Gerade das Mittel des wörtlichen Zitats ermöglicht es, eine Meinungsäußerung in verfremdetem Zusammenhang wiederzugeben und dadurch die Aussage so zu verfälschen, dass der ursprüngliche Sinn der Äußerung verändert oder sogar in ihr Gegenteil verkehrt wird und dem Autor eine Erklärung zugeschrieben wird, die dieser nie beabsichtigt hat. Zwar darf der Beklagte die aus seiner Sicht unsachliche Angstkampagne gegen das Impfen und die Impfgegnerszene als solche und auch des Wirken des Klägers kritisieren, er darf die Äußerungen des Klägers aber nicht bewusst verfälschen und seine vertrauliche E-Mail als Äußerung des „größten lebenden Deutschen Denkers“ im Internet der Öffentlichkeit zugänglich machen um die Person des Klägers der Lächerlichkeit preiszugeben. Die Abwägung der Interessen fiel daher zu Lasten des Beklagten aus. …

Hinweis der Redaktion: Das Verfahren wird beim OLG Stuttgart unter dem Az. 4 U 96/10 geführt.

Unbefugte Nutzung fremder WLAN-Netze nicht strafbar

LG Wuppertal, Beschluss vom 19. 10. 2010 – 25 Qs-10 Js 1977/08-177/10

Vorinstanz: AG Wuppertal, 3. 8. 2010 – 26 Ds 282/08

§§ 89 S. 1, 148 Abs. 1 Nr. 1 TKG; §§ 44, 43 Abs. 2 Nr. 3 BDSG; § 202 b StGB

Die Einwahl in ein offenes und über einen WLAN-Router betriebenes Funknetzwerk mittels einer drahtlosen Netzwerkverbindung erfüllt weder den Tatbestand des unbefugten Abhörens von Nachrichten noch des unbefugten Abrufens oder Verschaffens personenbezogener Daten. Auch liegt weder eine Strafbarkeit wegen Ausspähens oder Abfangens von Daten vor noch wegen eines versuchten Computerbetrugs oder einer Leistungserschleichung. (Leitsatz der Redaktion)

Sachverhalt

Mit Anklageschrift vom 8. 12. 2008 hat die Beschwerdeführerin dem Angeschuldigten vorgeworfen, am 26. und 27. 8. 2008 das Haus I-Straße in Wuppertal aufgesucht zu haben, um sich mit seinem Laptop mittels einer drahtlosen Netzwerkverbindung in das offene und über einen WLAN-Router betriebene Funknetzwerk des Zeugen J einzuwählen. Dabei habe er beabsichtigt, die Internetnutzung ohne Zahlung eines Entgeltes zu erlangen. Mit Beschl. v. 3. 8. 2010 hat das AG Wuppertal die Eröffnung der Hauptverhandlung aus rechtlichen Gründen abgelehnt, da ein hinreichender Tatverdacht im Sinne des § 203 StPO mangels strafbaren Verhaltens des Angeschuldigten nicht gegeben sei. Das Verhalten des Angeschuldigten erfülle weder den Tatbestand des unbefugten Abhörens von Nachrichten nach §§ 89 S. 1, 148 Abs. 1 TKG noch des unbefugten Abrufens oder Verschaffens personenbezogener Daten nach §§ 44, 43 Abs. 2 Nr. 3 BDSG. Auch eine Strafbarkeit nach § 202 b StGB liege nicht vor. Gegen den ihr am 6. 8. 2010 zugestellten Beschluss wendet sich die Beschwerdeführerin mit der am 11. 8. 2010 eingelegten sofortigen Beschwerde.

Aus den Gründen

Die sofortige Beschwerde ist zulässig, aber unbegründet. Ein hinreichender Tatverdacht gemäß § 203 StPO liegt nicht vor. Bei vorläufiger Tatbewertung ist die Verurteilung des Angeschuldigten in der Hauptverhandlung nicht wahrscheinlich, da, wie das AG Wuppertal im Ergebnis zutreffend ausgeführt hat, ein strafbares Verhalten nicht ersichtlich ist. Das vorgeworfene Einwählen in das unverschlüsselt betriebene Funknetzwerk des Zeugen J erfüllt nicht den Tatbestand des unbefugten Abhörens von Nachrichten nach §§ 89 S. 1, 148 Abs. 1 Nr. 1 TKG. Jeder Computer, der sich in ein unverschlüsselt betriebenes WLAN einwählt, erhält von dem im WLAN-Router befindlichen DHCP (dynamic host configuration protocol) Server automatisch eine freie, interne (private) IP-Adresse zugeteilt. Dieser von dem Angeschuldigten ausgelöste Vorgang erfüllt nicht die Voraussetzungen eines strafbaren Abhörens von Nachrichten nach §§ 89 S. 1, 148 Abs. 1 Nr. 1 TKG.

Hierzu hat das AG ausgeführt, ein Abhören im Sinne des § 89 TKG liege nicht vor. Dies ergebe sich bereits aus dem Wortlaut der Vorschrift. Unter Abhören sei das unmittelbare Zuhören oder das Hörbarmachen für andere, aber auch das Zuschalten einer Aufnahmevorrichtung zu verstehen. Dies erfordere jedenfalls einen zwischen anderen Personen stattfindenden Kommunikationsvorgang, den ein Dritter als Täter mithöre (vgl. Bär MMR, 2005, 434, 440). Es müsse ein bewusster und gezielter Empfang durch den Täter gegeben sein, um von einem Abhören von Nachrichten sprechen zu können. Für einen solchen bewussten und gezielten Empfang von Nachrichten durch den Angeschuldigten gebe es keine Anhaltspunkte. Dem Angeschuldigten sei es ausweislich der Anklage und des Ermittlungsergebnisses nur darauf angekommen, durch Einwählen in das Netzwerk des Zeugen dessen Internetzugang mitbenutzen zu können. Das dabei notwendige Empfangen der IP-Adresse stelle kein Abhören fremder Nachrichten dar, denn hierdurch werde die Vertraulichkeit fremder Kommunikation nicht angegriffen (vgl. Popp, jurisPR-ITR 16/2008 Anm. 4).

Dieser Argumentation schließt sich die Kammer an. Sofern das AG Wuppertal demgegenüber in einer Entscheidung aus dem Jahr 2007 (AG Wuppertal, Urt. v. 3. 4. 2007 – 22 Ds 70 Js) in einem vergleichbaren Sachverhalt noch eine Strafbarkeit nach §§ 89 S. 1, 148 Abs. 1 Nr. 1 TKG angenommen hatte, ist diese Entscheidung nicht überzeugend, da hierbei nicht berücksichtigt wurde, dass der Nutzer eines offenen WLAN selbst den maßgeblichen Kommunikationsprozess auslöst. Das Abhörverbot im TKG dient, wie sich schon aus der systematischen Stellung des § 89 TKG in dem mit „Fernmeldegeheimnis“ überschriebenen Abschnitt ergibt, dem Schutz vertraulicher Kommunikation (vgl. Popp, jurisPR-ITR 17/2008, Anm. 4). Dieser Schutzzweck ist bei der Zuteilung und dem Empfang einer IP-Adresse nicht tangiert. Der Angeschuldigte hat nicht zwischen anderen Kommunikationspartnern vertraulich ausgetauschte Daten wahrgenommen, sondern war vielmehr dadurch, dass er die Datenübermittlung initiiert und die darauf übermittelten Daten empfangen hat, selbst Teilnehmer des fraglichen Kommunikationsvorgangs (vgl. Bär, MMR 2008, 632, 633). Geht es dem Täter nur darum, ein fremdes Netzwerk zum Zwecke der eigenen Kommunikation zu nutzen, so greift er die Vertraulichkeit fremder Kommunikation ebenso wenig an, wie jemand, der ungefragt ein fremdes Telefon zu einem eigenen Gespräch nutzt (vgl. Popp, jurisPR-ITR 17/2008 Anm. 4).

Überdies war die zugeteilte IP-Adresse auch keine Nachricht, die nicht für den Angeschuldigten, die Allgemeinheit oder einen unbestimmten Personenkreis bestimmt war. Vielmehr hat der Zeuge J durch den unverschlüsselten Betrieb des WLANs schlüssig erklärt, dass die dem Laptop des Angeschuldigten durch den DHCP-Server zugeteilte IP-Adresse auch für den Angeschuldigten bestimmt war. Es ist ohne weiteres möglich vorab einzugrenzen, welche Computer sich in ein WLANs einwählen können. Es kann z. B. eine Verschlüsselung aktiviert und so festgelegt werden, dass nur Computer, die den Schlüssel kennen, durch den DHCP-Server eine interne IP-Adresse zugeteilt erhalten. Durch die DHCP-Konfiguration seines Routers und den Verzicht auf die Verschlüsselung äußert der Betreiber eines offenen WLAN bei technischer Betrachtung den Willen, dass jedes Gerät in Reichweite sich mit dem Router verbinden darf (Ernst/Spoenle, CR 2008, 439, 440). Der Betreiber eines WLAN-Routers muss sich die von dem Gerät getroffene Bestimmung zurechnen lassen, auch wenn er selbst später einen abweichenden Willen bildet und nach außen zu erkennen gibt (vgl. Bär, MMR 2008, 632, 634). Letztlich versendet der Router die internen IP-Adressen lediglich entsprechend der ihm, durch entsprechende Konfiguration, aufgetragenen Vorgehensweise, welche bei einem unverschlüsselt betriebenen Netzwerk lautet, dass Zugangsdaten ohne weitere Prüfung zugeteilt werden sollen.

Das vorgeworfene Einwählen in das unverschlüsselt betriebene WLAN-Netz mit dem Zweck der Mitbenutzung des Internetzuganges des Zeugen J erfüllt auch nicht den Tatbestand des unbefugten Abrufens oder Verschaffens personenbezogener Daten, §§ 43 Abs. 2 Nr. 3, 44 BDSG. Demnach macht sich strafbar, wer unbefugt personenbezogene Daten, die nicht allgemeinzugänglich sind, in der Absicht sich zu bereichern abruft. Bei dem Einwählen in ein unverschlüsselt betriebenes WLAN und der anschließend hierüber erfolgten Nutzung des Internetzuganges werden, wie das AG zutreffend ausgeführt hat, keine personenbezogenen Daten abgerufen. Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person, § 3 Abs. 1 BDSG. Die von dem WLAN-Router übermittelte interne IP-Adresse ist schon deshalb nicht personenbezogen, da sich mittels dieser keine natürliche Person bestimmen lässt. Vielmehr werden die zugeteilten Adressbereiche weltweit tagtäglich von unzähligen Endgeräten – allerdings jeweils in einem anderen, nach außen abgeschotteten privaten Netzwerk – verwendet (vgl. Ernst/Spoenle, CR 2007, 439, 441).

Aber auch die externe, dem Zeugen J für den Aufbau der Internetverbindung durch den Provider zugewiesene, IP-Adresse stellt für den Angeschuldigten kein personenbezogenes Datum dar. In der IP-Adresse selbst ist zunächst die den Internetanschluss betreibende Person nicht eindeutig bezeichnet. Auch ist diese Person für den Nutzer eines offenen WLANs normalerweise nicht anhand der externen IP-Adresse bestimmbar. Denn bestimmbar ist eine natürliche Person nur dann, wenn sie durch die das Datum abrufende Stelle mit den dieser zur Verfügung stehenden Mitteln identifiziert werden kann (vgl. Ernst/Spoenle, CR 2007, 439, 441), wenn also die abrufende Stelle in der Lage ist, eine Beziehung zu der Person herzustellen (vgl. Ambs in Erbs/Kohlhaas, Strafrechtliche Nebengesetze, Stand November 2006, D 25 § 3 Rn. 3.) Zwar ist die einem Telekommunikationsanschluss zugewiesene externe IP-Adresse grundsätzlich geeignet, den Anschlussinhaber zu individualisieren. Eine solche Individualisierung erfordert jedoch eine nur dem Access-Provider vorliegende Datenbank mit den Bestandsdaten aller Anschlussinhaber (vgl. Ernst/Spoenle, CR 2007, 439, 441). Da der Angeschuldigte auf diese Datenbank nicht zugreifen konnte und auch nicht ersichtlich ist, dass er auf andere Weise über zusätzliche Identifizierungsmerkmale verfügen konnte, stellt die externe IP-Adresse für ihn kein personenbezogenes Datum dar (so auch: Ernst/Spoenle, CR 2007, 439, 441; Bär, MMR 2008, 632, 635).

Überdies handelt es sich bei der betroffenen externen IP-Adresse nicht um ein „nicht allgemein zugängliches" Datum. Vielmehr hätte jeder, der sich mit einem WLAN- und internetfähigen empfangsbereiten Gerät im Sendebereich des von dem Zeugen J betriebenen WLAN-Routers befunden hätte, diese Adresse abrufen können (vgl. Ernst/Spoenle, CR 2007, 439, 442).

Nicht in Betracht kommt weiterhin eine Strafbarkeit wegen eines Ausspähens von Daten gemäß § 202 a StGB, da die Daten, zu denen der Angeschuldigte durch das bloße Einwählen in das unverschlüsselt betriebene Netzwerk Zugang hatte, gerade nicht gegen einen unberechtigten Zugang gesondert gesichert waren.

Das vorgeworfene Einwählen in das fremde, unverschlüsselt betriebene Netzwerk begründet auch keine Strafbarkeit wegen eines Abfangens von Daten nach § 202 b StGB. Hierfür fehlt es schon an dem Merkmal einer nichtöffentlichen Datenübermittlung. Entscheidend für die Nichtöffentlichkeit der Datenübermittlung ist die Art des Übertragungsvorganges und nicht Art oder Inhalt der Daten (vgl. Eisele in Schönke/Schröder, Strafgesetzbuch, 28. Aufl., 2010, § 202 b Rn. 4). Da § 202 b StGB ebenso wie das in § 89 TKG normierte Abhörverbot die Vertraulichkeit von Datenübermittlungen schützt (vgl. Bär, MMR 2008, 632, 634) sind solche Datenübermittlungen von vornherein auszuscheiden, die für einen unbestimmten Personenkreis (z. B. beim Amateurfunk: für jeden empfangsbereiten Teilnehmer) wahrnehmbar sein sollen (vgl. Gröseling/Höfinger, MMR 2007, 549, 552). Nichtöffentlich ist eine Datenübermittlung, die objektiv erkennbar für einen beschränkten Nutzerkreis bestimmt ist, ohne dass es auf die Wahrnehmbarkeit durch Unberechtigte ankommt (vgl. Gröseling/Höfinger, MMR, 2007, 549, 552). Dies ist vorliegend nicht der Fall, da in keiner Weise objektiv erkennbar ist, dass das von dem Zeugen J betriebene WLAN nur einem beschränkten Nutzerkreis dienen soll. Vielmehr sind bei einem objektiven Verständnis die IP-Daten an einen zahlenmäßig nicht begrenzten Personenkreis gerichtet und auch für den Angeschuldigten als den Initiator des Kommunikationsvorganges bestimmt.

Aus dem vorgeworfenen Einwählen in das Netzwerk in der Absicht, einen fremden Internetanschluss zu nutzen, ergibt sich auch keine Strafbarkeit wegen eines versuchten Computerbetruges gemäß §§ 263 a, Abs. 1, Abs. 2, 263 Abs. 2, 22 StGB. Der Angeschuldigte hat nach seiner Vorstellung von der Tat nicht unbefugt Daten verwandt. Nach der ständigen Rechtsprechung des BGH, der sich die Kammer anschließt, ist das Merkmal der Unbefugtheit betrugsspezifisch auszulegen (vgl. statt aller BGHSt 47, 160 ff.). Unbefugt ist die Verwendung, wenn sie gegenüber einer natürlichen Person Täuschungscharakter hätte (vgl. Fischer, Strafgesetzbuch und Nebengesetze, 57. Aufl., 2010, § 263 a Rn. 11). An einer solchen täuschungsgleichen Handlung fehlt es. Bei einem unverschlüsselt betrie-

benen WLAN wird dem Clienten durch den Router automatisch eine interne IP-Adresse zugewiesen. Da hierbei eine wie auch immer geartete Prüfung einer Zugangsberechtigung – anders als bei dem Betrieb eines verschlüsselten WLANs – durch den Router nicht vorgenommen wird, kommt dem mit dem Einwählen verbundenen Verwenden der erhaltenen IP-Adresse kein Täuschungswert zu (vgl. Bär, MMR 2005, 434, 437).

Auch nach § 265 a StGB ist das dem Angeschuldigten vorgeworfene Verhalten nicht strafbar. Der objektive Tatbestand des § 265 a StGB setzt als ungeschriebenes Tatbestandsmerkmal die Entgeltlichkeit der erschlichenen Leistung voraus (vgl. Perron in Schönke/Schröder, a. a. O., § 265 a Rn. 2). Da die von dem Angeschuldigten erlangte „Leistung", nämlich die Nutzung des von dem Zeugen J2 betriebenen Funknetzwerkes, generell nicht gegen Entrichtung eines Entgeltes angeboten wurde, dürfte es schon an der Tatbestandsvoraussetzung der Entgeltlichkeit fehlen.

Jedenfalls aber hat der Angeschuldigte die von ihm in Anspruch genommene Leistung nicht erschlichen. Sowohl hinsichtlich der Nutzung von Leistungsautomaten als auch eines Telekommunikationsnetzes liegt ein Erschleichen nicht schon in der unbefugten unentgeltlichen Inanspruchnahme. Vielmehr muss hinzukommen, dass die Inanspruchnahme unter Umgehung der von dem Berechtigten gegen unerlaubte Benutzung geschaffenen Sicherungsvorkehrungen erfolgt (vgl. Perron in Schönke/Schröder, a. a. O., § 265 a Rn 8). Hieran fehlt es, da der Einwählvorgang in das WLAN und hierüber in das Internet ordnungsgemäß und ohne Überwindung irgendwelcher Sicherungsvorkehrungen erfolgte. Ähnlich wie das unbefugte aber ordnungsgemäß vorgenommene Telefonieren von fremden Apparaten (vgl. hierzu Fischer, a. a. O., § 265 a Rn. 18) ist auch das ordnungsgemäße Nutzen eines offenen – und damit technisch jedermann zur Verfügung gestellten – WLAN nicht nach § 265 a StGB strafbar. …

Kommentar

Nulla poena sine lege: Zur Strafbarkeit der Nutzung offener WLAN-Netze

RA Thomas Gramespacher und RAin Uta Wichering, Bonn*

Das Einwählen in ein unverschlüsselt betriebenes WLAN-Netzwerk mit dem Ziel, den hierüber verfügbaren Internetanschluss (mit-) nutzen zu können[1], ist nicht strafbar. Mit Blick auf die aktuelle materielle Gesetzeslage überrascht es nicht, dass das LG Wuppertal dieses eindeutige Ergebnis gefunden hat und damit den vorinstanzlichen Nichteröffnungsbeschluss des AG Wuppertal[2] bestätigte. Art. 103 Abs. 2 GG und der Grundsatz „nulla poena sine lege" lassen hier keinen Spielraum.

Nachdem das AG Wuppertal noch drei Jahre zuvor zu einem anderen Ergebnis gelangte,[3] sogar das bei der „Tat" benutzte Laptop als Tatwerkzeug gemäß § 74 Abs. 2 Nr. 1 StGB einzog und allein damit eine nicht unerhebliche Bedeutung des vermeintlich delinquenten Verhaltens zum Ausdruck brachte, gleichwohl lediglich eine Verwarnung mit Strafvorbehalt (§ 59 f. StGB) ausgesprochen wurde, konnten nunmehr sowohl das AG als auch das LG Wuppertal ein strafwürdiges Verhalten nicht mehr erkennen. Das LG Wuppertal arbeitet die denkbaren Tatbestände aus TKG, BDSG und StGB systematisch ab und kommt zu zutreffenden Ergebnissen.

1. Eine Strafbarkeit nach §§ 89 S. 1, 148 Abs. 1 TKG verneint das Gericht, da in der vorliegenden Konstellation kein „unbefugtes Abhören von Nachrichten" vorliege. Bereits der Schutzzweck der Norm sei nicht tangiert. § 89 TKG diene dem Schutz vertraulicher Kommunikation.[4] Soweit jedem, der sich an einem unverschlüsselten WLAN-Netzwerk anmeldet, bei entsprechender DHCP-Konfiguration[5] technisch bestimmungsgemäß und automatisch eine interne (private) IP-Adresse zugeteilt wird, nehme der Einwählende gerade nicht die zwischen anderen Kommunikationspartnern vertraulich ausgetauschten Daten wahr, sondern sei selbst Teilnehmer und auch Initiator eines – eigenen – Kommunikationsvorgangs.[6] Ein solches Verhalten betreffe aber die Vertraulichkeit fremder Kommunikation genauso wenig wie z. B. die ungefragte Nutzung eines fremden Telefons für ein eigenes Gespräch.[7] Zudem handele es sich bei der zugeteilten (internen) IP-Adresse letztlich um eine für Dritte, die Allgemeinheit oder einen unbestimmten Personenkreis bestimmte Nachricht. In dem unverschlüsselten Betreiben des WLANs liege – aus objektiver Sicht – die schlüssige Erklärung, dass sich jedes Gerät in Sendereichweite mit dem Router verbinden darf.

Dem ist zuzustimmen. Die Abwicklung eigenen Datenverkehrs wird auch dann nicht nach § 89 TKG sanktioniert, wenn dies vermittels fremder Infrastruktur (hier: eines fremden, ungeschützten WLAN-Netzes) geschieht. Die Norm untersagt das Mithören eines Dritten bei der Kommunikation (wenigstens zweier) anderer und schützt damit ausschließlich Individualkommunikationsvorgänge.[8] Während diskutiert werden kann, ob die zwischen Router und Client getätigte „technische Kommunikation" überhaupt vom Nachrichtenbegriff in § 89 TKG erfasst ist,[9] fällt die im „offenen WLAN" vom „fremden Nutzer" geführte eigene Kommunikation bereits nicht in den Schutzbereich der Norm.[10]

* Mehr über die Autoren erfahren Sie auf S. XII.

1 Insbesondere bei systematischem Vorgehen auch „Wardriving" genannt: http://de.wikipedia.org/wiki/Wardriving (15. 11. 2010).

2 AG Wuppertal, 3. 8. 2010 – 26 Ds-10 Js 1977/08-282/08.

3 AG Wuppertal, 3. 4. 2007 – 22 Ds-70 Js 6906/06 (16/07), NStZ 2008, 161, hinsichtlich der Einziehung aufgehoben durch LG Wuppertal, 29. 6. 2007 – 28 Ns 70 Js 6906/06 – 107/07, da die Einziehung eines wertvollen Gegenstandes unverhältnismäßig (§ 74 b Abs. 1 StGB) sei, wenn lediglich eine Verwarnung mit Strafvorbehalt ausgesprochen werde und damit die zugrundeliegende Straftat im Bagatellbereich angesiedelt werden kann.

4 LG Wuppertal, K&R 2010, 838 ff. m. Verw. auf: *Popp*, jurisPR-ITR 17/2008, Anm. 4; vgl. auch: *Buermeyer*, HRRS 2004, 290.

5 Dynamic Host Configuration Protocol, vgl. http://de.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol, (15. 11. 2010).

6 So auch: *Höfinger*, MMR 2008, 632, 633 – Anm. zu AG Wuppertal, 3. 4. 2007 – 22 Ds 70 Js 6906/06; *Bär*, MMR 2005, 434, 440.

7 LG Wuppertal, K&R 2010, 838 ff. m. Verw. auf: *Popp* jurisPR-ITR 17/2008 Anm. 4.

8 *Schuster*, in: Beck'scher TKG-Kommentar, 3. Aufl. 2006, § 89 Rn. 1, 3; *Bär*, MMR 2005, 434, 440; zutreffend ebenfalls: *Buermeyer*, HRRS 2004, 290 f.

9 Dies zutreffend ablehnend etwa: *Höfinger*, MMR 2008, 632, 633 – Anm. zu AG Wuppertal, 3. 4. 2007 – 22 Ds 70 Js 6906/06; *Buermeyer*, HRRS 2004, 285, 290; a. A. *Bär*, MMR 2005, 434, 440; *Schuster*, in: Beck'scher TKG-Kommentar (Fn. 7), § 89 Rn. 7.

10 Ebenso: *Höfinger*, MMR 2008, 632, 633 – Anm. zu AG Wuppertal, 3. 4. 2007 – 22 Ds 70 Js 6906/06; *Buermeyer*, HRRS 2004, 285, 290.

2. Das LG Wuppertal verneint auch die Strafbarkeit wegen unbefugten Abrufens oder Verschaffens personenbezogener Daten, §§ 43 Abs. 2 Nr. 3, 44 BDSG. Die vom jeweiligen WLAN-Router regelmäßig durch einen DHCP-Server übermittelte interne IP-Adresse sei bereits deshalb nicht personenbezogen, weil sich mit dieser keine natürliche Person bestimmen lasse (§ 3 Abs. 1 BDSG). Auch die externe, vom Internet-Provider zugewiesene IP-Adresse sei hier regelmäßig kein personenbezogenes Datum. Die hinter dieser IP-Adresse stehende natürliche Person (Internetanschlussinhaber) könne der „fremde Nutzer" als abrufende Stelle nicht mit diesem zur Verfügung stehenden Mitteln identifizieren. Zudem könne die IP-Adresse von jedem empfangsbereiten Gerät im Sendebereich des Netzwerkes abgerufen werden, so dass es sich überhaupt nicht um ein „nicht allgemein zugängliches" Datum im Sinne von § 43 Abs. 2 Nr. 3 BDSG handele.

Ungeachtet der Frage, ob dynamische IP-Adressen personenbezogene Daten darstellen, handelt es sich bei der zugeteilten internen (privaten) IP-Adresse vielmehr um ein personenbezogenes Datum des betreffenden (fremden) Nutzers selbst. Bei der externen IP-Adresse, die dem Netzwerkbetreiber vom Internetanbieter zugeteilt wird, handelt es sich im Fall eines unverschlüsselt betriebenen WLAN-Netzwerkes jedenfalls nicht um Daten, die „nicht allgemein zugänglich" sind.[11] § 10 Abs. 5 BDSG definiert Daten als allgemein zugänglich, „die jedermann, sei es ohne oder nach vorheriger Anmeldung, Zulassung oder Entrichtung eines Entgelts, nutzen kann". Es müssten also Beschränkungen auf bestimmte Benutzer vorliegen.[12]

3. Eine Strafbarkeit nach §§ 202 a und 202 b StGB lehnt das Gericht ebenso konsequent wie zutreffend ab.

a) Bei dem bloßen Einwählen in ein unverschlüsselt betriebenes WLAN-Netzwerk erlange der Nutzer keinen Zugang zu Daten, die gegen einen unberechtigten Zugang im Sinne von § 202 a Abs. 1 StGB gesondert gesichert sind.

Frei einsehbare Daten sind von der Vorschrift nicht geschützt.[13] Ein Datenabruf bei fehlender Zugangssicherung – wie hier – ist nicht tatbestandsmäßig.[14] Eine Zugangssicherung muss insoweit objektiv geeignet und subjektiv nach dem Willen des Berechtigten dazu bestimmt sein, den Zugriff auf die Daten auszuschließen oder zumindest nicht unerheblich zu erschweren; gleichwohl braucht dies nicht ihr einziger Zweck sein.[15] Offene WLAN-Netze ohne Sicherungsmaßnahmen werden daher vom Anwendungsbereich des § 202 a StGB überhaupt nicht erfasst.[16]

b) Da im Fall des Einwählens in ein unverschlüsseltes WLAN-Netzwerk weiterhin keine nichtöffentliche Datenübermittlung im Sinne von § 202 b StGB vorliege, sei auch keine Strafbarkeit wegen eines Abfangens von Daten gegeben. Entscheidend für die Nichtöffentlichkeit der Datenübermittlung sei die Art des Übertragungsvorgangs und nicht Art oder Inhalt der Daten.[17] Die bei dem Betrieb eines unverschlüsselten WLAN-Netzwerkes übermittelten (IP-) Daten seien bei objektivem Verständnis aber an einen zahlenmäßig nicht begrenzten Personenkreis gerichtet und für Dritte, die einen Kommunikationsvorgang mit dem Netzwerk initiieren, bestimmt. „Nichtöffentlich" im Sinne von § 202 b StGB sei (nur) eine Datenübermittlung, die objektiv erkennbar für einen beschränkten Nutzerkreis bestimmt ist, ohne dass es hierbei auf die Wahrnehmbarkeit durch einen Unberechtigten (Dritten) ankomme.[18]

Im Fall eines unverschlüsselt betriebenen WLAN-Netzwerkes liegen solche Umstände gerade nicht vor. Da es auf den Übertragungsvorgang ankommt, kann eine nichtöffentliche Übermittlung im Sinne von § 202 b StGB zwar auch vorliegen, wenn die übermittelten Daten ansonsten öffentlich zugänglich sind. Entscheidend ist aber, ob die Datenübermittlung nach Zielsetzung des Übermittelnden nur an einen beschränkten Adressatenkreis gerichtet ist und nicht an die Allgemeinheit.[19] Dies ist bei einem unverschlüsselt betriebenen offenen WLAN-Netzwerk nicht anzunehmen.

4. Weiterhin vermochte das LG Wuppertal auch einen versuchten Computerbetrug nach §§ 263 a Abs. 1, Abs. 2, 263 Abs. 2, 22 StGB nicht zu erkennen. Der Angeschuldigte habe nach seiner Vorstellung nicht unbefugt Daten verwendet. Es fehle schon an einer täuschungsgleichen Handlung, da dem Client bei einem unverschlüsselt betriebenen WLAN-Netzwerk durch den jeweiligen Router automatisch eine interne IP-Adresse zugewiesen wird, ohne dass eine Zugangsberechtigung geprüft werde.

Auch der Computerbetrug ist insoweit „betrugsspezifisch" zu verstehen. Nur eine täuschungsäquivalente Verwendung von Daten ist als „unbefugt" im Sinne der Vorschrift anzusehen.[20] Bei einem offenen WLAN-Netzwerk stellt sich das bloße Einwählen und die automatisierte Zuteilung einer IP-Adresse an einen Dritten aber selbst dann nicht als eine Verwendung dar, die gegenüber einer natürlichen Person Täuschungscharakter hätte,[21] wenn der Betreiber des betreffenden Netzwerks eigentlich eine Mitbenutzung durch Dritte nicht wünscht. Maßgeblich ist allein das „Verhältnis" der technischen Geräte; hier des WLAN-fähigen Rechners des Dritten – dem Client – und dem entsprechend konfigurierten Router. Diese agieren in einem solchen Fall aber bestimmungsgemäß und entsprechend der gewählten Konfiguration. Für die Annahme einer täuschungsgleichen Handlung ist dann kein Raum.

5. Schließlich wird auch die Strafbarkeit nach § 265 a StGB verneint. Zum einen liege das Tatbestandsmerkmal der „Entgeltlichkeit" nicht vor, wenn die Nutzung des betreffenden Funknetzwerkes generell überhaupt nicht gegen Entrichtung eines Entgeltes angeboten wird, zum anderen sei das Merkmal des „Erschleichens"[22] nicht einschlägig, da die Inanspruchnahme des Netzzugangs nicht unter der Umgehung der von dem Berechtigten gegen unerlaubte Benutzung geschaffene Sicherheitsvorkehrungen erfolgt.

Zudem dürfte es aber schon an der Bestimmung eines (privaten) WLAN-Netzes fehlen, öffentlichen Zwecken zu dienen, d. h. an einer Einrichtung zur Benutzung für die Allgemeinheit.[23]

11 *Ernst/Spoenle* CR 2007, 439, 442.
12 *Schultze-Melling*, in: Taeger/Gabel, Kommentar zum BDSG, 2010, § 10 Rn. 4; *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 10 Rn. 17.
13 Vgl. *Schultz*, MIR 2006, Dok. 180, Rn. 14, abrufbar unter: http://miur.de/398; im Ergebnis ebenso: *Lenckner/Eisele*, in: Schönke/Schröder, Strafgesetzbuch, 28. Aufl. 2010, § 202 a Rn. 1, 7.
14 *Lenckner/Eisele*, in: Schönke/Schröder (Fn. 12), § 202 a Rn. 6.
15 *Lenckner/Eisele*, in: Schönke/Schröder (Fn. 12), § 202 a Rn. 7.
16 Ebenso bereits: *Bär*, MMR 2005, 434, 436.
17 LG Wuppertal, K&R 838 ff. m. Verw. auf: *Eisele*, in: Schönke/Schröder (Fn. 12), § 202 b Rn. 4.
18 LG Wuppertal, K&R 2010, 838 ff. m. Verw. auf: *Gröseling/Höfinger* MMR 2007, 549, 552.
19 *Eisele*, in: Schönke/Schröder (Fn. 12), § 202 b Rn. 4.; *Gröseling/Höfinger*, MMR 2007, 549, 552; *Schultz*, MIR 2006, Dok. 180, abrufbar unter: http://miur.de/398.
20 *Buermeyer*, HRRS 2004, 285, 288 m. w. N.; BGH, 21. 11. 2001 – 2 StR 260/01, BGHSt 47, 160.
21 *Fischer*, Strafgesetzbuch und Nebengesetze, 57. Aufl. 2010, § 263 a Rn. 11.
22 Vgl. hierzu: *Perron*, in: Schönke/Schröder (Fn. 12), § 265 a Rn. 8, 10.
23 *Buermeyer*, HRRS 2004, 285, 289; *Perron*, in: Schönke/Schröder (Fn. 12), § 265 a Rn. 5.

6. Mangels entsprechender einschlägiger Strafvorschriften ist das Einwählen in unverschlüsselt betriebene WLAN-Netzwerke zur Nutzung eines hierüber verfügbaren Internetanschlusses strafrechtlich – derzeit – nicht relevant. Anders läge der Fall freilich bei verschlüsselt betriebenen Funknetzen, wenn also die unbefugte und ggf. vom Betreiber gerade nicht gewollte Mitbenutzung unter Überwindung einer entsprechenden Zugangssicherung erfolgt.

Angesichts der hier behandelten Entscheidung stellt sich letztlich aber die rechtspolitische Frage, ob überhaupt die Notwendigkeit und das Bedürfnis bestehen, derartige Sachverhalte mit einem staatlichen Strafanspruch zu belegen und auch das Einwählen in ein unverschlüsseltes WLAN-Netzwerk strafrechtlich zu sanktionieren. Strafrecht wird dann als „ultima ratio" eingesetzt, „wenn ein bestimmtes Verhalten über sein Verbotensein hinaus in besonderer Weise sozialschädlich und für das geordnete Zusammenleben der Menschen unerträglich, seine Verhinderung daher besonders dringlich ist".[24] Seine Verwendung unterliegt dabei den Anforderungen der Verhältnismäßigkeit.[25]

Wenn mit dem insoweit unscharfen und sachlich inakzeptablen[26] Begriff des „Schwarzsurfens" auch Sachverhalte bezeichnet werden, bei denen es um das bloße Einwählen in ein unverschlüsselt betriebenes WLAN-Netzwerk durch Dritte geht, ist zu betonen, wie leicht und damit letztlich wie zumutbar es regelmäßig für die Betreiber solcher Netzwerke ist, ihre Interessen durch entsprechende Standardkonfigurationen zu schützen. Es ist nicht Aufgabe des Strafrechts denjenigen zu schützen, der auf einfache Weise den Schutz seiner eigenen (privaten) Interessen selbst erreichen kann;[27] im Fall eines WLAN-Netzwerkes also das Interesse am Schutz vor einer ungewollten Mitbenutzung durch Dritte. Selbstverständlich bedürfen diejenigen, die ihren Internetzugang und ihr WLAN-Netzwerk zur freien Nutzung für jedermann bereitstellen wollen, keines solchen staatlichen Schutzes. Diverse „Freifunkprojekte"[28] legen vielmehr nahe, das Einwählen in offen betriebene WLAN-Netzwerke auch unter dem Gesichtspunkt eines – möglicherweise – „sozialadäquaten Verhaltens" zu betrachten. Die Mitbenutzung eines offenen Funknetzes stellt nicht generell einen Missbrauch dar; sie deutet nicht einmal von vornherein auf ein delinquentes Verhalten hin. Genauso ist danach zu fragen, ob ein unverschlüsselt betriebenes WLAN-Netzwerk heute nicht vielmehr auf eine bewusste Entscheidung des Betreibers schließen lässt und sogar von einem altruistischen Austauschgedanken geleitet wird.[29] Eine solche Gegenüberstellung zeigt jedenfalls, dass es im vorgenannten Sinne nicht dringlich und nicht verhältnismäßig sein kann, das Risiko der möglichen Einwahl in ein zwar offenes, aber tatsächlich vom Betreiber nicht absichtlich zur freien Nutzung bereitgestellten WLAN-Netzwerks auf den „fremden Nutzer" zu überlagern und ein solches Verhalten zu pönalisieren; auch nicht durch den Versuch einer extensiven Auslegung vorhandener Strafnormen. Es kann nicht generell davon ausgegangen werden, dass „offene Netze" Rechtsverletzungen über das Internet generell Vorschub leisten und die vorhandenen Instrumentarien des Straf- und auch Zivilrechts gegenwärtig hiermit überfordert sind.

Auch wenn der weithin schlagwortartig benutzte Begriff des „Schwarzsurfen" es suggeriert: Gerade bei den unter großer öffentlicher Beachtung behandelten Konstellationen, die vor Wuppertaler Gerichten verhandelt wurden, ging es nicht um „Schwarzsurfen", sondern um ein schlicht strafloses – möglicherweise sogar sozialadäquates – Verhalten.

Die Entscheidung des LG Wuppertal ist damit keinesfalls so bemerkenswert wie sie vielleicht in der „medialen Wirklichkeit" kommuniziert wurde. Sie ist schlicht konsequent.

24 BVerfGE 90, 145 – Cannabis; BVerfGE 88, 203, 258.
25 BVerfGE 88, 203, 258.
26 *Garcia*, Die Mär vom „Schwarzsurfen", http://blog.delegibus.com/2010/10/20/die-mar-vom-schwarzsurfen/ (15. 11. 2010).
27 *Buermeyer*, HRRS 2004, 285, 292.
28 Vgl. http://start.freifunk.net.
29 Dazu: *Garcia*, Die Mär vom „Schwarzsurfen", http://blog.delegibus.com/2010/10/20/die-mar-vom-schwarzsurfen/ (15. 11. 2010).

Anforderungen an Ausgestaltung einer AdWords-Anzeige

LG Berlin, Urteil vom 22. 9. 2010 – 97 O 55/10

§§ 14, 15, 19 MarkenG; §§ 9, 3, 4 Nr. 10 UWG

Die AdWords-Anzeige des Beklagten suggeriert keine wirtschaftliche Verbindung zwischen ihm und dem Markeninhaber. Der Text enthält nicht die Marke des Klägers oder eine Bezugnahme hierauf. Sie ist nicht so vage gehalten, dass der Nutzer nicht erkennen kann, ob der Werbende im Verhältnis zum Markeninhaber Dritter oder doch mit diesem wirtschaftlich verbunden ist. (Leitsatz der Redaktion)

Sachverhalt

Die Parteien vertreiben Kontaktlinsen nebst Zubehör u. a. über das Internet. Der Kläger ist Inhaber der beim Deutschen Patent- und Markenamt eingetragenen Wortmarke w… für die in diesem Unternehmensbereich einschlägigen Warenklassen. Die unter der Bezeichnung d… auftretende Beklagte schloss mit der Suchmaschine Google einen Vertrag über die Werbung mit so genannten Keyword-Advertising-Anzeigen. Gab der Nutzer der Suchmaschine w… als Suchbegriff ein, erschien nachfolgend in schwarz-weißer Ablichtung wiedergegebenes Ergebnis: … Ähnlich verhielt es sich bei dem Ausdruck für den vom Kläger als weiteren Suchbegriff eingeführten „www.w…de" bei Google. Auf die Abmahnung des Klägers gab die Beklagte ohne Anerkennung einer Rechtspflicht eine strafbewehrte Unterlassungserklärung ab.

Aus den Gründen

Die auch im Feststellungsantrag zulässige Klage ist unbegründet. Dem Kläger stehen wegen der in der Suchmaschine Google veröffentlichten Anzeigen nicht die geltend gemachten Folgeansprüche aus §§ 14, 15, 19 MarkenG oder §§ 9, 3, 4 Nr. 10 UWG gegen die Beklagte zu.

Markenrechtliche Ansprüche aus der eingetragenen Marke des Klägers oder einem Unternehmenskennzeichen nach §§ 14, 15 MarkenG scheiden aus, obwohl die Beklagte das Zeichen w… in einer nach Auffassung der Kammer ihr zurechenbaren Weise in Verbindung mit ihr obliegenden Prüfungspflichten (vgl. BGH [K&R 2004, 486 ff. =] GRUR 2004, 860, 864 – Internetversteigerung I) im geschäftlichen Verkehr nutzte, weil das Zeichen als Schlüsselwort im Rahmen eines von ihr bei Google beauftragten Referenzierungsdienstes der Auslöser für das Erscheinen der Werbung war (vgl. EuGH [K&R 2010, 397 ff. =] GRUR 2010,