

Skimming (= Auslesen von auf dem Magnetstreifen gespeicherten Daten einer Zahlungskarte mit Kreditfunktion zur Herstellung von Kartendoubletten) nicht als Ausspähen von Daten (§ 202a Abs. 1 StGB) strafbar

**Gericht**

BGH

**Datum**

14.01.2010

**Aktenzeichen**

4 StR 93/09

**Branche/ Lebenslage**

Skimming, Ausspähen von Daten, § 202a StGB, Auslesen von Daten, Magnetstreifen, Geldautomat, Kreditkarte, EC-Karte

**Akteure**

Täter, Opfer

**Wer haftet?**

Grundsätzlich Täter, aber keine Strafbarkeit nach § 202a StGB

**Haftungsart**

Grundsätzlich Freiheitsstrafe, Geldstrafe, hier (-)

**Haftungsumfang**

Bis zu drei Jahre, hier (-)

**Haftungsbegründendes Verhalten**

Erfüllung des Straftatbestandes des § 202a StGB, hier (-)

**Technische Umstände**

-

**Persönliche Umstände**

-

**Möglichkeiten der Haftungsvermeidung**

-

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

Das bloße Auslesen von Daten, die auf dem Magnetstreifen einer Zahlungskarte (Kreditkarte oder EC-Karte) gespeichert sind (das sind bei einer EC-Karte beispielsweise unter anderem Kontonummer und Bankleitzahl bzw. IBAN), um mit diesen Daten Kartendoubletten herzustellen (sog. Skimming), erfüllt zumindest nicht den Tatbestand des „Ausspähens von Daten“ i.S.d. § 202a Abs. 1 StGB (juris Rn. 3).

§ 202a Abs. 1 StGB setzt unter anderem voraus, dass der Täter sich oder einem anderen den Zugang zu Daten, die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft. Wenn die jeweiligen Daten jedoch lediglich ausgelesen werden, wird keine Zugangssicherung „überwunden“. Das Auslesen ist nämlich ohne Weiteres mittels eines handelsüblichen Lesegeräts und einer ebenfalls im Handel erhältlichen Software möglich. Es ist keine besondere Sicherung gegen unberechtigten Zugang, wenn Daten magnetisch und damit nicht unmittelbar wahrnehmbar gespeichert sind. Vielmehr handelt es sich gemäß § 202a Abs. 2 StGB erst um Daten, wenn sie auf diese Weise gespeichert sind (juris Rn. 3)

### **ANMERKUNGEN**

Mit der vorliegenden Entscheidung stellt der Bundesgerichtshof klar, dass das sog. „Skimming“ nicht als Ausspähen von Daten i.S.d. § 202a Abs. 1 StGB zu qualifizieren ist.

Als Skimming bezeichnet man das Auslesen und Kopieren von auf dem Magnetstreifen gespeicherten Daten einer Bank- oder Kreditkarte, um damit Kartendoubletten herzustellen und mit diesen und der ebenfalls ausspionierten PIN Geldabhebungen im Ausland vorzunehmen.

Eine Strafbarkeit zumindest nach § 202a Abs. 1 StGB scheitert am fehlenden Vorliegen einer besonderen Zugangssicherung, die überwunden werden müsste.

Die Täter sind indes nicht straffrei, da andere Zahlungskartendelikte in Betracht kommen, neben denen eine etwaige Tat nach § 202a StGB ohnehin nicht ins Gewicht fällt. Genannt seien hier die (gewerbs- und bandenmäßige) Fälschung von Zahlungskarten mit Garantiefunktion (§ 152b StGB) und ein (gewerbs- und bandenmäßiger) Computerbetrug (§ 263a StGB).

An der vorliegenden Rechtsprechung hält der Bundesgerichtshof fest (vgl. BGH, Beschl. v. 18.03.2010 – 4 StR 555/09; Beschl. v. 06.07.2010 – 4 StR 555/09).