STELLUNGNAHME

Berlin, 8. April 2015

Deutscher Industrie- und Handelskammertag

Entwurf eines Zweiten Gesetzes zur Änderung des Telemediengesetzes (Zweites Telemedienänderungsgesetz – 2. TMGÄndG)

I. Vorbemerkungen

Der Deutsche Industrie- und Handelskammertag (DIHK) nimmt gern die Gelegenheit wahr, den Referentenentwurf aus gesamtwirtschaftlicher Sicht zu kommentieren.

Der Gesetzentwurf soll richtiger Weise in erster Linie dazu dienen, den Zugang zu öffentlich drahtlosen Internetzugängen rechtssicher zu ermöglichen. Er soll den flächendeckenden Zugang zu breitbandigen Internetanschlüssen fördern, der Voraussetzung für die Teilhabe der Bevölkerung an Wissen und Bildung sowie für die Präsenz des Staates mit seinen digital angebotenen Dienstleistungen (E-Government) ist. Hinzu kommt, dass die Kunden von Gastronomie, Einzelhandel und Tourismus mittlerweile ganz natürlich davon ausgehen, dass sie in den entsprechenden Räumlichkeiten auf das Internet zugreifen können. Die Zurverfügungstellung öffentlicher WLANs ist somit in einigen Branchen ganz selbstverständlich zum Standard geworden, auch als Infrastruktur für Location based Services, und muss rechtssicher möglich sein.

Der Gesetzentwurf muss zwei Zielen Rechnung tragen: Zum Einen muss das Potenzial der drahtlosen Internetzugänge stärker ausgeschöpft werden, zum Anderen müssen die berechtigten Interessen von Rechteinhabern geschützt werden. Zu letzteren gehören insbesondere Inhaber von Urheberrechten, aber auch alle Personen, deren Persönlichkeitsrecht durch Dritte im Wege der Nutzung des Internets verletzt werden können. Sie müssen auch bei öffentlichen WLANs die Möglichkeit haben, rechtlich gegen den Schädiger vorgehen zu können. Erscheinungen wie Cybermobbing oder anonyme Negativbewertungen von Unternehmen, die häufig auf unwahren Behauptungen beruhen, können mit offenen WLAN-Zugängen verstärkt auftreten.

DIHK | Deutscher Industrie- und Handelskammertag e. V.
Registriernummer des DIHK im Register der Europäischen Kommission: 22400601191-42
Breite Straße 29 | 10178 Berlin-Mitte | Telefon ++49-(0)30-20308-0 | Fax ++49-(0)30-20308-1000
E-Mail Berlin: infocenter@dihk.de | E-Mail Brüssel: dihk@bruessel.dihk.de | Internet: www.dihk.de

Die Evaluierung des Gesetzes ist daher notwendig, um zu überprüfen, ob die Wertung des Gesetzgebers zugunsten der Öffnung von WLAN-Zugängen richtig war. Dies sollte im Gesetz selbst geregelt werden.

Aus Sicht der Wirtschaft ist grundsätzlich zu begrüßen, dass die Haftungsrisiken der Anbieter von WLAN-Internetzugängen für Rechtsverletzungen ihrer Nutzer (sog. Störerhaftung) durch Beseitigung von Rechtsunsicherheiten eingeschränkt werden sollen. Die bestehende Rechtsunsicherheit ist jedoch mit den gewählten Formulierungen nicht durchgängig beseitigt.

Der Referentenentwurf wird u. a. begründet mit der Entscheidung des BGH (BGH Urteil v. 12.05.2010, Az. I ZR 121/08, „Sommer unseres Lebens“). Das angesprochene Urteil bezieht sich jedoch nicht auf öffentliche sondern explizit auf private WLAN-Zugänge. Fraglich erscheint daher, ob die Prinzipien, die vom BGH für private Zugänge entwickelt wurden, auf die öffentlichen Zugänge ausgeweitet werden können. Denn im Bereich öffentlicher WLAN-Zugänge soll die Nutzungsmöglichkeit von Dritten gerade gefördert werden.

Zudem entwickelt sich derzeit eine Rechtsprechung, nach der die Anbieter von öffentlichen WLAN-Zugängen als Access Provider angesehen werden und damit auch nach bereits geltender Gesetzeslage von der Haftung freigestellt sind (AG Charlottenburg, Beschluss vom 17.12.2014, 217 C 121/14; AG Hamburg, Urt. v. 10.06.2014 – 25b C 431/13, Urt. v. 24.06.2014 – 25b C 924/13)
Das LG München I (Beschluss vom 18.09.2014, Az. 7 O 14719/12) hat die Frage der Haftung von WLAN-Betreibern dem EUGH vorgelegt. Die dort aufgeworfenen Rechtsfragen betreffen im Wesentlichen die im Gesetzentwurf enthaltenen Regelungen. Insofern kann die Rechtslage der E-Commerce-Richtlinie zum jetzigen Zeitpunkt wohl nicht als gesichert angesehen werden. Ein Abwarten der Entscheidung des EuGH wäre daher sinnvoll.

II. Im Einzelnen:

E. Erfüllungsaufwand

Das Angebot eines öffentlichen Internetzugangs ist an eine Erklärung der Nutzer gebunden, im Rahmen der Nutzung keine Rechtsverletzungen zu begehen. Eine solche Bestätigung kann mit den üblichen Routern nicht eingeholt werden. Die WLAN-Anbieter müssen also eine Infrastruktur schaffen, die die Möglichkeit zur Bestätigung bietet. Zusätzlich werden neue Administrationskosten für die Einrichtung, Wartung und Prüfung dieser Funktion entstehen. Der entstehende Aufwand sollte im Gesetz dargestellt werden.

DIHK | Deutscher Industrie- und Handelskammertag e. V.
Registriernummer des DIHK im Register der Europäischen Kommission: 22400601191-42
Breite Straße 29 | 10178 Berlin-Mitte | Telefon ++49-(0)30-20308-0 | Fax ++49-(0)30-20308-1000
E-Mail Berlin: infocenter@dihk.de | E-Mail Brüssel: dihk@bruessel.dihk.de | Internet: www.dihk.de

§ 8 Absatz 4 Nr. 1 TMGÄndG-E

Rechtsverletzungen durch Nutzer sollen durch Verschlüsselung oder vergleichbare Maßnahmen gegen den unberechtigten Zugriff auf das drahtlose Funknetz durch außenstehende Dritte verhindert werden. Hierzu merken wir an, dass sich

1. ein öffentlicher Netzzugang gerade an einen nicht näher bestimmten Nutzerkreis richtet – und damit in der Regel an außenstehende Dritte.
2. die Frage stellt, inwiefern technische Maßnahmen einen tatsächlichen Zugangsschutz darstellen.

Zu 1.

Insbesondere für Unternehmen stellt sich die Frage, wer überhaupt unter einem „außenstehenden Dritten“ zu verstehen ist. Die fehlende Definition des „außenstehenden Dritten“ führt zu praktischen Umsetzungsproblemen. Als außenstehender Dritter ist wohl jeder zu verstehen, der nicht in einem vertraglichen oder sonstigem Verhältnis zum Anbieter steht. In diesem Sinne als nicht außenstehend wären damit vermutlich die Kunden des Anbieters zu verstehen, nicht aber sämtliche Personen, die sich lediglich z. B. im Empfangsbereich eines Hotels aufhalten.

Gleich gelagert wäre wohl die Beantwortung der Frage, wann ein Zugriff berechtigt ist und wann nicht. Solange der Nutzer den Anschluss im Rahmen eines zum Anbieter bestehenden Vertragsverhältnisses nutzt, dürfte der Zugriff als berechtigt anzusehen sein. Nachdem das Vertragsverhältnis beendet ist und der Anbieter damit auch nicht mehr von der Attraktivitätssteigerung durch den WLAN-Anschluss profitiert, dürfte er kein Interesse mehr daran haben, dass der Nutzer sich immer noch einloggen kann, weshalb der Zugriff ab diesem Zeitpunkt als unberechtigt anzusehen wäre. Dabei stellt sich aber die Frage, was nach einer Beendigung des Vertragsverhältnisses zwischen dem Anbieter und dem Nutzer gelten soll. Insbesondere besteht diese Problematik in Geschäftsbereichen mit einem stetigen Kundenwechsel, wie etwa bei Cafés oder Hotels. Wenn ein Kunde z. B. das Café nach dem Bezahlen verlässt, könnte er aufgrund der Beendigung des Vertragsverhältnisses als außenstehender Dritter zu bewerten sein. Da er aber noch im Besitz des Passwortes ist und sich insbesondere der Zugriff auf einen WLAN-Anschluss nicht nur auf ein Gebäude beschränkt, sondern darüber hinaus auch noch von weiter entfernten Stellen (ca. bis zu 300 Meter) genutzt werden kann, besteht nach wie vor die Möglichkeit der Anschlussnutzung.

Damit vergleichbar ist die Situation, dass der Nutzer später wieder in den Empfangsbereich des WLAN-Anschlusses kommt, ohne aber erneut ein Vertragsverhältnis zum Anbieter einzugehen. In der Regel erkennen Smartphones oder Notebooks, die sich einmal in ein WLAN-Netz eingeloggt haben, dieses wieder, wenn sie sich das nächste Mal im Empfangsbereich befinden, sodass die

DIHK | Deutscher Industrie- und Handelskammertag e. V.
Registriernummer des DIHK im Register der Europäischen Kommission: 22400601191-42
Breite Straße 29 | 10178 Berlin-Mitte | Telefon ++49-(0)30-20308-0 | Fax ++49-(0)30-20308-1000
E-Mail Berlin: infocenter@dihk.de | E-Mail Brüssel: dihk@bruessel.dihk.de | Internet: www.dihk.de

erneute Eingabe des Passwortes nicht notwendig ist. Damit würde sich ein außenstehender Dritter in das Netz einloggen, obwohl nach dem Wortlaut der vorgeschlagenen Fassung gerade dagegen der Anschluss gesichert werden sollte.

Streng nach dem Wortlaut müssten die Anbieter somit sicherstellen, dass sich auch ehemalige Kunden nicht mehr in das Netz einloggen können. Dies wäre praktisch aber kaum möglich. Die Folge daraus ist, dass für Anbieter auch nach der vorgeschlagenen Fassung nach wie vor die Unsicherheit besteht, wann der Zugriff auf das WLAN-Netz hinreichend gesichert ist. Die Anbieter müssen deshalb befürchten, dass ihnen von der Rechtsprechung Pflichten auferlegt werden, die über die in der Begründung aufgezählten Verschlüsselungsmaßnahmen hinausgehen.

Da das Gesetz nach der Begründung aber letztendlich nur dafür sorgen möchte, dass der WLAN-Anschluss angemessen verschlüsselt wird, würde der Wortlaut ohne die Formulierung „durch außenstehende Dritte“ ausreichen.

Zu 2.
Die Verwendung des Begriffs „Verschlüsselung“ im Referentenentwurf wirft Fragen auf. Der eigentliche Zweck von Verschlüsselungstechnologien ist es, die Vertraulichkeit und Authentizität der ausgetauschten Informationen zu sichern. Die Konsequenz der vorgesehenen Regelung ist, dass die Nutzung des Zugangs für rechtswidrige Zwecke von keinem Dritten ausgelesen und unerkannt manipuliert werden kann; die rechtswidrige Nutzung selbst wird nicht verhindert oder minimiert.

Verschlüsselung im Referentenentwurf bezweckt wohl, dass Nutzer einen Zugangsschlüssel bzw. ein Passwort vom Anbieter für die Nutzung des WLANs erhalten sollen. Aus IT-Sicherheits-Perspektive müsste für jeden Nutzer ein eigener Zugangscode generiert werden. Dies würde erneuten Administrationsaufwand beim Anbieter bedeuten. Der Aufwand wäre geringer, wenn alle Nutzer denselben Zugangscode bzw. Schlüssel verwenden. Ob die Verschlüsselung dann noch einen Sicherheitsgewinn bedeutet, ist fraglich, insbesondere wenn anschließend keine weitere Sicherheitsprüfung erfolgt und die Zugangsdaten ggf. weitergegeben werden.

Die Formulierung „vergleichbare Sicherungsmaßnahmen ist zwar offen für die technische Entwicklung, gleichzeitig verursacht sie aber auch Rechtsunsicherheit, weil es dem Betreiber allein überlassen bleibt, die Vergleichbarkeit ausreichend zu definieren. Daher wäre es hilfreich, einige grundlegende Kriterien als Mindeststandard festzulegen.

Eine Alternative wäre zu prüfen, ob eine Beispielsnennung von entsprechenden Maßnahmen in der Gesetzesbegründung den Rechtsanwendern Hilfestellung geben könnte (z. B. Beschränkung des

DIHK | Deutscher Industrie- und Handelskammertag e. V.
Registriernummer des DIHK im Register der Europäischen Kommission: 22400601191-42
Breite Straße 29 | 10178 Berlin-Mitte | Telefon ++49-(0)30-20308-0 | Fax ++49-(0)30-20308-1000
E-Mail Berlin: infocenter@dihk.de | E-Mail Brüssel: dihk@bruessel.dihk.de | Internet: www.dihk.de

Datenvolumens oder die Nutzung von Webfiltern). Die Begründung sollte ebenfalls eine Aussage dazu treffen, ob vom Anbieter ein „Stand der Technik“ eingehalten werden muss (z. B. WPA ./. WPA 2).

§ 8 Absatz 4 Nr. 2 TMGÄndG-E

Der Entwurf lässt offen, wie die Erklärung zu erfolgen hat und wie sie der Anbieter protokollieren/dokumentieren muss. Denn nur dann kann er im Streitfalle den erforderlichen Nachweis führen. Hier bedarf es näherer Hinweise durch den Gesetzgeber.

Zudem führt der Nachweis der Erklärung zu erheblichen praktischen Problemen:
Damit die Bestätigung zweifelsfrei einer bestimmten rechtswidrigen Nutzung im Einzelfall zugeordnet werden kann, muss sie zusammen mit weiteren Informationen zu dem genutzten Internetzugang gespeichert werden. Das könnten sein: Informationen zu dem angemeldeten Gerät, zu den Anmeldezeiträumen sowie zu den aufgerufenen Seiten und Internetdiensten. Auf diese Weise würde der Zugangsanbieter gezwungen, eine eigene „Vorratsdatenspeicherung“ vorzuhalten – ein Widerspruch zum Datenschutz.

§ 8 Absatz 5 TMGÄndG-E

Die Verschärfung für die Anbieter privater Zugänge ist zwar nachvollziehbar, die Begründung überzeugt jedoch nicht. Die Gefährdung der Rechte Dritter bzw. das Begehen strafbarer Handlungen z. B. in einem Einkaufszentrum sind im Zweifel genauso hoch wie in einem privaten Umfeld.

Hinweis: Im zweiten Absatz der Begründung ist ein Widerspruch enthalten:
„Der **geschäftsmäßig** handelnde Diensteanbieter hat zudem grundsätzlich die Möglichkeit, einem Nutzer, …, die weitere Nutzung des WLAN zu untersagen. Die namentliche Kenntnis des Nutzers ist daher **verzichtbar**.“

§ 10 TMGÄndG-E

Mit der vorgeschlagenen Formulierung wird nicht die heute zu § 10 TMG bekannte Rechtsprechung umgesetzt, sondern die Haftung verschärft und Rechtsunsicherheit geschaffen. Das bislang anerkannte Prinzip, dass der Diensteanbieter nur die Infrastruktur für seine Nutzer bereithält und erst bei Kenntnis von Rechtsverletzungen einzuschreiten hat, wird ohne Not über Bord geworfen.

DIHK | Deutscher Industrie- und Handelskammertag e. V.
Registriernummer des DIHK im Register der Europäischen Kommission: 22400601191-42
Breite Straße 29 | 10178 Berlin-Mitte | Telefon ++49-(0)30-20308-0 | Fax ++49-(0)30-20308-1000
E-Mail Berlin: infocenter@dihk.de | E-Mail Brüssel: dihk@bruessel.dihk.de | Internet: www.dihk.de

Hinzukommt, dass die vorgesehenen Anwendungsfälle Fragen aufwerfen:

Abs. 2 a ist zu weit gefasst: Es kann nicht pauschal davon ausgegangen werden, dass ab einem Anteil rechtswidriger Inhalte von weit über 50% dem Anbieter dies auch bekannt ist. Insbesondere bei Blog- oder Forenbetreibern, bei denen sich die dargestellten Inhalte minütlich aktualisieren, können die Anbieter nicht jeden einzelnen Eintrag überprüfen. Letztendlich würde Anbietern, die ihren Nutzern das Speichern von Informationen auf Servern ermöglichen, eine Prüfpflicht sämtlicher Inhalte auferlegt. Dies widerspricht aber dem Privilegierungsgrund des § 10 TMG, der ja gerade darin besteht, dass die Anbieter nicht selbst die fremden Informationen speichern, sondern dies nur anderen ermöglichen. Für die betroffenen Anbieter hätte das einen ganz erheblichen Arbeitsaufwand zur Folge. Es müssten praktisch in regelmäßigen Abständen die gespeicherten Informationen überprüft und ggf. gelöscht werden. Anderenfalls könnte es zu einem übermäßigen Anteil rechtswidrig gespeicherter Informationen kommen, so dass zu Lasten der Anbieter die Vermutungswirkung des Abs. 2 a eintritt. Um dieser zu entgehen, müssten die Anbieter dem also aktiv entgegenwirken.

Da die weitere Aufzählung in Abs. 2 ausreichend erscheint, diejenigen Anbieter von einer Privilegierung auszunehmen, die bewusst Rechtsverstöße fördern, sollte deshalb auf die gesetzliche Vermutung im Abs. 2 a verzichtet werden.

Abs. 2 b
Es ist unklar, welche Fallkonstellationen hiermit erfasst werden sollen. Jede Plattform z. B. zum Datenaustausch kann zu rechtswidrigen Zwecken genutzt werden. Damit ist jede Werbung für eine solche Plattform grundsätzlich geeignet, die Gefahr der rechtsverletzenden Nutzung zu fördern. Sie ist auch „gezielt“, da sie darauf abzielt, die Nutzung zu steigern und mit erhöhter Nutzung fast zwangsläufig die Gefahr steigt, dass sie auch rechtsverletzend genutzt ist.

Abs. 2 c
Die Bedeutung von Werben mit „Nichtverfolgbarkeit bei Rechtsverstößen“ sollte näher konkretisiert werden. Denn jede Plattform, die sich zum Ziel setzt, die Verfolgbarkeit Ihrer Nutzer zu verhindern, wird gleichzeitig die „Nichtverfolgbarkeit bei Rechtsverstößen“ anstreben, da sich die Verfolgbarkeit nicht nach „Rechtsverstöße“ und „keine Rechtsverstöße“ trennen lässt. Wer also nun mit „Nichtverfolgbarkeit“ wirbt, tut dies fast zwangsläufig auch für den Fall eines (möglicherweise fehlerhaft unterstellten) Rechtsverstoßes. Plattformen mit einem hohen Anspruch auf Schutz der Privatheit werden so voraussichtlich als „gefahrgeneigt“ angesehen.

DIHK | Deutscher Industrie- und Handelskammertag e. V.
Registriernummer des DIHK im Register der Europäischen Kommission: 22400601191-42
Breite Straße 29 | 10178 Berlin-Mitte | Telefon ++49-(0)30-20308-0 | Fax ++49-(0)30-20308-1000
E-Mail Berlin: infocenter@dihk.de | E-Mail Brüssel: dihk@bruessel.dihk.de | Internet: www.dihk.de

Leider werden viele Anbieter von Inhalten, die für offenkundig illegale Zwecke betrieben werden, außerhalb des europäischen Einflussbereichs agieren und sich so einer Verfolgung entziehen können.

Ansprechpartnerinnen:

Dr. Katrin Sobania, Tel.: 030/203082109
E-Mail: sobania.katrin@dihk.de

Annette Karstedt-Meierrieks, Tel.: 030/203082706
E-Mail: karstedt-meierrieks.annette@dihk.de