

# Strafbarkeit des Betriebens eines Card-Sharing-Servers für Pay-TV-Sender als Computerbetrug, unerlaubten Eingriffs in technische Schutzmaßnahmen und Beihilfe zum Ausspähen von Daten

**Gericht**

OLG Celle

**Datum**

31.08.2016

**Aktenzeichen**

2 Ss 93/16

**Branche/ Lebenslage**

Computerbetrug, Eingriff in technische Schutzmaßnahmen, Card-Sharing-Server für Pay-TV

**Akteure**

Anbieter Card-Sharing-Server, Ermittlungsbehörde

**Wer haftet?**

Strafbarkeit des Anbieters des Card-Sharing-Servers

**Haftungsart**

Computerbetrug, § 263a StGB (Täterschaft), unerlaubter Eingriff in technische Schutzmaßnahmen, § 108 UrhG (Täterschaft), Ausspähen von Daten, § 202a StGB (Beihilfe, § 27 Abs. 1 StGB)

**Haftungsumfang**

-

**Haftungsbegründendes Verhalten**

Ermöglichung, das Sendeprogramm eines Bezahlsenders zu nutzen, ohne Abonnement des Bezahlsenders zu sein und diesem ein Entgelt zu zahlen

**Technische Umstände**

Über die (unbefugte) Nutzung des Kontrollwortes konnten Kunden des Card-Sharing-Servers auf die verschlüsselten Inhalte des Pay-TV-Senders zugreifen

**Persönliche Umstände**

Der Anbieter des Card-Sharing-Servers handelte vorsätzlich. Ihm kam es gerade auf die Zahlung eines Entgelts für die Schaffung der Zugangsmöglichkeit zu den Angeboten des Bezahlsenders an. Aufgrund der Erfassung sämtlicher Kunden samt Name und Adresse war sich der Anbieter darüber im Klaren, nicht ausschließlich mit Kunden aus Ländern in Kontakt zu stehen, für die der Bezahlsender keine Sendelizenz hatte

## **Möglichkeiten der Haftungsvermeidung**

Sowohl die unbefugte Zurverfügungstellung von Zugangsdaten eines Bezahlsenders, als auch deren Nutzung kann strafrechtliche Konsequenzen haben; das gilt selbst dann, wenn für die Nutzung der Zugangsdaten ein Entgelt an der Vermittler gezahlt wird

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

Gegen den Anbieter eines Card-Sharing-Servers wurde wegen Computerbetrugs, § 263a Abs. 1 StGB, Eingriffs in technische Schutzmaßnahmen, § 108 Abs. 1 Nr. 1 UrhG und Ausspähen von Daten, § 202a Abs. 1 StGB ermittelt. Der Anbieter hatte den Nutzern seines Servers ermöglicht, auch die Pay-TV-Signale des Pay-TV-Senders zu entschlüsseln, bei dem der Server-Anbieter selbst Kunde war. Das Abonnement des Pay-TV-Senders war so konzipiert, dass nur die an den Sender direkt zahlenden Kunden Zugang zum Sendeangebot haben sollten.

Ein Computerbetrug war gegeben. Sowohl bei dem – verschlüsselt – gesendetem Pay-TV-Fernsehprogramm als auch dem – ebenfalls verschlüsselten – Kontrollwort handelt es sich um Daten im Sinne des § 263a StGB (Computerbetrug). Im Bereich des Bezahlfernsehens ist eine Beeinflussung eines Datenverarbeitungsvorgangs insbesondere dann gegeben, wenn „das verschlüsselt ausgestrahlte Pay-TV-Programm durch Manipulation einer Smartcard oder unter Einsatz einer unbefugt hergestellten sogenannten Piratenkarte entschlüsselt und damit sichtbar gemacht wird.“ Die Kunden des Card-Sharing-Servers nutzten das Kontrollpasswort des Bezahlsenders unbefugt, weil diese selbst nicht Abonnenten des Senders waren. Die Versendung des Kontrollwortes durch den Anbieter des Card-Sharing-Servers war unbefugt, weil dieser im Rahmen seines Pay-TV-Abonnements nicht zur Weitergabe berechtigt war.

Den Kunden des Card-Sharing-Servers wurde „die Möglichkeit gegeben [...], das entschlüsselte Pay-TV-Programm [des Pay-TV-Senders] anzuschauen, ohne hierfür Geld an [den Pay-TV-Sender] zu zahlen.“ Durch die unbefugte Entschlüsselung des Pay-TV-Senders und Sichtbarmachung des Programms, wurde „das beim Pay-TV-Sender liegende Nutzungsrecht an den Programminhalten angegriffen.“ Dies stellt auch einen Vermögensnachteil dar.

Der Card-Sharing-Server-Anbieter kann sich nicht auf fehlenden Vorsatz mit der Begründung berufen, er habe die Zugangsmöglichkeit nur an Kunden mit Sitz in Ländern, in denen der Sender keine Sendelizenz habe, vermitteln wollen. Der Anbieter hatte in seiner Kundendatei Namen und Anschriften seiner Kunden erfasst und wusste somit, dass es sich sämtlich um Kunden aus dem Bundesgebiet handelte.

Auch eine Strafbarkeit wegen unerlaubten Eingriffs in technische Schutzmaßnahmen ist gegeben. Die Verschlüsselungstechnologie des Pay-TV-Senders ist eine technische Maßnahme im Sinne des § 108 Abs. 1 Nr. 1 UrhG. „Diese Maßnahme ist [vom Anbieter des Card-Sharing-Servers] umgangen worden.“

Eine Strafbarkeit wegen des Ausspähens von Daten als Täter ist nicht gegeben. Dazu führt das Gericht aus, dass „Daten im Sinne der Norm (§ 202a StGB) nur gerade nicht für den Täter bestimmte Daten sein können. Das bloß zweckwidrige Verwenden von Daten durch einen grundsätzlich berechtigten Verwender wird von § 202a Abs. 1 StGB nicht erfasst.“ Ein solches Verhalten war hier aber gegeben. Dem Anbieter des Card-Sharing-Servers waren die Nutzungsdaten gerade aufgrund der Abonnement-Vereinbarung bestimmungsgemäß überlassen worden. Eine Strafbarkeit wegen Beihilfe zum Ausspähen von Daten durch die Kunden des Card-Sharing-Servers ist nicht dadurch ausgeschlossen, dass der Anbieter des Servers gegenüber dem Bezahlsender zur Datennutzung berechtigt war. „Eine Teilnahme an einer Tat nach „202a StGB ist [...] auch durch berechtigte Personen möglich.“ Die Kunden des Servers hatten die Daten dadurch ausgespäht, dass sie die Schutzvorkehrungen, zur Verhinderung eines unbefugten Zugriffs überwunden haben, um Zugang zu den dort vermittelten Inhalten zu erlangen.

## **ANMERKUNGEN**

Das Gericht äußerte sich zu der strafrechtlichen Beurteilung des entgeltlichen Anbietens einer Möglichkeit, Zugriff auf verschlüsselte Inhalte eines Bezahlsenders nehmen zu können, ohne selbst Abonnement dieses Senders zu sein.

Eine Strafbarkeit wegen Computerbetrugs und unerlaubten Eingriffs in technische Schutzmaßnahmen bejahte das Gericht. Eine Strafbarkeit wegen Ausspähen von Daten in Täterschaft wurde zwar abgelehnt, das Gericht nahm hier allerdings eine Strafbarkeit wegen Beihilfe an.

Der Einsatz des Kontrollpassworts des Pay-TV-Senders durch die Kunden des Card-Sharing-Servers war unbefugt, weil diese selbst nicht Abonnenten des Pay-TV-Senders waren. Auch die Weitersendung des Kontrollpasswortes war unbefugt, weil eine Weitergabe des Kontrollwortes nicht von den Rechten aus dem Abonnement umfasst wurde.

Das Gericht sah eine Umgehung von technischen Schutzmaßnahmen im Sinne des § 108 UrhG in jedem Verhalten, welches eine Nutzung ermöglicht, das ohne dieses Verhalten gerade aufgrund der technischen Schutzmöglichkeit nicht möglich gewesen wäre. Es vertritt damit eine weite Auslegung des Umgehungsbegriffs. Im vorliegenden Fall sah das Gericht diese Voraussetzung aufgrund der, vertraglich nicht erlaubten, Verschaffung der Zugangsmöglichkeit zu den Inhalten des Bezahlsenders als erfüllt an.

Eine Täterschaft beim Ausspähen von Daten im Sinne des § 202a StGB lehnte das Gericht mit der Begründung ab, dass die Norm hier keine Anwendung finde, weil der Anbieter des Card-Sharing-Servers grundsätzlich zu der Datennutzung berechtigt war. Dass er sich aufgrund der Weitergabe an Kunden des Card-Sharing-Servers vertragswidrig verhielt, änderte nichts an der Beurteilung, dass dieser grundsätzlich die Daten nutzen durfte. Die Beihilfe zu der Tat sei aber auch bei eigentlicher Berechtigung der Datennutzung möglich. Hier hatte der Server-Anbieter Beihilfe zur Ausspähung von Daten durch seine Server-Kunden geleistet.

Praxishinweis: Dem Urteil muss sich nicht nur der Betreiber eines Card-Sharing-Servers einer strafrechtlichen Verantwortung stellen. Auch dessen Kunden kann, zumindest hinsichtlich des Ausspähen von Daten, § 202a StGB ein Tatvorwurf gemacht werden.