Fortgeschrittenenklausur: Kontaktloses Bezahlen

*PD Dr. Boris Burghardt, Marburg, Stud. Hilfskraft Ricarda Bardowicks, Göttingen**

Der Fall wurde im Sommersemester 2022 im Rahmen der Übung im Strafrecht für Fortgeschrittene an der Georg-August-Universität Göttingen als dreistündige Klausur gestellt. Im Zentrum steht die strafrechtliche Bewertung der Vornahme eines elektronischen Zahlungsvorgangs ohne Eingabe einer Persönlichen Identifikationsnummer (PIN) mittels einer fremden EC-Karte. Von 145 Studierenden haben 36 % die Klausur nicht bestanden. Der Notendurchschnitt lag bei 4,7 Punkten.

Sachverhalt

V ist mit seinem zweijährigen Sohn S auf dem Kinderspielplatz im Göttinger Cheltenham-Park. Da er sich in einem angeregten Gespräch mit F, einer befreundeten Mutter, befindet, bemerkt er nicht, dass S das Portemonnaie seines Vaters aus dessen Beutel geangelt und damit begonnen hat, sämtliche Karten und Ausweise zunächst aus- und sodann wieder in das Portemonnaie einzuräumen. Dabei vergisst S leider eine auf den Namen seines Vaters ausgestellte EC-Karte der Sparkasse Göttingen, die unter der Bank, auf der V und F sitzen, verbleibt, als die Gruppe kurz darauf den Spielplatz verlässt. Erst knapp drei Stunden später bemerkt V den Verlust der Karte und veranlasst daraufhin umgehend eine Kontosperrung.

In der Zwischenzeit hat A die Karte gefunden und eingesteckt, um sie in der nächsten Sparkassenfiliale abzugeben. Als er in der Innenstadt ankommt, überlegt er es sich anders und beschließt, die Karte vor der Rückgabe noch im Rahmen eines kurzen Abstechers in den nahegelegenen Supermarkt der R-GmbH dazu zu nutzen, sich einen kleinen „Finderlohn“ zu gönnen. Angesichts der Möglichkeit, mit der Karte „kontaktlos“ zu bezahlen, sei das doch eine Sache von Sekunden.

A begibt sich also in den Supermarkt und sucht dort einige Lebensmittel und Getränke im Wert von insgesamt 32,76 € zusammen. Dem an der Kasse tätigen K sagt A, dass er die Waren „mit Karte“ zahlen möchte. Sodann hält er die im Park gefundene Karte des V an das von K aktivierte Kartenlesegerät. Wie von ihm erhofft, kann er dadurch den Zahlungsvorgang abschließen, ohne eine Persönliche Identifikationsnummer (PIN) eingeben zu müssen. Vielmehr zeigt das Kartenlesegerät nach einigen Sekunden schlicht „Zahlung erfolgt“ an.

Dabei funktioniert dieser Zahlungsvorgang vereinfacht wie folgt:[1] Die EC-Karte ist mit einem NFC-/Near Field Communication-Chip ausgestattet. Als A die Karte in unmittelbare Nähe des aktivierten Kartenlesegeräts hält, überträgt dieser Chip Kartennummer und Gültigkeitsdatum der Karte an das Kartenlesegerät. Dort wird mit diesen Daten sowie mit den Kontodaten der R-GmbH als Zahlungsempfängerin eine Anfrage zur Autorisierung einer Zahlung in Höhe des Rechnungsbetrages an das Zahlungssystem der Sparkasse Göttingen gesendet. Das Zahlungssystem prüft sodann, ob die eingesetzte EC-Karte gesperrt ist und ob der Verfügungsrahmen des Kontos noch nicht ausgeschöpft

* PD *Dr. Boris Burghardt* vertritt derzeit eine Professur für Strafrecht, Strafprozessrecht und Rechtsphilosophie an der Philipps-Universität Marburg. *Ricarda Bardowicks* ist Stud. Hilfskraft am Lehrstuhl für Strafrecht und Strafprozessrecht (Prof. *Dr. Uwe Murmann*) an der Georg-August-Universität Göttingen.

[1] Vgl. auch die Erläuterungen bei *Christoph/Dorn-Haag*, NStZ 2020, 697 f.

ist. Weiterhin wird geprüft, ob die Voraussetzungen für den Verzicht auf die Eingabe der PIN vorliegen. Das ist der Fall, wenn der Zahlungsbetrag 50 € nicht überschreitet. Zudem dürfen seit der letzten PIN-Eingabe nicht mehr als fünf Zahlungsvorgänge ohne eine solche Authentifizierung vorgenommen worden sein und deren Gesamtvolumen darf 150,- € nicht überstiegen haben.

In zivilrechtlicher Hinsicht[2] erwirbt die R-GmbH durch die Autorisierung des Zahlungsvorgangs unabhängig von der Berechtigung des tatsächlichen Kartennutzers eine einredefreie Forderung in der Höhe des Rechnungsbetrages gegen die kartenausstellende Sparkasse. Anders wäre es nur dann, wenn K als die für die R-GmbH handelnde natürliche Person positive Kenntnis hätte, dass der Zahlungsvorgang durch eine dazu nichtberechtigte Person vorgenommen wurde. Zugleich werden durch die Autorisierung, die im Zahlungssystem der Sparkasse gespeicherten Datensätze aktualisiert, d.h. der Datensatz zum Zahlungsvorgang im Supermarkt der R-GmbH wird gespeichert, der verfügbare Betrag bis zum Erreichen des Verfügungsrahmens wird angepasst, und es werden die Daten aktualisiert, die erforderlich sind, um zu überprüfen, ob beim nächsten Zahlungsvorgang die Voraussetzungen eines Verzichts auf die PIN-Eingabe erneut vorliegen.

Im Verhältnis zwischen der Sparkasse und V als dem berechtigten Karteninhaber wird auf dem Konto des V zwar zunächst eine Belastung in Höhe des Rechnungsbetrages vermerkt. Als V einige Tage später die Buchung entdeckt und gegenüber der Sparkasse geltend macht, der Zahlungsvorgang sei nicht von ihm vorgenommen worden, schreibt die Bank V aber entsprechend den gesetzlichen Regelungen zur Risikotragung eines Kartenmissbrauchs durch Dritte (vgl. §§ 675u, 675v BGB) den Betrag wieder gut, so dass letztlich sie den Schaden i.H.v. 32,76 € trägt.

A verlässt nach dem Zahlungsvorgang mit den Waren den Supermarkt. Sodann wirft er die EC-Karte wie geplant in den Briefkasten des nächstgelegenen SB-Centers der Sparkasse. Wie die elektronische Zahlung mit einer EC-Karte ohne PIN-Eingabe im Einzelnen funktioniert und welche zivilrechtlichen Regeln insofern gelten, weiß A nicht. Ihm ist aber bewusst, dass dabei Daten übertragen und gespeichert werden und niemand einfach fremde EC-Karte nutzen darf.

Aufgabe

Wie hat sich A nach dem StGB strafbar gemacht? Eventuell erforderliche Strafanträge sind gestellt.

Übergreifende Hinweise

Es handelt sich um einen Fall von überdurchschnittlicher Schwierigkeit. Es sind zwar nicht viele Tatbestände zu prüfen. Auch weist die Gliederung des Gutachtens keine Probleme auf. Die zu prüfenden Tatbestände sind aber ohne Ausnahme unübersichtlich, schwierig und bei Studierenden erfahrungsgemäß unbeliebt. Es bedarf zudem sowohl einer sorgfältigen Erfassung des technischen Ablaufs des sog. „kontaktlosen" Zahlungsvorgangs wie auch der zivilrechtlichen Hintergründe. Zwar teilt der Sachverhalt die für die strafrechtliche Bewertung relevanten Details explizit mit. Erwartungsgemäß taten sich aber viele Studierenden sehr schwer damit, diese Informationen an der Stelle zu berücksichtigen, an der sie rechtlich bedeutsam sind. Im Falle der Fälschung beweiserheblicher Daten gem. § 269 StGB und der Datenveränderung gem. § 303a StGB dürfte es sich für viele Studierende überdies um gänzlich unbekannte Normen handeln. In vielen Bearbeitungen wurden diese Tatbestände schlicht übersehen. Auch für eine weit überdurchschnittliche Bewertung wurde nicht erwartet, dass die Ar-

[2] Siehe dazu *Göhler*, JR 2021, 6 (8) m.w.N.

gumentation zu den einzelnen Fragen auch nur annähernd die Ausführlichkeit der Lösungshinweise erreichte.

In der Rechtsprechung liegt zu der Fallkonstellation der missbräuchlichen Vornahme eines kontaktlosen Zahlungsvorgangs ohne PIN-Eingabe mit fremder EC-Karte eine Entscheidung des OLG Hamm (OLG Hamm, Beschl. v. 7.4.2020 – 4 RVs 12/20 = NStZ 2020, 673 ff.) vor, die vielfach besprochen worden ist und Eingang in die gängigen Lehrbücher sowie die Ausbildungszeitschriften gefunden hat. Allerdings bleiben die Ausführungen vielfach ungenau. Zudem lässt sich hinsichtlich sämtlicher Tatbestände Kritik an der Begründung, zum Teil auch an dem Ergebnis der Entscheidung anbringen. Selbst wenn die Entscheidung des OLG Hamm einzelnen Studierenden bekannt ist, bleibt daher erheblicher Bedarf und Spielraum für eigene Überlegungen.

Bei einer dreistündigen Bearbeitungszeit sollte jedenfalls hinreichend Zeit bleiben, zumindest zum Betrug, zum Computerbetrug und zur Urkundenunterdrückung in Form der Datenunterdrückung sorgfältig Stellung zu nehmen und ausführlicher zu argumentieren. Die Prüfung der Strafbarkeit gem. § 269 Abs. 1 StGB sowie gem. § 303a Abs. 1 StGB ist eher als Bonus zu betrachten.

Lösungsvorschlag

Strafbarkeit des A

A. Erster Handlungsabschnitt: Das Einstecken der EC-Karte

I. Diebstahl der EC-Karte gem. § 242 Abs. 1 StGB

Durch das Einstecken der EC-Karte könnte sich A wegen Diebstahls gem. § 242 Abs. 1 StGB strafbar gemacht haben.

1. Tatbestandsmäßigkeit

Bei der EC-Karte handelt es sich um einen körperlichen Gegenstand, der tatsächlich fortschaffbar ist und im Alleineigentum der kartenausgebenden Sparkasse steht. Es handelt sich mithin um eine bewegliche Sache, die für A fremd ist.[3] Diese müsste A weggenommen haben. Wegnahme ist der Bruch fremden und die Begründung neuen Gewahrsams.[4] Gewahrsam meint die tatsächliche, vom Herrschaftswillen getragene Verfügungsgewalt über eine Sache, deren Reichweite sich nach der Verkehrsanschauung bestimmt.[5] V verlor die EC-Karte im Cheltenham-Park. Zudem hatte er zu dem Zeitpunkt, als A die Karte einsteckte, noch keine Kenntnis von dem Verlust der Karte. Ob V überhaupt ahnte, wo er die Karte verloren haben könnte, wird im Sachverhalt jedenfalls nicht mitgeteilt. Ungeachtet seines fortdauernden Herrschaftswillens fehlte es V daher an einer tatsächlichen Verfügungsgewalt. Weil der Verlust der Zugriffsmöglichkeit außerhalb seines räumlichen Herrschaftsbereichs erfolgte, ordnet auch die Verkehrsauffassung als sozial-normatives Korrekturelement dem V nicht mehr den Gewahrsam an der Karte zu. Da der Park als öffentlich zugängliche Grünanlage nicht der räumlichen Herrschaftssphäre einer anderen Person zugehört, erlangte mit dem Verlust auch kein Dritter neuen Gewahrsam, bevor A die EC-Karte einsteckte.[6]

2. Ergebnis

Mangels Wegnahme scheidet eine Strafbarkeit des A gem. § 242 Abs. 1 StGB aus.

II. Unterschlagung der EC-Karte gem. § 246 Abs. 1 StGB

Durch dieselbe Handlung könnte sich A wegen Unterschlagung gem. § 246 Abs. 1 StGB strafbar gemacht haben.

Bei der EC-Karte handelt es sich um eine fremde bewegliche Sache, welche sich A unter objektiver Manifestation des Zueignungswillen hätte zueignen müssen.[7] Da A jedoch vorhatte, die EC-Karte in der nächsten Sparkassenfiliale abzugeben, und somit einen festen Rückführungswillen aufwies, fehlt

[3] Vgl. *Wessels/Hillenkamp/Schuhr,* Strafrecht, Besonderer Teil 2, 44. Aufl. 2021, Rn. 79, 83 f.

[4] *Schmidt*, in: Matt/Renzikowski, Strafgesetzbuch, Kommentar, 2. Aufl. 2020, § 263 Rn. 32.

[5] *Kindhäuser*, in: NK-StGB, Bd. 4, 6. Aufl. 2023, § 242 Rn. 28; BGH NStZ 2019, 726 (727).

[6] Vgl. zu den Gewahrsamsverhältnissen an verlorenen Gegenständen im öffentlichen Raum aus der Rechtsprechung zuletzt BGH, Beschl. v. 14.5.2020 – 5 StR 10/20 = NStZ 2020, 483; aus der Lit. z.B. *Bosch*, in: Schönke/Schröder, Strafgesetzbuch, Kommentar, 30. Aufl. 2019, § 242 Rn. 28; *Kudlich*, JA 2020, 865 (866); *Rönnau*, JuS 2009, 1088 (1089).

[7] Vgl. *Hilgendorf/Valerius,* Strafrecht, Besonderer Teil II, 2. Aufl. 2021, § 5 Rn. 9.

es bereits am erforderlichen Zueignungswillen, der den Vorsatz zur dauernden Enteignung umfasst.[8] Eine Strafbarkeit gem. § 246 Abs. 1 StGB scheidet aus.

III. Ergebnis zum ersten Handlungsabschnitt

Durch das Einstecken der EC-Karte hat sich A nicht strafbar gemacht.

B. Zweiter Handlungsabschnitt: Im Supermarkt

I. Betrug ggü. K zu Lasten der R-GmbH gem. § 263 Abs. 1 StGB

A könnte sich durch das Bezahlen mit der EC-Karte des V im Supermarkt der R-GmbH wegen Betruges nach § 263 Abs. 1 StGB strafbar gemacht haben.

1. Tatbestandsmäßigkeit

a) Objektiver Tatbestand

aa) Täuschung

Zunächst müsste A den K über Tatsachen getäuscht haben. Eine Täuschung ist jede Einwirkung auf das Vorstellungsbild eines anderen, welche zu einer Fehlvorstellung bei diesem führt.[9] Tatsachen sind dem Beweis zugängliche Ereignisse oder Zustände der Gegenwart oder Vergangenheit.[10]

Indem A die EC-Karte des V für den kontaktlosen Bezahlvorgang einsetzte, könnte er über den Umstand getäuscht haben, dass er *der berechtigte Karteninhaber* oder doch zumindest eine durch den berechtigten Karteninhaber bevollmächtigte Person sei.[11] Da A sich nicht explizit über seine Berechtigung zur Nutzung der Karte geäußert hat, müsste seinem Verhalten eine entsprechende stillschweigende Erklärung zu entnehmen sein.

Der konkludente Erklärungsgehalt eines Verhaltens im Rechtsverkehr wird regelmäßig durch eine *normative Betrachtung* bestimmt, d.h. unter Berücksichtigung der rechtlichen Pflichten, die der handelnden Person obliegen, und den Verpflichtungen, die ihr aus der Vornahme eines Verhaltens erwachsen, sowie der rechtlichen Risikoverteilung im Falle eines Schadenseintritts.[12] Eine normative Betrachtung könnte hier dagegensprechen, dem Einsatz der EC-Karte für einen Bezahlungsvorgang ohne Eingabe des PIN eine Aussage über die Berechtigung hierzu zu entnehmen. Denn grundsätzlich ist der Erwerb einer einredefreien Forderung des Geschäftspartners (hier der R-GmbH) gegen die kartenausstellende Bank in Höhe des Rechnungsbetrages unabhängig von der Berechtigung des tatsächlichen Kartennutzers zum Gebrauch der EC-Karte.[13] Es lässt sich daher argumentieren, dass der

[8] BGH NZV 2015, 95 (96); *Kudlich/Koch,* JA 2017, 184 (185).

[9] *Duttge*, in: Dölling u.a., Handkommentar, Gesamtes Strafrecht, 5. Aufl. 2022, § 263 Rn. 8; BGH NJW 2001, 2187 (2188).

[10] *Rengier,* Strafrecht, Besonderer Teil I, 24. Aufl. 2022, § 13 Rn. 4.

[11] Vgl. BGH NJW 2007, 782 (784).

[12] *Hefendehl*, in: MüKo-StGB, Bd. 5, 4. Aufl. 2022, § 263 Rn. 85; *Perron*, in: Schönke/Schröder, Strafgesetzbuch, Kommentar, 30. Aufl. 2019, § 263 Rn. 14/15; *Becker*, JuS 2014, 307 (310).

[13] Vgl. zum kontaktlosen Bezahlen mit fremder EC-Karte OLG Hamm NStZ 2020, 673 (674), *Heghmanns*, ZJS 2020, 494 (495).

tatsächliche Kartennutzer (hier: A) nicht gezwungen ist, explizit oder konkludent Erklärungen über seine Berechtigung zum Einsatz der EC-Karte abzugeben.

Indes betrifft dieser Gesichtspunkt nicht so sehr den Erklärungsgehalt des Verhaltens von A als vielmehr den Bewusstseinshorizont der Personen, die auf der Seite der R-GmbH handeln. Hinzu kommt folgende Überlegung, die sowohl das faktische Geschehen als auch rechtliche Aspekte betrifft: A hält eine Karte an das Kartenlesegerät, auf der der Name des eigentlich berechtigten Karteninhabers (hier: V) eingeprägt ist. Zugleich behalten sämtliche Banken in ihren Vertragsbedingungen den Einsatz der EC-Karte allein dem berechtigten Karteninhaber vor. Schließlich ist allen am Rechtsverkehr beteiligten Personen auch ohne detaillierte Kenntnisse der gesetzlichen und vertragsrechtlichen Ausgestaltung bewusst, dass EC-Karten grundsätzlich nur durch den berechtigten Karteninhaber und jedenfalls nicht durch irgendwelche Dritte ohne bzw. gegen den Willen des berechtigten Karteninhabers verwendet werden dürfen. Die besseren Gründe sprechen daher im Ergebnis dafür, dass in dem Halten der EC-Karte an das Kartenlesegerät die konkludente Erklärung liegt, der berechtigte Karteninhaber zu sein.

Hinweis: A.A. vertretbar.

bb) Irrtum

A müsste durch die Täuschung einen Irrtum erregt haben. Unter einem Irrtum ist jeder Widerspruch zwischen Vorstellung und Wirklichkeit zu verstehen.[14] Als natürliche Person,[15] auf deren Vorstellungsbild A eingewirkt haben könnte, kommt nur der an der Kasse beschäftigte K in Betracht. Fraglich ist, ob sich K während des Einsatzes der EC-Karte durch A überhaupt Gedanken über dessen Berechtigung gemacht hat. Mangels näherer Angaben kommt allenfalls ein sog. sachgedankliches Mitbewusstsein des K in Betracht, wonach bei dem durch A vorgenommenen Zahlungsvorgang „alles in Ordnung“ war.[16] Ob zu dem allgemeinen sachgedanklichen Mitbewusstsein eines Kassenangestellten bei der Vornahme elektronischer Zahlungsvorgänge mittels EC-Karte durch Kunden auch der Umstand gehört, dass diese die berechtigten Karteninhaber sind, ist erneut unter Berücksichtigung normativer Gesichtspunkte zu bestimmen.

Zu beachten ist daher insbesondere, dass die R-GmbH, in deren Interesse K als Ladenvertreter gem. § 56 HGB tätig ist, grundsätzlich auch dann eine einredefreie Forderung gegen den Zahlungsdienstleister (hier: die Sparkasse Göttingen) erwirbt, wenn der autorisierte Zahlungsvorgang durch einen nichtberechtigten Dritten initiiert worden ist. K als die für die R-GmbH handelnde natürliche Person muss sich also keine Vorstellung über die Berechtigung des A machen, um für die R-GmbH einen wirtschaftlich validen Anspruch in Rechnungshöhe zu erwerben. Das spricht dagegen, dass zu dem allgemeinen sachgedanklichen Mitbewusstsein des K die Vorstellung gehörte, A sei der berechtigte Karteninhaber. Ein Irrtum des K ist nicht gegeben.[17]

[14] *Perron*, in: Schönke/Schröder Strafgesetzbuch, Kommentar, 30. Aufl. 2019, § 263 Rn. 33; *Rengier*, Strafrecht, Besonderer Teil I, 24. Aufl. 2022, § 13 Rn. 42.

[15] Nur natürliche Personen können irren, vgl. etwa *Hefendehl*, in: MüKo-StGB, Bd. 5, 4. Aufl. 2022, § 263 Rn. 344.

[16] Vgl. zum sachgedanklichen Mitbewusstsein *Rönnau/Becker*, JuS 2014, 504 (505); *Wessels/Hillenkamp/Schuhr,* Strafrecht, Besonderer Teil 2, 44. Aufl. 2021, Rn. 358.

[17] Vgl. zur Ablehnung des Irrtums, wenn der Getäuschte sich keine Vorstellung macht, *Duttge*, in: Dölling u.a., Handkommentar, Gesamtes Strafrecht, 5. Aufl. 2022, § 263 Rn. 23; *Kindhäuser/Hilgendorf,* Strafgesetzbuch, Lehr- und Praxiskommentar, 9. Aufl. 2022, § 263 Rn. 100.

Hinweis: A.A. vertretbar.

b) Zwischenergebnis

Mangels Irrtums ist der objektive Tatbestand des Betruges nicht erfüllt.

Hinweis: Bei Annahme eines Irrtums auf Seiten des K läge die tatbestandlich vorausgesetzte Vermögensverfügung darin, dass K stellvertretend (§ 56 HGB) für die R-GmbH die Waren an A übereignet und den Besitz an ihnen überträgt und dadurch unmittelbar das Vermögen der R-GmbH mindert.[18] Diese verfügungsbedingte Vermögensminderung wird durch den Erwerb der Forderung infolge der Autorisierung des elektronischen Zahlungsvorgangs jedoch im Wege der Gesamtsaldierung[19] ausgeglichen, sodass bei der R-GmbH kein Schaden eintritt. Bei der Sparkasse Göttingen, die eine einredefreie Forderung der R-GmbH gegen sich gelten lassen muss, und dem Karteninhaber V, dessen Konto vorläufig belastet wird, resultiert ein Vermögensschaden jedenfalls nicht daraus, dass K die Waren an A übereignet und ihm den Besitz an diesen übertragen hat, sondern allenfalls aus dem computergestützten Zahlungsvorgang. Insoweit fehlt es also an einem fortlaufenden Kausal- und Unmittelbarkeitszusammenhang[20] zwischen der Vermögensverfügung des K und einem möglichen Vermögensnachteil. Überdies handelt K auch nicht mit Ermächtigung oder „im Lager" der Sparkasse oder des V.[21] Der Tatbestand des Betruges ist daher jedenfalls nicht erfüllt.

2. Ergebnis

Eine Strafbarkeit des A wegen Betruges gem. § 263 Abs. 1 StGB scheidet aus.

II. Computerbetrug gem. § 263a Abs. 1 Var. 3 StGB

Durch das Bezahlen mit der EC-Karte könnte sich A wegen Computerbetruges gem. § 263a Abs. 1 Var. 3 StGB strafbar gemacht haben.

1. Tatbestandsmäßigkeit

a) Objektiver Tatbestand

A müsste das Vermögen eines anderen durch die unbefugte Verwendung von Daten beschädigt haben.

aa) Verwendung von Daten

Erforderlich ist zunächst, dass A Daten verwendet hat. Daten sind alle codierten oder zumindest

[18] Vgl. zur Vermögensminderung BGH NJW 1960, 1068 (1069); *Duttge*, in: Dölling u.a., Handkommentar, Gesamtes Strafrecht, 5. Aufl. 2022, § 263 Rn. 27 ff.

[19] Vgl. zur Gesamtsaldierung BGH NStZ 2015, 89 (91); BGH NStZ 2016, 286 (287); *Rengier*, Strafrecht, Besonderer Teil I, 24. Aufl. 2022, § 13 Rn. 181.

[20] Vgl. zur erforderlichen Unmittelbarkeit *Wessels/Hillenkamp/Schuhr*, Strafrecht, Besonderer Teil 2, 44. Aufl. 2021, Rn. 568.

[21] Vgl. zu den Voraussetzungen des Dreiecksbetrugs *Perron*, in: Schönke/Schröder, Strafgesetzbuch, Kommentar, 30. Aufl. 2019, § 263 Rn. 65 f.; BGH NJW 1963, 1068 (1069).

codierbaren Informationen.[22] Indem A die Karte ans Kartenlesegerät gehalten hat, wurden die auf der EC-Karte gespeicherten Daten mit den Daten des Verkäufers zu einer Autorisierungsanfrage vervollständigt und an das Zahlungssystem des Kartenausstellers gesendet. Es wurden mithin codierte Informationen übertragen, eine Verwendung von Daten i.S.d. § 263a StGB liegt vor.

bb) Unbefugt

Die Verwendung der Daten müsste unbefugt erfolgt sein. Die Auslegung dieses Tatbestandmerkmals ist umstritten.

(1) Vertragsspezifische/subjektivierende Auslegung

Denkbar ist zunächst, das Merkmal so zu verstehen, dass eine Verwendung immer dann unbefugt ist, wenn sie dem tatsächlichen oder mutmaßlichen Willen des Berechtigten widerspricht.[23] Dies wäre im vorliegenden Fall zu bejahen, und zwar unabhängig davon, ob insoweit auf die kartenausstellende Bank oder auf den berechtigten Karteninhaber abzustellen ist. Weder die Sparkasse Göttingen noch V sind damit einverstanden, dass die EC-Karte von einem Dritten (hier dem nichtberechtigten A) eingesetzt wird.

(2) Computerspezifische Auslegung

Als computerspezifische Auslegung wird eine Anreicherung des Begriffes „unbefugt" bezeichnet, die eine unbefugte Verwendung von Daten nur in den Fällen annimmt, wenn der entgegenstehende Wille der Berechtigten in der Ausgestaltung des Computerprogramms durch einen Kontroll- oder Prüfungsmechanismus zum Ausdruck gekommen ist und daher durch eine irreguläre Einwirkung überwunden werden muss.[24] Weil es in der Programmgestaltung für das kontaktlose Bezahlen ohne PIN-Eingabe einen Prüfungsschritt hinsichtlich der Berechtigung nicht gibt, liegt kein unbefugtes Verwenden von Daten in einem computerspezifischen Sinn vor. Geprüft wird lediglich, ob die Karte gesperrt ist, das Verfügungslimit noch nicht ausgeschöpft ist und ob die Voraussetzungen des Verzichts auf die starke Authentifizierung vorliegen. Da die Voraussetzungen des kontaktlosen Bezahlens bei der von A eingesetzten EC-Karte vorliegen, ist kein entgegenstehender Wille der Berechtigten erkennbar, welcher zu überwinden ist. Das Kreditinstitut verzichtet vielmehr bewusst auf eine Prüfung der Berechtigung.[25]

Nach dieser Ansicht liegt keine unbefugte Verwendung von Daten vor.

(3) Betrugsspezifische Auffassung

Nach der sog. betrugsspezifischen Auffassung soll es darauf ankommen, ob das Verhalten Täuschungsäquivalenz aufweist. Dies ist dann der Fall, wenn der Verwendung der Daten eine Erklärung entnommen werden kann, die, wenn sie gegenüber einer natürlichen Person abgegeben worden wäre, Täuschungsgehalt gehabt hätte.[26]

---

[22] *Hefendehl/Noll*, in: MüKo-StGB, Bd. 5, 4. Aufl. 2022, § 263a Rn. 23 f.

[23] BGH NJW 1995, 669 (670); *Kindhäuser*, in: NK-StGB, Bd. 4, 6. Aufl. 2023, § 263a Rn. 27.

[24] Aus der Rechtsprechung z.B. OLG Celle NStZ 1989, 367; LG Freiburg NJW 1990, 2635 (2636), aus dem Schrifttum z.B. *Achenbach*, JR 1994, 293 (295); *Arloth*, Jura 1996, 354 (357 f.); *Neumann*, JuS 1990, 535.

[25] *Schrott*, JuS 2022, 138 (140).

[26] In diesem Sinne z.B. BGH JuS 2002, 506 (507); *Fischer*, Strafgesetzbuch mit Nebengesetzen, Kommentar, 70. Aufl. 2023, § 263a Rn. 11; *Perron*, in: Schönke/Schröder, Strafgesetzbuch, Kommentar, 30. Aufl. 2019, § 263a Rn. 9; *Wachter,* NStZ 2018, 241 (242); *Wessels/Hillenkamp/Schuhr,* Strafrecht, Besonderer Teil 2, 44. Aufl. 2021, Rn. 613.

Umstritten ist allerdings, zu welchem Ergebnis der betrugsspezifische Ansatz im vorliegenden Fall gelangt. Denkbar wäre es, zur Überprüfung der Täuschungsäquivalenz auf das Vorstellungsbild eines fiktiven Bankangestellten abzustellen, welcher die Interessen der Bank umfassend wahrnimmt und daher auch die Berechtigung des A überprüft, um die Bank gegen die Entstehung von Ansprüchen abzusichern.[27] Damit liefe die betrugsspezifische Auslegung im Ergebnis auf eine subjektivierende Auslegung hinaus, die Täuschungsäquivalenz der Verwendung der Daten wäre hier gegeben.

Das *OLG Hamm und* einige *Stimmen aus der Lit.* verneinen dagegen die Täuschungsäquivalenz der Datenverwendung beim kontaktlosen Bezahlen ohne PIN-Eingabe.[28] Entscheidend sei das Vorstellungsbild eines Schalterangestellten, der sich nur mit den Fragen befasse, die auch der Computer prüfe bzw. für die sich auch im Computerprogramm Ansätze zur Kontrolle fänden.[29] Weil bei dem konkreten Zahlungsvorgang die Voraussetzungen für den Verzicht auf eine weitere Legitimierung des Kartennutzers in Form der PIN-Eingabe vorlägen, würde auch der fiktive Bankangestellte neben dem Besitz der Karte nicht die Berechtigung des A prüfen, sondern lediglich die Sperrung der Karte oder die Ausschöpfung des Verfügungsrahmens.[30] Die Verwendung der Daten durch A habe daher nicht die erforderliche Täuschungsäquivalenz und sei folglich nicht unbefugt im Sinne des Tatbestands. In der Sache läuft diese Konkretisierung des betrugsspezifischen Ansatzes auf eine computerspezifische Betrachtung hinaus, weil für das Vorstellungsbild des fiktiven Schalterangestellten auf die in der Programmgestaltung angelegten Kontrollmechanismen abgestellt wird.

Denkbar ist schließlich noch eine *dritte Konkretisierung der betrugsspezifischen Auffassung* für den vorliegenden Fall. Entscheidend für die Frage der Täuschungsäquivalenz der Verwendung von Daten ist danach, welcher Erklärungswert der Vorlage der EC-Karte gegenüber einem hypothetischen Bankangestellten zukäme. Die Täuschungsäquivalenz der Verwendung der auf der EC-Karte gespeicherten Daten ohne Eingabe einer PIN ist demnach gegeben, wenn sich der Vorlage der EC-Karte gegenüber einer natürlichen Person ohne weiteren Legitimationsnachweis die Erklärung entnehmen ließe, der berechtigte Karteninhaber zu sein. Dies ist zu bejahen: Wer eine EC-Karte gegenüber einem Bankangestellten vorlegt, erklärt damit auch ohne weitere Erläuterung konkludent, der berechtigte Karteninhaber zu sein. Das ergibt sich daraus, dass der Name des Berechtigten auf der Karte eingeprägt ist und zugleich eine EC-Karte sowohl nach den Vertragsbedingungen, die zwischen der kartenausstellenden Bank und dem berechtigten Karteninhaber gelten, als auch nach laienhaften Verständnis der am Rechtsverkehr Beteiligten nur dann zur Auslösung von Zahlungsvorgängen eingesetzt werden darf, wenn man der berechtigte Karteninhaber ist oder doch zumindest durch den berechtigten Karteninhaber dazu bevollmächtigt wurde.[31] Demnach käme der Vorlage der EC-Karte gegenüber einem Bankangestellten Täuschungscharakter zu, so dass die Verwendung der auf der EC-Karte gespeicherten Daten auch ohne Eingabe der PIN täuschungsäquivalent ist. Eine unbefugte Datenverwendung liegt vor.

---

[27] Vgl. zur weiten betrugsspezifischen Auslegung etwa *Perron*, in: Schönke/Schröder, Strafgesetzbuch, Kommentar, 30. Aufl. 2019, § 263a Rn. 9.

[28] OLG Hamm NStZ 2020, 673 (674 f.); *Göhler*, JA 2021, 6 (19); *Heghmanns*, ZJS 2020, 494 (495); *Ceffinato*, JuS 2020, 311 (313).

[29] Vgl. zur engen betrugsspezifischen Auslegung BGH JuS 2002, 506 (507); BGH NStZ 2013, 281 (282); *Waßmer*, in: Leitner/Rosenau, Wirtschafts- und Steuerstrafrecht, 2. Aufl. 2022, § 263a Rn. 38 f.

[30] Vgl. zur Prüfung *Göhler*, JA 2021, 6 (17 f.).

[31] In diesem Sinne auch *Puschke/Haas*, Recht der Zahlungsdienste 2022, 4 (7 f.); *Schmidt*, in: BeckOK StGB, Stand: 1.2.2023, § 263a Rn. 29.

Hinweis: In der sorgfältigen Konkretisierung der betrugsspezifischen Auslegung auf den vorliegenden Fall liegt die eigentliche Schwierigkeit.

(4) Streitentscheid

Gegen den subjektivierenden Ansatz sprechen historische, systematische und übergeordnete teleologische Gründe. Der Tatbestand des Computerbetruges wurde 1986 eingeführt, um Handlungen zu erfassen, die, wenn sie nicht maschinell gesteuerte Geschehensabläufe auslösen würden, als Betrug gem. § 263 StGB zu bewerten wären.[32] Der neu geschaffene § 263a StGB sollte aber nicht den Bereich des strafbaren Verhaltens bei der Auslösung computergestützter Vermögensverfügungen im Vergleich zur Betrugsstrafbarkeit erweitern.[33] Eben dies wäre aber die Konsequenz einer Auslegung des Merkmals „unbefugt", die sich darin erschöpft, dass die Datenverwendung gegen den Willen des Berechtigten verstößt. Denn beim Betrug ist es nicht ausreichend, dass es gegen den Willen des Vermögensinhabers zu einer Vermögensverfügung und einem Vermögensschaden kommt. Vielmehr muss das tatbestandsmäßige Verhalten selbst noch eine spezifische, das tatbestandliche Unrecht prägende Qualität aufweisen, nämlich täuschenden Charakter haben. Die subjektivierende Auslegung des Merkmals „unbefugt" verzichtet darauf, für den Computerbetrug eine entsprechende Qualifikation des Verhaltens vorauszusetzen. Sie erfasst damit auch bloß vertragswidriges Verhalten. Dies läuft auch dem Ultima-Ratio-Prinzip zuwider, nach dem das Strafrecht nur zur Anwendung kommen soll, wenn andere Mittel nicht ausreichen.[34] Diese Argumente lassen sich auch einer weiten betrugsspezifischen Auslegung entgegenhalten, die eine Täuschungsäquivalenz des Verhaltens bereits dann bejaht, wenn fiktive Bankangestellte einen bestimmten Umstand bei einer umfassenden Wahrnehmung der Interessen der kartenausgebenden Bank überprüft hätten, weil dies im Interesse des Berechtigten lag. Auch diese Auffassung läuft letztlich darauf hinaus, jedes vertragswidrige Verhalten, das zu einem Vermögensschaden der Bank führt, in den Tatbestand einzubeziehen.

Gegen die computerspezifische Auslegung spricht, dass diese die aus systematischen Gründen gebotene Parallelität mit dem Betrugstatbestand nicht dadurch zu erreichen versucht, dass das tatbestandsmäßige Verhalten näher qualifiziert wird. Stattdessen wird auf mögliche Schutzmaßnahmen des Vermögensinhabers geschaut, die dieser in der Gestaltung der elektronischen Datenverarbeitungsprozesse hätte vorsehen können. Dieser viktimodogmatische Ansatz vernachlässigt, dass es anerkennenswerte Gesichtspunkte geben kann, die den Verzicht auf Kontrollmechanismen begründen. So verhält es sich gerade in dem vorliegenden Fall der Zahlung mit EC-Karte ohne starke Kundenauthentifizierung mittels Eingabe von PIN oder Unterschrift. Dadurch werden die Zahlungsvorgänge für alle Beteiligten schneller und bequemer, möglicherweise sprechen auch hygienische Gründe durch die Reduzierung von Kontaktflächen dafür – ein Argument, das in Pandemiezeiten zumindest in sozialpsychologischer Hinsicht Bedeutung entfaltet. Diese Überlegungen lassen sich auch einer Konkretisierung des betrugsspezifischen Auslegungsansatzes entgegenhalten, welche die Täuschungsäquivalenz der unberechtigten Verwendung von Daten danach bemisst, ob dabei Kontrollmechanismen überwunden werden, die in der Gestaltung des elektronischen Datenverarbeitungsvorgangs angelegt sind und damit im Ergebnis der computerspezifischen Auslegung entspricht.

---

[32] BGH StV 2014, 684 (685); *Rengier*, Strafrecht, Besonderer Teil I, 24. Aufl. 2022, § 14 Rn. 19.

[33] *Heger*, in: Lackner/Kühl/Heger, Strafgesetzbuch, Kommentar, 30. Aufl. 2023, § 263a Rn. 1.

[34] Vgl. zur Kritik *Rengier*, Strafrecht, Besonderer Teil I, 24. Aufl. 2022, § 14 Rn. 16; *Schmidt*, in: BeckOK StGB, Stand: 1.2.2023, § 263a Rn. 21; ebenso ablehnend *Perron*, in: Schönke/Schröder, Strafgesetzbuch, Kommentar, 30. Aufl. 2019, § 263a Rn. 9.

Überzeugen kann demnach allein eine betrugsspezifische Auslegung, die die Täuschungsäquivalenz einer unberechtigten Datenverwendung danach bemisst, ob in einem entsprechenden Verhalten gegenüber einer natürlichen Person die Täuschung über einen Umstand vorläge. Nur dieser Ansatz nimmt die systematisch gebotene Parallelisierung des Computerbetrugs mit dem Betrug wirklich ernst und berücksichtigt zugleich, dass es für die Begründung auf eine nähere Betrachtung des Verhaltens des Täters ankommt, nicht auf die Möglichkeit des Vermögensinhabers, weitere Schutzmechanismen computertechnisch vorzusehen. Wie bereits erläutert, ist danach bei der Bezahlung mittels EC-Karte die Täuschungsäquivalenz des Verhaltens zu bejahen, auch wenn keine Eingabe der PIN erforderlich ist, weil bereits in dem Einsatz der Karte für einen Bezahlvorgang die konkludente Erklärung liegt, der berechtigte Karteninhaber oder doch zumindest durch diese zum Karteneinsatz bevollmächtigt worden zu sein.[35]

Hinweis: A.A. vertretbar. Entscheidend ist nicht das Ergebnis, sondern die Subsumtion des konkreten Falls.

(5) Zwischenergebnis

Durch das kontaktlose Bezahlen mit der EC-Karte des V hat unbefugt Daten i.S.d. § 263a Abs. 1 Var. 3 StGB verwendet.

cc) Beeinflussung des Ergebnisses eines Datenverarbeitungsvorgangs

Durch die unbefugte Verwendung beeinflusst T das Ergebnis des elektronischen Zahlungsvorgangs als Datenverarbeitungsvorgang, den K für die R-GmbH eingeleitet hat. Denn er bewirkt dadurch, dass die vom Zahlungssystem der R-GmbH erstellte Autorisierungsanfrage mit den Kontodaten des V vervollständigt wird und in dieser Form an das Zahlungssystem der Sparkasse Göttingen gesendet wird.

dd) Vermögensschaden

Infolge der unbefugten Datenverwendung müsste ein Schaden eingetreten sein.
Die Beeinflussung des Datenverarbeitungsvorgangs im Zahlungssystem *führte zu* einer Autorisierung des Zahlungsvorgangs und damit zum Erwerb einer einredefreien Forderung der R-GmbH gegen die Sparkasse Göttingen. Dadurch trat auch ein Vermögensschaden bei der Sparkasse ein, weil diese keinen Aufwendungsersatzanspruch gegen V erwarb.

Zugleich wird durch die Auslösung des Zahlungsvorgangs unmittelbar das Konto von V mit dem Rechnungsbetrag belastet. Zwar kann V diese Belastung wieder rückgängig machen, indem er der Sparkasse gegenüber anzeigt, dass die Belastung infolge eines nicht-autorisierten Zahlungsvorgangs erfolgte, vgl. § 675u BGB. Weil der Zahlungsvorgang durch T ausgelöst werden konnte, ohne dass eine starke Kundenauthentifizierung durch Eingabe der PIN erforderlich war, steht der Sparkasse gem. § 675v Abs. 4 Nr. 1 BGB auch kein Ersatzanspruch gegen V gem. § 675v Abs. 1 BGB zu. Dennoch bedarf es aber eines Tätigwerdens des V, um die Belastung seines Kontos rückgängig zu machen. Darin liegt bei wirtschaftlicher Betrachtungsweise bereits eine Verschlechterung seiner gegenwärtigen Vermögenslage und mithin ein Gefährdungsschaden in Höhe des Rechnungsbetrages.

[35] So auch *Schmidt*, in: BeckOK StGB, Stand: 1.2.2023, § 263a Rn. 29; a.A. *Christoph*, ZJS 2022, 761 (767).

b) Subjektiver Tatbestand

aa) Vorsatz

A müsste vorsätzlich gehandelt haben. Unschädlich ist, dass er keine genauere Kenntnis über den technischen Ablauf und die rechtliche Ausgestaltung des Zahlungsvorgangs hatte. Jedenfalls im Sinne einer Parallelwertung in der Laiensphäre war ihm bewusst, dass er durch den Einsatz der Karte unbefugt Daten der Karte verwendete, dadurch einen Datenverarbeitungsvorgang der Bank bewirkte und das Vermögen eines anderen beschädigte. Vorsatz liegt somit vor.

bb) Absicht rechtswidriger und stoffgleicher Bereicherung

Fraglich ist allerdings, ob A mit der Absicht rechtswidriger und stoffgleicher Bereicherung handelte. Voraussetzung ist demnach, dass A nach einem Vermögensvorteil strebte. Rechtswidrig ist die von ihm beabsichtigte Bereicherung, wenn er keinen einredefreien und fälligen Anspruch auf die Bereicherung hatte.[36] Stoffgleichheit liegt vor, wenn die beabsichtigte Bereicherung sich als die Kehrseite des herbeigeführten Schadens darstellt, also insbesondere unmittelbar durch dieselbe Vermögensverfügung vermittelt wird, auf der auch der Schaden beruht.[37]

Als angestrebte (und auch erlangte) Bereicherung kommt zunächst die Übergabe und Übereignung der im Supermarkt gekauften Waren in Betracht. Diese Bereicherung war auch rechtswidrig: A beglich nicht die Kaufpreisforderung der R-GmbH, sondern erweckte durch den Einsatz der fremden EC-Karte lediglich den Anschein, dies zu tun. Er hatte daher auch keinen Anspruch auf Übergabe und Übereignung der Waren. Dies war dem A auch bewusst, sodass er hinsichtlich der Rechtswidrigkeit der beabsichtigten Bereicherung mit Vorsatz gehandelt hat.

Problematisch erscheint allerdings die Stoffgleichheit zwischen dem Vermögensschaden und der angestrebten Bereicherung. Der Vermögensschaden entsteht bei der Sparkasse, der angestrebte Vermögenszuwachs fließt A dagegen aus dem Vermögen der R-GmbH mittels einer Verfügung des K zu. Es ist jedoch zu berücksichtigen, dass der Vermögensschaden der Sparkasse das unmittelbare Resultat des Bezahlvorgangs an der Kasse der Supermarkt-Filiale der R-GmbH ist.[38] Im Zuge dieses Vorgangs findet auch die Besitzübertragung und Übereignung der Waren durch K als Vertreter der R-GmbH statt. Obgleich die Digitalisierung des Zahlungsvorgangs dazu führt, dass – für A im Zweifel nicht einmal erkennbar – weitere (juristische) Personen involviert sind und Vermögensverfügungen vornehmen, bildet die beabsichtigte Bereicherung (Erhalt der Waren) daher die Kehrseite[39] des vorsätzlich herbeigeführten Vermögensschadens bei der Sparkasse. Vorteil und Schaden beruhen mithin auf derselben Verfügung[40], sodass die Stoffgleichheit im Ergebnis vorliegt.

Hinweis: In den bislang vorliegenden Besprechungen der Fallkonstellation wird das Problem der Stoffgleichheit nicht vertieft, obgleich die Bewertung keineswegs eindeutig erscheint. Wird eine Stoffgleichheit zwischen dem Vermögensschaden der R-GmbH und der von A angestrebten eigennützigen Bereicherung durch den Erhalt der Waren verneint, ist nicht erkennbar, wie sich sonst eine

[36] Zur Rechtswidrigkeit *Saliger*, in: Matt/Renzikowski, Strafgesetzbuch, Kommentar, 2. Aufl. 2020, § 263 Rn. 289.
[37] Zur Stoffgleichheit *Perron*, in: Schönke/Schröder, Strafgesetzbuch, Kommentar, 30. Aufl. 2019, § 263 Rn. 168; BGH NStZ 2003, 264 (264).
[38] Vgl. zum Erfordernis der Unmittelbarkeit BayObLG NStZ 1994, 491 (492); *Jäger*, JuS 2010, 761 (765); *Kindhäuser*, in: NK-StGB, Bd. 4, 6. Aufl. 2023, § 263 Rn. 360.
[39] Vgl. BGH NStZ 2015, 89 (92).
[40] Vgl. *Perron*, in: Schönke/Schröder, Strafgesetzbuch, Kommentar, 30. Aufl. 2019, § 263 Rn. 168

stoffgleiche, rechtswidrige Bereicherungsabsicht begründen lässt. Zwar lässt sich argumentieren, dass A als notwendiges Zwischenziel auch die Drittbereicherung der R-GmbH anstrebt.[41] Allerdings ist diese Bereicherung nicht rechtswidrig, weil der R-GmbH nach der zivilrechtlichen Ausgestaltung der Rechtsverhältnisse tatsächlich ein einredefreier und fälliger Anspruch gegen die Sparkasse zustand, auch wenn der Zahlungsvorgang durch A als nichtberechtigten Dritten ausgelöst wurde.[42]

2. Rechtswidrigkeit und Schuld

A handelte rechtswidrig und schuldhaft.

3. Ergebnis

A hat sich wegen Computerbetruges gem. § 263a Abs. 1 Var. 3 StGB strafbar gemacht.

III. Fälschung beweiserheblicher Daten gem. § 269 Abs. 1 StGB i.V.m. § 270 StGB

Durch die Verwendung der EC-Karte könnte A beweiserhebliche Daten gem. § 269 Abs. 1 StGB i.V.m. § 270 StGB gefälscht haben.

1. Tatbestandsmäßigkeit

a) Objektiver Tatbestand

aa) Veränderung oder Speicherung beweiserheblicher Daten

A müsste beweiserhebliche Daten zur fälschlichen Beeinflussung einer Datenverarbeitung im Rechtsverkehr gespeichert oder verändert haben. Als beweiserhebliche Daten kommen die Datensätze der Autorisierungsanfrage in Betracht, die an das Zahlungssystem der Sparkasse Göttingen übermittelt wird. Die Autorisierungsanfrage beinhaltet, wie bereits festgestellt, Daten, vgl § 202a Abs. 2 StGB. Diese sind auch beweiserheblich, weil sie dazu bestimmt sind, einen elektronischen Zahlungsvorgang dem Konto des berechtigten Karteninhabers zuzuordnen.[43] Zur Übermittlung der Autorisierungsanfrage an das Zahlungssystem der kartenausstellenden Bank müssen die Daten auch (zwischen)gespeichert werden.

bb) Dadurch Herstellung einer unechten Datenurkunde

Die beweiserheblichen Daten müssten so verändert oder gespeichert werden, dass bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde vorliegen würde.[44] D.h. durch den gespeicherten

[41] Vgl. etwa Provisionsvertreterfälle *Duttge*, in: Dölling u.a., Handkommentar, Gesamtes Strafrecht, 5. Aufl. 2022, § 263 Rn.82; OLG Braunschweig NJW 1961, 1272 (1273); OLG Saarbrücken NJW 1968, 262 (263).

[42] Bei einem wirksamen, fälligen und einredefreien Anspruch fehlt es an der Rechtswidrigkeit, siehe *Hefendehl*, in: MüKo-StGB, Bd. 5, 4. Aufl. 2022, § 263 Rn. 1157. Das wird für die vorliegende Konstellation übersehen von *Puschke/Haas*, Recht der Zahlungsdienste 2022, 4 (7).

[43] Vgl. zur Beweiserheblichkeit von Daten z.B. *Maier*, in: Matt/Renzikowski, Strafgesetzbuch, Kommentar, 2. Aufl. 2020, § 269 Rn. 5 ff.; zur Erfassung von Codekarten *Weidemann*, in: BeckOK StGB, Stand: 1.2.2023, § 269 Rn. 5 ff.; zustimmend *Christoph*, ZJS 2022, 761 (768).

[44] *Koch*, in: Dölling u.a., Handkommentar, Gesamtes Strafrecht, 5. Aufl. 2022, § 269 Rn. 5; *Heger*, in: Lackner/Kühl/Heger, Strafgesetzbuch, Kommentar, 30. Aufl. 2023, § 269 Rn. 2.

oder veränderten Datensatz muss eine sog. unechte Datenurkunde hergestellt werden, also ein Datensatz, der im Falle einer Verkörperung alle Merkmale einer unechten Urkunde im Sinne der Urkundenfälschung gem. § 267 Abs. 1 StGB aufwiese. Der veränderte Datensatz müsste also, wenn er als Gedankenerklärung verkörpert wäre, einen anderen Aussteller erkennen lassen als den tatsächlichen Aussteller.

(1) Ansicht des OLG Hamm

Diese Voraussetzung hat das OLG Hamm für die Vornahme eines kontaktlosen Bezahlvorgangs durch einen nichtberechtigten Dritten verneint. In der Entscheidung heißt es:

> „Zwar werden bei dem Einsatz einer EC-Karte im POS-Verfahren am Kartenlesegerät die Transaktionsdaten (z.B. Kontonummer und Gültigkeitsdatum der EC-Karte) als Gedankenerklärung in das Autorisierungssystem eingelesen. Allerdings ist in Bezug auf die Transaktionsdaten bei den hier vorliegenden kontaktlosen Zahlungen mittels EC-Karte ohne PIN-Abfrage die Garantiefunktion des Urkundenbegriffs nicht erfüllt. Diese erfordert, dass der vermeintliche Aussteller der Gedankenerklärung erkennbar ist. An einer solchen eindeutigen Identifikationsmöglichkeit fehlt es aber mangels PIN-Abfrage."[45]

Das OLG meint, dass die Übermittlung der auf der EC-Karte gespeicherten Daten an das Zahlungssystem zwar eine Gedankenerklärung sei. Es fehle aber mangels PIN-Eingabe ein Aussteller dieser Gedankenerklärung, der im Rechtsverkehr für die Richtigkeit dieser Gedankenerklärung einstehen will.[46]

(2) Kritik der Literatur

In der Literatur haben diese Ausführungen vielfach Kritik erfahren. Das OLG Hamm überspanne die Anforderungen an die Erkennbarkeit eines Ausstellers dieser Gedankenerklärung. Bei dem Einsatz einer EC-Karte erscheine der berechtigte Karteninhaber stets als vermeintlicher Aussteller der Transaktionsdaten.[47] Das gelte auch dann, wenn sich der Kartennutzer nicht durch PIN-Eingabe legitimiere. Denn nach den Vertragsbedingungen zur Verwendung der EC-Karte sei diese „höchstpersönlich", d.h. die Karte dürfe vom berechtigten Karteninhaber nicht anderen überlassen werden. Die Verkehrsanschauung rechne daher dem berechtigten Karteninhaber alle mit der EC-Karte ausgelösten Zahlungsanweisungen als Aussteller zu,[48] auch solche, die nicht durch PIN-Eingabe noch einmal gesondert authentifiziert werden. Daher liege in allen Fällen, in denen jemand mit einer fremden EC-Karte ohne Bevollmächtigung des berechtigten Karteninhabers Zahlungsvorgänge auslöse oder Geld vom Bankautomaten abhebe, eine Fälschung beweiserheblicher Daten gem. § 269 StGB.[49]

---

[45] OLG Hamm NStZ 2020, 673 (675). Vgl. zur Garantiefunktion bei § 269 StGB *Kindhäuser*, in: NK-StGB, Bd. 4, 6. Aufl. 2023, § 269 Rn. 6.

[46] Zustimmend *Göhler*, JA 2021, 6 (20 f.); *Schrott*, JuS 2022, 138 (140 f.); *Ladiges*, WuB 2020, 600 (604).

[47] *Christoph/Dorn-Haag*, NStZ 2020, 697 (699); *Kulhanek*, wistra 2021, 220 (223 f.); *Puschke/Haas*, Recht der Zahlungsdienste 2022, 4 (10).

[48] Vgl. *Christoph*, ZJS 2022, 761 (770).

[49] Bejahend ebenso *Rengier*, Strafrecht, Besonderer Teil II, 23. Aufl. 2022, § 35 Rn. 8; *Erb*, in: MüKo-StGB, Bd. 5, 4. Aufl. 2022, § 269 Rn. 35.

(3) Stellungnahme

Die an den Ausführungen des OLG Hamm geäußerte Kritik in der Literatur überzeugt nicht. Sie unterscheidet nicht hinreichend zwischen dem konkludenten Erklärungswert, der dem Bezahlen mit der EC-Karte als menschlicher Handlung (hier: des A) gegenüber dem Kassenpersonal (hier: K) zukommt, und den in den Daten verkörperten Gedankenerklärungen. Zutreffend ist, dass mit dem Einsatz einer EC-Karte schlüssig erklärt wird, der dazu berechtigte Karteninhaber zu sein (vgl. oben). Der automatisierte Transfer des Datensatzes von der EC-Karte ohne Authentifizierung durch eine PIN ist davon aber zu unterscheiden. Dieser maschinelle Vorgang enthält keine eigenständige Gedankenerklärung, als deren Aussteller der berechtigte Karteninhaber erkennbar wäre. Vielmehr vervollständigen die Daten lediglich eine Autorisierungsanfrage, die durch das Zahlungssystem des Verkäufers (hier: der R-GmbH) erstellt wird.[50] Erst in dieser Autorisierungsanfrage liegt eine Datenurkunde. Deren erkennbare und auch tatsächliche Ausstellerin ist die R-GmbH. Die durch A bewirkte Datenübertragung an das Kartenlesegerät gleicht insofern einem Schriftstück, in das eine Person Daten einträgt, das dann aber durch eine andere Person hinsichtlich seiner Richtigkeit im Rechtsverkehr als Aussteller verantwortet wird. Erst bei einer Eingabe der PIN würde der Kartennutzer Authentizität des zwischengespeicherten Datensatzes reklamieren und damit Mitaussteller der Autorisierungsanfrage werden.

b) Zwischenergebnis

Indem A die Übertragung der auf der EC-Karte gespeicherten Daten bewirkt, verändert oder speichert er für sich betrachtet noch keine beweiserheblichen Daten. Eine Speicherung beweiserheblicher Daten erfolgt erst durch das Zahlungssystem der R-GmbH im Rahmen der Erstellung der Autorisierungsanfrage an das Zahlungssystem der Sparkasse. Die Autorisierungsanfrage ist aber eine echte Datenurkunde, weil der aus dem Datensatz hervortretende Aussteller (die R-GmbH) mit dem tatsächlichen Austeller übereinstimmt. Mangels unechter Datenurkunde ist der objektive Tatbestand des §§ 269 Abs. 1, 270 StGB somit nicht erfüllt.

Hinweis: A.A. vertretbar. Werden die objektiven Voraussetzungen bejaht, ist im Rahmen des subjektiven Tatbestandes festzustellen, dass A zumindest im Sinne einer Parallelwertung in der Laiensphäre bewusst war, dass durch den bewirkten Zahlungsvorgang Daten übertragen oder verändert werden, welche sodann die Grundlage für eine Autorisierung durch die kartenausstellende Bank (Zahlung erfolgt) bilden. A handelte vorsätzlich sowie mit der Absicht zur Täuschung im Rechtsverkehr bzw. zur fälschlichen Beeinflussung eines Datenverarbeitungsvorgangs im Rechtsverkehr.[51] Ebenso handelte er rechtswidrig und schuldhaft.

2. Ergebnis

A hat sich nicht wegen Fälschung beweiserheblicher Daten gem. §§ 269 Abs. 1, 270 StGB strafbar gemacht.

---

[50] So zutreffend *Heghmanns*, ZJS 2020, 494 (496 f.).

[51] Bedingter Vorsatz genügt vgl. etwa *Heine/Schuster*, in: Schönke/Schröder, Strafgesetzbuch, Kommentar, 30. Aufl. 2019, § 269 Rn. 22; *Weidemann*, in: BeckOK StGB, Stand: 1.2.2023, § 269 Rn. 12.

IV. Urkundenunterdrückung gem. § 274 Abs. 1 Nr. 2 StGB

Durch dieselbe Handlung kommt eine Strafbarkeit wegen Urkundenunterdrückung gem. § 274 Abs. 1 Nr. 2 StGB in Betracht.

1. Tatbestandsmäßigkeit

a) Objektiver Tatbestand

Der von A mit der EC-Karte des V bewirkte Zahlungsvorgang könnte zu einer Veränderung und Anpassung von Daten im Zahlungssystem der Sparkasse Göttingen geführt haben. Zum einen wird der Verfügungsrahmen des Kontoinhabers angepasst, zum anderen werden die Daten aktualisiert, die erforderlich sind, um bei dem nächsten Zahlungsvorgang zu überprüfen, ob erneut die Voraussetzungen für den Verzicht auf die PIN-Eingabe vorliegen, also die Anzahl der vorangegangenen Zahlungsvorgänge ohne Eingabe der PIN und der Gesamtbetrag dieser Zahlungsvorgänge. Beweiserheblich sind diese Daten, weil sie für die Autorisierung weiterer Bezahlvorgänge mit der EC-Karte relevant sind.

A hatte als nichtberechtigter Kartennutzer über diese Daten kein Verfügungsrecht. Beweisführungsrechte an diesen Daten bestanden vielmehr auf Seiten des berechtigten Karteninhabers und des Kartenausstellers.[52]

Die Voraussetzungen des objektiven Tatbestands liegen somit vor.[53]

b) Subjektiver Tatbestand

aa) Vorsatz

Da A zumindest im Sinne einer Parallelwertung in der Laiensphäre bewusst war, dass durch den elektronischen Zahlungsvorgang Daten verändert werden, die zur Beweisführung durch andere Personen bestimmt waren, handelte er vorsätzlich.[54]

bb) Nachteilzufügungsabsicht

Zweifelhaft ist allerdings, ob A mit der tatbestandlich vorausgesetzten Absicht handelte, einem anderen einen Nachteil zuzufügen. Hierfür soll nach ganz überwiegender Ansicht sicheres Wissen um den Nachteilseintritt im Sinne von dolus directus zweiten Grades genügen.[55] Für die vorliegende Fallkonstellation haben daher das OLG Hamm und zahlreiche Stimmen aus der Literatur die Nachteilszufügungsabsicht angenommen, wenn der nichtberechtigte Kartennutzer weiß, dass er durch den elektronischen Zahlungsvorgang an einer Veränderung von Datensätzen mitwirkt, und diese Datensätze dann auch für die Autorisierung weiterer Zahlungsvorgänge relevant sind.[56]

---

[52] Ebenso OLG Hamm NStZ 2020, 673 (675); *Göhler*, JA 2021, 6 (21).

[53] Vgl. zur Überschreibung des ursprünglichen Verfügungsrahmen auch *Christoph*, ZJS 2022, 761 (770).

[54] Vgl. zum Vorsatz *Heine/Schuster*, in: Schönke/Schröder, Strafgesetzbuch, Kommentar, 30. Aufl. 2019, § 274 Rn. 13.

[55] BGH NStZ 2010, 332 (333); *Heinrich*, in: Arzt u.a., Strafrecht, Besonderer Teil, 4. Aufl. 2021, § 33 Rn. 34; *Wessels/Hettinger/Engländer*, Strafrecht, Besonderer Teil 1, 46. Aufl. 2022, Rn. 883; A.A. *Erb*, in: MüKo-StGB, Bd. 5, 4. Aufl. 2022, § 274 Rn. 18 f.

[56] OLG Hamm NStZ 2020, 673 (676).

Diese Argumentation erscheint aus mehreren Gründen nicht überzeugend. Zum einen setzt die Nachteilszufügungsabsicht damit nicht mehr voraus als schon der Tatbestandsvorsatz hinsichtlich Veränderung beweiserheblicher Daten. Die Auslegung verstößt daher gegen das vom Bundesverfassungsgericht aus dem Bestimmtheitsgrundsatz abgeleitete Verschleifungsverbot.[57]

Zudem ist aber auch nicht erkennbar, dass die durch A bewirkte Datenveränderung zu einer Verschlechterung der Beweissituation der Sparkasse Göttingen oder des berechtigten Karteninhabers V als den Beweisführungsberechtigten führt. A beabsichtigt – im Sinne zielgerichteten Wollens – die Herbeiführung eines Vermögensschadens durch Vornahme des Zahlungsvorgangs, wobei er im Zweifel keine genaue Vorstellung hat, ob dieser Vermögensschaden letztlich bei V, der R-GmbH oder der Sparkasse Göttingen eintritt. Dieser Nachteil soll aber nicht durch die Veränderung fremder beweiserheblicher Daten bewirkt werden. Die Veränderung fremder beweiserheblicher Daten ist vielmehr ein Reflex der erfolgreichen Vermögensbeeinträchtigung.

Aus der Veränderung der Datensätze erwächst dagegen weder V noch der kartenausstellenden Sparkasse Göttingen ein Nachteil bei der Beweisführung. Die durch den Einsatz der Karte bewirkte Veränderung der Datensätze, die zu der EC-Karte im Zahlungssystem gespeichert werden, verbessert vielmehr die Beweissituation der Beweisführungsbefugten. Das Beweisinteresse der Sparkasse an den im Rahmen dieses Vorgangs veränderten Daten besteht darin, diese bei weiteren Zahlungsvorgängen zur Überprüfung nutzen zu können, ob erneut auf die PIN-Eingabe verzichtet werden kann, ggf. auch darin, gegenüber dem nichtberechtigten Kartennutzer Schadenersatzansprüche geltend machen zu können. Dazu bedarf es jeweils gerade der Anpassung der Datensätze, nicht der Erhaltung des Status quo. Auch das Interesse des berechtigten Karteninhabers hinsichtlich der gespeicherten Daten besteht vor allem darin, dass möglichst keine weiteren unbefugten Zahlungen mit der EC-Karte bewirkt werden können und dass zudem die Möglichkeit besteht, durch die gespeicherten Datensätze unbefugt bewirkte Zahlungen zu erkennen und gegenüber der kartenausstellenden Bank zu melden, so dass die Belastung des Kontos erstattet wird. Dieses Interesse wird ebenfalls nicht durch den Erhalt des Status quo an den Daten gesichert, sondern gerade durch die Anpassung.

Im Ergebnis sprechen daher – entgegen der Entscheidung des OLG Hamm und der überwiegenden Ansicht in der Literatur – die besseren Gründe gegen das Vorliegen einer Nachteilszufügungsabsicht.[58]

2. Ergebnis

Mangels Nachteilszufügungsabsicht hat sich A nicht wegen Urkundenunterdrückung gem. § 274 Abs. 1 Nr. 2 StGB strafbar gemacht.

V. Missbrauch von Scheck- und Kreditkarten gem. § 266b Abs. 1 StGB

Da die EC-Karte dem V überlassen wurde, scheidet eine Strafbarkeit aus. A als Nichtberechtigter kann nicht Täter des § 266b Abs. 1 StGB sein.[59]

[57] Vgl. zum Verschleifungsverbot BVerfGE 126, 170 (198).

[58] Ablehnend auch *Heghmanns*, ZJS 2020, 494 (497); *Puschke/Haas*, Recht der Zahlungsdienste 2022, 4 (10).

[59] *Kudlich*, JA 2020, 710 (712); *Maier*, in: Matt/Renzikowski, Strafgesetzbuch, Kommentar, 2. Aufl. 2020, § 266b Rn. 12; OLG Hamm NStZ 2020, 673 (675).

VI. Datenveränderung gem. § 303a Abs. 1 StGB

1. Tatbestandsmäßigkeit

A müsste rechtswidrig Daten i.S.d. § 202a Abs. 2 StGB verändert haben. Eine Veränderung von Daten liegt vor, siehe oben.

Fraglich ist, ob diese Datenveränderung auch rechtswidrig war. Die Rechtswidrigkeit ist hierbei als einschränkendes unrechtsbegründendes Merkmal und nicht als Verweis auf die allgemeinen Rechtfertigungsgründe zu verstehen.[60]

Wann eine Datenveränderung rechtswidrig im Sinne der Vorschrift ist, ist umstritten. Ein Ansatz stellt darauf ab, dass es sich um fremde Daten handeln müsse, d.h. dass einer anderen Person das eigentümerähnliche Verfügungsrecht an den Daten zusteht.[61] Nach anderer Auffassung ist darüber hinaus zusätzlich erforderlich, dass an dem unveränderten Zustand ein rechtlich anerkennenswertes Interesse besteht.[62] Nur die letztgenannte Auffassung wird verfassungsrechtlichen Anforderungen gerecht, weil der Einsatz des Strafrechts zum Schutz eines gegenwärtigen Zustands von Daten nur dann verhältnismäßig ist, wenn es ein schützenswertes Interesse am Erhalt des Status quo gibt.[63] Für die Datensätze, die durch die Vornahme des kontaktlosen Zahlungsvorgang im Zahlungssystem der kartenausstellenden Sparkasse verändert werden, lässt sich ein solches schützenswertes Interesse nicht benennen. Denn wie bereits zu der Frage der Nachteilszufügungsabsicht gem. § 274 Abs. 1 Nr. 2 StGB ausgeführt, besteht das schützenswerte Interesse von Bank und berechtigten Karteninhaber, dass die Karte nicht unbefugt von Dritten für elektronische Zahlungsvorgänge eingesetzt wird. Es besteht aber kein schützenswertes Interesse daran, dass infolge dieses Einsatzes keine Datensätze verändert und abgespeichert werden. Die Dokumentation des Karteneinsatzes und die Anpassung der Daten, die zur Überprüfung der Möglichkeit eines erneuten Verzichts auf die PIN-Eingabe erforderlich sind, liegen vielmehr im Interesse derjenigen, die datenverfügungsbefugt sind.[64]

2. Ergebnis

Mangels Rechtswidrigkeit der Datenveränderung, hat sich A nicht wegen Datenveränderung gem. § 303a Abs. 1 StGB strafbar gemacht.

Hinweis: A.A vertretbar. Wird eine Strafbarkeit gem. § 274 Abs. 1 Nr. 2 StGB angenommen, erfüllt das Verhalten des A auch den Tatbestand der Datenveränderung. Diese tritt aus Gründen der Spezialität jedoch hinter der Datenunterdrückung zurück.[65]

---

[60] Vgl. *Eisele*, Strafrecht, Besonderer Teil II, 6. Aufl. 2021, Rn. 504; *Heger*, in: Lackner/Kühl/Heger, Strafgesetzbuch, Kommentar, 30. Aufl. 2023, § 303a Rn. 4

[61] *Heger*, in: Lackner/Kühl/Heger, Strafgesetzbuch, Kommentar, 30. Aufl. 2023, § 303a Rn. 4.

[62] *Hecker*, in: Schönke/Schröder, Strafgesetzbuch, Kommentar, 30. Aufl. 2019, § 303a Rn. 3 m.w.N.

[63] *Hilgendorf*, in: Satzger/Schluckebier/Widmaier, Strafgesetzbuch, Kommentar, 5. Aufl. 2020, § 303a Rn. 5 f.; *Wessels/Hillenkamp/Schuhr*, Strafrecht, Besonderer Teil 2, 44. Aufl. 2021, Rn. 61.

[64] So auch *Heghmanns*, ZJS 2020, 494 (498).

[65] Vgl. zur Subsidiarität des § 303a StGB *Altenhain*, in: Matt/Renzikowski, Strafgesetzbuch, Kommentar, 2. Aufl. 2020, § 303a Rn. 14; *Wieck-Noodt*, in: MüKo-StGB, Bd. 5, 4. Aufl. 2022, § 303a Rn. 23; *Heghmanns*, ZJS 2020, 494 (497).

VII. Unterschlagung gem. § 246 Abs. 1 StGB

Da A die ganze Zeit beabsichtigte, die EC-Karte wieder an V bzw. die Sparkasse Göttingen zurückgelangen zu lassen, liegt in dem Einsatz der Karte für die Vornahme des kontaktlosen Zahlungsvorgangs keine Zueignung, sondern lediglich eine straflose Gebrauchsanmaßung.[66] Die im Supermarkt erworbenen Waren werden dagegen durch K in Vertretung der R-GmbH an A übereignet, so dass sich die Zueignung nicht auf fremde Sachen bezieht.

Gesamtergebnis

A ist strafbar wegen Computerbetrugs gem. § 263a Abs. 1 Var. 3 StGB. Der gem. §§ 263a Abs. 2, 263 Abs. 4 StGB i.V.m. § 248a StGB erforderliche Strafantrag liegt vor.

Hinweis: Wird zusätzlich eine Strafbarkeit gem. § 269 Abs. 1 StGB und gem. § 274 Abs. 1 Nr. 2 StGB bejaht, stehen diese Tatbestände in Idealkonkurrenz/Handlungseinheit nach § 52 StGB zueinander.

[66] Vgl. *Kindhäuser*, in: NK-StGB, Bd. 4, 6. Aufl. 2023, § 246 Rn. 33.