LG Hamburg: Störerhaftung bei ungesichertem Funknetz

UrhG § 97 Abs. 1 Satz 1; BGB § 1004
Urteil vom 26.7.2006 – 308 O 407/06; nicht rechtskräftig

Leitsätze der Redaktion

1. Wer ein nicht gesichertes WLAN-Funknetz mit Internetzugang betreibt, haftet als Störer für über das Funknetz durch Unbekannte begangene Urheberrechtsverletzungen.

2. Den Betreiber eines Funknetzes trifft die Pflicht, dieses abzusichern.

3. Zur Abwendung der Wiederholungsgefahr reicht es nicht aus, nach der Mahnung einen Passwortschutz einzurichten.

Anm. d. Red.: Die Entscheidung wurde mitgeteilt und die Leitsätze wurden verfasst von Wiss. Mitarb. *Reto Mantz*, Universität Göttingen. Die Berufung ist beim *OLG Hamburg* unter dem Az. 5 U 163/06 anhängig.

Sachverhalt

Gegenstand des Verfahrens ist ein Unterlassungsbegehren der Ast. gegen die Ag. wegen der öffentlichen Zugänglichmachung von Musikaufnahmen in einem Filesharing-System über den Internetanschluss der Ag. Die Ast. ist Tonträgerherstellerin. Am 29.12.2005 wurde festgestellt, dass unter der IP-Adresse xxx insgesamt 244 Audiodateien mittels einer Filesharing-Software, die auf dem Gnutella-Protokoll basiert, zum Kopieren und Hören vorgehalten wurden, darunter Dateien mit den Musikaufnahmen „der Künstlergruppe" XXX. Die IP-Adresse war zum streitgegenständlichen Zeitpunkt den Ag. zugeordnet. Die Ast. hat eine solche Nutzung ihrer Aufnahmen nicht gestattet.

Die Ag. sind der Auffassung, nicht Täter der Rechtsverletzung zu sein und sich die Verletzung auch nicht als Störer zurechnen lassen zu müssen. Die streitgegenständliche Urheberrechtsverletzung sei nicht über einen der zwei in ihrem Haushalt befindlichen Computer erfolgt. Weder sie selbst noch ihr Sohn hätten die o.g. Musikaufnahmen auf ihren Computern zum Abruf durch andere Teilnehmer von Filesharing-Systemen bereitgestellt. Sie hätten vielmehr eine nicht durch ein Geheimwort geschützte schnurlose Funkverbindung, eine sog. „WLAN"-Internetverbindung genutzt. Die streitgegenständliche Nutzung durch Dritte sei möglich. Sie hätten dann unverzüglich einen Passwortschutz einrichten lassen. Eine Prüfpflicht habe nicht bestanden. Die Ast. trägt vor, sie besitze die ausschließlichen Verwertungsrechte an den streitgegenständlichen Musikaufnahmen. Sie ist der Auffassung, dass die Ag. als Störer haften. Es sei nur eine Schutzbehauptung, dass die streitgegenständliche Nutzung durch Dritte über die ungeschützte WLAN-Internetverbindung erfolgt sei.

Aus den Gründen

... Die Ast. hat gegen die Ag. einen Anspruch aus § 97 Abs. 1 Satz 1 UrhG auf Unterlassung der öffentlichen Zugänglichmachung der streitgegenständlichen Musikaufnahmen in einem Filesharing-System.

1. Die Ast. ist Inhaberin der Tonträgerherstellerrechte aus § 85 Abs. 1 UrhG. Ihr steht danach u.a. das ausschließliche Recht zur öffentlichen Zugänglichmachung der Aufnahme zu. Die Ast. hat die Rechtekette nachvollziehbar dargestellt und durch die eidesstattliche Versicherung des XXX glaubhaft gemacht. ...

2. Dieses Recht ist widerrechtlich verletzt worden, indem die Aufnahme über den Internetanschluss der Ag. über ein Filesharing-System im Internet zum Kopieren und Anhören bereitgestellt und damit der Öffentlichkeit zugänglich gemacht worden war, ohne dass dazu eine Rechtseinräumung durch die Ast. vorlag.

3. Die Ag. haben für diese Rechtsverletzungen einzustehen. Zwar konnte weder festgestellt werden, dass sie selbst die Rechtsverletzung begangen haben, noch konnte es durch die Vorlage der eidesstattlichen Versicherung ausgeschlossen werden. Denn die eidesstattliche Versicherung sagt nichts dazu aus, ob die Ag. persönlich zum streitgegenständlichen Zeitpunkt die Rechtsverletzung begangen haben, da sie sich auf eine erst am 20.3.2006 erfolgte Überprüfung bezieht. Auch XXX kann letztendlich nur vermuten, wie seine Eltern, die Ag., den Internetanschluss genutzt haben. Es ist aber nicht auszuschließen, dass die Rechtsverletzungen durch andere nicht bekannte Nutzer

des Anschlusses erfolgt sind, die die ungeschützte WLAN-Internetverbindung der Ag. genutzt haben.

Ob die Ag. die Rechtsverletzungen selbst begangen haben oder ob die Rechtsverletzungen auf Grund einer Nutzung der ungeschützten WLAN-Internetverbindung durch Dritte erfolgten, kann aber dahinstehen. Denn die Ag. haben für diese Rechtsverletzung jedenfalls nach den Grundsätzen der Störerhaftung einzustehen.

a) I.R.d. Unterlassungsanspruchs haftet in entsprechender Anwendung des § 1004 BGB jeder als Störer für eine Schutzrechtsverletzung, der – ohne selbst Täter oder Teilnehmer zu sein – in irgendeiner Weise willentlich und adäquat kausal an der rechtswidrigen Beeinträchtigung mitgewirkt hat. Um eine solche Haftung nicht über Gebühr auf Dritte zu erstrecken, die nicht selbst die rechtswidrige Beeinträchtigung vorgenommen haben, setzt die Haftung des Störers die Verletzung von Prüfungspflichten voraus. Deren Umfang bestimmt sich danach, ob und inwieweit dem als Störer in Anspruch Genommenen nach den Umständen eine Prüfung zuzumuten ist (*BGH* GRUR 2004, 860 ff., 864 [= MMR 2004, 668 m. Anm. *Hoeren*] – Störerhaftung des Internetauktionshauses bei Fremdversteigerung – m.w.Nw.), wobei sich die Art und der Umfang der gebotenen Prüf- und Kontrollmaßnahmen nach Treu und Glauben bestimmen (*v. Wolff*, in: Wandtke/Bullinger, a.a.O., § 97 Rdnr. 15). So hat sich auch die Verpflichtung, geeignete Vorkehrungen zu treffen, durch welche die Rechtsverletzungen so weit wie möglich verhindert werden, i.R.d. Zumutbaren und Erforderlichen zu halten (*BGH* GRUR 1984, 54, 55 – Kopierläden).

b) Unter Anwendung dieser Grundsätze haften die Ag. als Störer. Wenn die Ag. es Dritten auf Grund einer ungeschützten WLAN-Verbindung ermöglicht haben, ihren Internetzugang zu nutzen und die streitgegenständliche Rechtsverletzung zu begehen, dann ist dies adäquat kausal für die Schutzrechtsverletzung gewesen. Adäquat ist eine Bedingung dann, wenn das Ereignis im Allgemeinen und nicht nur unter besonders eigenartigen, unwahrscheinlichen und nach dem gewöhnlichen Verlauf der Dinge außer Betracht zu lassenden Umständen geeignet ist, einen Erfolg der fraglichen Art herbeizuführen (*BGH* NJW 2005, 1420 ff., 1421 m.w.Nw.). Davon ausgehend ist eine Adäquanz hier zu bejahen.

Zunächst haben Rechtsverletzungen über das Internet allgemein zugenommen durch das Herunterladen und öffentliche Zugänglichmachung insb. urheberrechtlich, geschmacksmusterrechtlich und markenrechtlich geschützter Leistungen. Darunter fallen auch die Aneignung und das Bereitstellen von Musikaufnahmen im Internet über Peer-to-Peer-Dienste und mit Hilfe von Filesharing-Software, verharmlosend „Tauschbörsen" genannt. Jedenfalls seit dem Auftreten der Filesharing-Software „Napster" im Herbst 1999 ist Derartiges auch nicht mehr ungewöhnlich, sondern wird gerade von Kindern, Jugendlichen und jungen Erwachsenen vielfältig in Anspruch genommen. Weiter ist allgemein bekannt, dass ungeschützte WLAN-Verbindungen von Dritten missbraucht werden können, um über einen fremden Internetanschluss ins Internet zu gelangen.

Die Verwendung einer ungeschützten WLAN-Verbindung für den Zugang ins Internet birgt danach die keinesfalls unwahrscheinliche Möglichkeit, dass von – unbekannten – Dritten, die die ungeschützte Verbindung nutzen, solche Rechtsverletzungen begangen werden. Das löst Prüf- und ggf. Handlungspflichten aus, um der Möglichkeit solcher Rechtsverletzungen vorzubeugen. Rechtlich und tatsächlich sind die Ag. in die Lage versetzt gewesen, wirksame Maßnahmen zur Verhinderung der streitgegenständlichen Rechtsverletzung zu treffen. Hier haben die Ag. aber nach eigenem Eingeständnis keine Schutzmaßnahmen getroffen mit der Begründung, sie seien sich der Missbrauchsmöglichkeiten nicht bewusst gewesen. Weder das fehlende technische Verständnis noch die eigene Unkenntnis von der Möglichkeit der illegalen Musiknutzung über leicht zu installierende Tauschbörsenprogramme sowie von der Möglichkeit der Nutzung einer WLAN-Verbindung durch unbefugte Dritte entlasten sie. Es hätte ihnen oblegen, sich zu informieren, welche Möglichkeiten für Rechtsverletzungen sie schaffen und wie sie solchen Verletzungen hätten vorbeugen können. Zudem hätten sie technische Möglichkeiten in Anspruch nehmen können, um die streitgegenständliche Rechtsverletzung zu verhindern. So hätten sie etwa einen Passwortschutz einrichten können. Eine derartig ihnen mögliche Maßnahme haben die Ag. jedoch nicht ergriffen, sondern die WLAN-Verbindung „ungeschützt" genutzt.

Die Durchführung der vorgenannten Maßnahmen ist zumutbar. Das gilt auch für den Fall, dass die Ag. selbst nicht in der Lage sein sollten, sie einzurichten und sich dazu entgeltlicher fachkundiger Hilfe bedienen müssten. Den dadurch bedingten Geldaufwand erachtet die *Kammer* als durchaus noch verhältnismäßig.

4. Die danach den Ag. zurechenbare widerrechtliche Nutzung begründet die Vermutung einer Wiederholungsgefahr. Zur Ausräumung dieser Vermutung wäre neben einer Einstellung der Nutzung die Abgabe einer ernsthaften, unbefristeten, vorbehaltlosen und hinreichend strafbewehrten Unterlassungsverpflichtungserklärung erforderlich gewesen (vgl. Möhring/Nicolini/*Lütje*, UrhG, 2. Aufl., § 97 Rdnr. 120, 125; Schricker/*Wild*, Urheberrecht, 2. Aufl., § 97 Rdnr. 42; *Schulze/Dreier*, UrhG, 2. Aufl., § 97 Rdnr. 41, 42; *v. Wolff*, in: Wandtke/Bullinger, Urheberrecht, 2. Aufl., § 97 Rdnr. 34, 35), wie sie erfolglos verlangt worden ist. Allein das Einrichten eines Passwortschutzes nach einer bereits erfolgten Rechtsverletzung reicht nicht aus. ...

Anmerkung

Das *LG Hamburg* musste sich – soweit ersichtlich – als erstes Gericht mit einem Fall beschäftigen, der auch in der rechtswissenschaftlichen Lit. in dieser Form noch nicht betrachtet wurde. Mehrfach ist über das sog. Wardriving, also die Nutzung fremder offener Funknetze ohne Einwilligung des Inhabers durch einen Dritten, berichtet worden. Auch Aufsätze über die strafrechtliche oder zivilrechtliche Verantwortlichkeit des Dritten existieren bereits. Außer Acht gelassen wurde allerdings meist, welche Folgen die Nutzung eines offenen Netzes für den Betreiber haben kann, bzw. die Störerhaftung allgemein (so z.B. *Heidrich*, c't 13/2004, 102).

Das Problem ist zunächst technischer Natur. Wenn ein Internetnutzer sich im Internet bewegt, so ist er grds. über seine IP-Adresse identifizierbar. Wer also wie im vorliegenden Fall urheberrechtlich geschützte Werke über ein Filesharing-Programm anbietet, der ist mitnichten anonym. Mittels des Schlüssels aus IP-Adresse und Nutzungszeit kann, sofern der Provider diese Daten gespeichert hat, der Nutzer festgestellt und damit auch verfolgt werden. Mit der zunehmenden Verbreitung von Netzwerken und speziell Funknetzwerken kommt hier allerdings eine weitere Ebene zum Tragen. Da sich häufig mehrere

Personen ein Netzwerk teilen, über das Internet aber unter nur einer IP-Adresse auftreten, ist unmittelbar nicht mehr der Nutzer selbst, sondern nur noch der Anschlussinhaber feststellbar. Während bei Haus- oder Wohngemeinschaften der potentielle Verletzerkreis relativ klein ist, eröffnen offene bzw. ungeschützte Funknetze einen hohen Grad an Anonymität für den Rechtsverletzer. Sofern der Betreiber des Funknetzes keine Daten speichert, kann er den unberechtigten Nutzer auch selbst kaum identifizieren. Zudem sind Daten wie die MAC-Adresse einer Netzwerkkarte zur Identifikation kaum geeignet, persönliche Daten dürften schon auf Grund von Datenschutzbestimmungen nicht erfasst und gespeichert werden.

Für den Geschädigten bleibt also nur noch, den Intermediär, also den Betreiber des Funknetzwerkes, zu belangen. Dabei ist der Betreiber eines – auch privaten – Funknetzes mit Internetzugang durchaus als Access-Provider i.S.d. § 3 Nr. 1 TDG anzusehen und ist folglich nach § 9 TDG privilegiert (*Spindler*, in: Spindler/Schmitz/Geis, TDG, vor § 8 TDG Rdnr. 21; § 9 TDG Rdnr. 14). Diese Privilegierung wirkt jedoch nach der Rspr. des *BGH* gerade nicht in die Störerhaftung hinein (*BGH* MMR 2004, 668 – Rolex), sodass auf diesem Wege durchaus ein Risiko des Betreibers bestehen kann.

Das *Gericht* hat anlässlich des Falls ausgeführt, dass der Betreiber eines ungesicherten Funknetzes adäquat kausal an der Rechtsverletzung mitwirkt, selbst wenn die eigentliche Rechtsverletzung nachweislich durch einen unbekannten Dritten erfolgt ist. Mit der Gewährung des Zugangs zum Internet setzt der Betreiber zweifelsfrei eine äquivalent kausale Bedingung. Die Frage der Adäquanz begründet das Gericht ausführlich und auch zutreffend. Tatsächlich wurde bereits mehrfach und in allgemein empfangbaren Medien über die Problematik der Tauschbörsen und damit zusammenhängende Urheberrechtsverletzungen berichtet, sodass auch bei einem Durchschnittsnutzer von einer entsprechenden Kenntnis auszugehen ist. Darüber hinaus ist auch das Problem der ungesicherten Funknetze sowie die Möglichkeit der Einrichtung eines Passwortschutzes vielfach thematisiert worden. Das *Gericht* spricht hier von einem bekannten möglichen Missbrauch. Was es außer Acht lässt, ist, dass die Nutzung eines fremden Netzes nicht zwangsläufig als Missbrauch anzusehen ist. So ist die „normale" Internetnutzung eines Dritten über ein ungesichertes Funknetz meist strafrechtlich nicht relevant (vgl. *Buermeyer*, HRRS 2004, 285, 292; *Bär*, MMR 2004, 434, 441). Auch zivilrechtlich stehen dem Betreiber lediglich Unterlassungsansprüche nach §§ 906 und 862 BGB sowie evtl. bereicherungsrechtliche Ansprüche zu (*Gietl*, DuD 2006, 37 ff.). Es stellt sich zudem die Frage, ob das Offenlassen eines ungesicherten Funknetzes im Wege der Auslegung nach dem Empfängerhorizont entsprechend §§ 133, 157 BGB nicht sogar als Einwilligung zur Nutzung zu werten sein könnte. Weiter existieren freie Netzprojekte, bei denen bewusst auf Sicherungsmaßnahmen, die über eine weitgehend anonyme oder pseudonyme Anmeldung hinausgehen, verzichtet wird (so z.B. Freifunk in Berlin, http://www.freifunk.net). Dort sollen Dritte gerade unkompliziert – auch in sozialer Hinsicht – Teilnehmer des Netzwerks werden können. Dennoch kann man mit den Ausführungen des *Gerichts* durchaus davon ausgehen, dass sich der Betreiber eines ungesicherten Funknetzes der Möglichkeit der Nutzung durch Dritte bewusst ist bzw. bewusst sein müsste, zumal er selbst bei der eigenen Nutzung durch die Einrichtung eines ungesicherten Netzes keinerlei weitere Einstellungen für die Nutzung mehr vornehmen musste.

Knackpunkt der Entscheidung ist deshalb, inwieweit den Betreiber Handlungspflichten zur Sicherung des Netzwerks treffen. Wer als potenzieller Störer eine Gefahrenquelle schafft und beherrscht, dem sind i.R.d. Zumutbaren durchaus auch Sicherungsmaßnahmen zum Schutz gefährdeter Dritter aufzubürden (*BGH* GRUR 1984, 54, 55 – Kopierläden; *Spindler*, a.a.O., vor § 8 TDG Rdnr. 45). Ohne spezielle Maßnahmen zu nennen – verlangt werden nur „wirksame Maßnahmen" –, geht das *Gericht* davon aus, dass jedenfalls der vollständig ungeschützte Betrieb eines Netzes, also das Nichtergreifen jeglicher Maßnahmen die Störerhaftung zu begründen vermag. Die wohl einfachste ergreifbare Maßnahme, die auch die Betroffenen nach der einstweiligen Verfügung gewählt haben, ist die Einrichtung eines Passwortschutzes. Hierfür ist die Lektüre der Anleitung eines WLAN-Routers notwendig, aber im Normalfall auch ausreichend. Die vom *Gericht* als zumutbar bezeichnete kostenpflichtige Herbeiziehung eines Experten dürfte dementsprechend nur in den seltensten Fällen notwendig werden. Zwar gibt es auch beim Passwortschutz verschiedene unterschiedlich wirksame Methoden, hier reicht aber bereits die einfachste Möglichkeit aus. So kann der technisch kundige Nutzer unter Einsatz von frei verfügbaren Programmen z.B. den Passwortschutz des Wired Equivalent Privacy-Protokoll (WEP) brechen, begibt sich aber in den Bereich der strafrechtlich relevanten Haftung (*Buermeyer*, HRRS 2004, 285, 287; *Bär*, MMR 2004, 434, 437 f.; *Ernst*, CR 2003, 898, 899 ff.; *Dornseif/Schumann/Klein*, DuD 2002, 1, 4). Trotz der relativen Unsicherheit dieser Methode genügt sie als wesentliche Zugangshürde bereits den Handlungspflichten, zumal der Tatsache der Unsicherheit der WEP-Verschlüsselung noch nicht derselbe Bekanntheitsgrad wie der Unsicherheit eines ungesicherten Netzes zuzumessen ist. Hier stellt sich bei einem Einbruch anschließend nur die Problematik des Beweises, dass das Netz gesichert war. Wer sein Netz ohne Passwort betreiben möchte, der kann auch andere, technisch erheblich anspruchsvollere Alternativen ergreifen. So könnte der Betreiber zwar den Zugang ohne Passwort gewähren, aber bestimmte Rechtsverletzungsmöglichkeiten verhindern. Für Tauschbörsen typische Verbindungen könnten unterbunden werden, indem entsprechende Ports gesperrt werden. Allerdings ist auch dieser Schutz bei weitem kein absolutes Hindernis. Des Weiteren hilft er nicht gegen Verletzungen, die nicht durch Verbreitung von urheberrechtlich geschütztem Material begangen werden, wie z.B. Persönlichkeitsrechtsverletzungen oder den Versand von Spam-Mails. Schließlich ist auch eine personalisierte Nutzung, also nur nach vorheriger Anmeldung, denkbar. Daran schlösse sich aber die Frage an, inwieweit der Betreiber die eindeutige Identifikation des Nutzers sicherstellen muss, um diese Vorkehrung als wirksame Maßnahme zu bezeichnen. Vor genau diesem Problem stehen selbstverständlich auch kommerzielle Hotspot-Betreiber.

Die Handlungspflichten des Betreibers decken sich mit der Haftung nach § 823 Abs. 1 BGB wegen der Verletzung von entsprechenden Verkehrssicherungspflichten (*BGH* NJW-RR 2001, 1208; *BGH* NJW 1995, 2633, 2634). Auch dort ist die Eröffnung einer Gefahrenquelle, nämlich hier des anonym nutzbaren Internetzugangs, Anknüpfungspunkt für die Herleitung von Handlungspflichten. Mit Schadensersatzforderungen hat der Betreiber allerdings wegen der Privilegierung des § 9 TDG

nicht zu rechnen. Nichtsdestotrotz ergibt sich durch die Störerhaftung bei Betrieb eines Funknetzes ein erhebliches Prozess- und Kostenrisiko. Den Betreiber trifft demnach ein hohes Maß an Eigenverantwortung (ebenso *Sury*, Informatik-Spektrum 2005, 504, 505 f.; *Heidrich*, c't 20/2006, 52).

Wichtig ist weiter, dass es nach Bekanntwerden der Verletzung und einer entsprechenden einstweiligen Verfügung nicht ausreicht, ab diesem Zeitpunkt den ungesicherten Betrieb einzustellen. Notwendig ist die Abgabe einer ernsthaften und hinreichend strafbewehrten Unterlassungserklärung (Palandt/*Bassenge*, § 1004 Rdnr. 32).

Privatleute und Unternehmen, die Netzwerke betreiben, müssen nach der festgestellten Rechtslage also nicht nur aus dem Interesse des Schutzes der eigenen Anlagen oder Daten Sicherheitsmaßnahmen ergreifen, sondern sind vielmehr auch Dritten gegenüber in der Pflicht. Während die Haftung bei ihnen durch die Sicherung vermieden werden kann, könnte das Urteil zu erheblichen Umwälzungen im Bereich der freien Netzprojekte führen. Bei diesen wird meist ein offener und nach Möglichkeit auch unbeschränkter Zugang gewährt. Die häufig auf der Ad-hoc-Struktur, also der Vermaschung von Funkzellen, basierenden Netzwerke sollen bzw. wollen möglichst viele Nutzer einbinden. Technische Hürden und Sicherungsmaßnahmen laufen diesem Ziel grundlegend zuwider. Der Internetzugang ist bei solchen Projekten nicht Hauptmotiv, aber häufig ein wesentlicher Grund für viele Teilnehmende. Rechtsverletzungen und Missbräuche sollen nach der Meinung vieler Aktiver soweit möglich durch soziale Kontrolle, nicht durch technische Restriktionen, vermieden werden. Beim Projekt Wireless Weimar (http://wireless.subsignal.org) beispielsweise benötigt man Kontakte zu anderen Teilnehmern, bevor die Nutzung ermöglicht wird. Das dargestellte Risiko tragen in diesen Netzen also diejenigen, deren Anlagen als Gateway ins Internet fungieren, sie sind potenzielle Störer nach § 1004 BGB.

Zur Teilnahme an freien Netzen ist häufig die Verwendung von spezieller Software wie z.B. einer Implementierung des OLSR-Protokolls sowie spezieller Einstellungen nötig. Die Software ist aber gerade frei verfügbar. Die Notwendigkeit der Installation und Einrichtung allein kann deshalb nicht als ausreichend wirksame Sicherungsmaßnahme gelten, um eine Haftung auszuschließen.

Es bleibt zu hoffen, dass Rechtsverletzungen aus diesen Netzen ausbleiben bzw. durch soziale Gegensteuerung unterbunden werden. Eventuell werden auch gemeinschaftliche Spendentöpfe gebildet, um den betroffenen Gateway-Betreibern im Falle eines Falles wenigstens finanzielle Sicherheit zu bieten. Alternative wäre das Erfordernis einer Anmeldung oder die weitgehende technische Sicherung, die aber nur gegen bestimmte Formen der Rechtsverletzung wirkt. Beides könnte die Entwicklung der hoch-dynamischen freien Netzwerke negativ beeinträchtigen.

Wiss. Mitarb. Reto Mantz, Universität Göttingen.