

 **SCHUMACHER**
PARAGRAFENSCHNACK

Examenswissen aus dem Herzen von Münster

Entscheidung im Strafrecht,
30.9.2026

Worum geht es? Abgrenzung Betrug – Computerbetrug, § 263 / § 263a StGB | Selbstbedienungsläden und Vermögensdelikte | Digitalisierung des Zahlungsverkehrs | Täuschungsäquivalent, § 263a StGB | „unbefugt“, § 263a StGB | Zahlungskarten-Fälle: Tap&Go... & Knast?

Hinweis vom HLB-Team:

Klausuren im Bereich der Vermögensdelikte gehören im strafrechtlichen Examen zu den absoluten Klassikern. Aufgrund der Vielzahl an möglichen Konstellationen sowie der dogmatisch bedeutsamen Unterscheidung von Selbst- und Fremdschädigungsdelikten, gelten sie zuweilen als „kompliziert“ und „undurchsichtig“. Die Digitalisierung und Autonomisierung des alltäglichen Zahlungsverkehrs (Tap&Go; NFC-Pay u. w.) spielt dabei den Prüfungsämtern in die Karten: Selbstbedienungsläden etwa, gleich in welcher Form, ob Tankstelle, Tabakladen, Super- oder Getränkemarkt, sind immer häufiger „Tatort“ im strafrechtlichen Klausursachverhalt. Doch ihr werdet sehen: Nur weil „Computer“ drauf steht, es aussieht wie ein Computer und es piepst wie ein Computer, ist nicht gleich auf § 263a StGB zu rekurrieren.

*Dies zeigt auch ein aktueller Fall des Bundesgerichtshofs (BGH, Beschl. v. 28.01.2026 – 4 StR 672/25, BeckRS 2026, 8088). Der Täter hatte dem Geschädigten zunächst eine Kreditkarte abgenötigt. Diese nutzte er im Folgegeschehen sowohl in einer Tankstelle als auch in einem Tabakgeschäft und kaufte dort Waren zum Preis zwischen 10 und 50 EUR **per kontaktloser Bezahlung ohne Eingabe der PIN**. Das Konto des Geschädigten wurde im Gesamtwert der Waren belastet. Das Landgericht (LG) Essen hatte A unter anderem wegen Computerbetrugs in zwei Fällen verurteilt. Andere Ansicht: BGH. Der Fall eignet sich für Ausbildungszwecke besonders gut, da er die Unterschiede zwischen einzelnen (Vermögens-)Delikten (§§ 263 f. StGB) eingängig darstellt, den Blick über den Horizont ermöglicht (§§ 261, 274, 303a StGB) und Anlass gibt, sich die materiellen Besonderheiten der einschlägigen Tatbestände in Erinnerung zu rufen. Die kompakte Wiederholung und Systematisierung typischer Klausurkonstellationen gibt im Examen die nötige Sicherheit. Zahlungskarten stellen ein Schnittstellenproblem dar, sollten Prüflingen aber keineswegs Sorgen bereiten.*

Die Hintergründe der Entscheidung

Der Entscheidung des Bundesgerichtshofs (BGH) vom 28. Januar 2026¹ ging ein Urteil des Landgerichts (LG) Essen vom 30. Juli 2025 (56 KLS-75 Js 59/25-8/25) voraus. Das LG hatte A wegen besonders schwerer räuberischer Erpressung in Tateinheit mit gefährlicher Körperverletzung sowie wegen Computerbetruges in drei Fällen und Fahrens ohne Fahrerlaubnis in zwei Fällen zu einer Gesamtfreiheitsstrafe von acht Jahren verurteilt. Ferner ordnete es dessen Unterbringung in einer Entziehungsanstalt sowie eine Sperrfrist für die Erteilung einer Fahrerlaubnis an. Hiergegen wandte sich A mit seiner auf die allgemeine Sachrüge gestützten Revision (§ 337 StPO).

DEFINITION **BEGRÜNDETHEIT SACHRÜGE, § 337 StPO**

Mit der Sachrüge oder auch materiellen Rüge werden Fehler in der Anwendung des materiellen Rechts geltend gemacht. Hierzu zählen etwa Fehler bei der Anwendung der dem Urteil zugrunde gelegten Strafnorm oder bei der Strafzumessung (§ 46 StGB) sowie solche bei der Beweismwürdigung. Die Sachrüge ist begründet, wenn die Urteilsfeststellungen keine tragfähige Grundlage für die rechtliche Prüfung bieten oder soweit das (materielle) Recht auf den festgestellten Sachverhalt nicht oder nicht richtig angewendet worden ist (vgl. Schmitt/Köhler, 69. Aufl., § 337).

A zwang den O unter Einsatz von Gewalt, ihm seinen Pkw, einen 1967er Chevrolet Impala, zu überlassen; O wurde dabei verletzt. Im Handschuhfach lagen, wie A wusste, eine Kreditkarte und eine Debitkarte des O, beide ausgegeben von der B-Bank. A wollte auch die Karten behalten. Er fuhr mit dem Impala samt Karten davon, obwohl er keine Fahrerlaubnis besaß.

Am nächsten Morgen verabredete A mit seiner Bekannten M, mit den Karten des O für sich einzukaufen. Die Rollen waren so verteilt: M sollte die Karten an der Kasse einsetzen. A sollte sie mit dem Pkw des O zu den Geschäften fahren, dort im Wagen warten und danach mit ihr wegfahren. Die Waren wollten beide gemeinsam verbrauchen oder verwerten. Von vornherein planten sie, beide Karten einzusetzen. A übergab M die Karten. Die PINs kannten weder A noch M. Sie wollten nur kontaktlos zahlen, ohne eine PIN einzugeben.

¹ BGH, Beschl. v. 28.1.2026 – 4 StR 672/25, BeckRS 2026, 8088.

Zum technischen Hintergrund:

Beide Karten können kontaktlos eingesetzt werden. Dazu hält man die Karte an das Near Field Communication (NFC) fähige Kartenterminal. Bei Beträgen bis 50 Euro wird in der Regel keine PIN verlangt.

Vor der Freigabe prüft ein Computer der B-Bank nur, ob die Karte gesperrt ist und ob der Verfügungsrahmen des Karteninhabers eingehalten ist. Ob die Person, die die Karte vorhält, sie nutzen darf, wird nicht geprüft.

Mit der Freigabe hat der Händler gegen die B-Bank einen Anspruch auf den Kaufpreis. Das gilt auch, wenn ein Unberechtigter die Karte eingesetzt hat.

Bei jedem Einsatz werden Daten auf dem Chip der Karte automatisch aktualisiert, unter anderem zum verbleibenden Verfügungsrahmen und zu den bisherigen Kartennutzungen.

Gegen 9:00 Uhr fuhr A die M zu einer Tankstelle des T1 an der Autobahn zwischen Münster Süd und Nord und wartete im Wagen. Im Verkaufsraum kaufte M Waren für 34 Euro. Unmittelbar danach bezahlte sie in einem zweiten Vorgang weitere Waren für 10 Euro. Beide Male hielt sie wie verabredet die Kreditkarte des O an das Terminal. Beide Zahlungen wurden ohne PIN-Abfrage freigegeben. Der Kassierer K händigte M die Waren aus. Wie bei kontaktlosen Zahlungen üblich, dachte er nicht darüber nach, wem die Karte gehörte.

Gegen 11:00 Uhr erreichten A und M ein Tabakgeschäft des T2 in der Münsteraner Innenstadt. A wartete wieder im Wagen. M bezahlte dort in zwei unmittelbar aufeinanderfolgenden Vorgängen je Zigaretten für 50 Euro, wieder kontaktlos und ohne PIN mit der Kreditkarte. Einen dritten Vorgang mit dieser Karte lehnte das Terminal ab. M nahm daraufhin, wie von Anfang an geplant, die Debitkarte. Mit ihr bezahlte sie kontaktlos und ohne PIN weitere Zigaretten für 40 Euro. Einen weiteren Vorgang mit der Debitkarte lehnte das Terminal ebenfalls ab. Auch das Personal des T2 dachte nicht über die Berechtigung der M nach und händigte ihr die bezahlten Zigaretten aus. Danach fuhren A und M davon.

Die Waren aus der Tankstelle verbrauchten A und M gemeinsam. Die Zigaretten tauschten sie noch am selben Tag bei einem Bekannten gegen Betäubungsmittel.

Das Konto des O wurde mit allen erfolgreichen Zahlungen belastet, insgesamt 184 Euro. T1 und T2 erhielten die Kaufpreise vollständig.

A wusste, dass er und M mit Karten bezahlten, die ihnen nicht zustanden, und dass die Einkäufe zulasten des O abgerechnet würden. Welche Vorstellungen A darüber hinaus von den technischen Abläufen hatte, lässt sich nicht aufklären. Das gilt insbesondere für die Fragen, ob er wusste, dass dabei Daten auf dem Chip verändert werden, und dass diese Daten für O oder die B-Bank Beweisbedeutung haben können.

Fallfrage: Wie hat sich A nach dem StGB strafbar gemacht?

Bearbeitervermerk:

1. Es ist davon auszugehen, dass A sich durch die Erlangung des Pkw und der Karten wegen besonders schwerer räuberischer Erpressung in Tateinheit mit gefährlicher Körperverletzung strafbar gemacht hat (§§ 253, 255, 250 Abs. 2, 223, 224, 52 StGB). Weitere Straftatbestände sind insoweit nicht zu prüfen.
2. Die Strafbarkeit der M ist nicht zu prüfen.
3. Nicht zu prüfen sind § 248b StGB sowie Strafvorschriften außerhalb des StGB.
4. Etwa erforderliche Strafanträge sind gestellt.

HINWEIS: STRAFBARKEIT NACH § 21 StVG

Unser Bearbeitervermerk schließt das Nebenstrafrecht aus; die Lebenswirklichkeit freilich nicht, daher folgender Hinweis: Der Täter hat dem Geschädigten ein Auto abgenötigt, mit dem er dann u. a. die Tankstelle sowie das Tabakgeschäft angesteuert hatte, obwohl er nicht im Besitz einer gültigen Fahrerlaubnis war. Der Senat führt hierzu aus, dass das Dauerdelikt des Fahrens ohne Fahrerlaubnis (§ 21 StVG), wenn es der Wegfahrt vom Tatort mit dem abgenötigten Pkw dient, mit der Erpressungstat bis zu deren Beendigung in **Tateinheit** steht. Es vermag als minderschwere Straftat aber **nicht** zeitlich und örtlich auseinanderfallende unberechtigte Karteneinsätze zu **verklammern**, da es sich insoweit um schwerere Straftaten handelt (Kudlich, JA 2026, 609).

Abwandlung (optional):

A hatte früher als Servicetechniker für Kartenterminals gearbeitet. Er wusste daher:

- dass bei jeder kontaktlosen Zahlung die Angaben auf dem Chip zum Verfügungsrahmen und zu den bisherigen Kartennutzungen überschrieben werden,
- dass Karteninhaber und Bank diese Angaben etwa im Streit über unberechtigte Abbuchungen als Nachweis heranziehen,
- und dass diese Nachweismöglichkeit durch jeden Karteneinsatz zwangsläufig beeinträchtigt wird.

All das hatte er M vor der Fahrt erklärt. Beiden war es gleichgültig; es kam ihnen nur auf die Waren an.

Wie hat sich A durch die Karteneinsätze strafbar gemacht?

Die Entscheidung

Erster Tatkomplex: Abnötigen des Pkw samt Zahlungskarten

A hat sich, indem er O unter Einsatz von Gewalt zwang, ihm seinen Pkw samt der im Handschuhfach befindlichen Kredit- und Debitkarte zu überlassen, und O dabei verletzte, wegen besonders schwerer räuberischer Erpressung in Tateinheit mit gefährlicher Körperverletzung gem. **§§ 253, 255, 250 Abs. 2, 223, 224, 52 StGB** strafbar gemacht.²

HINWEIS: VERHÄLTNIS ERSTER UND ZWEITER TATKOMPLEX

Der erste Tatkomplex ist kurz zu halten. Er wirkt aber im zweiten Tatkomplex fort:

Er ist die Vortat, aus der die Karten „herrühren“ (**§ 261 Abs. 1 StGB**).

Er begründet die Vortatbeteiligung des A (**§ 261 Abs. 7 StGB**).

Er erklärt, warum eine erneute Zueignung der Karten ausscheidet (unten G.).

² BGH, Beschl. v. 28.1.2026 – 4 StR 672/25, BeckRS 2026, 8088, Rn. 2 f.; Der BGH hat diesen Schuldspruch als solchen nicht aufgehoben, sondern lediglich die konkurrenzrechtliche Einordnung des zugleich verwirklichten Fahrens ohne Fahrerlaubnis (**§ 21 StVG**) korrigiert.

Zweiter Tatkomplex: „Tap & Go“ – Kontaktloses Bezahlen mit den Karten des O

A könnte sich durch die gemeinsam mit M veranlassten kontaktlosen Bezahlvorgänge in der Tankstelle des T1 und dem Tabakgeschäft des T2 strafbar gemacht haben.

HINWEIS: MITTÄTERSCHAFT NACH § 25 Abs. 2 StGB

Da M die Karten jeweils selbst an das Lesegerät hielt, A aber aufgrund des gemeinsamen Tatplans handelte, M zu den Geschäften chauffierte und beide die erlangten Waren anschließend gemeinsam verwendeten, sind die Karteneinsätze im Ausgangspunkt als **gemeinschaftliches Vorgehen** zu betrachten. Auch der BGH legt seiner Entscheidung ein einvernehmliches Vorgehen beider Täter zugrunde und behandelt M hinsichtlich der Karteneinsätze als Mittäterin gem. § 25 Abs. 2 StGB.¹

Für den **Aufbau Eures Gutachtens** folgt daraus: Die Zahlungsvorgänge sind gleich gelagert und werden zusammen geprüft. Besonderheiten (abgelehnte Vorgänge, Kartenwechsel) kommen dort zur Sprache, wo sie relevant werden. Die Karten hat M eingesetzt, nicht A. Für A kommt daher nur Mittäterschaft (§ 25 Abs. 2 StGB) in Betracht. Die Zurechnung ist erst zu prüfen, wenn das Handeln der M einen Tatbestand objektiv erfüllt. Vorher gibt es nichts zuzurechnen (unten D. I. 4.).

A. Computerbetrug, §§ 263a Abs. 1 Var. 3, 25 Abs. 2 StGB

A könnte sich wegen gemeinschaftlichen Computerbetruges gem. §§ 263a Abs. 1 Var. 3, 25 Abs. 2 StGB strafbar gemacht haben, indem M absprachegemäß die Kredit- und Debitkarte des O kontaktlos zur Bezahlung der Waren verwendete.

Hierfür müsste durch unbefugte Verwendung von Daten das Ergebnis eines Datenverarbeitungsvorgangs beeinflusst und dadurch das Vermögen eines anderen geschädigt worden sein.

1. Verwendung von Daten

Beim kontaktlosen Vorhalten der Kredit- bzw. Debitkarte werden die auf der Karte gespeicherten Zahlungsdaten in den elektronischen Zahlungsvorgang eingebracht, mithin Gegenstand einer Datenverarbeitung, und damit verwendet.

Problematisch ist jedoch, ob diese Verwendung auch **unbefugt** i. S. d. § 263a Abs. 1 Var. 3 StGB erfolgte.

2. Unbefugte Verwendung

Fraglich ist, ob die Verwendung unbefugt war. Wie das Merkmal auszulegen ist, ist umstritten.

STREIT: **UNBEFUGTE VERWENDUNG § 263a Abs. 1 Var. 3 StGB**

- a) Nach der **subjektiven Auslegung** ist jede Verwendung unbefugt, die dem wirklichen oder mutmaßlichen Willen des Verfügungsberechtigten widerspricht. Die B-Bank gestattet den Einsatz nur dem Karteninhaber, und O war nicht einverstanden. Danach wäre die Verwendung unbefugt.
- b) Nach der **computerspezifischen Auslegung** ist die Verwendung nur unbefugt, wenn sich der entgegenstehende Wille in der Programmgestaltung niedergeschlagen hat, etwa in einer Zugangssperre. Das System prüfte nur Sperrstatus und Verfügungsrahmen, und beides war in Ordnung. Eine programmierte Berechtigungsprüfung hat M weder umgangen noch überlistet. Danach wäre die Verwendung nicht unbefugt.
- c) Nach der **betrugsspezifischen Auslegung** (st. Rspr., h.L.) ist die Verwendung nur unbefugt, wenn sie eine Täuschung i.S.d. **§ 263 Abs. 1 StGB** darstellt. Maßgeblich ist danach, ob die konkrete Verwendung der Daten bei einer gedachten Ersetzung des Datenverarbeitungsvorgangs durch einen Menschen der an Stelle des Computers dieselben Prüfungen vornähme (fiktiver Bankangestellter), einen Betrug darstellen würde. Ihm gegenüber müsste das Verhalten eine zumindest konkludente Täuschung darstellen (**Täuschungsäquivalent**).

Welchen Erklärungswert ein Verhalten hat, richtet sich nach dem Empfängerhorizont und dem normativen Gesamtzusammenhang.

Hier ist entscheidend: Das kartenausgebende Institut verzichtet bewusst auf die starke Kundenauthentifizierung nach **§ 55 ZAG** und nimmt damit Missbrauch in Kauf. Dann kann es dem Zahlungsvorgang nicht zugleich den Erklärungswert beimessen, dass es auf die Identität des Verwenders ankomme. Der fiktive Bankangestellte würde dem bloßen Vorhalten der Karte also keine Erklärung entnehmen, der Verwender sei berechtigt.

Bei der PIN ist das anders. Weil der Karteninhaber die Geheimzahl vertraglich nicht weitergeben darf, ist allein er zur Autorisierung befugt. **Wer die PIN eingibt, erklärt daher seine Berechtigung.** Die PIN-lose Zahlung bringt dagegen keine Legitimationsinformation in den Vorgang ein (BGH 4 StR 672/25, Rn. 8; so bereits BGH 5 StR 362/25, Rn. 12). Nach dieser Ansicht fehlt es am Täuschungsäquivalent.

d) **Stellungnahme**

Die Ansichten kommen zu unterschiedlichen Ergebnissen; der Streit ist zu entscheiden.

Gegen die subjektive Auslegung: Sie dehnt den Tatbestand uferlos aus, weil jede vertragswidrige Nutzung eines Datenverarbeitungssystems Computerbetrug wäre. Außerdem unterläuft sie **§ 266b StGB**. Dieser erfasst den berechtigten Karteninhaber, der seinen Rahmen missbraucht, mit einem milderen Strafraum (bis drei statt bis fünf Jahre).

Gegen die computerspezifische Auslegung: Sie ist zu eng. **Var. 3** wurde gerade eingefügt, um den Missbrauch von Geldautomatenkarten zu erfassen. Gibt der Täter dort die richtige PIN ein, führt das Programm den Vorgang „ordnungsgemäß“ aus. Ein entgegenstehender Wille hat sich im Programm also gerade nicht niedergeschlagen.

Für die betrugsspezifische Auslegung: **§ 263a StGB** soll die Lücke schließen, die entsteht, weil ein Computer nicht getäuscht werden kann. Strafwürdig ist daher nur, was gegenüber einem Menschen Betrug wäre (Systematik zu und Struktur- und Wertgleichheit mit **§ 263 StGB**). Es ist der hM zu folgen: Durch das bloße Vorhalten der Karte des O bei T1 und T2 an das jeweilige Kartenlesegerät wird keine – auch keine konkludente – Erklärung darüber abgegeben, dass der Verwender zur Benutzung der Karte berechtigt ist. Gleiches gilt für den späteren Einsatz der Debitkarte. Anders als bei einem Zahlungsvorgang unter Eingabe der persönlichen Geheimzahl wird gerade keine Legitimationsinformation in den Zahlungsvorgang eingebracht.³ Eine PIN wurde aber bei keinem erfolgreichen Zahlungsvorgang abgefragt oder eingegeben. Damit enthielten die Karteneinsätze keine Erklärung über die Berechtigung der M beziehungsweise des A zur Verwendung der Karten.

Eine **unbefugte Verwendung von Daten** i. S. d. **§ 263a Abs. 1 Var. 3 StGB** liegt nach der betrugsspezifischen Auslegung des BGH daher nicht vor.

3. § 263a Abs. 1 Var. 4 StGB Auch eine „sonst unbefugte Einwirkung auf den Ablauf“ scheidet aus. Diese Auffangvariante ist ihrerseits betrugsspezifisch auszulegen. Zudem hat M nicht auf den Ablauf eingewirkt, sondern das System bestimmungsgemäß genutzt.

4. A hat sich durch die kontaktlosen Bezahlvorgänge **nicht wegen Computerbetruges** gem. **§§ 263a Abs. 1 Var. 3, 25 Abs. 2 StGB** strafbar gemacht.

³ BGH, Beschl. v. 28.1.2026 – 4 StR 672/25, BeckRS 2026, 8088, Rn. 8.

B. Betrug, §§ 263 Abs. 1, 25 Abs. 2 StGB

A könnte sich durch die Kartenzahlungen jedoch wegen gemeinschaftlichen Betruges gem. **§§ 263 Abs. 1, 25 Abs. 2 StGB** zulasten der jeweiligen Händler T1 und T2 strafbar gemacht haben.

Dafür müsste ein Mitarbeiter des jeweiligen Händlers durch Täuschung einem Irrtum unterlegen sein und aufgrund dieses Irrtums eine Vermögensverfügung vorgenommen haben, die unmittelbar zu einem Vermögensschaden geführt hat.

1. Täuschung

In Betracht kommt nur eine konkludente Täuschung über die Berechtigung zur Kartennutzung. Mit der Autorisierung erhält der Händler eine einredefreie Forderung gegen das kartenausgebende Institut (abstraktes Schuldversprechen, **§ 780 BGB**). Die Karte wirkt insoweit **wie Bargeld**: Der Händler steht so, als hätte er bar kassiert, und fragt deshalb so wenig nach der Berechtigung des Kunden wie beim Barkauf nach dem Eigentum am Geld, das er wegen **§ 935 Abs. 2 BGB** ohnehin erwirbt. Im Vorhalten der Karte liegt daher keine Erklärung über die Berechtigung. Eine Täuschung liegt nicht vor.⁴

2. Irrtum

Zudem dachten K und das Personal des T2 nicht über die Berechtigung der M nach. Bloße Unkenntnis ist keine Fehlvorstellung. Für ein „sachgedankliches Mitbewusstsein“ fehlt jeder Anlass, weil die Berechtigung für den Händler wegen der Zahlungsgarantie bedeutungslos ist. Der BGH verneint deshalb sowohl die Täuschung als auch einen entsprechenden Irrtum.

3. Vermögensschaden

Jedenfalls fehlt ein Schaden. Die erfolgreichen Zahlungsvorgänge wurden abgewickelt, den abgegebenen Waren steht ein vollwertiger Zahlungsanspruch gegen die B-Bank gegenüber, und

⁴ Täuschung und Irrtum wegen des fehlenden Schadens offenzulassen („Ob bereits im Vorhalten der fremden Karte eine Täuschung über die Berechtigung zur Kartennutzung zu sehen und ein entsprechender Irrtum des Kassenpersonals anzunehmen ist, kann dahinstehen. Jedenfalls müsste den jeweiligen Händlern ein Vermögensschaden entstanden sein.“), ist methodisch zulässig. Es verschenkt hier aber die Pointe: Der BGH verneint schon die Täuschung, und zwar mit dem eingängigen Vergleich zum Bargeld.

T1 und T2 haben die Kaufpreise erhalten. Bereits deshalb scheidet ein Betrug zulasten des jeweiligen Händlers aus.⁵

4. Ergebnis

A hat sich folglich **nicht wegen Betruges gem. §§ 263 Abs. 1, 25 Abs. 2 StGB** zulasten von T1 oder T2 strafbar gemacht.⁶

HINWEIS: DREIECKSBETRUG ZULASTEN DER B-BANK ODER DES O, § 263 Abs. 1 StGB

Geometrieliebhaber sehen u. U. ein Dreiecksverhältnis. Ein Dreiecksbetrug scheidet jedoch aus. Die Kontobelastung beruht nicht auf einer Verfügung des Kassenpersonals, sondern auf der automatisierten Freigabe durch den Bankcomputer. Wo ein Computer „verfügt“, ist allein **§ 263a StGB** einschlägig.

C. (Selbst-)Geldwäsche, § 261 Abs. 7 StGB

A könnte sich durch die Verwendung der zuvor erbeuteten Karten und die anschließende Verwertung der damit erworbenen Waren wegen Geldwäsche gem. **§ 261 Abs. 7 StGB** strafbar gemacht haben.

A war selbst an der Vortat beteiligt, aus welcher die Karten stammten. Die spätere Verwendung der Karten diene allein dazu, die erlangte Beute zum eigenen Vorteil einzusetzen.

Nach Auffassung des BGH verwirklicht die **bloße eigennützige Verwertung eines aus der eigenen Vortat erlangten Gegenstandes** jedoch noch kein gegenüber der Vortat eigenständiges Geldwäscheunrecht. Erforderlich wäre vielmehr eine darüber hinausgehende verschleiende Umgehung insbesondere solcher Mechanismen, die dem Schutz der Integrität des Wirtschafts- und Finanzkreislaufs dienen. Eine solche zusätzliche Verschleierungshandlung liegt hier nicht vor.⁷

A hat sich somit **nicht wegen (Selbst-)Geldwäsche gem. § 261 Abs. 7 StGB** strafbar gemacht.⁸

D. Urkundenunterdrückung, § 274 Abs. 1 Nr. 2 StGB

⁵ BGH, Beschl. v. 28.1.2026 – 4 StR 672/25, BeckRS 2026, 8088, Rn. 10.

⁶ BGH, Beschl. v. 28.1.2026 – 4 StR 672/25, BeckRS 2026, 8088, Rn. 10.

⁷ BGH, Beschl. v. 28.1.2026 – 4 StR 672/25, BeckRS 2026, 8088, Rn. 10.

⁸ BGH, Beschl. v. 28.1.2026 – 4 StR 672/25, BeckRS 2026, 8088, Rn. 10.

A könnte sich durch die Verwendung der Karten jedoch wegen Urkundenunterdrückung gem. **§ 274 Abs. 1 Nr. 2 StGB** strafbar gemacht haben.

1. Objektiver Tatbestand

a. Verändern beweiserheblicher Daten

§ 274 Abs. 1 Nr. 2 StGB schützt beweiserhebliche Daten, über die der Täter nicht oder nicht ausschließlich verfügen darf.

DEFINITION **Beweiserhebliche Daten, § 274, 202a StGB**

Daten i.S.d. **§ 202a Abs. 2 StGB** sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert oder übermittelt werden. **Achtung:** Der Gesetzgeber hat den Datenbegriff ausdrücklich nicht näher definiert. Die Legaldefinition (**§ 202a Abs. 2 StGB**) dient nur der Einschränkung des dort (!) vorausgesetzten allgemeinen Datenbegriffs.

Beweiserheblich sind Daten, wenn sie dazu bestimmt und geeignet sind, im Rechtsverkehr Beweis für rechtlich erhebliche Tatsachen zu erbringen. Wären sie sichtbar, müssten sie also eine Urkunde darstellen (Datenurkunde, vgl. **§ 269 StGB**).

Auf dem Chip der Kredit- bzw. Debitkarte befinden sich unter anderem gespeicherte Daten über den noch bestehenden Verfügungsrahmen sowie die Umstände bisheriger Kartennutzungen. Ausstellerin ist die B-Bank. Diese Daten können eine urkundengleiche Beweisfunktion besitzen, etwa im Streit zwischen Bank und Karteninhaber über unberechtigte Belastungen. Jeder unbefugte Karteneinsatz hat die Angaben zum Verfügungsrahmen und zu den Nutzungen aktualisiert und damit **verändert**. Eine Verwirklichung des objektiven Tatbestands des **§ 274 Abs. 1 Nr. 2 StGB** kommt daher grundsätzlich in Betracht.⁹

b. Zurechnung, § 25 Abs. 2 StGB

Die Tathandlungen hat M vorgenommen. Sie sind A zuzurechnen, wenn beide nach einem gemeinsamen Tatplan arbeitsteilig handelten und A einen Beitrag in Täterqualität leistete.

aa) Gemeinsamer Tatplan:

A und M verabredeten, beide Karten zur Bezahlung einzusetzen, und verteilten die Rollen. Ob

⁹ BGH, Beschl. v. 28.1.2026 – 4 StR 672/25, BeckRS 2026, 8088, Rn. 11; nach dem BGH liegt ein Unterdrücken bereits darin, dass dem Berechtigten durch die Wegnahme der Karte der Zugriff auf die inkorporierten Daten zumindest vorübergehend genommen wird. Dieser Entzug fällt hier in Tatkomplex 1, der nach dem Bearbeitervermerk nicht zu prüfen ist. Für Tatkomplex 2 kommt es auf das Verändern an.

A die datenbezogene Bedeutung des Geschehens erfasste, ist eine Frage des Vorsatzes (s. „2.“).

bb) Täterschaftlicher Tatbeitrag (Wiederholung):

Die Abgrenzung von Mittäterschaft und Beihilfe ist umstritten.

Die *Rspr.* nimmt eine **wertende Gesamtbetrachtung** vor. Anhaltspunkte sind das eigene Interesse am Taterfolg, der Umfang der Tatbeteiligung und die Tatherrschaft oder wenigstens der Wille dazu. A wollte die Waren mitverbrauchen, stellte die selbst erbeuteten Karten, organisierte die Fahrten und wartete fluchtbereit. Er ist danach Mittäter.

Die in der Literatur herrschende *Tatherrschaftslehre* verlangt **funktionelle Tatherrschaft**, also einen wesentlichen Beitrag im arbeitsteiligen Zusammenwirken. Ob ein Beitrag im Vorbereitungsstadium genügt, ist innerhalb dieser Lehre streitig. Darauf kommt es hier aber nicht an: A sicherte während der Ausführung die sofortige Abfahrt, und der ganze Plan beruhte auf den von ihm beschafften Karten. Auch danach ist er Mittäter.

Ein Streitentscheid ist entbehrlich. Der objektive Tatbestand ist erfüllt.

2. Subjektiver Tatbestand

A müsste jedoch auch den subjektiven Tatbestand verwirklicht haben, [§ 15 StGB](#).

Hierfür reicht es nicht aus, dass der Täter lediglich weiß, eine fremde Karte zum Bezahlen zu verwenden. Vielmehr muss der Kartenverwender **(1)** die technischen Vorgänge der kontaktlosen Kartenzahlung jedenfalls **in seiner Laiensphäre nachvollziehen**. Darüber hinaus muss er **(2)** die Vorstellung besitzen, dass der Karte beziehungsweise den durch ihren Einsatz betroffenen Daten eine **potenzielle Beweisbedeutung** zukommt. Schließlich muss er **(3)** erkennen, dass durch sein Handeln ein hierauf bezogenes Beweisführungsrecht des berechtigten Karteninhabers oder der Bank als notwendige Folge beeinträchtigt wird.¹⁰

HINWEIS: BGH ALS REVISIONSGERICHT

Der BGH hat als Revisionsgericht aufgehoben und zurückverwiesen, weil das LG zur subjektiven Tatseite nichts festgestellt hatte. Im Gutachten gibt es diese Möglichkeit nicht. Lässt sich laut Sachverhalt etwas „nicht aufklären“, ist die für den Täter günstigste Variante zugrunde zu legen (in dubio pro reo). Sätze wie „das Tatgericht wird weitere Feststellungen treffen müssen“ gehören nicht in eine Klausurlösung.

¹⁰ BGH, Beschl. v. 28.1.2026 – 4 StR 672/25, BeckRS 2026, 8088, Rn. 11.

A wusste nur, dass er mit fremden Karten zulasten des O bezahlte. Das genügt gerade nicht. Ob er darüber hinaus Vorstellungen von der Datenveränderung und ihrer Beweisbedeutung hatte, lässt sich nicht aufklären. Nach dem Grundsatz **in dubio pro reo** ist zu seinen Gunsten davon auszugehen, dass er sie nicht hatte. Es fehlen Vorsatz und Nachteilszufügungsabsicht. Mangels Tatentschlusses scheidet auch ein Versuch (§ 274 Abs. 2 StGB) aus.¹¹

3. Ergebnis

A hat sich im Ursprungssachverhalt nicht wegen **Urkundenunterdrückung** gem. § 274 Abs. 1 Nr. 2 StGB strafbar gemacht.¹²

Ein anderes Bild ergibt sich mit Blick auf die **Fallabwandlung**: Hier wusste A, dass die Chipdaten bei jedem Einsatz überschrieben werden und als Nachweis dienen. Er wusste auch, dass die Beweismöglichkeit zwangsläufig beeinträchtigt wird. Dass ihm das gleichgültig war und es ihm nur um die Waren ging, schadet nicht, denn sicheres Wissen um die notwendige Folge genügt. Auch die **Nachteilszufügungsabsicht** ist zu bejahen. Er handelte zudem rechtswidrig und schuldhaft.

E. Datenveränderung, § 303a Abs. 1 StGB

A könnte sich wegen Datenveränderung gem. § 303a Abs. 1 StGB strafbar gemacht haben.

1. Objektiver Tatbestand

Nach § 303a Abs. 1 StGB macht sich strafbar, wer rechtswidrig Daten löscht, unterdrückt, unbrauchbar macht oder verändert.

HINWEIS: DATEN, § 303a Abs. 1 StGB

Anders als bei § 274 StGB kommt es bei § 303a StGB nicht darauf an, ob die Daten beweiserheblich oder besonders gesichert sind.

Ein **Unterdrücken** von Daten liegt vor, wenn dem Berechtigten die Möglichkeit genommen wird, auf die Daten zuzugreifen.

¹¹ BGH, Beschl. v. 28.1.2026 – 4 StR 672/25, BeckRS 2026, 8088, Rn. 11.

¹² BGH, Beschl. v. 28.1.2026 – 4 StR 672/25, BeckRS 2026, 8088, Rn. 11.

Nach Auffassung des BGH erfüllt das festgestellte Geschehen den objektiven Tatbestand jedenfalls insoweit, als dem O durch die Wegnahme der Karten der Zugriff auf die darin inkorporierten Daten zumindest vorübergehend genommen wurde. Darüber hinaus kommt eine Veränderung der auf der Karte gespeicherten Daten durch die einzelnen Kartennutzungen selbst in Betracht.¹³

Der objektive Tatbestand des **§ 303a Abs. 1 StGB** ist damit grundsätzlich erfüllt.¹⁴

2. Subjektiver Tatbestand

A müsste jedoch auch vorsätzlich gehandelt haben, **§ 15 StGB**.

Hierfür müssten hinreichende Feststellungen dazu bestehen, dass sich sein Vorsatz auch auf die tatsächlichen Vorgänge hinsichtlich der auf der Karte gespeicherten Daten erstreckte.

Gerade daran fehlt es. Ob A wusste, dass beim Bezahlen Daten auf der Karte verändert werden, lässt sich nicht aufklären. In dubio pro reo ist der Vorsatz zu verneinen. Auch ein Versuch (**§ 303a Abs. 2 StGB**) scheidet aus.¹⁵

3. Ergebnis

Eine Strafbarkeit des A wegen **Datenveränderung gem. § 303a Abs. 1 StGB** scheidet in dubio pro reo aus.¹⁶ Zudem ist zusätzlich das grundsätzliche Antragserfordernis des **§ 303c StGB** zu beachten, der im Sachverhalt aber laut Vermerk gestellt ist.¹⁷

Auch hier ergibt sich jedoch mit Blick auf die **Fallabwandlung** anderes: Eine Strafbarkeit des A wegen Datenveränderung gem. **§ 303a Abs. 1 StGB** ist aufgrund der vertieften Kenntnisse des A der technischen Feinheiten des Zahlungsvorgangs zu bejahen.

Konkurrenzen der Karteneinsätze

1. In der Abwandlung stellt sich mit Blick auf **§§ 274 Abs. 1 Nr. 2** und **303a Abs. 1 StGB** abschließend die Frage nach dem Konkurrenzverhältnis der einzelnen Kartennutzungen. für **Gesetzeskonkurrenz** spricht: **§ 274 Abs. 1 Nr. 2 StGB** enthält im Wesentlichen alle Merkmale

¹³ BGH, Beschl. v. 28.1.2026 – 4 StR 672/25, BeckRS 2026, 8088, Rn. 12.

¹⁴ BGH, Beschl. v. 28.1.2026 – 4 StR 672/25, BeckRS 2026, 8088, Rn. 12.

¹⁵ BGH, Beschl. v. 28.1.2026 – 4 StR 672/25, BeckRS 2026, 8088, Rn. 12.

¹⁶ BGH, Beschl. v. 28.1.2026 – 4 StR 672/25, BeckRS 2026, 8088, Rn. 12.

¹⁷ BGH, Beschl. v. 28.1.2026 – 4 StR 672/25, BeckRS 2026, 8088, Rn. 12.

des **§ 303a** und verlangt zusätzlich Beweiserheblichkeit und Nachteilsabsicht. Das OLG Hamm hat **§ 303a StGB** entsprechend nur nachrangig herangezogen. Für **Tateinheit** spricht die unterschiedliche Schutzrichtung: hier das Beweisführungsinteresse, dort die Integrität und Verfügbarkeit von Daten.

2. Mehrere Zahlungen in demselben Geschäft: Die beiden Zahlungen in der Tankstelle bilden eine natürliche Handlungseinheit. Das sind mehrere gleichartige Handlungen, die auf einem einheitlichen Willensentschluss beruhen und räumlich und zeitlich so eng zusammenhängen, dass sie natürlich betrachtet als ein Tun erscheinen. Dasselbe gilt für die Zahlungen im Tabakgeschäft einschließlich der abgelehnten Vorgänge.

3. Was den Wechsel von der Kredit- auf die Debitkarte im Tabakgeschäft des T2 angeht, hatte das Landgericht diesem eine Zäsurwirkung beigemessen und deshalb eine weitere selbstständige Tat angenommen. Dem tritt der BGH entgegen. Hatten A und M von vornherein vor, beide erbeuteten Karten einzusetzen, liegt im bloßen Kartenwechsel innerhalb desselben Geschäfts **kein neuer Tatentschluss**. Allein der Wechsel des verwendeten Zahlungsmittels kann unter diesen Umständen daher keine Tatmehrheit gem. **§ 53 StGB** begründen.¹⁸

4. Tankstelle und Tabakgeschäft. Zwischen den zwei Tatorten liegen – anders als beim Fernsehmarathon Eurer Großeltern in der ARD-Mediathek – zwei Stunden und ein Ortswechsel, eine natürliche Handlungseinheit scheidet aus. Der gemeinsame Gesamtplan allein verbindet die Einsätze nicht, denn die fortgesetzte Handlung gibt es nicht mehr (BGHSt 40, 138). Es liegen zwei Taten vor (**§ 53 StGB**).

F. Gesamtergebnis

A hat sich im ersten Tatkomplex wegen **besonders schwerer räuberischer Erpressung in Tateinheit mit gefährlicher Körperverletzung** strafbar gemacht.

Die anschließenden kontaktlosen Kartenzahlungen erfüllen hingegen **nicht den Tatbestand des Computerbetruges gem. § 263a Abs. 1 Var. 3 StGB**, da es beim kontaktlosen Bezahlen

¹⁸ BGH, Beschl. v. 28.1.2026 – 4 StR 672/25, BeckRS 2026, 8088, Rn. 24.

ohne PIN-Eingabe am erforderlichen Täuschungsäquivalent fehlt.¹⁹ Auch ein **Betrug gem. § 263 Abs. 1 StGB** zulasten von T1 und T2 scheidet mangels Vermögensschadens aus; ebenso liegt keine **(Selbst-)Geldwäsche gem. § 261 Abs. 7 StGB** vor.²⁰

Eine Strafbarkeit wegen **Urkundenunterdrückung gem. § 274 Abs. 1 Nr. 2 StGB** sowie **Datenveränderung gem. § 303a Abs. 1 StGB** kommt dagegen grundsätzlich in Betracht. Auf Grundlage der bisherigen Feststellungen kann sie jedoch nicht bejaht werden, da das Landgericht keine hinreichenden Feststellungen zum erforderlichen Vorstellungsbild des A getroffen hat.²¹ Insoweit ist in dubio pro reo zugunsten des A zu entscheiden und eine Strafbarkeit abzulehnen.

Dogmatische Vertiefung

Bankkarte, Kreditkarte, Smartphone oder Smartwatch: Bezahlen wird technisch immer einfacher, strafrechtlich nicht. Zahlt nicht der berechtigte Karteninhaber, überlagern sich binnen (juristischer) Sekunden Diebstahls-, Betrugs-, Computer- und Datenstrafrecht. Für die Klausur müsst Ihr deshalb keine zwanzig „Kartenfälle“ auswendig kennen. Entscheidend ist, **die Funktion des konkreten Zahlungsmittels und den technischen Ablauf des Zahlungsvorgangs zu verstehen.**

Drei Fragen bestimmen das Vorgehen: **Welche Funktion hat die Karte? Wer verwendet sie? Und wie wird sie verwendet?** Die Antworten entscheiden darüber, ob ein Eigentumsdelikt, **§ 263 StGB, § 263a StGB** oder ein Daten- bzw. Urkundendelikt einschlägig ist.

A. Erste Weichenstellung: Erlangung und Verwendung der Karte trennen

Schon die Sachverhaltsskizze sollte zwei Tatkomplexe trennen: **Wie gelangt der Täter an die Karte? Was macht er anschließend mit ihr?** Bei der Erlangung stehen die Eigentumsdelikte im Vordergrund, bei der Verwendung die Vermögens-, Computer- und Datendelikte. Unser Fall folgt genau diesem Muster.

¹⁹ BGH, Beschl. v. 28.1.2026 – 4 StR 672/25, BeckRS 2026, 8088, Rn. 8.

²⁰ BGH, Beschl. v. 28.1.2026 – 4 StR 672/25, BeckRS 2026, 8088, Rn. 10.

²¹ BGH, Beschl. v. 28.1.2026 – 4 StR 672/25, BeckRS 2026, 8088, Rn. 11 f.

Wegnahme der Karte – nicht vorschnell § 242 StGB bejahen!

Nimmt T eine fremde Girocard an sich, ist der objektive Tatbestand des § 242 Abs. 1 StGB schnell erfüllt. Die Hürde liegt in der **Zueignungsabsicht**: Will T die Karte nur benutzen und anschließend zurücklegen, fehlt hinsichtlich der Kartensubstanz der dauerhafte Enteignungsvorsatz; das ist bloße **Gebrauchsanmaßung**. Will T sie dagegen behalten, liegt Zueignungsabsicht vor. Gleiches gilt, wenn T die Karte erst benutzen und danach wegwerfen will. Nimmt T sie hingegen nur weg, um sie wegzuerwerfen oder zu vernichten, fehlt die Aneignungsabsicht; es bleibt bei einer straflosen Sachentziehung im Rahmen des § 242 (BGH NStZ 2011, 699 – Kuttenfall), in Betracht kommen dann §§ 303, 274 Abs. 1 Nr. 1 StGB.

Auch der Zugriff auf das Bankguthaben ändert nichts. Die Girocard verkörpert das Geld auf dem Konto nicht, sie ist nur der **Schlüssel** dazu. Das Guthaben ist deshalb kein der Karte innewohnender Sachwert – kein *lucrum ex re* –, den sich der Täter mit der Karte zueignen könnte.

HINWEIS: LUCRUM EX RE § 242 StGB

§ 242 StGB schützt das Eigentum an einer bestimmten Sache. Er darf nicht dadurch zum allgemeinen Vermögensdelikt werden, dass jeder wirtschaftliche Vorteil, den eine Sache nur mittelbar vermittelt, als ihr „Sachwert“ behandelt wird.

Gegenbeispiel **Sparbuch**: Als qualifiziertes Legitimationspapier i.S.d. § 808 BGB verkörpert es nach h.M. gerade den Wert des Guthabens. Wer es wegnimmt, Geld abhebt und es zurücklegt, handelt daher mit Zueignungsabsicht. Bei der Girocard bleibt das Guthaben dagegen rechtlich von der Karte getrennt.

B. Mensch oder Maschine? – Betrug und Computerbetrug

Bei der Kartenverwendung lautet die erste Frage erstaunlich schlicht: **Trifft ein Mensch die vermögensrelevante Entscheidung – oder ein Computer?**

§ 263 StGB ist ein **Kommunikations- und Selbstschädigungsdelikt**: Der Getäuschte mindert das Vermögen irrtumsbedingt **selbst**. Ein Automat kann dagegen weder getäuscht werden noch irren. Diese Lücke schließt § 263a StGB. Soweit der Computer „verfügt“, etwa über die Belastung des Kontos, ist nicht zugleich der Mensch an der Kasse der Verfügende (vgl. den Hinweis zum Dreiecksbetrug oben).

Für Kartenfälle ist außerdem wichtig, dass regelmäßig drei Vermögenssphären beteiligt sind: **Karteninhaber, Bank und Händler**. Wer geschädigt ist, bestimmt nicht das Gefühl im Sachverhalt, sondern die rechtliche Wirkung des Zahlungsvorgangs.

C. Herzstück des „Kartenstrafrechts“: § 263a Abs. 1 Var. 3 StGB

Dass beim Karteneinsatz Daten verwendet werden, ist unproblematisch. Die Klausur entscheidet sich am unscheinbaren Wort „**unbefugt**“. Die drei Auslegungsmodelle kennt Ihr aus der Streitbox oben. Merken solltet Ihr vor allem die Denkfigur von BGH und h.M.: Man ersetzt den Computer gedanklich durch einen Menschen, der **genau dieselben Prüfungen** vornimmt wie das System (fiktiver Bankangestellter), und fragt, ob das Verhalten ihm gegenüber eine zumindest konkludente Täuschung wäre. Nur dann liegt das erforderliche **Täuschungsäquivalent** vor. **Übrigens:** „Unbefugt, weil T nicht berechtigt war“ ist keine Begründung, sondern eine Behauptung. Bei § 263a Abs. 1 Var. 3 StGB müsst Ihr vielmehr erklären, **welche hypothetische Täuschung** in der Datenverwendung liegen soll.

D. Der entscheidende Unterschied: Karte mit PIN oder ohne PIN

I. Einsatz einer fremden Karte unter Eingabe der PIN

Gibt der Nichtberechtigte die zutreffende PIN ein, liegt das Täuschungsäquivalent vor. Die PIN dient gerade der **Authentifizierung**: Wer sie eingibt, erklärt dem gedachten Bankangestellten zumindest, zur Nutzung der Karte berechtigt zu sein. Das ist der Klassiker: gestohlene Karte plus ausgespähte oder im Portemonnaie notierte PIN.

Anders liegt es, wenn der Berechtigte Karte und PIN **freiwillig überlassen** hat und der Empfänger nur interne Absprachen überschreitet, etwa 200 statt 100 Euro abhebt. Die Bank prüft allein Karte und PIN; über die Absprache würde ihr gegenüber nichts erklärt. Nach dem BGH gilt das sogar, wenn der Täter sich Karte und PIN zuvor durch Täuschung verschafft hat; in Betracht kommt dann ein Betrug zulasten des Karteninhabers bereits bei der Erlangung.²²

²² BGH, Beschl. v. 16.7.2015 – 2 StR 15/15, StV 2016, 359 (Kein Computerbetrug durch Verwendung einer zuvor durch Täuschung erlangten Karte und PIN).

MERKE: Nicht jede zivilrechtliche Pflichtverletzung ist „unbefugt“ i.S.d. **§ 263a StGB**.

II. „Tap & Go“ – kontaktloses Bezahlen ohne PIN

Hält T die Karte nur an das Terminal und läuft die Zahlung **ohne PIN, Unterschrift oder sonstige Authentifizierung**, werden zwar ebenfalls Daten verwendet. Der gedachte Bankangestellte prüft aber nur, ob die Karte gesperrt und der Verfügungsrahmen eingehalten ist, nicht die Person. Wer die Karte vorhält, erklärt deshalb nicht konkludent: „Ich bin berechtigt.“ Es **fehlt gerade das Täuschungsäquivalent**; **§ 263a Abs. 1 Var. 3 StGB** scheidet aus.

Gerade hierin liegt der entscheidende Klausurunterschied:

Kartenverwendung	§ 263a Abs. 1 Var. 3 StGB
Fremde Karte mit PIN	grundsätzlich (+), Täuschungsäquivalent durch Authentifizierung
Fremde Karte kontaktlos ohne PIN	nach BGH (-), keine Erklärung über die Berechtigung
Eigene Karte durch berechtigten Inhaber	§ 263a regelmäßig (-); ggf. § 266b StGB
Freiwillig überlassene Karte, aber abredewidrige Nutzung	nach h.M. (-); interne Pflichtverletzung genügt nicht

E. Hilft **§ 263 StGB** weiter? – Der Händlerbetrug

Scheitert **§ 263a StGB**, liegt der Griff zum „normalen“ Betrug nahe: Immerhin steht ein Kassierer vor dem Täter und gibt die Ware heraus. Mit der Autorisierung erwirbt der Händler aber einen **garantierten Zahlungsanspruch** gegen die Bank; die Karte wirkt für ihn wie Bargeld. Nach der BGH-Linie fehlt es daher schon an Täuschung und Irrtum, jedenfalls aber am **Vermögensschaden** des Händlers (Einzelheiten in der Lösung).

Die Gegenprobe schärft den Blick: Beim **elektronischen Lastschriftverfahren** (Unterschrift statt PIN) gibt es keine Zahlungsgarantie. Der Händler trägt das Risiko einer Rückbelastung,

die Berechtigung des Kunden ist für ihn also bedeutsam. Hier kommt **§ 263 StGB** zulasten des Händlers ernsthaft in Betracht, für die fremde Unterschrift zudem **§ 267 StGB**.

HINWEIS: KLAUSURTAKTIK

Ist ein Merkmal eindeutig zu verneinen, dürft Ihr Streitige Vorfragen offenlassen („Dies kann dahinstehen, da jedenfalls kein Vermögensschaden eingetreten ist.“). Tut das aber nicht reflexhaft: Liegt die Pointe gerade in der Vorfrage – wie hier beim fehlenden Erklärungswert –, verschenkt das Offenlassen Punkte.

F. Sonderfall: Der berechtigte Karteninhaber – **§ 266b StGB**

Handelt nicht ein Nichtberechtigter, sondern derjenige, dem der Aussteller die Karte selbst überlassen hat, verschiebt sich die Deliktsstruktur. Beispiel: T kauft mit seiner eigenen Kreditkarte ein, obwohl er weiß, dass er den Saldo nicht ausgleichen kann. **§ 263a StGB** passt nicht, weil T die Daten verwenden darf; **§ 263 StGB** zulasten des Händlers scheitert an der Zahlungsgarantie.

Hier greift **§ 266b StGB** als untreuähnlicher **Angriff von innen: rechtliches Können nach außen bei Überschreitung des rechtlichen Dürfens im Innenverhältnis**. Geschädigt ist der Kartenaussteller.

Die Vorfrage lautet deshalb immer: **Ist T Nichtberechtigter oder derjenige, dem die Karte selbst überlassen wurde?** Der Dieb einer Kreditkarte ist nie Täter des **§ 266b StGB**.

G. Wenn die Vermögensdelikte nicht greifen: Daten- und Urkundendelikte

Dass **§§ 263, 263a StGB** beim kontaktlosen Bezahlen ohne PIN ausscheiden, bedeutet nicht Straflosigkeit. Die Karte ist nicht nur Zahlungsmittel, sondern auch **Datenträger**. Drei Normen, drei Schutzrichtungen:

§ 269 StGB schützt die **Echtheit** beweisheblicher Daten (digitale Urkundenfälschung). Für das klassische Tap & Go hat das OLG Hamm die Norm mangels Datenurkunde verneint.

§ 274 Abs. 1 Nr. 2 StGB schützt den **Bestand** beweisheblicher Daten als Beweismittel.

§ 303a StGB schützt **Integrität und Verfügbarkeit** von Daten; auf eine Beweisfunktion kommt es nicht an. Die Norm ist das digitale Gegenstück zu **§ 303 StGB** und relatives Antragsdelikt (**§ 303c StGB**).

Beim Tap & Go sind **§ 274 Abs. 1 Nr. 2** und **303a StGB** objektiv regelmäßig erfüllt; die Hürde liegt im **subjektiven Tatbestand** (dazu die Lösung oben). Nicht genügen darf in der Klausur das Argument: „Jeder weiß heute, dass Kartenzahlungen gespeichert werden.“ Das ersetzt nicht die Feststellung, dass gerade dieser Täter die Beweisfunktion der Chipdaten erkannt hat.

H. Ein Prüfungssystem statt zwanzig auswendig gelernter Kartenfälle

- 1. Erlangung der Karte:** Eigentumsdelikte, **§§ 242 ff. StGB**. Soll die Karte zurück, fehlt der Ent-eignungsvorsatz; das Guthaben ist kein Sachwert der Karte.
- 2. Wer entscheidet?** Ein Mensch (**§ 263**) oder ein Datenverarbeitungssystem (**§ 263a StGB**)?
- 3. Wer handelt?** Ein Nichtberechtigter (**§ 263a**) oder der berechtigte Karteninhaber (**§ 266b StGB**)?
- 4. Wie wird bezahlt?** Mit PIN: Täuschungsäquivalent (+). Kontaktlos ohne PIN: (-).
- 5. Wer ist geschädigt?** Händler, Bank und Karteninhaber auseinanderhalten; eine Zahlungs-garantie schließt den Schaden des Händlers aus.
- 6. Nicht zu früh aufhören:** Die Karte ist auch Datenträger. **§§ 269, 274 Abs. 1 Nr. 2, 303a StGB** prüfen und den subjektiven Tatbestand ernst nehmen.

Das scheinbar unübersichtliche „Kartenstrafrecht“ reduziert sich damit auf eine klassische Frage: **Welches Rechtsgut wird durch welche konkrete Handlung angegriffen?** Eine Karte kann Sache, Zahlungsmittel, Legitimationsmittel und Datenträger zugleich sein. Wirtschaftlich ist der Tap-&-Go-Fall eindeutig: Ein Nichtberechtigter kauft auf fremde Kosten ein. Strafrechtlich folgt daraus noch kein Vermögensdelikt. Eine Berechtigungserklärung, die das Zahlungs-system bewusst nicht abfragt, darf nicht nachträglich in den Vorgang hineingelesen werden,

nur um eine gefühlte Strafbarkeitslücke zu schließen. **Das ist die eigentliche examensrelevante Erkenntnis:** Nicht das gewünschte Ergebnis bestimmt den Tatbestand, sondern dessen dogmatische Struktur.²³

²³ Verfasser: Christian Lederer, Wissenschaftlicher Mitarbeiter bei HLB Schumacher Hallermann
Supervision: Dr. Lennart Brüggemann, Rechtsanwalt & Partner bei HLB Schumacher Hallermann