dass sie keine Rechtsverletzungen begehen. Diese Rechtsprechung zur Störerhaftung wurde von der Bundesregierung in § 8 Abs. 4 TMG-Entwurf aufgegriffen und soll dort nun im Rahmen der TMB-Novelle kodifiziert werden.

Jedenfalls für im gewerblichen Ausmaß agierende Diensteanbieter besteht gemäß § 101 UrhG, § 19 MarkenG etc. eine **Pflicht auf Auskunft über Nutzer**, die den Dienst in rechtsverletzender Weise genutzt haben. Diese Pflicht könnte je nach Angebotsumfang auch private und öffentliche Anbieter treffen, da es nicht auf die Gewerblichkeit, sondern nur auf das "gewerbliche Ausmaß" der Diensteerbringung ankommt. Da eine ausdrückliche Pflicht zur Speicherung der für eine Auskunftserteilung notwendigen Daten jedoch nicht besteht, wird der Auskunftsanspruch bei Hot Spot-Betreibern wohl weitgehend ins Leere laufen, soweit diese nicht von der DTAG, KDG etc. betrieben werden (freiwillige Speicherung nach § 100 TKG).

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

Die Frage unterstellt, dass bestimmte WLAN-Betreiber nicht in den Anwendungsbereich des TMG und dessen Privilegierungen fallen. Ob WLAN-Betreiber in das TMG fallen oder nicht, ist für die relevanten Haftungsrisiken jedoch weitgehend unerheblich:

Für die bloße Zugangsvermittlung zu fremden Informationen können auch große Access-Provider (wie z.B. die Deutsche Telekom) grundsätzlich auf Beseitigung und Verhinderung von Rechtsverletzungen (Unterlassung) im Rahmen des Zumutbaren haften (Störerhaftung, die von § 8 TMG generell nicht privilegiert wird).

(Stellungnahme Mindbase, Landtag Hessen Seite 7)

Ebenso würde ein großer Access-Provider haften, wenn er die rechtsverletzende Handlung selbst begeht (z.B. Telekom verschickt Spam-Mails) oder mit dem Rechtsverletzer kollusiv zusammenwirkt.

Wer eine Rechtsverletzung selbst begeht, fällt auch nach dem TMG generell nicht unter die Privilegierung. Und wer selbst keinen Haftungstatbestand (z.B. § 97 UrhG, § 823 BGB) erfüllt, der braucht generell keine Privilegierung nach dem TMG, da er ohnehin nicht haftet.

Gerade bei (kleineren/privaten) WLAN-Betreiben sollte jedoch nicht übersehen werden, dass diese möglicherweise auch selbst Rechtsverletzungen über ihr WLAN begehen. Die Behauptung, es handle sich um einen anonymen Nutzer im sog. "Hotspot", kann insofern die o.g. Haftungskriterien wieder nivellieren.

Diese Haftung für eigene Informationen etc. kann naturgemäß keiner Haftungsprivilegierung unterliegen (vgl. insofern auch § 7 Abs. 1 TMG).

e) Welche Haftungsprivilegierungen sind de lege ferenda denkbar?

Im Grundsatz könnten sich die Haftungsprivilegien nur im Rahmen der Art. 12 bis 15 ECRL bewegen, da insofern das Gebot der Vollharmonisierung gilt. Der deutsche Gesetzgeber kann die Provider daher weder stärker noch schwächer privilegieren.

Eine Ausnahme wäre aber wohl bei nichtkommerziellen und öffentlichen Anbietern denkbar, da diese in der ECRL nicht geregelt sind. Darüber hinaus sind bei einer Haftungsprivilegierung immer auch die übrigen verfassungs- und europarechtlichen Vorgaben (InfoSoc, EnforcementRL) zu berücksichtigen und die betroffenen Rechte Dritter (Eigentums-, Persönlichkeitsrechte etc.) dürfen nicht gänzlich schutzlos gestellt werden.

Im Falle einer möglichen Öffnung der EC-RL ist es *de lege ferenda* sinnvoll im Rahmen eines stringenten Haftungskonzeptes die Haftungsprivilegierung für W-Lan Betreiber, wie auch für Access- und Hostingprovider generell an eine Pseudonymisierung/Authentifizierung des Nutzers im entsprechenden Dienst durch die verschiedenen Provider knüpfen. Im Rahmen eines Log-Ins in ein offenes WLANs könnte der Betreiber dann von der Haftung freigestellt werden, wenn er die Identität des Nutzers anhand von Mobiltelefonnummer, Klarnamen, Bankverbindung, etc. verifiziert. Es gibt jetzt bereits diverse hinreichende Verifizierungsdienstleister (PayPal, KlarNa, Microsoft.net Passport. Post-Identverfahren, etc.), bzw. ganze Businesspakete, die einem WLAN-Betreiber die Zertifizierung abnehmen.

Eine entsprechende Verifizierung des Nutzers auf Plattformen und innerhalb offener WLANs wirkt nicht nur Rechtsverletzungen selbstregulativ entgegen, sie wäre auch für alle Parteien verhältnismäßig einfach handhabbar.

(Stellungnahme Mindbase, Landtag Hessen Seite 8)

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

Eine Privilegierung hat nur dort ihre Berechtigung, wo der Privilegierte auch seinen gesellschaftspolitischen Pflichten nachkommt. Dies ist gegenwärtig nur bei denjenigen Accessprovidern der Fall, die ihre Informations-, Überwachungs-, Datensicherheits-, Auskunfts-, Meldepflichten etc. erfüllen (z.B. aus den §§ 109ff TKG).

Der (nichtkommerzielle) private Betreiber eines WLAN erfüllt die für "geschäftsmäßig" erbrachte Telekommunikationsdienstleistungen geltenden Pflichten momentan nicht. Für eine Privilegierung sollte daher auch ein nichtkommerzieller Anbieter offener W-LANS daher zumindest einem vergleichbaren Pflichtenkatalog unterworfen werden, wie z.B. ein Internet Service Provider. Dies ist auch aufgrund der in 1.g gemachten Sicherheitserwägungen sinnvoll (siehe 1.(g)).

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

Je nach Austarierung des Haftungsregimes beim Betrieb offener (anonymer) WLAN-Hotspots besteht die Gefahr, dass Rechtsverletzer gezielt diese Hotspots aufsuchen, da das Risiko identifiziert zu werden, minimiert ist. Es entstünde die theoretische Situation, dass Rechtsverletzer zwar zuhause von einer Nutzung des Internets möglicherweise Abstand nehmen würden (insbesondere im Hinblick auf eine anstehende Vorratsdatenspeicherung), diese aber aufgrund der möglichen Anonymisierung gerade in öffentlichen W-Lans präferiert ausüben. Momentan ist nicht vorgesehen, dass freie W-Lans der Vorratsdatenspeicherung unterworfen werden, hier bestünde also eine Regulierungslücke, die freie WLANs ggf. zum bevorzugten Einfallort für cyberkriminelle Aktivitäten durch Benutzer innerhalb des Netzwerkes machen würden, da eine Rechtsverletzung maximal bis zum Betreiber des WLANs zurückverfolgt werden kann.

Auch hier geht es darum, einen Haftungsrahmen zu schaffen, der die Ansprüche Geschädigter nicht ins Leere laufen lässt, analog zur Entscheidung UPC-Telekabel des EuGH.

Neben der Frage, inwiefern unregistrierte Nutzer in W-Lans Sicherheitsprobleme verursachen können, eröffnen freie W-Lans noch weitere Sicherheitsprobleme:

Öffentliche Hotspots bieten vielerlei Möglichkeit Daten abzugreifen, sofern sie nicht verschlüsselt werden. Ein krimineller Betreiber eines W-Lans hat die Möglichkeit aus einem kompromittierten und fingierten W-Lan („Telekom Alexanderplatz“, „Freifunk Frankfurt“, „Landtag Hessen, Besucher“) vielerlei unverschlüsselte Daten & Passwörter abzugreifen. Aus cyberkrimineller Sicht ist das Betreiben eines öffentlichen W-Lans eine ideale Eingriffsstelle. Jeder unverschlüsselte Datenverkehr über den Hotspot ist insbesondere für den Betreiber abgreifbar. Ebenfalls gibt es Möglichkeiten für den Betreiber die Kontrolle über den Computer zu erlangen, zum Beispiel über das Installieren gefälschter Windows-Updates, oder das Abfangen von Passwörtern durch das Unterschieben anderer gefälschter Webseiten.

Das Betreiben eines solchen fingierten W-Lans und gerade das Abfangen von Datenströmen (inkl. Passwörter, und weitere sensible Daten, etc.) ist somit verhältnismäßig einfach, und stellt kaum ein Problem für Kriminelle mit versierten IT-Kenntnissen dar. Eine VPN-Verschlüsselung kann dazu beitragen dieses Sicherheitsrisiko deutlich zu minimieren.

(Stellungnahme Mindbase, Landtag Hessen Seite 9)

Bei einer steigenden Popularität von freien W-Lans in Hessen ist es absehbar, dass dieses Einfallstor zunehmend von Cyberkriminellen eingesetzt werden wird. Dieser Sicherheitslücke könnte man mit einer Authentifizierung des W-Lans beim Provider oder durch eine zentrale Registrierungsstelle für zertifizierte W-Lans entgegenwirken, so dass nur noch vertrauenswürdige W-Lans beim Rechner der Nutzer als solche zertifiziert würden. Auch hier ist eine Ungleichstellung kommerzieller und nichtkommerzieller Betreiber von Öffentlichen WLAN-Spots nicht zielführend.

Abschließend möchten wir hinzufügen, dass es trotz eines gewissen öffentlichen Drucks nicht Aufgabe des Gesetzgebers sein kann, Sicherheitsrisiken durch unterregulierte WLAN aktiv zu fördern, solange das Haftungsregime dermaßen lückenhaft ist. Der Gesetzgeber bemüht sich seit Jahren den Nutzer für die Gefahren und die Risiken von Onlinekriminalität zu sensibilisieren, gleichzeitig fördern wir unkritisch Strukturen, die neue Sicherheitsrisiken darstellen.

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

Dem Betreiber des WLAN kann nach momentaner Rechtslage aufgrund des bloßen Betriebs des WLANs kein hinreichend konkreter Vorsatz für eine Beihilfe oder Mittäterschaft unterstellt bzw. vorgeworfen werden. Jedoch könnten hier entsprechende Registrierungs- und Zertifizierungspflichten für den Betrieb eines OFFENEN Hotspots eingezogen werden.

2. Datensicherheit und Datenschutz

Keine Angaben.

3. Internationaler Vergleich

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

Ein abschließender internationaler Rechtsvergleich würde den Rahmen dieser Stellungnahme sprengen, und wäre selbst für ein rechtswissenschaftliches Institut eine nicht zu unterschätzende Herausforderung. Wir versuchen aber zumindest die uns bekannten Sachverhalte zusammen zu tragen.

Soweit ersichtlich wurden die Art. 12 ff. der ECRL in sämtlichen Mitgliedstaaten umgesetzt. In der überwiegenden Zahl der Mitgliedstaaten sind entsprechend Art. 8 Abs. 3 InfoSoc **richterliche Beseitigungs-und Unterlassungsanordnungen gegenüber Internetzugangsdiensten** anerkannt und werden vielfach praktiziert. Die **Kosten** des Rechtsstreits werden nach dem jeweiligen mitgliedstaatlichen Recht **in aller Regel dem unterliegenden Internetzugangsdienst auferlegt. Auch hier ist dioe rechtsfortschreibung durch die Judikative weit gediehen:**

In **Belgien** hat das Berufungsgericht Antwerpen eine zivilrechtliche Unterlassungsanordnung für rechtmäßig erachtet, die zwei Access-Provider zur Sperrung des Zugangs zur Internetseite *„The Pirate Bay“* verpflichtet hatte. Die Kosten des Rechtsstreits wurden den Providern auferlegt.(Hof van Beroep Antwerpen, 26.09.2011, 2010/AR/2541). Der Oberste Gerichtshof Belgiens hat zudem eine strafrechtliche Unterlassungsanordnung gegenüber weiteren Access-Providern bestätigt, die diese zur

(Stellungnahme Mindbase, Landtag Hessen Seite 10)

Sperrung des Zugangs zur Internetseite *„The Pirate Bay“* und zur Überwachung zukünftiger Domainnamen verpflichtet hatte. Die Kosten wurden den Providern auferlegt. (Hof van Cassatie van België, 22.10.2013, P.13.0550.N/1)

In **Dänemark** hat der Oberste Gerichtshof eine gerichtliche Anordnung für zulässig erachtet, die einen Access-Provider verpflichtet, es zu unterlassen, urheberrechtlich geschützte Inhalte von FTP-Servern zu übertragen, die von Kunden des Providers betrieben wurden. Der Provider könne dieser Anordnung ohne weiteres nachkommen, indem die Internetverbindung zu den konkreten FTP-Servern oder allgemein zu den dahinter stehenden Kunden getrennt wird (Højesteret, 10.02.2006, 59/2005 (UfR 2006.1474 H). Der Oberste Gerichtshof hat zudem eine Unterlassungsanordnung bestätigt, die einen Access-Provider verpflichtet, nicht an Urheberrechtsverletzungen der Internetseite *„The Pirate Bay“* mitzuwirken und Maßnahmen zu ergreifen, die einen Zugriff seiner Kunden hierauf verhindern. (Højesteret, 27.05.2010, 153/2009 (UfR 2010.2221 H).

In **Finnland** hat das Bezirksgericht Helsinki verschiedene Unterlassungsanordnungen in Bezug auf Internetanschlüsse von Privatpersonen erlassen, über die urheberrechtlich geschützte Inhalte öffentlich zugänglich gemacht wurden. Das Gericht hat hervorgehoben, dass auch die Trennung der Internetverbindung keine unverhältnismäßige Maßnahme darstelle. Auch das Berufungsgericht Helsinki hat Sperrverfügungen gegenüber verschiedenen Access-Providern bestätigt. (Helsingin käräjäoikeus, 23.06.2008, 18661 (H 08/3008); 09.05.2011, 172228 (H 11/11018). 36 Hlesingin hovioikeus, 15.06.2012, S 11/3097; 11.02.2013, S 12/2223; 08.02.2013, S 12/1850)

In den **Niederlanden** hat das Bezirksgericht Den Haag mehrere Access-Provider zur Sperrung des Zugangs zur Internetseite *„The Pirate Bay“* verpflichtet und den Access-Providern die Gerichts- und Rechtsanwaltskosten auferlegt.37 Zwar wurde diese Anordnung später durch das Berufungsgericht Den Haag aufgehoben, weil die Maßnahme im konkreten Fall nicht effektiv genug, insbesondere nur gegen *„The Pirate Bay“* und nicht auch weitere pirateriefördernde Internetseiten gerichtet war. Das Gericht hat jedoch die grundsätzliche Möglichkeit gerichtlicher Anordnungen zur Beendigung oder Verhinderung von Rechtsverletzungen auch gegenüber privilegierten Access-Providern unterstrichen.38

(37 Rechtbank 's-Gravenhage, 11.01.2012, 374634/HA ZA 38 Gerechtshof Den Haag, 28.01.2014, 374634/HA ZA 10-3184, Fn. 5.3 und insbesondere 6.2)

In **Spanien** hat das Berufungsgericht Barcelona einen Access-Provider verpflichtet, die Internetverbindung eines Nutzers zu trennen, der illegales Filesharing betrieben hatte.39 Auch in **Irland** ist die Möglichkeit richterlicher Unterlassungsanordnungen gegenüber Access-Providern anerkannt.40 In **Österreich** hat der Oberste Gerichtshof nach der Entscheidung des Gerichtshofs in der Rechtssache UPC Telekabel die Zulässigkeit einer entsprechenden Unterlassungsanordnung gegenüber einem Access-Provider ebenfalls bestätigt.41

(39 Audiencia Provincial de Barcelona, 18.12.2013, 470/2013 40 Irish High Court of Justice, 27.07.2009, [2009] IEHC 411; 16.04.2010, [2010] IEHC 108; 12.06.2013, [2013] IEHC 274 41 Oberster Gerichtshof, 24.06.2014, 4 Ob 71/14s nach EuGH, 27.03.2014, Rs. C-314/12)

Auch im **Vereinigten Königreich** von Großbritannien und Nordirland erlässt das oberste erstinstanzliche Zivilgericht regelmäßig Unterlassungsanordnungen gegenüber Access-Providern.42 Die Kosten der Anordnungen werden hier nach dem nationalen Recht zwar grundsätzlich dem Rechteinhaber auferlegt. Soweit sich der Provider jedoch widersetzt, können diesem die Kosten auferlegt werden.

(42 High Court of Justice, 28.07.2011, [2011] EWHC 1981 (Ch), 26.10.2011, [2011] EWHC 2714 (Ch), 20.02.2012, [2012] EWHC 268 (Ch), 02.05.2012, [2012] EWHC 1152 (Ch), 28.02.2013, [2013] EWHC 379 (Ch), 16.07.2013, [2013] EWHC 2058 (Ch), 13.11.2013, [2013] EWHC 3479 (Ch), 13.11.2013, [2014] EWHC 937 (Ch))

(Stellungnahme Mindbase, Landtag Hessen Seite 11)

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

Nach wie vor besteht die diffizile Aufgabe des Gesetzgebers darin, die Interessen der Beteiligten unter einen Hut zu bekommen. Hierbei hat das höchste Europäische Gericht explizit auf die Berücksichtigung der Rechtsgüter Dritter hingewiesen.

Eine weitgehende „Enthaftung“ von W-Lan-Betreibern ist somit nach vielerlei Gesichtspunkten europarechtswidrig. Sinnvoller ist es daher auf einen stringenten Haftungsrahmen hinzuarbeiten, auf den das Betreiben eines offenen WLAN-Hotspots sinnvoll aufsetzen kann. Momentan ist dies nicht gegeben, Rechtsunsicherheiten für WLAN-Betreiber sind absehbar.

4. Ausbau

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

Der Massenbetrieb freier WLANs hat – im Falle einer umfassenden Liberalisierung - möglicherweise entsprechende Auswirkungen auf die Geschwindigkeit und die Notwendigkeit des Ausbaus von Breitbandverbindungen. Hier weisen wir darauf hin, dass die Europäische Kommission sich momentan darauf verständigt hat, Roaminggebühren für mobile Telefon- und Internetanschlüsse sukzessive erst zu harmonisieren, und danach möglicherweise komplett entfallen zu lassen. Das benutzen von mobilen Internetanschlüssen durch Mobiltelefone, Laptops oder Tablets dürfte insofern in absehbarer Zeit für den EU-Bürger kostengünstiger werden. Eine flächendeckende Förderung von W-Lans könnte somit hinsichtlich des privatwirtschaftlichen Breitbandausbaus, oder auch des Ausbaus von Mobiltelefonnetzen wettbewerbsverzerrend wirken, und einem flächendeckenden Ausbau entgegenwirken.

Ebenfalls ist die weitere technische Entwicklung von Mobilfunkstandards über den aktuellen LTE-Standard hinaus bereits absehbar (sog. 5g),. Es ist geplant, dass 5g Mobiltelefonverbindungen in der Zukunft ggf. sogar schneller sein könnten als private Breitbandverbindungen. Auch hier träten – im Falle einer umfassenden Förderung freier WLANs die Hotspots in Wettbewerb mit Mobiltelefonanbindungen. Dieser Wettbewerb könnte durch entsprechende öffentliche Förderungen verzerrt werden.

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

Keine Angabe.

(Stellungnahme Mindbase, Landtag Hessen Seite 12)

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

Wer seinen Kunden einen Hotspot anbieten möchte, kann auch auf Hotspot-Komplettlösungen der klassischen Access-Provider zurückgreifen. Hierbei stellt der Access-Provider neben dem Internetanschluss entsprechende Hardware für die Bereitstellung eines Hotspots zur Verfügung. Der Access-Provider übernimmt dabei die Registrierung der Nutzer sowie weitere erforderliche Sicherungsmaßnahmen. Die für den Betreiber des Hotspots anfallenden Kosten liegen in der Regel bei unter 50 Euro im Monat. Exemplarische Angebote: Kabel Deutschland WLAN-Hotspot für Unternehmen (http://www.kabeldeutschland.de/wlan-hotspots/hotspot-fuer-ihr-business.html);

Telekom Hotspot Partnerprogramm (http://www.hotspot.de/content/partner.html); BSkyB The Cloud(http://www.thecloud.eu/).

Auch eigene Lösungen mittels Registrierung und Speicherung von NAT-Tabellen sind möglich. Um eine Rechtsverletzung einem registrierten Nutzer zuordnen zu können, muss dabei auch nicht der gesamte Netzwerkverkehr überwacht oder gespeichert werden. Der Betreiber des WLAN muss lediglich die externen IP-Adressen und Ports speichern, mit denen ein registrierter Nutzer Verbindungen ins Internet aufgebaut hat. Die erforderlichen Informationen sind bei WLAN-Routern in der sog. NAT-Tabelle94 hinterlegt. Die Identifizierung eines WLAN-Nutzers entspricht dabei im Wesentlichen der Zuordnung von IP-Adressen durch einen Access-Provider. Entsprechende Systeme, die WLAN-Betreibern die Registrierung und Identifizierung ihrer Nutzer ermöglichen, sind bereits für wenige hundert Euro erhältlich. Exemplarische Angebote: Envel WLAN-BS (http://www.envel.com/Produkte/WLAN-BS/Envel-WLAN-Hotspot); Contelio Hotspot (http://www.wlanticket.de/die-professionelle-hotspot-wlanloesung.html); ZYXel Basic (http://www.zyxel-hotel.de/hotellerie/loesungen/basic.html)

Einige Beispiel für öffentliche WLANs mit Registrierungen:

- Berlin „Berlin wireless“ von The Cloud (über 260x in Berlin)
- London „The Cloud’s City WiFi network“
- Paris „Paris Wi-Fi“
- Mailand: „Open Wi-Fi Milano“
- Rom „romawireless“
- Warschau „UMWarszawa“
- Flughafen Frankfurt „Telekom HotSpot“ (bundesweit 50.000)
- Flughafen Zürich „Monzoon“
- Flughafen Madrid-Barajas „KubiWireless“
- Flughafen Barcelona-El Prat „KubiWireless“
- Flughafen Palma de Mallorca „KubiWireless“

(Stellungnahme Mindbase, Landtag Hessen Seite 13)

- Flughafen Brüssel „Brussels Airport Wi-Fi“
- Flughafen London „Heathrow Wi-Fi“
- Schweizer Bahnhöfe „SBB WiFi“
- Italienische Hochgeschwindigkeitszüge „Wi-Fi Frecciarossa/Frecciargento“
- Lissabonner Metro „ON-FI“
- Polnische Busse „ZTM Warszawa“
- Straßenbahnen Antwerpen und Gent „WiFi De Lijn“

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

Keine Angabe

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

Keine Angabe

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?

Keine Angabe

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

Keine Angabe

5. Wirtschaftliche Bedeutung und Effekte:

Keine Angabe

6. Förderprojekte im Bundesvergleich:

Keine Angabe

Eisert, Martina (HLT)

Betreff: WG: Öffentliche mündliche Anhörung des Auschusses für Wirtschaft, Energie, Verkehr und Landesentwicklung "Freie WLAN-Hotspots in Hessen" am 12.11.2015

Wichtigkeit: Hoch

Von: Attermeyer, Kordula [mailto:Kordula.Attermeyer@stk.nrw.de]
Gesendet: Dienstag, 10. November 2015 13:51
An: Lingelbach, Claudia (HLT)
Betreff: Öffentliche mündliche Anhörung des Auschusses für Wirtschaft, Energie, Verkehr und Landesentwicklung "Freie WLAN-Hotspots in Hessen" am 12.11.2015
Wichtigkeit: Hoch

Sehr geehrte Damen und Herren,
sehr geehrte Frau Lingelbach,

ich bedanke mich herzlich für die Einladung zur Öffentlichen Anhörung des Ausschusses für Wirtschaft, Energie, Verkehr und Landesentwicklung am 12.11.2015 zum Thema "Freie WLAN-Hotspots in Hessen" .

In Umsetzung des Antrages der Fraktion der SPD, der Fraktion BÜNDNIS 90/DIE GRÜNEN sowie der Fraktion der PIRATEN (Landtag Nordrhein-Westfalen DrS 16/8970 " Freifunk in Nordrhein-Westfalen: Bürgernetze ausbauen und weiter stärken!") sind wir damit gestartet, die Kooperationen mit den sehr engagierten Freifunk-Initiativen im Land auszubauen.

Auch vor diesem Hintergrund hat Nordrhein-Westfalen sich soeben mit Anträgen im Bundesrat in die zukünftige Gesetzgebung zur sog. Störerhaftung im Telemediengesetz eingebracht, die am 6.11.2015 im Bundesrat angenommen wurden.

In Umsetzung der Regierungserklärung von Frau Ministerpräsidentin Hannelore Kraft vom 29.01.2015 sind aber auch in Nordrhein-Westfalen die Möglichkeiten von öffentlichen WLAN ein wichtiges Thema. Überlegungen dazu sind aber noch nicht abgeschlossen.

Ich bedauere es daher sehr, dass ich wegen einer Terminverpflichtung an der Anhörung leider nicht werde teilnehmen können.

Ich wünsche Ihnen einen guten Austausch sowie viele hilfreiche und anregende Erkenntnisse aus dem vielfältigen Kreis von eingeladenen Expertinnen und Experten.

Mit freundlichen Grüßen
Im Auftrag

Kordula Attermeyer

Kordula Attermeyer
Referat IV C 4 Digitale Gesellschaft, Medienkompetenz
Referatsleitung

Staatskanzlei des Landes Nordrhein-Westfalen
Der Minister für Bundesangelegenheiten, Europa und Medien
und Chef der Staatskanzlei Nordrhein-Westfalen

Postanschrift 40190 Düsseldorf
Fürstenwall 25, 40219 Düsseldorf
Telefon +49 (0) 211 837 1257
Telefax +49 (0) 211 837 187 1257

E-Mail kordula.attermeyer@stk.nrw.de
Internet www.mbem.nrw
Twitter: http://twitter.com/DGNRW

Hessischer Städtetag
Verband der kreisfreien und kreisangehöriger Städte in Hessen

Hessischer Städtetag · Frankfurter Straße 2 · 65189 Wiesbaden

Hessischer Landtag
Der Vorsitzende des Ausschusses für Wirtschaft,
Energie, Verkehr und Landesentwicklung
Postfach 32 40

65022 Wiesbaden

Ihre Nachricht vom: 06.10.2015
Ihr Zeichen: I A 2.9

Unser Zeichen: TA 612.6 Sl/Ve
Durchwahl: (0611) 1702-32
E-Mail: schlukat@hess-staedtetag.de

Datum: 10.11.2015
Stellungnahme: 116-2015

Freie WLAN-Hotspots in Hessen - Mündliche Anhörung des Ausschusses für Wirtschaft, Energie, Verkehr und Landesentwicklung

Sehr geehrter Herr Abgeordneter Reif,
sehr geehrte Damen und Herren Abgeordnete,

wir nehmen Bezug auf das Schreiben vom 14. September 2015. Wir bedanken uns für die Gelegenheit zur Stellungnahme zum betreffenden Thema.

Unsere Umfrage unter den Mitgliedstädten hat ergeben, dass die Mehrheit die Errichtung von frei zugänglichen WLAN-Netzen als einen sinnvollen, nützlichen und wirksamen Beitrag sowohl in touristischer Hinsicht als auch mit Blick auf das Standort- und Citymarketing in den Städten bewertet. Überdies erwarten sie durch die Errichtung von WLAN-Netzen positive Auswirkungen auf die Wirtschaftsförderung, beispielsweise durch eine höhere Frequentierung der Innenstädte.

Dementsprechend bestehen vielerorts bereits konkrete Überlegungen, freizugängliche WLAN-Netze in den Städten anzubieten oder schon errichtete WLAN-Netze in den Innenstädten, wenngleich die einzelnen Umsetzungswege sehr unterschiedlich sind. In diesem Zusammenhang ist darauf hinzuweisen, dass die Errichtung von frei zugänglichen WLAN-Netzen in den Innenstädten keine kommunale Pflichtaufgabe darstellt. Eine Förderung würde die Möglichkeit eröffnen, eine solche Leistung anzubieten, die sonst aufgrund fehlender Mittel nicht zur Umsetzung gelangen würde.

Der Ausschuss für Wirtschaft, Verkehr und Energie des Hessischen Städtetages hat sich Anfang November mit dem Thema „WLAN-Hotspots in Hessen“ befasst und darin die Bedeutung öffentlicher drahtloser lokaler Netzwerke als wichtigen Beitrag in wirtschaftlicher und touristischer Sicht für eine Stadt betont. Da die Einrichtung von WLAN-Hotspots auch für die wirtschaftliche, touristische und gesellschaftliche Entwicklung des Landes Hessen von Bedeutung ist, sei aus Sicht des Ausschusses auch das Land gefordert, den Ausbau öffentlicher drahtloser lokaler Netzwerke zu unterstützen und auch finanziell zu fördern.

Für Rückfragen stehen wir Ihnen gerne zur Verfügung.

Mit freundlichen Grüßen

Dr. Jürgen Dieter
Direktor

Hessischer Landkreistag

Hessischer Landkreistag · Frankfurter Str. 2 · 65189 Wiesbaden

Hessischer Landtag
Ausschuss für Wirtschaft,
Verkehr und Landesentwicklung
Frau Ausschussgeschäftsführerin
Claudia Lingelbach
Schlossplatz 1-3
65183 Wiesbaden

Frankfurter Str. 2
65189 Wiesbaden

Telefon (0611) 17 06 - 0
Durchwahl (0611) 17 06- 15

Telefax-Zentrale (0611) 17 06- 27
PC-Fax-Zentrale (0611) 900 297-70
PC-Fax-direkt (0611) 900 297-99

e-mail-Zentrale: info@hlt.de
e-mail-direkt: wobbe@hlt.de
www.HLT.de

Datum: 09.11.2015
Az. : Wo/re 048.06

Landtagsanhörung Freie WLAN-Hotspots
Ihr Schreiben v. 14.09.2015, Az. I A 2.2
Stellungnahme des Hessischen Landkreistages

Sehr geehrter Herr Ausschussvorsitzender,
sehr geehrte Damen und Herren Abgeordnete,
sehr geehrte Frau Lingelbach,

wir bedanken uns für Ihr o.g. Schreiben, mit dem Sie uns Gelegenheit gegeben haben, im Rahmen der Anhörung des Ausschusses für Wirtschaft, Verkehr und Landesentwicklung zum Thema „Freie WLAN-Hotspots in Hessen“ eine Stellungnahme abzugeben.

Auf Grundlage einer Befragung seiner Mitglieder sowie einer Beratung der Verbandsgremien erklärt sich der Hessische Landkreistag hierzu wie folgt:

Hintergrund des Konzeptes der Fraktionen ist, dass im Ausbau von öffentlichen drahtlosen lokalen Netzwerken (WLAN-Hotspots) „ein wichtiger Beitrag für die wirtschaftliche und touristische, aber auch gesellschaftliche Entwicklung Hessens“ gesehen wird.

Im Rahmen der Landtagsanhörung sollen eine Vielzahl von rechtlichen und tatsächlichen Fragen geklärt werden, die mit dem Aufbau von WLAN-Hotspots im Zusammenhang stehen. Hierzu wurde ein umfangreicher Fragenkatalog mit der Bitte um Rückmeldung vorgelegt. Hierzu wurde durch unsere Mitglieder darauf hingewiesen, dass eine solche Beantwortung in weiten Teilen nur durch Spezialisten verschiedener Fachdisziplinen möglich erscheint, die auf der kommunalen Ebene derzeit nicht vorhanden sind. Auch unsere Mitgliedskreise bedienen sich, sofern beispielsweise solche Netzwerke in Landratsämtern oder Teilen derselben eingerichtet wurden, externen Sachverstandes.

Im Rahmen unserer politischen Gremienberatung zeigte sich weiter, dass angesichts der Problematik der Datensicherheit (z. B. mögliche Hackerangriffe) sowie der damit einhergehenden Haftungsproblematik seitens der Hessischen Landkreise gegenwärtig nur ein sehr geringes Interesse an einem eigenständigen kommunalen Betrieb von freien WLAN-Hotspots in größerem Umfang besteht.

In manchen kreiseigenen Einrichtungen, z.B. den Zulassungsstellen wird zwar derzeit die Möglichkeit eines WLAN-Zugangs für Besucher geboten. Die Access-Points werden jedoch aus vorgenannten Gründen regelhaft von Drittanbietern betrieben.

Dass die Einrichtung solcher Netzwerke, vor allem im ländlichen Raum, einen nennenswerten eigenständigen Nutzen, insbesondere für die wirtschaftliche und touristische Entwicklung unter Berücksichtigung der damit zusammenhängenden Unsicherheiten und auch Kosten hat, erscheint aus der Sicht der Landkreise aus derzeitiger Sicht eher nicht der Fall zu sein.

Im Rahmen der mündlichen Anhörung könnten keine Aspekte vorgetragen werden, die über die vorgenannte Einschätzung hinausgehen. Wir bitten daher um Verständnis, wenn wir auf eine Teilnahme an der mündlichen Anhörung verzichten.

Wir bitten um Kenntnisnahme.

Mit freundlichen Grüßen

Matthias Drexelius
Direktor

mabb medienanstalt_berlin_brandenburg

Steffen Meyer-Tippach
Telefon_030 264 967 47
E-mail_meyer@mabb.de

Berlin, 11. November 2015

Stellungnahme zum Thema „Freie WLAN-Hotspots in Hessen“ im Ausschuss für Wirtschaft, Energie, Verkehr und Landesentwicklung des Hessischen Landtags

Sehr geehrte Damen und Herren,

die Medienanstalt Berlin-Brandenburg (mabb) begrüßt den Antrag der SPD-Fraktion des Hessischen Landtags vom 28.04.2015 und möchte hiermit von der Möglichkeit der Stellungnahme Gebrauch machen. Die mabb befürwortet ausdrücklich das Vorhaben des Landtags,den Zugang zu öffentlichen drahtlosen lokalen Netzwerken in Hessen zu unterstützen und zu fördern. Ebenso begrüßen wir das Engagement, sich auf Bundesebene für weitere Verbesserungen bei der Novellierung des Telemediengesetzes einzusetzen und auf eine Überarbeitung der bisherigen Regelung der Störerhaftung hin zu wirken. Wir weisen in diesem Zusammenhang auf die Stellungnahme des Bundesrats vom 06.11.2015 hin, in der einige Änderungen am aktuellen Regierungsentwurf gefordert wurden.

WLAN – Eine technologische und ökonomische Erfolgsgeschichte

WLAN hat eine beeindruckende Erfolgsgeschichte hinter sich und ist heute ein weltweiter Übertragungs-Standard für die mobile Internetnutzung. Die große Nachfrage nach Smartphones und Tablets hat dazu geführt, dass WLAN in der alltäglichen Nutzung dieser Geräte nicht mehr wegzudenken ist. Wurden die WLAN-Frequenzen 2,4 und 5 GHz in der Vergangenheit noch als garbage bands, als Schrottfrequenzen bezeichnet, für die man außer für den Betrieb von Mikrowellen und Babyphones keine weiteren Anwendungen sah, sind sie heute ein wichtiger Baustein einer digitalen Gesellschaft und übersteigen das Verkehrsvolumen von Mobilfunknetzen um ein Vielfaches. WLAN- und Mobilfunk-Netze stehen sich aber nicht frontal gegenüber, sie sind vielmehr komplementär zueinander zu betrachten und nicht als Substitute. WLAN entlastet die Mobilfunknetze erheblich und hat einen enormen volkswirtschaftlichen Nutzen. So hat eine Studie der EU-Kommission zu Off-Loading von Datenverkehr ergeben, dass die annualisierten Kostenersparnisse bei den Mobilfunknetzbetreibern durch die Nutzung von WLAN-Netzen erstaunlich groß sind. So wurden die kumulierten Einsparungen der Netzkosten durch WLAN-Off-Loading für Deutschland im Jahr 2015 auf 84 Mrd. Euro berechnet. 2016 sollen die Einsparungen bei über 140 Mrd. Euro liegen. Neben den Einsparungen bei den Mobilfunknetzbetreibern ist der ökonomische Nutzen selbstverständlich auch im Einzelhandel, der Gastronomie und der Hotelbranche zu sehen. FREE WIFI ist in den letzten Jahren zu einem wichtigen Verkaufsargument geworden und wird verstärkt von den Kunden nachgefragt. Öffentliche WLAN-Netze steigern die Attraktivität von Innenstädten, sie ermöglichen Teilhabe und befriedigen das Informationsbedürfnis der Bevölkerung und von Touristen, vor allem dann, wenn das mobile Datenvolumen der Nutzer aufgebraucht oder das mobile Netz zu langsam oder instabil ist.

WLAN-Projekte der mabb

Die mabb setzt sich bereits seit mehreren Jahren für den Breitbandausbau ein und hat verschiedene WLAN-Projekte durchgeführt. Seit 2012 können in Berlin und Potsdam 100 von der mabb geförderte WLAN-Hotspots von Kabel Deutschland/Vodafone täglich für 30 Minuten kostenfrei genutzt werden. Erforderlich ist lediglich eine Bestätigung der Nutzungsbedingungen auf einer Landing-Page, kein Nutzer muss sich mit E-Mail-Adresse, Mobilnummer oder einem Passwort anmelden. Die Hotspots werden durchschnittlich 60.000 Mal im Monat genutzt. Dieses Public-Wifi-Netz nimmt hierbei mehrere Funktionen ein: Es schont das Datenvolumen, das den Nutzern über das mobile Internet zur Verfügung steht und ist als Zugang vor allem auch für Touristen interessant, die sich ansonsten mit Roaming-Gebühren konfrontiert sehen würden.

Darüber hinaus fördert die mabb seit 2013 auch die gemeinnützige Initiative der Freifunker bei der Errichtung eines BerlinBackBone, das auf Richtfunk basiert. Über 15.000 WLAN-Zugänge im öffentlichen Raum wurden in den letzten Jahren von den Freifunk-Communitys deutschlandweit aufgebaut. Allein in Berlin gibt es über 400 Zugänge.

Der Erfolg dieser beiden mabb-Projekte war in den letzten Jahren ein Anstoß für die Ausweitung öffentlicher WLAN-Zugänge in anderen Städten. In der mündlichen Anhörung am 12. November 2015 berichten wir gerne von unseren ganz praktischen Erfahrungen im Bereich öffentlicher WLAN-Netze und stellen gern die Genese unserer Projekte vor. Die wichtigsten Erkenntnise aus den letzten drei Jahren lassen sich wie folgt zusammenfassen.

Der einfache Zugang zu WLAN-Netzen muss gewährleistet sein

Öffentliche WLAN-Netze brauchen, um praktikabel und nutzerfreundlich zu sein, einen einfachen Zugang. Eine Verschlüsselung von öffentlichen WLAN-Netzen –wie es der Regierungsentwurf zur Änderung des Telemediengesetzes (TMG) vorsieht - darf nicht zu den Vorgaben für eine Haftungsbefreiung gehören. Eine Verschlüsselung ist mit bereits bestehenden und zukünftigen öffentlichen WLAN-Angeboten nicht vereinbar. Diese sind gerade deswegen so attraktiv und werden häufig genutzt, weil keine Registrierung und kein Passwort erforderlich ist. Die Rechtssprechung versteht unter „Verschlüsselung“ eines WLAN-Angebots die Zugangssicherung via Passwort. Diese Lösung steht einer Förderung von öffentlichen WLAN-Angeboten aber entgegen und erleichtert zudem auch nicht die Verfolgung von Urheberrechtsverletzungen. Der einzelne Nutzer ist durch die Eingabe eines WLAN-Passworts nicht identifizierbar.

Zudem besteht auch kein Anlass für diese Art der Zugangssicherung. Im Rahmen unseres Projekts mit Kabel Deutschland wurden die Public-Wifi-Hotspots nicht für Urheberrechtsverletzungen genutzt. Es gab bei Kabel Deutschland in dieser Zeit keine IP-Adressabfragen wegen Urheberrechtsverletzungen. Eine Verschlüsselung dient zudem auch nicht dem Interesse des WLAN-Betreibers oder Nutzers, da die Datensicherheit und die Wahrung des Kommunikationsgeheimnisses nicht durch ein verschlüsseltes WLAN-Netz mit öffentlichem oder geteiltem WLAN-Passwort sichergestellt werden kann. Ausschlaggebend für die IT-Sicherheit ist die Verschlüsselung seitens der Nutzer.

Die rechtliche Ungleichbehandlung von kommerziellen und nicht-kommerziellen Anbietern behindert den Ausbau öffentlicher WLAN-Netze

Die mabb kritisiert die rechtliche Diskriminierung von nichtgewerblichen und privaten WLAN-Anbietern. Diese Diskrimierung bremst den weiteren Ausbau von WLAN-Netzen in Deutschland drastisch aus und schiebt zudem das ehrenamtliche Engagement der vielen Freifunk-Communities in eine rechtliche Grauzone. Der Regierungsentwurf zur Änderung des TMG sieht vor, dass nur WLAN-Anbieter privilegiert werden, die anlässlich einer geschäftsmäßigen Tätigkeit oder als öffentliche Einrichtung ihr Internet zur Verfügung stellen. Nicht-kommerzielle Anbieter oder Privatpersonen die ihr WLAN aus altruistischen Motiven der Allgemeinheit zur Verfügung stellen, sollen hingegen einen Forderungskatalog erfüllen, der an der Realität vorbei geht und praktisch nicht umsetzbar ist. Diese Anbieter sollen:

1. das „öffentliche WLAN“ verschlüsseln
2. die Nutzer einwilligen lassen
3. die Nutzer beim Namen kennen

Dies ist ein herber Rückschlag für die Freifunk-Bewegung, die im Laufe der letzten Jahre digitale Infrastrukturen oft auch an Orten aufgebaut hat, wo das Interesse kommerzieller Anbieter zu gering war. So setzen sich aktuell viele Freifunk-Communities für WLAN-Zugänge in Flüchtlingsunterkünften ein. Der Regierungsentwurf würde vielleicht nicht das Ende eines wichtigen zivilgesellschaftlichen Engagements sein, nachhaltig geschwächt würde es allemal.

Öffentliche WLAN-Netze sind keine Basis eines kommerziellen Geschäftsmodells

Auf Grundlage unserer Erfahrungen aus dem WLAN-Projekt mit Kabel Deutschland/Vodafone schätzen wir den Erfolg eines Geschäftsmodells, das allein auf WLAN-Hotspots im öffentlichen Raum beruht, als äußerst gering ein. Anhand der Nutzungsdaten des Projekts wurde ersichtlich: Über 90 Prozent der WLAN-Nutzer von PUBLIC WIFI wählten den kostenfreien Zugang und nutzen auch nur die vorgesehene Zeit von maximal 30 Minuten, die durchschnittliche Nutzungsdauer lag bei 15 Minuten. Die Bereitschaft, eine zusätzliche Gebühr nach Ablauf der täglich zur Verfügung stehenden 30 Minuten zu zahlen, war äußerst gering. Die Nutzung dieser Hotspots muss entweder in einem bereits bestehenden Mobilfunk- oder Festnetzvertrag inkludiert sein, oder generell kostenfrei zur Verfügung stehen. Die der mabb bekannten WLAN-Projekte im öffentlichen Raum werden fast ausnahmslos mit öffentlichen Mitteln gefördert.

Bei öffentlich geförderten WLAN-Projekten müssen die Rahmenbedingungen in der Verwaltung optimiert werden

Zu den wichtigsten Erkenntnissen, die die mabb in den letzten Jahren gesammelt hat, gehört, dass die Rahmenbedigungen bei öffentlichen WLAN-Projekten verbessert werden müssen. Dies bezieht sich vorrangig auf Prozesse und Abstimmungen auf regionaler bzw. lokaler Ebene. Um Hotspots im öffentlichen Raum, in öffentlichen Gebäuden in Betrieb zu nehmen oder um Freifunk-Antennen auf Dächern zu installieren gibt es mehrere ganz praktische Hürden, die einen Projektstart erheblich verzögern können. Dazu gehören Fragen nach der Übernahme der Stromkosten, ob und inwieweit

Stromquellen verfügbar sind, manchmal muss bei der Installation auch der Denkmalschutz und das Facility Management hinzugezogen werden. Außerdem gibt es in einigen Fällen bereits Verträge mit einem Internet Service Provider, die diesem Exklusivrechte einräumen. Ein weiteres Problem ist die Kennzeichnung der Hotspots im öffentlichen Raum. In unserer WLAN-Broschüre haben wir das in Arnsberg (NRW) gewählte Modell vorgestellt, wo eine Zusammenarbeit von Stadtverwaltung, Verkehrsverein, Unternehmen und Freifunkern stattgefunden hat, um die Innenstadt zu vernetzen. Solche Kooperationen lassen sich in einer kleineren Kommune, in der die Beteiligten einander gut kennten, einfacher realisieren als in Städten wie Berlin, Hamburg oder Frankfurt/Main.

Mit freundlichen Grüßen,

Steffen Meyer-Tippach

Referent für Hörfunk und Digitale Projekte

Über die mabb

Die mabb ist die gemeinsame Medienanstalt der Länder Berlin und Brandenburg. Ihre Regulierungsaufgaben nimmt sie bei bundesweiten Veranstaltern und Plattformen zusammen mit den gemeinsamen Organen der Medienanstalten der Länder wahr. Entsprechend ihrem gesetzlichen Auftrag fördert die mabb in Berlin und Brandenburg Medienkompetenz und -ausbildung sowie Projekte für neue Übertragungstechniken. Der Erfüllung dieser Aufgaben dienen als Einrichtungen in Trägerschaft der mabb ALEX Offener Kanal Berlin und das Medieninnovationszentrum Babelsberg (MIZ).