HRRS-Nummer: HRRS 2010 Nr. 452
Bearbeiter: Karsten Gaede
Zitiervorschlag: BGH HRRS 2010 Nr. 452, Rn. X

BGH 4 StR 555/09 - Beschluss vom 18. März 2010 (BGH)

Anfrageverfahren zum Skimming; Auslesen der auf dem Magnetstreifen einer Zahlungskarte mit Garantiefunktion gespeicherten Daten (Herstellung von Kartendubletten; Ausspähen von Daten; gegen unberechtigten Zugang besonders gesicherte Daten; Überwindung der Zugangssicherung); redaktioneller Hinweis.

§ 202a Abs. 1 StGB n.F.

Leitsätze des Bearbeiters

1. Der Senat beabsichtigt zu entscheiden: Das bloße Auslesen der auf dem Magnetstreifen einer Zahlungskarte mit Garantiefunktion gespeicherten Daten, um mit diesen Daten Kartendubletten herzustellen, erfüllt nicht den Tatbestand des Ausspähens von Daten (§ 202a Abs. 1 StGB n.F.).

2. Eine Schutzvorkehrung ist nur dann eine Zugangssicherung im Sinne des § 202a Abs. 1 StGB n.F., wenn sie jeden Täter zu einer Zugangsart zwingt, die der Verfügungsberechtigte erkennbar verhindern wollte.

Entscheidungstenor

Der Senat beabsichtigt zu entscheiden: Das bloße Auslesen der auf dem Magnetstreifen einer Zahlungskarte mit Garantiefunktion gespeicherten Daten, um mit diesen Daten Kartendubletten herzustellen, erfüllt nicht den Tatbestand des Ausspähens von Daten (§ 202 a Abs. 1 StGB n.F.).

Der Senat fragt daher beim 3. Strafsenat an, ob an dem Urteil vom 10. Mai 2005 - 3 StR 425/04 (NStZ 2005, 566) festgehalten wird. Ferner fragt er bei dem 1., 2. und 5. Strafsenat an, ob dortige Rechtsprechung entgegensteht.

Gründe

1. Das Landgericht hat den Angeklagten u.a. der gewerbs- und bandenmäßigen Fälschung von Zahlungskarten mit Garantiefunktion in Tateinheit mit gewerbs- und bandenmäßigem Computerbetrug und mit dem Ausspähen von Daten in drei Fällen schuldig gesprochen. Diesen Schuldsprüchen liegt im Wesentlichen Folgendes zu Grunde: 1

Der Angeklagte und die gesondert verfolgten, aus Rumänien nach Deutschland eingereisten V., N. und C. sowie der seit Jahren in Deutschland lebende P. schlossen sich Anfang Februar 2007 als Bande zusammen, um gewerbsmäßig zur Täuschung im Rechtsverkehr in einer Vielzahl von Fällen falsche Zahlungskarten mit Garantiefunktion herzustellen und mit diesen Karten im Ausland an Geldautomaten Geld abzuheben. Um sich die zum Nachmachen echter Zahlungskarten mit Garantiefunktion benötigten Daten zu verschaffen, die auf den Magnetstreifen solcher Karten gespeichert sind, setzten der Angeklagte und seine Mittäter ein mit einem Speichermedium versehenes Kartenlesegerät ein, das unauffällig vor den in die Geldautomaten eines bestimmten Typs eingebauten Einzugslesegeräten angebracht werden konnte. Die bei der Benutzung des Geldautomaten vom Inhaber der Zahlungskarte eingegebene PIN erlangten sie mittels eines über der Tastatur des Geldautomaten angebrachten, ebenfalls mit einem Speichermedium versehenen Tastaturaufsatzes. Auf diese Weise verschafften sich der Angeklagte und seine Mittäter am 17. Februar 2007 durch Anbringen solcher Geräte an einem Geldautomaten in einer Bank in M. 21 Datensätze von Zahlungskarten und die jeweils zugehörige PIN, am 24. Februar 2007 durch Anbringen der Geräte an einem Geldautomaten einer Bank in D. 21 Datensätze und am 7. Juli 2007 in O. weitere 35 Datensätze von Zahlungskarten. Nach dem Entfernen der Aufsatzgeräte von den Geldautomaten wurden die Speichermedien der Geräte jeweils vom Angeklagten allein oder mit Hilfe eines weiteren Mittäters ausgelesen. Mit den Datensätzen der echten Zahlungskarten wurden dann die Magnetstreifen von Payback-Karten, die Bandenmitglieder zuvor beschafft hatten, beschrieben. In der Folgezeit hoben Mitglieder der Bande unter Verwendung der nachgemachten Karten und der zu diesen Datensätzen jeweils zugehörigen PIN an Geldautomaten im Ausland Bargeld ab. 2

2. Der Senat beabsichtigt, das Urteil dahin zu ändern, dass in den vorgenannten Fällen jeweils der Schuldspruch wegen tateinheitlichen Ausspähens von Daten entfällt. Nach Auffassung des Senats erfüllt das bloße Auslesen der auf dem Magnetstreifen einer Zahlungskarte mit Garantiefunktion gespeicherten Daten, um mit diesen Daten Kartendubletten herzustellen, nicht den Tatbestand des Ausspähens von Daten (vgl. Senatsbeschl. vom 14. Januar 2010 - 4 StR 93/09). 3

Zwar haben sich der Angeklagte und seine Mittäter mittels des an dem jeweiligen Geldautomaten angebrachten Lesegeräts unberechtigt den Zugang zu Daten verschafft, die nicht für sie bestimmt waren. § 202 a Abs. 1 StGB n.F. setzt aber darüber hinaus voraus, dass sich der Täter Daten, "die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft". Das ist jedoch nicht der Fall, wenn sich der Täter - wie hier - den Zugang zu den auf dem Magnetstreifen der Zahlungskarte gespeicherten Daten mittels eines vor dem Einzugslesegerät eines Geldautomaten angebrachten weiteren Lesegeräts verschafft (sog. Skimming), um mit diesen Daten in ihrer ursprünglichen Form den Magnetstreifen einer Kartendublette zu beschreiben. 4

Dass Daten magnetisch und damit nicht unmittelbar wahrnehmbar gespeichert sind, stellt keine besondere Sicherung gegen unberechtigten Zugang dar. Vielmehr handelt es sich gemäß § 202 a Abs. 2 StGB n.F. nur bei Daten, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert oder übermittelt werden, um Daten im Sinne des Abs. 1 dieser Vorschrift. Demgemäß schützt § 202 a Abs. 1 StGB n.F. nur diejenigen nicht unmittelbar wahrnehmbar gespeicherten Daten im Sinne des Abs. 2 dieser Vorschrift, die darüber hinaus besonders gesichert sind. Das sind nur solche Daten, bei denen der Verfügungsberechtigte durch seine Sicherung sein Interesse an der Geheimhaltung der Daten dokumentiert hat (vgl. BT-Drucks. 10/5058, S. 29 zu § 202 a StGB a.F.; BT-Drucks. 16/3656, S. 10). Erforderlich ist, dass der Verfügungsberechtigte - hier das Unternehmen, das die Zahlungskarte mit Garantiefunktion ausgegeben hat (vgl. BGH, Urt. vom 10. Mai 2005 - 3 StR 425/04, NStZ 2005, 566) - Vorkehrungen getroffen hat, den Zugriff auf die auf dem Magnetstreifen der Zahlungskarte gespeicherten Daten auszuschließen oder wenigstens nicht unerheblich zu erschweren (vgl. BT-Drucks. 16/3656, S. 10; Fischer StGB 57. Aufl. § 202 a Rdn. 8, jew. m.w.N.). Eine Schutzvorkehrung ist jedoch nur dann eine Zugangssicherung im Sinne des § 202 a Abs. 1 StGB n.F., wenn sie jeden Täter zu einer Zugangsart zwingt, die der Verfügungsberechtigte erkennbar verhindern wollte (BT-Drucks. 16/3656 aaO; Fischer aaO). 5

Der Überwindung einer solchen Zugangssicherung bedarf es jedoch nicht, wenn die auf dem Magnetstreifen einer Zahlungskarte gespeicherten Daten lediglich ausgelesen werden. Dies ist ohne Weiteres mittels eines handelsüblichen Lesegeräts und der ebenfalls im Handel erhältlichen Software möglich. Dass sich der Angeklagte und seine Mittäter mittels des an den jeweiligen Geldautomaten angebrachten Lesegeräts den Zugang auch zu jenen Daten verschafft haben, die in Verbindung mit der über eine Tastatur gesondert einzugebenden persönlichen Geheimzahl (PIN) vor der unbefugten Verwendung einer Zahlungskarte schützen sollen, führt entgegen der Auffassung des Generalbundesanwalts zu keinem anderen Ergebnis. Zwar erfolgt die Autorisierung bei der Verwendung einer Zahlungskarte mit Garantiefunktion ausschließlich über die Eingabe der PIN (vgl. Gößmann in Schimansky/Bunte/Lwowski Bankrechts-Handbuch § 54 Rdn. 14 b). Diese wird aber nicht durch Lesen der Daten aus dem Magnetstreifen ermittelt, sondern mit dem Triple-DES-Algorithmus, einem 128-Bit-Schlüssel, aus der auf dem Magnetstreifen gespeicherten Konto-Nummer, der Kartenfolge-Nummer und der jeweiligen Bankleitzahl des Karten ausgebenden Instituts - nunmehr ausschließlich online (vgl. Gößmann aaO) - errechnet und mit der vom Benutzer des Geldautomaten eingegebenen PIN verglichen (vgl. BGH, Urt. vom 5. Oktober 2004 - XI ZR 210/03, BGHZ 160, 308, 311; Gößmann aaO; Koch/Vogel in Langenbucher/Gößmann/Werner Zahlungsverkehr § 5 Rdn. 10). Die Sicherung der der Berechnung der PIN zu Grunde liegenden Daten mittels eines kryptografischen Schlüssels (vgl. Koch/Vogel aaO) schützt die auf dem Magnetstreifen einer Zahlungskarte gespeicherten Daten zwar vor unbefugter Verwendung der Daten, nicht aber vor dem unberechtigten Zugang zu diesen Daten durch Auslesen mittels eines Lesegeräts. 6

Es kann dahinstehen, ob auf den Magnetstreifen der von dem Angeklagten und seinen Mittätern ausgelesenen Magnetstreifen Daten auch in verschlüsselter Form gespeichert waren. Eine Verschlüsselung von Daten schützt nur vor der Erfassung des Bedeutungsgehalts (kryptierter) Daten (vgl. MünchKomm StGB/Graf § 202 a Rdn. 40 zu § 202 a StGB a.F.), nicht aber vor dem bloßen Auslesen und Abspeichern der verschlüsselten Daten auf einem Datenträger des Täters und erfüllt demgemäß nicht den Tatbestand des § 202 a StGB n.F., weil es hierzu nicht der Überwindung einer Zugangssicherung bedarf (vgl. Gröseling/Höfinger MMR 2007, 549, 551). 7

3. Der Senat sieht sich durch das Urteil des 3. Strafsenats vom 10. Mai 2005 - 3 StR 425/04 (NStZ 2005, 566) gehindert, wie beabsichtigt zu entscheiden. In jener Entscheidung hat der 3. Strafsenat - ohne nähere Begründung - bei identischem Sachverhalt die Verurteilung wegen Ausspähens von Daten (§ 202 a StGB a.F.) durch das Landgericht nicht beanstandet. Der Senat fragt daher gemäß § 132 Abs. 3 Satz 1 GVG bei dem 3. Strafsenat an, ob an der genannten Rechtsauffassung festgehalten wird. 8

Vorsorglich fragt der Senat auch bei dem 1., 2. und 5. Strafsenat an, ob dortige Rechtsprechung der beabsichtigten Entscheidung entgegensteht. 9

[**Redaktioneller Hinweis:** Dem anfragenden Senat zustimmend bereits Tyszkiewicz HRRS 2010, 207 ff.]