Finanzbehörde
Gz.: 126-610-2/84

Hamburg, den 04.06.2012
☎ 428 23-1448

Anlage zum Prüfantrag der Bezirksversammlung Hamburg Nord anlässlich des Themas „Freier WLAN-Zugang für Hamburg-Nord“

Unbeschadet der nicht geklärten Frage, ob die Finanzbehörde auf der Grundlage ihrer zentralen Zuständigkeit für den IT-Bereich der hamburgischen Verwaltung für die Klärung dieser Rechtsfrage aus dem Bezirk überhaupt zuständig ist - schließlich verfügt jedes Bezirksamt über ein eigenes Rechtsamt - , ist aus rechtlicher Sicht Folgendes anzumerken:

1. Gesetzliche Rahmenbedingungen

Wesentliche Rechtsgrundlage sind das Telemediengesetz (TMG) und das Telekommunikationsgesetz (TKG). Das Bundesdatenschutzgesetz (BDSG) regelt den Umgang mit personenbezogenen Daten, die im Rahmen von Sicherungsmaßnahmen evtl. auch für den Hotspot Betreiber anfallen können. Das entscheidende Problem stellt eine mögliche Haftung des Betreibers für Rechtsverletzungen Dritter dar, die innerhalb des von ihm betriebenen Hotspots begangen wurden. Weitere juristische Fragestellungen schließen sich an, so z.B. ob ein Anspruch auf Schadensersatz besteht, wenn der tatsächliche Schadensverursacher ermittelt werden kann. Als Schädigung können z.B. Urheberrechtsverletzungen, Eingriffe in das allgemeine Persönlichkeitsrecht und sonstige Verstöße im Internet angesehen werden.

Die Wahl der richtigen Rechtsgrundlage ist für die rechtliche Beurteilung ausschlaggebend. Einschlägig sind sowohl Begriffsdefinitionen im TKG als auch im TMG. In § 3 Abs. 6 TKG und in § 2 Abs. 1 TMG ist der Begriff des Telekommunikationsdiensteanbieters bzw. des Dienstanbieters definiert. Der Nutzer ist definiert in § 3 Abs. 14 TKG und § 2 Abs. 4 TMG. Für gewerblich betriebene Funknetze gilt nach allgemeiner Auffassung, dass der Hotspotanbieter rechtlich als Access-Provider einzustufen ist, da er Dritten den Zugang zu einem Netz bzw. zu fremden Informationen vermittelt; folglich muss er den Verkehrssicherungspflichten beim Betrieb seines Netzes nachkommen. Beispiele für Diensteanbieter sind neben den klassischen Telekommunikationsunternehmen auch Krankenhäuser, Hotels, Altenheime, Anbieter

firmeninterner Telefonanlagen und jeweils die mitwirkenden Personen, soweit den Patienten, Gästen bzw. Mitarbeitern die Möglichkeit zur Nutzung von Telekommunkationsdiensten eingeräumt wird.

Neben dem TMG und dem TKG unterliegen die Betreiber offener WLAN-Hotspots im Grundsatz auch dem BDSG. Dieses regelt den Umgang mit personenbezogenen Daten. Die für den Hotspot-Betreiber wichtigen datenschutzrechtlichen Vorschriften stammen allerdings alle aus dem TKG und ggfs. aus dem TMG und verdrängen damit als lex specialis die Vorschriften aus dem BDSG.

Die zentrale Frage für den Betreiber eines WLAN-Hotspot ist die Störerhaftung. In den letzten Jahren kam es zu einem regelrechten Abmahnwahn, so wurden im Jahr 2010 ca. 575.800 Abmahnungen im Wert von über 412 Millionen Euro verschickt. Die Abmahnung hat sich zu einem Geschäftsmodell etabliert. Der Rechteinhaber ist bestenfalls in der Lage, die IP-Adresse des Verletzters mit Hilfe eines Staatsanwaltes (§ 133 TKG) oder dem Richterbeschluss (§ 101 Abs. 9 UrhG) per Bestandsdatenabfrage über den Provider festzustellen. Die IP-Adresse liefert allerdings keine klare Auskunft über den tatsächlichen Nutzer. Dies ist den Klägern zumeist gleichgültig, denn sie wollen Schadenersatz erwirken oder auf Unterlassung klagen. Als die Anschlussinhaber allerdings bestritten, für die Rechtsverletzung verantwortlich zu sein, wurde die Haftung des Anschlussinhabers eingeführt. Dabei geht es um zumutbare Prüf- und Aufsichtspflichten und ob der Anschlussinhaber diesen in ausreichendem Maße nachgekommen ist. Er muss technische Vorkehrungen nach dem jeweiligen Stand der Technik treffen, um naheliegende Rechtsverstöße (zumeist urheberrechtliche Verstöße) technisch zu verhindern (z.B. technische Zugangssperren bei Tauschbörsen).

2. Störerhaftung

Die Haftung des Hotspot Betreibers ist stark umstritten und es gab in den vergangenen Jahren zahlreiche Entscheidungen, die eine Haftung bejahen, aber auch solche, die eine pauschale Haftung ablehnten. Problematisch ist hierbei auch der fliegende Gerichtsstand bei Internet-Delikten, der inzwischen auch vielfach kritisiert wird. Reto Mantz kommt in seiner Dissertation "Rechtsfragen offener Netze" (2008) zu folgendem Ergebnis: *"Wenn über den Knoten eines Netzbetreibers Rechtsverletzungen begangen werden, so liegt eine mittelbare willentliche und adäquat-kausale Mitverursachung auf Seiten des Betreibers vor."* (S. 248). Netzbetreiber ist der Hot-

spot-Betreiber. Dies bedeutet, dass dem Anschlussinhaber eine indirekte Mitverantwortung im Sinne der derzeit gültigen Rechtslage zugeschrieben wird.

Für Privatpersonen ist die Rechtslage seit dem BGH Urteil zu "Sommer unseres Lebens" (BGH 12.05.2010 – 1 ZR 121/08) einigermaßen klar. Darin stellt der BGH fest, dass die fortlaufende Anpassung der Netzwerksicherheit an den "neuesten Stand der Technik" für Privatpersonen nicht zumutbar ist. Die Prüfungspflicht bezieht sich auf die Einhaltung der üblichen Sicherungsmaßnahmen zum Zeitpunkt der Installation. Der private Anschlussinhaber kann demzufolge nicht auf Schadensersatz verklagt werden, sondern lediglich auf Unterlassung und die Erstattung von Anwaltskosten. Die Abmahnkosten sind im § 97a Abs. 2 UrhG auf 100 € gedeckelt, so dass Privatpersonen, die ihr WLAN mit einem ausreichend langen Passwort gesichert haben, rechtlich relativ sicher sind.

Jaeschke, kam in einem Interview des Heise-Verlags zu dem Schluss, dass *"gewerbliche Netze privilegiert sind"*. Er begründet dies damit, dass sich der BGH in seiner Urteilsfindung nicht mit der Anwendbarkeit von § 8 TMG hinsichtlich der Durchleitung von Informationen auseinandergesetzt hat. *"Hiernach sind Diensteanbieter für fremde Informationen, die sie in einem Kommunikationsnetz übermitteln oder zu denen sie den Zugang zur Nutzung vermitteln, nicht verantwortlich, sofern sie die Übermittlung nicht veranlasst, den Adressaten der übermittelten Informationen nicht ausgewählt und die übermittelten Informationen nicht ausgewählt oder verändert haben. Dies trifft etwa auf alle Anbieter von Unternehmens-, Stadt-, Universitäts- oder Hotel-WLAN-Netzen usw. zu, auf Internetcafes ohnehin."* Des Weiteren stellt er heraus, dass *"die Bereitstellung von Netzwerkinfrastruktur [...] wirtschaftlich und sozial gewollt und sinnvoll ist".* Ferner führt er auf, dass die Haftung häufig an der *"Unzumutbarkeit der Verhinderung weiterer Verstöße"* scheitert. Ein Zuwiderhandeln, z.B. die Protokollierung des Datenverkehrs, würde gegen das Fernmeldegeheimnis verstoßen und strafrechtliche Konsequenzen nach § 206 Strafgesetzbuch (StGB) nach sich ziehen.

Das LG Hamburg verurteile im Beschluss vom 25.11.2010 – (AZ 310 O 433/10) einen Internet-Café-Betreiber als Störer auf Unterlassung wegen Urheberrechtsverletzungen. Zitat: *"Der Antragsgegner haftet als Anschlussinhaber jedenfalls nach den Grundsätzen der Störerhaftung verschuldensunabhängig auf Unterlassung. Dies gilt auch unter Berücksichtigung des Umstandes, dass er vorgerichtlich geltend gemacht hat, die Rechtsverletzung sei durch einen Kunden seines Internet-Cafés begangen*

worden. Das Überlassen eines Internetzugangs an Dritte birgt die nicht unwahrscheinliche Möglichkeit in sich, dass von den Dritten Urheberrechtsverletzungen über diesen Zugang begangen werden. Dem Inhaber des Internetanschlusses sind Maßnahmen möglich und zumutbar, solche Rechtsverletzungen zu verhindern. So können insbesondere die für das Filesharing erforderlichen Ports gesperrt werden. Dass der Antragsgegner irgendwelche in diesem Sinne geeigneten Maßnahmen ergriffen hat, ist nicht ersichtlich. Dagegen spricht vielmehr der Umstand, dass es zu der vorliegenden Rechtsverletzung kommen konnte.".

Derzeit haben "Access-Provider" und damit auch gewerbliche Hotspot Betreiber, weder eine in der Praxis umsetzbare noch eine rechtliche Möglichkeit zur Verhinderung urheberrechtsverletztender Handlungen ihrer Nutzer, weil es keine wirksame Internet-Sperre gibt, weil hierfür ohnehin derzeit keine Rechtsgrundlage besteht und die Inhalte der Kommunikation dem Fernmeldegeheimnis unterliegen, so Rechtsanwalt Dr. Jaeschke. Es herrscht ein Drohpotenzial bis zu einer Entscheidung des BGH, denn die einzelnen Instanzgerichte kommen immer wieder zu unterschiedlichen rechtlichen Bewertungen.

3. Erfassung der Nutzerdaten

Das Bundesverfassungsgericht hat mit Entscheidung vom 02.03.2010 die bis dato gültigen gesetzlichen Bestimmungen zur Vorratsdatenspeicherung für grundgesetzwidrig erklärt und mit sofortiger Wirkung gestoppt. Im Fokus des höchstrichterlichen Beschlusses standen insbesondere die §§ 113a und b des Gesetzes zur Neuregelung des Telekommunikationsgesetzes. Das Verfassungsgericht sah vor allem in der anlasslosen Speicherung und unzureichenden Beachtung des Verhältnismäßigkeitsgrundsatzes eine Verletzung der Grundrechte als gegeben. Die obersten Richter gaben damit der Beschwerde von rund 30.000 Klägern statt, die durch die umfassende 6-monatige Vorratsdatenspeicherung ihr Grundrecht auf informationelle Selbstbestimmung gefährdet sahen.

Das Protokollieren aufgerufener IP-Adressen, das Speichern von MAC-Adressen oder eine Anmeldeprozedur am Hotspot, um kaum überprüfbare Nutzerdaten zu erfassen, verhilft dem Betreiber eines freien Hotspots in der Praxis leider nicht dazu, im Ernstfall einen Rechtsverletzer beweiskräftig identifizieren zu können. Kommerzielle Hotspot-Anbieter haben da ein besseres Mittel in der Hand: Wenn Zahlungstransaktionen für Nutzungsgebühren etwa über eine Kreditkarte oder einen Internetbezahl-

dienst wie PayPal abgewickelt werden, lässt sich relativ zuverlässig ermitteln, wer zum Zeitpunkt einer Rechtsverletzung das WLAN genutzt hat. Um dann noch herauszubekommen, welcher der insgesamt bekannten Teilnehmer denn nun genau der gesuchte Übeltäter war, muss der kommerzielle WLAN-Betreiber noch wissen, welche der dynamischen IP-Adressen des Routers sich für den fraglichen Moment der Rechtsverletzung zuordnen lassen.

Wer einen öffentlichen WLAN-Hotspot betreibt, muss sich über das Risiko im Klaren sein, dass er trotz (rechtlich unsicherem) Haftungsprivileg mit Unterlassungsansprüchen in Bezug auf Rechtsverletzungen Dritter konfrontiert wird, sofern er nicht alles Erforderliche und Zumutbare getan hat, um dergleichen zu vermeiden. Dabei ist es nicht entscheidend, ob der WLAN-Betreiber mit seinem Hotspot Geld verdient oder nicht. Wird der WLAN-Zugang allerdings kostenlos zur Verfügung gestellt, entfallen die Möglichkeiten einer Datenspeicherung weitgehend (vgl. BVergG, siehe oben). Damit entfallen dann aber auch die Beweismöglichkeiten bei missbräuchlicher Nutzung.

4. Ergebnis

Zusammenfassend lässt sich sagen, dass die aktuelle Rechtslage offener WLAN-Hotspots in Deutschland nach inzwischen schon über zehn Jahren immer noch nicht hinreichend geklärt ist. Die Frage, ob der Hotspot-Betreiber unter das Haftungsprivileg des TMG fällt, ist auch nach dem BGH-Urteil "Sommer unseres Lebens" vom 12.05.2010 weiterhin offen. Es gibt zahlreiche Stimmen, die das TMG nicht für anwendbar halten. Fiele der Hotspot-Betreiber unter das Haftungsprivileg, wäre dies eine Art Freifahrtschein und er würde nicht einmal auf Unterlassung in Anspruch genommen werden können. Den Gerichten fehlt es zum Teil erkennbar am technischen Sachverstand und teilweise werden technische Sachverständige einfach nicht zu Rate gezogen. So werden Entscheidungen auf unterschiedlichen Rechtsgrundlagen getroffen, die dann jeweils weite Interpretationsspielräume lassen. Bestes Beispiel hierfür ist der Versuch, die Rechte von Markenbesitzern durchzusetzen und gleichzeitig die Datenschutzbestimmungen einzuhalten.

Es fehlt gegenwärtig an einer umfassenden Rechtsgrundlage, die so konkret formuliert ist, dass keine anderen Rechtsgrundlagen einbezogen werden müssen. Es müssen klare technische Vorgaben rechtlich festgelegt werden, solange es keine besseren technischen Möglichkeiten gibt. Daran fehlt es bislang ebenso wie an einer siche-

ren Rechtsgrundlage für die erforderliche Vorratsdatenspeicherung, sofern diese überhaupt mit dem Grundgesetz für vereinbar gehalten wird.

Für den WLAN-Hotspot Betreiber sollte sichergestellt sein, dass Ansprüche gegen kriminell Handelnde auch an die tatsächlichen Verursacher weitergereicht werden können. Dies kann jedoch einzig durch eine Identifikation der Nutzer, z.B. durch Protokollierung der Mobilfunknummer, erfolgen. Diese eher technisch determinierte Forderung ist abzuwägen mit dem Fernmeldegeheimnis, welches jegliche Kommunikation über öffentliche Netze schützt. Bei einem WLAN-Netzt spielt jedoch die Mobilfunknummer keine Rolle, weil sie technisch nicht benötigt wird. Protokollieren ließe sich stattdessen die MAC-Adresse des WLAN-Nutzers, die aber kaum Rückverfolgungsmöglichkeiten bei Rechtsverstößen erlaubt, weil es – aus gutem Grund - keinerlei Verzeichnisse gibt, die eine Zuordnung der MAC-Adresse zu natürlichen Personen erlauben. Im Ergebnis muss daher von der Einrichtung frei zugänglicher WLAN-Hotspots, die unentgeltlich den Zugang zum Internet bereitstellen, abgeraten werden, weil die damit zusammenhängenden Rechtsfragen nach wie vor nicht ausreichend geklärt sind. Der Betrieb eines öffentlichen WLAN-Zugangs ohne stringente Protokollierung der Zugangsnutzung stellt in Deutschland ein unkalkulierbares Haftungsrisiko für den Betreiber – hier das Bezirksamt Hamburg-Nord - dar.

Gez. Dieter Carmesin