Wenn sich hingegen Werbe- oder Bildagenturen, die dem grundgesetzlichen Schutz des Art. 5 III GG nicht unterfallen, in ihrer Arbeit mit Abbildungen von nackten Kindern und Jugendlichen bald beschränkt sehen, so lässt sich dies nach Abwägung der berührten Rechtsgüter gut vertreten. An diesem Beispiel zeigt sich, wie eingangs angesprochen, wie sich vor dem Hintergrund eines gesellschaftlichen und technischen Wandels die Grenzen dessen verschieben, was für vertretbar oder nicht mehr vertretbar erachtet wird. Die größere Zurückhaltung bei der Akzeptanz für den realen kindlichen Akt, jedenfalls in seiner kommerzialisierten Form, kann durchaus als zivilisatorischer Fortschritt gesehen werden. Die frühere Unbedarftheit bei der Verwendung von Darstellungen von nicht oder nur teilweise bekleideten Kindern und Jugendlichen in der Werbung oder zur Bebilderung redaktioneller Inhalte darf angesichts der heute offenbaren Gefahren eines Missbrauchs der Bilder durch pädosexuelle Täter schlechterdings nicht mehr maßstabgebend sein. Im Zeitalter des Internets und anderer Massenmedien mit erhöhter Reichweite und fehlender Halbwertszeit für einmal veröffentlichte Bilder kann auch die punktuelle Einwilligung der Eltern kein Freibrief sein: das kommerzielle Interesse – auch der Eltern – muss vor einem umfassenden Schutz der Minderjährigen zurückstehen. ■

Professor Dr. Thomas Hoeren und Ref. iur. Sebastian Jakopp*

WLAN-Haftung – A never ending story?

Viele Kommunen überlegen derzeit, ob sie in ihrem Gemeindegebiet frei zugängliche WLAN-Netze einführen sollen. In Berlin, Pforzheim oder Heidenheim finden sich bereits solche Netze. Doch die Haftung der Betreiber von freien WLANs ist zurzeit noch ungeklärt, trotz zunehmender Rechtsprechung zu dieser Frage und des Versuchs der Bundesregierung, diese Frage im Koalitionsvertrag 2013 zu lösen.

I. Einführung

Seit Jahren wird über die Verantwortlichkeit eines WLAN-Betreibers gestritten. Klare Linien zeichnen sich erst allmählich ab. Ausgangspunkt für die Deliktshaftung im Zivilrecht sind die strafrechtlichen Beurteilungsmaßstäbe hinsichtlich Täter, Teilnehmer, Anstifter und Gehilfe[1]. Hinzu kommt gerade für den WLAN-Sektor die zivilrechtliche Sonderkonstruktion des so genannten Störers.

Kann der WLAN-Inhaber nicht als Täter/Teilnehmer eingestuft werden, weil ein Dritter (ohne das Wissen des WLAN-Betreibers) die Rechtsverletzung begangen hat, muss er sich nach den Grundsätzen der Störerhaftung verantworten, §§ 823, 1004 BGB analog. Daneben können je nach Rechtsverletzung auch andere Anspruchsgrundlagen einschlägig sein, etwa § 97 UrhG, § 3 UWG, §§ 14, 15 MarkenG, §§ 22, 23 KUG et al.

Als Störer kann nach ständiger Rechtsprechung derjenige in Anspruch genommen werden, der – ohne Täter oder Teilnehmer zu sein – in irgendeiner Art und Weise zur Rechtsverletzung adäquat kausal beigetragen hat[2].

Die Adäquanz der Bedingung ist dann gegeben, 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[3].

Die Haftung des Dritten soll jedoch nicht über Gebühr auf den Dritten erstreckt werden. Deswegen rekurriert der *BGH* auf die Verletzung der Prüfpflichten des vermeintlichen Störers. Deren Umfang soll sich wiederum danach bestimmen, inwieweit dem in Anspruch genommenen Störer eine Prüfung oblag[4].

II. Privat betriebene WLAN-Netzwerke

1. Entscheidung des BGH v. 12.5.2010

Der *BGH* geht davon aus, dass der Betrieb eines nicht ausreichend gesicherten privaten WLAN-Netzwerks adäquat kausal für Urheberrechtsverletzungen sei, die Dritte unter Ausnutzung dieser Sicherungslücke begehen. Zum einen sei nicht unwahrscheinlich, dass sich Dritte eines solchen ungesicherten WLANs bedienten; zum anderen sei es Privatpersonen zumutbar, ihr WLAN vor dem Eingriff Dritter zu schützen, was sich schon aus dem individuellen Interesse am Schutz der eigenen Daten ergebe[5]. Deswegen sei es zumutbar, dass der WLAN-Betreiber, der das Netzwerk in Benutzung nimmt, überprüft, ob die Sicherungsmaßnahmen ausreichend sind, damit Dritte das WLAN nicht für Rechtsverletzungen nutzen. Die Pflichten bestimmten sich wiederum nach dem Einzelfall[6].

Kritisch wurde in der Literatur zu diesem Urteil angemerkt, es könne nicht angenommen werden, dass jeder Netzwerkbetreiber Interesse am Schutz der eigenen Daten habe[7]. Ferner sei es nicht nachvollziehbar, warum der *BGH* an dieser Stelle das Eigeninteresse des Privaten an dem Schutz seiner eigenen Daten mit dem der Zumutbarkeit von Maßnahmen zum Schutze vor Rechtsverletzungen Dritter vermischt[8].

2. Ab wann gelten die Sicherungspflichten?

Nach Aussage des *BGH* besteht die Sicherungspflicht schon vor dem ersten Rechtsverstoß, genauer gesagt ab Inbetriebnahme des Anschlusses. Zur Begründung führt der *BGH* an, dass die bekannten Grundsätze zur Provider-Störerhaftung, nach welchen entsprechende Sicherungspflichten erst ab Kenntnis einer Rechtsverletzung zu ergreifen sind, auf private WLAN-Netzwerke keine Anwendung fänden, da in diesem Zusammenhang kein Geschäftsmodell bestünde, welches durch Sicherungspflichten torpediert werden könnte; des Weiteren ist der *BGH* der Ansicht, dass die Haftungsprivile-

* Der Autor *Hoeren* ist Professor für Medienrecht an der Universität Münster, der Autor *Jakopp* ist zurzeit Rechtsreferendar.

1 So zuletzt *LG Frankfurt a. M.*, GRUR-RR 2013, 507 = ZUM-RD 2014, 36 (37 f.), unter Verw. auf *BGH*, GRUR 2011, 152 (154) – Kinderhochstühle im Internet.

2 Vgl. nur *BGH*, NJW 2010, 2061 = MMR 2010, 565 (566) – Sommer unseres Lebens, unter Verw. auf *BGH*, NJW-RR 2008, 1136 = CR 2008, 579 (581) – Internet-Versteigerung III.

3 *LG Hamburg*, MMR 2006, 763 (764).

4 Vgl. nur *BGH*, NJW 2010, 2061 = MMR 2010, 565 – Sommer unseres Lebens.

5 Vgl. nur *BGH*, NJW 2010, 2061 = MMR 2010, 565 – Sommer unseres Lebens.

6 *BGH*, NJW 2010, 2061 = MMR 2010, 565 (566) – Sommer unseres Lebens.

7 *Spindler*, CR 2010, 592 (596).

8 *Spindler*, CR 2010, 592 (596), Anm. *Leible/Jahn*, LMK 2010, 306719, sowie Anm. *Nenninger*, NJW 2010, 2064.

gien der § 10 TMG bzw. Art. 14 f. der RL 2000/31/EG nicht für private WLAN-Netze gelten[9].

Nach anderer Ansicht sollen Sicherungs- und Prüfungspflichten erst dann entstehen, wenn konkrete Anhaltspunkte für einen Rechtsverstoß bestehen[10]. Diese Ansicht geht zu Recht davon aus, dass der *BGH* die Reichweite des TMG falsch einschätzt. Der *BGH* geht zum Beispiel auf die Anwendbarkeit des § 8 TMG auf den privaten WLAN-Betreiber nicht ein. Unklar bleibt, ob der *BGH* § 8 TMG von vornherein nicht für Vorschriften anwendbar hält, so dass er diesen nicht geprüft hat, oder vielleicht § 8 und § 10 TMG „verwechselt"[11] hat[12]. Der *BGH* konstatiert ferner in gewisser Weise eine Pflicht des WLAN-Betreibers, Rechtsverstöße bzw. Straftaten eines Dritten zu verhindern. Es kann argumentiert werden, dass diese Pflicht nicht mit der Werteordnung des Grundgesetzes vereinbar ist[13]. Die Ausstrahlungswirkung des Grundgesetzes auf zivilrechtliche Sachverhalte begründet die Pflicht zur Einbeziehung der Grundsätze des Vertrauens und der Eigenverantwortlichkeit. Die freiheitliche Werteordnung des Grundgesetzes könne nicht mit einer „Präventionsgesellschaft" in Einklang gebracht werden[14].

3. WLAN-Betreiber als Access Provider

Nach überwiegender Auffassung ist der WLAN-Betreiber als Access-Provider iSv § 8 TMG anzusehen[15], unabhängig davon, ob er gewerblich oder privat tätig ist[16].

Eine weitere Meinung schließt die Anwendbarkeit des § 8 TMG auf Private aus[17]. Wiederum andere sind der Ansicht, dass § 8 TMG zumindest analog zur Anwendung kommen müsse[18].

Der *BGH* rekurriert nur auf § 10 TMG und hält diesen für nicht einschlägig[19]. Insoweit ist ihm zuzustimmen, da der WLAN-Betreiber in seiner Ursprungsform nur Daten durchleitet, aber nicht speichert. Der *BGH* hat die mögliche Einstufung des privaten WLAN-Betreibers als Access-Provider iSv § 8 TMG nicht gesehen.

Dabei muss die Anwendung des § 8 TMG bejaht werden. Der Anwendungsbereich des TMG erstreckt sich ausweislich der Regierungsbegründung auch auf Private[20]. Es wäre überdies nicht einzusehen, warum dem Privaten strengere Anforderungen auferlegt werden sollten als dem geschäftlichen Betreiber eines WLAN-Netzes, welcher in der Regel bestimmungsgemäß mit weitaus mehr Nutzern und mithin potenziellen Rechtsverletzern in Berührung kommt als Private[21].

4. Tatbestandliches Wollen der Zugangsvermittlung

Nach einer differenzierenden Ansicht in der Literatur soll der Diensteanbieter im Sinne des TMG nur derjenige sein, der den Zugang zum Internet auch willentlich vermittelt. Bei WLAN-Betreibern kann es offensichtlich zu ungewollten Vermittlungen kommen. Argumentativ wird unter anderem vorgetragen, dass §§ 2 S. 1, 8 I TMG von „Zugang (...) vermitteln" sprechen, was eine subjektive Komponente beinhalte[22].

Soweit die Autoren jedoch diese Ansicht vertreten, erkennen sie weitergehend an, dass § 8 TMG die strafrechtliche und deliktsrechtliche Verantwortlichkeit regelt, bei welchen Formen es auch zu einer fahrlässigen Begehung kommen kann. Da ein Tatbeitrag in fahrlässiger Begehungsweise weniger schwer wiege als ein die Kenntnis der Durchleitung von Informationen durch die angebotene Infrastruktur, müsse die ungewollte Zugangsvermittlung erst Recht nach den §§ 8, 9 TMG analog privilegiert werden[23]. Nach einer anderen Ansicht soll auch die fahrlässige Zugangsvermittlung von § 8 TMG direkt erfasst werden[24].

Im Ergebnis scheinen alle Ansichten zu demselben Schluss zu kommen und die Anwendung des § 8 TMG (zumindest analog) zu befürworten. Eine Stellungnahme hätte allenfalls klarstellende Funktion: Ob der Gesetzgeber und der europäische Richtliniengeber dieses Problem gesehen haben, mag dahinstehen; jedenfalls erscheint es aus dieser Sicht zu kurz gegriffen, auf die subjektive Komponente des Verbs „vermitteln" zurückzugreifen. Unzählige Verben im deutschen Sprachgebrauch haben eine subjektive Komponente.

In § 8 TMG geht es vielmehr um den – Vorgang – der Zugangsvermittlung. Dieser Vorgang geschieht rein objektiv und ist im Grunde schon durch die Bereitstellung und Aktivierung des WLAN-Netzwerks dauerhaft erbracht. Die Tatsache, dass ein Dritter sich in dieses Netzwerk unerlaubt einwählt, ändert nichts daran, dass der Vorgang der Zugangsvermittlung schon stattgefunden hat. Im Übrigen würde der Anwendungsbereich des § 8 TMG ad absurdum geführt, wenn es auf die Willentlichkeit ankäme: Die Nrn. 1-3 des § 8 I 1 TMG lassen gerade die Verantwortlichkeit für fremde Informationen ausscheiden, wenn der Provider an deren Auswahl nicht mitgewirkt und deren Übermittlung nicht veranlasst hat. § 8 I 1 TMG ist also so zu verstehen, dass der 1. Halbsatz die Verantwortlichkeit für objektive Handlungen ausscheiden lässt, sofern nicht die im 2. Halbsatz durch die Nrn. 1-3 konkretisierten subjektiven Mitwirkungshandlungen vorliegen.

5. Teleologische Reduktion des § 8 TMG bei Kontrollmöglichkeit des Nutzers?

Teilweise wird vertreten, dass die Haftungsprivilegierung des § 8 TMG wegfallen soll, wenn der WLAN-Betreiber die Möglichkeit der Kontrolle des Nutzers hat, beispielsweise durch Sichtkontrolle oder auf Grund der Überschaubarkeit der Daten. In diesem Fall sei der eigentliche Sinn des § 8 TMG, nämlich den übergeordneten Provider nicht mit dem

9 *BGH*, NJW 2010, 2061 = MMR 2010, 565 (567) – Sommer unseres Lebens.
10 *OLG Frankfurt a.M.*, MMR 2008, 603 (605); zustimmend *Gietl/Mantz*, MMR 2008, 608; *Gietl*, MMR 2007, 630 (632 f.); krit. *Mühlberger*, GRUR 2009, 1022 (1023).
11 So *Mantz*, MMR 2010, 569.
12 Ebenfalls unschlüssig *Leible/Jahn*, LMK 2010, 306719; *Nenninger*, NJW 2010, 2064.
13 *Breyer*, NJOZ 2010, 1085.
14 *Breyer*, MMR 2009, 14 (15).
15 *Heckmann*, in: jurisPK-InternetR, 2. Aufl. 2009, Kap. 1.8 Rn. 17; *Hoffmann*, in: *Spindler/Schuster*, Recht der elektronischen Medien – Komm., 2. Aufl. 2011, § 8 TMG Rn. 1; *Sieber/Höfinger*, in: *Hoeren/Sieber/Holznagel*, Hdb. MultimediaR, 35. Erg-Lfg. 2013, Teil 18.1 Rn. 64 – jedoch differenzieren *Sieber/Höfinger* noch zwischen dem willentlichen und dem „fahrlässigen" Diensteanbieter, auf welchen TMG aber im Wege eines Erst-Recht-Schlusses analoge Anwendung finden soll (ebd. Fn. 2); *Mantz*, GRUR-RR 2013, 497 (498); *Spindler*, CR 2010, 592 (595 f.); wohl auch *Kirchberg*, ZUM 2012, 544 (548 f.).
16 *Sieber/Höfinger*, in: *Hoeren/Sieber/Holznagel* (o. Fn. 15), Teil 18.1 Rn. 64; Anm. *Mantz*, MMR 2006, 765.
17 *Popescu*, VuR 2011, 327 (332).
18 *Mantz*, Rechtsfragen offener Netze, S. 48, zu finden über google.de.
19 *BGH*, NJW 2010, 2061 = MMR 2010, 565 (567) – Sommer unseres Lebens.
20 BT-Drs. 16/6098, 23; *Spindler*, CR 2010, 592 (598).
21 So auch *Mantz* (o. Fn. 18); *Spindler*, CR 2010, 592 (598).
22 *Sieber/Höfinger*, in: *Hoeren/Sieber/Holznagel* (o. Fn. 15), Teil 18.1 Rn. 64 und Fn. 2; vgl. auch darstellend *Gietl*, MMR 2007, 630 (631); *Hornung*, CR 2007, 88 (90).
23 *Sieber/Höfinger*, in: *Hoeren/Sieber/Holznagel* (o. Fn. 15), Teil 18.1 Rn. 64 u. Fn. 2; *Gietl*, MMR 2007, 630 (631).
24 Anm. *Mantz*, MMR 2006, 763 (765).

Haftungsrisiko für eine unüberschaubare Informationsmasse zu belasten, situationsbedingt nicht mehr gegeben[25].

Diese teleologische Reduktion des § 8 TMG ist unseres Erachtens praktisch nicht umsetzbar. Es käme immer auf den Einzelfall an, ob der WLAN-Betreiber gerade die Möglichkeit hat, seine Kunden zu überprüfen oder nicht. Gegebenfalls überschreitet der WLAN-Betreiber dabei die Grenze des Persönlichkeitsschutzes des Nutzers[26]. Im Übrigen müssten sich Kleinbetriebe wahrscheinlich eher der teleologischen Reduktion des § 8 TMG hingeben als Großbetriebe, wo die Kontrolle des Einzelnen von Natur aus schlechter zu gewährleisten ist, was zu einer ungerechtfertigten Benachteiligung nach Art. 3 I GG führen könnte.

6. WLAN generell als Gefahrenquelle?

Die Relevanz dieser Frage ist darin begründet, dass eine Sicherungs- bzw. Prüfpflicht überhaupt erst dann begründet sein kann, wenn das WLAN-Netzwerk eine Gefahrenquelle darstellt, derer sich der Verantwortliche annehmen muss. In der Rechtsprechung wird größtenteils pauschalisiert, dass ein offenes WLAN-Netzwerk die nicht unwahrscheinliche Möglichkeit berge, dass ein Dritter das Netzwerk zum Zwecke von Rechtsverletzungen nutzen wird[27]. Dieser Ansicht treten zu Recht das *OLG Frankfurt a. M.*[28] sowie Stimmen in der Literatur[29] mit dem Argument entgegen, dass es nicht als pflichtwidrig angesehen werden kann, Dritten die technische Möglichkeit zum Austausch von Informationen anzubieten[30]. Man mag die Ansicht des *BGH* zur Kenntnis nehmen, aber gleichzeitig auch in Frage stellen, dass der problemlose und „anonyme" Fernabsatzverkehr im Internet die Hemmschwelle zu Rechtsverstößen herabsetze[31]. Jedoch begründen sozialadäquate und daher erlaubte Lebensrisiken keine Garantenstellung, welche wiederum Sicherungspflichten zu begründen vermögen[32].

7. Beweislast

a) *Prima facie Beweis.* Wird ein urheberrechtlich geschütztes Werk von einer IP-Adresse aus der Öffentlichkeit zugänglich gemacht, so geht die Rechtsprechung von der tatsächlichen Vermutung aus, dass der Person, welcher die IP-Adresse im fraglichen Zeitpunkt zugeteilt ist, auch die Rechtsverletzung zuzurechnen ist[33]. Es gibt allerdings technische Möglichkeiten, die es ermöglichen, die IP-Adresse einem anderem zuzuordnen oder auch zu verschleiern, so dass es zweifelhaft erscheint, den Beweis des ersten Anscheins an dieser Stelle anzuwenden[34]. Zu Recht konstatiert daher das *LG Köln*: „Für die etwaige Verletzung von Sicherungspflichten bzgl. der Einrichtung des Routers gilt Entsprechendes. Es ist schon nicht substanziiert dargelegt, dass etwaige Verletzungen für die Urheberrechtsverletzungen kausal geworden wären."[35]

b) *Sekundäre Darlegungslast.* Den Anschlussinhaber trifft im Falle der Rechtsverletzung die sekundäre Darlegungslast, dass ein anderer die streitgegenständliche Rechtsverletzung begangen hat[36]. Fraglich erscheint jedoch, wie der WLAN-Betreiber seiner sekundären Beweislast nachkommen soll oder kann. Wie der *BGH* ausführt, müssen zumindest Router-Protokolle nicht angelegt oder gespeichert werden[37]. Allerdings plädieren Rechtsprechung sowie Teile der Literatur für eine Passwortpflicht des WLAN-Betreibers, um die Missbrauchsmöglichkeit durch Dritte zu reduzieren/eliminieren[38]. Dagegen meinen andere, dass der WLAN-Betreiber erst bei Anzeichen einer Rechtsverletzung gegebenenfalls agieren müsse[39].

Fraglich ist darüber hinaus, welcher Sicherheitsstandard einzuhalten ist. Eine Ansicht geht davon aus, dass es zumindest des WPA, wohl eher des WPA2-Standards bedürfe, da der WEP-Standard mit frei verfügbaren Softwares zu durchbrechen sei[40]. Nach anderer Ansicht wird genau dieses Argument in konträrer Richtung genutzt mit dem Hinweis darauf, dass das „Einbrechen" in ein WLAN-Netzwerk strafrechtliche Relevanz haben kann, so dass es dem WLAN-Betreiber nicht angelastet werden soll, wenn ein Dritter sich in strafrechtlich relevanter Weise Zugang zu dessen Netzwerk verschafft[41].

Darüber hinaus schließt der *BGH* eine Pflicht zur Anpassung des WLANs an neueste Sicherungsstandards aus. Zur Argumentation trägt er vor, dass solche Maßnahmen im Hinblick auf die damit einhergehenden finanziellen Belastungen die Grenze der Zumutbarkeit und damit der Verhältnismäßigkeit überschreiten[42]. Jedoch müsse der WLAN-Router im Zeitpunkt des Kaufs die marktüblichen Sicherungsstandards erfüllen[43]. Weiterhin müsse ein Passwort vergeben werden, dass nicht persönlich sowie ausreichend lang und sicher ist[44].

Diese Aussagen des *BGH* sind vage, da im Hinblick auf die schnelle Entwicklung im IT-Software und Hardware-Bereich der Begriff des „marktüblichen Sicherungsstandards" fortlaufend angepasst werden muss. Der WLAN-Betreiber kann dieser Aussage des *BGH* also keinen rechtssicheren Gehalt entnehmen[45]. *Spindler* hält die Grenze der finanziellen Belastung für zu eng: Er verweist darauf, dass die meisten PC's heutzutage mit vorinstallierten Viren-Softwares ausgeliefert werden, welche ihren vollen Schutz nur durch Updates entfalten können, was wiederum zumeist nur gegen Entgelt erworben werden kann. Dementsprechend sei für einen ausreichenden Schutz auf den Einzelfall abzustellen und finanzielle Opfer seien gegebenenfalls abzuverlangen[46].

---

25 *Liesching/Knupfer*, MMR 2003, 562 (567).
26 So auch *Heckmann*, in: jurisPK-InternetR (o. Fn. 15), Kap. 1.8 Rn. 27.
27 *OLG Düsseldorf*, MMR 2008, 256; *LG Hamburg*, MMR 2011, 475; CR 2007, 54 (55). *LG Mannheim*, MMR 2007, 537.
28 MMR 2008, 603 (605).
29 Anm. *Ernst*, MMR 2007, 537 (539); *Gercke*, CR 2007, 54 (56); *Hornung*, CR 2007, 88 (91); so wohl auch *Mantz/Gietl*, MMR 2008, 608; *Spindler*, MMR 2008, 168.
30 *Breyer*, NJOZ 2010, 1085.
31 *BGH*, NJW 2008, 758 (760): Zum einen scheinen dieser Ansicht keine wissenschaftlichen Begründungsansätze zu Grunde zu liegen; zum anderen hat auch der Fernabsatzverkehr im Internet eine Grenze der Anonymität und zwar im Zeitpunkt der Kaufpreiszahlung.
32 *Breyer*, NJOZ 2010, 1085 (1086); *Popescu*, VuR 2011, 327 (331).
33 *BGH*, NJW 2010, 2061 = MMR 2010, 565 – Sommer unseres Lebens; *OLG Köln*, ZUM 2010, 269 (270); *LG Frankfurt a. M.*, ZUM-RD 2014, 36 (38).
34 *Spindler*, CR 2010, 592 (593); *Leicht*, VuR 2009, 346 (348 ff.).
35 ZUM 2013, 66 (69).
36 *BGH*, NJW 2010, 2061 = MMR 2010, 565 – Sommer unseres Lebens; *OLG Köln*, ZUM 2010, 269 (270).
37 *BGH*, NJW 2010, 2061 = MMR 2010, 565 (566).
38 *BGH*, NJW 2010, 2061 = MMR 2010, 565 (566 f.); *OLG Düsseldorf*, MMR 2008, 256; *Borges*, NJW 2010, 2624; *Mühlberger*, GRUR 2009, 1022 (1023); *Stang/Hühner*, GRUR-RR 2008, 273 (275).
39 *Gietl*, MMR 2007, 630 (632); *Hornung*, CR 2007, 88 (91); *Röhl/Bosch*, NJW 2008, 1415 (1418).
40 Vgl. *Borges*, NJW 2010, 2624.
41 *Ernst/Seichter*, ZUM 2007, 513 (516); Anm. *Mantz*, MMR 2006, 765; zur strafrechtlichen Relevanz vgl. *Heckmann*, in: jurisPK-InternetR (o. Fn. 15), Kap. 8 Rn. 178 ff.; *Bär*, MMR 2005, 434 (436).
42 NJW 2010, 2061 = MMR 2010, 565 (567) – Sommer unseres Lebens.
43 *BGH*, NJW 2010, 2061 = MMR 2010, 565 (567) – Sommer unseres Lebens.
44 *BGH*, NJW 2010, 2061 = MMR 2010, 565 (567) – Sommer unseres Lebens.
45 So auch *Borges*, NJW 2010, 2624 (2626).
46 CR 2010, 592 (597); *ders.*, in Verantwortlichkeit von IT-Herstellern, Nutzern und Intermediären, Gutachten für das BSI 2007, Rn. 277 ff., 295.

III. Geschäftlich betriebene WLAN-Netzwerke

Für den Betrieb kommerzieller, offener WLANs, beispielsweise in Internetcafés, hat sich bisher noch keine einheitliche Rechtsprechung herausgebildet: Das *LG Hamburg* entschied, dass der Betreiber eines Internetcafés für die Bereitstellung eines Liedes mittels eines Filesharingprogramms durch einen Dritten in seinem (des Internetcafé-Betreibers) WLAN verschuldensunabhängig auf Unterlassung hafte. Es sei dem WLAN-Betreiber möglich und zumutbar, solche Rechtsverletzungen zu verhindern, beispielsweise durch Sperrung etwaiger Ports[47]. Hier wird allerdings nicht bedacht, dass einige DSL-Router nicht in der Lage sind, Ports zu sperren. Außerdem sei nicht absehbar, welcher Port zu sperren ist, da verschiedene Filesharingprogramme verschiedene Ports benützten[48].

Das *LG Frankfurt a. M.* lässt dem Hotelier gewisse Exkulpationsmöglichkeiten zukommen, indem es den Vorgang für ausreichend hält, dem Gast ein sicherheitsaktiviertes und verschlüsseltes Netzwerk zur Verfügung zu stellen und ihn vor der Nutzung auf die Einhaltung der gesetzlichen Vorschriften hinzuweisen[49]. Ähnlich entschied das *LG Frankfurt a. M.* in einem weiteren Fall, in dem es um die Nutzung des WLANs der Ferienwohnungsvermieter ging, welche die entsprechende Nutzung vertraglich nur zum Abruf der E-Mails und allenfalls zu geschäftlicher Nutzung erlaubt hatten[50].

So urteilte auch das *AG München* im Zuge eines Mietvertrags. Dort hatte sich der Vermieter vom Mieter vertraglich zusichern lassen, dieser werde das vom Vermieter zur Verfügung gestellte WLAN nicht rechtswidrig verwenden[51].

Wenn man die oben viel zitierte Entscheidung des *BGH* zu Grunde legt, welche zwar keine klaren Aussagen zu geschäftlich betriebenen WLANs getroffen hat, so kann man dieser dennoch als Hauptaussage entnehmen, dass geschäftliche Modelle durch Sicherungsmaßnahmen nicht gefährdet werden sollen[52].

IV. Fazit

Sowohl für die privaten als auch für die gewerblichen WLAN-Betreiber müssen die bekannten Grundsätze der Provider-Störerhaftung gelten. Insbesondere kommt § 8 TMG zumindest analog zur Anwendung, so dass WLAN-Betreiber nicht als Störer in Anspruch genommen werden können. Auch trifft sie keine generelle Überwachungs- oder Prüfpflicht.

Diese Lösung entspricht dem, was im Koalitionsvertrag 2013 formuliert wurde. Denn dort heißt es: „Wir wollen, dass in deutschen Städten mobiles Internet über WLAN für jeden verfügbar ist. Wir werden die gesetzlichen Grundlagen für die Nutzung dieser offenen Netze und deren Anbieter schaffen. Rechtssicherheit für WLAN-Betreiber ist dringend geboten, etwa durch Klarstellung der Haftungsregelungen (analog zu Accessprovidern)":

Angesichts der oben erwähnten Kontroversen könnte es sich anbieten, diese Privilegierung durch eine Änderung des TMG klarzustellen, gerade auch zur Vermeidung von Alleingängen der Kölner und Hamburger Justiz. ■

47 *LG Hamburg*, MMR 2011, 475.
48 *Füglein/Lagardère*, MMR-Aktuell 341646.
49 MMR 2011, 401 (402).
50 GRUR-RR 2013, 507 (509).
51 NJOZ 2012, 1463.
52 Vgl. *BGH*, NJW 2010, 2061 = MMR 2010, 565 (567); so auch *Spindler*, CR 2010, 592 (599), der dem sogar eine weitestgehende Befreiung von Sicherungspflichten entnimmt.

Professor Dr. Joachim Renzikowski*

Überfällige Reglementierung der Prostitution

Der Koalitionsvertrag 2013 zwischen CDU, CSU und SPD sieht unter der Überschrift „Menschenhandel und Prostitutionsstätte" vor, „das Prostitutionsgesetz im Hinblick auf die Regulierung umfassend [zu] überarbeiten und ordnungsbehördliche Kontrollmöglichkeiten gesetzlich [zu] verbessern". Dieses längst überfällige Vorhaben wird begleitet von schrillen medialen Tönen, wonach Deutschland zur Drehscheibe des Menschenhandels und zum Freudenhaus Europas geworden sei. Zu erwarten sind also hitzige Diskussionen.

I. Einleitung

Prostitution ist ein komplexes Feld, dem man nicht gerecht wird, indem man eine ihrer Erscheinungsformen zum Paradigma erhebt. Vielmehr findet Prostitution in einer großen Bandbreite statt[1]. Auf der einen Seite steht das Luxuscallgirl mit sehr hohen Einnahmen und größeren Freiheiten in der Gestaltung ihrer Arbeit als gewöhnliche Arbeitnehmer. Dem entspricht die Vorstellung von der Ausübung der Prostitution als selbstbestimmter Tätigkeit emanzipierter Frauen. Folgerichtig wird Prostitution als ein Beruf wie jeder andere auch angesehen und seine völlige rechtliche Gleichstellung eingefordert[2]. Auf der anderen Seite steht das düstere Bild eines mehr oder weniger bedrückenden Milieus, in dem die Ausübung der Prostitution für die Betroffenen mit erheblichen psychischen und physischen Beeinträchtigungen verbunden ist.

Zur Veranschaulichung der verschiedenen Abhängigkeitsverhältnissen im Prostitutionsmilieu eignet sich die für die Arbeitsausbeutung entwickelte Metapher der Pyramide[3]. Den Sockel bilden die Fälle freiwilliger sexueller Dienstleistungen zu in verschiedener Hinsicht ungünstigen Bedingungen, die aber noch nicht strafrechtlich relevant sein müssen. Die Ausnutzung einer Zwangslage wird hier noch nicht voraus-

* Der Autor ist Inhaber der Professur für Strafrecht und Rechtsphilosophie/Rechtstheorie an der Martin-Luther-Universität Halle-Wittenberg.
1 Vgl. etwa *Helfferich/Fischer/Kavemann/Leopold/Rabe*, Untersuchungen zu den Auswirkungen des Prostitutionsgesetzes, Gutachten im Auftrag des BMFSFJ, 2007 (unter: http://www.bmfsfj.de/doku/Publikationen/prostitutionsgesetz/, abgerufen am 6. 12. 2013); *Leopold/Steffan/Paul*, Dokumentation zur rechtlichen und sozialen Lage von Prostituierten in der Bundesrepublik Deutschland, 2. Aufl. 1997, S. 63 ff. (Berichte über einzelne Städte), S. 257 ff.
2 Vgl. BT-Drs. 14/4456, 8; BT-Drs. 14/7174, 9.
3 Zur „Pyramide der Arbeitsausbeutung" s. *Cyrus/de Boer*, in: KOK, Entwicklung tragfähiger Unterstützungsstrukturen für die Betroffenen von Menschenhandel zur Arbeitsausbeutung. Studie im Auftrag des Bundesministeriums für Arbeit und Soziales, März 2011, S. 41 (48 f.) (unter: www.bmas.de/SharedDocs/Downloads/DE/PDF-Meldungen/studie-menschenhandel.pdf?__blob=publicationFile, abgerufen am 6.12.2013).