



# Stellungnahme

des Deutschen Anwaltvereins durch  
den Ausschuss Informationsrecht

zum Entwurf eines Zweiten Gesetzes zur  
Änderung des Telemediengesetz (Zweites  
Telemedienänderungsgesetz – 2. TMGÄndG) vom  
11.03.2015

Stellungnahme Nr.: 17/2015

Berlin, im April 2015

## Mitglieder des Ausschusses

- Rechtsanwalt Dr. Helmut Redeker, Bonn (Vorsitzender und Berichterstatter)
- Rechtsanwältin Dr. Christiane Bierekoven, Nürnberg
- Rechtsanwältin Isabell Conrad, München
- Rechtsanwalt Dr. Malte Grützmaker, LL.M., Hamburg
- Rechtsanwalt Prof. Niko Härting, Berlin (Berichterstatter)
- Rechtsanwalt Peter Huppertz, LL.M., Düsseldorf
- Rechtsanwalt Dr. Robert Selk, LL.M. (EU), München
- Rechtsanwalt Prof. Dr. Holger Zuck, Stuttgart

## Zuständig in der DAV-Geschäftsführung

- Rechtsanwalt Thomas Marx, Berlin

**Deutscher Anwaltverein**  
Littenstraße 11, 10179 Berlin  
Tel.: +49 30 726152-0  
Fax: +49 30 726152-190  
E-Mail: [dav@anwaltverein.de](mailto:dav@anwaltverein.de)

**Büro Brüssel**  
Rue Joseph II 40  
1000 Brüssel, Belgien  
Tel.: +32 2 28028-12  
Fax: +32 2 28028-13  
E-Mail: [bruessel@eu.anwaltverein.de](mailto:bruessel@eu.anwaltverein.de)  
Transparenz-Registernummer:  
87980341522-66

## **Verteiler**

---

Bundesministerium der Justiz und für Verbraucherschutz  
Bundesministerium für Wirtschaft und Energie

Ausschuss für Recht und Verbraucherschutz im Deutschen Bundestag  
Ausschuss für Wirtschaft und Energie im Deutschen Bundestag  
Ausschuss Digitale Agenda im Deutschen Bundestag

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit  
Die Datenschutzbeauftragten der Bundesländer

Arbeitskreise Recht der Bundestagsfraktionen  
Justizministerien und Justizsenatoren der Länder  
Wirtschaftsministerien der Länder

Europäische Kommission - Vertretung in Deutschland  
Bundesrechtsanwaltskammer  
Bundesnotarkammer  
Bundesverband der Freien Berufe  
Deutscher Richterbund  
Deutscher Notarverein e.V.  
Deutscher Steuerberaterverband  
Bundesverband der Deutschen Industrie (BDI)  
GRUR  
BITKOM  
DGRI

DAV-Vorstand und Geschäftsführung  
Vorsitzende der DAV-Gesetzgebungsausschüsse  
Vorsitzende der DAV-Landesverbände  
Vorsitzende des FORUMs Junge Anwaltschaft

Frankfurter Allgemeine Zeitung  
Süddeutsche Zeitung GmbH  
Berliner Verlag GmbH  
Redaktion NJW  
Juve-Verlag  
Redaktion Anwaltsblatt  
Juris  
Redaktion MultiMedia und Recht (MMR)  
Redaktion Zeitschrift für Datenschutz ZD  
Redaktion heise online  
Redaktion Der Spiegel  
Redaktion FAZ

**Der Deutsche Anwaltverein (DAV) ist der freiwillige Zusammenschluss der deutschen Rechtsanwältinnen und Rechtsanwälte. Der DAV mit derzeit ca. 66.000 Mitgliedern vertritt die Interessen der deutschen Anwaltschaft auf nationaler, europäischer und internationaler Ebene.**

---

Auf S. 46 des Koalitionsvertrages findet sich das Vorhaben der Schaffung von Rechtssicherheit für W-LAN-Betreiber, etwa durch Klarstellung der Haftungsregelungen, die analog zu Access Providern geregelt werden sollten. Dazu hatte der DAV schon durch seine Stellungnahme Nr. 13/2014 Stellung bezogen, die Rechtslage aufgearbeitet und vorgeschlagen, zunächst in einer Expertenanhörung mögliche Maßnahme zur Verhinderung von Straftaten durchzuführen, die bei der Nutzung offener W-LANs begangen werden könnten.

Ein Jahr später liegt jetzt ein Referentenentwurf aus dem (federführenden) Bundeswirtschaftsministerium vor, der versucht, den Koalitionsvertrag umzusetzen.

Der Referentenentwurf ist nicht geeignet, das im Koalitionsvertrag angestrebte Ziel zu erreichen. Ganz im Gegenteil: Er verschärft die Haftung und führt zu zusätzlichen juristischen Unsicherheiten.

Im Einzelnen:

1.

Bei der Beurteilung der derzeitigen Rechtslage greift der Referentenentwurf die These des Koalitionsvertrages auf, die Rechtslage sei für Betreiber offener W-LANs in Deutschland unsicher, ohne sich mit seitdem eingetretenen Rechtsentwicklung auseinanderzusetzen. Von einer unsicheren Rechtslage war zwar auch noch die Stellungnahme des DAV 13/2014 ausgegangen. Im Jahre 2014 hat es aber weitere Entscheidungen zur Haftung der Betreiber offener W-LANs gegeben, die zwar nicht alle Rechtsfragen lösen, aber deutlich belegen, dass die Haftungsrisiken geringer sind als vorher angenommen.

Es gab im Jahre 2014 insgesamt 5 Entscheidungen zu diesen Fragen, nämlich AG Hamburg v. 24.5.2014, Az. 25b C 924/13; AG Koblenz v. 18.6.2014, Az. 161 C 145/14; AG Hamburg v. 10.6.2014, Az. 25b C 431/13, CR 2014, 536 m. Anm. Mantz; AG Charlottenburg v. 17.12.2014, Az. 217 C 121/14, CR 2015, 192 m. Anm. Bergt und AG Frankfurt v. 16.12.2014, Az. 30 C 2801/14 (32), ITRB 2015, 58 (Rössel). In keiner dieser Entscheidungen wurde eine Haftung des Betreibers eines offenen W-LANs angenommen. Nachdem es vor 2014 nur fünf weitere Entscheidungen gegeben hatte, von denen nur die Entscheidung LG Hamburg v. 25.11.2010, Az. 310 O 433/10, CR 2011, 331 eine Haftung annahm, kann man davon ausgehen, dass jedenfalls nach der Rechtsprechung der Instanzgerichte keine nennenswerten Haftungsrisiken bestehen. Verlangt werden nur ein passwortgeschützter Zugang und gegebenenfalls eine Belehrung des Nutzers darüber, dass illegale Nutzungen zu unterbleiben haben.

Für Freifunk hat das AG Charlottenburg eine Haftung auch ohne Passwortschutz abgelehnt – ebenso das AG Frankfurt a.M. für den Betreiber eines Hotspots. Unsicherheit besteht damit allenfalls noch bei der Frage, ob ein Passwortschutz und ein Hinweis auf das Verbot rechtswidriger Nutzungen erforderlich sind oder nicht. Die Klärung dieser eher technischen Ablauffragen bedarf schon prinzipiell keiner gesetzlichen Regelung, zumal ein Hotel-W-LAN, das nur Hotelgästen zur Verfügung gestellt werden soll, andere Lösungen verlangt als öffentliche Hot-Spots oder Freifunk. Der Referentenentwurf verkennt daher schon die Ausgangslage.

2.

Von den Einzelregelungen ist nur die Einfügung des § 8 Abs. 3 TMGRefE uneingeschränkt zu begrüßen. Dadurch werden Betreiber offener W-LANs Access-Provider gleichgestellt. Diese Regelung entspricht der h.M., die dies für öffentliche W-LANs ohnehin annimmt (vgl. schon Stellungnahme 13/2014). Dies schließt Strafbarkeits- und Schadensersatzrisiken aus.

3.

Die weiteren Absätze des Referentenentwurfs (§ 8 Abs. 4 u. 5 TMGRefE) regeln die Störerhaftung und damit Unterlassungsansprüche. Der in Abs. 4 S. 1 vorgeschlagene Regelung kann inhaltlich zugestimmt werden. Sie schließt einen Unterlassungsanspruch aus, wenn der W-LAN-Betreiber zumutbare Maßnahmen gegen

die missbräuchliche Nutzung des W-LANs ergriffen hat. Insoweit gibt die Regelung aber nur gefestigte Grundsätze der durch den BGH in unzähligen Entscheidungen ausgestalteten Störerhaftung wieder und ist in dieser Form entbehrlich. Der eigentliche neue Regelungsgehalt der geänderten Norm findet sich ausschließlich in den folgenden Absätzen.

In § 8 Abs. 4 S. 2 und § 8 Abs. 5 TMGRefE definiert der Gesetzgeber zumutbare Maßnahmen, die der Anbieter treffen soll. § 8 Abs. 4 S. 2 TMGRefE nennt als Regelbeispiele den Einsatz anerkannter Verschlüsselungsverfahren und eine Erklärung des Nutzers, bei der Nutzung keine Rechtsverletzungen begehen zu wollen. Setzt der Anbieter beide Maßnahmen ein, haftet er nicht.

Beide Voraussetzungen sind ungeeignet, das angestrebte Ziel der Gesetzgebung (mehr Möglichkeiten der Nutzung freier W-LANs) zu erreichen. Anerkannte Verschlüsselungsverfahren sind geeignet, die unerlaubte Nutzung von nicht jedermann zugänglichen W-LANs zu verhindern. Bei Hot-Spots, die jedermann zur Verfügung stehen, oder beim Freifunk machen sie keinen Sinn: Da jedermann die W-LANs nutzen soll, muss der Zugangscodex öffentlich sein. Der Einsatz des Verschlüsselungsverfahrens ist dann sinnlos. Sinnlose Maßnahmen kann der Gesetzgeber nicht ernsthaft verlangen.

Auch das Verlangen an den Nutzer, zu versichern, dass er das W-LAN nicht zur Begehung rechtswidriger Handlungen nutzen wolle, ist untauglich und unzumutbar. In der Regelung liegt ein Generalverdacht: Jeder, der ein W-LAN nutzt, nutzt es potentiell illegal. Der Gesetzgeber macht deutlich: Aus seiner Sicht ist jeder Internetnutzer möglicherweise ein Straftäter oder beabsichtigt zumindest, rechtswidrige Handlungen zu begehen. Dieser Generalverdacht ist als solcher verfassungswidrig. Schon deshalb ist die Regelung rechtswidrig. Unabhängig davon dürfte sich kaum ein Nutzer, der rechtswidrig handeln will, von einer solchen Versicherung davon abhalten lassen, dies zu tun. Wäre dem anders, wäre es sicher wert, zu prüfen, ob solche Erklärung auch bei anderen Handlungen (etwa dem Verkauf von Taschenmessern oder der Überlassung von Kraftfahrzeugen) verlangt werden müssen.

Wegen dieser Überlegungen sind Passwortschutz und Verpflichtungserklärung auch in der Freifunk-Entscheidung des AG Charlottenburg vom Freifunker nicht verlangt worden.

§ 8 Abs. 4 S. 2 TMGRefE verlangen daher ungeeignete und unverhältnismäßige Maßnahmen. Sie bringen keine Haftungserleichterungen, sondern führen zumindest teilweise zu Haftungsverschärfungen. Sie sind daher abzulehnen.

4.

Das gleiche gilt für § 8 Abs. 5 TMGRefE: Über die oben genannten Anforderungen hinaus verlangt der Referentenentwurf bei privaten W-LANs, dass der Anschlussinhaber die Namen der Nutzer kennt. Der Anschlussinhaber wird den Namen kennen, wenn er die Erlaubnis erteilt. Ohne Aufschreiben der Namen (und damit Datenerhebung im Sinne des BDSG) ist aber nicht sichergestellt, dass dies auch dann noch so ist, wenn Unterlassungsansprüche (in der Regel Monate später) geltend gemacht werden. Jedenfalls bei einer Nutzung nicht nur durch Mitbewohner, sondern auch durch Besucher ist nicht anzunehmen, dass sich der Anschlussinhaber bei jedem Besucher erinnert, ob er diesem die Nutzung gestattet hat oder nicht. Schon wegen der faktischen Speicherpflicht ist die Regelung unverhältnismäßig und daher abzulehnen: Die Regelung läuft darauf hinaus, dass der private Anschlussinhaber, der sich an Besuchernamen nicht erinnert, haftbar gemacht wird mit der Folge, dass sich eine Haftung nur durch eine Protokollierung von Besuchernamen vermeiden lässt.

Darüber hinaus ist nicht klar, warum bei der Nutzung privater W-LANs durch Dritte striktere Anforderungen gestellt werden als bei öffentlichen W-LANs. Der Referentenentwurf unterstellt hier höhere Gefahren, weil im Privatraum eher Straftaten begangen werden. Empirische Untersuchungen zu dieser Behauptung legt der Referentenentwurf nicht vor. Plausibel erscheint sie allenfalls begrenzt – für Hotel-W-LANs ist sie z.B. nicht plausibel. Ohne Aufzeichnung des Nutzungsverhaltens der einzelnen Nutzer hilft sie im Übrigen auch nicht bei der Rechtsdurchsetzung (vgl. schon Stellungnahme 13/2014). Auch deswegen ist die Regelung unverhältnismäßig.

Sie schafft außerdem weitere Rechtsunsicherheit, schon deswegen, weil die Frage, wann ein Dienst geschäftsmäßig erbracht wird und nur der Regelung des § 8 Abs. 4

TMGRefE unterliegt, und wann er privat ist und daher zusätzlich § 8 Abs. 5 TMGRefE gilt, keinesfalls immer klar zu entscheiden ist. Die auftretenden Probleme mögen zwar in der Praxis lösbar sein, dem Ziel des Gesetzesentwurfs widersprechen sie aber.

Die Regelung des § 8 Abs. 5 TMGRefE ist daher insgesamt abzulehnen.

5.

Neben den Vorschlägen zur Ergänzung des § 8 TMG enthält der Gesetzentwurf auch den Vorschlag einer Ergänzung des § 10 TMG. Durch diese Regelung soll sogenannten „gefährdungen Diensten“ die Privilegierung als Hostprovider faktisch entzogen werden. Die entsprechende Regelung greift Überlegung aus der Rechtsprechung auf (grundlegend BGH, *Urteil* vom 15. 1. 2009 - I ZR 57/07 Cybersky, GRUR 2009, 841; vgl. auch BGH, *Urteil* v. 12. 7. 2012 – I ZR 18/11, GRUR 2103, 370). Ein ernst zu nehmendes Bedürfnis für einer solche Regelung ist nicht zu erkennen – die Rechtsprechung zeigt deutlich, dass sie die auftretenden Einzelfälle lösen kann. Dies sollte dann auch ihr überlassen bleiben – zumal sie auch flexibler auf neue Entwicklungen reagieren kann.

Außerdem ist die Privilegierung der Hostprovider europarechtlich durch die E-Commerce-Richtlinie (Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt ("Richtlinie über den elektronischen Geschäftsverkehr") Amtsblatt Nr. L 178 vom 17/07/2000 S. 0001 - 0016) vorgegeben. Letztendlich interpretiert das Gesetz Art. 14 Abs. 1 der E-Commerce-Richtlinie. Ob die Interpretation zutrifft, bleibt der Entscheidung des Europäischen Gerichtshofs überlassen. Zumindest bei den Regelungen unter § 10 Abs. 2 S. 2 Buchst. a und d TMGRefE, die sog. „gefährdungen Dienste“ nicht aufgrund von zielgerichteten Maßnahmen des Diensteanbieters zur Gefahrerhöhung, sondern aufgrund objektiver, vom Diensteanbieter nur begrenzt beeinflussbarer Tatsachen annehmen, ist zweifelhaft, ob die Interpretation zutreffend ist. Der BGH äußert sogar Zweifel, ob die gesamte Rechtsfigur der „gefährdungen Dienste“ mit der Rechtsprechung des EuGH vereinbar ist (BGH, *Urteil* v. 12. 7. 2012 – I ZR 18/11, GRUR 2103, 370 (371)). Wegen des Vorrangs des Europarechts kann diese

Frage durch eine deutsche Gesetzesregelung nicht geklärt werden. Rechtssicherheit erreicht die Norm gewiss nicht.

Auch die im Referentenentwurf vorgeschlagene Ergänzung des § 10 Abs. 4 TMG ist daher abzulehnen.