E n t s c h e i d u n g s a n m e r k u n g

Kontaktloses Bezahlen mit EC-Karte ohne PIN-Abfrage

1. Löst ein Nichtberechtigter mit einer EC-Karte kontaktlos einen elektronischen Zahlungsvorgang aus und fragt das kartenemittierende Kreditinstitut im Zuge der Abwicklung des Zahlungsvorgangs im „Point-of-sale-Verfahren" die zu der Karte gehörende Geheimnummer (PIN) nicht ab, verwirklicht dieses Verhalten mangels Täuschung nicht den Betrugstatbestand gemäß § 263 Abs. 1 StGB.
2. Ein solches Verhalten verwirklicht auch nicht – mangels Betrugsähnlichkeit – die Tatbestände des Computerbetruges gemäß § 263a Abs. 1 StGB und – mangels Vorliegens einer „Datenurkunde" – der Fälschung beweiserheblicher Daten gemäß §§ 269 Abs. 1, 270 StGB.
3. Ein solches Verhalten kann aber als Urkundenunterdrückung gemäß § 274 Abs. 1 Nr. 2 StGB sowie nachrangig als Datenveränderung gemäß § 303a Abs. 1 StGB strafbar sein. Insbesondere für die Verwirklichung des § 274 Abs. 1 Nr. 2 StGB ist allerdings in subjektiver Hinsicht zumindest eine laienhafte Vorstellung von den technischen Abläufen einer kontaktlosen Zahlung im POS-Verfahren erforderlich.
(Amtliche Leitsätze)

StGB §§ 263, 263a, 269, 270, 274
ZAG § 55

OLG Hamm, Beschl. v. 7.4.2020 – 4 RVs 12/20 (LG Paderborn)[1]

I. Einführung

Kontaktloses Bezahlen an der Supermarktkasse ist in Zeiten gesteigerter Infektionsgefahren nicht nur bequem, sondern auch erwünscht. Technisch geschieht dies mittels des NFC-Verfahrens[2] per elektromagnetischer Induktion auf die kurze Entfernung von wenigen Zentimetern zwischen EC-Karte und Lesegerät.[3] Hierbei identifiziert das Lesegerät die vorgehaltene EC-Karte, um sodann zu überprüfen, ob für diese Karte eine Sperre eingetragen oder der Verfügungsrahmen überschritten wird.[4] Ist das nicht der Fall, kann der Bezahlvorgang erfolgen. Zur Steigerung der Bequemlichkeit sind die kartenausgebenden Institute zudem dazu übergegangen, auf die bis dahin erforderliche Kontrolle der Berechtigung der kartenvorlegenden Person qua Abfrage einer (gewöhnlich nur dem Berechtigten bekannten) PIN[5] zu verzichten, sofern der Zahlungsvorgang unter der Schwelle von 25,- € bleibt. Missbrauchsmöglichkeiten durch unberechtigte Kartenbesitzer (Diebe, Hehler oder wie hier den Finder einer verloren gegangenen EC-Karte), die fremde Karten ohne weiteres zur Bezahlung kleinerer Einkäufe nutzen können, solange der Berechtigte die Karte noch nicht hat sperren lassen, liegen auf der Hand. Die strafrechtliche Erfassung solcher unberechtigt initiierter Bezahlvorgänge bereitet offenbar Schwierigkeiten, wie die hier zu besprechende Entscheidung des OLG Hamm aufdeckt, die auf der Basis einer sorgfältigen Durchsicht und Erörterung der in Betracht kommenden Strafvorschriften zu einem überraschenden (und angreifbaren) Schuldspruch wegen Urkundenunterdrückung gelangt. Das Ergebnis muss man nicht teilen, aber die Entscheidung bleibt in jedem Fall lehrreich und für eine fundierte Examensvorbereitung lesenswert.

II. Sachverhalt

Nach den vom *Senat* nicht beanstandeten Feststellungen der Berufungsstrafkammer (kleine Strafkammer) des Landgerichts war der Angeklagte durch seine Freundin K in den Besitz einer am 15.12.2018 gegen 11.00 Uhr von dem Eigentümer A verlorenen Geldbörse gelangt, in welcher sich u.a. die EC-Karte einer Sparkasse befand. Im Bewusstsein fehlender Berechtigung nutzte der Angeklagte am selben Tag zwischen 12.59 Uhr und 13.07 Uhr die besagte Karte zur Bezahlung von vier Einkäufen in einem Supermarkt und einem zugehörigen Getränkemarkt. Da die Rechnungsbeträge jeweils unter 25,- € lagen, konnte der Angeklagte die fremde EC-Karte auf das Kartenlesegerät auflegen und so ohne weitere Abfrage einer PIN den Bezahlungsvorgang zu Lasten der Sparkasse und zu Gunsten des Marktes auslösen, wodurch der Markt einen einredefreien Zahlungsanspruch in Höhe des Rechnungsbetrages gegen die Sparkasse erlangt hat.[6]

III. Die Entscheidung des Senats

Im Hinblick auf dieses geschilderte Geschehen war der Angeklagte vom Strafrichter in Paderborn wegen Computerbetruges in vier Fällen (§§ 263a, 248a, 53 StGB) zu einer Gesamtfreiheitsstrafe von sechs Monaten verurteilt worden. Auf seine Berufung hin hatte die kleine Strafkammer des Landgerichts Paderborn den Schuldspruch abgeändert und ihn wegen Betruges in vier Fällen (§§ 263, 248a, 53 StGB) schuldig gesprochen, es aber bei der ausgeurteilten Gesamtfreiheitsstrafe belassen. Auf die Revision des Angeklagten hin änderte der *Senat* unter Verwerfung der weitergehenden Revision den Schuldspruch ein weiteres Mal, und zwar jetzt in einen solchen wegen Urkundenunterdrückung in vier Fällen (§§ 274 Abs. 1 Nr. 2, 53 StGB). Erneut blieb es bei der ausgeurteilten Gesamtfreiheitsstrafe. In seiner Begründung geht der *Senat* in einer Tour d'Horizon durch nahezu das gesamte Computerstrafrecht, hält jedoch neben § 274 Abs. 1

[1] Die Entscheidung ist abrufbar unter http://www.justiz.nrw.de/nrwe/olgs/hamm/j2020/4_RVs_12_20_Beschluss_20200407.html (27.8.2020) und veröffentlicht in BeckRS 2020, 9059.
[2] NFC = near field communication; das Verfahren basiert auf der sog. RFID-Technologie (RFID = radio-frequency identification).
[3] Technisch ähnlich verhält es sich, wenn ein Smartphone zur Bezahlung eingesetzt wird. In diesem Fall ist jedoch durch das Einloggen in das Betriebssystem des Mobilgerätes die Berechtigung des Vorlegenden letztlich besser gewährleistet als in dem hier praktizierten Verfahren des Vorhaltens einer EC-Karte.
[4] OLG Hamm, Beschl. v. 7.4.2020 – 4 RVs 12/20, Rn. 24.
[5] PIN = Persönliche Identifikations-Nummer.
[6] OLG Hamm, Beschl. v. 7.4.2020 – 4 RVs 12/20, Rn. 9–13.

Nr. 2 StGB lediglich § 303a StGB für verwirklicht, der aber als subsidiär zurücktrete.

1. Betrug

Der *Senat* beginnt damit, den vom Strafrichter angenommenen Betrug (§§ 263 Abs. 1 und 4, 248a StGB) zu verneinen.[7] Im Kern geht es dabei um die Frage, ob das Personal des Marktes irrt, wenn ein Unberechtigter mittels einer ihm nicht zustehenden EC-Karte seine Einkäufe bezahlt. Möglicherweise kann dabei noch von einer konkludenten Täuschung über die Berechtigung zur Nutzung der EC-Karte ausgegangen werden. Denn kaum ein Täter wird sich (zutreffende) Gedanken über die zivilrechtlichen Hintergründe des angestrebten Zahlungsvorganges machen und im Zweifel vielmehr annehmen, es sei notwendig, die fehlende Berechtigung zu verbergen. Tatsächlich bleibt die fehlende Berechtigung jedoch, wie der *Senat* ausführt, ohne Belang dafür, weil der Markt unabhängig von diesem Umstand einen garantierten Zahlungsanspruch gegen das kartenausgebende Institut erlangt.[8]

Hintergrund ist das komplexe Regelungssystem für kontaktlose Zahlungsvorgänge. An sich wäre nach § 55 Abs. 1 ZAG[9] der Zahlungsdienstleister (hier die Sparkasse) verpflichtet, beim Auslösen eines elektronischen Zahlungsvorganges eine sog. „starke Kundenauthentifizierung" zu verlangen. Das kann nach § 1 Abs. 24 ZAG beispielsweise durch die Kombination der Abfrage von Wissen, über welches an sich nur der berechtigte Nutzer verfügen kann (etwa die PIN), und dem Einsatz von etwas, das nur der berechtigte Nutzer besitzen dürfte (etwa die EC-Karte) geschehen. Eine solche Kombination wird z.B. an Geldautomaten zur Authentifizierung des berechtigten Kunden eingesetzt. Ausnahmen von der Pflicht zur starken Kundenauthentifizierung gestattet § 55 Abs. 5 ZAG durch Verweis auf den delegierten Rechtsakt nach Art. 98 der Richtlinie (EU) 2015/2366 in Gestalt der VO (EU) 2018/389 v. 27.11.2017.[10] Art. 11 der VO (EU) 2018/389 erlaubt nämlich ein solches Absehen von der starken Kundenauthentifizierung, sofern der einzelne Zahlungsvorgang 50,- € nicht überschreitet, seit der letzten starken Kundenauthentifizierung nicht mehr als fünf kontaktlose Zahlungsvorgänge ausgelöst wurden und deren Gesamtvolumen 150,- € zudem nicht überstiegen hat. Von dieser Ermächtigung hat die deutsche Kreditwirtschaft Gebrauch gemacht, dabei jedoch den einzelnen Zahlungsvorgang zusätzlich auf 25,- € begrenzt.[11] Die Kundenauthentifizierung ist dann keine „starke" mehr, weil statt zweier nur noch eine Komponente durch den Zahlungsdienstleister geprüft wird, nämlich der Besitz einer gültigen EC-Karte. Wenn dies geschieht und die Zahlung sodann durch den Zahlungsdienstleister autorisiert wird, erlangt der Markt unmittelbar eine einredefreie Forderung gegen die Sparkasse in Höhe des autorisierten Betrages.[12] Die Haftung des Zahlungsdienstleisters entfällt lediglich bei vorsätzlich kollusivem Zusammenwirken mit dem Kunden, d.h. bei positiver Kenntnis der Nichtberechtigung.[13] Es besteht aber keinerlei Pflicht (und folglich auch keinerlei Interesse), die Berechtigung des kartenvorlegenden Kunden seitens des Marktes zu prüfen, womit auch kein Irrtum des Kassenpersonals angenommen werden kann und ein Betrug ausscheidet.[14]

2. Computerbetrug

Angesichts des weitgehend automatisch verlaufenden Vorganges widmet der *Senat* ebenfalls eingehendere Überlegungen dem vom Berufungsgericht bejahten Computerbetrug (§§ 263a Abs. 1 und 2, 263 Abs. 4, 248a StGB), der im Ergebnis jedoch genauso wenig vorlag.[15] Bemerkenswert ist dabei die Klarheit, mit welcher der *Senat* die unbefugte Datenverwendung als einzige ernsthaft in Betracht kommende Tatvariante verwirft. Verwendet werden die auf der EC-Karte gespeicherten Daten, die beim kontaktlosen Bezahlen dem Lesegerät zur Identifikation der Karte und damit des kartenausgebenden Instituts sowie des bezogenen Kontos zugänglich gemacht, also zur Identifikation seitens des Bezahlenden benutzt werden. Über das Merkmal „unbefugt" in § 263a Abs. 1 StGB herrscht bekanntlich Streit, den der *Senat* nur streift, um – insoweit fest auf dem Boden der Rspr. stehend[16] – sodann die vorzugswürdige[17] betrugsäquivalente Deutung anzuwenden.[18]

Bemerkenswert ist dabei die präzise Zuspitzung der Subsumtionsfrage: „Um die Vergleichbarkeit sicherzustellen, ist für die Täuschungsäquivalenz dabei nicht auf einen fiktiven Bankangestellten abzustellen, der die Interessen der Bank im Autorisierungsverfahren einer EC-Zahlung umfassend wahrzunehmen hat, sondern auf das Vorstellungsbild eines Schalterangestellten, der sich nur mit den Fragen befasst, die auch der Computer prüft bzw. für die sich auch im Computerprogramm Ansätze zur Kontrolle finden."[19] Nur mit dieser

[7] OLG Hamm, Beschl. v. 7.4.2020 – 4 RVs 12/20, Rn. 20–27.
[8] OLG Hamm, Beschl. v. 7.4.2020 – 4 RVs 12/20, Rn. 22.
[9] Gesetz über die Beaufsichtigung von Zahlungsdiensten (Zahlungsdiensteaufsichtsgesetz) v. 17.7.2017 (BGBl. I 2017, S. 2446).
[10] Delegierte Verordnung (EU) 2018/389 der Kommission v. 27.11.2017 zur Ergänzung der Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards für eine starke Kundenauthentifizierung und für sichere offene Standards für die Kommunikation (ABl. EU 2018 Nr. L 69/23).
[11] Nr. 8 der Bedingungen für die Teilnahme am electronic cash-System der deutschen Kreditwirtschaft, gültig ab 9.6.2016 (https://www.einfachzahlen.de/uploads/haendlerbedingungen.pdf, 27.8.2020)
[12] *Casper*, in: Säcker u.a. (Hrsg.), Münchener Kommentar zum BGB, Bd. 6., 8. Aufl. 2020, § 675c Rn. 131, 133.
[13] *Hoyer*, in: Wolter (Hrsg.), Systematischer Kommentar zum Strafgesetzbuch, Bd. 5, 9. Aufl. 2019, § 263 Rn. 79.
[14] OLG Hamm, Beschl. v. 7.4.2020 – 4 RVs 12/20, Rn. 26 f.
[15] OLG Hamm, Beschl. v. 7.4.2020 – 4 RVs 12/20, Rn. 29–36.
[16] BGH NJW 2014, 711 (712); BGH NJW 2013, 2608 (2610); BGH NJW 2002, 905 (906).
[17] Zur Darstellung des Streitstandes siehe *Heghmanns*, ZJS 2014, 323 (326 f.).
[18] OLG Hamm, Beschl. v. 7.4.2020 – 4 RVs 12/20, Rn. 33.
[19] OLG Hamm, Beschl. v. 7.4.2020 – 4 RVs 12/20, Rn. 34.

Einschränkung, die selbst der BGH nicht stets beachtet,[20] gelangt man zu einer tatsächlich betrugsäquivalenten Bestimmung der Grenzen des Computerbetruges. Bei der gedanklichen Ersetzung des Computers durch einen Menschen darf man also nicht gleichzeitig die überlegenen Prüfungsmöglichkeiten (oder -interessen) des Menschen hinzudenken. Vielmehr muss man sich den ersatzweise hinzugedachten Menschen als eine Person vorstellen, die sich nur für über diejenigen Aspekte des Handelns ihres Gegenübers Gedanken macht (und sodann u.U. darüber irren kann), mit denen sich auch der Computer befassen (und seine Reaktion entsprechend differenzieren) kann. Verzichtet hingegen das Datenverarbeitungssystem auf die Überprüfung bestimmter Aspekte einer Dateneingabe, so entspricht dieses „Verhalten" dem Verhalten desjenigen Menschen, dem in gleicher Weise bestimmte Aspekte des Handelns seines Gegenübers völlig gleichgültig sind, etwa bei der Kreditkartenvorlage die Deckung des Kundenkontos bei dem kartenausgebenden Kreditinstitut. Ebenso wenig, wie der Mensch hierüber i.S.v. § 263 StGB irrt, darf bei betrugsäquivalenter Auslegung ein Computerbetrug angenommen werden; der Datenverwender „beeinflusst" durch diesen Aspekt seiner Dateneingabe dann nicht das Ergebnis des Datenverarbeitungsvorganges. Andernfalls würde nämlich § 263a StGB zu einer Strafbarkeitsausdehnung führen und sich nicht auf seine Rolle beschränken, allein diejenigen Strafbarkeitslücken zu schließen, die durch die Digitalisierung von Geschäftsabläufen zwangsläufig (und nicht infolge anderer Kontrollverzichtsentscheidungen) entstehen. Folgerichtig führt der *Senat* aus, der allenfalls täuschungsfähige Umstand, nämlich die fehlende Berechtigung des Angeklagten, die Karte in eigener Person zu verwenden, werde vom Datenverarbeitungssystem nicht überprüft, weil dieses lediglich eine etwaige Kartensperre sowie eine Überschreitung der Betrags- und Häufigkeitsgrenzen kontaktlosen Zahlungsverkehrs überprüfe, nicht dagegen die Berechtigung des die Karte Vorlegenden.[21] Technisch wäre das selbstverständlich möglich gewesen; man bräuchte nur die PIN-Eingabe zu verlangen. Das aber soll zwecks größtmöglicher Attraktivität der kontaktlosen Zahlungsweise gerade nicht geschehen. Folgerichtig liegt nichts vor, was einem Irren i.S.v. § 263 StGB entspräche, und der Datenverarbeitungsvorgang wird i.S.v. § 263a StGB nicht durch die unbefugte Datenverwendung beeinflusst: Ob nun der legitime Karteninhaber oder der Unberechtigte die Karte verwendet – die Zahlung an den kartenannehmenden Markt wird in den oben genannten Grenzen des kontaktlosen Zahlungsverkehrs garantiert. Die damit gänzlich unnötig und nur der Kundenbequemlichkeit halber eröffneten Missbrauchsmöglichkeiten könnte man geradezu als eigenverantwortliche Selbstgefährdung der kartenausgebenden Institute verstehen; ein Grund mehr, keine Ausdehnung des Strafrechtsschutzes unter Verletzung systematischer Auslegungsgrundsätze vorzunehmen. Der *Senat* ist – an dieser Stelle – mit seiner präzisen Vorgehensweise einer solchen Versuchung entgangen und hat einen Computerbetrug zu Recht abgelehnt.[22]

3. Datenfälschung (§ 269 StGB)

Interessanterweise befasst sich der *Senat* im Anschluss mit einer Fälschung beweiserheblicher Daten (§ 269 Abs. 1 StGB), die er im Ergebnis zwar zutreffend ablehnt, dies jedoch mit einer nicht ganz überzeugenden Begründung.[23] Der Tatbestand setzt in der hier denkbaren Variante voraus, Daten so zu speichern, dass bei ihrer Wahrnehmung eine unechte Urkunde vorläge. Als fragliche Daten begreift der *Senat* zutreffend die Transaktionsdaten (Konto- und Kartendaten, weiterhin wohl auch Zeitpunkt der Vorlage sowie Höhe des Zahlbetrages).[24] Er verneint dann aber die hypothetische Urkundenqualität des gespeicherten Datensatzes, weil er mangels Identifikation des Eingebenden keinen hypothetischen Urkundenaussteller ausweise. Denn nur, wenn man per PIN-Abfrage gewährleiste, dass die Eingabe allein durch den berechtigten Kartenbesitzer erfolgt sei, könne man diesen als (vorgeblichen) Urheber des Datensatzes bezeichnen, was dann zu einer hypothetischen Urkundenqualität führe.[25] Diese Argumentation erscheint nicht unbedingt schlüssig. Wenn das Vorhalten der EC-Karte der Herstellungsakt des Datensatzes sein sollte (dazu sogleich mehr), so ist die Nutzung von EC-Karten durch Unberechtigte trotz des Verzichts auf eine Identitätskontrolle vermutlich (und glücklicherweise) die große Ausnahme. Die Eingabe ließe sich daher dem Anschein nach (und nur auf diesen käme es dann ja an) dem legitimen Kartenbesitzer zuordnen; damit gelangte man im Falle des Missbrauchs zu einem Auseinanderfallen von vorgeblichem und tatsächlich Speichernden und mithin zur Unechtheit einer entsprechenden hypothetischen Urkunde. Von seinem Ausgangspunkt her hätte der *Senat* daher auch zur Bejahung von § 269 StGB gelangen können. Aus einer anderen Überlegung heraus bleibt sein Ergebnis gleichwohl richtig. Diese Erwägung setzt ebenfalls an der Frage an, wem denn die Datenspeicherung nach außen hin als Urheber zuzuordnen ist, tut dies aber in grundsätzlicherer Weise. Denn der gespeicherte Datensatz wird ja mindestens teilweise nicht durch Daten erzeugt, welche der Kartennutzer gezielt eingibt. Zwar verwendet er die eigentlichen Kartendaten, aber Zeitpunkt und Betragshöhe übernimmt das System von der Kasse. Der anschließende Datensatz beruht also auf mehreren Inputquellen und wird zudem inhaltlich weitgehend vom Datenverarbeitungssystem vorgegeben. Der Speichervorgang selbst stellt also keine einseitige Angelegenheit dar, wie sie § 269 StGB idealtypisch zu Grunde legt. Vielmehr liest das Lesegerät die ihm angebotenen Daten aus; welche das im Einzelnen sind, bestimmt aber keineswegs der Kartennutzer, sondern derjenige, der die Datenverarbeitungsanlage gestaltet hat. Im Ergebnis enthält die Speicherung als hypothetische Urkunde sodann die Erklärung, mit der Karte Nr. X sei am Datum Y zur Uhrzeit Z im Markt A an der Kasse Z ein Rechnungsbetrag in Höhe von *n* € kontaktlos zur

[20] Vgl. etwa BGH NJW 2014, 711 (712), wo dieser Aspekt nicht bedacht wurde; demgegenüber zutreffend aber BGH NJW 2013, 2608 (2610); BGH NJW 2002, 905 (906).
[21] OLG Hamm, Beschl. v. 7.4.2020 – 4 RVs 12/20, Rn. 35.
[22] OLG Hamm, Beschl. v. 7.4.2020 – 4 RVs 12/20, Rn. 36.
[23] OLG Hamm, Beschl. v. 7.4.2020 – 4 RVs 12/20, Rn. 38–43.
[24] OLG Hamm, Beschl. v. 7.4.2020 – 4 RVs 12/20, Rn. 41.
[25] OLG Hamm, Beschl. v. 7.4.2020 – 4 RVs 12/20, Rn. 42 f.

Zahlung angewiesen worden. Diesen komplexen Datensatz, der auch nur in dieser Kombination beweisgeeignet ist, wird man kaum demjenigen zuordnen können, der mit einer Handbewegung seine Erzeugung ausgelöst, ihn inhaltlich aber in keiner Weise gesteuert hat. Er erscheint vielmehr als Produkt des Betreibers der Datenverarbeitungsanlage. Die Situation ähnelt derjenigen eines Parkplatznutzers, der durch Eingabe von Münzen an einem Parkscheinautomaten die Herstellung eines Parkscheines auslöst und diesen sogar inhaltlich mit beeinflusst, weil die ausgedruckten Angaben von der jeweiligen Geldmenge und dem Zeitpunkt des Einwurfs abhängen. Gleichwohl wird die entstandene Urkunde dem Systembetreiber als Aussteller zugeordnet.[26] Entsprechend muss bei hypothetischen Urkunden verfahren werden. Der Betreiber der Datenverarbeitungsanlage wirkt daher als geistiger Urheber und ist folgerichtig als erkennbarer Aussteller der hypothetischen Urkunde anzusehen.[27] Im Ergebnis wird also tatsächlich eine hypothetische Urkunde erzeugt; sie ist jedoch echt und § 269 StGB schied aus diesem Grunde aus.

4. Datenunterdrückung (§ 274 Abs. 1 Nr. 2 StGB)

Nach kurzen Bemerkungen, warum weder § 266b StGB[28] noch § 202a Abs. 1 StGB[29] erfüllt sind, erörtert (und bejaht) der *Senat* ein Vergehen nach § 274 Abs. 1 Nr. 2 StGB.[30] Die zu unterdrückenden, beweiserheblichen Daten sieht er dabei in den Informationen über die Höhe des Verfügungsrahmens, die Anzahl kontaktloser Einsätze der Karte seit der letzten PIN-Abfrage und die Geldbeträge, über welche jeweils verfügt wurde, die allesamt im Autorisierungssystem des kartenausgebenden Instituts gespeichert werden.[31] Diese nicht dem Angeklagten gehörenden Daten seien nun „überschrieben, also gelöscht, bzw. verändert im Sinne der Norm“ worden.[32] Schon diese Annahme erscheint fraglich, weil bei lebensnaher Betrachtung wohl keine der bestehenden Speicherungen verändert, sondern diese um einen weiteren Datensatz ergänzt worden sein dürften. Es wäre lebensfremd anzunehmen, der Systembetreiber würde Daten über einen vorherigen Karteneinsatz überschreiben und damit löschen, weil selbstverständlich ein erhebliches Interesse daran besteht, jede Benutzung der EC-Karte dauerhaft zu dokumentieren, und zwar schon aus Gründen der Abrechnung gegenüber dem Kontoinhaber. Gleichwohl könnte man im Hinblick auf die hinzukommenden Daten noch eine Veränderung i.S.v. § 274 Abs. 1 Nr. 2 StGB annehmen, wenn man auf den gesamten Datenbestand abstellt.

Ernsthafte Schwierigkeiten bereitet anschließend aber die Nachteilszufügungsabsicht, für die nach h.M. *sicheres Wissen* um den Nachteilseintritt i.S.v. dolus directus zweiten Grades genügt.[33] Im Hinblick auf das Schutzgut der Beweisführungsbefugnis besteht der vorherzusehende Nachteil jedenfalls aus einem Verlust bzw. einer Verschlechterung von Beweismöglichkeiten wegen der erfolgten Veränderung der Daten.[34] An dieser Stelle bleibt die Entscheidung auffällig abstrakt; der *Senat* sieht, ohne dies jedoch näher auszuführen, den fraglichen Nachteil beim berechtigten Karteninhaber, der nun keinen Beweis (mit dem veränderten Datensatz) mehr führen könne.[35] Welcher Verlust an Beweismöglichkeiten sollte ihm aber tatsächlich drohen? Die zusätzlich dokumentierte Kartennutzung erlaubt dem berechtigten Karteninhaber vielmehr, gegenüber dem kartenausgebenden Institut darzulegen, nicht selbst die entsprechende Verfügung vorgenommen zu haben (und damit eine Rückbuchung der Kontobelastung zu erreichen). Sähe man den Nachteil hingegen in dem „Aufbrauchen“ der begrenzten Zahl von kontaktlosen Zahlungsakten ohne PIN-Abfrage, wie es in der Entscheidung ebenfalls anklingt,[36] so wäre das zwar ein potenzieller Nachteil, der aber nur dann eintreten könnte, wenn die benutzte Karte erneut dem Berechtigten zugänglich würde und dieser sie nun wegen Erschöpfung des Rahmens zur Nutzung ohne PIN-Abfrage erst einmal nicht mehr in dieser nutzerfreundlichen Weise einsetzen könnte. Allerdings wird der Täter üblicherweise die Karte behalten, wegwerfen oder vernichten, nicht jedoch dem Berechtigten zurückgeben wollen, womit der beschriebene Nachteil von ihm zum Zeitpunkt des Einsatzes auch nicht vorhergesehen wird; § 274 Abs. 1 Nr. 2 StGB könnte daher allenfalls später, nämlich bei einem etwaigen Vernichtungsakt, verwirklicht werden, jedoch kaum bei den verfahrensgegenständlichen Geschehen an den Kassen des Marktes.

5. Datenveränderung (§ 303a StGB)

Konsequent musste der *Senat* nach seinem zur Datenunterdrückung erzielten Ergebnis zugleich eine Datenveränderung nach § 303a Abs. 1 StGB bejahen,[37] deren Merkmale vollständig in § 274 Abs. 1 Nr. 2 StGB enthalten sind, welcher deshalb insoweit eine Qualifikation bildet und § 303a Abs. 1 StGB folgerichtig verdrängt. Da sich dessen Tatbestand auf die Veränderung von (fremden) Daten beschränkt und keine überschießenden subjektiven Merkmale aufweist, mag seine Annahme auf den ersten Blick auch durchaus plausibel er-

[26] OLG Köln NJW 2002, 527 f.; *Hoyer* (Fn. 13), § 267 Rn. 18 ff.
[27] Vgl. dazu *Heine/Schuster*, in: Schönke/Schröder, Strafgesetzbuch, Kommentar, 30. Aufl. 2019, § 269 Rn. 12; *Erb*, in: Joecks/Miebach (Hrsg.), Münchener Kommentar zum StGB, Bd. 5, 3. Aufl. 2019, § 269 Rn. 31.
[28] OLG Hamm, Beschl. v. 7.4.2020 – 4 RVs 12/20, Rn. 45 (Angekl. ist nicht der berechtigte Kartenbesitzer).
[29] OLG Hamm, Beschl. v. 7.4.2020 – 4 RVs 12/20, Rn. 47 f. (keine besondere Zugangssicherung der Daten, weil ohne weiteres auslesbar).
[30] OLG Hamm, Beschl. v. 7.4.2020 – 4 RVs 12/20, Rn. 50–60.
[31] OLG Hamm, Beschl. v. 7.4.2020 – 4 RVs 12/20, Rn. 52.
[32] OLG Hamm, Beschl. v. 7.4.2020 – 4 RVs 12/20, Rn. 56.
[33] BGH NJW 1953, 1924; *Heine/Schuster* (Fn. 27), § 274 Rn. 15; *Fischer*, Strafgesetzbuch und Nebengesetze, Kommentar, 67. Aufl. 2020, § 274 Rn. 9a; a.A. *Hoyer* (Fn. 13), § 274 Rn. 17 (dolus directus ersten Grades).
[34] *Freund*, in: Joecks/Miebach (Fn. 27), § 274 Rn. 53; *Fischer* (Fn. 33), § 274 Rn. 9a; BGHSt 29, 192 (196); BGH NStZ 2010, 332 (333).
[35] OLG Hamm, Beschl. v. 7.4.2020 – 4 RVs 12/20, Rn. 57 f.
[36] OLG Hamm, Beschl. v. 7.4.2020 – 4 RVs 12/20, Rn. 54.
[37] OLG Hamm, Beschl. v. 7.4.2020 – 4 RVs 12/20, Rn. 62–64.

scheinen. Als Parallele zur Sachbeschädigung in der virtuellen Welt genügt aber für § 303a StGB nicht jedwede Veränderung von Daten, sondern diese muss in irgendeiner Form schädigend für den berechtigten Datenbesitzer wirken, indem sie den ursprünglichen Verwendungszweck des Datensatzes beeinträchtigt.[38] Das wiederum ist, wie oben (4.) gezeigt, jedoch nicht der Fall; Kartenbesitzer und kartenausgebendes Institut werden die Dokumentation der missbräuchlichen Kartennutzung vielmehr gerade nicht als nachteilig werten, sondern von einer zweckentsprechenden Datenergänzung ausgehen, die daher den Tatbestand von § 303a Abs. 1 StGB ebenfalls nicht zu erfüllen vermag.

6. Leistungserschleichung (§ 265a StGB)

Nicht angesprochen wird in der Entscheidung ein Vergehen der Leistungserschleichung, was aus Sicht des *Senats* wegen der Subsidiaritätsklausel in § 265a Abs. 1 StGB allerdings konsequent war. Im Falle anderweitiger Straflosigkeit könnte man jedoch auf die Idee kommen, der Angeklagte habe als Leistung des „Bezahlautomaten" die Freigabe der gekauften Waren durch die unberechtigte Vorlage der fremden EC-Karte erschlichen. Aber selbst diese Strafvorschrift greift bei näherem Hinsehen nicht ein, weil das Kartenlesegerät zwar das Recht auf die gekauften Waren, aber eben nicht diese selbst vermittelt,[39] denn sie werden dem Kunden vom Kassenpersonal nach Erhalt der Mitteilung über die erfolgte Bezahlung übergeben. Dann aber fehlt es an der Entgeltlichkeit der Leistung, die § 265a StGB voraussetzt. Entgelt schuldet der Kunde nämlich allein für die eingekauften Dinge und nicht für die Benutzung des Kartenlesegerätes, das damit nicht zu den tatbestandlich erfassten Automaten zählt.

7. Schuldspruchberichtigung ohne Aufhebung des Strafausspruchs?

Ein letzter Aspekt der Entscheidung verdient noch kritische Erwähnung. Der *Senat* nimmt eine Berichtigung des Schuldspruchs im Sinne der von ihm für richtig erachteten Lösung vor, was als solches zur Vereinfachung des weiteren Verfahrens sinnvoll und anerkannt ist.[40] Allerdings belässt es der *Senat* zugleich bei dem Strafausspruch der Strafkammer, obschon infolge der Auswechselung des abgeurteilten Delikts (§ 274 StGB statt § 263a StGB) nunmehr ein Nichtvermögensdelikt an die Stelle eines Vermögensdeliktes getreten ist. Zwar kann sich der *Senat* auf die Identität der Strafrahmen berufen,[41] aber die strafzumessungsrelevanten Tatsachen sind dann doch unterschiedlich. Bei § 263a StGB spielen auf der Ebene des Tatschuldgehaltes die Höhe des Schadens und das Raffinement der Vorgehensweise maßgebende Rollen, während § 274 StGB die Relevanz der unterdrückten Datei als Beweismittel für den Berechtigten in den Vordergrund rückt. Dazu verhält sich die Entscheidung nicht weiter, sondern verweist auf die (identischen, aber eben nur für § 263a StGB auch tatbestandlichen) finanziellen Auswirkungen der Tat. Zugleich betont der *Senat* die von der Strafkammer angeführten Vorbelastungen des Angeklagten, die freilich nur für den Computerbetrug, nicht aber für das nunmehr zu Grunde zu legende Urkundendelikt auch einschlägig sind. Das überspielt der *Senat* mit dem Hinweis, die Strafkammer habe ihr Hauptaugenmerk auf den Umstand bereits verbüßter Strafhaft und die Rückfallgeschwindigkeit gelegt.[42] In der Gesamtschau erweckt das nicht nur den Eindruck einer gewissen Beliebigkeit des Schuldspruchs sowie einer tendenziellen Abkehr vom Tat- zum Täterstrafrecht, sondern auch eines revisionsgerichtlichen Einbruchs in die Strafzumessungsentscheidung als klassische Domäne des Tatrichters. Eine Aufhebung des Strafausspruchs und Zurückverweisung der Sache zur neuen Strafbemessung, die ohnehin von § 354 Abs. 2 S. 1 StPO als normativer Regelfall vorgesehen ist, wäre von daher die sachgerechtere Vorgehensweise gewesen.

IV. Ergebnis und Ausblick

Nach eingangs richtiger Verneinung der §§ 263 f., 269 StGB begibt sich die Entscheidung des *Senats* also auf Abwege und gelangt zu einem insgesamt wenig überzeugenden Ergebnis. Materiellrechtlich müsste dieses schon bei oberflächlicher Betrachtung stutzen lassen: Immerhin ging es um eine rechtswidrige Bereicherung, die der Täter angestrebt und erreicht hatte, und deren Bewertung als Urkundenunterdrückung verfehlt geradezu offenkundig den Kern des potenziellen Tatunrechts. Richtigerweise hatte der Angeklagte jedoch bei dem Karteneinsatz überhaupt kein strafbares Unrecht verwirklicht; ob dies zuvor der Fall war – man könnte immerhin an Hehlerei oder Unterschlagung anlässlich der Erlangung der EC-Karte denken –, war offensichtlich nicht (mehr) Gegenstand dieses Verfahrens. War es nun die Sorge vor drohender Straflosigkeit, die den *Senat* geleitet hat, oder hat er sich schlicht in der nicht ganz einfachen Welt der Datendelikte verheddert?

Die richtigerweise anzunehmende Straflosigkeit missbräuchlichen Einsatzes fremder EC-Karten beim kontaktlosen Bezahlen ohne PIN-Abfrage könnte nun freilich zu Überlegungen verleiten, ob es nicht eines korrigierenden Eingriffs seitens des Gesetzgebers bedürfte. Dem ist mit Nachdruck entgegen zu treten: Wenn die Kreditwirtschaft der Bequemlichkeit ihrer Kunden zuliebe ohne jede Not auf mögliche Sicherungen verzichtet, hier in Gestalt der völlig unaufwendigen und daher allen Beteiligten zumutbaren PIN-Abfrage, so begibt sie sich sehenden Auges in Gefahr. Das Strafrecht ist nicht dazu da, vor derartigen Selbstgefährdungen zu schützen, zumal die drohenden Schäden angesichts der für einen derartigen Karteneinsatz gezogenen Betragsgrenzen überschaubar bleiben.

Prof. Dr. Michael Heghmanns, Münster

[38] BGH NStZ 2018, 401 (403); *Hecker*, in: Schönke/Schröder (Fn. 27), § 303a Rn. 8; *Fischer* (Fn. 33), § 303a Rn. 12; Bericht des Rechtsausschusses zum 2. WiKG, BT-Drs. 10/5058, S. 35.

[39] Vgl. dazu *Perron*, in: Schönke/Schröder (Fn. 27), § 265a Rn. 4; *Fischer* (Fn. 33), § 265a Rn. 14.

[40] *Wohlers*, in: Wolter (Hrsg.), Systematischer Kommentar zur Strafprozessordnung, Bd. 7, 5. Aufl. 2018, § 354 Rn. 21 f.; BVerfG (Kammer) NJW 1996, 116.

[41] OLG Hamm, Beschl. v. 7.4.2020 – 4 RVs 12/20, Rn. 71.

[42] OLG Hamm, Beschl. v. 7.4.2020 – 4 RVs 12/20, Rn. 72.