Anmerkung zu BGH, Urteil vom 12.5.2010 – I ZR 121/08 – Sommer unseres Lebens, MMR 2010, 565

- erschienen in MMR 2010, 568 -

Anmerkung

Die Haftung des Inhabers eines Internetanschlusses mit WLAN-Router ist seit der Entscheidung des LG Hamburg im Jahre 2006 (LG Hamburg MMR 2006, 763) mehrfach Gegenstand von Rechtsstreitigkeiten gewesen. Nach nunmehr rund vier Jahren war die erste Entscheidung eines solchen Falles durch den BGH mit großer Spannung erwartet worden. Sowohl die mündliche Verhandlung im März als auch die Entscheidung im Mai 2010 haben weitreichende mediale Aufmerksamkeit mit Berichten und Interviews in praktisch allen großen Nachrichtensendungen erfahren. Grund hierfür ist, dass rund um die Thematik der Haftung für den Betrieb eines WLAN große Rechtsunsicherheit besteht, die bei weitem nicht nur den Bereich der privaten Nutzer von Internetanschlüssen inklusive Wohnanlagen und-gemeinschaften betrifft, sondern auch gewerbliche und institutionelle Anbieter wie z.B. Cafés mit Internetangebot, Firmen mit WLANs für Besucher, Universitäten, Bibliotheken und schließlich offene Netze wie z.B. die Netzwerke der Freifunk-Initiative (http://www.freifunk.net). Für diese Anbieter war die bestehende Unsicherheit ein ständiger Hemmschuh für neue Entwicklungen oder eine Ausweitung ihrer Angebote.

Dem BGH hat sich daher im vorliegenden Fall die Chance geboten, für alle diese Fälle Rechtssicherheit zu schaffen und dabei die in Rechtsprechung und Literatur aufgeworfenen Rechtsfragen zu beantworten (für eine weitgehende Haftung LG Hamburg MMR 2006, 763 m. Anm. Mantz; LG Frankfurt, Urt. v. 5.10.2007 – 2/3 O 19/07; LG Frankfurt ZUM 2007, 406 m. Anm. Gietl; OLG Düsseldorf MMR 2008, 256; gegen eine Haftung OLG Frankfurt MMR 2008, 603 m. Anm. Mantz/Gietl; dazu auch Stang/Hühner, GRUR-RR 2008, 273; Hornung, CR 2008, 585; Übersichtsaufsätze zur Problematik Garcia, Telepolis v. 19.4.2010, http://www.heise.de/tp/r4/artikel/32/32466/1.html; Stadler, http://www.internet-law.de/2010/04/grundrecht-auf-offene-netze.html; Mantz, JurPC Web-Dok. 95/2010, Rn. 3 ff., 29; Breyer, NJOZ 2010, 1085; Gietl, MMR 2007, 630).

Diese Chance hat der BGH leider vertan. Denn zum einen hat er den Blick über den Tellerrand nicht gewagt oder die Möglichkeit dazu verkannt und sich auf eine strikt auf den vorliegenden Fall bezogene Entscheidung beschränkt. Zum anderen hat er selbst bei Rechtsfragen, die er entscheiden musste und entschieden hat, sehr eng argumentiert, teilweise neue Rechtsfragen aufgeworfen und Unsicherheiten geschaffen. Die erhoffte Klärung ist daher ausgeblieben.

Im wesentlichen hat der BGH zu drei Kernpunkten Stellung genommen: Zum Anspruch auf Schadensersatz, zum Vorliegen der Störerhaftung sowie zur Reichweite des Unterlassensanspruchs. Bezüglich letzterem Teil und der Kostenentscheidung hat der BGH den Fall an das OLG Frankfurt zurückverwiesen.

I. Schadensersatz. Wenig Überraschendes hat sich zur Haftung des Beklagten auf Schadensersatz nach § 97 Abs. 1 UrhG ergeben. Allerdings hat sich der BGH ohne weitere Begründung dem insoweit meinungsführenden OLG Köln (OLG Köln MMR 2010, 44, 45) angeschlossen und eine sekundäre Darlegungslast des Beklagten angenommen. Bei der sekundären Darlegungslast trifft auch die nicht beweisbelastete Partei eine Darlegungspflicht, soweit ihr dies möglich und zumutbar ist (BGH NJW-RR 2004, 989, 990; BGHZ 109, 139, 149; kritisch insgesamt

MünchKommBGB-Wagner, § 138 Rn. 22). Dies gilt besonders für den privaten Bereich der gegnerischen Partei, also den Bereich, der außerhalb des von der darlegungspflichtigen Partei vorzutragenden Geschehensablaufs liegt (BGH NJW 1999, 577). Dabei ist zu beachten, dass die sekundäre Darlegungslast keinen Vollbeweis erfordert. Es reicht vielmehr aus, den Vortrag der Klägerin substantiiert zu erschüttern, was zugegebenermaßen häufig einem Vollbeweis nahekommt. Der Beklagte konnte hier von Glück sagen, dass er zur Tatzeit im Urlaub war. Denn nach mehreren Monaten substantiiert darzulegen, wo man zu einem bestimmten Zeitpunkt war, dürfte in der Regel kaum möglich sein. Interessanterweise geht der BGH in diese Zusammenhang noch auf Routerprotokolle bzw. Routerlogs ein und stellt fest, dass der Beklagte als nicht versierter Computernutzer nicht zur Vorlage von Routerprotokollen verpflichtet war. Es ist nicht ganz klar, was der BGH mit diesen für die Entscheidung nicht zwingend nötigen Hinweis bezweckt hat. Man könnte daraus lesen, dass versierte Computernutzer zur Vorlage von Routerlogs verpflichtet sein könnten. Allerdings speichern nicht alle Router solche Logs oder löschen sie nach einer gewissen Zeit. Wenn die Abmahnung erst spät kommt und dann keine Daten mehr vorliegen, so kann der BGH kaum vom (selbst versierten) Nutzer die Vorlage nicht existierender Routerlogs verlangen.

Interessant sind weiter die Ausführungen zur Entscheidung Jugendgefährdende Medien bei Ebay (BGH MMR 2007, 634). Der BGH stellt sich einer Übertragung der Überlegungen auf Urheberrechtsfälle (dazu Köhler, GRUR 2008, 1) nicht grundsätzlich entgegen, stellt aber andere Anforderungen als im

Wettbewerbsrecht. Zudem deutet er eine restriktive Handhabung aus dem Grunde an, dass diese Entscheidung maßgeblich mit dem geschäftlichen Interesse des damaligen Beklagten begründet wurde. Nicht übertragbar ist hingegen die Halzband-Entscheidung (BGH MMR 2009, 391) zur Haftung bei Überlassung eines Ebay-Accounts. Denn eine IP-Adresse hat gerade keine eindeutige Identifizierungsfunktion. Ganz im Gegenteil stellt der zu Recht BGH fest, dass der Inhaber des Anschlusses dazu berechtigt ist, beliebigen Dritten seinen Anschluss zur Verfügung zu stellen.

II. Störerhaftung. 1. Sachverhalt. Für die Frage der Störerhaftung haben sich Unsicherheiten schon im Hinblick auf den festgestellten Sachverhalt ergeben. Denn bis zuletzt ist unklar, welche Sicherheitsvorkehrungen der Beklagte getroffen hatte. Das LG Frankfurt hatte festgestellt, dass der Beklagte ein 16-stelliges Passwort auf seinem Fritz!Box-WLAN-Router eingestellt hatte, dieses aber auf der werkseitigen Voreinstellung belassen hatte. Der BGH hat dies als Unsicherheitsfaktor erkannt und darauf seine Auffassung gestützt, dass der Beklagte nicht alles ihm Mögliche getan hat. Wie sich demgegenüber aus dem erstinstanzlichen Urteil ergibt, hat der Hersteller des Routers des Beklagten WLAN-fähige Router von Anfang an nur mit Passwörtern ausgeliefert, die auf den Router individualisiert waren und aus 16 zufälligen Ziffern bestanden (s. http://www.avm.de/de/News/artikel/2010/wlan_urteil.html). Das Passwort war damit eindeutig und mindestens ebenso sicher wie ein vom Beklagten gewähltes gewesen wäre. Die vom BGH gewählte Formulierung des BGH deutet hingegen darauf hin, dass er von einem für alle Router der Modellreihe gleichen Passwort ausging.
2. Auch im Rahmen der Begründung der Störerhaftung lässt der BGH leider einige klärende Antworten vermissen. Der BGH hat – auf einer Linie mit dem LG Hamburg und der erstinstanzlichen Entscheidung des LG Frankfurt - die adäquate Kausalität der Handlungen des

Beklagten angenommen. Adäquate Kausalität liegt verkürzt gesprochen vor, wenn ein Ergebnis oder Kausalverlauf nicht vollkommen unwahrscheinlich und fern jeder Lebenserfahrung ist. Das OLG Frankfurt hatte hier darauf abgestellt, dass keine Daten dazu vorliegen, ob WLAN-Netze durch Dritte genutzt werden (dazu näher Mantz, JurPC Web-Dok. 95/2010, Rn. 25 mwN). Darauf ist der BGH nicht eingegangen, sondern hat pauschal festgestellt, dass es nicht gänzlich unwahrscheinlich sei, dass ein unzureichend gesichertes WLAN durch unbekannte Dritte genutzt werde. Dies mag bei einem vollständig offenen Netz vertretbar sein. Das Netz des Beklagten war aber tatsächlich selbst nach dem vom BGH festgestellen Sachverhalt mit Passwort und Verschlüsselung gesichert. Unabhängig davon, ob das Passwort sicher war, geht der BGH also davon aus, dass es nicht unwahrscheinlich sein soll, dass Dritte sich unter Verstoß gegen § 202a StGB in strafrechtlich relevanter Art und Weise Zugang zum Netz eines Dritten verschaffen (vgl. BeckOK-StGB-Weidemann, § 202a Rn. 11). Hier hätte der BGH schon im Hinblick auf die Zweifel des OLG Frankfurt deutlich mehr Begründungsaufwand betreiben müssen .

3. Zumutbarkeit. a) Anschließend stellt der BGH fest, dass es dem privaten Inhaber eines WLAN zumutbar ist, sein WLAN-Kennwort zu ändern.
Interessanterweise stützt der BGH die Zumutbarkeit auf das Eigeninteresse des Betroffenen am Schutz der eigenen Daten, also im Grunde auf ein Verschulden gegen sich selbst (s. hierzu Möller, http://www.telemedicus.info/article/1774-Der-BGH-zur-WLAN-Haftung.html). Weiter hätte der BGH hier sauber trennen müssen: Die Unsicherheit des WLAN bedingt nicht auch die Unsicherheit der Daten. Trotz Zugangs zum WLAN kann der Beklagte die Freigaben auf seinem Computer restriktiv und damit sicher eingestellt haben. Hierzu haben aber weder die Instanzgerichte noch der BGH tatsächliche Feststellungen getroffen. Ob ein solches Interesse also vorlag, lässt sich nicht ohne weiteres postulieren. Auch die Daten auf dem Router selbst, also z.B. die Zugangsdaten zum DSL-Anbieter, müssen nicht zwingend unsicher gewesen sein. Denn das Kennwort zum Zugang zum WLAN und das Administratorpasswort des Routers sind in der Regel nicht identisch.
b) Bei der Bemessung der Pflichten des Beklagten stellt der BGH darauf ab, dass derjenige, der einen WLAN-Router kauft, wenigstens diejenigen Sicherheitseinstellungen einhalten muss, die zum Zeitpunkt des Kaufs marktüblich sind. Eine Überwachungspflicht sieht der BGH hingegen als unzumutbar an. In der Folge widerspricht der BGH sich jedoch selbst deutlich: Denn der Beklagte hat den Router im Jahre 2004 gekauft. Die Rechtsverletzung erfolgte erst 2006. Anzulegen wäre also der Maßstab gewesen, der im Jahr 2004 marktüblich war. Dennoch stellt der BGH im folgenden auf den Maßstab für Mitte 2006 ab und verlangt ein individuelles Kennwort. Im Jahr 2004 wurden Router aber häufig noch gänzlich ohne Verschlüsselung oder mit WEP und einheitlichem Standardkennwort ausgeliefert. Ob die Änderung des Kennworts 2004 marktüblich war, spricht der BGH hingegen nicht an. Desweiteren sah die Literatur im Jahr 2006/2007 die vom BGH angenommene Marktüblichkeit wohl nicht (Hornung, CR 2007, 88, 89; Gercke, ZUM 2006, 593, 598).
Auf die vom LG Frankfurt auch nur angedeutete Problematik, dass das Kennwort auf dem (in den Räumlichkeiten des Beklagten befindlichen) Router aufgedruckt war, ist der BGH hingegen nicht eingegangen.

4. Privilegierung § 8 TMG. Überraschend sind die Ausführungen zur Haftungsprivilegierung. Der BGH lehnt die Anwendung der Privilegierung nach § 10 TMG ab. Dies hat zur Folge, dass die Haftung nicht erst ab Kenntnis von der Rechtsverletzung einsetzt. Dabei ist davon auszugehen, dass der BGH § 8 TMG gemeint hat, da § 10 TMG für Host Provider und § 8 TMG für Access Provider gilt. Unabhängig davon hat der BGH an dieser Stelle bisher immer auf seine

entsprechenden Entscheidungen dahingehend verwiesen, dass die Privilegierungen ohnehin nicht auf Unterlassungsansprüche anwendbar sind. Damit wäre dieser Punkt abschließend behandelt gewesen. Stattdessen führt der BGH aus, dass hier das berechtigte Interesse an der Nutzung von WLAN nicht entgegensteht. Fraglich ist, wie dies zu verstehen ist. Denn dieses Satzes hätte es nicht bedurft, wenn der BGH seine Linie beibehielte. Man könnte das als Hinweis darauf sehen, dass der BGH von seiner grundsätzlichen Ablehnung der Anwendung der Privilegierungen auf Unterlassungsansprüche abrückt und stattdessen eine neue Begründung benötigt. Eine ähnliche Tendenz hat der BGH bereits im Urteil zu Google-Thumbnails (Urt. v. 29.4.2010 - I ZR 69/08) erkennen lassen (s. zu dieser Problematik Stadler, http://www.internet-law.de/2010/05/anmerkung-zum-urteil-des-bgh-zur-google-bildersuche.html; und Mantz, http://bit.ly/dwpCsp).

5. Verwertung von IP-Adressen. Das OLG Frankfurt hatte in seinem Urteil noch ein Verbot der Verwertung der erlangten IP-Adressen gesehen, da es sich um Verkehrsdaten handele (s. dazu auch Gietl/Mantz, CR 2008, 810, 816 mwN). Dem tritt der BGH entgegen und betrachtet IP-Adressen als Bestandsdaten und verweist u.a. auf die Gesetzesbegründung zur TKÜV. Er missachtet dabei leider, dass der

Gesetzgeber bei der Schaffung von § 101 IX UrhG selbstverständlich davon ausgeht, dass IP-Adressen Verkehrsdaten nach § 3 Nr. 30 TKG sind. Damit entzieht der BGH dem § 101 IX UrhG praktisch den Anwendungsbereich und hebelt dessen Richtervorbehalt aus. Außerdem setzt er sich mit dieser Auffassung in Widerspruch zum BVerfG. Denn das BVerfG behandelt IP-Adressen als Verkehrsdaten und sieht in der Speicherung und Herausgabe von IP-Adressen einen Eingriff in Art. 10 GG, auch wenn es dem Gesetzgeber bei der Ausgestaltung von Auskunftsmöglichkeiten einen weiteren Spielraum gibt (BVerfG NJW 2010, 356 Rn. 45, 258 ff.).

6. Protokollsoftware. Keine Entscheidung hat der BGH übrigens zur Beweisthematik bei der Verwendung der Software zur Protokollierung von IP-Adressen getroffen (zur Beweisfuehrung s. Schultz, MIR 2008, Dok. 102; Gietl/Mantz, CR 2008, 810, 815; zur Zuverlässigkeit der Software s. AG Frankfurt, Urt. V. 16.4.2010 - 30 C 562/07 – 47). Denn der Beklagte hatte die Zuverlässigkeit nicht hinreichend bestimmt bestritten, so dass weder OLG Frankfurt noch BGH darauf weiter eingehen mussten.

III. Kostendeckelung, § 97a UrhG. Das Urteil enthält entgegen der Pressemitteilung keine Erwähnung der Kostenkappung für die Abmahnung auf EUR 100,- nach § 97a II UrhG. Alle diesbezüglichen Ausführungen in die eine oder andere Richtung sind damit hinfällig. Allerdings gilt dies auch für den Hinweis in der Pressemitteilung, dass § 97a UrhG auf den vorliegenden Fall nicht anwendbar sein soll. Denn der BGH hat die komplette Kostenentscheidung an das OLG Frankfurt zurückverwiesen. Es liegt jetzt in der Hand des OLG Frankfurt, nicht nur den Streitwert zu bestimmen, sondern auch über eine Anwendung von § 97a UrhG auf Altfälle zu entscheiden, da der BGH hierzu keine nach § 563 II ZPO bindende Ansicht geäußert hat. Die Anwendbarkeit auf Altfälle nimmt beispielsweise das OLG Brandenburg (MMR 2009, 258) an.

IV. Zurückverweisung. Weiter hat der BGH neben der Kostenentscheidung auch die Entscheidung über den Unterlassensantrag mit der Begründung zurückverwiesen, der Antrag der Klägerin erfasse nicht die nun festgestellte Verletztungshandlung. Offenbar hat der BGH dies

nicht als Minus nach § 308 ZPO angesehen. Es ist allerdings aus der Begründung nicht ersichtlich, warum der BGH keinen Hinweis nach § 139 ZPO erteilen konnte. Denn dieser dient u.a. dazu, dass die Parteien ihre Anträge auf den (vorläufigen) Standpunkt des Gerichts einstellen können (MünchKommBGB-Wagner, 3. Aufl. 2008, § 139 Rn. 1).
Nicht gänzlich ausgeschlossen ist übrigens, dass das OLG Frankfurt aufgrund der oben dargestellten Unklarheiten im Sachverhalt doch zu einer Klageabweisung gelangt. Das OLG wird überlegen müssen, ob die Bindungswirkung nach § 563 II ZPO bei einem Fehlverständnis greift, oder der Beklagte den Sachverhalt noch nach §§ 529-531 ZPO klarstellen kann. Denn wie dargestellt hat der Beklagte zwar kein persönliches Kennwort, wohl aber ein sicheres Kennwort verwendet.

V. Auswirkungen des Urteils. Die Auswirkungen des Urteils lassen sich aufgrund der weiter bestehenden dargestellen Unsicherheiten nicht endgültig feststellen. Sicher ist nur, dass Private, die ihr Netz privat nutzen, ihr WLAN nun nach dem zum Kaufzeitpunkt geltenden Standard absichern müssen (zum daraus entstehenden Widerspruch Mantz, Rechtsfragen offener Netze, Karlsruhe 2008, S. 291 ff., online abrufbar).
Für institutionelle Anbieter iwS, wie z.B. Cafes mit Internet, Universitäten, Bibliotheken, aber auch offene Netze wie z.B. Freifunk (http://www.freifunk.net) zeichnet sich ein differenziertes Bild ab. Zum einen verfängt das Argument des BGH nicht, dass der Betroffene ein Eigeninteresse an der Sicherung des Netzwerks hat – denn die Öffnung erfolgt hier ganz bewusst. Gerade bei offenen Netzen ist es üblich, dass das Setup zwei Router umfasst, von denen nur einer das offene Netz bereitstellt. Durch diese Aufteilung erfolgt eine netzwerktopologische Trennung der Netze, und damit eine Sicherung des privaten lokalen Netzes vor Zugriffen der Nutzer. Wenn der Anbieter eines offenen Netzwerks aber seine Daten schützt und dennoch das Netz bewusst öffnet, dann kann sich der BGH nicht auf das Eigeninteresse des Anbieters stützen und daraus Pflichten ableiten.
Zum anderen begründet der BGH die Zumutbarkeit der Pflichten auch damit, dass der private Anbieter gerade kein „Geschäftsmodell“ verfolgt. In der Rechtsprechung des BGH zur Störerhaftung hat sich immer wieder gezeigt, dass der BGH Geschäftsmodelle grundsätzlich schützt – wenigstens insoweit, als eine auferlegte Pflicht nicht zur Einstellung des Geschäftsbetriebes führen darf (BGH MMR 2004, 668 - Internetversteigerung I;
BGH MMR 2007, 507 - Internetversteigerung II; näher Mantz, JurPC Web-Dok. 95/2010, Rn. 28 ff.). Man kann den BGH also so verstehen, dass er geringere Pflichten auferlegt, sobald hinter dem Angebot ein wie auch immer geartetes Geschäftsmodell steht. Dies darf allerdings nicht in einem streng wirtschaftlichen Sinne verstanden werden, sondern dürfte sich auf jegliches organisierte und bewusste Öffnen des Netzes beziehen.
Zusätzlich gibt der BGH institutionellen Anbietern ein weiteres wichtiges Argument an die Hand, indem er befindet, dass das Interesse an „leichtem und räumlich flexiblem Zugang zum Internet“ hoch zu bewerten und berechtigt ist. Hier hat der BGH tatsächlich Farbe bekannt – und damit einen Baustein für künftige Abwägunsentscheidungen gelegt. Wichtig ist dies insbesondere auch für offene Netze, da das Interesse am Zurverfügungstellen von Infrastruktur u.a. im Hinblick auf den „Digital Divide“ sogar noch höher zu bewerten ist (s. dazu ausf. Mantz, JurPC Web-Dok. 95/2010, Rn. 28 ff.; und ausführlich Mantz, Rechtsfragen offener Netze, Karlsruhe 2008, S. 14 ff. mwN, online abrufbar).
Auf der anderen Seite ist zu beachten, dass der BGH bei der Bewertung des Sicherheitsstandards die Beschränkung auf den zum Zeitpunkt der Einrichtung marktüblichen Standard ausdrücklich nur auf Private bezieht. Insgesamt deutet der BGH aber an, dass er institutionelle Anbieter eher

nicht als Störer betrachten wird. Ob diese Tendenz bestehen bleibt, wenn dem BGH ein solcher Fall vorliegt, muss sich erst noch zeigen.

VI. Fazit. Insgesamt hat der BGH viele bedeutsame Fragen nicht beantwortet, obwohl Anlass dazu bestanden hätte, und diese im Vorfeld wiederholt durch die Literatur angesprochen wurden (Garcia, aaO; Stadler, http://www.internet-law.de/2010/04/grundrecht-auf-offene-netze.html; Mantz, JurPC Web-Dok. 95/2010, Rn. 3 ff., 29; s. auch Gietl, MMR 2007, 630; Mantz/Gietl, MMR 2008, 606; Stang/Hühner, GRUR-RR 2008, 273). Weiter ist es sehr schade, dass der BGH sich mit den in der Literatur geäußerten Auffassungen überhaupt nicht auseinander gesetzt hat. Insbesondere die Anmerkungen zu einem ähnlichen Urteil des LG Frankfurt (LG Frankfurt ZUM 2007, 406 m. Anm. Gietl) sowie zum Urteil des OLG Frankfurt (s.o.) sowie die kurz vor dem Urteil veröffentlichten Aufsätze hätten Anlass für eine vertiefte Betrachtung geboten.

Dr. jur. Dipl.-Inf. Reto Mantz, Frankfurt/M.