

Standpunkt

Schwarz-Surfen mit weißer Weste? Zur Strafbarkeit des Einloggens in ein fremdes unverschlüsseltes WLAN. Weite Schatten hatte eine 2008 veröffentlichte Entscheidung des AG *Wuppertal* (NSTZ 2008, 161) geworfen, das die Nutzung eines offenen WLAN durch einen Dritten als strafbares Abhören von Nachrichten gem. § 89 S. 1 TKG sowie einen Verstoß gegen Strafvorschriften des Bundesdatenschutzgesetzes (§ 44 i.V. mit § 43 II Nr. 3 BDSG, Unbefugtes Abrufen oder Verschaffen personenbezogener Daten) bewertet hatte. Bis heute wird die Meinung zwar immer wieder heftig kritisiert, doch wurde ihr durchaus auch gefolgt, so zuletzt Ende 2009 durch das AG *Zeven*.

Kürzlich hatte sich das AG *Wuppertal* erneut mit dieser Rechtsfrage zu beschäftigen. Im Zuge dessen hat es seine frühere Rechtsprechung unter Verweis auf ein bisheriges „Überspannen des Schutz- und Strafbereichs der in Betracht kommenden Strafvorschriften“ aufgegeben und die Eröffnung eines Hauptverfahrens gegen den „Schwarzsurfer“ mangels hinreichenden Tatverdachts abgelehnt (Beschl. v. 3. 8. 2010 – 26 Ds-10 Js 1977/08-282/08, BeckRS 2010, 19628). Eine Strafbarkeit des Angeschuldigten, dem vorgeworfen worden war, sich „mit seinem Laptop mittels einer drahtlosen Netzwerkverbindung in das offene Funknetzwerk eines Dritten eingewählt zu haben, um ohne Erlaubnis (...) die Internetnutzung zu erlangen“ sei nicht ersichtlich. Zum einen sei ein Abhören von Nachrichten, die für die Allgemeinheit oder einen unbestimmten Personenkreis bestimmt sind, also eine Strafbarkeit nach § 89 TKG nicht gegeben. Noch im Urteil von 2008 war genau das in Bezug auf den insoweit gleich gelagerten Sachverhalt angenommen worden: In der Zuweisung der IP-Adresse durch den Router habe eine Nachricht im Sinne der Strafvorschrift, in der Internetnutzung ein „Abhören“ gelegen. Die Nachricht sei überdies nicht für den Angeklagten bestimmt gewesen.

Die Korrektur dieser Sichtweise war überfällig. Es erscheint unübersehbar, dass es sich nur dann um eine Nachricht handelt, wenn diese Gegenstand einer Kommunikation zwischen zwei Personen ist. Denn Schutzzweck des § 89 TKG ist einzig die Vertraulichkeit von Kommunikation. Die Vergabe einer IP-Adresse unterfällt also dem Schutzbereich nicht. Damit ist dies auch keine „Nachricht“ im Sinne der Norm. Der aktuelle Beschluss lässt diesen Punkt letztlich offen und spricht nur davon, dass es „fraglich“ sei, ob es sich bei der Vergabe der IP-Adresse um eine „Nachricht“ handele. Deutlicher bezieht das Urteil Stellung, wenn es klarstellt, dass insbesondere das Nutzen des Internetzugangs kein „Abhören“ im Sinne der Vorschrift sei. Dies ergebe sich bereits aus dem Wortlaut der Norm. Dieser erfordere einen zwischen anderen Personen stattfindenden Kommunikationsvorgang, den der Täter als Dritter mithöre. Ein bewusster und gezielter Empfang und das bewusste und gezielte Wahrnehmen fremder Nachrichten lägen bei dem Nutzer eines fremden WLAN nicht vor. Schließlich sei die IP-Adresse auch für den Angeschuldigten bestimmt gewesen, da er der einzige Teilneh-

mer der Internetverbindung gewesen ist. Damit scheidet es wohl auch nach Ansicht des AG *Wuppertal* spätestens an der Fremdheit der Nachricht, die nach soeben erfolgter Darstellung unabdingbar für ein „Abhören“ ist.

Auch der Kurswechsel betreffend die datenschutzrechtliche Bewertung des Schwarz-Surfens war erforderlich. Der Tatbestand des § 44 i.V. mit § 43 II Nr. 3 BDSG war – insoweit trifft der Beschluss die Rechtslage – nicht erfüllt. Durchaus undeutlich gestaltet sich jedoch die Begründung: Der Angeschuldigte habe keine personenbezogenen Daten abgerufen oder sich verschafft. In Betracht seien auch hier allenfalls die IP-Daten gekommen. Diese seien jedoch keine personenbezogenen Daten i. S. des § 3 I BDSG. Personenbezogene Daten seien hiernach alle Informationen über persönliche und sachliche Verhältnisse, die einer natürlichen Person zuzuordnen seien und nicht allgemein zugänglich seien. Zudem könne, wer sich in ein WLAN einwählt, grundsätzlich nicht erkennen, wer der Betreiber des WLANs ist. Dass dies bei dem Angeschuldigten anders sein sollte, sei nicht ersichtlich. In diesen Aussagen liegen gewisse Unklarheiten: So dürfte sich seit der sich an das Urteil des AG *Berlin* vom 27. 3. 2007 (5 C 314/06, BeckRS 2007, 18728) anschließenden Diskussion nicht mehr per se behaupten lassen, dass „IP-Daten“ keine personenbezogenen Daten seien. Treffend wäre es gewesen, hier darauf zu verweisen, dass es sich bei der IP-Adresse zwar sehr wohl um ein personenbezogenes Datum i.S. von § 3 I BDSG handelt, jedoch eben nicht um ein fremdes personenbezogenes Datum, welches für ein „unbefugtes“ Abrufen oder Verschaffen im Sinne der Normen erforderlich ist, sondern um ein eigenes Datum des Schwarzsurfers gem. § 1 I BDSG. Damit hätte sich auch der irreführende Verweis darauf, dass man schließlich nicht wissen könne, wer das WLAN betreibe, erledigt. Dieses Wissen steht angesichts der Zuteilung der IP-Adresse an den Schwarz-Surfer außer Frage und ist Spiegelbild der Feststellung, dass es sich bei der IP-Adresse um ein eigenes personenbezogenes Datum des Schwarz-Surfers handelt. Weiterhin verweist die Begründung – wie dargestellt – auf § 3 I BDSG, doch ist das Negativmerkmal „nicht allgemein zugänglich“ keine Frage der Personenbezogenheit von Daten, sondern, etwa im Zusammenhang mit § 28 I Nr. 3 BDSG, der Rechtfertigung deren Verarbeitung. Genau eine solche Rechtfertigung ist übrigens in Bezug auf den durch den Schwarzsurfer bei Einloggen zur Kenntnis genommenen SSID (Service Set Identifier bzw. Netzwerkname) gegeben. Dieses regelmäßig als personenbezogen einzuordnende Datum ist auf dem Wege des SSID Broadcasting bewusst und freiwillig durch den Netzwerkinhaber veröffentlicht worden. Damit war dieses allgemein zugänglich gem. § 28 I Nr. 3 BDSG. Die Kenntnisnahme des Netzwerknamens ist demnach nicht nach BDSG strafbar. Genau das wäre allerdings immer der Fall, wenn man hinsichtlich der datenschutzrechtlichen Bewertung die nach dem Urteil aus 2008 zu Grunde liegende Meinung verträte, was nicht vertretbar erscheint: Schließlich wäre ansonsten schon jeder User, der einen WLAN-Client betreibt und automatisch mitgeteilt bekommt, welche Netzwerke sich in

seiner Umgebung befinden und welche Namen diese tragen, strafrechtlich dafür verantwortlich.

Die *Staatsanwaltschaft Wuppertal* hat Beschwerde gegen den Beschluss des *Amtsgerichts* eingelegt. Kommt eine Korrektur der Korrektur?

Rechtsanwalt Dr. Karsten Kinast, LL.M., Bonn