

NFC-Zahlung und unbefugtes Verwenden von Daten

BayObLG, Beschluss vom 29.7.2024 – 201 StRR 49/24

mit einer Anmerkung von Janick Haas*

A. Sachverhalt

Randnummer 5

a) Nach den Feststellungen des Landgerichts hat der Angeklagte eine von ihm aufgefundene EC-Karte für das Konto von M. bei der S-Bank aufgrund jeweils neu gefasster Tatentschlüsse im Juli 2023 in jeweils zwei Fällen bei den Discounter A. und N. in X zur Bezahlung von Einkäufen in Höhe von 16,40 Euro, 16,56 Euro, 7,67 Euro und 9,45 Euro verwendet. In einem weiteren Fall am 27.07.2023 versuchte er, mit der inzwischen gesperrten Karte bei der genannten Filiale der Firma A. einen Einkauf in Höhe von 23,40 Euro zu bezahlen, was jedoch nicht gelang.

B. Aus den Gründen

Randnummer 6

b) Das Landgericht hat keine Feststellungen dazu getroffen, ob der Angeklagte die EC-Karte unter Eingabe einer PIN verwendet hat oder ob die Bezahlung beim Einkauf jeweils kontaktlos erfolgte. Auch in einer Gesamtschau der Urteilsgründe sind die genauen Zahlungsmodalitäten nicht erkennbar, sodass dem Senat die rechtliche Überprüfung anhand der Urteilsfeststellungen nicht möglich ist.

* Dr. Janick Haas ist Staatsanwalt bei der Staatsanwaltschaft Gießen.
Kontakt: Janick.Haas@StA-Giessen.Justiz.Hessen.de.



Randnummer 7

aa) Sollte der Angeklagte die aufgefundene EC-Karte bzw. Girocard bei der elektronischen Bezahlung von Waren mit Eingabe der dazugehörigen PIN benutzt haben, ist der Tatbestand des § 263a Abs. 1 StGB in der Variante der unbefugten Verwendung von Daten erfüllt. Das POS-System („Point of Sale“) ermöglicht das elektronische Bezahlen von Waren oder Dienstleistungen an automatisierten Kassen mittels der Girocard bzw. Debitkarte. An einem Zahlungsvorgang über ein POS-System nehmen der Karteninhaber, das am System angeschlossene Vertragsunternehmen (etwa ein Händler) sowie der Kartenemittent teil. Der Karteninhaber autorisiert einen Zahlungsvorgang durch das Einführen der Karte am POS-Terminal und die Eingabe der dazugehörigen PIN. Das kartenausgebende Institut überprüft die Korrektheit der Daten und die Wahrung des Verfügungsrahmens. Bei einem wirksam autorisierten Zahlungsvorgang übernimmt der Kartenemittent gegenüber dem Vertragsunternehmen (z.B. Händler) ein Zahlungsversprechen, das überwiegend als abstraktes Schuldversprechen i.S.d. § 780 BGB qualifiziert wird. Aufgrund des vertraglichen Verbots der Weitergabe der Geheimzahl (PIN) kann eine wirksame Autorisierung des Zahlungsvorgangs nur durch den berechtigten Karteninhaber persönlich erfolgen. Eine Strafbarkeit ist demnach zu bejahen, wenn der Täter im Rahmen eines POS-Zahlungsvorgangs eine gefälschte bzw. manipulierte Karte verwendet oder wenn er die Karte (nebst PIN) vom Karteninhaber im Wege der verbotenen Eigenmacht erlangt hat (vgl. zum Ganzen MüKo/Hefendehl/Noll StGB 4. Aufl. § 263a Rn. 107 f.; Schumann/Mosbacher/König/Nadeborn Medienstrafrecht 1. Aufl. § 263a StGB Rn. 24; LK/Tiedemann/Valerius StGB 12. Aufl. § 263a Rn. 52; LG Heilbronn StraFo 2022, 120).

Randnummer 8

bb) Wurde die gefundene EC-Karte bzw. Girocard beim Einkaufen durch den Angeklagten ohne PIN mittels NFC (Near Field Communication) verwendet, also kontaktlos bezahlt, kommt eine Verurteilung wegen Computerbetrugs nach § 263a Abs. 1, 3. Variante StGB (unbefugte Verwendung von Daten) nicht in Betracht. Beim kontaktlosen Bezahlen werden die auf der Karte gespeicherten Daten, der Rechnungsbetrag und Daten zum Zahlungsempfänger an die Autorisierungszentrale des kartenausgegebenen Kreditinstituts übermittelt, wo ein Computer überprüft, ob die Girocard in keine Sperrdatei eingetragen ist, der Verfügungsrahmen

nicht überschritten wird und ob die Voraussetzungen für das Absehen von einer PIN-Abfrage im konkreten Fall vorliegen (Göhler, Kontaktloses Bezahlen mit der Girocard (k) eine Herausforderung für das Strafrecht, JR 2021, 6, 8). Anders als in den Fällen, in denen der Bankcomputer die PIN vom Kartenverwender anfordert, wird hierbei die Berechtigung desjenigen, der den elektronischen Zahlungsvorgang durch Vorhalten der Karte vor das Lesegerät auslöst, gerade nicht durch Anwendung einer starken Kundenauthentifizierung i.S.v. § 55 Abs. 1 Nr. 2 ZAG überprüft, so dass eine Strafbarkeit nach § 263a StGB regelmäßig nicht gegeben ist. Eine Verwendung von Daten ist nach der vorzunehmenden betrugsspezifischen Auslegung nämlich nur dann „unbefugt“, wenn sie gegenüber einer natürlichen Person Täuschungscharakter hätte (OLG Hamm, Beschluss vom 07.04.2020 – 4 RVs 12/20 = WM 2020, 1674 = wistra 2021, 84 = ZIP 2021, 342 = NStZ 2020, 673, 674 m. Anm. Kudlich JA 2020, 710 und Christoph/Dorn-Haag NStZ 2020, 676). Da aber bei einer derartigen Zahlungsabwicklung das Kassenpersonal durch den Angeklagten nicht getäuscht wird (vergleiche hierzu nachfolgend IV. 1.), kommt auch eine Strafbarkeit wegen Computerbetrugs nicht in Betracht.

[...]

Randnummer 14

1. Sollte der neue Tatrichter zu dem Ergebnis gelangen, dass bei den jeweiligen Bezahlvorgängen eine PIN-Abfrage nicht erfolgt ist, wird eine Strafbarkeit wegen Betruges gemäß § 263 Abs. 1 StGB regelmäßig nicht in Betracht kommen. Der Händler erlangt im Fall des kontaktlosen Bezahls unmittelbar eine einredefreie Forderung gegen die Bank in Höhe des autorisierten Betrags, gerade auch dann, wenn ein Nichtberechtigter die Karte verwendet und die kartenausgebende Bank auf die Abfrage der PIN verzichtet hat. Es fehlt damit schon mangels Täuschung des Angeklagten über seine Berechtigung zur Verwendung der Karte und mangels damit korrespondierenden Irrtums des Kassenpersonals an den tatbestandlichen Voraussetzungen des § 263 Abs. 1 StGB (OLG Hamm a.a.O.; Göhler a.a.O. S. 9 ff.).

C. Würdigung von Janick Haas

Die Entscheidung des BayObLG stellt – soweit ersichtlich – die zweite obergerichtliche Entscheidung zur Strafbarkeit des Verwendens einer fremden EC-Karte zur Zahlung im NFC-Verfahren dar. Ebenso wie das

OLG Hamm¹ vermag das BayObLG in einem solchen Verhalten keinen Computerbetrug i.S.v. § 263a I Var. 3 StGB zu erkennen.

I. Die Vorinstanz schien ausweislich der Urteilsfeststellungen davon auszugehen, dass unberechtigte Zahlungen mit EC-Karten unabhängig von der konkreten Zahlungsvariante einheitlich strafrechtlich zu bewerten seien. Das BayObLG ist hingegen der Auffassung, dass rechtliche Unterschiede zwischen kontaktlosen und kontaktbedürftigen Nutzungen der EC-Karte bestehen.

1. Ausgangspunkt für den kurz skizzierten Streit ist die Auslegung des Begriffs der „unbefugten“ Datenverwendung i.S.v. § 263a I Var. 3 StGB. Ganz im Sinne der herrschenden Rechtsprechung definiert das BayObLG den diesbezüglichen Prüfungsmaßstab im Ausgangspunkt betrugsnah im Wege einer Täuschungsäquivalenz des Verhaltens gegenüber einer fiktiven Erklärungsempfängerin.² Dieser fiktive Maßstab ist aber weiter zu präzisieren. So ist das Vorstellungsbild einer solchen gedachten Person für maßgeblich zu erachten, welches sich mit dem Themenbereich deckt, der der Prüfung des Computers entspricht bzw. für dessen Prüfung sich im Computerprogramm Kontrollansätze finden.³ Nur bei einer solchen Interpretation der Unbefugtheit der Datenverwendung wird der vom Gesetzgeber angestrebte Gleichlauf der §§ 263, 263a StGB konsequent eingehalten.⁴

2. Insbesondere bei technisch komplexen Vorgängen, welche nicht bilateral abgewickelt werden, gilt es, die konkreten Anforderungen an den fiktiven Erklärungsempfänger genau zu bestimmen. Dabei sind die Besonderheiten der jeweiligen Geschäftsausgestaltung zu berücksichtigen.⁵

a) Das BayObLG stellt insoweit zwar zutreffend auf das Kassenpersonal als fiktiven Erklärungsempfänger ab. Allerdings gibt es den fiktiven Prüfungsmaßstab nur verkürzt wieder: Bei einer Kartenzahlung im NFC-Verfahren könne das Personal aufgrund einer unabhängig von der Berechtigung zur Zahlungsanweisung zu erlangenden einredefreien Forderung

¹ OLG Hamm NStZ 2020, 673 ff.

² S. etwa *Hefendehl/Noll*, in Münchener Kommentar StGB, Bd. 5, 4. Aufl. 2022, § 263a Rn. 78 ff.

³ S. etwa BGH NJW 2002, 905, 906; OLG Hamm NStZ 2020, 673, 674 f.; s. auch *Böse/Tomiak* ZfIS 2023, 265, 274; ebenfalls unter Heranziehung von BGH NJW 2002, 905, aber mit Beschränkung auf den tatsächlich angefallenen Kontrollinhalt *Göhler* JR 2021, 6, 17 f.

⁴ S. hierzu etwa *Hefendehl/Noll* (Fn. 2), § 263a Rn. 87; *Burghardt/Bardowicks* ZJS 2023, 593, 604.

⁵ Vgl. BGH NJW 2013, 1017, 1018.

gegen die Bank in Höhe des autorisierten Betrags bereits nicht getäuscht werden.⁶

b) Gänzlich unbeachtet bleibt in der Entscheidung dadurch die Herleitung einer möglichen Täuschungsäquivalenz über den Prüfungs- und Kontrollumfang der am Bezahlvorgang beteiligten kartenemittierenden Bank. Dies ist bereits deshalb beachtlich, weil auch das BayObLG für Fälle des Missbrauchs von fremden EC-Karten im herkömmlichen POS-Verfahren eine Täuschungsäquivalenz aufgrund eines wirksam autorisierten Zahlungsvorgangs herleitet. Die im Programm angelegte Kontrolle der Bank wird vom Gericht also herangezogen.⁷ Das vertragliche Verbot, die eigene EC-PIN weiterzugeben, führe dazu, dass eine solche Autorisierung nur von der berechtigten Person wirksam herbeigeführt werden kann. Lediglich im Fall der wirksamen Autorisierung übernehme die Kartenemittentin gegenüber dem Zahlungsempfänger ein Zahlungsverprechen. Es ist also der Erklärungswert der PIN-Eingabe im Verhältnis zur Bank, der sie nach Ansicht des Gerichts als unbefugte Datenverwendung qualifiziert.⁸

3. Entgegen der Auffassung des BayObLG sind diese Erwägungen auch auf eine unberechtigte Zahlung im NFC-Verfahren übertragbar.⁹ Auch im Rahmen einer NFC-Zahlung wohnt der Verwendung der EC-Karte ein computerbetrugsrelevanter Erklärungswert inne.

a) Eine Zahlung im NFC-Verfahren ist genau wie eine kontaktbedürftige Zahlung mit PIN-Eingabe grundsätzlich erst nach vorheriger Kontrolle des Kreditinstituts möglich.¹⁰ Gem. Art. 97 I b), 98 I b), III EU-Richtlinie 2015/2366 i.V.m. Art. 11 VO (EU) 2018/389 i.V.m. § 55 V ZAG kann das Kreditinstitut von der Einforderung einer starken Kundenauthentifizierung allein bei Vorliegen bestimmter Bedingungen ausnahmsweise absehen: Der einzelne Zahlungsbetrag darf 50 € nicht übersteigen, die Summe aller aufeinander folgenden kontaktlosen Transaktionen darf 150 € nicht übersteigen und es dürfen nicht mehr als fünf NFC-Zahlungen hintereinander vorgenommen werden. Liegen diese Voraussetzungen nicht

⁶ S. auch OLG Hamm NSTZ 2020, 673, 674; diesbezüglich kritisch *Ladiges* WuB 2020, 604, 604.

⁷ S. hierzu grundlegend *Altenhain* JZ 1997, 752, 754 ff.

⁸ So auch *Göhler* JR 2021, 6, 17.

⁹ A.A. etwa *Christoph/Dorn-Haag* NSTZ 2020, 676 f.; *Eisele* in Hilgendorf/Kudlich/Valerius (Hrsg.), Handbuch des Strafrechts, Bd. 6, 2022, § 63 Rn. 137; *Hefendehl/Noll* (Fn. 2), § 263a Rn. 87; *Heghmanns* ZJS 2020, 494, 496.

¹⁰ Dies ausblendend etwa *Bechtel* JR 2024, 481, 483 Rn. 12.

kumulativ vor, ist die Bank zur Abfrage der starken Kundenauthentifizierung – der PIN-Eingabe – verpflichtet. Insofern wird im Falle einer durchgeführten NFC-Zahlung aufgrund einer Überprüfung der einschlägigen Voraussetzungen durch die Bank die tatsächliche Umsetzung einer starken Kundenauthentifizierung i.S.v. § 55 I Nr. 2 ZAG ausgesetzt. Ein kontaktloser Bezahlvorgang erfolgt daher gerade nicht unter Verzicht¹¹ auf die starke Kundenauthentifizierung.¹² Die Notwendigkeit des Nachweises der Berechtigung zur Kartennutzung ist somit auch bei kontaktlos initiierten Zahlungen grundsätzlich angelegt.¹³

b) Hierdurch verliert die Benutzung der EC-Karte im NFC-Verfahren nicht jeglichen Erklärungswert.¹⁴ Eine NFC-Zahlung kann entsprechend den dargestellten Maßstäben nicht insgesamt kontrollfrei im Verhältnis zum Kreditinstitut realisiert werden. Der Nutzung der Karte im Wege einer kontaktlosen Zahlung wohnt somit die konkludente Erklärung inne, die Berechtigung zur Kartennutzung im Zweifel per starker Kundenauthentifizierung nachweisen zu können.¹⁵ Dieser Nachweis erfolgt selbstredend über eine PIN-Eingabe. Das vertragliche Verbot der Weitergabe der PIN prägt also auch im Rahmen einer kontaktlosen Zahlung den Erklärungswert des Verhaltens.¹⁶ Eine bloße Erklärung über den Besitz der Karte¹⁷ geht mit einer NFC-Zahlung nicht einher.

c) Hieran ändert auch die gesetzgeberische bzw. vertragliche Wertung nichts, dass die Abfrage der Berechtigung bei Zahlungsbeträgen unter 50 € die Ausnahme und nicht die Regel darstellt.¹⁸ Das Absehen von einer zwingenden Abfrage einer starken Kundenauthentifizierung dient allein der Vereinfachung von Geschäftsabläufen. Die Nutzung einer EC-Karte soll in puncto Einfachheit der Handhabung bei Transaktionen mit geringen Beträgen der Nutzung von Bargeld angeglichen werden.¹⁹ Der

¹¹ So aber etwa *Ceffinato* JuS 2021, 311, 313; *Christoph/Dorn-Haag* NStZ 2020, 697, 702; ähnlich ebenso *Bär* in *Wabnitz/Janovsky/Schmitt* (Hrsg.), *Handbuch Wirtschafts- und Steuerstrafrecht*, 6. Aufl. 2025, 15. Kapitel Rn. 25; *Schrott* JuS 2022, 138, 140.

¹² *Puschke/Haas* RdZ 2022, 4, 8.

¹³ Vgl. entsprechend BGH NJW 2016, 1336, 1337.

¹⁴ A.A. *Christoph/Dorn-Haag* NStZ 2020, 697, 702.

¹⁵ *Böse/Tomiak* ZfStw 2023, 265, 273 f.; *Burghardt/Bardowicks* ZJS 2023, 593, 602; *Puschke/Haas* RdZ 2022, 4, 8; *Schmidt*, in *Beck'scher Online-Kommentar StGB*, 65. Ed. 2025, § 263a Rn. 29.

¹⁶ Vgl. auch *Burghardt/Bardowicks* ZJS 2023, 593, 602; *Lichtenthäler* FD-StrafR 2024, 823638; *Schmidt* (Fn. 15), § 263a Rn. 29.

¹⁷ So etwa OLG Hamm NStZ 2020, 673, 675; *Göhler* JR 2021, 6, 18.

¹⁸ So etwa *Christoph* ZJS 2022, 761, 767.

¹⁹ Vgl. *Omlor* RdZ 2021, 180, 184.

Gesetzgeber hat sich zur Umsetzung dieses Ziels aber gerade dazu entschieden, keinen gänzlichen Verzicht der Berichtigungsabfrage, sondern nur einen bedingten, also kontrollbasierten Verzicht zu erlauben. Die Annäherung von EC-Karte und Bargeld ergibt sich im Falle einer NFC-Zahlung also im Wege einer faktisch vereinfachten Kartennutzung. Der Nutzung der Karte wohnt in Abgrenzung zur Nutzung von Bargeld in jedem Fall einer NFC-Zahlung eine Erklärung über die Berechtigung zur Nutzung inne.²⁰

d) Dies gilt umso mehr, wenn man berücksichtigt, dass Unberechtigte im Vorfeld regelmäßig keine Kenntnis hinsichtlich der berechtigten Nutzung der Karte haben. Ohne hinzutretendes Sonderwissen ist es eine Frage des Zufalls, ob sich die unberechtigte Person einem Berechtigungsnachweis entziehen kann oder nicht.²¹ Ebenso entspricht es der Lebenswirklichkeit, dass auch berechtigte Personen nicht in jedem Fall einer kontaktlos initiierten Zahlung sichere Kenntnis über das Vorliegen der Voraussetzungen für die Aussetzung der Abfrage der starken Kundenauthentifizierung haben. So wird sich bei Geschäften des täglichen Lebens etwa nur in Ausnahmefällen in Erinnerung zu rufen sein, ob die Gesamtzahlungsgrenze von 150 € mit der vierten oder der fünften Transaktion überschritten wird.

II. Zusammenfassend ist zu sagen, dass das BayObLG zu Unrecht von einem zwingenden Gleichlauf der Durchsetzung einer starken Kundenauthentifizierung i.S.v. § 55 I Nr. 2 ZAG im Einzelfall und unbefugter Datenverwendung i.S.v. § 263a I Var. 3 StGB durch eine unberechtigte EC-Kartennutzung ausgeht.²² Wird eine fremde EC-Karte im kontaktlosen NFC-Verfahren missbraucht, ist der objektive Tatbestand des Computerbetrugs erfüllt.²³

²⁰ S. entsprechend die Wertung von § 935 II BGB; demgegenüber schließt *Kudlich* JA 2020, 710, 712 aufgrund der Nähe der NFC-Zahlung zur Barzahlung auf einen Gleichlauf zur Straflosigkeit der Zahlung mit gestohlenem Bargeld; ebenso *Ceffinato* JuS 2021, 311, 313; ablehnend zudem *Bechtel* ZJS 2023, 1339, 1351.

²¹ *Böse/Tomiak* ZfIStw 2023, 265, 274; *Puschke/Haas* RdZ 2022, 4, 8 f.

²² Ebenso *Schmidt* (Fn. 15), § 263a Rn. 29; i.E. auch *Oğlakcioğlu* JA 2018, 338, 341.

²³ S. zu Anforderungen an den Vorsatznachweis *Puschke/Haas* RdZ 2022, 4, 9; s. zu Bedenken bezüglich der notwendigen Stoffgleichheit zwischen Vermögensschaden und angestrebter Bereicherung *Burghardt/Bardowicks* ZJS 2023, 593, 605 f.