NJW-aktuell

Heft 23/2010, S. 12

Standpunkt

Pflicht zur Sicherung privater WLAN-Anschlüsse Ende der digitalen Gastfreundschaft im Café? Fortsetzung der Gretchenfrage um die Haftung für missbrauchtes WLAN: Im beck-blog wurde bereits in der Vergangenheit allerdings insbesondere hinsichtlich der Frage nach Amtshaftungsansprüchen für ex post fälschlicher Weise erfolgtes Verwaltungshandeln diskutiert, ob ein WLAN Betreiber fremdes rechtswidriges Handeln unter Missbrauch seines WLAN-Anschlusses zu vertreten hat. Der im Rahmen dieser Diskussion in der NJW, Heft 34/2009, S. XVI, von hiesiger Seite eingenommene Standpunkt meinte: Der, der sich eines technischen Mittels wie dem der kabellosen Internettechnik bedient, weiß oder muss wissen, dass die Verschlüsselung des WLAN vielerlei Schutzwirkung entfaltet und deshalb nicht nur angemessen, sondern unbedingt erforderlich ist.

Der u. a. für das Urheberrecht zuständige *I. Zivilsenat* des *BGH* urteilt nun korrespondierend (Urt. v. 12. 5. 2010 I ZR 121/08). Privatpersonen können auf Unterlassung, nicht dagegen auf Schadensersatz in Anspruch genommen werden, wenn ihr nicht ausreichend gesicherter WLAN-Anschluss von unberechtigten Dritten für Urheberrechtsverletzungen im Internet genutzt wird.

Hintergrund des Urteils ist folgender Sachverhalt: Die Klägerin, Inhaberin der Rechte an dem Musiktitel Sommer unseres Lebens , begehrt vom Beklagten, von dessen Internetanschluss der Titel gem. § 19 a UrhG öffentlich zugänglich gemacht wurde, Unterlassung, Schadensersatz und Erstattung von Abmahnkosten, obwohl Letzterer in der fraglichen Zeit im Urlaub weilte. Der Beklagte hatte seinen Anschluss nicht extra geschützt, sondern hatte es bei der werkseitigen Sicherheitseinstellung des WLAN-Routers belassen.

Das *LG* hatte den Beklagten antragsgemäß verurteilt (*LG Frankfurt a. M.,* Urt. v. 5. 10. 2007 2/3 O 19/07). Das Berufungsgericht (*OLG Frankfurt a. M.*, MMR 2008, 603) wies die Klage ab, wurde jedoch mit seinem Urteil durch den *BGH* aufgehoben, soweit es die Klage mit dem Unterlassungsantrag und mit dem Antrag auf Zahlung der Abmahnkosten abgewiesen hatte. Schadensersatzansprüche kamen angesichts der urlaubsbedingten Abwesenheit und damit auszuschließenden Täter- oder Teilnehmerschaft des Anschlussinhabers nicht in Betracht. Doch ist auch der abwesende WLAN-Anschlussinhaber Störer i. S. des § 1004 BGB und damit Unterlassungsverpflichteter. Denn, so der *BGH* nun, der private Anschlussinhaber hat zu prüfen, ob sein WLAN-Anschluss durch angemessene Sicherungsmaßnahmen vor der Gefahr geschützt ist, von unberechtigten Dritten zur Begehung von Urheberrechtsverletzungen missbraucht zu werden. Doch sind dieser Pflicht jedenfalls im privaten Bereich Grenzen gesetzt: Die Netzwerksicherheit ist nicht fortlaufend dem neuesten Stand der Technik anzupassen. Es wäre unangemessen, dafür entsprechende finanzielle Mittel aufwenden zu müssen. Die Prüfpflicht bezieht sich daher auf die Einhaltung der im Zeitpunkt der Installation des Routers für den privaten Bereich marktüblichen Sicherungen. Neben Unterlassung haftet der Störer auch auf Erstattung der Abmahnkosten.

Diese liegen gem. § 97 a II UrhG außerhalb des geschäftlichen Verkehrs in einfach gelagerten Fällen mit einer nur unerheblichen Rechtsverletzung bei 100 Euro. Sowohl über die Einfachheit des Falls als auch über die Erheblichkeit der Verletzung lässt sich trefflich streiten. So erklären Anwaltskollegen wohl zum Schutz des eigenen Geschäftsmodells, dass es sich schon dann um keinen einfach gelagerten Fall mehr handelt, wenn der Abgemahnte eine modifizierte Unterlassungserklärung abgibt. Entscheidend dürfte aber sein, wie kompliziert die Abmahnung des Rechtsbruchs und nicht wie schwierig die Prüfung der Unterlassungserklärung ist. Daher dürfte sich ein Filesharing-Fall als ein tendenziell einfacher Fall darstellen. Dies muss für den Massenabmahner und angesichts der reichhaltigen Besprechung dieser Fälle auch für den Gelegenheitsabmahner gelten. Die Erheblichkeit der Rechtsverletzung durch rechtswidrige Uploads wird noch ausgelotet. Das *LG Köln* (MMR 2010, 48) sah bei mehr als 900 Liedern keine unerhebliche Rechtsverletzung mehr. Das *AG Frankfurt a. M.* (Urt. v. 1. 2. 2010 20 C 2353/09-75, BeckRS 2010, 12644) bejahte die Unerheblichkeit bei einem vollständigen Album. Wer sich vom *BGH* hier eine abschließende Lösung für diese Fälle erhofft hatte, wird weiter warten müssen. Für die zu Grunde liegende Klage aus dem Jahre 2006 galt die Regel des § 97 UrhG noch nicht. Dennoch hat der *BGH* in seiner Presseerklärung auf die Anwendbarkeit der Norm für künftige Fälle hinzuweisen (vgl. dazu *Möller*, NJW-Editorial 23/2010, S. 3 [in diesem Heft]). Die genauen Grenzen sind damit freilich nicht geklärt.

Ebenfalls einer Klarstellung bedarf es, welche Einstellungen ein Router aufweisen muss, um als sicher zu gelten. Der *BGH* setzt ein persönliches, ausreichend langes und sicheres Passwort voraus. Ob dazu die immer noch häufig eingesetzte WEP-Verschlüsselung ausreicht, muss bezweifelt werden. Dies gilt umso mehr, als jede gängige technische Schutzmaßnahme, die gem. § 108 b UrhG Schutz erfährt, ihren Sicherheitsstandard betreffend unterhalb einer WEP-Verschlüsselung liegt. Näheres wird sich hoffentlich aus dem Urteil im Volltext ergeben. Wenngleich eine technische Spezifizierung kaum zu erwarten ist, wäre jede Referenz rechtssicherheitsstiftend.

Fraglich bleibt auch, wie mit offenem WLAN in Hotels oder Lokalen umzugehen ist. Nach allgemeinen Grundsätzen dürfte damit zu rechnen sein, dass die hier aufgezeigten Regeln zwar für Privatpersonen entwickelt wurden, aber erst recht für Unternehmer gelten. Dies könnte sich als das Ende der digitalen Gastfreundschaft erweisen. Alternativ bedürfte es eines Anmeldeprozesses, ohne den eine sichere Verschlüsselung schlechterdings undenkbar ist. Das aber dürfte sich für alle Beteiligten als unverhältnismäßig darstellen. Ob ein solcher Anmeldeprozess überhaupt zu einer Enthaftung führt, ist ohnehin die Frage. Es wäre jedenfalls konsequent, eine Öffnung des WLAN für Dritte als

per se pflichtwidrig einzuordnen und hier damit de facto auszuschließen. Sollten sich die Betreiber von offenen Netzen technischen Lösungen zuwenden, die eine Identifikation der Nutzer vorsehen, dürfte die Haftungsfrage der datenschutzrechtlichen weichen. Damit wäre wohl auch die TK-rechtliche Seite (insbes. § 4 TKG, Anmeldepflicht bei der BNetzA), derzeit kaum diskutiert, endlich im Fokus. Das Thema Hot Spots bleibt heiß.

RA Dr. Karsten Kinast, LL.M.,
Scheja & Kinast Rechtsanwälte, Bonn