
Datum: 19.10.2010
Gericht: Landgericht Wuppertal
Spruchkörper: 5. große Strafkammer
Entscheidungsart: Beschluss
Aktenzeichen: 25 Qs 10 Js 1977/08-177/10
ECLI: ECLI:DE:LGW:2010:1019.25QS10JS1977.08.1.00

Vorinstanz: Amtsgericht Wuppertal, 26 Ds 282/08
Sachgebiet: Strafrecht

Tenor:

Die sofortige Beschwerde wird auf Kosten der Staatskasse (§ 473 Abs. 1 StPO) als unbegründet verworfen.

Gründe

Die zulässig erhobene sofortige Beschwerde ist unbegründet. Denn das Amtsgericht hat durch den angefochtenen Beschluss zu Recht die Eröffnung der Hauptverhandlung aus rechtlichen Gründen abgelehnt. 1 2

Mit Anklageschrift vom 08. Dezember 2008 hat die Beschwerdeführerin dem Angeschuldigten vorgeworfen, am 26. und 27. August 2008 das Haus I-Straße in X aufgesucht zu haben, um sich mit seinem Laptop Xx Satellite 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. 3

Mit Beschluss vom 03. August 2010 hat das Amtsgericht X 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 § 202b StGB liege nicht vor. Gegen den ihr am 06. August 2010 zugestellten Beschluss wendet sich die Beschwerdeführerin mit der am 11. August 2010 4

eingelegeten sofortigen Beschwerde.

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 Amtsgericht X im Ergebnis zutreffend ausgeführt hat, ein strafbares Verhalten nicht ersichtlich ist. 5

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. 6

Hierzu hat das Amtsgericht 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*) 7

Dieser Argumentation schließt sich die Kammer an. Sofern das Amtsgericht X demgegenüber in einer Entscheidung aus dem Jahr 2007 (AG X, Urteil vom 03.04.2007, Az: 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*). 8

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 9

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 abrufen. Bei dem Einwählen in ein unverschlüsselt betriebenes WLAN und der anschließend hierüber erfolgten Nutzung des Internetzuganges werden, wie das Amtsgericht zutreffend ausgeführt hat, keine personenbezogenen Daten abgerufen. Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlicher 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*). 10

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*). 11

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 12

WLAN-Routers befunden hätte, diese Adresse abrufen können (vgl. *Ernst/Spoenle CR 2007, 439, 442*).

Nicht in Betracht kommt weiterhin eine Strafbarkeit wegen eines Ausspäehens von Daten gemäß § 202a 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. 13

Das vorgeworfene Einwählen in das fremde, unverschlüsselt betriebene Netzwerk begründet auch keine Strafbarkeit wegen eines Abfangens von Daten nach § 202b 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. Auflage, 2010, § 202b Rn. 4*). Da § 202b StGB ebenso wie das in § 89 TKG normierte Abhörverbot die Vertraulichkeit von Datenübermittlungen schützt (vgl. *Bär MMR 2008, 632, 634*) sind solche Datenübermittlungen von vorneherein auszuschließen, die für einen unbestimmten Personenkreis (z.B. beim Amateurfunk: für jeden empfangsbereiten Teilnehmer) wahrnehmbar sein sollen (vgl. *Gröseling/Höfingler 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/Höfingler 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. 14

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 §§ 263a, 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, 160ff.*). Unbefugt ist die Verwendung, wenn sie gegenüber einer natürlichen Person Täuschungscharakter hätte (vgl. *Fischer, Strafgesetzbuch und Nebengesetze, 57. Auflage, 2010, § 263a Rn. 11*). An einer solchen täuschungsgleichen Handlung fehlt es. Bei einem unverschlüsselt betriebenen 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*). 15

Auch nach § 265a StGB ist das dem Angeschuldigten vorgeworfene Verhalten nicht strafbar. Der objektive Tatbestand des § 265a StGB setzt als ungeschriebenes Tatbestandsmerkmal die Entgeltlichkeit der erschlichenen Leistung voraus (vgl. *Perron in Schönke/Schröder, aaO, § 265a 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. 16

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 17

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, aaO, § 265a 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, aaO, § 265a Rn. 18*) ist auch das ordnungsgemäße Nutzen eines offenen - und damit technisch jedermann zur Verfügung gestellten - WLAN nicht nach § 265a StGB strafbar.

Die Kostenentscheidung folgt aus § 473 Abs. 1 S. 1 StPO.

18