tion auf dem Grundstück der Antragsgegnerin bis zum 13.4.2006, 12:00 Uhr. Mit Telefaxschreiben der Prozessbevollmächtigten der Antragsgegnerin v. 13.4.2006 wurde mitgeteilt, dass dieser Forderung seitens der Antragsgegnerin nicht nachgekommen werde.

II. Die einstweilige Verfügung war antragsgemäß in der aus dem Tenor ersichtlichen und sich aus einer sachgerechten Auslegung des Begehrens der Antragstellerin ergebenden Form zu erlassen.

Der Verfügungsanspruch ergibt sich aus § 861 Abs. 1 BGB. Die Antragstellerin war bis zur Erteilung des Hausverbots mit Schreiben v. 1.3.2006 Besitzerin der auf der streitgegenständlichen Grundstück errichteten Mobilfunkstation: Sie hat diese Station errichtet und hatte bis zu diesem Zeitpunkt entsprechend den in dem Mietvertrag v. 5.12.2005/14.12.2005 festgelegten Bedingungen ungehinderten Zugang und ungehinderte Einwirkungsmöglichkeit auf diese Mobilfunkanlage. Mit der Erteilung des Hausverbotes bzw. der Weigerung der Antragsgegnerin, der Antragstellerin auch weiterhin den ungehinderten Zugang zur Mobilunkanlage zu gewähren, wurde der Antragstellerin der Besitz an dieser Anlage i.S.d. § 861 Abs. 1 BGB entzogen. Dies geschah durch verbotene Eigenmacht, nämlich ohne Willen der Antragstellerin. Eine gesetzliche Gestattung der Entziehung ist weder vorgetragen noch ersichtlich. Ob neben der Antragstellerin bis zur Sperrung des Zugang durch die Antragsgegnerin auch diese Besitzerin der Mobilfunkanlage war, ob bis zu diesem Zeitpunkt also Mitbesitz i.S.d. § 866 BGB vorlag, kann offen bleiben: Die Beschränkung des Besitzschutzes aus § 866 BGB greift nicht ein, soweit es sich nicht um die Grenzen des dem einzelnen Besitzer zustehenden Gebrauchs handelt, so bei völliger Besitzentziehung (vgl. Palandt/Bassenge, BGB, 65. Aufl. 2006, § 866 Rz. 5).

Auf materiellrechtliche Einwände der Antragsgegnerin, insb. auf alle Einwände gegen die Wirksamkeit, Widerruflichkeit, Anfechtbarkeit sowie auf die geltend gemachten sonstigen Unwirksamkeitsgründe des Mietvertrags v. 5.12.2005/14.12.2005, die u.a. in der Schutzschrift v. 13.4.2006 vorgetragen werden, kommt es aus Rechtsgründen nicht an, § 863 BGB.

Zur Geltendmachung des nach dem Gesetz auf zügige Durchsetzung angelegten Besitzschutzanspruchs im Verfügungsverfahren bedarf es eines besonderen Verfügungsgrundes nicht (OLG Stuttgart v. 19.1.1996 – 2 U 164/95, NJW-RR 1996, 1516; Palandt/Bassenge, BGB, 65. Aufl. 2006, § 861 Rz. 18).

Die Dringlichkeit i.S.d. § 937 Abs. 2 ZPO ergibt sich ebenfalls aus der Natur des possessorischen Besitzschutzes sowie ferner daraus, dass die auf dem streitgegenständlichen Grundstück von der Antragstellerin errichtete Mobilfunkstation im Wesentlichen nur noch der Einbindung in das Mobilfunknetz bedarf und dann auf Sendung gehen könnte, so dass erhebliche Umsatzverluste der Antragstellerin drohen, sollte ihr nicht umgehend der Zugang zur Anlage wieder ermöglicht werden.

BGH: Faxumleitung auf PC – Telefax-Werbung II

UWG a.F. § 1; BGB §§ 670, 677, 683 Satz 1; UWG i.d.F. v. 3.7.2004 § 7 Abs. 2 Nr. 3

Leitsatz

Der Umstand, dass Telefaxsendungen immer häufiger unmittelbar auf einen PC geleitet und nicht mit einem herkömmlichen Faxgerät ausgedruckt werden, ändert nichts daran, dass eine per Telefax unaufgefordert übermittelte Werbung auch gegenüber Gewerbetreibenden grundsätzlich als wettbewerbswidrig anzusehen ist (im Anschluss an BGH, Urt. v. 25.10.1995 – I ZR 255/93, CR 1996, 337 = GRUR 1996, 208 = WRP 1996, 100 – Telefax-Werbung I).

BGH, Urt. v. 1.6.2006 – I ZR 167/03
(LG Hildesheim, Urt. v. 26.6.2003 – 1 S 16/03; AG Hildesheim, Urt. v. 17.1.2003 – 49 C 150/02)

Medienrecht

Gerrit Hornung

Die Haftung von W-LAN Betreibern

Neue Gefahren für Anschlussinhaber – und die Idee „offener" Netze

Der Internetzugang über Wireless-LAN (W-LAN) findet immer weitere Verbreitung im öffentlichen Raum und in Privathaushalten. Die Betreiber sind dabei insbesondere aus zwei Richtungen Gefahren ausgesetzt: Zum einen drohen technische Angriffe Dritter gegen mangelhaft gesicherte Netzwerke und die in ihnen gespeicherten oder transportierten Daten, zum anderen die rechtliche Verantwortlichkeit für Handlungen dieser Dritten über den Internetzugang des Anschlussinhabers. Ausgehend von zwei Entscheidungen des LG Hamburg und des AG Euskirchen erörtert der Beitrag die zweite Frage; dabei ist weithin zwischen willentlichen Angeboten für Dritte („Hotspots") und privaten Betreibern eigener Netze zu unterscheiden.

▷ Dr. Gerrit Hornung, LL.M. (European Law), ist Geschäftsführer der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) an der Universität Kassel.

Die Haftung von W-LAN Betreibern

I. W-LAN zwischen Nutzerfreundlichkeit und Nutzersorglosigkeit

Der Internetzugang mittels W-LAN[1] – oder, exakter, nach den Standards der Serie 802.11 des *Institute of Electrical and Electronics Engineers*(IEEE)[2] – wird von immer mehr Nutzern verwendet. Für Ende 2006 wurde die Zahl der kommerziellen Hotspots mit weltweit 147.000 angegeben.[3] Soweit ersichtlich gibt es für den privaten Bereich keine Erhebungen, die Zahl dürfte aber um ein Vielfaches höher liegen. Die Vorteile von W-LAN sind offensichtlich: Die Notwendigkeit der Verkabelung (gerade in Altbauten) entfällt, eine örtliche Veränderung der Endgeräte ohne Neuaufbau der Verbindung wird ermöglicht, in Gaststätten, Hotels, Bahnhöfen und Flughäfen – aber auch innerhalb freier Funknetze[4] – kann eine größere und ständig wechselnde Nutzerzahl einfach und bedienerfreundlich Internetverbindungen aufbauen.

So groß die Vorteile drahtloser Kommunikation mittels W-LAN sind, so groß sind die Risiken beim Betrieb ohne sachverständige Konfiguration des Verschlüsselungssystems. So kann ein Angreifer die übertragenen – mit hoher Wahrscheinlichkeit auch die auf den angeschlossenen Rechnern gespeicherten – Daten mitlesen und ggf. verfälschen, außerdem Konfigurationen am eingesetzten Router ändern, etwa Passwörter austauschen, und schließlich den Online-Zugang des Anschlussinhabers nutzen. Bei letzterem ist der Missbrauch nach außen nicht erkennbar, da lediglich die IP des Routers sichtbar ist. Selbst wenn anhand des Nutzerverhaltens deutlich wird, dass mehrere Personen gleichzeitig den Zugang nutzen, ist zumindest nicht nachvollziehbar, ob dies mit oder ohne den Willen des Anschlussinhabers erfolgt. Wird eine Verschlüsselung nach dem Wired Equivalent Privacy Protocol (WEP)-Standard verwendet, ergibt sich zwar ein Schutz gegen technisch Uninformierte, mit entsprechenden Kenntnissen und Software ist die Überwindung dieser Art der Sicherung aber kein größeres Problem und dauert je nach übertragenem Datenvolumen lediglich Minuten.[5] Erst die neueren Standards Wireless Fidelity Protected Access (WPA und WPA2) gelten als derzeit sicher.

Nach Erhebungen aus der Praxis sind diese Sicherheitsprobleme entweder weithin unbekannt oder werden als nicht erheblich bewertet: Nach einer Untersuchung aus dem Jahre 2006 wird beispielsweise derzeit jedes vierte W-LAN unverschlüsselt betrieben, und 60 % der verschlüsselten Netze verwenden das unsichere WEP.[6] Das hängt bis zu einem gewissen Grad sicherlich damit zusammen, dass erst in jüngster Zeit Router angeboten werden, die bereits in der Ausgangskonfiguration eine Verschlüsselung vorsehen.

II. Anschlussinhaber zwischen rechtlichem Schutz und rechtlicher Haftung

Die Verwendung sicherer Verschlüsselungen sollte die rechtlichen Probleme von W-LAN an sich auf die einschlägigen Fragen des Telekommunikationsrechts (Frequenzzuweisung, Meldepflicht, technische Schutzmaßnahmen etc.)[7] und der Vertragsmodelle der Hotspot-Betreiber[8] reduzieren. Solange der Anschlussinhaber und Betreiber des W-LANs nutzerspezifische Kennungen vergibt und derartige kryptographische Sicherungen einsetzt, lässt sich sowohl ein Missbrauch durch Dritte verhindern als auch im Einzelfall die Zuordnung rechtlich relevanten Verhaltens klären.

Wenn der Betrieb von W-LANs dennoch wichtige Rechtsfragen aufwirft,[9] so hat das mehrere Gründe. Kurzfristig ist das Problem des rechtlichen Umgangs mit Angriffen auf nicht oder unzureichend gesicherte Netzwerke zu lösen – mit anderen Worten zivilrechtliche Abwehransprüche und strafrechtliche Folgen des Hackens von W-LAN-Verbindungen und der Internetnutzung über fremde Hotspots. Langfristig geht es um die Frage, ob die Abschottung der einzelnen Netze gesellschaftlich wünschenswert ist oder nicht umgekehrt durch weitgehende Haftungszurechnungen für die Betreiber von W-LANs die perspektivisch positive Idee einer Welt der „offenen Netze" unrealistisch wird.

Der erste Themenkomplex wird seit einiger Zeit diskutiert und soll deshalb hier nur erwähnt werden.[10] Wird die Sicherung eines verschlüsselten W-LANs überwunden, so greift regelmäßig § 202a StGB ein.[11] Das gilt nach herrschender Ansicht auch für die Verschlüsselung mittels WEP[12] und bereits dann, wenn der Täter – etwa am Bildschirm – die Daten lediglich visuell zur Kenntnis nimmt. Bei Bereicherungsabsicht (insbesondere bei verbindungsabhängiger Abrechnung) kommt auch § 263a StGB in Betracht.[13] Unabhängig von der Frage der Verschlüsselung können je nach Tathandlung bei Manipulationen §§ 303a, 303b StGB, bei der Verschaffung oder Sicherung von Geschäfts- oder Betriebsgeheimnissen § 17 Abs. 2 Nr. 1 UWG, beim Mitschneiden der Kommunikation zwischen Router und Endgerät §§ 148 Abs. 1 Nr. 1, 89 TKG und bei unbefugtem Abruf oder unbefugter Verarbeitung personenbezogener Daten Ordnungswidrigkeiten bzw. bei Bereicherungs- oder Schädigungsabsicht Straftaten des Datenschutzrechts (§§ 43 Abs. 2, 44 Abs. 1 BDSG) einschlägig sein.[14] Schlussendlich hat der Betreiber unabhängig von der Verschlüsselung einen Abwehranspruch analog § 1004 BGB; das gilt jedenfalls dann, wenn der Dritte durch den nicht genehmigten Zugang zusätzliche Verbindungsentgelte verursacht oder die Übertragungsgeschwindigkeit reduziert.[15]

1 Zur Funktionsweise s. z.B. *Rech*, Wireless LANs, 2. Aufl. 2006; *Hein*, Wireless LAN, 2003; zu Angriffen und Schutzmöglichkeiten AK Technik der Datenschutzbeauftragten, DuD 2005, 700; *www.bsi.de/fachthem/sinet/basis/basis_WLAN.htm*.

2 Wörtlich bezeichnet „Wireless Local Area Network" an sich nur ein kabelloses lokales Netzwerk beliebiger drahtloser Übertragungstechnologie, umgangssprachlich und fachöffentlich ist aber rglm. die IEEE 802.11-Reihe gemeint; so auch im Folgenden.

3 Siehe *www.heise.de/newsticker/meldung/80665*.

4 Eine zunehmende Zahl von Initiativen bietet W-LAN kostenlos an (zum Teil ohne Anmeldepflicht), s. z.B. freifunk.net/, fon.com, freewlan.org und free-hotspot.com; vgl. ausführlich *Medosch*, Freie Netze, 2004.

5 *Dornseif/Schumann/Klein*, DuD 2002, 226 (228) m.w.N.

6 *Endres*, c't 25/2006, 98; 2004 waren 50 % der privaten (*Bachfeld*, c't 13/2004, 92) und 34 % der in Unternehmen betriebenen (*www.dsl-news.de/modules.php?name=News&file=article&sid=520*) W-LANs ungeschützt.

7 Dazu *Zimmer*, CR 2003, 893; *Röhrborn/Katko*, CR 2002, 882.

8 Siehe *Hornike/Boës*, MMR 2003, 457.

9 Siehe außer den Nachw. in Fn. 7, 8 und 10 z.B. *Gietl*, DuD 2006, 37; *Mantz*, MMR 2006, 764; zur Rechtslage in den USA *Kern*, CRi 2006, 33.

10 Siehe *Ernst*, CR 2003, 898; *Buermeyer*, HRRS 2004, 285; *Bär*, MMR 2005, 434; *Dornseif/Schumann/Klein*, DuD 2002, 226, (228); zur unklaren Lage in den USA *Kern*, CRi 2006, 33 (35 ff.).

11 *Ernst*, CR 2003, 898 f.; *Bär*, MMR 2005, 434 (435 f.), jeweils m.w.N.; a.A. wohl nur *Dornseif/Schumann/Klein*, DuD 2002, 226 (228 ff.).

12 *Ernst*, CR 2003, 898 (899); *Buermeyer*, HRRS 2004, 285 (286 f.); *Bär*, MMR 2005, 434 (436); *Lenckner* in Schönke/Schröder, StGB, 27. Aufl. 2006, § 202a Rz. 8.

13 *Bär*, MMR 2005, 434 (437 f.); a.A. *Buermeyer*, HRRS 2004, 285 (289).

14 Siehe näher *Ernst*, CR 2003, 898 (899 f.); *Bär*, MMR 2005, 434 (438 ff.); *Buermeyer*, HRRS 2004, 285 (289 ff., tlw. abl.).

15 Siehe auch *Gietl*, DuD 2006, 37.

III. Die Haftung des Betreibers

Wesentlich neueren Datums ist die Frage, inwieweit die Anschlussinhaber und Betreiber für das Verhalten Dritter einzustehen haben, die ohne oder gegen ihren Willen über das W-LAN das Internet nutzen. Rechtspraktisch stellt sich außerdem das Problem der Beweislast, falls dies nicht ausgeschlossen werden kann.

1. Die Haftung in der Rechtsprechung

Beide Themenkreise haben bislang – soweit ersichtlich – explizit nur in je einem zivil- und strafrechtlichen Fall die Rechtsprechung beschäftigt.

a) Zivilrechtliche Störerhaftung

In Sommer 2006 bejahte das LG Hamburg die Haftung des Betreibers für Handlungen Dritter, wenn das W-LAN ungesichert verwendet wird.[16] In dem Verfahren ging es um einen Antrag auf einstweilige Verfügung einer Tonträgerherstellerin zur Abgabe einer Unterlassungserklärung wegen der Bereitstellung von Musikdateien in einem Filesharing-System. Unter einer den Antragsgegnern zuordnenbaren IP-Adresse waren mehrere Musikaufnahmen zum Kopieren vorgehalten worden, für die der Antragstellerin die Tonträgerherstellrechte und das ausschließliche Recht zur öffentlichen Zugänglichmachung zustanden. Die Antragsgegner lehnten die Abgabe der Unterlassungserklärung ab und verteidigten sich mit dem Argument, sie hätten unter der IP-Adresse ein ungeschütztes W-LAN betrieben; mithin käme als Verletzer eine nahezu unbegrenzte Anzahl Dritter in Betracht. Die Möglichkeit der Verschlüsselung sei ihnen erst nachträglich bekannt geworden.

Nach Ansicht des Gerichts ließ sich dieses Vorbringen zwar nicht widerlegen, war jedoch unbeachtlich, da die Antragsgegner in beiden Fällen nach § 97 Abs. 1 Satz 1 UrhG als Störer verantwortlich seien. Die hierfür erforderliche Mitwirkung an der rechtswidrigen Beeinträchtigung durch willentliche und adäquat kausale Verletzung von Prüfungspflichten liege vor. Die Möglichkeit von Urheberrechtsverletzungen über das Internet sei ebenso allgemein bekannt wie die Gefahr des Missbrauchs ungeschützter W-LAN-Verbindungen. Die Antragsgegner seien auch rechtlich und tatsächlich in der Lage gewesen, wirksame Gegenmaßnahmen – nämlich sichere Verschlüsselungen – zu ergreifen. Dies sei zumutbar, eine etwa erforderliche Inanspruchnahme fachkundiger Hilfe „durchaus noch verhältnismäßig". Bei Abschluss des Manuskripts war die Berufung gegen das Urteil noch anhängig.[17]

b) Strafbarkeit des Betreibers

Aus strafrechtlicher Sicht hatte das AG Euskirchen sich mit einem parallel gelagerten Fall zu beschäftigen.[18] Der Angeklagte hatte eine längere Auseinandersetzung mit einer Zeugin gehabt, und parallel dazu waren von der IP-Adresse seines Unternehmensrechners mehrere Handlungen in deren Namen erfolgt (Kfz-Versteigerungsangebot, Wohnungsanzeige bei eBay, Bestellung von CD-Rohlingen über knapp 20.000 €). Auch hier verteidigte sich der Angeklagte mit dem Argument, in seinem Unternehmen werde ein ungesichertes W-LAN betrieben.

Da insoweit keine Feststellungen getroffen werden konnten, unterstellt das AG Euskirchen diese Behauptung zu seinen Gunsten. Anders als das LG Hamburg in seiner zivilrechtlichen Beurteilung konnte es allerdings nicht darüber hinaus die Handlung eines Dritten unterstellen, ohne zugunsten des W-LAN Betreibers zu entscheiden. Für eine Verurteilung hätte es dann – da keine Fahrlässigkeitstatbestände ersichtlich waren – der Feststellung einer Mittäterschaft oder mittelbaren Täterschaft bedurft; für beides gab es keine Anhaltspunkte.

Im Ergebnis verurteilte das Gericht den Angeklagten dennoch wegen Verfälschung beweiserheblicher Daten gem. §§ 269 Abs. 1, 53 StGB. Zu den Zeitpunkten der jeweiligen Tathandlungen habe sich außer dem Angeklagten, der zudem unter der gleichen Anschrift wohnhaft war, niemand in dem Unternehmen aufgehalten. Außer dem Angeklagten habe niemand ein Motiv für die Tat gehabt. Ein Verleumdungsversuch seitens der Zeugin oder ihres Mannes scheide aus, da festgestellt werden könne, dass beide sich an anderen Orten aufgehalten hätten. Nach alldem gebe es an der Täterschaft keine vernünftigen Zweifel.

2. Zivilrechtliche Haftung

Zivilrechtlich ist zwischen den denkbaren Anspruchsgegnern und -arten zu unterscheiden. Anspruchsgegner können einerseits Private sein, die das W-LAN lediglich für sich selbst nutzen (diese sind keine Diensteanbieter nach § 3 Nr. 1 TDG[19] bzw. § 2 Nr. 1 TMG-E[20]), andererseits Access-Provider, die – entgeltlich oder kostenfrei – über ein W-LAN einen Zugang zum Internet anbieten. Handelt es sich dabei um private Anschlüsse, stellen sich zusätzlich Rechtsfragen im Verhältnis zu den Netzbetreibern, die die Bereitstellung für Dritte zum Teil in ihren AGB untersagen.[21] Da aus einem Verstoß gegen die Verträge aber kein Anspruch Dritter – z.B. der Inhaber von Urheberrechten – abgeleitet werden kann, bleibt dieses Problem im Folgenden ausgeklammert.[22]

Bei kommerziellen Hotspots kann die Arbeitsteilung schließlich auch dahin gehen, dass der Besitzer vor Ort lediglich Räumlichkeiten und Anschlüsse zur Verfügung stellt und der Netzbetreiber rechtlich direkt mit den Nutzern in Kontakt tritt.[23] In diesem Fall ist der Besitzer lediglich Erfüllungsgehilfe des Netzbetreibers und haftet nicht selbst.

Hinsichtlich der Anspruchsarten ist zwischen Unterlassungs- und Schadensersatzansprüchen zu differenzieren. Das gilt insbesondere wegen des Haftungsprivilegs der §§ 8 ff. TDG, 6 ff. MDStV (§§ 7 ff. TMG-E).[24]

16 LG Hamburg v. 26.7.2006 – 308 O 407/06, CR 2007, 54; s. *Gercke*, CR 2007, 55; *Mantz*, MMR 2006, 764; *Rössel*, ITRB 2006, 247; *Heidrich*, c't 20/2006, 52.

17 OLG Hamburg – 5 U 163/06.

18 AG Euskirchen v. 19.6.2006 – 5 Ds 279/05 (rkr., n.v.).

19 A.A. *Mantz*, MMR 2006, 764 (765) (der dort als Beleg angeführte *Spindler* in Spindler/Schmitz/Geis, TDG, 2004, vor § 8 TDG Rz. 21 bezieht sich auf privat „angebotene Dienste", aber nicht auf Selbstnutzer). Richtigerweise halten Selbstnutzer keine Teledienste „zur Nutzung" (§ 3 Nr. 1 TDG) bereit.

20 Entwurf des Telemediengesetzes vom 11.8.2006, BR-Drucks. 556/06.

21 Die Bandbreite der AGB reicht hier vom totalen Verbot über das Verbot der kommerziellen Bereitstellung bis hin zur völligen Freigabe.

22 Siehe näher *Kern*, CRi 2006, 33 (33 f.).

23 Zu entsprechenden Geschäftsmodellen s. *Hoenike/Boës*, MMR 2003, 457.

24 Der Entwurf des Telemediengesetzes vom 11.8.2006, BR-Drucks. 556/06 übernimmt den Wortlaut, sodass die folgenden Ausführungen auch für die Zeit nach der Reform gelten.

a) Unterlassungsansprüche

aa) Allgemeine Anspruchsvoraussetzungen

Nach der Rechtsprechung des BGH sind die §§ 8 ff. TDG auf Unterlassungsansprüche unanwendbar.[25] Dies folge sowohl aus dem Begriff „verantwortlich" in § 11 Satz 1 TDG, der nur die strafrechtliche Verantwortlichkeit und die Schadensersatzhaftung meine, als auch aus dem Verweis in § 8 Abs. 2 Satz 2 TDG und der Gesetzgebungsgeschichte. Die Entscheidung ist in der Literatur kontrovers aufgenommen worden.[26] Folgt man ihr, so besteht hinsichtlich der Unterlassungsansprüche kein Unterschied zwischen Anbietern und rein privaten Nutzern.

Tatbestandlich setzt ein solcher Anspruch einen willentlichen und adäquat kausalen Beitrag und die Verletzung von Prüfungspflichten voraus, deren Einhaltung dem Störer zumutbar sein muss.[27] Eine Konkretisierung ist bislang vor allem für die Betreiber von Internet-Foren[28] und -Versteigerungen erfolgt.[29] Bei letzteren ist beispielsweise eine Prüfung von Angeboten nur zumutbar, wenn der Störer auf „eine klare Rechtsverletzung hingewiesen worden ist".[30] In diesem Fall muss allerdings nicht nur gegen das konkrete Angebot vorgegangen werden; vielmehr sind auch weitere Vorsorgemaßnahmen gegen gleichartige Verletzungen zu treffen.

bb) Zumutbarkeit der Verschlüsselung?

Nach der Entscheidung des LG Hamburg ist eine solche bereits erfolgte Rechtsverletzung bei W-LANs nicht erforderlich, vielmehr ist der Schutz eines privaten Netzes stets und per se erforderlich und zumutbar. Zumindest in dieser Konsequenz ist das Urteil nicht überzeugend; dies auch, weil es internetspezifische Besonderheiten ignoriert.[31]

Angesichts der empirischen Erhebungen über die Verwendung ungesicherter W-LANs kann man bereits mit guten Gründen daran zweifeln, ob die insoweit bestehenden Gefahren tatsächlich „allgemein bekannt" sind. Letztlich dürfte die Unkenntnis die Betreiber allerdings nicht entlasten; abgesehen davon wird nicht zuletzt die Entscheidung des LG Hamburg dazu beitragen, das Bewusstsein für die Problematik zu erhöhen.

Was die Möglichkeit sicherer (WAP-/WAP2-) Verschlüsselungen angeht, so bieten die gängigen W-LAN Router diese Option. Die Handhabung ist anscheinend bislang nicht sonderlich benutzerfreundlich, dabei handelt es sich aber im Wesentlichen um eine Frage des Rechtsverhältnisses des Betreibers zum Verkäufer.[32] Offen bleibt nur die Frage, wie zu entscheiden wäre, wenn sich der Betreiber mit dem Vortrag zur Wehr setzte, er habe die WEP-Verschlüsselung gewählt, da diese aber leicht zu überwinden sei, könne dennoch nicht ausgeschlossen werden, dass ein Dritter die Verletzungshandlung begangen habe.[33]

Abzulehnen ist jedenfalls die Annahme einer anlasslosen Prüfpflicht privater Betreiber, die Voraussetzung für die Konstruktion einer allgemeinen Rechtspflicht zur Verschlüsselung privater W-LANs wäre. Angesichts der nur mittelbaren Verantwortlichkeit des Betreibers (die Eigenverantwortung des unmittelbaren Verletzers ist wesentlich zu berücksichtigen),[34] der Tatsache, dass er die Nutzung durch Dritte regelmäßig weder erkennen kann noch unterstellen muss und des Fehlens finanzieller Interessen fehlt es hier an der Zumutbarkeit.[35]

cc) Langfristige Auswirkungen

Darüber hinaus ist die Entscheidung bedenklich, weil über den Umweg des Unterlassungsanspruchs eine grundlegende Infrastrukturentscheidung getroffen wird. Das LG Hamburg war erkennbar bemüht, eine als Schutzbehauptung beurteilte Verteidigung der Antragsgegner als unerheblich zu werten, um Anbietern von illegal kopierten Daten keine einfache Ausrede zu eröffnen. Dabei dürfte das Gericht aber die Dimension der generellen Anwendung von Unterlassungsansprüchen auf die Betreiber von W-LANs nicht berücksichtigt haben. Im konkreten Fall hätten diese zwar durch eine Verschlüsselung den Anspruch möglicherweise abwenden können. Schon bei der gemeinsamen Nutzung eines Routers durch eine zahlenmäßig größere, aber geschlossene Nutzergruppe (Wohngemeinschaften, Unternehmen) tun sich kaum zu überwindende Schwierigkeiten auf, weil die gängigen Router die Netzwerktätigkeiten der Computer nicht aufzeichnen und eine gemeinschaftliche Haftung kaum begründbar sein dürfte.

Darüber hinaus gibt es Betreiber, denen es gerade auf das jedermann offen stehende Angebot ankommt, etwa altruistische freie Funknetze, Universitäten oder Gastronomiebetriebe, die sich hiervon einen erhöhten Umsatz versprechen. In der Logik der Entscheidung müssten diese Access-Provider (an sich auch unabhängig vom Einsatz von W-LAN jedermann, der einen öffentlich zugänglichen PC mit Internet-Anschluss bereitstellt) erst recht haften, da sie – anders als die Antragsgegner – die Nutzung durch unbekannte Dritte sogar zum Ziel haben. Es erscheint weder technisch praktikabel noch verhältnismäßig, die entsprechenden Anbieter von Hotspots zur Vermeidung einer Haftung für das Verhalten ihrer Kunden auf deren lückenlose Identifizierung – oder gar die fortlaufende personalisierte Verhaltensprotokollierung – zu verpflichten.[36]

25 BGH v. 11.3.2004 – I ZR 304/01, CR 2004, 763 (764 ff.); s.a. OLG Brandenburg v. 16.11.2005 – 4 U 5/05, OLGReport Brandenburg 2006, 624 = CR 2006, 124 = NJW-RR 2006, 1193 (1194 f.); für Betreiber von Internetforen OLG Hamburg v. 22.8.2006 – 7 U 50/06, OLGReport Hamburg 2006, 718 = MMR 2006, 744 (745); OLG Düsseldorf v. 7.6.2006 – I-15 U 21/06, CR 2006, 682 (683 f.); hierzu *Libertus/Schneider*, CR 2006, 626.

26 Siehe u.a. einerseits *Lement*, GRUR 2005, 210 („einzig widerspruchsfreie Interpretation") m.w.N. für beide Ansichten; andererseits abl. *Gercke*, CR 2005, 233 f.; *Gercke*, MMR 2006, 493; *Stadler*, K&R 2006, 253 (254) m.w.N.; differenzierend *Leible/Sosnitza*, NJW 2004, 3225; zum Ganzen *Volkmann*, Der Störer im Internet, 2005, S. 100 ff.; *Spindler* in Spindler/Schmitz/Geis, TDG, 2004, § 8 TDG Rz. 15 ff.; zur Störerhaftung bei Urheberrechtsverletzungen s. *Gercke*, ZUM 2006, 593; zur Störerhaftung des „Admin-C" *Wimmers/Schulz*, CR 2006, 754.

27 BGH v. 11.3.2004 – I ZR 304/01, CR 2004, 763 (766 f.).

28 Siehe einerseits OLG Düsseldorf v. 26.4.2006 – I-15 U 180/05, OLGReport Düsseldorf 2006, 581 = CR 2006, 482 = MMR 2006, 553 (weitgehender Haftungsausschluss des Betreibers), andererseits LG Hamburg v. 2.12.2005 – 324 O 721/05, CR 2006, 638 m. Anm. *Wimmers* = MMR 2006, 491 mit abl. Anm. *Gercke*; vermittelnd OLG Hamburg v. 22.8.2006 – 7 U 50/06, OLGReport Hamburg 2006, 718 = MMR 2006, 744 (das LG Hamburg korrigierend); OLG Düsseldorf v. 7.6.2006 – I-15 U 21/06, CR 2006, 682.

29 Zur Anwendung auf Zugangsprovider *Gercke*, CR 2006, 210 (241 ff.); s.a. *Spindler/Dorschel*, CR 2005, 38.

30 BGH v. 11.3.2004 – I ZR 304/01, CR 2004, 763 (767).

31 Zu dieser allgemeinen Tendenz vgl. *Jürgens*, AfP 2006, 219 (221 f.); *Stadler*, K&R 2006, 253.

32 Siehe unten 4.

33 Einerseits ließe sich erwidern, auch die WAP-Verschlüsselung sei möglich und zumutbar. Andererseits kann man vom Nutzer kaum mehr verlangen, als eine von mehreren standardmäßig bereitgestellten Verschlüsselungen einzusetzen; so auch *Mantz*, MMR 2006, 764 (765). Allerdings besteht das Risiko, dass das Gericht dann trotz der Unsicherheit des WEP eine Handlung des Betreibers annehmen könnte.

34 Siehe auch *Wimmers/Schulz*, CR 2006, 754 (763 f.).

35 Zur weitgehenden Haftungsfreistellung im US-amerikanischen Recht vgl. *Kern*, CRi 2006, 33 (34 f.).

36 Siehe auch *Kern*, CRi 2006, 33 (33 ff.).

Will man diese Weiterungen vermeiden, die auch der BGH in seiner Entscheidung sicher nicht beabsichtigt hat (dort wurde die Vorsorgepflicht maßgeblich unter Bezug auf das Provisionsinteresse des Betreibers der Versteigerungs-Plattform begründet),[37] müssen Access-Provider und private Nutzer von W-LANs von der Unterlassungshaftung ausgenommen werden oder diese darf zumindest – vergleichbar der der Foren-Betreiber oder Internetversteigerer (s.o.) – erst eingreifen, wenn der Betreiber auf eine Rechtsverletzung aufmerksam geworden ist.[38] Geschieht beides vor dem Hintergrund der Interessen der Rechteinhaber nicht, muss man sich zumindest darüber im Klaren sein, dass damit zukunftsträchtige Bausteine einer künftigen Netzwerkinfrastruktur verhindert werden.

b) Schadensersatzansprüche und Haftungsprivileg

Während die generelle Anwendbarkeit von TDG und MDStV auf Access-Provider umstritten ist, genießen sie jedenfalls nach ganz h.M. die Haftungsprivilegien nach §§ 8 ff. TDG bzw. 6 ff. MDStV.[39] Die Frage der drahtlosen oder drahtgebundenen Kommunikation spielt insoweit keine Rolle. Da weder die Begriffe des Tele- und Mediendienstes noch der des Diensteanbieters eine Gewinnerzielungsabsicht voraussetzen, sind auch freie Funknetze im Rahmen der Privilegierung von der Haftung für fremde Informationen freigestellt. Wenn der Besitzer des Hotspots lediglich Erfüllungsgehilfe des eigentlichen Anbieters ist (s.o.), haftet er ohnehin nicht.

Die Frage des Schadensersatzanspruchs ist folglich nur für private Nutzer von W-LANs relevant,[40] also in der Konstellation, die der Entscheidung des LG Hamburg zugrunde lag. Das Gericht musste sich zwar mit der Frage des Verschuldens nicht befassen, die nur für den Schadensersatz-, nicht aber für den Unterlassungsanspruch relevant ist. Mit den Argumenten des Gerichts zur Störerhaftung ließe sich aber auch ein Verschulden bejahen: Wenn die Möglichkeit des Missbrauchs offener W-LAN-Verbindungen und die Gefahr von Urheberrechtsverletzungen über das Internet allgemein bekannt sind, könnte dies die Vorhersehbarkeit begründen; angesichts der Verfügbarkeit von Verschlüsselungstechnik ließe sich der schädigende Erfolg auch vermeiden.[41]

Allerdings würde diese Argumentation dazu führen, dass den Betreiber eines W-LANs, das Dritte ohne sein Wissen nutzen, mehr Überwachungspflichten treffen würden als die Betreiber kommerzieller oder freier Hotspots, die den Zugang für Dritte absichtlich eröffnen. Um dieses schwer hinnehmbare Ergebnis zu vermeiden, kann der reine Betrieb eines ungeschützten W-LANs noch keinen Fahrlässigkeitsvorwurf begründen, sondern höchstens das Hinzutreten weiterer Umstände, etwa die Kenntnis von Urheberrechtsverletzungen Dritter über das Netzwerk.

Der Ausschluss der Fahrlässigkeitshaftung lässt sich im Wege des Erst-Recht-Schlusses aus §§ 8 ff. TDG, 6 ff. MDStV, mit den Grundsätzen des erlaubten Risikos[42] oder – letztlich wohl entscheidend – mit dem fehlenden Zurechnungszusammenhang (vorsätzliches Handeln eines Dritten)[43] begründen.[44] Auf der Wertungsebene ist jedenfalls eindeutig, dass der Privatmann, dessen W-LAN gegen seinen Willen genutzt wird, nicht weiter haften darf als Anbieter freier Netze, die die Nutzung durch Dritte nicht nur in Kauf nehmen, sondern sogar anstreben.

3. Strafrechtliche Verantwortlichkeit

In strafrechtlicher Hinsicht müssen zwei Konstellationen unterschieden werden:

(a) Zum einen können sich Betreiber unzureichend gesicherter W-LANs dem Vorwurf aussetzen, Dritten verbotene oder jugendgefährdende Inhalte zugänglich zu machen.

(b) Zum anderen besteht die Gefahr, dass Dritte über das W-LAN Straftaten begehen und dies auf den Betreiber zurückfällt (so die Behauptung des Angeklagten im Fall des AG Euskirchen).

a) Zugänglichmachen von Inhalten

Die Frage des Zugänglichmachens von Inhalten ist bislang vor allem hinsichtlich einer entsprechenden Verantwortlichkeit von Internetcafé-Betreibern (insbesondere nach §§ 131, 184 Abs. 1, 3 StGB, 23 f. JMStV) erörtert worden. Für diese wird zumindest in der Literatur eine Unterlassungstäterschaft als möglich erachtet, da wegen des Betriebs eine Garantenstellung aus Ingerenz und angesichts der Offensichtlichkeit der Verfügbarkeit der entsprechenden Inhalte im Internet auch Eventualvorsatz zu bejahen seien.[45] Allerdings ist die Strafbarkeit wegen der Haftungsprivilegierung nach § 9 TDG umstritten.[46] Dieses Problem soll hier nicht vertieft werden, weil insoweit jedenfalls kein Unterschied zwischen leitungsgebundenen und drahtlosen Zugangsangeboten besteht.

Für private Betreiber offener W-LANs kommen jedenfalls ausschließlich Fahrlässigkeitsdelikte in Betracht, im konkreten Fall damit wohl nur § 23 Satz 2 JMStV und Ordnungswidrigkeiten nach § 24 JMStV. Der Fahrläs-

37 BGH v. 11.3.2004 – I ZR 304/01, CR 2004, 763 (767); s.a. OLG München v. 21.9.2006 – 29 U 2119/06, OLGReport München 2006, 904 = MMR 2006, 739 (740 f.); *Feldmann*, MMR 2006, 746 (748); *Spindler* in Spindler/Schmitz/Geis, TDG, 2004, § 8 TDG Rz. 28.

38 In diese Richtung auch *Gercke*, ZUM 2006, 593 (598 f.); *Gercke*, CR 2007, 55; s.a. für den „Admin-C" *Wimmers/Schulz*, CR 2006, 754 (762 f.).

39 *Volkmann*, Der Störer im Internet, 2005, S. 19 f.; *Sieber*, Verantwortlichkeit im Internet, 1999, Rz. 262 f.; *Spindler* in Spindler/Schmitz/Geis, TDG, 2004, § 9 TDG Rz. 14, jeweils m.w.N.; für Mediendienste OVG NW v. 9.3.2003 – 8 B 2567/02, CR 2003, 361 (364); für W-LAN *Liesching/Knupfer*, MMR 2003, 562 (567) m.w.N.; a.A. *Stadler*, Haftung für Informationen im Internet, 2002, Rz. 38 f.

40 Diese genießen entgegen *Mantz*, MMR 2006, 764 (765 f.) kein Haftungsprivileg nach § 9 TDG (s.o. Fn. 19).

41 Vorhersehbarkeit und Vermeidbarkeit sind Voraussetzungen des Fahrlässigkeitsvorwurfs, s. BGH v. 21.5.1963 – VI ZR 254/62, BGHZ 39, 271 (285); *Heinrichs* in Palandt, BGB, 65. Aufl. 2006, § 276 Rz. 20 f.

42 Dazu im Zusammenhang mit den §§ 8 ff. TDG *Vassilaki*, MMR 2002, 659.

43 Hierfür wird nur in Herausforderungsfällen und dann gehaftet, wenn der entstandene Schaden vom Schutzzweck der verletzten Norm miterfasst ist (BGH v. 6.1.1989 – III ZR 192/87, MDR 1989, 798 = BGHZ 106, 313; *Heinrichs* in Palandt, BGB, 65. Aufl. 2006, Vorb. v. § 249 Rz. 76 ff.) Beides ist beim bloßen Betrieb eines privaten offenen W-LANs nicht der Fall.

44 Eine Parallele ließe sich auch zur Frage der Verkehrssicherungspflicht durch den bloßen Betrieb eines mit dem Internet verbundenen Computers (hinsichtlich der Verbreitung von Viren) ziehen, die für Privatleute nicht oder nur sehr eingeschränkt besteht, s. *Schneider/Günther*, CR 1997, 389 (396); *Koch*, NJW 2004, 801 (804 ff.); *Libertus*, MMR 2005, 507 (507 ff.).

45 *Liesching/Günter*, MMR 2000, 260 (262 f.); *Liesching/Knupfer*, MMR 2003, 562 (563 f., 570) – a.A. aber die dort zitierten StA München und Heidelberg.

46 Gegen die Verantwortlichkeit *Lenckner/Perron* in Schönke/Schröder, StGB, 27. Aufl. 2006, § 184 Rz. 55 m.w.N.; a.A. *Liesching/Günter*, MMR 2000, 260 (263 ff.); *Liesching/Knupfer*, MMR 2003, 562 (567 f.); vermittelnd *Spindler*, MMR 2004, 440 (443 f.); *Spindler* in Spindler/Schmitz/Geis, TDG, 2004, § 9 TDG Rz. 11 ff. (Pflicht zu deutlichen Hinweisen auf die Rechtslage, aber keine Kontrollbefugnis der Betreiber).

sigkeitsvorwurf an die Betreiber von Internetcafés wird allerdings maßgeblich mit der Verfügungsgewalt über die Räume und den engen persönlichen Kontakt zu den Nutzern begründet.[47] Beides trifft hier nicht zu. Allein das Bewusstsein, dass sich in Reichweite des W-LANs Kinder und Jugendliche aufhalten könnten und diese ggf. über das Netz jugendgefährdende Inhalte zur Kenntnis nehmen könnten, begründet keine Fahrlässigkeitstäterschaft des Betreibers.

b) Straftaten durch die Nutzer des W-LANs

Hinsichtlich der Begehung von Straftaten durch einen Nutzer des W-LANs ist nochmals zu betonen, dass hier die Frage regelmäßig nicht offen bleiben kann, wer die konkrete Handlung begangen hat. Dies ist nur der Fall, wenn zwischen den in Betracht kommenden Personen Mittäterschaft besteht oder eine wahlweise Verurteilung wegen unmittelbarer oder mittelbarer Täterschaft möglich ist. Denkbar ist darüber hinaus eine Beihilfe zu einer Straftat Dritter durch die Bereitstellung des drahtlosen Internetzugangs. Für den Gehilfenvorsatz, der sich auf die wesentlichen Merkmale der Haupttat beziehen muss,[48] ist aber die Kenntnis des Betreibers Grundvoraussetzung; allein das abstrakte Bewusstsein der Möglichkeit der Begehung von Straftaten über ein offenes W-LAN reicht hierzu nicht aus.

Wenn nach diesen Grundsätzen die tatrichterliche Feststellung des Handelnden erforderlich ist, so führt der nicht widerlegte Einwand, über das offen betriebene W-LAN habe mehr oder weniger jedermann die Straftat begehen können, für die meisten Delikte zum Ausschluss der Strafbarkeit. Der Fall des AG Euskirchen ist insofern eine Besonderheit, als es sich um eine Beziehungstat handelte, bei der das Gericht aufgrund der langen Vorgeschichte, d.h. anhand sonstiger Umstände eine Beweiswürdigung vornehmen konnte. Bei dem praktisch wichtigen § 106 UrhG kommt dagegen im Regelfall jeder musikinteressierte Inhaber eines W-LAN fähigen Computers, der sich zum fraglichen Zeitpunkt in der Nähe hätte aufhalten können, als Täter in Betracht. Selbst innerhalb geschlossener Nutzergruppen (verschlüsseltes W-LAN in Familien, Wohngemeinschaften, Unternehmen oder ähnliches) dürfte es in vielen Fällen schwer sein, den tatsächlichen Täter zu ermitteln.[49] Nur wenn die Nutzerzahl überschaubar ist, kommt eine Beschlagnahme und Untersuchung der Rechner aller denkbaren Täter in Betracht.

4. Verantwortlichkeit der Hersteller

Den bisherigen Ausführungen liegt mehr oder weniger implizit die Annahme zugrunde, dass es den Betreibern technisch möglich ist, ihr W-LAN sicher gegen Angriffe zu verschlüsseln. Offenbar lässt die Nutzerfreundlichkeit der Software aber in einer Vielzahl von Fällen deutlich zu wünschen übrig. Überdies enthalten die Produkte keine Hinweise auf die möglichen Haftungsrisiken der Betreiber.

Die daraus resultierenden produkthaftungs- und verbraucherschutzrechtlichen Probleme können hier nur aufgeworfen werden. Sollte sich die Rechtsauffassung des LG Hamburg durchsetzen, wäre unter dem Gesichtspunkt der Instruktionspflicht des Herstellers[50] ein entsprechender Hinweis zu fordern, der auch eine leicht verständliche Bedienungsanleitung für die Verschlüsselung und Informationen über die Sicherheitslücken des WEP umfassen müsste. Noch sinnvoller wäre es, die WAP- oder WAP2-Verschlüsselung standardmäßig schon in die Konfiguration des Erstbetriebs aufzunehmen. Mittlerweile existieren Produkte, bei denen dies der Fall ist.[51]

IV. Reichweite der EU-Richtlinie über die Vorratsdatenspeicherung

Die rechtliche Verantwortlichkeit der Betreiber von W-LANs wird in naher Zukunft eine weitere Dimension erhalten, wenn das deutsche Umsetzungsgesetz zur europäischen Richtlinie über die Vorratsdatenspeicherung[52] in Kraft tritt.

Nach § 110a Abs. 1 Satz 1 des Referentenentwurfes vom 8.11.2006[53] trifft die Pflicht zur Speicherung der Verkehrsdaten jeden, der „Telekommunikationsdienste für die Öffentlichkeit erbringt oder daran mitwirkt". Werden Internetzugangsdienste angeboten, so sind nach § 110a Abs. 4 TKG-E die zugewiesene IP-Adresse, eine eindeutige Anschlusskennung sowie Beginn und Ende der Internetnutzung zu speichern.

1. Speicherpflicht für Hotspot-Betreiber

Beim Betrieb von W-LANs ist damit zu differenzieren. Kommerzielle Anbieter von Hotspots erbringen Telekommunikationsdienste für die Öffentlichkeit und unterfallen folglich der Speicherungspflicht. Gleiches gilt – da weder Gewinnerzielungsabsicht noch Geschäftsmäßigkeit erforderlich sind – für freie Funknetze.[54] Diese müssen entweder den Betrieb einstellen oder eine Nutzerkennung einführen. Sie unterfallen zwar nicht der Registrierungspflicht nach § 111 TKG-E, die Speicherung der „dem Teilnehmer für eine Internetnutzung zugewiesenen IP-Adresse" nach § 110a Abs. 4 Nr. 1 TKG-E ist aber nur möglich, wenn der Betreiber den Teilnehmer kennt. Diese Folgen für freie W-LANs waren zwar offenbar von der *Kommission* nicht beabsichtigt,[55] ergeben sich aber eindeutig aus dem Wortlaut des Entwurfs. Inhaltlich verbirgt sich dahinter das Problem, dass eine zunehmende Zahl freier W-LANs ohne Speicherpflicht den Sinn der Richtlinie ad absurdum führen könnte.

Auch nach der Begründung des Entwurfs sollen allerdings unternehmensinterne Netze nicht erfasst sein.[56] Angesichts des Tatbestandsmerkmals „für die Öffentlichkeit" muss das für alle geschlossenen Nutzergruppen gelten. Wenn also private Netzwerke, Nachbarschafts-

47 *Liesching/Knupfer*, MMR 2003, 562 (564 f.).
48 BGH v. 18.4.1996 – 1 StR 14/96, BGHSt 42, 135 (137) = MDR 1996, 837; *Tröndle/Fischer*, StGB, 53. Aufl. 2006, § 27 Rz. 8.
49 Siehe auch *Dietrich*, NJW 2006, 809 (811).
50 Vgl. BGH v. 24.1.1989 – VI ZR 112/88, BGHZ 106, 273 = MDR 1989, 534; v. 12.11.1991 – VI ZR 7/91, BGHZ 116, 60 = MDR 1992, 130; *Sprau* in Palandt, BGB, 65. Aufl. 2006, § 3 ProdHaftG Rz. 10 ff. m.w.N.
51 Siehe *Endres*, c't 25/2006, 99.
52 RL 2006/24/EG v. 15.3.2006, ABl. EU Nr. L 105, 54; zu den Rechtsfragen s. u.a. *Breyer*, Die systematische Aufzeichnung und Vorhaltung von Telekommunikations-Verkehrsdaten für staatliche Zwecke in Deutschland, 2005; *Alvaro*, DANA 2006, 52; *Roßnagel*, EuZ 2006, 30; *Sierck/Schöning/Pöhl*, Zulässigkeit der Vorratsdatenspeicherung, 2006 (Gutachten des Wissenschaftlichen Dienstes des Bundestages).
53 Abrufbar unter *www.humanistische-union.de/fileadmin/hu_upload/doku/vorratsdaten/de-recht/bmj_2006.11.pdf*.
54 Entgegen *Gercke*, ZUM 2006, 593 (596) wird sich die Rechtslage für diese folglich ändern.
55 Diese führt in einer Stellungnahme gegenüber dem Europäischen Parlament (*www.edri.org/docs/Technical_Questions_on_Data_Retention_ans.vers.pdf*) aus, bei offenen W-LANs könne der tatsächliche Nutzer zwar nicht identifiziert werden, die Standortbestimmung sei aber eine für die Behörden wichtige Information.
56 Siehe S. 144 des Entwurfs unter *www.humanistische-union.de/file/admin/hu_upload/doku/vorratsdaten/de-recht/bmj_2006.11.pdf*.

gruppen, studentische Wohnheime und vergleichbare Gruppen das W-LAN technisch auf registrierte Nutzer beschränken, entfällt die Speicherpflicht.

2. Auswirkungen für private Selbstnutzer?

Zweifelhaft ist dagegen die Rechtslage für private, unverschlüsselte W-LANs, die nur zum eigenen Gebrauch verwendet werden. Es ließe sich argumentieren, dass diese zumindest faktisch öffentlich sind. Die Speicherpflicht ergibt hier jedoch keinen Sinn, weil die Betreiber davon ausgehen, das Netz nur selbst zu nutzen. Außerdem lässt sich der Formulierung „für" die Öffentlichkeit (§ 110a Abs. 1 Satz 1 TKG-E) entnehmen, dass ein Widmungsakt des Betreibers – zumindest konkludent, etwa durch das bewusste Tolerieren der Drittnutzung – erforderlich ist und private W-LANs folglich im Regelfall vom Entwurf nicht erfasst werden.

Schließlich käme in Betracht, die Regelung gerade wegen der Ungeeignetheit der Speicherpflicht für private Selbstnutzer so zu verstehen, dass der Betrieb unverschlüsselter privater W-LANs unzulässig ist. Ein solches allgemeines Verbot für die ausschließlich private Nutzung kann jedoch ohne ausdrückliche Regelung nicht angenommen werden. Das muss gerade wegen der erheblichen Bußgeldandrohung im Falle eines Verstoßes (bis zu 500.000 € nach § 149 Abs. 1 Nr. 28a, Abs. 2 TKG-E) gelten.

V. „Offene" Netze als Komponenten einer zukünftigen Informations-Infrastruktur

Die mittel- und langfristige Perspektive der hier erörtern Rechtsfragen betrifft nicht nur die Haftungsrisiken privater W-LAN Nutzer (die durch sichere Verschlüsselungstechnik weithin vermieden werden können) und die Gefährdung von Geschäftsmodellen der Gaststätten und Cafés, die sich durch das kostenlose Angebot des drahtlosen Internetzugangs höhere Umsätze erhoffen. Vielmehr wird gerade in der Verbindung aus Unterlassungsanspruch und Vorratsdatenspeicherung deutlich, dass es um eine Grundentscheidung über die Kommunikationsinfrastruktur von morgen geht.

Schon das Risiko, Unterlassungsansprüchen ausgesetzt zu sein, würde dazu führen, dass die Anbieter freier W-LANs entweder auf eine Identifizierung der Nutzer bestehen oder – da dies vielfach undurchführbar sein wird – den Betrieb einstellen. Das gilt erst recht, wenn der TKG-Entwurf in der bisherigen Fassung Gesetz wird und alle freien Funknetze der Pflicht zur Vorratsspeicherung unterwirft. Angesichts der weitreichenden Vorteile von Ad-hoc-Netzwerken, die gerade keine Aushandlung von Nutzungsbedingungen im Einzelfall erfordern,[57] ist diese Entwicklung mehr als bedenklich.

Begreift man die flächendeckende Verfügbarkeit von W-LAN als einen ersten Schritt hin zu einer Welt des Ubiquitous Computing, so werden darüber hinausgehende Gefahren deutlich: Wenn durch die Anordnung einer umfassenden Vorratsdatenspeicherung oder über den Umweg einer zivilrechtlichen Inanspruchnahme der Einzelne, der als Nutzer von Location Based Services und anderen kontextsensitiven Diensten praktisch ständig Netzverbindungen unterhalten wird, fortlaufend gezwungen ist sich zu identifizieren und seine Daten über einen langen Zeitraum gespeichert werden, ergeben sich weitreichende Gefahren der Bildung von Persönlichkeitsprofilen.[58] Diese Dimension mag von der Entscheidung des LG Hamburg relativ weit in die Zukunft gedacht sein; indes sollte die langfristige Wirkung technischer und rechtlicher Strukturentscheidungen nicht unterschätzt werden.

57 Siehe *Kern*, CRi 2006, 33 (33 ff.).

58 Zu den datenschutzrechtlichen Problem des Ubiquitous Computing s. *Roßnagel/Müller*, CR 2004, 625; *Roßnagel*, MMR 2005, 71; *Roßnagel/Jandt/Müller/Gutscher/Heesen*, Datenschutzfragen mobiler kontextbezogener Systeme, 2006; sowie den Abschlussbericht des TAUCIS-Projekts, *www.taucis.hu-berlin.de/content/de/ueberblick/index.php*; zum Problem der Persönlichkeitsprofile *Jandt/Laue*, K&R 2006, 316.

Robert Kazemi

Online-Nachrichten in Suchmaschinen

Ein Verstoß gegen das deutsche Urheberrecht?

Seitdem der amerikanische Suchmaschinenriese „google" im Juli 2003 mit seinen „google-news" ein deutschsprachiges Nachrichtenangebot freigeschaltet hat, werden hier im Schnitt täglich über 700 deutschsprachige Online-Nachrichtenquellen ausgewertet. Ähnliches bietet seit Juli 2004 auch Microsoft mit seinem Angebot „newsboot" über die Plattform „msn" an. Diese kostenlosen und (zumindest derzeit) „werbefreien" Angebote vermitteln über ein Schlagzeilensystem – wie es auch die großen Boulevardzeitungen verwenden – einen schnellen, nach Rubriken geordneten Überblick über das aktuelle Geschehen. So praktisch diese Angebote auch für den Internet-User sein mögen, um so mehr sind sie einigen Presseagenturen und Zeitungsverlegern ein Dorn im Auge. Sie sehen durch die Angebote ihre Urheberrechte verletzt und haben sich zuletzt in einigen europäischen Ländern (erfolgreich) gerichtlich gegen Google und Co. gewendet. Obwohl es in der Bundesrepublik bislang (noch) nicht zu gerichtlichen Auseinandersetzungen dieser Art gekommen ist, soll die Problematik nachfolgend unter dem Blickwinkel des deutschen Urheberrechts betrachtet werden.

I. Einleitung

1. Funktionsweise der Online-Nachrichten-Portale

Bei jeder Recherche im Internet sieht sich der Nutzer einer Quelle unzähliger und unüberschaubarer Informationen gegenüber. Stets steht er vor dem Problem, Wesentliches von Unwesentlichem zu unterscheiden. Die beliebteste Form der Problembewältigung ist der Einsatz

▷ Robert Kazemi ist Rechtsreferendar am OLG Koblenz.