HRRS-Nummer: HRRS 2010 Nr. 742
Bearbeiter: Karsten Gaede
Zitiervorschlag: BGH HRRS 2010 Nr. 742, Rn. X

BGH 4 StR 555/09 - Beschluss vom 6. Juli 2010 (LG Münster)

Skimming kein Ausspähen von Daten; gewerbs- und bandenmäßige Fälschung von Zahlungskarten mit Garantiefunktion; gewerbs- und bandenmäßiger Computerbetrug; redaktioneller Hinweis.

§ 202a StGB; § 152a StGB; § 263a StGB

Leitsätze des Bearbeiters

1. Das bloße Auslesen der auf dem Magnetstreifen einer Zahlungskarte mit Garantiefunktion gespeicherten Daten, um mit diesen Daten Kartendubletten herzustellen (sog. Skimming), erfüllt nicht den Tatbestand des § 202a Abs. 1 StGB. Soweit beim Auslesen die zur Berechnung der PIN verschlüsselt gespeicherten Daten in verschlüsselter Form erlangt werden, wird die in der Verschlüsselung liegende Zugangssicherung nicht überwunden.

2. Die Strafvorschrift des § 202a Abs. 1 StGB setzt voraus, dass die Angriffshandlung des Täters sich auf solche Daten im Sinne des § 202a Abs. 2 StGB bezieht, die nicht für den Täter bestimmt und gegen unberechtigten Zugang besonders gesichert sind. Bereits nach der alten Fassung der Norm war darüber hinaus erforderlich, dass bei dem damals tatbestandsmäßigen Verschaffen der Daten die besondere Zugangssicherung überwunden wird. Hieran anknüpfend verlangt § 202a Abs. 1 StGB n.F. nunmehr ausdrücklich, dass der Täter sich oder einem anderen den Zugang zu Daten unter Überwindung der Zugangssicherung verschafft.

3. Dass Daten magnetisch und damit nicht unmittelbar wahrnehmbar gespeichert sind, stellt keine besondere Sicherung gegen unberechtigten Zugang dar. Vielmehr handelt es sich gemäß § 202a Abs. 2 StGB nur bei Daten, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert oder übermittelt werden, um Daten im Sinne des ersten Absatzes dieser Vorschrift. Erforderlich ist, dass der Verfügungsberechtigte - hier das Unternehmen, das die Zahlungskarte mit Garantiefunktion ausgegeben hat Vorkehrungen getroffen hat, um den Zugriff auf die auf dem Magnetstreifen der Zahlungskarte gespeicherten Daten auszuschließen oder wenigstens nicht unerheblich zu erschweren. Eine Schutzvorkehrung ist jedoch nur dann eine Zugangssicherung im Sinne des § 202a Abs. 1 StGB, wenn sie jeden Täter zu einer Zugangsart zwingt, die der Verfügungsberechtigte erkennbar verhindern wollte.

4. Der Umstand, dass sich der Angeklagte und seine Mittäter mittels des an den jeweiligen Geldautomaten angebrachten Lesegeräts den Zugriff auch auf jene Daten verschafften, die in Verbindung mit der über eine Tastatur gesondert einzugebenden PIN vor der unbefugten Verwendung einer Zahlungskarte schützen sollen, führt zu keinem anderen Ergebnis.

Entscheidungstenor

1. Auf die Revision des Angeklagten wird das Urteil des Landgerichts Münster vom 24. Juli 2009 im Schuldspruch dahin geändert, dass in den Fällen II. 1 bis 3 der Urteilsgründe jeweils die tateinheitliche Verurteilung wegen Ausspähens von Daten entfällt.

2. Die weiter gehende Revision wird verworfen.

3. Der Angeklagte trägt die Kosten seines Rechtsmittels.

Gründe

Das Landgericht hat den Angeklagten wegen gewerbs- und bandenmäßiger Fälschung von Zahlungskarten mit Garantiefunktion in Tateinheit mit gewerbs- und bandenmäßigen Computerbetrug und mit Ausspähen von Daten in drei 1

Fällen, wegen versuchter gewerbsmäßiger Fälschung von Zahlungskarten mit Garantiefunktion in fünf Fällen, davon in einem Fall auch bandenmäßig handelnd, und wegen gewerbsmäßiger Fälschung von Zahlungskarten mit Garantiefunktion in Tateinheit mit gewerbsmäßigem Computerbetrug zu der Gesamtfreiheitsstrafe von sieben Jahren und sechs Monaten verurteilt. Hiergegen richtet sich die auf eine Verfahrensbeanstandung und die Sachrüge gestützte Revision des Angeklagten. Das Rechtsmittel führt zu der aus der Entscheidungsformel ersichtlichen Änderung des Schuldspruchs; im Übrigen ist es unbegründet im Sinne des § 349 Abs. 2 StPO.

1. Nach den Feststellungen zu den Fällen II. 1 bis 3 der Urteilsgründe schlossen sich der Angeklagte und die gesondert Verfolgten V., N., C. und P. 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 Kartelesegerät 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 persönliche Geheimzahl (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 Münster 21 Datensätze von Zahlungskarten und die jeweils zugehörige PIN, am 24. Februar 2007 durch Anbringen der Geräte an einem Geldautomaten in einer Bank in Dinslaken 21 Datensätze und am 7. Juli 2007 in Osnabrück weitere 35 Datensätze von Zahlungskarten. Nach dem Entfernen der Aufsatzgeräte von dem Geldautomaten las der Angeklagte allein oder mit Hilfe eines Mittäters jeweils die Speichermedien der Geräte aus. Die Datensätze der echten Zahlungskarten wurden anschließend in Amsterdam auf die Magnetstreifen von Payback-Karten übertragen, welche Bandenmitglieder zuvor beschafft hatten. In der Folgezeit hoben Mitglieder der Bande unter Verwendung der nachgemachten Karten und der zu diesen Datensätzen jeweils gehörenden PIN an Geldautomaten im Ausland Bargeld ab. 2

2. Die Verurteilung wegen tateinheitlich begangenen Ausspähens von Daten hält einer rechtlichen Prüfung nicht stand. Das bloße Auslesen der auf dem Magnetstreifen einer Zahlungskarte mit Garantiefunktion gespeicherten Daten, um mit diesen Daten Kartendubletten herzustellen, erfüllt nicht den Tatbestand des § 202 a Abs. 1 StGB. 3

a) Die Strafvorschrift des § 202 a Abs. 1 StGB sowohl in ihrer zur Tatzeit geltenden, als auch in der durch das 41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität vom 7. August 2007 (BGBl. I 1786) neu gestalteten Fassung setzt voraus, dass die Angriffshandlung des Täters sich auf solche Daten im Sinne des § 202 a Abs. 2 StGB bezieht, die nicht für den Täter bestimmt und gegen unberechtigten Zugang besonders gesichert sind. Bereits nach der alten Fassung der Norm war darüber hinaus erforderlich, dass bei dem damals tatbestandsmäßigen Verschaffen der Daten die besondere Zugangssicherung überwunden wird (vgl. MünchKomm StGB/Graf § 202 a Rdn. 48; Hoyer in SK-StGB 7. Aufl. § 202 a Rdn. 12; Lenckner in Schönke/ Schröder, StGB 27. Aufl. § 202 a Rdn. 10). Hieran anknüpfend (vgl. BT-Drucks. 16/3656 S. 10) verlangt § 202 a Abs. 1 StGB n.F. nunmehr ausdrücklich, dass der Täter sich oder einem anderen den Zugang zu Daten unter Überwindung der Zugangssicherung verschafft. 4

Diese Strafbarkeitsvoraussetzungen werden beim Auslesen der auf dem Magnetstreifen einer Zahlungskarte gespeicherten Daten mittels eines am Einzugslesegerät eines Geldautomaten angebrachten weiteren Lesegeräts (sog. Skimming), um mit den erlangten Daten in der ursprünglichen Form den Magnetstreifen einer Kartendublette zu beschreiben, nicht erfüllt (Senatsbeschluss vom 14. Januar 2010 - 4 StR 93/09; NStZ 2010, 275). Bei den unverschlüsselt auf dem Magnetstreifen gespeicherten Daten fehlt es bereits an einer besonderen Sicherung gegen unberechtigten Zugang, sodass diese Taten als taugliches 5 Tatobjekt im Sinne des § 202 a Abs. 1 StGB ausscheiden. Soweit beim Auslesen die zur Berechnung der PIN verschlüsselt gespeicherten Daten in verschlüsselter Form erlangt werden, wird die in der Verschlüsselung liegende Zugangssicherung nicht überwunden. 5

aa) 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 nur bei Daten, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert oder übermittelt werden, um Daten im Sinne des ersten Absatzes dieser Vorschrift. Demgemäß schützt § 202 a Abs. 1 StGB nur diejenigen nicht unmittelbar wahrnehmbar gespeicherten Daten im Sinne des § 202 a Abs. 2 StGB, 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, um den Zugriff auf die auf dem Magnetstreifen der Zahlungskarte gespeicherten Daten auszuschließen oder wenigstens nicht unerheblich zu erschweren (vgl. BTDrucks. 16/3656 aaO; Fischer StGB 57. Aufl. § 202 a Rdn. 8 6

jeweils m.w.N.). Eine Schutzvorkehrung ist jedoch nur dann eine Zugangssicherung im Sinne des § 202 a Abs. 1 StGB, wenn sie jeden Täter zu einer Zugangsart zwingt, die der Verfügungsberechtigte erkennbar verhindern wollte (BTDrucks. 16/3656 aaO; Fischer aaO Rdn. 9).

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. 7

bb) Der Umstand, dass sich der Angeklagte und seine Mittäter mittels des an den jeweiligen Geldautomaten angebrachten Lesegeräts den Zugriff auch auf jene Daten verschafften, die in Verbindung mit der über eine Tastatur gesondert einzugebenden PIN vor der unbefugten Verwendung einer Zahlungskarte schützen sollen, führt entgegen der Auffassung des Generalbundesanwalts zu keinem anderen Ergebnis. Die Autorisierung bei der Verwendung einer Zahlungskarte mit Garantiefunktion erfolgt ausschließlich über die Eingabe der PIN (vgl. Gößmann in Schimansky/Bunte/Lwowski Bankrechts-Handbuch § 54 Rdn. 14 b). Diese wird 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 Kontonummer, der Kartenfolgenummer 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). 8

Die für die Berechnung der PIN erforderlichen Daten sichern die auf dem Magnetstreifen einer Zahlungskarte gespeicherten Daten aber lediglich vor unbefugter Verwendung der Daten beim Benutzen der Karte, nicht jedoch vor dem unberechtigten Zugang zu den Daten durch Auslesen mit einem Lesegerät. 9

cc) Die Sicherung der der Berechnung der PIN zugrunde liegenden Daten durch Verschlüsselung mittels kryptografischer Schlüssel (Koch/Vogel aaO) stellt zwar nach wohl herrschender Meinung (vgl. Fischer aaO Rdn. 9 a) eine besondere Zugangssicherung dar, die aber ausschließlich vor der Erfassung des Bedeutungsgehalts der Daten schützt (MünchKomm StGB/Graf aaO Rdn. 40). Beim bloßen Auslesen und Abspeichern der verschlüsselten Daten auf einen Datenträger des Täters bleibt die Verschlüsselung indes unangetastet, sodass mangels Überwindung der Zugangssicherung der Tatbestand des § 202 a Abs. 1 StGB nicht erfüllt ist (vgl. MünchKomm StGB/Graf aaO Rdn. 46; Bosch in Satzger/Schmitt/Widmaier StGB § 202 a Rdn. 6; Gröseling/Höfinger MMR 2007, 549, 551). Gleiches gilt für sonstige möglicherweise in verschlüsselter Form auf dem Magnetstreifen einer Zahlungskarte gespeicherte Daten. 10

b) Auf Anfragebeschluss des Senats hat der 3. Strafsenat seine entgegenstehende, dem Urteil vom 10. Mai 2005 - 3 StR 425/04 (NStZ 2005, 566) zu Grunde liegende Rechtsprechung aufgegeben. Der 2. Strafsenat ist der hier vertretenen Rechtsansicht beigetreten, der 1. und 5. Strafsenat haben mitgeteilt, an möglicherweise entgegenstehender Rechtsprechung nicht festzuhalten. 11

3. Der Wegfall der tateinheitlichen Verurteilungen wegen Ausspähens von Daten in den Fällen II. 1 bis 3 der Urteilsgründe lässt den Strafausspruch unberührt. Der Senat kann ausschließen, dass der Tatrichter auf der Grundlage einer zutreffenden rechtlichen Bewertung auf mildere Einzelstrafen erkannt hätte. 12

Die Strafkammer, die die Einzelstrafen jeweils dem - Freiheitsstrafe nicht unter zwei Jahre vorsehenden - Regelstrafrahmen des § 152 b Abs. 2 StGB entnommen hat, hat die jeweiligen Verurteilungen wegen Ausspähens von Daten - anders als die tateinheitliche Verwirklichung des Verbrechenstatbestandes des § 263 a Abs. 2 StGB i.V.m. § 263 Abs. 5 StGB - weder bei der Prüfung des Vorliegens eines minder schweren Falles nach § 152 b Abs. 3 StGB im Zuge der Strafrahmenwahl, noch bei der Strafzumessung im engeren Sinne zum Nachteil des Angeklagten berücksichtigt. 13

4. Der nur geringfügige Teilerfolg der Revision rechtfertigt es nicht, den Angeklagten nach § 473 Abs. 4 StPO teilweise von den durch das Rechtsmittel entstandenen Kosten und Auslagen frei zu stellen. 14

[Redaktioneller Hinweis: Vgl. so auch bereits Tyszkiewicz HRRS 2010, 207 ff.] 15