# Strafbarkeit der Installation eines Backdoor-Trojaners mittels Einsatzes einer Software zur Passwortentschlüsselung von ICQ zur Aktivierung der Webcam am Zielrechner und Übersendung von Aufnahmen hierüber wegen Ausspähens von Daten und Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen

**Gericht**

AG Düren

**Datum**

10.12.2010

**Aktenzeichen**

10 Ls 275/10, 10 Ls – 806 Js 644/10 – 275/10

**Branche/ Lebenslage**

Backdoor-Trojaner, Webcam, Bildaufnahmen, Ausspähen von Daten, Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen, § 202a StGB, § 201a StGB, heimliche Bildaufnahmen, Passwort, Entschlüsselung, ICQ

**Akteure**

Täter, Opfer

**Wer haftet?**

Täter

**Haftungsart**

Freiheitsstrafe oder Geldstrafe

**Haftungsumfang**

Hier: Gesamtfreiheitsstrafe von 1 Jahr und 10 Monaten, Verfahrenskosten

**Haftungsbegründendes Verhalten**

Erfüllung der Straftatbestände des Ausspähens von Daten, § 202a StGB, und der Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen, § 201a StGB

**Technische Umstände**

Übersendung eines Trojaners, der ein Backdoor-Programm installiert, und anschließende Aktivierung der an dem Opferrechner angeschlossenen Webcam zur Erstellung von heimlichen Bildaufnahmen

**Persönliche Umstände**

Vorsätzliche, rechtswidrige und schuldhafte Begehung einer Straftat

**Möglichkeiten der Haftungsvermeidung**

–

**Zitate, Zusammenfassende Würdigung, Strategien zur Haftungsvermeidung**

Der Täter hat sich durch den Einsatz einer Software zum Entschlüsseln von Passwörtern die Anmeldedaten verschiedener Nutzer eines Instant-Messaging-Dienstes (konkret: ICQ) verschafft.

Anschließend meldete er sich unter Vortäuschung der Identität des jeweiligen Nutzers unter dessen Profil bei dem Chat-Dienst an und forderte Mitglieder aus der Kontaktliste des Nutzers auf, eine vom ihm gesendete Bild-Datei zu öffnen, die einen Trojaner enthielt. Mit Hilfe eines durch den Trojaner installierten sog. Backdoor-Programms konnte der Täter an dem jeweiligen Opferrechner angeschlossene Webcams aktivieren und durch diese Bildaufnahmen anfertigen und sich selbst übersenden lassen.

Nach den Feststellungen des AG Düren machte sich der Täter durch das beschriebene Vorgehen wegen Ausspähens von Daten, § 202a StGB, in Tateinheit mit Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen, § 201a StGB, strafbar.

**ANMERKUNGEN**

Das AG Düren äußerte sich zur Strafbarkeit der Installation eines Backdoor-Trojaners mittels Einsatzes einer Software zur Passwortentschlüsselung von ICQ zur Aktivierung der Webcam am Zielrechner und Übersendung von Aufnahmen hierüber. Im Ergebnis zutreffend bejaht das Gericht ohne allzu ausführliche Begründung eine Strafbarkeit wegen Ausspähens von Daten und Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen.

§ 202a StGB (Ausspähen von Daten) schützt dabei die Verfügungsbefugnis des Berechtigten über seine Daten. Ein entsprechendes Ausspähen wird daher oftmals auch als „elektronischer Hausfriedensbruch“ bezeichnet (Spitz, jurisPR-ITR 17/2011 Anm. 4). Hervorzuheben bleibt, dass der Tatbestand dem Wortlaut und seiner systematischen Stellung nach keine wirtschaftlichen Interessen beim Täter erfordert – solche waren beim Täter im vorliegenden Fall nicht gegeben. Der Täter hat die ausgespähten und gefilmten Opfer nicht etwa zu einer Zahlung aufgefordert oder ähnliches.

In der Literatur umstritten ist, ob die Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen, § 201a StGB infolge einer durch Schadsoftware herbeigeführten Manipulation der am Opferrechner angeschlossenen Webcam eine spezifische Verletzung der Intimsphäre des Opfers erfordert. So sei der Begriff des „höchstpersönlichen Lebensbereichs“ nach Spitz nicht zwingend deckungsgleich mit dem vom Bundesverfassungsgericht im Rahmen der Grundsätze zum allgemeinen Persönlichkeitsrecht entwickelten Begriff der „Intimsphäre“ (Spitz, jurisPR-ITR 17/2011 Anm. 4). Da sich der Begriff des „persönlichen Lebensbereichs“ nach dem Willen des Gesetzgebers jedoch an demjenigen der „Intimsphäre“ orientieren soll, ist die Anwendung der Vorschrift nach herrschender Meinung zwingend auf Fälle zu begrenzen, in denen eine Verletzung der Intimsphäre vorliegt (Heuchemer, in: BeckOK StGB, 37. Edition, Stand: 01.02.2018, § 201a Rn. 14.1). Als Folge dieser Einschränkung ist die Videoüberwachung eines fremden Wohn-, Ess- oder Arbeitszimmers (in der letzten Variante bspw. auch durch den Arbeitgeber) also grundsätzlich nach wie vor straflos (Heuchemer, in: BeckOK StGB, 37. Edition, Stand: 01.02.2018, § 201a Rn. 15). Im Einzelfall kann jedoch auch hier die Intimsphäre des Aufgezeichneten berührt sein.