Schmidt et Schmidt
Rechtsanwälte

Offenes WLAN
Die rechtlichen Fallstricke und eine Darstellung der Haftungsfrage

Vorwort:

Wer ein offenes WLAN-Netz „betreiben will“, tut dieses in der Regel mit der Bereitschaft, Dritten (und somit der Öffentlichkeit) den Zugang über den eigenen Internetanschluss zu ermöglichen. Dieses zumeist nicht nur aus altruistischen, sondern auch oder gerade aus gewerblichen Interessen.

Er kann, um den Interessen gerecht zu werden, ein offenes WLAN-Netz „selbst“ oder aber durch einen Dritten betreiben lassen.

Der Dritte wiederum kann in seinem Auftrag oder aber eigenständig verantwortlich ein Netz betreiben.

Betreibt der Dritte das Netz eigenständig, so hat man als Anschlussinhaber lediglich dem Dritten seinen Internetzugang zur Nutzung eines offenen WLAN-Netzes zur Verfügung gestellt.

Dieses erfolgt zumeist in gesonderten schuldrechtlichen Vereinbarungen, die Elemente der Miete und der Gebrauchsüberlassung beinhalten und insgesamt als ein Mischvertrag anzusehen sein sollten.

Die eigentliche Verantwortung trifft in diesen Fällen den Nutzungsberechtigten. Die bestehende gesetzliche Vermutung, dass der Anschlussinhaber auch gleichzeitig der Verantwortliche ist, kann dadurch widerlegt werden.

Die folgenden Ausführungen behandeln jedoch vorrangig die Haftungs- und weiteren Rechtsfragen für die tatsächlichen Betreiber eines offenen Netzes (nur peripher werden die Haftungsfragen der Eigentümer/Nutzungsberechtigten, die den Internetanschluss Dritten zur Nutzung eines offenen Netzes überlassen, angesprochen):

1. Offenes WLAN—Netz (Fremdnutzung des Anschlusses)

Will man ein offenes WLAN-Netz betreiben, so ist zunächst zu klären, ob der jeweilige Internetanbieter jene „Fremdnutzung“, also den eigenen Anschluss für eine Mitnutzung durch Dritte freizugeben, erlaubt.

Das ist gesetzlich grundsätzlich nicht verboten, die Internetanbieter können es aber durchaus vertraglich ausschließen mit der Folge einer Kündigung der bestehenden Verträge.

So bedarf es zum Beispiel bei den einen Anbietern einer vorherigen schriftlichen Genehmigung, bei den anderen Anbietern hingegen darf kein Entgelt verlangt werden.

Insoweit ist man gut beraten, sich im Vorfelde und auch im Laufe der bestehenden vertraglichen Beziehung über die Bedingungen der einzelnen Internetanbieter zu informieren.

Ob das Fremdnutzungsverbot wirksam durch AGBs ausgeschlossen werden können, steht hierbei sicherlich noch unter einem anderen Stern. Gerade als gewerblicher Kunde eines Anschlusses sollte das Verbot keinesfalls zu einer Berufseinschränkung führen. Derartige Interessensabwägungen würden im Ergebnis sicherlich zugunsten des Kunden ausgehen.

Exkurs:
Will man nicht selbst seinen Anschluss nutzen, sondern seinen Internetanschluss einem Dritten zur Nutzung übergeben (vermieten/verpachten), gilt umso mehr die Frage zu klären, ob diese Fremdnutzung durch den jeweiligen Internetanbieter gewünscht und erlaubt ist. Doch auch hier müsste man im Zweifel zusätzlich unterscheiden, ob der Anschlussinhaber eine Privatperson oder ein Unternehmer ist.

2. Technisches

WLAN-Netzwerke funktionieren normalerweise in einer Art „Infrastruktur-Modus“:
Ein Router fungiert als zentrale Vermittlungsstelle. Er sendet ständig Datenpakete („Beacons“), die Geräten mit WLAN-Ausstattung signalisieren, dass ein WLAN-Netzwerk vorhanden ist. Die Beacons enthalten gewöhnlich auch den Namen des Netzwerks und ggf. die verwendete Verschlüsselung.

Empfängt ein Endgerät im Übertragungsbereich des Routers die Beacons, kann es sich mit dem Netzwerk verbinden, indem es seinerseits Datenpakete mit einer Verbindungsanfrage an den Router sendet. Der Router lässt die Verbindung dann entweder unmittelbar zu (offenes WLAN) oder fragt zunächst ein Kennwort ab (geschlossenes WLAN). Ist die Verbindung hergestellt, besteht ein lokales Netzwerk mit der Möglichkeit, zwischen allen Endgeräten, die eine Verbindung aufgebaut haben, miteinander zu kommunizieren.

WLAN-Netzwerke im Infrastrukturmodus sind technisch gesehen eigene Telekommunikationsnetzwerke.

Die meisten WLAN-Router bieten Anschlussmöglichkeiten für Ethernet-Kabel, mit denen eine Verbindung ins Internet hergestellt werden kann. Verbinden sich die angeschlossenen Endgeräte auf diese Weise ins Internet, übernimmt der WLAN-Router für diese Geräte die Funktion der Verbindung des WLAN-Netzwerkes mit dem Internet.

Technisch gesehen sind Anbieter von WLAN-Netzwerken daher zugleich auch Zugangsvermittler ins Internet.

Daran ändert sich auch nichts, wenn der Traffic über die AccessPoints durch einen VPN-Tunnel zu den Gateways des W-LAN-Anbieters (selbst oder durch Dritte) geleitet wird und damit technisch gesehen der AccessProvider dorthin verlagert wird.

3. Access-Provider und Genehmigungspflichten

Wer also die technische Struktur für den Internetzugang bereitstellt und Informationen aus dem Netz zum jeweiligen Internetnutzer durchleitet, sollte als ein Access-Provider auch rechtlich behandelt werden.

Access Provider sind Anbieter von Telekommunikationsdiensten; für sie gelten die Bestimmungen des Telekommunikationsgesetzes (TKG), aber auch Regelungen aus dem Telemediengesetz (TMG).

Wer ein solches Funknetz in Betrieb nimmt, braucht grundsätzlich hierzu keinerlei Genehmigung.

Nach den Vorgaben des TKG **kann** aber eine Mitteilung erforderlich sein, wenn es sich um ein „gewerbliches öffentliches Telekommunikationsnetz" handelt. In diesem Fall müsste es bei der Bundesnetzagentur angemeldet werden.

Ein freies Netz, das einer unbestimmten Nutzerzahl zur Verfügung stehen soll, ist unstreitig öffentlich.

Um darüber hinaus gewerblich zu sein, bzw. als gewerblich eingestuft zu werden, muss es nicht unbedingt mit der Absicht eingerichtet worden sein, einen Gewinn zu erzielen.

Es würde bereits genügen, dass ein Entgelt von den Nutzern erhoben wird, um allein die Betriebskosten zu decken. Unternehmer, die mit einem kostenlosen WLAN-Netz (Hot Spot), dem Kunden „Annehmlichkeiten" bieten wollen, handeln ebenso „gewerblich", da die Unterhaltung eines WLAN-Netzes in den Geschäftsräumen dem eigenen Geschäftsbetrieb förderlich ist.

4. Schutzunterrichtungen/-informationspflichten

Das Telekommunikationsgesetz (TKG) sieht einige technische Schutzmaßnahmen vor, die alle Anbieter von Telekommunikationsdiensten beachten müssen.

Sie dienen u.a. dem Schutz des Fernmeldegeheimnisses und personenbezogener Daten.

Bei offenen Netzen ist dieser Aspekt dann überschaubar, wenn vom WLAN-Betreiber keine oder auch nur kaum Nutzerdaten erfasst werden.

Für gewöhnlich speichert der Router bestimmte Daten, so dass dessen Administrator-Zugang durch ein sicheres Passwort geschützt sein sollte. Ebenso versteht es sich, dass die WLAN-Geräte selbst vor unbefugtem Zugriff durch Dritte geschützt werden.

Für Risiken, die sich daraus ergeben, dass die Nutzer ihre eigenen Daten nicht schützen können, ist der Anbieter des offenen Netzes und somit des Zugangs nicht verantwortlich. Aber:

Wer eine für die Öffentlichkeit bestimmte Telekommunikationsanlage betreibt, muss streng genommen bestimmte Maßnahmen treffen, um das Netzwerk vor Störungen, Angriffen und Katastrophen zu schützen.

Den TKG-Vorgaben entsprechend ist es verpflichtend, einen Sicherheitsbeauftragten zu benennen, ein passendes und geeignetes Sicherheitskonzept zu erstellen und der Bundesnetzagentur bei der Anmeldung vorzulegen.

Der Betreiber eines kleinen offenen Netzes wird hierbei sicherlich nicht unter den formalen Regelungen kapitulieren müssen, es ist aber sicherlich nicht verkehrt, ein vereinfachtes Konzept zu erarbeiten, das eine schematische Darstellung des Netzwerks sowie Angaben zu den eingesetzten Telekommunikationssystemen umfasst.

5. Haftung des offenen WLAN-Betreibers

Während eine strafrechtliche Verantwortung des WLAN-Betreibers für das Fehlverhalten von Nutzern allein aufgrund des bloßen Bereitstellens eines Zugangs ausgeschlossen ist, kann es mit möglichen zivilrechtlichen Ansprüchen anders aussehen:

Hier **kann** u.U. der Betreiber für das Verhalten eines dritten Nutzers haften. Um einen Schadensersatz wird es jedoch hierbei eher selten gehen; dafür müsste der WLAN-Betreiber selbst Täter oder Teilnehmer der begangenen Rechtsverletzung sein. Dieses ist er jedoch nicht allein durch das Vorhalten eines Zugangs.

Die derzeitige überwiegende Rechtsprechung macht jedoch dann eine Ausnahme, wenn es um die Frage der Unterlassungsansprüche geht. Hier kommt die sogenannte **Störerhaftung** ins Spiel.

Ein Störer ist jemand, der selbst nicht Täter ist, aber mit seinem Handeln dazu beiträgt, dass Rechtsverletzungen geschehen. Wer als Störer für eine Rechtsverletzung mitverantwortlich gemacht wird, haftet dann auf zumindest Beseitigung und (zukünftiger) Unterlassung.

Für Betreiber privater WLAN-Zugänge werden mittlerweile die folgenden Ansichten vertreten:

Ein Teil der Rechtsprechung geht davon aus, dass Prüfungspflichten verletzt werden, wenn „zumutbare Sicherungsmaßnahmen“ für den WLAN-Zugang unterlassen werden.

Diese bestünden in der Verschlüsselung des Zugangs und der Vergabe von Benutzerkonten (OLG Düsseldorf ZUM-RD 2008, 170). Es sei auch zumutbar, zur Sicherung fachkundige Hilfe in Anspruch zu nehmen (LG Hamburg JurPC Web-Dok 6/2008, bestätigt durch OLG Hamburg, Beschluss vom 21. 11. 2006, AZ 5 W 171/06).
Ein Teil der Literatur unterstützt diese Ansicht (Stang/Hühner GRUR RR 2008, 273; Mühlberger GRUR 2009, 1022).

Das OLG Frankfurt sieht hingegen eine Störerhaftung privater WLAN-Betreiber nicht als gegeben an, so lange keine konkreten Hinweise auf einen Missbrauch den Zugangs bestünden, ansonsten würde die Prüfungspflichten ins Unzumutbare überspannt (ZUM-RD 2009, 68).

Der BGH hat das Urteil des OLG Frankfurt aufgehoben. Auch privaten WLAN-Betreibern sei es zuzumuten zu prüfen, ob der Zugang durch angemessene Sicherheitsmaßnahmen dagegen geschützt ist, dass Dritte ihn für Schutzrechtsverletzungen missbrauchen. Es seien daher die beim Kauf des Routers marktüblichen Sicherungen zu aktivieren und ein persönliches Kennwort zu verwenden (GRUR 2010, 633–„Sommer unseres Lebens“). Das OLG Frankfurt ist dem BGH nach Zurückverweisung gefolgt (MMR 2011, 420).

Zu den Prüfungspflichten der Betreiber „professionell“ betriebene WLANs werden folgende Ansichten vertreten:

Das LG Hamburg hat in einer einstweiligen Verfügung ausgeführt, der Betreiber eines Internetcafes mit WLAN hafte als Störer, wenn er keine Maßnahmen wie etwa Portsperren ergreift, um Filesharing zu verhindern (K&R 2011, 215) Das LG Frankfurt hat die Ansicht vertreten, jedenfalls bei einer Verschlüsselung des WLAN hafte ein Hotelier nicht für Urheberrechtsverletzungen seiner Gäste (ZUM RD 2011, 371). Diese Ansicht findet auch in der Literatur Zustimmung (Füglein Lagadère MMR-Aktuell 2013, 341464; Schmidt-Bens/Suhren K&R 2013, 1).

Kaeding vertritt die Ansicht, bereits vor Kenntnis von Rechtsverletzungen sei eine Registrierungspflicht für die Nutzer zumutbar und geeignet, um Missbrauch einzudämmen. Ferner sei es angezeigt, in den Nutzungsbedingungen missbräuchliche Nutzung zu untersagen. Nach Kenntnis von Rechtsverletzungen müssten diese künftig verhindert werden, etwa durch Sperren von IP-Adressen oder Filter (CR 2010, 164). Gietl vertritt die Ansicht, eine Haftung komme erst nach Kenntnis von Rechtsverletzungen in Betracht. Auch dann seien Maßnahmen zur Verhinderung von Rechtsverletzungen zumeist unzumutbar. Sperrungen seien wegen Verstoßes gegen das Fernmeldegeheimnis nach §88 TKG unzulässig (MMR 2007, 630).

Dagegen halten der Großteil der Literatur die Handlungspflichten für kommerzielle WLAN-Betreiber in jedem Fall für unzumutbar:

Der Ausschluss von Benutzern sei unzumutbar, da diese zu Wettbewerbern abwandern würden. Filterpflichten seien ungeeignet, da jeweils nur bestimmte Ports gesperrt werden könnten, Filesharing aber über alle Ports möglich sei (Breyer, NJOZ 2010, 1085; Manz, JurPCWeb-Dok 95/2010; Feldmann K&R 2011, 225). Darüber hinaus dürften bei einem von der Rechtsordnung gebilligten Geschäftsmodell dem Diensteanbieter keine Kontrollmaßnahmen auferlegt werden, die sein Geschäftsmodell gefährden (Ungern-Sternberg GRUR 2012, 321; Kirchberg ZUM 2012, 544).

In der Tat würde eine Pflicht zur Verschlüsselung das Geschäftsmodell von Internetcafes erheblich einschränken, wenn nicht unmöglich machen (so Spindler CR 2010, 592).

Ein solcher Eingriff in das Grundrecht der Gewerbefreiheit bedürfte einer eindeutigen gesetzlichen Grundlage, die das Urheberrecht alleine nicht bieten kann.

Die Frage der Haftung professioneller WLAN-Betreiber ist aber noch nicht höchstrichterlich entschieden.

Ein Anbieter eines offenen WLAN-Netzes vermittelt lediglich den Zugang zum Internet, wenn über das drahtlose Netz eine Verbindung zum Internet besteht (Hoeren/Sieber-Sieber/Hoefinger, Teil 18.1 RN 64; Beck'scher Kommentar–Jandt, § 8 TMG RN 12). Gleiches gilt auch für den Betreiber eines Internetcafés. Dass dort in der Regel auch Hardware zur Verfügung gestellt wird, ändert daran nichts (Hoeren/Sieber-Sieber/Hoefinger, Teil 18.1 RN 64; Jandt aaO. RN 13). Dabei werden weder Adressaten noch Informationen ausgewählt, dies erfolgt ausschließlich durch die Endnutzer (Redeker ITRB 2011, 186).

Der „Ruf“ dem kommerziellen WLAN-Betreiber als Access-Provider nicht nur technisch sondern auch rechtlich endgültig zu sehen, ist lauter geworden.

§ 8 TMG ist daher nach einhelliger Meinung der Literatur grundsätzlich anwendbar.

Alle von Rechtsprechung und Literatur diskutierten Maßnahmen bedeuten jedoch einen Konflikt mit den Grundrechten des Betreibers und seiner Kunden:

Eine Verschlüsselung des Zugangs beschneidet für Internetcafe-Betreiber bereits die Werbefunktion, da nur Personen das WLAN benutzen können, die bereits Kunden sind. Eine Weitergabe des Kennwortes an die Kunden ermöglicht jedoch Urheberrechtsverletzungen. Eine Kennungsvergabe an die jeweiligen Benutzer würde nur dann einen Sinn machen, wenn die Benutzer auch überwacht und bei Verstößen die Kennungen gesperrt werden. Eine Überwachung kann jedoch dem Gewerbetreibenden, der ein Hot Spot unterhalten will, nicht zugemutet werden. Eine Portsperre, wie vom LG Hamburg vorgeschlagen, ergibt nur Sinn, wenn der Betreiber weiß, über welche Ports die Kunden Rechtsverletzungen, wie zum Beispiel Filesharing betreiben.

Ohne eine solche Benutzerüberwachung wären weder eine Verschlüsselung, noch eine Portsperre wirkungsvoll. Wirkungslose Eingriffe können jedoch im Rahmen der Störerhaftung niemals zumutbar sein (so ausdrücklich LG Hamburg ZUM 2010, 902).

Es stellt sich daher die Frage, ob eine solche Überwachung der Benutzer nicht in die Rechte oder die Grundrechte der Benutzer eingreifen würde. Davon dürfte auszugehen sein.

Nach der Rechtsprechung des BGH haftet der WLAN-Betreiber als Anschlussinhaber nicht unmittelbar als Täter, es besteht jedoch eine widerlegliche Vermutung, dass er der Täter ist. Er kann und sollte die tatsächliche Vermutung der Täterschaft jedoch bereits durch den Vortrag entkräften (können), dass er in seiner Betriebsstätte ein offenes WLAN betreibt. Denn in solchen Fällen erscheint es eher fernliegend, dass das Netz hauptsächlich vom Gaststättenbetreiber selbst genutzt wird (Manz MMR 2011, 401). Die alltägliche Erfahrung in einer Gesellschaft, in der das Internet einen immer größeren Anteil einnimmt und nicht mehr wegzudenken ist, belegt vielmehr das Gegenteil einer Vermutung. (vgl. OLG Hamm, Beschluss v. 27.10.2011, I-22 W 82/11; OLG Hamm, Beschluss v. 04.11.2013, I-22 W 60/13; OLG Köln NJW-RR 2012, 1327; AG Hamburg, Urteil v. 30.10.2013, 31 C 20/13; AG Mün-chen, Urteil v. 31.10.2013, 155 C 9298/13). Die Beweislast für die Täterschaft liegt dann wieder beim Verletzten (LG München ZUM 2013, 538).

Derzeit macht sich ein kleiner Wandel in der Rechtsprechung bemerkbar:
Die unteren Gerichte beginnen, den offenen WLAN-Betreiber als Access-Provider einzustufen (vgl. etwa AG Hamburg, es 2014, 536; AG Charlottenburg, Beschluss vom 17.12.2014, Az. 217 C 121/14; Roggenkamp, jurisPR-ITR 12/2006 Anm. 3; Röhrborn/Katko, ca 2002, 882, 887).

Dieser ist als anerkannter Access-Provider für fremde Informationen grundsätzlich nicht verantwortlich und deshalb auch nicht verpflichtet, Nutzer oder Kunden zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen.
Der lediglich den Zugang zu fremden Informationen eröffnende Provider haftet nicht, wenn er die Übermittlung nicht veranlasst, den Adressaten nicht ausgewählt und die übermittelten Informationen weder ausgewählt noch verändert hat.

Unberührt von dieser Privilegierung der bloßen Durchleitung von Informationen bleibt der Access-Provider zur Entfernung oder Sperrung der Nutzung von Informationen nach den allgemeinen Gesetzen nur verpflichtet, wenn er Kenntnis von rechtswidrigem Tun erlangt hat (vgl. auch LG Flensburg, Urt. v. 25.11.2005 - 6 0 108/05).

Diese Privilegierung erstreckt sich jedoch nicht auf Unterlassungsansprüche, d.h. auf die Haftung des Störers (BGHZ 158, 236 - Rolex).

In derartigen Fällen sind allerdings an die Zumutbarkeit von Maßnahmen und Pflichten ganz besonders strenge Anforderungen zu stellen; dem Betreiber eines WLAN-Netzwerkes darf nichts abverlangt werden, was sein “Geschäftsmodell” gefährdet. Das wäre jedenfalls bei schweren Eingriffen, etwa Port- oder DNS--Sperren, Registrierungspflichten etc. der Fall (vgl. auch Sassenberg/Mantz, WLAN und Recht, Rdn. 227 ff.). Eine Pflicht zur Belehrung kann nicht verlangt werden und erscheint bei einem klassischen Hot-Spot-Modell nicht praktikabel (vgl. AG Hamburg a.a.O.; Sassen-berg/Mantz a.a.O., Rdn. 235; so wohl auch Hoeren/Jakopp, ZRP 2014,72, 75).

Ohne einen konkreten Anlass für die Annahme, dass Nutzer Rechte Dritter im Rahmen der Nutzung des Internetzugangs verletzen, ist dem offenen WLAN-Betreiber eine ständige Überwachung nicht zumutbar (vgl. etwa LG Mannheim, Urt. v. 29.09.2006 - 7 0 62/06).

Fazit:
Die Stimmen der Literatur hatten den Betrieb eines offenen WLAN als förderndes Geschäftsmodell stets die Privilegierung eines Access-Providers gefordert.

Höchstrichterlich gab und gibt es jedoch noch keine Entscheidungen und die Prüfpflichten, die der BGH den privaten WLAN-Besitzern auferlegte, können nicht auf die Geschäftsmodelle professionell betriebener WLAN-Hot-Spots gestülpt werden.

Eine klare gesetzliche Regelung war geschuldet. Nunmehr mehren sich jedoch die Spruchkörper der kleinen Amtsgerichte, die die Stimmen der Literatur folgend und den Geist der Zeit erkennend, das Geschäftsmodell der offenen WLAN-Netze den rechtlichen Status eines Access-Providers zuerkennen wollen, mit den dadurch sich ergebenden Haftungsprivilegierungen und zumutbaren Prüf- und Handlungspflichten.
Es ist davon auszugehen, dass dieser Wandel Bestand haben und auch durch die nächsten Instanzen aufgegriffen und gefestigt wird.
Die Haftung des Anschlussinhabers, der ein offenes WLAN-Netz betreibt und/oder betreiben lässt, wird sich auf die Privilegierungen des TMG berufen können. Eine Haftung würde nur dann entstehen, wenn er trotz Kenntnis der konkreten Verletzungen untätig bleibt.