Julius-Maximilians-
UNIVERSITÄT
WÜRZBURG

famos

Der Fall des Monats
im Strafrecht
Online-Zeitschrift

Herausgeber: Prof. Dr. Tobias Reinbacher, Professur für Strafrecht und Strafprozessrecht, Julius-Maximilians-Universität Würzburg
Redaktion: Prof. Dr. Tobias Reinbacher und die Mitarbeiterinnen und Mitarbeiter der Professur
www.fall-des-monats.de

06
2020

Juni 2020

NFC-Fall

Täuschungsäquivalenz / Unbefugt / (Quasi) Sachgedankliches Mitbewusstsein

§§ 263 Abs. 1, 263a Abs. 1 Var. 3, 269 Abs. 1, 274 Abs. 1 Nr. 2 StGB

***famos*-Leitsätze**:

1. Bezahlt ein Nichtberechtigter mit einer Girocard ohne PIN-Eingabe, stellt dies keine konkludente Erklärung über eine berechtigte Karteninhaberschaft dar, weshalb weder ein täuschungsbedingter Irrtum noch eine unbefugte Datenverwendung vorliegt.
2. Die Überschreibung der Logdateien verwirklicht vielmehr eine Urkundenunterdrückung.

OLG Hamm, Beschluss vom 7. April 2020 – 4 RVs 12/20; veröffentlicht in BeckRS 2020, 9059.

1. Sachverhalt[1]

A gelangt in den Besitz der Girocard des B bei der C-Bank, welcher seine Geldbörse zuvor verloren hat. Diese möchte A sogleich für seinen bevorstehenden Einkauf im Supermarkt D nutzen. Im Laden angekommen tätigt A einen Einkauf in Höhe von 24,95 Euro, indem er an der Kasse die Girocard zur Bezahlung auf das Kartenlesegerät legt. Da der Einkauf einen Warenwert unter 25 Euro aufweist, ist die Eingabe einer PIN nicht erforderlich. Der technisch versierte A nutzt hierbei diese Überprüfungslücke beim Bezahlvorgang bewusst aus. Mit den Waren verlässt A das Geschäft.

Das AG verurteilt A wegen Computerbetruges gem. §§ 263a Abs. 1, 2 StGB[2]. In der Berufungsinstanz wird A vom LG stattdessen wegen Betruges gem. § 263 Abs. 1 verurteilt. A legt Revision zum OLG ein.

2. Probleme und bisheriger Meinungsstand

Technische Neuerungen, wie das kontaktlose Bezahlen ohne PIN-Eingabe, gewinnen zunehmend an Bedeutung und bereiten Schwierigkeiten bei der rechtlichen Einordnung. Bei der Verwendung einer Girocard durch einen Nichtberechtigten kommen aus strafrechtlicher Sicht eine Reihe an Normen in Betracht. Zu denken ist hier insbesondere an die §§ 263, 263a sowie an die §§ 269, 270, 274.

Eine Kartenzahlung mittels Girocard (früher: ec-Karte) erfolgt zumeist im Point of Sale-Verfahren (POS).[3] Dieses kann zum einen durch Einführen der Girocard in ein Kartenlesegerät, verbunden mit einer PIN-Eingabe, abgewickelt werden.[4] Zum anderen kann es, wie hier, mittels Near Field Communication (NFC) erfolgen, bei der ein bloßes in die Nähe Halten des in der Girocard verbauten NFC-Chips an ein Kartenlesegerät genügt. Bei beiden Verfahren werden Daten an den

---

1 Der Sachverhalt wurde verändert, um die Hauptprobleme des Falles deutlicher hervortreten zu lassen.

2 Normen ohne Gesetzesbezeichnung sind solche des StGB.

3 *Casper*, in MüKoBGB, 8. Aufl. 2020, Bd. 6, § 675f Rn. 128 f.; *Hopt*, in Baumbach/Hopt, HGB, 39. Aufl. 2020, (7) Bankgeschäfte Rn. F/2.

4 *Werner*, in Hoeren/Sieber/Holznagel, Multimedia-R-Hdb, 50. EL Oktober 2019, Teil 13.5 Rn. 2 f.

Computer des kartenausgebenden Bankinstituts übermittelt.[5] Diese auf dem Chip der Girocard gespeicherten Transaktionsdaten umfassen einerseits Logdateien (z.B. Informationen über die letzten Zahlungsvorgänge) sowie andererseits personenbezogenen Daten (z.B. die Kartennummer).[6] Nach der Datenübermittlung überprüft der Bankcomputer u.a., ob die PIN korrekt eingegeben wurde bzw. ob die Voraussetzungen für deren Verzicht vorliegen.[7] Dieser freiwillige PIN-Verzicht der kartenausgebenden Bank im NFC-Verfahren ist nur bei Zahlungen unter 50 Euro[8] möglich.[9]

Zunächst kommt i.R.d. Vermögensdelikte eine Strafbarkeit des A wegen Betruges gem. § 263 Abs. 1 zu Lasten des D bzw. der C-Bank in Betracht. Erforderlich wäre dafür eine Täuschungshandlung, durch die ein Irrtum, d.h. eine Fehlvorstellung über Tatsachen, hervorgerufen wird.[10] Fraglich erscheint bereits das Vorliegen einer Täuschungshandlung. Man könnte hier auf eine Täuschung gegenüber dem Kassenpersonal bei D und dabei darauf abstellen, dass A durch das Nutzen der Karte konkludent erklärt habe, dass er hierzu berechtigt sei.[11] Nimmt man dies an, so muss diese Erklärung zu einem Irrtum beim Kassenpersonal geführt haben. Hinsichtlich des Irrtums ist eine aktive Reflexion des Aussagegehalts der Täuschung nicht erforderlich. Es reicht ein **sachgedankliches Mitbewusstsein**, sprich ein ständiges Begleitwissen. Insbesondere bei konkludenten Täuschungen sieht der Adressat das Vorliegen bestimmter Umstände als selbstverständlich gegeben an.[12] Aus der zwischen C und D bestehenden Zahlungsgarantie könnte sich ergeben, dass es mangels eines Zahlungsrisikos für D keine Rolle spiele, ob A zur Zahlung mit der Girocard berechtigt war.[13] Es könnte genügen, dass D die wahre Sachlage unbekannt sei.[14] Ein sachgedankliches Mitbewusstsein wäre hiernach abzulehnen. Allerdings kann die Zahlungsgarantie im Ausnahmefall, z.B. unter dem Gesichtspunkt des Rechtsmissbrauchs bei kollusivem Zusammenwirken, entfallen.[15] Hieraus könnte zu folgern sein, dass sich D Gedanken über die Berechtigung des Kartenbesitzers mache.[16] Ein sachgedankliches Mitbewusstsein würde vorliegen.

Darüber hinaus kommt ein Computerbetrug gem. § 263a Abs. 1 Var. 3 zu Lasten der C bzw. des B in Betracht.[17] Da nach der h.M. Daten einer Originalkarte nie unrichtig sein können, scheidet Var. 2 aus.[18] Die Eingabe der Kartendaten in das Lesegerät stellt eine Datenverwendung dar.[19] Fraglich ist, ob diese auch unbefugt erfolgt. Dieses Tatbestandsmerkmal ist umstritten,[20] wobei die h.L. und

---

5 *Haertlein*, in MüKoHGB, 4. Aufl. 2019, Bd. 6, E. Bankkartenverfahren Rn. 238; *Koch*, in Schimansky/Bunte/Lwowski, BankR-Hdb, 5. Aufl. 2017, § 68 Rn. 3 f.

6 ULD SH, LT-Drs. SH 18/555, S. 78.

7 *Zahrte*, in Bunte/Zahrte, AGB-Banken, AGB-Sparkassen, Sonderbedingungen, 5. Aufl. 2019, 4. Teil II. Bedingungen für die Sparkassen-Card (Debitkarte) Rn. 28, 33b f.

8 Die Deutsche Kreditwirtschaft gab in ihrer Pressemitteilung vom 15.04.2020 bekannt, dass die Wertgrenze für einen PIN-Verzicht nun von 25 auf 50 Euro gestiegen ist.

9 *Zahrte*, in Bunte/Zahrte, AGB-Banken (Fn. 7), 4. Teil II. Bedingungen für die Sparkassen-Card (Debitkarte) Rn. 9a, 22, 33b f.

10 *Hefendehl*, in MüKoStGB, 3. Aufl. 2019, Bd. 5, § 263 Rn. 249.

11 *Kindhäuser*, in NK, StGB, 5. Aufl. 2017, § 263 Rn. 135; *Perron*, in Schönke/Schröder, StGB, 30. Aufl. 2019, § 32 Rn. 14 ff.

12 *Hefendehl*, in MüKoStGB (Fn. 10), § 263 Rn. 252.

13 Vgl. *Lenk,* JuS 2020, 407, 410.

14 Vgl. *Kindhäuser*, in NK (Fn. 11), § 263 Rn. 188.

15 *Sprau*, in Palandt, 79. Aufl. 2020, § 675f Rn. 60, 57.

16 Vgl. *Kindhäuser*, in NK (Fn. 11), § 263 Rn. 188.

17 *Fischer*, StGB, 67. Aufl. 2020, § 263a Rn. 22.

18 *Heger*, in Lackner/Kühl, StGB, 29. Aufl. 2018, § 263 Rn. 10; *Rossa*, CR 1997, 219, 222.

19 *Mühlbauer*, in MüKoStGB (Fn. 10), § 263a Rn. 75; *Rossa*, CR 1997, 219, 221 f.

20 Vgl. dazu ausführlich *Tacke/Wolf*, famos 08/2015, S. 1 ff.

die st.Rspr. einer betrugsspezifischen Auslegung folgen.[21] Danach ist eine Datenverwendung unbefugt, wenn diese gegenüber einer natürlichen Person eine Täuschungshandlung darstellen würde.[22] Allerdings ist innerhalb dieser Ansicht umstritten, ob die fiktive natürliche Person denselben Prüfungsmaßstab anzulegen hat wie das Computerprogramm.[23] Nach einer Ansicht, die auf eine **Täuschungsäquivalenz** abstellt, ist derselbe Prüfungsumfang maßgeblich, welcher für den Computer entscheidend ist. Andernfalls bestehe die Gefahr einer vom Gesetzgeber nicht gewollten Strafbarkeitsausdehnung.[24] Vorliegend wäre bei der Überprüfung der Daten durch den Bankcomputer darauf abzustellen, ob ein fiktiver Schalterangestellter, der dieselben Kriterien wie der Computer prüft, getäuscht würde.[25] Mangels PIN-Eingabe wäre die Berechtigung zur Kartennutzung nicht vom Prüfungsumfang umfasst, weshalb folglich keine Täuschungshandlung vorliegen würde.

Nach einer anderen Ansicht ist auf eine **Irrtumsäquivalenz** und somit auf eine natürliche Person mit erweiterten Prüfpflichten abzustellen, da ansonsten erneut Strafbarkeitslücken eröffnet würden, welche durch § 263a geschlossen werden sollten.[26] Demzufolge würde im POS-Verfahren mit PIN-Eingabe ein fiktiver Bankangestellter durch die Vorlage von Karte und PIN über eine berechtigte Karteninhaberschaft getäuscht.[27] Im NFC-Verfahren wird zwar keine PIN eingegeben, allerdings könnte im Rahmen eines quasi sachgedanklichen Mitbewusstseins des Computers angenommen werden, dass in dem Benutzen der Karte eine konkludente Täuschung über die Berechtigung liegt.[28] Hier wäre zu überlegen, wie der freiwillige Verzicht der C auf eine PIN-Eingabe in Bezug auf das erweiterte Prüfprogramm einzuordnen ist und ob daraus ein Verzicht auf eine Identitätsprüfung herzuleiten ist.

Daneben könnten auch Urkundendelikte verwirklicht sein. Insbesondere könnte sich A wegen der Fälschung beweiserheblicher Daten gem. den §§ 269 Abs. 1, 270 strafbar gemacht haben. Um beweiserhebliche Daten handelt es sich, wenn die Daten nach ihrem Informationsgehalt Gedankenerklärungen sind, die abgesehen von ihrer visuellen Wahrnehmbarkeit sämtliche Urkundenmerkmale erfüllen.[29] Als in Betracht kommende Daten könnte man zunächst auf die personenbezogenen Transaktionsdaten (z.B. Kontonummer und Gültigkeitsdatum der Girocard) abstellen. Diese werden bei jedem Bezahlvorgang als eigenständige Gedankenerklärung in das Autorisierungssystem eingelesen. Problematisch erscheint allein, ob die **Garantiefunktion** gewahrt wird, wenn eine PIN-Eingabe ausbleibt. Kenntlich zu machen ist, wer hinter dem Datenbestand steht und auf wen dieser beweisrechtlich zurückgeführt werden kann.[30] Im vorliegenden Fall könnte dies der Karteninhaber B sein. Problematisch ist, dass bei einem Bezahlvorgang ohne PIN-Eingabe weder der berechtigte noch der unberechtigte Kartennutzer identifiziert wird. Es könnte, anders als bei einem Bezahlvorgang mit PIN-Eingabe, gerade keine vergleichbare Identifikation des Anweisenden stattfinden.[31] Ohne erkennbaren Aussteller wäre die Ga-

---

21 BGH NJW 2002, 905, 906; *Fischer* (Fn. 17), § 263a Rn. 11.

22 BGH NJW 2002, 905, 906; *Perron*, in Schönke/Schröder (Fn. 11), § 263a Rn. 9.

23 *Rengier*, Strafrecht BT I, 22. Aufl. 2020, § 14 Rn. 22.

24 BGH NJW 2002, 905, 906; *Rengier* (Fn. 23), § 14 Rn. 45.

25 BGH NJW 2002, 905, 906; *Kindhäuser*, in NK (Fn. 11), § 263a Rn. 25 f.

26 *Lenk*, JuS 2020, 407, 409; *Perron*, in Schönke/Schröder (Fn. 11), § 263a Rn. 13, 9 f.

27 *Mühlbauer*, in MüKoStGB (Fn. 10), § 263a Rn. 54 ff.

28 *Fischer* (Fn. 17), § 263a Rn. 11.

29 *Fischer* (Fn. 17), § 269 Rn. 5; *Heger*, in Lackner/Kühl (Fn. 18), § 269 Rn. 4.

30 *Heine/Schuster*, in Schönke/Schröder (Fn. 11), § 269 Rn. 11.

31 Vgl. *Koch*, in Schimansky/Bunte/Lwowski (Fn. 5), § 68 Rn. 19.

rantiefunktion nicht gewahrt. Die Transaktionsdaten wären keine Datenurkunde.

Weiterhin könnten die Logdateien, insbesondere die Angaben zum Kontostand, als beweiserhebliche Daten in Betracht kommen. Die Daten sind auf die Bank C als Ausstellerin zurückzuführen. Es wird jedoch vertreten, dass die Erklärung über den Kontostand durch den Eingriff des A keinen rechtswidrigen neuen Inhalt erhalte, da die Bezahlung und mithin die Änderung des Kontostands aufgrund der Zahlungsgarantie rechtmäßig sei.[32] Ein Verändern liege nicht vor.

Es könnte ferner ein Fall der Urkundenunterdrückung gem. § 274 Abs. 1 Nr. 2 vorliegen. In Frage kommen die Logdateien hinsichtlich der Höhe des Verfügungsrahmens sowie der Informationen über die Anzahl und Höhe der letzten Transaktionen, über die B bzw. C verfügungsbefugt ist.[33] Indem durch den Einkauf des A die Logdateien überschrieben wurden, sind diese verändert bzw. gelöscht worden, weshalb der objektive Tatbestand erfüllt ist. Fraglich ist jedoch, ob das Überschreiben der Transaktionsdaten auch vorsätzlich erfolgte. Auf die Überschreibung kommt es dem Täter nicht primär an. Vielmehr ist, abhängig vom Sachverhalt, zwischen einem billigenden Inkaufnehmen (dolus eventualis) des Täters und einem Vertrauen auf das Ausbleiben des Erfolgs (luxuria) desselben zu differenzieren. Für diese Abgrenzung ist hier u.a. auf das technische Hintergrundwissen des A abzustellen, da sich sein Vorsatz nur auf Umstände beziehen kann, von denen er Kenntnis hat.[34]

Bei § 266b Abs. 1 ist darauf einzugehen, ob dieser Tatbestand auch die Girocard umfasst und ob dieser von einem Nichtberechtigten begangen werden kann.[35]

Zudem könnte § 202a Abs. 1 einschlägig sein, sofern sich A die auf der Girocard gespeicherten Daten unter Überwindung einer Zugangssicherung verschafft hat.[36]

Hinsichtlich der Logdateien kommt schließlich eine Datenveränderung nach § 303a Abs. 1 in Betracht.

3. Kernaussagen der Entscheidung

Das OLG verurteilt A anstelle des Betruges wegen Urkundenunterdrückung nach § 274 Abs. 1 Nr. 2.

Ein Betrug nach § 263 Abs. 1 sei nicht verwirklicht. Es liege schon keine Täuschung des A vor. Jedenfalls fehle es aber an einem korrespondierenden Irrtum des Kassenpersonals des D. Aus Sicht des D gebe es keinen Anlass, sich über eine Berechtigung Gedanken zu machen und womöglich im zivilrechtlichen Sinne bösgläubig zu werden. Weiter müsse D die Berechtigung weder überprüfen noch müsse er sie sich vorgestellt haben.

Das OLG stellt bei der Prüfung des § 263a Abs. 1 auf eine Täuschungsäquivalenz i.R.d. betrugsspezifischen Auslegung ab. Dies begründet es u.a. damit, dass beim NFC-Verfahren ohne PIN-Eingabe mangels starker Authentifizierung gerade keine Identitätskontrolle stattfinde und somit auch ein fiktiver Bankangestellter nicht getäuscht würde. Die Datenverwendung sei somit nicht unbefugt, weshalb § 263a Abs. 1 ausscheide.

Eine Strafbarkeit wegen Fälschung beweiserheblicher Daten nach §§ 269 Abs. 1, 270 lehnt das OLG aus oben genannten Gründen ab. Hierbei beschränken sich die Ausführungen auf die Transaktionsdaten als Datenurkunde. Mangels PIN-Abfrage fehle es an einer Identifikation des Ausstellers der Gedankenerklärung. Allein der unmittelbare Besitz an der Girocard vermöge eine solche

---

[32] *Erb*, in MüKoStGB (Fn. 10), § 269 Rn. 37; *Heger*, in Lackner/Kühl (Fn. 18), § 269 Rn. 9.

[33] BayObLGSt 1993, 86, 89 f.; *Hecker*, in Schönke/Schröder (Fn. 11), § 303a Rn. 3; *Heger*, in Lackner/Kühl (Fn. 18), § 274 Rn. 22d, 5.

[34] Vgl. *Heine/Schuster*, in Schönke/Schröder (Fn. 11), § 274 Rn. 13.

[35] *Radtke*, in MüKoStGB (Fn. 10), § 266b Rn. 9 ff., 31 f., 4 ff.

[36] *Heger*, in Lackner/Kühl (Fn. 18), § 202a Rn. 4.

nicht zu bewirken. Im Ergebnis seien die Transaktionsdaten keine Datenurkunde.

Das OLG geht hingegen von einer Strafbarkeit des A nach § 274 Abs. 1 Nr. 2 aus. A habe durch das Benutzen der Girocard die Transaktionsdaten hinsichtlich der Logdateien, über welche er nicht verfügungsberechtigt sei, verändert. Ihm sei es gerade darauf angekommen, die Daten zu verändern, um so die Sicherheitslücken des NFC-Verfahrens aufzuzeigen. A habe über das notwendige Wissen hinsichtlich der technischen Abläufe bei einer Kartenzahlung mittels NFC verfügt und von dem Absehen einer PIN-Eingabe bei einem Einkaufswert unter 25 Euro gewusst.

Der Tatbestand des Scheck- und Kreditkartenmissbrauchs gem. § 266b Abs. 1 sei nicht verwirklicht, da A nicht der berechtigte Karteninhaber sei. Mangels Überwindung einer Zugangssicherung liege auch kein Ausspähen von Daten gem. § 202a Abs. 1 vor. Eine Datenveränderung nach § 303a sei zwar gegeben, trete aber im Wege der Spezialität hinter § 274 Abs. 1 Nr. 2 zurück.

4. Konsequenzen für Ausbildung und Praxis

Der vorliegende Fall eignet sich besonders für Klausuren, da er ein problemorientiertes Arbeiten an einer Vielzahl von Normen unter Einbeziehung eigener Argumente erfordert. Entscheidender Unterschied zu den bisherigen Girocard-Fällen ist der Wegfall einer PIN-Eingabe. Es gilt den einschlägigen Tatbestand zu bestimmen. Eine der maßgeblichen Fragen ist hierbei, ob allein das Verwenden einer Girocard eine konkludente Erklärung über eine Kartenberechtigung darstellt. Dies ist entscheidend für die Beurteilung, ob i.R.d. § 263 eine Täuschung vorliegt, welche einen Irrtum im Wege eines sachgedanklichen Mitbewusstseins nach sich ziehen könnte, und ob bei § 263a die Datenverwendung unbefugt erfolgt. Bei § 263 ist darauf zu achten, zwischen dem Vorliegen einer Täuschung und eines Irrtums zu unterscheiden. Im Hinblick auf § 263a, vor allem wenn man die unbefugte Verwendung von Daten entgegen der Ansicht des OLG bejaht, ist relevant, zu wessen Lasten der Vermögensschaden erfolgt. Hierbei sind die zivilrechtlichen Verhältnisse ausschlaggebend. Vorliegend erleidet der Händler aufgrund der Zahlungsgarantie keinen Vermögensschaden. Für die Entscheidung zwischen dem Kartenberechtigten und der Bank als Geschädigter ist auf § 675v BGB[37] sowie die Frage, ob es B möglich war, das Abhandenkommen seiner Girocard zu bemerken, abzustellen.[38] Zudem muss bei den Urkundendelikten zwischen den Logdateien, welche sich nur auf die Transaktionsvorgänge beziehen, und den personenbezogenen Transaktionsdaten unterschieden werden.

5. Kritik

Die fortwährenden technischen Neuerungen scheinen dem StGB stets einen Schritt voraus zu sein. Die damit einhergehenden Herausforderungen führen im hier besprochenen Fall dazu, dass drei Gerichte jeweils unterschiedliche Tatbestände für einschlägig halten. Diesen Herausforderungen begegnet das Urteil des OLG souverän, vermag aber in manchen Punkten nicht vollends zu überzeugen. Der Fall könnte vor allem hinsichtlich § 263a auch anders beurteilt werden. Diskussionsbedürftig ist die Frage, ob die Datenverarbeitung, abgestellt auf eine Irrtumsäquivalenz, unbefugt erfolgt. Für die Einordnung der Fälle ohne PIN-Eingabe erscheint es hilfreich, diese mit bereits bekannten Fallgruppen zu vergleichen. Man könnte diese Konstellation mit den Fällen, in denen der Täter ohne Täuschung an die PIN gelangt ist, gleichstellen.[39] Erhält der Täter die Girocard samt PIN einvernehmlich vom Berechtigten mit der Maß-

---

[37] Der Haftungsausschluss nach Abs. 4 greift nicht, da es sich hier um eine Ausnahme von der Pflicht zur starken Authentifizierung nach Art. 11 DelVO (EU) 2018/389 handelt.

[38] *Beesch*, jurisPR-BKR 11/2019 Anm. 1; *Hofmann*, in BeckOGK, BGB, Stand: 01.09.2019, § 675v Rn. 119; *Zahrte*, BKR 2019, 484, 486 ff.

[39] *Mühlbauer*, in MüKoStGB (Fn. 10), § 263a Rn. 74.

gabe, Einkäufe in einer bestimmten Höhe zu tätigen und überschreitet der Täter diese Betragsgrenze, so erfolgt die Datenverwendung nicht unbefugt.[40] Ein lediglich abredewidriges Verhalten des Täters reicht hierfür nicht aus.[41] Stattdessen kommt § 266 bzw. § 263 in Betracht.[42] Kennzeichnend für diese Fälle ist ein Vertrauensverhältnis, welches im Innenverhältnis missbraucht wird. Ein solches ist bei der vorliegenden Fallgestaltung aber gerade nicht gegeben. Anders wäre der Fall zu beurteilen, wenn man eine Parallele zu den Bankautomaten-Missbrauchs-Fällen zieht.[43] In diesen Fällen findet bzw. entwendet der Täter eine Girocard, auf der die PIN notiert ist, und benutzt diese an Geldautomaten oder Bezahlterminals. Hier erfolgt die Datenverwendung unbefugt, weshalb § 263a einschlägig ist.[44] Diese Einordnung erscheint der Problematik am ehesten gerecht zu werden. In der Rspr. wurde bislang vertreten, dass weder die Girocard noch die PIN an sich eine Legitimation geschweige denn einen Vermögenswert darstellt.[45] Dies ist jedoch darauf zurückzuführen, dass bis dahin eine Transaktion ohne starke Authentifizierung nicht möglich war. Da nun das Verwenden einer Girocard ohne die dazugehörige PIN ausreicht, um Transaktionen zu veranlassen, muss auch dies allein als konkludente Täuschungshandlung gegenüber einem fiktiven Bankangestellten genügen. Darüber hinaus erscheint es befremdlich, dass die Verwirklichung von § 263a bzw. § 274 vom freiwilligen PIN-Verzicht durch die Bank abhängt. Somit entscheidet in Fällen, in denen der Täter zusätzlich an die PIN gelangt ist, nicht er sondern die Bank welchen Tatbestand er erfüllt.

Wenngleich der Strafrahmen der §§ 263, 263a und § 274 vergleichbar ist, stellt die Verwirklichung eines Urkunden- statt eines Vermögensdelikts dennoch einen beachtlichen Unterschied dar. Insbesondere da der Täter bewusst das Vermögen eines Einzelnen schädigt, erscheint eine anschließende Verurteilung wegen einer – für den Täter nur nachrangig mitverwirklichten – Urkundenunterdrückung als Allgemeindelikt schwer nachvollziehbar. Nicht ohne Grund wäre eine Wahlfeststellung trotz vergleichbarem Strafrahmen aufgrund unterschiedlichen Unrechtsgehalts nicht möglich.[46] Dies verdeutlicht zudem, dass die strafrechtliche Würdigung ein und derselben Tathandlung nicht aufgrund eines von der Bank getätigten Verzichts anders ausfallen und ihr kein anderer Unrechtsgehalt beigemessen werden kann.

Seit Einführung des NFC-Verfahrens werden dessen Unsicherheiten in Bezug auf Datenschutz und Kontosicherheit kontrovers diskutiert.[47] Zwar erfolgt aus Sicherheitsgründen nach fünf Transaktionen oder nach Erreichen einer Gesamtsumme von 150 Euro erneut eine PIN-Abfrage.[48] Allerdings wird immerhin die Verursachung eines Vermögensschadens von bis zu 150 Euro pro Girocard ermöglicht. Vor dem Hintergrund der derzeitigen Corona-Krise mag der Ausbau kontakt- und PIN-losen Bezahlens durchaus sinnvoll sein. Ob dieses Verfahren aber mit entsprechender Wertgrenze auf Dauer nicht doch in einen eigenen Kriminalitätsbereich erwächst, bleibt abzuwarten.

(Nina Fromm/Jacqueline Sittig)

---

40 OLG Köln NStZ 1991, 586, 587; *Mühlbauer*, in MüKoStGB (Fn. 10), § 263a Rn. 58, 63, 74.

41 *Fischer*, StGB (Fn. 17), § 263a Rn. 13 f.; *Schmidt*, in BeckOK, StGB, 46. Ed., Stand: 01.05.2020, § 263a Rn. 27.

42 OLG Düsseldorf NStZ-RR 1998, 137, 137; OLG Jena BeckRS 2007, 05394; *Stam*, NZWiSt 2017, 238, 239 f.

43 *Fischer* (Fn. 17), § 263a Rn. 15, 12a; *Mühlbauer*, in MüKoStGB (Fn. 10), § 263a Rn. 75, 57.

44 *Oğlakcıoğlu*, JA 2018, 338, 339.

45 BGH NJW 1988, 979, 980; BGH NStZ-RR 2004, 333, 334 f.; *Fest*, JuS 2009, 798, 799 f.

46 Vgl. OLG Düsseldorf NJW 1974, 1833, 1834; *Norouzi*, JuS 2008, 113, 114 f.

47 Vgl. *Rammos*, ZD 2013, 599, 600 ff.; ULD SH, LT-Drs. SH 18/555, S. 78 f.

48 *Hofmann*, in BeckOGK (Fn. 38), § 675v Rn. 119 ff.