3. Jg. | 24.2.2022 | Seiten 1–72 | www.rdz-online.de

# Recht der Zahlungsdienste

1. 2022 Betriebs-Berater Geldverkehr



Fachmedien Recht und Wirtschaft | dfv Mediengruppe | Frankfurt am Main

# Missbrauch von Zahlungskarten im digitalen Zeitalter – Zur strafrechtlichen Bewertung nicht autorisierter NFC-Zahlungen

Die Bedeutung bargeld- und kontaktloser Zahlungen nimmt auch in Deutschland zu. Insbesondere die Near-Field-Communication-(NFC-)Technik verspricht eine unkomplizierte und kontaktlose Abwicklung von Zahlungen vor Ort. Wie jeder technische Fortschritt bergen aber auch NFC-Zahlungen Missbrauchsmöglichkeiten. Der nachfolgende Beitrag analysiert die relevanten Straftatbestände in diesem Bereich, wobei ein Schwerpunkt auf der Erfassung des Tatunrechts als Vermögensstraftat liegt.

Prof. Dr. Jens Puschke, LL.M. (King's College), und Dipl.-Jur. Janick Haas

## I. Einleitung

Das Strafrecht ist eine Materie, die sich gesellschaftlichen und technischen Entwicklungen nur langsam anpasst. Der Bestimmtheitsgrundsatz und das Ultima Ratio-Prinzip verlangen eine passgenaue Normierung, welche Verhaltensweisen als (neues) strafrechtliches Unrecht zu erfassen sind und welche einer Bearbeitung durch andere Rechtsgebiete, insbesondere das Zivilrecht, überlassen bleiben können und sollen. Das Analogieverbot zu Lasten des Täters sperrt zudem eine Erfassung von Missbrauchsverhalten, welches den Tatbestandmerkmalen existierender Strafnormen nicht unmittelbar unterfällt. Folge dessen ist, dass Missbrauch technischer Innovationen häufig auf Strafnormen trifft, die hierauf nicht ausgerichtet sind und deren Anwendung deshalb auf erhebliche Schwierigkeiten stößt. Eine aktuelle Entwicklung, auf die dieser Befund zutrifft, stellt der bargeld- und mittels NFC-Technik kontaktlose Zahlungsverkehr dar. Entscheidende Besonderheit bei einer kontaktlosen Zahlung ist, dass unter bestimmten Bedingungen auf die Abfrage einer persönlichen Identifikationsnummer (PIN) am Bezahlterminal verzichtet wird, wodurch sich diese Zahlungsweise von der nach wie vor dominierenden Nutzung von Zahlungskarte und PIN-Eingabe maßgeblich unterscheidet. Während der strafrechtliche Umgang mit dem Missbrauch von Zahlungskarten und PIN zwar immer noch umstritten ist, aber auf Basis jahrzehntelanger wissenschaftlicher Diskussionen und vielzähliger einschlägiger Rechtsprechung rechtlich weitgehend durchdrungen zu sein scheint, werden für den Missbrauch bei NFC-Zahlungen die strafrechtlichen Pflöcke gerade erst eingeschlagen.

## II. Problemaufriss

### 1. Grundlagen

Die Zahlungsabwicklung mittels einer Zahlungskarte im Präsenzhandel erfolgt in Deutschland regelmäßig im Wege des sog. Point-of-Sale-Verfahrens (POS). Dieses Verfahren basiert auf einer Abrede zwischen der Deutschen Kreditwirtschaft, den kartenausgebenden Kreditinstituten und den Handelsunternehmen, die POS-Terminals betreiben, welche die bargeldlose Zahlung beim Handelsunternehmen ermöglicht.[1] Erfolgt die Zahlung mittels einer Zahlungskarte beim Handelsunternehmen und wird die Zahlungsabwicklung durch das Kreditinstitut autorisiert, gibt dieses gegenüber dem Handelsunternehmen eine Zahlungsgarantie gem. § 780 BGB ab, die es zur Begleichung des autorisierten Betrags irreversibel verpflichtet.[2] Der Anspruch des Zahlungsempfängers ist grundsätzlich vollwertig – unabhängig davon, ob die Zahlung unberechtigt in Auftrag gegeben wurde.[3] Nach Abschluss des elektronischen Zahlungsvorgangs werden die geschuldeten Waren an den Kartennutzer übereignet. Das Kreditinstitut erhält gegen den Karteninhaber einen Aufwendungsersatzanspruch gem. §§ 675c, 670 BGB, womit das entsprechende Konto belastet wird.[4]

Bei der herkömmlichen Nutzung der Zahlungskarte wird diese durch ein Lesegerät gezogen oder in ein solches geschoben. Der Kunde wird anschließend aufgefordert, eine PIN einzugeben. Die Autorisierung erfolgt nach Überprüfung der Karte und Kontodeckung sowie der zugehörigen PIN als Authentifizierungsmerkmal.[5] Bei der Nutzung der NFC-Technik wird die Zahlungskarte nur kurz in die Nähe des Lesegeräts gehalten, um den Bezahlvor-

1 Eingehend *Koch*, in: Schimansky/Bunte/Lwowski (Hrsg.), Bankrechts-Handbuch, 5. Aufl. 2017, § 68, Rn. 2.
2 *Omlor*, in: Staudinger, BGB, 2020, § 675f, Rn. 124.
3 *Göhler*, JR 2021, 6, 8; s. zum kollusiven Zusammenwirken *Hoyer*, in: Wolter (Hrsg.), Systematischer Kommentar zum StGB, 9. Aufl. 2021, § 263, Rn. 79.
4 S. nur *Sprau*, in: Grüneberg, BGB, 81. Aufl. 2022, § 675f, Rn. 52.
5 Vgl. nur *Omlor* (Fn. 2), § 675f, Rn. 121.

gang einzuleiten.[6] Eine Abfrage der PIN erfolgt nur unter bestimmten Voraussetzungen. Zwar besteht grundsätzlich die aufsichtsrechtliche Pflicht der kartenausgebenden Kreditinstitute, eine sog. starke Kundenauthentifizierung für die Abwicklung einer Zahlung im POS-Verfahren zu verlangen (Art. 97 Abs. 1 Buchst. b PSD II[7], § 55 Abs. 1 Nr. 2 ZAG), die etwa durch Eingabe der PIN gewährleistet wird. Allerdings gestattet Art. 98 Abs. 1 Buchst. b Abs. 3 PDS II die Schaffung von technischen Regulierungsstandards, wovon durch die VO (EU) 2018/389[8] Gebrauch gemacht wurde, die gem. § 55 Abs. 5 ZAG Anwendung findet. Art. 11 dieser Verordnung normiert, dass von einer sog. starken Kundenauthentifizierung abgesehen werden kann, wenn ein einzelner Zahlungsbetrag 50 Euro nicht überschreitet und zusätzlich entweder alle erfolgten Zahlungen ohne PIN-Eingabe 150 Euro in Summe nicht übersteigen oder nicht mehr als fünf Zahlungen ohne PIN-Eingabe getätigt werden. Darüber hinaus steht es den Kreditinstituten frei, die PIN in weiteren Fällen, etwa nach dem Zufallsprinzip, abzufragen, um Missbrauch vorzubeugen. In grundsätzlich vergleichbaren Bahnen erfolgt die kontaktlose Zahlung im Wege des Mobile Payment v. a. mittels App-Unterstützung. Es können so Konten eingepflegt und unkompliziert zur Zahlung ausgewählt werden. Hier dient das NFC-fähige mobile Endgerät als virtuelle Zahlungskarte und wird an das POS-Terminal gehalten.[9]

Hält man eine Zahlungskarte zur kontaktlosen Zahlung vor ein Lesegerät, werden die relevanten Kartendaten, wie der zu zahlende Rechnungsbetrag und etwaige Daten zum Zahlungsempfänger (im Falle des Mobile Payment auch weitere appspezifische Daten[10]), an einen zentralen Rechner des Kreditinstituts übermittelt. Dort werden die grundsätzlichen Voraussetzungen für eine elektronische Transaktion sowie die notwendigen Parameter für ein kontaktloses Zahlen ohne PIN überprüft.[11] Mangels starker Kundenauthentifizierung liegt dann bereits in der Vorhaltung der Zahlungskarte am POS-Terminal die Zustimmung für eine nachfolgende Autorisierung der Zahlung.[12] Sind die Voraussetzungen für den Verzicht auf die PIN-Abfrage nicht gegeben, wird eine Authentifizierung wie im herkömmlichen Verfahren verlangt.

### 2. Missbrauchskonstellationen

Strafrechtlich relevante Missbrauchskonstellationen ergeben sich für Zahlungskarten allgemein bzgl. der Erlangung der Karten und der Karteninformationen im Vorfeld einer Nutzung.[13] Von Bedeutung ist zudem die Nutzung der Zahlungskarte nach vorangegangenem Eigentumsdelikt[14] sowie bei Überschreitung eines grundsätzlich eingeräumten Verfügungsspielraums.[15] Schließlich wird die Strafbarkeit der Verwendung von gefälschten Karten diskutiert.[16] Die missbräuchliche Nutzung der NFC-Technik erfolgt vorrangig zur Bezahlung von Waren an POS-Terminals im Handel mittels einer echten NFC-fähigen (virtuellen) Zahlungskarte durch einen Nichtberechtigten. Des Weiteren kann die NFC-Technik durch mobile POS-Terminals im Wege eines sog. elektronischen Taschendiebstahls ausgenutzt werden, um damit kleinere Beträge abzubuchen.[17] Dafür werden tragbare POS-Terminals mit voreingestellten abzubuchenden Beträgen möglichst nah an potenziell NFC-fähige Karten oder Geräte gehalten, um durch die Passivität der NFC-Technik unbemerkt einen Transaktionsvorgang auszulösen.[18] Der Beitrag nimmt die beiden letzten Missbrauchskonstellationen näher in den Blick.

## III. Strafrechtliche Bewertung

Für die strafrechtliche Bewertung ist zunächst bedeutsam, welche (natürlichen) Personen an der Transaktion beteiligt sind und an welcher Stelle ein Vermögensschaden eintritt. Hiernach entscheidet sich, ob das Verhalten eine Täuschung darstellt, die einen Irrtum hervorrufen kann, womit eine Betrugsstrafbarkeit gem. § 263 StGB in Betracht kommt, oder ob sich das Verhalten als unbefugte Verwendung von Daten gem. § 263a Abs. 1 Alt. 3 StGB darstellen kann. Zudem ist relevant, inwieweit auch ohne das Erfordernis der Eingabe einer PIN die nach außen erkennbare Behauptung einer Authentizität des Kartennutzers vorliegt. Das Bestehen oder Nichtbestehen des Anscheins, als Berechtig-

6 S. näher zur technischen Funktionsweise von NFC *Christoph/Dorn-Haag*, NStZ 2020, 697 f.
7 Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG, ABlEU vom 23.12.2015, L 337, 35.
8 Delegierte Verordnung (EU) 2018/389 der Kommission vom 27. November 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, ABlEU vom 13.3.2018, L 69, 23.
9 *Casper*, in: Säcker u. a. (Hrsg.), Münchener Kommentar zum BGB, 8. Aufl. 2020, § 675f, Rn. 149; *Köndgen*, in: Gsell u. a. (Hrsg.), BeckOGK BGB, Stand: 1.8.2021, § 675c, Rn. 125; *Omlor*, RdZ 2021, 180.
10 *Jungmann*, in: Säcker u. a. (Hrsg.), Münchener Kommentar zum BGB, 8. Aufl. 2020, § 675j, Rn. 61.
11 Vgl. *Göhler* (Fn. 3).
12 *Göhler* (Fn. 3), 6, 9.
13 S. etwa BGH, 17.8.2004 – 5 StR 197/04, NStZ-RR 2004, 333, zur abgenötigten Kenntnis der PIN; hierzu auch BGH, 11.8.2021 – 3 StR 63/21, NStZ-RR 2022, 14, 16; s. zur Strafbarkeit durch das Erschleichen der Zahlungskarte samt PIN BGH, 16.7.2015– 2 StR 16/15, wistra 2016, 71 ff.; s. hierzu beispielhaft auch *Tiedemann/Valerius*, in: Laufhütte/Rissing-van Saan/Tiedemann (Hrsg.), Leipziger Kommentar zum StGB, 5. Aufl. 2020, § 263a StGB, Rn. 47 ff.
14 S. BGH, 30.1.2001 – 1 StR 512/99, NStZ 2001, 316 f.
15 S. zu erschlichener Kenntnis der PIN und Überlassung der Zahlungskarte OLG Jena, 20.9.2006 – 1 Ss 226/06, wistra 2007, 236 f.; BGH, 31.3.2004 – 1 StR 482/03, NStZ 2005, 213.
16 BGH, 8.10.2013 – 2 StR 342/13, StV 2014, 543; BGH, 21.9.2000 – 4 StR 284/00, NStZ 2001, 140 ff.; BGH, 17.6.2008 – 1 StR 229/08, NStZ-RR 2008, 280.
17 S. hierzu *Christoph/Dorn-Haag* (Fn. 6), 697 ff.
18 S. zu entsprechenden Risiken *Christoph/Dorn-Haag* (Fn. 6), 697, 698.

ter die Zahlung zu veranlassen, kann sowohl für eine Strafbarkeit wegen Betrugs bzw. Computerbetrugs (§§ 263, 263a StGB) als auch bei den Datenurkundendelikten (§§ 269, 270, 274 Abs. 1 Nr. 2 StGB) eine Rolle spielen. Zudem ist für die Einschlägigkeit etwaiger Datendelikte nach der Datensicherung und der vorgenommenen Datenveränderung durch die Transaktion zu fragen.

Die Strafbarkeit einer unberechtigten Zahlung im NFC-Verfahren wird in Rechtsprechung und Literatur kontrovers diskutiert und in der soweit ersichtlich bisher einzigen einschlägigen veröffentlichten Entscheidung eines Oberlandesgerichts durch das OLG Hamm thematisiert.[19] Der Entscheidung lag der Sachverhalt zugrunde, dass eine verlorene Brieftasche samt Zahlungskarte gefunden, eingesteckt und anschließend mehrfach für kleinere Einkäufe zur kontaktlosen Zahlung genutzt wurde. Somit konnte – wie vom Angeklagten beabsichtigt – über fremdes Vermögen verfügt werden, ohne eine PIN eingeben zu müssen. Das Tatgericht (AG Paderborn) erfasste dieses Verhalten als Computerbetrug (§ 263a StGB). Das LG Paderborn hat daraufhin als Berufungsgericht den Schuldspruch hin zu einem Betrug (§ 263 StGB) geändert.[20] Das OLG Hamm als Revisionsgericht konnte in dem Verhalten lediglich eine Urkundenunterdrückung gem. § 274 Abs. 1 Nr. 2 StGB und nachrangig eine Datenveränderung gem. § 303a Abs. 1 StGB erkennen.

### 1. Vermögensdelikte

Für die unberechtigte Nutzung einer Zahlungskarte ist es naheliegend, zunächst das Vorliegen eines Vermögensdelikts näher in den Blick zu nehmen. Durch den Missbrauch der Zahlungskarte entsteht ein Vermögensschaden bei dem die Karte emittierenden Kreditinstitut, das den Schaden nur in Ausnahmefällen (§ 675v Abs. 4 BGB) an die Kunden weiterreichen kann. Da an der Abwicklung einer Transaktion bei Warenkauf sowohl Personen (Kassenpersonal am POS-Terminal) als auch Computer beteiligt sind, kommen vornehmlich Strafbarkeiten wegen Betrugs und Computerbetrugs in Betracht.

#### a) Betrug gem. § 263 StGB

Der Betrug setzt eine Täuschung eines Menschen und einen entsprechenden menschlichen Irrtum voraussetzt, weshalb für die Konstellation des Warenkaufs als Täuschungsadressat lediglich der Händler bzw. dessen Kassenpersonal relevant sein können. Aufgrund der Zahlungsgarantie des Kreditinstituts und des so bestehenden vollwertigen Zahlungsanspruchs des Händlers tritt bei diesem jedoch kein Vermögensschaden ein. Die Vermögensabflüsse durch die Übereignung und Herausgabe der Ware werden vollständig kompensiert. Ein Betrug zu seinen Lasten scheidet damit aus. Auch ein Betrug zu Lasten des Karteninhabers liegt nicht vor. Zum einen geht die kontobelastende Vermögensverfügung nicht vom Händler, sondern vom Kreditinstitut aus. Bei diesem fehlt es jedoch an einem menschlichen Täuschungsadressat. Zum anderen erleidet auch der Karteninhaber in aller Regel keinen Vermögensschaden, da das Missbrauchsrisiko bei der Nutzung der NFC-Technik bei dem Kreditinstitut liegt.

Möglich erscheint daher nur die Bewertung als Dreiecksbetrug gegenüber dem Händler und zu Lasten des Kreditinstituts.[21] Vorausgesetzt bleibt jedoch, dass der Händler bzw. das Kassenpersonal getäuscht wurden und einem Irrtum unterlagen. Es kann allerdings nur über solche Tatsachen getäuscht werden, über die sich der potenzielle Täuschungsadressat in der konkreten Situation tatsächlich Gedanken macht oder wenigstens machen müsste.[22] Aufgrund der Zahlungsgarantie des Kreditinstituts, die auch im Falle einer unberechtigten Kartennutzung gilt,[23] spielt die Berechtigung für das Handelsunternehmen jedoch keine Rolle. Dementsprechend müssen sich Händler bzw. dessen Kassenpersonal keine Gedanken über die tatsächliche Berechtigung der Kartennutzung machen. Ein Betrug kommt also auch in dieser Konstellation nicht in Betracht.

Bei einer Vermögensschädigung im Wege eines elektronischen Taschendiebstahls fehlt es darüber hinaus von vornherein an einer aktiven Kommunikation mit einer natürlichen Person, sodass auch hier eine Täuschung und damit eine Strafbarkeit wegen Betrugs ausscheidet.[24]

#### b) Computerbetrug gem. § 263a StGB

Eine Strafbarkeit wegen Computerbetrugs gem. § 263a StGB erfordert anders als eine solche gem. § 263 StGB keine Täuschung eines Menschen. Wird eine echte Zahlungskarte missbraucht, kommt eine Strafbarkeit wegen der unbefugten Verwendung von Daten gem. § 263a Abs. 1 Alt. 3 StGB in Betracht. Durch die Nutzung der Zahlungskarte im NFC-Verfahren werden kodierte Kunden- und Transaktionsinformationen in einen Datenverarbeitungsvorgang eingebracht, der zur Autorisierung der veranlassten Zahlung durch das Kreditinstitut führt. Die Verwendung dieser Daten durch einen Nichtberechtigten führt zudem zu einem Vermögensschaden beim Kreditinstitut. In subjektiver Hinsicht erstrebt der Kartennutzer einen Vermögensvorteil. Zwar kommt es ihm primär auf die Erlangung der Waren an. Die vorausgesetzte Stoffgleichheit zwischen Vermögensschaden und angestrebtem Vermögensvorteil ergibt sich jedoch daraus, dass als notwendiges Zwischenziel zur Erlangung der Ware ohne eige-

19 OLG Hamm, 7.4.2020 – 4 RVs 12/20, NStZ 2020, 673.
20 LG Paderborn, 14.10.2019 – 3 Ns 109/19, BeckRS 2019, 57601.
21 S. aber *Göhler* (Fn. 3), 6, 14 ff.
22 Hierzu und zu Folgendem OLG Hamm (Fn. 19), 673, 674.
23 Vgl. *Altenhain*, JZ 1997, 752, 754; *Waßmer*, in: Satzger/Schluckebier/Widmaier (Hrsg.), StGB, 5. Aufl. 2021, § 263a, Rn. 15 ff.
24 *Christoph/Dorn-Haag* (Fn. 6), 697, 700.

ne Gegenleistung auch das Zahlungsversprechen des Kreditinstituts von der Bereicherungsabsicht erfasst ist. Dieser Vermögensvorteil entspricht dem bei dem Kreditinstitut eingetretenen Schaden und beruht auf demselben Verfügungsvorgang.[25] Insofern bestehen keine Unterschiede gegenüber der Bewertung der Nutzung einer Zahlungskarte mit PIN. Gleiches gilt im Grundsatz auch für die Konstellation des sog. elektronischen Taschendiebstahls, wobei sich hier die Bereicherungsabsicht unmittelbar auf das Zahlungsversprechen des Kreditinstituts bezieht.

### aa) Grundlagen zur unbefugten Datenverwendung

Die entscheidende Frage ist, ob es sich um eine unbefugte Verwendung der Daten gem. § 263a Abs. 1 Alt. 3 StGB handelt. Vor diesem Hintergrund hat im entsprechenden Fall das OLG Hamm gegen eine Erfassung als Computerbetrug argumentiert.[26] Dieser Einschätzung hat sich die Literatur bisher überwiegend angeschlossen.[27] Ausgangspunkt ist eine sog. betrugsspezifische Auslegung des Merkmals „unbefugt", die in der jüngeren Rechtsprechung und in der Literatur gegenüber anderen Auslegungsmöglichkeiten favorisiert wird.[28] Demnach kann eine Datenverwendung nur dann als unbefugt angesehen werden, wenn sie gegenüber einer fiktiven natürlichen Person als Täuschung zu werten wäre. Der Rückgriff auf eine betrugsspezifische Konturierung des Merkmals „unbefugt" überzeugt. Sie kann sich auf die Entstehungsgeschichte der Norm stützen und fördert ihre Harmonisierung mit dem Betrugstatbestand.[29] Dagegen überdehnt eine subjektive Auslegung[30] den Tatbestand, indem sie das Merkmal „unbefugt" als „gegen oder ohne den Willen des Verfügungsberechtigten" interpretiert und so die Art und Weise der Herbeiführung der Vermögensschädigung für unbeachtlich erklärt.[31] Die computerspezifische Auslegung, die von einer unbefugten Datenverwendung bei entgegenstehendem Willen des Berechtigten ausgeht, der sich in der Programmgestaltung niedergeschlagen hat,[32] ist dabei zu restriktiv angelegt. Fälle unberechtigter Nutzung authentischer Daten könnten so nicht adäquat erfasst werden.[33]

### bb) Prüfmaßstab der Rechtsprechung

Da die entscheidende Autorisierung vom Kreditinstitut ausgeht, ist auf eine fiktive Person auf Seiten der kartenemittierenden Bank als Täuschungsadressat abzustellen und zu fragen, ob der Kartennutzer gegenüber dieser fiktiven Person seine Berechtigung zur Verwendung der Karte täuschend vorspiegelt. Das OLG Hamm nimmt jedoch – dem BGH folgend[34] – eine Einschränkung hinsichtlich des Prüfmaßstabs vor. Es sei nicht auf einen fiktiven Bankangestellten abzustellen, der die Interessen der Bank im Autorisierungsverfahren 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.[35] Die fiktive Kontrollperson könne – genau wie das Programm – nur den Besitz der Karte und gerade keine Berechtigung i. S. e. starken Kundenauthentifizierung überprüfen.[36] Ein konkludenter Erklärungsgehalt der Kartennutzung i. S. e. Vorspiegelung der Berechtigung könne allein der Eingabe einer PIN zukommen, an der es bei der erfolgreichen kontaktlosen Zahlung gerade fehle.[37] Mit dieser Beschränkung des Prüfmaßstabs nähert die Rechtsprechung die betrugsspezifische Auslegung des Merkmals „unbefugt" der computerspezifischen Auslegung an. Auch dem ist im Grundsatz zuzustimmen. Nur ein Rückgriff auf die konkreten Umstände des Einzelfalls wird einer Beschränkung der Strafbarkeit wegen Computerbetrugs hinreichend gerecht. Würde demgegenüber auf eine fiktive Person abgestellt werden, die sich über alles unabhängig vom Einzelfall Gedanken machte, wäre die Parallele zum Betrug verlassen.

### cc) Normative Interpretation des Verhaltens

Diese im Ausgangspunkt richtige Argumentation greift allerdings für die strafrechtliche Beurteilung der Nutzung der NFC-Technik zu kurz. Da für die Feststellung der Täuschungsäquivalenz nicht auf eine konkrete natürliche Person zurückgegriffen werden kann, kommt es auf eine normative Interpretation des Verhaltens des Handelnden an.[38] Grundlage dieser Interpretation ist der jeweilige Geschäftstypus in seiner konkreten Ausgestaltung,[39] die bei einer computergestützten Abwicklung durch die Vorgaben des Prüfprogramms beeinflusst wird. Für die Bejahung des Merkmals „unbefugt" kann insoweit nicht entscheidend

25 *Altenhain* (Fn. 23), 752, 756; *Hefendehl/Noll*, in: Erb/Schäfer (Hrsg.), Münchener Kommentar zum StGB, 4. Aufl. 2022, § 263a, Rn. 185; krit. mit beachtlichen Gründen *Göhler* (Fn. 3), 6, 18 ff.
26 OLG Hamm (Fn. 19), 673, 674 f.
27 *Ceffinato*, JuS 2021, 311, 313; *Christoph/Dorn-Haag* (Fn. 6), 697, 700; *Duttge*, in: Dölling/Duttge/Rössner (Hrsg.), Gesamtes Strafrecht, 5. Aufl. 2022, § 263a StGB, Rn. 19; *Göhler* (Fn. 3), 6, 18; *Heghmanns*, ZJS 2020, 494, 495 f.; *Eisele*, in: Hilgendorf/Kudlich/Valerius (Hrsg.), Handbuch des Strafrechts, Bd. 6, 2022, § 63, Rn. 137; *Hefendehl/Noll* (Fn. 25), § 263a, Rn. 109; a. A. *Schmidt*, in: v. Heintschel-Heinegg (Hrsg.), BeckOK StGB, Stand: 1.11.2021, § 263a, Rn. 29.
28 S. nur BGH, 22.11.1991 – 2 StR 376/91, NJW 1992, 445, 446; BGH, 20.12.2012 – 4 StR 580/11, NJW 2013, 1017, 1018; *Perron*, in: Schönke/Schröder, StGB, 30. Aufl. 2019, § 263a, Rn. 2 m. w. N.
29 *Hefendehl/Noll* (Fn. 25), § 263a, Rn. 87.
30 BGH, 10.11.1994 – 1 StR 157/94, NJW 1995, 669 f.; *Mitsch*, JZ 1994, 877, 883.
31 *Hefendehl/Noll* (Fn. 25), § 263a, Rn. 89.
32 OLG Celle, 11.4.1989 – 1 Ss 287/88, NStZ 1989, 367, 368; *Achenbach*, JR 1994, 293, 295.
33 *Hefendehl/Noll* (Fn. 25), § 263a, Rn. 88.
34 BGH, 21.11.2001 – 2 StR 260/01, NJW 2002, 905, 906.
35 OLG Hamm (Fn. 19), 673, 674 f.
36 OLG Hamm (Fn. 19), 673, 675; s. zu den Elementen der starken Kundenauthentifizierung *Göhler* (Fn. 3), 6, 7.
37 *Christoph/Dorn-Haag*, NStZ 2020, 676.
38 *Hefendehl/Noll* (Fn. 25), § 263a, Rn. 79; *Hoyer*, in: Wolter (Hrsg.), Systematischer Kommentar zum StGB, 9. Aufl. 2019, § 263a, Rn. 20.
39 BGH, 20.12.2012 (Fn. 28); *Schmidt* (Fn. 27), § 263a, Rn. 25.

sein, ob das Programm bzw. die an dessen Stelle gedachte natürliche Person als Täuschungsadressat die Berechtigung tatsächlich überprüft bzw. in jedem Einzelfall die Möglichkeit der Überprüfung besteht. Die hier in Rede stehende Äquivalenz zu einer konkludenten Täuschung beim Betrug zeigt vielmehr, dass es ausreichend ist, dass bestimmte Tatsachen als miterklärt vorausgesetzt werden,[40] wie es etwa bei der Täuschung über die Zahlungswilligkeit der Fall ist. Ebenso schließt der Verzicht auf eine an sich bestehende Überprüfungsmöglichkeit eine Betrugsstrafbarkeit nicht aus.[41] Stellt man demgegenüber allein auf die nicht erfolgte tatsächliche Überprüfung im Einzelfall ab, würde die betrugsspezifische Auslegung auf eine rein computerspezifische Überprüfung reduziert werden.

dd) Täuschungsäquivalenz bei bedingtem Kontrollverzicht

Entsprechend kann auch der bedingte Verzicht auf die technische Überprüfung der Berechtigung mittels Abfrage der PIN allein nicht ausschlaggebend für die Annahme oder Ablehnung des Merkmals „unbefugt" sein.[42] Relevant ist vielmehr, ob sich bei der Würdigung der gesamten Umstände des Datenverwendungsvorgangs das Verhalten des Datenverwenders, hier des Kartennutzers, als unbefugt darstellt, mithin Täuschungscharakter hat. Bedeutsam ist dabei, ob einer fiktiven Person anstelle des die Autorisierung auslösenden Computerprogramms sachgedankliches Mitbewusstsein hinsichtlich der Berechtigung des Kartennutzers unterstellt werden kann. Verwendet der nicht berechtigte Kartennutzer eine Zahlungskarte mit zugehöriger PIN, ergibt sich der Täuschungscharakter über die Berechtigung ohne Weiteres daraus, dass die Nutzung der PIN nur dem Berechtigten zusteht. Wird eine Zahlungskarte unter Eingabe der PIN verwendet, wird dementsprechend überwiegend davon ausgegangen, dass hierin ein Computerbetrug gem. § 263a Abs. 1 Alt. 3 StGB zu erblicken sei.[43] Aber auch ohne die Eingabe der PIN kann die Nutzung einer Zahlungskarte täuschenden Charakter haben und damit unbefugt i. S. d. § 263a Abs. 1 Alt. 3 StGB erfolgen. Dies setzt voraus, dass bei der notwendigen Gesamtwürdigung des Verhaltens unter Zugrundelegung des Geschäftstypus und der Prüfmechanismen des Computerprogramms die Berechtigung zur Nutzung der Zahlungskarte miterklärt wird. Dabei ist zu beachten, dass nicht bei jeder kontaktlosen Zahlung mit einer Zahlungskarte im NFC-Verfahren auf die Eingabe einer PIN verzichtet, diese vielmehr lediglich unter gewissen Bedingungen ausgesetzt wird.[44] Die Bedingungen für diese Aussetzung der PIN-Eingabe muss der gedachte Erklärungsadressat wie auch das Programm bei jeder NFC-Zahlung mit einer Zahlungskarte überprüfen. Dies dient dem Schutz vor missbräuchlicher Verwendung und der Begrenzung des Verlustrisikos.[45] Eine die Berechtigung nachweisende Authentifizierung ist somit im Programm angelegt.[46] Insofern besteht auch ein entscheidender Unterschied zur Zahlung mit abhandengekommenem Bargeld.[47] Die Wertung des § 935 Abs. 2 BGB ist auf NFC-Zahlungen nicht übertragbar,[48] da die Überprüfung der Berechtigung zur Nutzung der Zahlungskarte anders als jene der Herkunft des Gelds im konkreten Geschäftstypus angelegt ist. Zudem regelt § 935 Abs. 2 BGB eine explizite Ausnahme gerade für Bargeld. Die Bargeldnähe einer kontaktlosen Zahlung ergibt sich daher nicht aus dem Verzicht auf die Prüfung einer Berechtigung, sondern vielmehr aus der im Vergleich zur herkömmlichen POS-Zahlung gesteigerten Effizienz der Bezahlweise.[49]

Für die Annahme der Täuschungsäquivalenz des Verhaltens ist zudem beachtlich, inwieweit bei einer objektivierten Betrachtung die Bedingungen für die Aussetzung der Berechtigungsüberprüfung durch das Kartennutzungsverhalten steuerbar sind. Ist die Geschäftsabwicklung so angelegt, dass eine Berechtigungsüberprüfung äußerlich unbemerkt stets und ohne Sonderwissen vermeidbar ist, kann dem Verhalten nicht die Aussage beigemessen werden, sich einer entsprechenden Überprüfung, wenn nötig, zu stellen. Es entfällt der Täuschungscharakter.[50] Allerdings liegt eine derartige Überprüfung durch die PIN-Abfrage bei einer NFC-Zahlung nicht allein in den Händen des Kartennutzers. Zwar kann dieser den Verfügungsrahmen unter 50 Euro halten, so dass jedenfalls diese Bedingung für das Absehen von einer starken Kundenauthentifizierung beeinflusst werden kann. Regelmäßig besteht jedoch keine Kenntnis des unberechtigten Kartennutzers über die seiner Nutzung vorausgehenden Verfügungen. Ob die Gesamtverfügungen, inklusive der nunmehr anstehenden Zahlung, weder 150 Euro noch fünf Verfügungen ohne PIN-Eingabe übersteigen, ist bei der Verwendung der Karte nicht erkennbar. Ob auf die PIN-Abfrage verzichtet wird, ist aus Sicht des Unberechtigten daher eine Frage des Zufalls. Verwendet er unter diesen Bedingungen die Zahlungskarte, wird konkludent miterklärt, dass er als Berechtigter handelt und die Berechtigung bei Abfra-

40 So auch *Hefendehl/Noll* (Fn. 25), § 263a, Rn. 82.
41 S. etwa für einen Irrtum über die Echtheit des Geldes BGH, 22.11.2013 – 3 StR 162/13, NStZ 2014, 215, 216.
42 Zur darin liegenden Verantwortungsverschiebung in Richtung der Bank *Heghmanns* (Fn. 27), 494, 496, was allerdings noch keine Aussage zum Ausschluss der strafrechtlichen Verantwortlichkeit des unberechtigten Kartennutzers beinhaltet.
43 S. hierzu und zu etwaigen Einschränkungen *Waßmer* (Fn. 23), § 263a, Rn. 16 m. w. N.
44 Anders etwa *Ceffinato* (Fn. 27).
45 *Hoffmann/Rastegar*, WM 2021, 957, 959.
46 S. zur Täuschungsaquivalenz auch BGH, 3.3.2016 – 4 StR 496/15, NJW 2016, 1336, 1337.
47 I. E. ebenso *Schmidt* (Fn. 27), § 263a, Rn. 29.
48 Anders *Ceffinato* (Fn. 27).
49 Vgl. etwa *Omlor* (Fn. 9), 180, 184.
50 BGH, 3.3.2016 – 4 StR 496/15, NJW 2016, 1336, 1337, lässt weitergehend im Programm angelegte Höchstgrenzen für Wetteinsätze als täuschungsäquivalent für die Behauptung einer Nichtmanipulation ausreichen; s. auch BGH, 20.12.2012 – 4 StR 580/1, NJW 2013, 1017, 1018.

ge nachweisen kann.[51] Die erfolgte Datenverwendung ist als unbefugt anzusehen. Dieses Ergebnis kann somit auf einer betrugsspezifischen Auslegung des Merkmals „unbefugt" unter Einbeziehung der Ausgestaltung des prüfenden Computerprogramms begründet werden. Einer Rückbesinnung auf eine subjektive Auslegung des Merkmals bedarf es hierfür nicht.[52]

#### ee) Vorsatz

Die abschließende Entscheidung über die Strafbarkeit gem. § 263a Abs. 1 Alt. 3 StGB hängt zudem von dem Vorliegen des Vorsatzes des Kartennutzers bzgl. der Modalitäten der PIN-Abfrage ab. Der Handelnde muss insofern die Möglichkeit erkennen, dass eine PIN-Abfrage erfolgen könnte, wovon jedenfalls bei weitergehender Etablierung der NFC-Technik regelmäßig auszugehen sein dürfte.

#### ff) Ergebnis und spezifische Tatkonstellationen

Die Bewertung der Strafbarkeit wegen Computerbetrugs gem. § 263a Abs. 1 Alt. 3 StGB bei einer Zahlung mittels NFC-Verfahrens verläuft damit in vergleichbaren Bahnen wie bei der Zahlung mittels Zahlungskarte und PIN-Eingabe.

Gleiches muss für die missbräuchliche Verwendung von Smart Devices für die Zahlung gelten. Auch hierin findet sich die konkludente Erklärung, zur Zahlung berechtigt zu sein und dies nachweisen zu können. Die bei der Nutzung etwa eines Smartphone darüber hinausgehenden Sicherungsmechanismen (Passwörter, Sicherheitsmuster, Fingerabdrücke oder Ähnliches) verringern zudem tatsächlich die Missbrauchsmöglichkeiten. Für die Auslegung des Merkmals „unbefugt" sind diese dann bedeutsam, wenn sie auch Eingang in die Überprüfung der Berechtigung durch die kartenausgebende Bank gefunden haben, mithin als vertragsspezifisches Authentifizierungsmerkmal genutzt werden.[53]

Das gefundene Ergebnis ist auch auf den Fall des elektronischen Taschendiebstahls übertragbar. Als gedachter Täuschungsadressat kommt erneut allein das Kreditinstitut in Betracht. Der fiktive Erklärungsgehalt, die Zahlungskarte werde durch den Berechtigten in einer dem Geschäftsverkehr entsprechenden Weise benutzt,[54] bildet dabei ein taugliches Täuschungsäquivalent.

Im Ergebnis stellt eine unberechtigte Nutzung fremder Zahlungskarten im NFC-Verfahren nach hier vertretener Auffassung damit regelmäßig einen Computerbetrug gem. § 263a Abs. 1 Alt. 3 StGB dar.

### 2. Urkundendelikte

Durch die Nutzung einer (virtuellen) Zahlungskarte im NFC-Verfahren werden Daten sowohl auf der Karte selbst bzw. dem Smartphone als auch bei der kartenausgebenden Bank verändert. Abgesehen von Vermögensdelikten sind somit auch die technikbezogenen Urkundentatbestände des 23. Abschnitts des StGB in die Betrachtung einzubeziehen.

#### a) Fälschung beweiserheblicher Daten gem. § 269 StGB

Wird eine fremde Zahlungskarte für eine vom Berechtigten im Einzelfall nicht autorisierte Zahlung missbraucht, kann dies den Tatbestand der Fälschung beweiserheblicher Daten gem. § 269 Abs. 1 i.V.m. § 270 StGB erfüllen. Bei Verwendung der Karten werden die Daten aus dem Kartenchip bzw. die kontoidentifizierenden Daten im Smart Device ausgelesen und die Kartendaten (International Bank Account Number – IBAN, Kartenverfallsdatum und Kartenfolgenummer) sowie die Zahlungsdaten (Abbuchungsbetrag und die geografischen und zeitlichen Daten aus dem Kassensystem) zur Autorisierung an die kartenausgebende Bank über den Netzbetreiber übermittelt und gespeichert. Zudem werden Daten zu den Umständen der bisherigen Karteneinsätze seit der letzten PIN-Abfrage im Computer der Autorisierungszentrale bzw. auf dem Chip der Zahlungskarte gespeichert. Die gespeicherten Datensätze können grundsätzlich eine sog. Datenurkunde darstellen.[55] Hierfür muss allerdings ein Aussteller der Datenurkunde erkennbar sein. Für eine Strafbarkeit muss zudem bei Wahrnehmung der Daten eine unechte oder verfälschte Urkunde vorliegen, was der Fall ist, wenn der wahre Aussteller nicht mit dem erkennbaren Aussteller übereinstimmt. Die Daten über die Umstände der bisherigen Karteneinsätze sind der kartenausgebenden Bank zuzuordnen.[56] Da die Veränderung der Daten von dem Computersystem der Bank selbst vorgenommen wird, ist hierin keine unechte bzw. verfälschte Urkunde zu erblicken. Entsprechendes gilt hinsichtlich der von der Datenverarbeitungsanlage des Händlers erzeugten Zahlungsdaten, die diesen als Aussteller erkennen lassen und als echte Daten zu qualifizieren sind. Hinsichtlich der Kartendaten verneint das OLG Hamm die Erkennbarkeit eines Ausstellers,[57] weil sich aufgrund einer fehlenden PIN-Eingabe durch den Nichtberechtigten keine Identifikation eines Berechtigten als scheinbarer Aussteller erkennen lasse.[58] Allerdings muss der Datenurkunde lediglich ent-

51 Der i.S.d. Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG, ABlEU vom 23.12.2015, L 337, 35, Art. 63 Abs. 1 Buchst. b, als anonym klassifizierten Verwendung der Karte (EuGH, 11.11.2020 – C-287/19, RIW 2021, 433, BKR 2021, 234, 239; s. hierzu auch *Omlor*, RDi 2021, 48) kann somit dennoch ein Erklärungsgehalt einer berechtigten Nutzung beigemessen werden.

52 So aber *Christoph/Dorn-Haag* (Fn. 6), 697, 703.

53 S. hierzu *Hoffmann/Rastegar* (Fn. 45), 957ff.; *Jungmann* (Fn. 10), § 675j, Rn. 61; *Omlor* (Fn. 9), 183f.

54 Anders *Christoph/Dorn-Haag* (Fn. 6), 697, 702.

55 S. hierzu *Puschke*, in: Hilgendorf/Kudlich/Valerius (Hrsg.), Handbuch des Strafrechts, Bd. 5, 2019, § 42, Rn. 59f.

56 OLG Hamm (Fn. 19), 673, 675f.; *Göhler* (Fn. 3), 6, 21.

57 OLG Hamm (Fn. 19), 673, 675.

58 So auch *Eisele* (Fn. 27), § 63, Rn. 139; *Göhler* (Fn. 3), 6, 20f.

nommen werden können, wem die Daten im Rechtsverkehr zuzurechnen sind, wobei eine kontextbezogene Erkennbarkeit genügt.[59] Jedenfalls für das Kreditinstitut ist jede Transaktion durch die ausgelesenen Kartendaten dem Karteninhaber zuzuordnen, da die Zahlungskarte konto- und personengebunden ist.[60] Die verwendeten Kartendaten können somit dem Karteninhaber als Aussteller zugerechnet werden. Da jedoch nicht der Karteninhaber die Speicherung veranlasst hat, sondern der unberechtigte Kartennutzer, handelt es sich um eine unechte Datenurkunde. Zum Teil wird zwar vertreten, dass erst die Kartendaten zusammen mit den von der Datenverarbeitungsanlage des Händlers erzeugten Zahlungsdaten eine für die Datenurkundenqualität hinreichende Beweiseignung ergeben, und dieser dann als alleiniger Aussteller nach außen auftritt.[61] Überzeugender erscheint es jedoch, bereits den verwendeten Kartendaten eigenständige Urkundenqualität beizumessen. Sie geben Auskunft über die erfolgte Anweisung, die Zahlung zu autorisieren.

Da die Kartendaten beim elektronischen Taschendiebstahl ohne Kenntnis und Autorisierung des Karteninhabers gespeichert und übermittelt werden, ist auch in diesen Konstellationen die Strafbarkeit gem. §§ 269 Abs. 1, 270 StGB gegeben.

### b) Urkundenunterdrückung

Das OLG Hamm sieht in der missbräuchlichen Zahlung im NFC-Verfahren allerdings eine Urkundenunterdrückung gem. § 274 Abs. 1 Nr. 2 StGB.[62] Gleiches wird auch für den elektronischen Taschendiebstahl angenommen.[63] Bei den in Rede stehenden Daten geht es um die Umstände der bisherigen Karteneinsätze und den Verfügungsrahmen. Diese Daten sind bei der kartenausgebenden Bank bzw. auf der Zahlungskarte gespeichert. Das Beweisführungsrecht hieran steht dem berechtigten Karteninhaber und der kartenausgebenden Bank zu.[64] Durch die herbeigeführte Transaktion werden diese Daten verändert. Neben dem technisch bedingt mit Nachweisproblemen behafteten Tatbestandsvorsatz[65] muss die Datenveränderung auch mit Nachteilszufügungsabsicht bewirkt werden. D.h., dass die Tathandlung zielgerichtet oder mit dem sicheren Wissen erfolgen muss, dass hierdurch die Lage des Berechtigten verschlechtert wird.[66] Da die Erstellung des Datensatzes durch die Nutzung der Karte überhaupt erst den Beweis einer unberechtigten Nutzung ermöglicht, kann ein beabsichtigter Nachteil nur in der Vereitelung einer umfassenden nutzerfreundlichen Handhabung kontaktloser Bezahlvorgänge gesehen werden.[67] Ob ein solcher Nachteil zur Strafbegründung ausreichen kann, erscheint bereits fraglich. Hierauf wird es dem unberechtigten Kartennutzer bei der Verwendung der Karte zudem nicht ankommen. Ob sicheres Wissen[68] hinsichtlich dieses Nachteils angenommen werden kann, ist eine Frage des Einzelfalls und hängt von der Kenntnis über die Speicherungsmodalitäten ab.[69] Zudem ist bedeutsam, dass der (Daten-)Urkunde seitens des Täters eine potenzielle Beweisbedeutung zugeschrieben werden muss, die sich jederzeit realisieren kann.[70] Geht der Täter davon aus, dass der Berechtigte mangels Zurückerlangung der Zahlungskarte nicht mehr in den Genuss der kontaktlosen Zahlung ohne PIN-Eingabe gelangen wird, erstreckt sich sein Bewusstsein bei der Kartenverwendung auch nicht auf eine solche Nachteilszufügung.[71] Da die Zahlungskarte beim elektronischen Taschendiebstahl allerdings beim Berechtigten verbleibt und von diesem weiterhin genutzt werden kann, scheitert die Nachteilszufügungsabsicht hier nicht an der angenommenen Beweisbedeutung für den Berechtigten.

## 3. Datendelikte

Die Verwendung und Veränderung fremder Daten durch die unberechtigte kontaktlose Nutzung von Zahlungskarten kann zudem Straftatbestände zum Schutz der Daten selbst erfüllen.

Eine Strafbarkeit wegen Ausspähens von Daten gem. § 202a StGB durch die unberechtigte Nutzung am POS-Terminal sowie durch die Verwirklichung eines elektronischen Taschendiebstahls scheidet i.d.R. aus. Entscheidend ist, dass die von der Zahlungskarte oder dem Smart Device ausgelesenen Daten nicht durch Überwindung einer besonderen Zugangssicherung verschafft werden.[72] Dies gilt jedenfalls dann, wenn die Tathandlung nicht die Überwindung der Zugangssicherung des Smart Device umfasst.[73]

Eine Strafbarkeit gem. § 303a Abs. 1 StGB ist regelmäßig durch die Veränderung der auf der Zahlungskarte und bei der kartenausgebenden Bank gespeicherten Daten hinsichtlich des Verfügungsrahmens und zu den Umständen der bisherigen Karteneinsätze

59 *Puschke* (Fn. 55), § 42, Rn. 60.
60 *Christoph/Dorn-Haag* (Fn. 37), 676, 677; i. E. ebenso *Ceffinato* (Fn. 27), 311, 314.
61 *Heghmanns* (Fn. 27), 494, 496f.
62 OLG Hamm (Fn. 19), 673, 675.
63 *Christoph/Dorn-Haag* (Fn. 6), 697, 699.
64 OLG Hamm (Fn. 19), 673, 676; *Göhler* (Fn. 3), 6, 21.
65 S. etwa *Kudlich*, JA 2020, 710, 712; *Göhler* (Fn. 3), 6, 18; *Erb*, in: Erb/Schäfer (Hrsg.), Münchener Kommentar zum StGB, 4. Aufl. 2022, § 274, Rn. 16.
66 *Puschke* (Fn. 55), § 42, Rn. 122.
67 *Heghmanns* (Fn. 27), 494, 497.
68 S. zu Einschränkungen der Anforderungen an die Absicht *Heine/Schuster*, in: Schönke/Schröder, StGB, 30. Aufl. 2019, § 274, Rn. 18.
69 S. zu diesbezüglichen Besonderheiten bei dem der Entscheidung des OLG Hamm zugrunde gelegten Sachverhalt OLG Hamm (Fn. 19), 673, 676.
70 BGH, 25.11.2009 – 2 StR 430/09, NStZ 2010, 332.
71 *Heghmanns* (Fn. 27), 494, 497. Dies ändert freilich nichts an einer Unterdrückung der Datenurkunde bereits durch Entziehung, Unterschlagung oder spätere Vernichtung.
72 Vgl. OLG Hamm (Fn. 19), 673, 675; *Graf*, in: Erb/Schäfer (Hrsg.), Münchener Kommentar zum StGB, 4. Aufl. 2021, § 202a, Rn. 29.
73 *Graf* (Fn. 72), § 202a, Rn. 29.

seit der letzten PIN-Abfrage gegeben.[74] Diese stehen dem Karteninhaber bzw. der kartenausgebenden Bank zu, weshalb eine Veränderung durch den nicht berechtigten Kartennutzer rechtswidrig erfolgt.[75] Allerdings tritt diese Strafbarkeit hinter § 274 Abs. 1 Nr. 2 StGB zurück, sofern dieser als verwirklicht angesehen wird.[76]

### 4. Nebenstrafrecht

Strafrechtlicher Datenschutz spielt darüber hinaus im Nebenstrafrecht eine Rolle. So stellt § 42 Abs. 2 Nr. 1 BDSG unter Strafe, wenn personenbezogene Daten, die nicht allgemein zugänglich sind, unberechtigt verarbeitet werden und dabei mit Bereicherungsabsicht gehandelt wird. Werden durch Zahlungskarten gestützte Zahlungen in Auftrag gegeben, werden die (virtuellen) Kartendaten im NFC-Verfahren vom Kartenlesegerät vollautomatisiert ausgelesen, sodass gem. § 1 Abs. 1 S. 2 BDSG ein tauglicher Datenverarbeitungsprozess an nicht allgemein zugänglichen Daten[77] vorliegt. Die Daten lassen dabei Rückschlüsse auf die natürliche Person des Karteninhabers zu, stellen also personenbezogene Daten i. S. d. Art. 4 Nr. 1 DSGVO[78] dar.[79] Insofern fällt eine unberechtigte NFC-Zahlung grundsätzlich in den Anwendungsbereich von § 42 Abs. 2 Nr. 1 BDSG.

Im Falle des elektronischen Taschendiebstahls ist daher von einer unmittelbaren Verwirklichung des § 42 Abs. 2 Nr. 1 BDSG auszugehen.[80] Für die unberechtigte Nutzung einer Zahlungskarte oder eines Smart Device am POS-Terminal wird die Datenverarbeitung vermittelt über das redliche Kassenpersonal in Gang gesetzt, weshalb es sich insoweit um einen Fall der mittelbaren Täterschaft handelt.

### 5. Mögliche Auffangtatbestände

Während eine Unterschlagung gem. § 246 StGB durch die unberechtigte Nutzung der Zahlungskarte oder des Smart Device regelmäßig verwirklicht wird, jedoch aufgrund der von der h. M. angenommenen Reichweite der formellen Subsidiarität des Tatbestands[81] zurücktritt, scheidet eine Strafbarkeit wegen Erschleichung einer Leistung gem. § 265a Abs. 1 StGB aus. Das Kartenlesegerät vermittelt allein das Recht und nicht die Waren selbst, für die das Entgelt entrichtet werden soll.[82]

## Fazit

Die missbräuchliche Nutzung von Zahlungskarten mit NFC-Funktion sowie entsprechender mobiler Endgeräte ist strafbar. Dies gilt sowohl für den Fall einer aktiven Zahlung als auch für den Fall des elektronischen Taschendiebstahls. Entgegen einer weit verbreiteten Auffassung lässt sich dieses Verhalten nicht nur als Urkunden- oder Datendelikt erfassen. Vielmehr ist in den klassischen Missbrauchsfällen auch das Vermögensstrafrecht in Form des § 263a Abs. 1 Alt. 3 StGB einschlägig. Das Strafrecht vermag in diesen Fällen daher auch das vermögensschädigende Unrecht bei der Verwendung neuer Technologien hinreichend abzubilden. Als strafrechtliches Bindeglied zwischen Daten- und Vermögensschutz ist zudem § 42 Abs. 2 Nr. 1 BDSG beachtlich.

### ZUSAMMENFASSUNG

1. § 263a Abs. 1 Alt. 3 StGB bietet auch bei Rückgriff auf die betrugsspezifische Auslegung des Merkmals „unbefugt" ausreichend Spielraum, um missbräuchliche NFC-Zahlungen zu erfassen.
2. Daneben werden regelmäßig Urkunden- und Datendelikte verwirklicht.
3. Strafrechtlicher Vermögens- und Datenschutz werden durch § 42 Abs. 2 Nr. 1 BDSG miteinander verknüpft.
4. Die strafrechtliche Bewertung des elektronischen Taschendiebstahls und der missbräuchlichen Nutzung von Zahlungskarten mit NFC-Funktion verläuft grundsätzlich in vergleichbaren Bahnen.

### AUTOREN

***Prof. Dr. Jens Puschke**, LL.M. (King's College), ist seit 2016 Inhaber einer Professur für Strafrecht, Strafprozessrecht, Kriminologie und Medizinstrafrecht an der Philipps-Universität Marburg.*

***Dipl.-Jur. Janick Haas** ist Wissenschaftlicher Mitarbeiter am Lehrstuhl von Prof. Dr. Jens Puschke. Er forscht im Rahmen seines Dissertationsprojekts zur Strafbarkeit des Betreibens von illegalen Handelsplattformen im Internet.*

74 OLG Hamm (Fn. 19), 673, 676; krit. zur Schädigung durch die Datenveränderung *Heghmanns* (Fn. 27), 494, 498.
75 *Göhler* (Fn. 3), 6, 22.
76 OLG Hamm (Fn. 19), 673, 676; s. grundsätzlich auch *Puschke* (Fn. 55), § 42, Rn. 141.
77 *Christoph/Dorn-Haag* (Fn. 6), 697, 700; grundsätzlich *Brodowski/Nowak*, in: Wolff/Brink (Hrsg.), BeckOK Datenschutzrecht, Stand: 1.11.2021, § 42 BDSG, Rn. 27.
78 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABlEU vom 4.5.2016, L 119, 1.
79 *Brodowski/Nowak* (Fn. 77), § 42 BDSG, Rn. 22.
80 *Christoph/Dorn-Haag* (Fn. 6), 697, 700.
81 S. nur BGH, 6.2.2002 – 1 StR 513/01, NJW 2002, 2188 ff.; *Otto*, NStZ 2003, 87 f.
82 Ebenso *Heghmanns* (Fn. 27), 494, 498.