Repetitorium

Der Computerbetrug (§ 263 a StGB)

Von Assessor Dr. Erik Kraatz, Berlin*

Der sehr praxisrelevante[1] wie klausurträchtige Tatbestand des Computerbetrugs bereitet den Studenten ersichtlich viele Schwierigkeiten. Dies liegt zum einen an der Notwendigkeit technischer wie wirtschaftsrechtlicher Vorkenntnisse (so z. B. vom POS- und POZ-System), zum anderen an dem vom Gesetzgeber bewusst weit geratenen Gesetzeswortlaut, der § 263 a StGB »eine erstaunliche Karriere hin zu einer der umstrittensten Vorschriften des Strafgesetzbuchs«[2] beschert hat.

I. Allgemeine Vorbemerkungen

1. Prägt bei einer Vielzahl strafrechtlicher Normen der Streit um das jeweils geschützte Rechtsgut die gesamte Auslegung des Tatbestandes, so übernimmt diese Funktion beim Computerbetrug die historisch geprägte **Tatbestandsstruktur**: Während in den 1970er Jahren noch bezweifelt wurde, dass es sich bei der Computerkriminalität überhaupt um eine nennenswerte Deliktsgruppe handele[3], sah der Gesetzgeber in den 1980er Jahren die Eindämmung gerade der computerbedingten Wirtschaftskriminalität »zum Schutze des freiheitlichen Wirtschaftssystems und aus Gründen einer gerechten und überzeugenden Rechtsordnung« als »eine dringende rechtspolitische Aufgabe von hohem Rang«[4] an. Diese echte Gesetzeslücke[5] wurde durch die Schaffung eines Sondertatbestandes geschlossen, der nach dem ursprünglichen Gesetzesentwurf – der nur die heutigen Tatvarianten 1 und 2 sowie die »Einwirkung auf den Ablauf« als Variante 4 enthielt – eng am Wortlaut des § 263 StGB angelegt werden sollte[6]. Wegen Zweifeln, ob die »Verwendung unrichtiger Daten« auch den missbräuchlichen Gebrauch eines Geldautomaten erfasst[7], schuf der Rechtsausschuss in Anlehnung an einen parallelen österreichischen Gesetzesentwurf die Handlungsvariante der »unbefugten Verwendung von Daten«[8] und führte so mit dem Merkmal »unbefugt« bewusst ein »dem Betrug wesensfremdes Moment«[9] ein, das zumindest für die dritte und vierte Tathandlungsvariante die ursprünglich gewollte Parallelität zum Betrug wieder in Frage stellte[10]. Der bedenklich weite Gesetzeswortlaut erfasst nämlich auch Fälle, in denen der Täter mit List oder mittels eines bloßen Vertrauensbruchs den Computer nutzt – Fälle, die parallel mangels Täuschung nicht unter den Betrugstatbestand fallen würden.

Nach dem Willen des Gesetzgebers hat sich »aufgrund der parallelen Ausgestaltung zu § 263 StGB die Auslegung des § 263 a StGB zu dessen Eingrenzung an der Auslegung des § 263 StGB zu orientieren«[11] und der Rechtsanwender sich somit zu fragen, ob hypothetisch ein Betrug vorliegen würde, wenn es sich beim Computer um einen Menschen handeln würde[12]: Dem Täuschungselement des Betruges entsprächen die vier Handlungsmodalitäten[13], an die Stelle des Irrtums und der hierdurch bedingten Vermögensverfügung trete das durch das Verhalten des Täters »beeinflusste Ergebnis eines Datenverarbeitungsvorgangs«[14]. Dieser **betrugsäquivalenten Auslegung** des Computer*betrugs*[15] ist die Rechtsprechung[16] sowie die überwiegende Ansicht im Schrifttum[17] gefolgt und überträgt so auf das Verhältnis zwischen Computerbetrug und Betrug den für das Verhältnis der Computerstrafrechtsnorm § 269 StGB (Fälschung beweiserheblicher Daten) zu § 267 StGB ausdrücklich gesetzlich vorgesehenen hypothetischen Vergleich (»wer zur Täuschung im Rechtsverkehr beweiserhebliche Daten so speichert oder verändert, dass bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde vorliegen würde«). Zugleich rechtfertigt diese

* Der Verfasser ist Habilitand bei Univ.-Prof. em. Dr. Klaus Geppert, Freie Universität Berlin und vertritt derzeit einen Lehrstuhl für Straf- und Strafprozessrecht an der Ruhr-Universität Bochum (Nachfolge Hörnle).

1 Nach der Polizeilichen Kriminalstatistik (PKS) von 2008 gab es 20.942 Fälle von Computerbetrugstaten mit Debitkarten mit PIN (Schadenssumme: 21,1 Mio €) und 14.422 sonstige Computerbetrugstaten (Schadenssumme: 30,2 Mio €).

2 Achenbach, Gössel-Festschrift (2002), S. 481.

3 Vgl. Lampe, GA 1975, 1 sowie zur Entwicklung und Struktur des Computerstrafrechts Hilgendorf, JuS 1996, 509.

4 BT-Drs. 10/318, S. 12.

5 Da Computer weder ein Bewusstsein noch eine Vorstellung von der Wirklichkeit entfalten können, konnten diese Fälle mangels Irrtums sowie einer irrtumsbedingten Vermögensverfügung nicht durch den Tatbestand des (einfachen) Betruges aufgefangen werden (vgl. hierzu BT-Drs. 10/318, S. 12). Menschliche Entscheidungsprozesse finden zwar bereits bei der Programmierung und dem Zugänglichmachen des Computers statt; zu diesem Zeitpunkt fehlt es aber zumeist noch an einer Täuschungshandlung des Täters (ebenso SK-StGB/Hoyer, § 263 a Rdn. 3). Die Eigentumsdelikte der §§ 242 ff. StGB können diese Lücke nur zum Teil auffangen, fehlt es doch bei Angriffsobjekten wie Buchgeldern an einer (verkörperten!) Sache (vgl. Tiedemann, WM 1983, 1326 (1328 f.) und LK/Tiedemann (11. Aufl.), § 263 a Rdn. 2; für eine Strafbarkeit nach § 242 StGB plädiert dagegen Haft, NStZ 1987, 6 (8)) und für den Diebstahl zudem an einer Wegnahme. Auch die Untreue bietet Schutz nur vor Manipulationen betriebsangehöriger Täter mit einer Vermögensbetreuungspflicht als selbstständiger Hauptleistungspflicht (vgl. nur Fischer (56. Aufl. 2009), § 266 Rdn. 28 m. w. N.).

6 Ein Bedürfnis dafür, darüber hinaus alle möglichen vermögensschädigenden Manipulationen beim Einsatz einer Datenverarbeitungsanlage mit Strafe zu bedrohen, wurde ausdrücklich als »unverhältnismäßig weit« abgelehnt, vgl. BT-Drs. 10/318, S. 19.

7 BT-Drs. 10/5058, S. 30.

8 BT-Drs. 10/5058, S. 30.

9 Achenbach (o. Fn. 2), S. 481 (487).

10 Ebenso Achenbach (o. Fn. 2), S. 481 (488), der von einem »Riss« durch den Tatbestand spricht; aA LK/Tiedemann (o. Fn. 5), § 263 a Rdn. 16 und Lampe, JR 1988, 437 (438), die die erste und vierte Tathandlungsvariante als betrugsfremd einstufen.

11 BT-Drs. 10/5058, S. 30.

12 BGHSt. 38, 120 (123), OLG Köln, NStZ 1991, 586 (587), OLG Zweibrücken, StV 1993, 196 (197), Lackner, Tröndle-Festschrift (1989), S. 52, Schlüchter, NStZ 1988, 53 (59) und SK-StGB/Hoyer, § 263 a Rdn. 7.

13 Vgl. nur BT-Drs. 10/318, S. 20, Arzt/Weber/Heinrich/Hilgendorf, Strafrecht Besonderer Teil (2. Aufl. 2009), § 21 Rdn. 32, MüKo-StGB/Wohlers, § 263 a Rdn. 3, NK-StGB/Kindhäuser (2. Aufl. 2005), § 263 a Rdn. 3, Möhrenschläger, wistra 1986, 128 (132) und Meier, JuS 1992, 1017 (1018).

14 Vgl. nur BT-Drs. 10/318, S. 19, MüKo-StGB/Wohlers, § 263 a Rdn. 3, NK-StGB/Kindhäuser (o. Fn. 13), § 263 a Rdn. 3, SK-StGB/Hoyer, § 263 a Rdn. 5, Lenckner/Winkelbauer, CR 1986, 654 (658) und Zahn, Die Betrugsähnlichkeit des Computerbetrugs (§ 263 a StGB) (2000), S. 129 f.

15 Die gesetzliche Deliktsbezeichnung alleine kann freilich nicht mehr als ein Fingerzeig sein (weiter: Kindhäuser, Grünwald-Festschrift (1999), S. 285 (293)), sind doch etwa der Subventionsbetrug in § 264 StGB oder der Kapitalanlagebetrug in § 264 a StGB als Vorfeldtatbestände des Betrugs nicht betrugsäquivalent auszulegen, vgl. zu diesem Einwand Achenbach (o. Fn. 2), S. 481 (486).

16 BGHSt. 38, 120 (122) (mit Anm. Cramer, JZ 1992, 1032 und Schlüchter, JR 1993, 493 ff.), BGHSt. 47, 160 (163), BGH, NStZ 2005, 213, OLG Köln, NStZ 1991, 586 (mit Anm. Otto, JR 1992, 252 ff.), OLG Zweibrücken, StV 1993, 196, OLG Düsseldorf, NStZ-RR 1998, 137, OLG Karlsruhe, NStZ 2004, 333 (334) und LG Bonn, NJW 1999, 3726.

17 Lackner (o. Fn. 12), S. 41 (54 ff.), Lackner/Kühl (26. Aufl. 2007), § 263 a Rdn. 13, Rengier, Strafrecht Besonderer Teil I (11. Aufl. 2009), § 14 Rdn. 1, Wessels/Hillenkamp, Strafrecht Besonderer Teil 2 (32. Aufl. 2009), Rdn. 600, Sch/Schr/Cramer/Perron (27. Aufl. 2006), § 263 a Rdn. 2, SK-StGB/Hoyer, § 263 a Rdn. 5 ff., Schlüchter, NStZ 1988, 53 (59), Zielinski, NStZ 1995, 345 (347), Lenckner/Winkelbauer, CR 1986, 654 (657 f.) und Meier, JuS 1992, 1017 (1019).

Auslegung den identischen Strafrahmen von § 263 StGB und § 263 a StGB sowie die Anwendung sämtlicher betrugsspezifischer Besonderheiten der § 263 Abs. 2 bis 7 StGB (Versuchsstrafbarkeit, Regelbeispiele, besonders schwerer Fall, Strafantragserfordernis bei Bagatellschaden etc.) aufgrund der Verweisnorm des § 263 a Abs. 2 StGB auf den Computerbetrug[18].

Eine beachtliche Minderposition hält diese Betrugsäquivalenz bereits im Ansatz für einen »gesetzgeberischen Fehlgriff«[19]. Mangels Vorstellungskraft von der Wirklichkeit könne die Beeinflussung des Ergebnisses einer Datenverarbeitung weder ontologisch noch wertungsmäßig mit einem Irrtum gleichgesetzt werden[20], geschweige denn, dass der Computer selbstständig ablaufend eigene Verfügungen treffe. Er enthalte vielmehr durch die Programmierung elektronische »Sperren« für einen vom Täter begehrten Vermögenszuwachs, den dieser durch Überwindung der Sperren (vergleichbar dem Überwinden des Sicherheitszauns eines Anwesens, das der Täter »ausräumen« wolle) mittels List (z. B. durch erschlichene Passwörter) erlange. Der Computermissbrauch stelle daher eher (wie bei § 265 a StGB) einen »von außen kommenden« Zugriff auf fremdes Vermögen im Sinne eines Leistungsentziehungs- oder Fremdschädigungsdelikts dar[21], das mit Elementen der Eigentumsdelikte und der Untreue nur verbal betrugsähnlich konstruiert sei[22], wesensmäßig zum Betrug statt einer Parallelität aber im »Verhältnis alternativer Exklusivität« stehe[23].

2. Der mit dem Merkmal jeder unbefugten Verwendung von Daten (3. Handlungsvariante) und jeder unbefugten Einwirkung auf den Ablauf (4. Handlungsvariante) bedenklich weit formulierte Wortlaut hat in Rechtsprechung[24] und Schrifttum[25] gelegentlich den Vorwurf **fehlender Bestimmtheit (Art. 103 Abs. 2 GG)** hervorgerufen. Ohne Verwendung allgemeiner Begriffe wie jenem der »Unbefugtheit«, die erst einer Auslegung durch den Richter bedürfen, ist der Gesetzgeber jedoch nicht in der Lage, der »Vielgestaltigkeit des Lebens« gerecht zu werden[26]; vielmehr hat er mit der Wortlaut- wie systematischen Anknüpfung an den Betrugstatbestand selbst eine hinreichend bestimmte Auslegungslinie vorgegeben[27].

Merke: Auch vor diesem Hintergrund kann jedem Studenten daher nur dringend angeraten werden, der betrugsäquivalenten Auslegung des Computerbetrug-Tatbestandes zu folgen!

3. Geschütztes **Rechtsgut** ist wie bei § 263 StGB ausschließlich das Individualrechtsgut Vermögen[28] (aller mit dem Datenverarbeitungsergebnis in Berührung kommenden Personen). Die mit Computermanipulationen zumeist verbundene Beeinträchtigung der Sicherheit und Zuverlässigkeit des Beweisverkehrs mit Daten wird über § 269 StGB – wie beim allgemeinen Betrugstatbestand – in das Urkundenstrafrecht verwiesen, so dass das Allgemeininteresse am Funktionieren und der Sicherheit der eingesetzten Datenverarbeitungssysteme als bloßer mittelbarer Reflex mitgeschützt wird[29].

4. Der Computerbetrug ist seiner **Rechtsnatur** nach wegen des Tatbestandserfordernisses eines Vermögensschadens ein *Erfolgsdelikt* klassischer Prägung[30] sowie angesichts des betrugsparallelen Verständnisses einer selbstständig verfügenden Datenverarbeitungsanlage ein *Vermögensverschiebungsdelikt*. Hieraus ergibt sich aufbautechnisch (wie bei § 263 StGB) das ungeschriebene Tatbestandsmerkmal einer Stoffgleichheit zwischen eingetretenem Schaden und beabsichtigtem Vorteil[31].

II. Objektiver Tatbestand

1. Als Zwischenschritt verlangt § 263 a StGB bei jeder Handlungsmodalität, dass der Täter »**das Ergebnis eines Datenverarbeitungsvorgangs** […] **beeinflusst**«. Dieses Merkmal verbindet – wie Irrtum und Vermögensverfügung beim Betrug – die Tathandlung mit der Vermögensschädigung.

a) Unter dem Begriff der **Daten**, der von § 263 a StGB selbst nicht definiert wird und bei dem mangels ausdrücklichem Verweis und mangels Beschränkung auf gespeicherte Daten ein Rückgriff auf § 202 a Abs. 2 StGB nicht möglich ist, sind alle durch Zeichen oder kontinuierliche Funktionen dargestellten Informationen (Bedeutungsinhalt) zu verstehen, die für den Computer codierbar[32] oder bereits »lesbar« codiert sind (idR in der üblichen binären Form[33]), so dass dieser damit arbeiten kann. Da diese Daten den Computer nur zu einem Ergebnis beeinflussen müssen, brauchen sie selbst nicht auf einem Datenträger fixiert zu sein[34].

b) Als **Datenverarbeitungsvorgänge** sind nach dem Gesamtzusammenhang der Vorschrift »alle technischen Vorgänge anzusehen […], bei denen durch Aufnahme von Daten und ihre Verknüpfung nach Programmen Arbeitsergebnisse erzielt werden«[35]. Erforderlich ist also, dass bestimmte Eingangsdaten (Input) durch das im Computer gespeicherte Programm – ggf. ergänzt durch weitere Eingaben zur Steuerung über Peripherie-

18 Ebenso SK-StGB/Hoyer, § 263 a Rdn. 7.
19 Ranft, NJW 1994, 2574.
20 LK/Tiedemann (o. Fn. 5), § 263 a Rdn. 16.
21 LK/Tiedemann (o. Fn. 5), § 263 a Rdn. 16, Mitsch, JZ 1994, 877 (883 f.), MüKo-StGB/Wohlers, § 263 a Rdn. 4 und Ranft, NJW 1994, 2574.
22 Vgl. Sieber, Informationstechnologie und Strafrechtsreform (1985), S. 40: »Computeruntreue«.
23 Ranft, NJW 1994, 2574.
24 LG Köln, NJW 1987, 667 (669) bezüglich der 3. Handlungsvariante.
25 Bezüglich der 3. Handlungsvariante: Ranft, wistra 1987, 79 (83 f.), Achenbach (o. Fn. 2), S. 481 (491 f.), Mitsch, JR 1995, 432, Kleb-Braun, JA 1986, 249 (259) und Thaeter, JA 1988, 547 (551); bezüglich der 4. Handlungsvariante zweifelnd auch Sch/Schr/Cramer/Perron (o. Fn. 17), § 263 a Rdn. 16 (»bedenklich weit und unbestimmt«) und NK-StGB/Kindhäuser (o. Fn. 13), § 263 a Rdn. 28.
26 BGHSt. 38, 120 (121) bezogen auf § 263 a StGB. Schmidhäuser, Martens-Gedächtnisschrift (1987), S. 231 ff. bezeichnet eine vollständige strafrechtliche Bestimmtheit [nur Legaldefinitionen!] folgerichtig als »eine rechtsstaatliche Utopie«.
27 Ebenso BGHSt. 38, 120 (122), Cramer, JZ 1992, 1032, LK/Tiedemann (o. Fn. 5), § 263 a Rdn. 4 sowie Berghaus, JuS 1990, 981 (982); aA Ranft, NJW 1994, 2574 (2575) und Achenbach (o. Fn. 2), S. 481 (491 f.), da innerhalb der betrugsäquivalenten Auslegung einzelne Fallgruppen streitig seien. Jedenfalls heutzutage kann aber von einer langjährigen einschlägigen Rechtssprechungslinie gesprochen werden, die nach BVerfGE 28, 175 (183 ff.), BVerfGE 37, 201 (208) und BVerfGE 86, 288 (311) für eine verfassungsmäßige Bestimmtheit genügt.
28 Ebenso BGHSt. 40, 331 (334 f.), Arzt/Weber/Heinrich/Hilgendorf (o. Fn. 13), § 21 Rdn. 31, Rengier (o. Fn. 17), § 14 Rdn. 1, LK/Tiedemann (o. Fn. 5), § 263 a Rdn. 13, NK-StGB/Kindhäuser (o. Fn. 13), § 263 a Rdn. 2, MüKo-StGB/Wohlers, § 263 a Rdn. 1, Fischer (o. Fn. 5), § 263 a Rdn. 2 und Ranft, NJW 1994, 2574.
29 So bereits Otto, Grundkurs Strafrecht: Die einzelnen Delikte (7. Aufl. 2005), § 52 Rdn. 30, LK/Tiedemann (o. Fn. 5), § 263 a Rdn. 13, SK-StGB/Hoyer, § 263 a Rdn. 2 und Krey/Hellmann, Strafrecht Besonderer Teil Band 2 (14. Aufl. 2005), Rdn. 512 c; aA Bandekow, Strafbarer Missbrauch des elektronischen Zahlungsverkehrs (1989), S. 300 ff.
30 Vgl. nur Arzt/Weber/Heinrich/Hilgendorf (o. Fn. 13), § 21 Rdn. 30, LK/Tiedemann (o. Fn. 5), § 263 a Rdn. 15 und MüKo-StGB/Wohlers, § 263 a Rdn. 2.
31 Ebenso LK/Tiedemann (o. Fn. 5), § 263 a Rdn. 15.
32 Ebenso Rengier (o. Fn. 17), § 14 Rdn. 3, Achenbach, **JURA** 1991, 225 (227), Möhrenschläger, wistra 1986, 128 (132) und Otto (o. Fn. 29), § 52 Rdn. 31; aA OLG Köln, NJW 1992, 125 (127), Wessels/Hillenkamp (o. Fn. 17), Rdn. 602 und SK-StGB/Hoyer, § 263 a Rdn. 11: bereits codierte Informationen.
33 Als Binärcode bezeichnet man eine Codeform, bei der Daten mit Hilfe nur zweier Zeichen codiert werden, zumeist mit »0« und »1«. So werden Texte im Computer werden zunächst mit ASCII (American Standard Code for Information Interchange: jedem Zeichen wird ein Bitmuster aus 7 Bit zugeordnet, wobei jedes Bit zwei verschiedene Werte annehmen kann) oder Unicode (internationaler Standard für die Codierung jedes Zeichens aller bekannten Schrift- und Zeichensysteme) zeichenweise als Zahlen kodiert, welche dann dualkodiert werden.
34 Ebenso LK/Tiedemann (o. Fn. 5), § 263 a Rdn. 21, MüKo-StGB/Wohlers, § 263 a Rdn. 13 sowie SK-StGB/Hoyer, § 263 a Rdn. 11.
35 BT-Drs. 10/318, S. 21; zustimmend Rengier (o. Fn. 17), § 14 Rdn. 3, LK/Tiedemann (o. Fn. 5), § 263 a Rdn. 22, SK-StGB/Hoyer, § 263 a Rdn. 9 und MüKo-StGB/Wohlers, § 263 a Rdn. 12, Lenckner/Winkelbauer, CR 1986, 654 (658) und Fischer (o. Fn. 5), § 263 a Rdn. 3.

geräte wie Tastatur oder Maus – verarbeitet und ausgegeben werden (Output)[36]. Dies begrenzt die Datenverarbeitung (nicht vom Wortlaut, wohl aber von der Tatbestandsstruktur einer selbstständigen Verfügung des »elektronisch denkenden und entscheidenden« Computers her) auf alle Fälle *elektronischer* Verarbeitung wie bei EDV-Systemen, PCs, elektronischen Wegfahrsperren sowie bei elektronischen Steuerelementen in Glücksspielautomaten[37]: und zwar jeweils unabhängig davon, ob die gleiche Aufgabe unter funktionellen Gesichtspunkten auch rein mechanisch von einem Automaten hätte erledigt werden können[38]. Nur wenn der »Entscheidungsprozess des Computers« tatsächlich rein mechanisch abläuft (wie z. B. im Fall eines Münzwechselautomaten, der nach Größe und Gewicht der eingeworfenen Münzen rein mechanisch im Innern einen Hebel umlegt, der die richtige Anzahl kleinerer Münzen auswirft), scheidet § 263 a StGB aus.

Teilweise wird im Schrifttum[39] der Begriff des Datenverarbeitungsvorgangs weiter eingegrenzt auf Fälle besonders komplexer, intellektersetzender Computerfunktionen von besonderer Wichtigkeit, die über ihre Programmdaten hinaus neue Daten aufnehmen und im Rahmen einer differenzierten Analyse Entscheidungen treffen. Hiernach würden zwar Bankomaten weiter erfasst werden, einfache Haushaltsgeräte sowie einfache elektronische Münzprüfer aus dem Anwendungsbereich des § 263 a StGB aber herausfallen. Eine generelle Abgrenzung wichtiger von unwichtigen Funktionen wird man jedoch kaum klar und mit der notwendigen Bestimmtheit treffen können, sind doch selbst Haushaltsgeräte zum Verarbeiten von Informationen in der Lage und ein Bankomat trotz der Vielzahl seiner Funktionen heutzutage noch weit von künstlicher Intelligenz entfernt[40].

c) Das **Ergebnis** eines solchen (elektronischen) Datenverarbeitungsvorgangs ist **beeinflusst**, wenn es von dem Resultat abweicht, das bei einem programmgemäßen Ablauf bzw. ohne die Tathandlung erzielt worden wäre[41]: sei es, dass das Ergebnis inhaltlich abweicht (ob die Anlage nun ordnungsgemäß bedient wurde[42] oder nicht) oder zeitlich, d. h. dass das Ergebnis zu einem Zeitpunkt eintritt, zu dem es programmgemäß noch nicht (Beschleunigung) oder bereits zuvor (Verzögerung) eingetreten wäre[43].

d) Verkörpert das beeinflusste Ergebnis des Datenverarbeitungsvorgangs beim Computerbetrug den »irrigen Denk- und Entscheidungsvorgang«[44] und somit Irrtum und irrtumsbedingte Vermögensverfügung beim Betrug und wird »*dadurch*« »das Vermögen eines anderen beschädigt«, so müssen die infolge des beeinflussten Ergebnisses vom Computer getroffenen Dispositionen sich (wie beim Betrug) **unmittelbar vermögensmindernd** auswirken, wodurch zugleich das Selbstschädigungsdelikt Computerbetrug (freiwillige Gewahrsamsaufgabe durch den Automatenaufsteller bei ordnungsgemäßer Bedienung – sog. »Lehre vom bedingten Einverständnis«[45]) vom Fremdschädigungsdelikt Diebstahl (Wegnahme) abgegrenzt wird. Für § 263 a StGB genügt es also nicht, wenn der Täter durch das beeinflusste Ergebnis lediglich die Möglichkeit zu einer weiteren deliktischen Handlung erlangt, wie z. B. die Möglichkeit der Wegnahme nach der Manipulation des elektronischen Türschlosses[46].

Merke: Für die klausurträchtigen Bankomaten ergibt sich hiernach, dass beim Abheben von Bargeld durch den Nichtberechtigten hinsichtlich des Verschaffens des vom Bankomaten ausgeworfenen Geldes stets (als lex specialis[47]) nur Computerbetrug und nicht Diebstahl bzw. Unterschlagung vorliegt[48].

2. Die Beeinflussung des Ergebnisses eines (elektronischen) Datenverarbeitungsvorgangs muss durch eine der enumerativ[49] aufgeführten und nicht (zu Lasten des Täters: Art. 103 Abs. 2 GG!) analogiefähigen vier **Tathandlungsmodalitäten** erfolgen.

a) Der Gesetzgeber hat hierbei die vierte Tathandlungsmodalität (»oder sonst durch unbefugte Einwirkung auf den Ablauf«) bewusst eingefügt, um neue Manipulationstechniken (insbesondere Hardware-Manipulationen) erfassen zu können[50]. Mit der Formulierung »oder *sonst*« im Sinne von »auf andere Weise« hat er die vierte Variante aber sogar als Grundtatbestand »mit vorangestellten Regelbeispielen«[51] ausgestaltet mit der Folge, dass sämtliche vier Manipulationsformen eine **(unbefugte) Einwirkung auf den Ablauf** eines Datenverarbeitungsvorgangs voraussetzen[52]. Dem Merkmal »unbefugt« kommt hierbei jedoch keine eigenständige, die übrigen Tatmodalitäten erweiternde Bedeutung zu, da der Gesetzgeber die ersten beiden Tatmodalitäten (»unrichtige Gestaltung des Programms« und »Verwendung unrichtiger oder unvollständiger Daten«) bereits vorwertend als Formen der unbefugten Einwirkung normiert hat (und so nicht erneut die Unbefugtheit zu prüfen ist) und die dritte Handlungsmodalität selbst über das Merkmal »unbefugt« verfügt.

Maßgeblich ist vielmehr stets, dass die Tathandlung auf den

36 Vgl. hierzu MüKo-StGB/Wohlers, § 263 a Rdn. 14 und Sch/Schr/Cramer/Perron (o. Fn. 17), § 263 a Rdn. 4.

37 Grundlegend hierzu BGHSt. 40, 331 ff.

38 MüKo-StGB/Wohlers, § 263 a Rdn. 14 und Zahn (o. Fn. 14), S. 203; aA Mitsch, JuS 1998, 307 (314).

39 So vor allem Hilgendorf, JR 1997, 347 (350), ders., JuS 1999, 542 (543 f.), Mitsch, JuS 1998, 307 (314) sowie Biletzki, NStZ 2000, 424 (425).

40 Kritisch ebenfalls MüKo-StGB/Wohlers, § 263 a Rdn. 16, LK/Tiedemann (o. Fn. 5), § 263 a Rdn. 22, Achenbach (o. Fn. 2), S. 481 (492) und Zahn (o. Fn. 14), S. 203 f.

41 Vgl. Lenckner/Winkelbauer, CR 1986, 654 (659), LK/Tiedemann (o. Fn. 5), § 263 a Rdn. 26, SK-StGB/Hoyer, § 263 a Rdn. 12, MüKo-StGB/Wohlers, § 263 a Rdn. 17, NK-StGB/Kindhäuser (o. Fn. 13), § 263 a Rdn. 32 und Sch/Schr/Cramer/Perron (o. Fn. 17), § 263 a Rdn. 18.

42 Vgl. grundlegend BGHSt. 40, 331 (334) (mit zust. Anm. Otto, JK 95, StGB § 263 a/8 [fälschlich selbst als § 263 a/44 ausgewiesen!]), und Hilgendorf, JuS 1997, 130 (131): »Programmwidrigkeit« sei kein trennscharfes Kriterium und seine Einführung würde das Kriterium »unbefugt« überflüssig werden.

43 Vgl. BT-Drs. 10/318, S. 20 und NK-StGB/Kindhäuser (o. Fn. 13), § 263 a Rdn. 32.

44 BT-Drs. 10/318, S. 19.

45 OLG Stuttgart, NJW 1982, 1659, OLG Celle, NJW 1997, 1518, OLG Düsseldorf, NJW 2000, 158 (159), Wessels/Hillenkamp (o. Fn. 17), Rdn. 108 und 674 sowie Sch/Schr/Eser (o. Fn. 17), § 242 Rdn. 36.

46 Ebenso SK-StGB/Hoyer, § 263 a Rdn. 50. Vgl. auch Vgl. auch OLG Hamm, NStZ 2006, 574 f.: Es liegt § 263 StGB und nicht § 263 a StGB vor, wenn dem Täter die Mitgliedschaft bei seiner Krankenkasse wirksam gekündigt wurde, er diese Karte aber bei seinem Arzt in den Computer einlesen und sich dann (auf Kosten der Krankenkasse) behandeln ließ, da die Vermögensverfügung erst durch die Arztbehandlung erfolgt.

47 So ausdrücklich BayObLGSt. 1986, 127 ff. und Sch/Schr/Cramer/Perron (o. Fn. 17), § 263 a Rdn. 23.

48 Ebenso BGHSt. 38, 120 (122 ff.), BayObLGSt. 1986, 127 ff., LK/Tiedemann (o. Fn. 5), § 263 a Rdn. 84, Weber, JZ 1987, 215 (216) und Sch/Schr/Cramer/Perron (o. Fn. 17), § 263 a Rdn. 23; aA AG Böblingen, CR 1989, 308 und Ranft, wistra 1987, 79 (84).

49 Aufgrund der Weite der vierten Tathandlungsmodalität als Auffangtatbestand für noch nicht bekannte Missbrauchsformen hat es bislang trotz zahlreicher neuer technischer Errungenschaften keinen strafwürdigen Computerbetrugsfall gegeben, der von § 263 a StGB nicht erfasst wird – ebenso LK/Tiedemann (o. Fn. 5), § 263 a Rdn. 25.

50 BT-Drs. 10/5058, S. 30.

51 MüKo-StGB/Wohlers, § 263 a Rdn. 56.

52 Ebenso NK-StGB/Kindhäuser (o. Fn. 13), § 263 a Rdn. 8, MüKo-StGB/Wohlers, § 263 a Rdn. 56, SK-StGB/Hoyer, § 263 a Rdn. 8, Ranft, wistra 1987, 79 (83) und Lackner/Kühl (o. Fn. 17), § 263 a Rdn. 5. Demgegenüber wird von einer beachtlichen Ansicht im Schrifttum das Wort »sonst« im Sinne von »andernfalls« verstanden und der vierten Variante entsprechend den Gesetzesmotiven die Funktion eines Auffangtatbestandes zugewiesen für all jene Fälle, die von den übrigen Alternativen nicht erfasst werden (so LK/Tiedemann (o. Fn. 5), § 263 a Rdn. 24, Achenbach, **JURA** 1991, 225 (228), ders. (o. Fn. 2), S. 481 (497), Rengier (o. Fn. 17), § 14 Rdn. 31, Lenckner/Winkelbauer, CR 1986, 654 (658), Sch/Schr/Cramer/Perron (o. Fn. 17), § 263 a Rdn. 16 und Fischer (o. Fn. 5), § 263 a Rdn. 18). Hiergegen spricht aber, dass das Wort »sonst« nach dieser Exklusivitäts-Auslegung die Bedeutung hätte, die das Wort »oder« bereits vermittelt und so gänzlich überflüssig wäre, so zutreffend SK-StGB/Hoyer, § 263 a Rdn. 8.

Ablauf des Datenverarbeitungsvorgangs einwirkt. Dies ist insbesondere für das unbefugte Abheben am Bankomaten bestritten worden, setzte der Täter durch das Einführen der Karte den Datenverarbeitungsvorgang doch erst in Gang[53]. Die Argumentation der Rechtsprechung, »Einfluss auf ein Ergebnis nimmt gerade auch derjenige, der einen Kausalverlauf unter Verwendung bestimmter Mittel in Gang setzt, die von Dritten geschaffen und bereitgestellt wurden, um ein anderes Ergebnis [...] zu erreichen«[54], zielt ersichtlich nur auf das Kriterium »Beeinflussung des Ergebnis eines Datenverarbeitungsvorgangs« ab. Es genügt aber, dass der Täter zu einem Zeitpunkt handelt, zu dem der Bankomat bereits mit dem Zentralrechner aufgrund seines Einschaltens verbunden ist[55]. Und jedenfalls bei der Eingabe der PIN läuft der konkrete, mit der Eingabe der Bankkarte in Gang gesetzte Datenverarbeitungsvorgang[56].

b) In Klausuren eine nur geringe Relevanz besitzt die allerdings sehr praxisrelevante erste Tathandlungsmodalität, die »(unbefugte) Einwirkung auf den Ablauf« »durch **unrichtige Gestaltung des Programms**« (sog. **Programmmanipulation**), in der »die Wiege der Computerkriminalität«[57] liegt und die daher vom Gesetzgeber bewusst wegen ihrer besonderen Gefährlichkeit (Dauer- und Wiederholungswirkung der Programmmanipulation) an den Anfang gestellt wurde[58]. Unter einem Programm ist hierbei die in Form von Daten fixierte Arbeitsanweisung an einen Computer zu verstehen, wie die einzelnen Schritte der Datenverarbeitung ablaufen sollen[59]. Zur »Gestaltung« des Programms gehört zugunsten eines umfassenden Schutzes neben der von vornherein unrichtigen Konzipierung eines Programms deren Um*gestaltung* in Form von Verändern interner Programmverzweigungen, Subroutinen oder Einsprungpunkte (sog. systemkonforme Manipulation) oder durch Löschen, Hinzufügen oder Überlagern ganzer Arbeitsschritte des Programms (sog. systemkonträre Manipulation)[60]. Bislang noch immer heftig umstritten ist, wann eine Programmgestaltung in diesem Sinne »unrichtig« ist. Hierzu der

1. Fall: Auf Bitten des alleinigen Inhabers A einer Privatbank verändert der Chefprogrammierer P das Buchhaltungsprogramm der Bank derart, dass die Zinsbeträge zwar genau auf einen Zehntel-Cent berechnet werden, dann aber stets entgegen den Zinsberechnungs-Richtlinien, die auch Gegenstand der Darlehensverträge mit den Kunden waren, auf ganze Cent-Beträge abgerundet werden. Die berechneten Zehntel-Cent-Beträge werden auf das Privatkonto des A überwiesen. So erzielt dieser einen jährlichen Gewinn von 500.000 €. Für seine guten Dienste erhält P eine Gehaltserhöhung. Strafbarkeit von A und P[61]?

Abwandlung: P bekommt nach den ersten Schädigungen der Kunden ein schlechtes Gewissen und nimmt die Abrundungsroutine entgegen dem Willen des A aus dem Programm wieder heraus. Strafbarkeit des P wegen des Löschens?

(1) Nach dem Willen des Gesetzgebers[62], dem ein Teil des Schrifttums[63] gefolgt ist, sei eine Programmgestaltung unrichtig, wenn sie »dem Willen des [über die Datenverarbeitungsanlage] Verfügungsberechtigten« (sprich: dem Willen des Systembetreibers) nicht entspreche (sog. **subjektive Theorie**). Denn eine vom Willen des Betreibers unabhängige objektive »Richtigkeit« des Programms existiere nicht, lege doch erst der Systembetreiber die Zielvorgaben frei fest, suche unter der vorhandenen Standardsoftware die für ihn passende aus und passe diese selbst oder mittelbar durch Programmierer seinen individuellen Bedürfnissen an[64].

Die Folge dieser Ansicht wäre, dass sich weder der Programmierer P noch der Bankinhaber A eines Computerbetrugs strafbar gemacht hätten, obwohl durch ihr Verhalten die Bankkunden computerbedingt in ihrem Vermögen beschädigt wurden. § 263 a StGB dient jedoch nicht nur dem Vermögensschutz desjenigen, der über das Programm verfügungsberechtigt ist, sondern er soll grundsätzlich vermögensschädigende Missbräuche der Datenverarbeitungsanlagen verhindern[65]. In der Abwandlung hätte sich P dagegen nach der subjektiven Ansicht nach § 263 a Abs. 1 Var. 1 StGB strafbar gemacht, obwohl er hier dem Vermögen der Kunden gerade dient. Die Ungereimtheiten sind offensichtlich. Zudem führt diese subjektive Ansicht zu Beweisschwierigkeiten, kann der Wille des Betreibers doch regelmäßig nur dann mit hinreichender Sicherheit ermittelt werden, wenn dieser einen konkreten Auftrag zur Herstellung eines Programms mit ganz bestimmten Funktionen erteilt[66].

(2) Kriminalpolitisch sowie teleologisch ist daher mit der überwiegenden Ansicht im Schrifttum[67] einem rein **objektiven Verständnis** zu folgen, wonach ein Programm unrichtig ist, wenn es nicht in der Lage ist, ein dem Zweck der jeweiligen Datenverarbeitung, d. h. der Beziehung zwischen den Beteiligten und der materiellen Rechtslage objektiv entsprechendes Ergebnis zu liefern. Maßgeblich sind hierbei im Sinne einer Normativierung des Richtigkeitsbegriffs[68] – wie jener der Täuschung beim Betrug[69] – zumeist die gesetzlichen Voraussetzungen der Vermögensverschiebung zwischen den Beteiligten.

Im *1. Fall* ist das Programm daher »unrichtig«, weil es objektiv der Zivilrechtslage (Vertrag zwischen Bank und Bankkunden über die Zinsberechnung) widerspricht, so dass P sich nach § 263 a Abs. 1 Var. 1 StGB strafbar gemacht hat und A nach §§ 263 a Abs. 1 Var. 1, 26 StGB.

In der *Abwandlung* bleibt P selbstverständlich straflos.

Merke: Systematisch führt diese Ansicht dazu, dass die Programmmanipulation (§ 263 a Abs. 1 Var. 1 StGB) nur einen Spezialfall der Verwendung unrichtiger Daten (§ 263 a Abs. 1 Var. 2 StGB) darstellt, der wegen seiner besonderen Gefährlichkeit zur Klarstellung vom Gesetzgeber nur besonders hervorgehoben wurde[70].

53 So LG Wiesbaden, NJW 1989, 2551 (2552), Ranft, wistra 1987, 79 (83 f.), Jungwirth, MDR 1987, 537 (542 f.), Kleb-Braun, JA 1986, 249 (259) und Sonnen, JA 1988, 464.

54 So grundlegend BGHSt. 38, 120 (121); ebenso Wessels/Hillenkamp (o. Fn. 17), Rdn. 602 und NK-StGB/Kindhäuser (o. Fn. 13), § 263 a Rdn. 32.

55 Kritisch hierzu Zahn (o. Fn. 14), S. 121 f., MüKo-StGB/Wohlers, § 263 a Rdn. 18 Fn. 70 und Bühler, MDR 1987, 448 (452).

56 Ebenso OLG Köln, NJW 1992, 125 (126), MüKo-StGB/Wohlers, § 263 a Rdn. 18 Rdn. 70 und Zahn (o. Fn. 14), S. 122.

57 Sieg, **JURA** 1986, 352 (354).

58 BT-Drs. 10/5058, S. 30.

59 Vgl. SK-StGB/Hoyer, § 263 a Rdn. 22, Sch/Schr/Cramer/Perron (o. Fn. 17), § 263 a Rdn. 5, NK-StGB/Kindhäuser (o. Fn. 13), § 263 a Rdn. 13, MüKo-StGB/Wohlers, § 263 a Rdn. 22 und Wessels/Hillenkamp (o. Fn. 17), Rdn. 606.

60 Ebenso LK/Tiedemann (o. Fn. 5), § 263 a Rdn. 27 f., MüKo-StGB/Wohlers, § 263 a Rdn. 23, NK-StGB/Kindhäuser (o. Fn. 13), § 263 a Rdn. 13, SK-StGB/Hoyer, § 263 a Rdn. 22 und Möhrenschläger, wistra 1986, 128 (132).

61 Der »Rundungstrick« gilt als der »Klassiker« unter den Computermanipulationen: vgl. nur Lenckner, Computerkriminalität und Vermögensdelikte (1981), S. 23, Rengier (o. Fn. 17), § 14 Rdn. 7, MüKo-StGB/Wohlers, § 263 a Rdn. 23 und Sieg, **JURA** 1986, 352 (355). Haft, NStZ 1987, 6 (7) hält diese Konstellation aus »technischen Buchhaltungsgründen« für unmöglich und daher dem »Reich der Legende« angehörend.

62 BT-Drs. 10/318, S. 20.

63 Zu den Anhängern zählen Lenckner/Winkelbauer, CR 1986, 654 (655), NK-StGB/Kindhäuser (o. Fn. 13), § 263 a Rdn. 14, Sch/Schr/Cramer/Perron (o. Fn. 17), § 263 a Rdn. 5, Möhrenschläger, wistra 1986, 128 (132) und Baumann/Bühler, JuS 1989, 49 (52).

64 Sch/Schr/Cramer/Perron (o. Fn. 17), § 263 a Rdn. 5.

65 Ebenso Otto, **JURA** 1993, 612 (613).

66 Vgl. Schlüchter, JR 1993, 493 (494) und MüKo-StGB/Wohlers, § 263 a Rdn. 22.

67 So LK/Tiedemann (o. Fn. 5), § 263 a Rdn. 31, Maurach/Schroeder/Maiwald, Strafrecht Besonderer Teil, Teilband 1 (10. Aufl. 2009), § 41 Rdn. 231, SK-StGB/Hoyer, § 263 a Rdn. 24, Haft, NStZ 1987, 6 (7), Otto, **JURA** 1993, 612 (613), Rengier (o. Fn. 17), § 14 Rdn. 7, Wessels/Hillenkamp (o. Fn. 17), Rdn. 606, Lackner (o. Fn. 12), S. 41 (55), MüKo-StGB/Wohlers, § 263 a Rdn. 22, Lackner/Kühl (o. Fn. 17), § 263 a Rdn. 7 und Fischer (o. Fn. 5), § 263 a Rdn. 6.

68 LK/Tiedemann (o. Fn. 5), § 263 a Rdn. 30.

69 Vgl. zur normativen Betrachtungsweise beim Betrug bereits OLG Celle, StV 1994,188 (189), LK/Tiedemann (o. Fn. 5), § 263 Rdn. 30, SK-StGB/Hoyer, § 263 Rdn. 42 ff. und Kutzner, JZ 2006, 712 (716).

70 Ebenso LK/Tiedemann (o. Fn. 5), § 263 a Rdn. 27, SK-StGB/Hoyer,

c) Der (ausdrücklichen wie konkludenten) Täuschung über Tatsachen beim Betrug am besten entspricht beim Computerbetrug die zweite Tathandlungsmodalität, die »**Verwendung unrichtiger oder unvollständiger Daten**« (sog. **Input- oder Eingabemanipulation**). **Unrichtig** sind Daten, wenn die in ihnen codierten (oder codierbaren) Informationen nicht der Wirklichkeit entsprechen, den von ihnen behaupteten Lebenssachverhalt also objektiv unzutreffend wiedergeben[71]. Daten, die keinen Tatsachenbezug haben (wie Werturteile oder Prognosen), sind für § 263 a Abs. 1 Var. 2 StGB daher ohne Belang[72].

Merke: Das Abheben am Bankomaten durch einen unbefugten Täter wird von § 263 a Abs. 1 Var. 2 StGB daher nicht erfasst, gibt der Täter doch die (entwendeten) richtigen Daten des Karteninhabers ein; nur bei der Verwendung einer gefälschten Karte kann die zweite Tathandlungsvariante erfüllt sein[73].

Die Daten sind – entsprechend der konkludenten Täuschung beim Betrug – **unvollständig**, wenn die in ihnen codierten Informationen den von ihnen behaupteten Lebenssachverhalt nicht (in dem für den Zweck der Datenverarbeitung maßgeblichen Umfang) hinreichend erkennbar enthalten[74], den Lebenssachverhalt also insbesondere durch Weglassen erheblicher Umstände entstellen[75]. **Verwendet** werden die Daten, wenn sie vom Täter derart in den Datenverarbeitungsprozess eingeführt werden, dass der Computer sie selbstständig verarbeiten kann (Erfordernis der Beeinflussung eines Datenverarbeitungsvorgangs!)[76]. Da der Gesetzgeber bewusst auf das Merkmal der »Eingabe« (dies war im Vorschlag der Sachverständigen-Kommission noch vorhanden) im Gesetzestext verzichtet hat[77], werden auch jene Daten verwendet, die der Computer im Rahmen der eingegebenen Daten aufgrund von deren Verarbeitung selbst erst geschaffen hat[78]. Dagegen genügt nicht das bloße Auslösen eines Datenverarbeitungsvorgangs ohne die Zuführung von Daten an den Computer, etwa durch das Eingeben von Falschgeld in einen Automaten[79]. Auch kann die bloße Verfälschung in den Computer einzugebender Belege mangels eigener Zuführung von Daten, die beim Computer in codierter Form ankommen, für eine unmittelbare Täterschaft nicht ausreichen[80]; werden die Belege aber von einem Dritten (ungeprüft oder trotz Prüfung irrtumsbedingt) in den Computer eingegeben, so bleibt eine Bestrafung nach den Grundsätzen der mittelbaren Täterschaft (§ 25 Abs. 1 Var. 2 StGB: Tatherrschaft!)[81].

Teile des Schrifttums[82] wollen demgegenüber **jede Nutzung der Daten** bei der Datenverarbeitung ausreichen lassen und verzichten auf das Erfordernis einer Eingabe durch den Täter selbst (bzw. zurechenbar über die Form der mittelbaren Täterschaft) und würden auch in der bloßen Fälschung in den Computer einzugebender Belege eine unmittelbare Täterschaft erblicken. Die Vertreter dieser Ansicht können sich zwar auf den Verzicht des Wortes »Eingabe« in den Gesetzestext zugunsten von »Verwenden« berufen; angesichts der Notwendigkeit der »Verwendung von *Daten*« zur »Beeinflussung des *Datenverarbeitungsvorgangs*« ist aber eine eigene Eingabe mit der Folge der Codierung notwendig, damit die Daten vom Computer auch verarbeitet werden können.

Noch immer dogmatisch nicht abschließend geklärt ist hierbei die Fallgruppe unrichtiger Angaben im automatisierten Mahnverfahren[83]. Hierzu unser

2. Fall: Gläubiger G trägt im Antrag auf Erlass eines Mahnbescheids gegen den Schuldner S eine Schadenssumme von 1.000 € ein, obwohl sein Schaden in Wahrheit nur 500 € betrug, wie er weiß. Auf dem Antrag stellt er zugleich den Antrag auf Erlass eines Vollstreckungsbescheids, wenn nicht innerhalb der Widerspruchsfrist Widerspruch von S eingelegt werden sollte. G ist bei der Antragstellung bekannt, dass das zuständige Amtsgericht die Mahnanträge (gemäß § 689 Abs. 1 S. 2 ZPO) rein maschinell bearbeitet. Der zuständige Computer erlässt den maschinengefertigten Mahnbescheid mit einer Schadenssumme von 1.000 €, der mit dem Gerichtssiegel versehen wird (§ 703 b Abs. 1 ZPO). Nachdem S zwei Wochen nach der Zustellung (§ 692 Nr. 3 ZPO) noch nicht Widerspruch eingelegt hat, fertigt der Computer mit gleicher Schadenssumme einen Vollstreckungsbescheid (§ 699 Abs. 1 ZPO, Vollstreckungstitel iSd § 794 Abs. 1 Nr. 4 ZPO!), mit dem G in das Vermögen des S vollstrecken könnte. Strafbarkeit des G?

(1) Im Mahnverfahren wird eine Schlüssigkeit weder bei einer menschlichen Bearbeitung durch den Rechtspfleger (§ 20 Nr. 1 RPflG) noch im maschinellen Verfahren geprüft (vgl. § 692 Abs. 1 Nr. 2 ZPO); der geltend gemachte Anspruch braucht daher nur individualisiert (und nicht mittels Beifügung von Unterlagen etc. substantiiert) angegeben werden[84], wobei der Antragsteller jedoch gemäß § 138 Abs. 1 ZPO der Wahrheitspflicht unterliegt. Hieraus folgert ein Teil des Schrifttums[85] – entsprechend einer Andeutung bereits des Gesetzgebers[86] –, dass eine der (objektiven) Wahrheit zuwider gemachte Angabe »unrichtig« sei und der Täter – wie im *2. Fall* der G – die zweite Tathandlungsvariante des Computerbetrugs erfülle. Hierfür spreche zudem, dass nur so ein umfassender Vermögensschutz der mit Datenverarbeitungsvorgängen in Kontakt kommenden Adressaten der Vielzahl täglich erlassener Mahnbescheide sichergestellt werden könne[87].

Beachte: Eine Vermögensschädigung (oder auch nur eine konkrete Gefährdung des Vermögens) des Schuldners tritt erst mit Erlass des vom Gericht auf Antrag des Gläubigers (§§ 696 Abs. 1, 699 Abs. 1 S. 1 ZPO) (!) zu erlassenden Vollstreckungsbescheids ein[88], so dass zuvor mangels

§ 263 a Rdn. 25, Wessels/Hillenkamp (o. Fn. 17), Rdn. 606 und Otto (o. Fn. 29), § 52 Rdn. 33.

71 Vgl. NK-StGB/Kindhäuser (o. Fn. 13), § 263 a Rdn. 17, LK/Tiedemann (o. Fn. 5), § 263 a Rdn. 30, SK-StGB/Hoyer, § 263 a Rdn. 26, Sch/Schr/Cramer/Perron (o. Fn. 17), § 263 a Rdn. 6, MüKo-StGB/Wohlers, § 263 a Rdn. 27, Otto, **JURA** 1993, 612 (613) und Hilgendorf, JuS 1997, 130 (131).

72 Ebenso LK/Tiedemann (o. Fn. 5), § 263 a Rdn. 33, der auch zutreffend darauf hinweist, dass ihre jeweilige Tatsachenbasis Gegenstand der codierten Information sein kann.

73 Vgl. Richter, CR 1989, 303 (306) und MüKo-StGB/Wohlers, § 263 a Rdn. 27.

74 Vgl. NK-StGB/Kindhäuser (o. Fn. 13), § 263 a Rdn. 17, SK-StGB/Hoyer, § 263 a Rdn. 26, MüKo-StGB/Wohlers, § 263 a Rdn. 26 und Sch/Schr/Cramer/Perron (o. Fn. 17), § 263 a Rdn. 6.

75 LK/Tiedemann (o. Fn. 5), § 263 a Rdn. 34.

76 Vgl. SK-StGB/Hoyer, § 263 a Rdn. 27, Sch/Schr/Cramer/Perron (o. Fn. 17), § 263 a Rdn. 6, NK-StGB/Kindhäuser (o. Fn. 13), § 263 a Rdn. 16, LK/Tiedemann (o. Fn. 5), § 263 a Rdn. 36, MüKo-StG/Wohlers, § 263 a Rdn. 29, Achenbach, JR 1994, 293 f. und Arloth, CR 1996, 359 (363).

77 Vgl. BT-Drs. 10/318, S. 20.

78 Ebenso SK-StGB/Hoyer, § 263 a Rdn. 27.

79 Letzteres wird ausschließlich über §§ 242 Abs. 1 StGB bzw. § 265 a StGB erfasst, je nach dem erlangten Vermögensvorteil (Ware im Zigarettenautomaten: § 242 StGB, Leistung des Automaten wie Fotokopieren oder Sonnenbank: § 265 a StGB).

80 NK-StGB/Kindhäuser (o. Fn. 13), § 263 a Rdn. 16 und MüKo-StGB/Wohlers, § 263 a Rdn. 29.

81 Umfassend hierzu LK/Tiedemann (o. Fn. 5), § 263 a Rdn. 36 ff. m. w. N. So liegt auch im Manipulieren von Computer-Lochkarten über angebliche Kindergeldanträge, die dann in den Zentralrechner der Bundesanstalt für Arbeit von gutgläubigen Mitarbeitern eingegeben werden und zu Überweisungen des Computers führen, ein Computerbetrug in mittelbarer Täterschaft, so der erste in Deutschland entschiedene Fall zu § 263 a StGB: ausführlich hierzu Sieber, Computerkriminalität und Strafrecht (1977), S. 47 ff. und Sieg, **JURA** 1986, 354 f.

82 So Otto (o. Fn. 29), § 52 Rdn. 35, ders., JK 99, StGB § 263 a/10, Bühler, NStZ 1991, 343 (344) und Westphal, CR 1987, 515 (520); ebenso BayObLG, NJW 1991, 439 (440).

83 Umfassend hierzu Münker, Der Computerbetrug im automatischen Mahnverfahren (2000).

84 Vgl. nur BGH, NJW 2000, 1420 ff. und BGH, NJW 2002, 520 f.

85 So LK/Tiedemann (o. Fn. 5), § 263 a Rdn. 39, NK-StGB/Kindhäuser (o. Fn. 13), § 263 a Rdn. 18, Haft, NStZ 1987, 6 (8), Otto (o. Fn. 29), § 52 Rdn. 37 sowie Münker (o. Fn. 83), S. 73 f. und 150.

86 BT-Drs. 10/318, S. 20 f.

87 LK/Tiedemann (o. Fn. 5), § 263 a Rdn. 39.

88 Wenn dieser auch nach § 696 Abs. 1 S. 2 ZPO im Antrag auf Erlass des Mahnbescheids bereits aufgenommen werden kann. Seine Wirkung ent-

unmittelbaren Ansetzens noch kein Versuch des Computerbetrugs vorläge[89]. Erst mit Erlass des Vollstreckungsbescheids aufgrund des Mahnbescheids mit deren Forderung (ebenfalls im automatisierten, maschinellen Verfahren) hätte der Täter unmittelbar angesetzt. Hätte S bereits auf den Mahnbescheid gezahlt, wäre der Streit daher nicht zu entscheiden.

(2) Hiergegen spricht aber, dass § 263 a StGB betrugsäquivalent auszulegen ist. Demzufolge erfasst § 263 a StGB tatbestandsmäßig nicht jene Fälle, die auch von § 263 StGB nicht erfasst würden, wenn statt des Computers ein Mensch handeln würde. Ein Rechtspfleger würde sich aber mangels Schlüssigkeitsprüfung gar keine Gedanken über das Bestehen des geltend gemachten Anspruchs machen und so keinem Irrtum unterliegen[90]. Durch die unrichtigen Angaben im automatisierten Mahnverfahren kann daher das Ergebnis des Datenverarbeitungsvorgangs (nochmals: entspricht Irrtum und Vermögensverfügung) nicht beeinflusst werden, so dass mit der überwiegenden Ansicht im Schrifttum[91] eine Tatbestandsmäßigkeit nach § 263 a Abs. 1 Var. 2 StGB zu verneinen ist. Im *2. Fall* bleibt G straflos[92].

d) Am klausurträchtigsten ist die dritte Tathandlungsmodalität, die »**unbefugte Verwendung von Daten**», die sich von der zweiten Tathandlungsvariante dadurch unterscheidet, dass die Daten zwar richtig sind, der Täter zu ihrer Verwendung aber keine Befugnis hat. Wann Daten »unbefugt«[93] verwendet (gleiche Auslegung wie bei der zweiten Variante[94]: Einführung in den Datenverarbeitungsvorgang) werden, ist Gegenstand eines Streits im Rahmen des § 263 a StGB, der von jedem Studenten beherrscht werden muss:

(1) Am weitesten reicht die **subjektive Ansicht** jener Stimmen im Schrifttum, die als »unbefugt« jede vertragswidrige, d. h. dem wirklichen oder mutmaßlichen Willen des Datenverarbeitungsbetreibers[95] oder »dem vertraglich vereinbarten Dürfen«[96] widersprechende Datenverarbeitung ansehen bzw. eine solche, die nicht durch Gesetz, Vertrag oder mutmaßliche Einwilligung gestattet sei[97]. Dies ergebe sich aus dem geschützten Rechtsgut des Individualvermögens, so dass der Erwartungshorizont des Rechtsgutsinhabers nicht außer Betracht bleiben könne[98]. So würde aber jede vertragswidrige Enttäuschung des Vertrauensverhältnisses zum Vertragspartner im Rahmen einer Computernutzung für eine Strafbarkeit nach § 263 a Abs. 1 Var. 3 StGB ausreichen, obwohl derartiges Verhalten niemals legitimer Gegenstand des Strafrechts sein kann[99], und so der Computer*betrug* letztlich zur Computer*untreue* verkommen[100].

(2) Nach einem restriktiven, von der Rechtsprechung[101] erdachten und von Teilen des Schrifttums[102] weiterentwickelten **computerspezifischen Ansatz** müsse sich der die Datenverwendung entgegenstehende Wille des Betreibers im Computerprogramm niedergeschlagen haben, die Befugnis zur Nutzung der Daten also vom Computer selbst (etwa durch die Anforderung und Überprüfung von Passwörtern oder PIN) im Sinne einer computerinternen Zugangssperre (»Missbrauchserkennungsmodul«[103]) überprüft werden und der Täter sich durch die Eingabe eines Zugangscodes in das Programm »einschleichen«[104]. Der Dieb einer Debit-Karte mit PIN würde diese Sperre aber im Sinne des Programms ordnungsgemäß passieren und nicht unbefugt handeln, so dass diese Ansicht gerade jene Strafbarkeitslücke wieder aufreißen würde, die der Gesetzgeber[105] mit dem nachträglichen Einfügen der dritten Tathandlungsvariante gerade schließen wollte[106]. Die computerinterne Sperre kann zudem vom Täter nur dann umgangen werden (sprich: Erlangung von Zugang ohne Eingabe des richtigen Passwortes), wenn er unrichtige Daten eingibt, so dass die dritte Tathandlungsmodalität zum Sonderfall der »Verwendung unrichtiger Daten« über die Befugnis verkommen, mit der zweiten Tatvariante verschmelzen[107] und so bedeutungslos würde.

(3) Abzustellen ist vielmehr mit der überwiegenden Ansicht[108] entsprechend der betrugsäquivalenten Tatbestandsstruktur auf ein **täuschungsäquivalentes Verhalten** des Täters, so dass solche Verwendungen von Daten »unbefugt« sind, die im Falle ihrer Vornahme gegenüber einer natürlichen Person als zumindest konkludente Täuschung[109] über die Befugnis zur Datennutzung oder als Täuschung durch Unterlassen trotz Aufklärungspflicht anzunehmen wären. Dafür muss die Feststellung der konkreten Befugnis zum Aufgabenbereich des Computers bzw. des fingierten natürlichen Menschen gehören, um hierüber »irren« zu können[110], was sich maßgeblich nach den Grundlagen des jeweiligen Geschäftstyps und der Verkehrsanschauung bestimmt[111].

faltet er aber erst nach nicht erfolgtem Widerspruch innerhalb von zwei Wochen seit der Zustellung des Mahnbescheids (§ 692 Abs. 1 Nr. 3 ZPO).

89 Ebenso LK/Tiedemann (o. Fn. 5), § 263 a Rdn. 68 und NK-StGB/Kindhäuser (o. Fn. 13), § 263 a Rdn. 18 ein.

90 Anders OLG Düsseldorf, NStZ 1991, 586 zur Vermeidung von »unvertretbaren Strafbarkeitslücken«.

91 SK-StGB/Hoyer, § 263 a Rdn. 30, Rengier (o. Fn. 17), § 14 Rdn. 9, Maurach/Schroeder/Maiwald (o. Fn. 67), § 41 Rdn. 232, Wessels/Hillenkamp (o. Fn. 17), Rdn. 606, Lenckner/Winkelbauer, CR 1986, 654 (656), MüKo-StGB/Wohlers, § 263 a Rdn. 28 und Lackner/Kühl (o. Fn. 17), § 263 a Rdn. 20.

92 Das dem Anspruch zugrunde liegende Schuldverhältnis reicht nicht, um eine Treuepflicht und damit eine Strafbarkeit nach § 266 Abs. 1 Var. 2 StGB zu begründen, vgl. dazu nur Fischer (o. Fn. 5), § 266 Rdn. 29.

93 Hierbei handelt es sich um ein Tatbestandsmerkmal und kein bloßes allgemeines Verbrechensmerkmal, da die nicht unbefugte Verwendung von Daten noch kein Unrecht verkörpert!

94 Ebenso NK-StGB/Kindhäuser (o. Fn. 13), § 263 a Rdn. 20 und MüKo-StGB/Wohlers, § 263 a Rdn. 35.

95 So BGHSt. 40, 331 (334 f.), BayObLG, NJW 1991, 439 (440) (mit abl. Anm. Schlüchter, CR 1991, 105 ff.), Otto (o. Fn. 29), § 52 Rdn. 40, Mitsch, JZ 1994, 877 (883 f.) sowie Hilgendorf, JuS 1997, 130 (132).

96 Maurach/Schroeder/Maiwald (o. Fn. 67), § 41 Rdn. 233.

97 Bühler, MDR 1991, 14 (16) und Scheffler/Dressel, NJW 2000, 2645 (als »heute herrschende Ansicht« bezeichnet).

98 BGHSt. 40, 331 (334 f.).

99 Vgl. zu letzterem BVerfGE 50, 142 (162), OLG Zweibrücken, StV 1993, 196 f. und MüKo-StGB/Wohlers, § 263 a Rdn. 44.

100 Ebenso SK-StGB/Hoyer, § 263 a Rdn. 15 und Wessels/Hillenkamp (o. Fn. 17), Rdn. 609.

101 OLG Celle, NStZ 1989, 367 (368), LG Freiburg, NJW 1990, 2635 (2636 f.) und LG Ravensburg, StV 1991, 214 (215).

102 Achenbach, JR 1994, 293 (295) und Lenckner/Winkelbauer, CR 1986, 654 (657 f.).

103 LK/Tiedemann (o. Fn. 5), § 263 a Rdn. 45 und SK-StGB/Hoyer, § 263 a Rdn. 17.

104 Weiter ist die computerspezifische Ansicht von Neumann, JuS 1990, 535 (537), ders., StV 1996, 375 und Arloth, **JURA** 1996, 357, wonach jede Veränderung des »Soll-Zustandes« des Datenverarbeitungssystems erfasst sei, »eben eine Computermanipulation«.

105 BT-Drs. 10/5058, S. 30.

106 So auch der Vorwurf von SK-StGB/Hoyer, § 263 a Rdn. 17 f., LK/Tiedemann (o. Fn. 5), § 263 a Rdn. 45, MüKo-StGB/Wohlers, § 263 a Rdn. 41, Fischer (o. Fn. 5), § 263 a Rdn. 10 a und Mühlbauer, wistra 2003, 244 (246).

107 Ebenso die Kritik von LK/Tiedemann (o. Fn. 5), § 263 a Rdn. 45, NK-StGB/Kindhäuser (o. Fn. 13), § 263 a Rdn. 24 und MüKo-StGB/Wohlers, § 263 a Rdn. 41.

108 BGHSt. 38, 120 (121 f.), BGHSt. 47, 160 (162 f.), BGHSt. 50, 174 (179 f.), BGH, NStZ 2005, 213, OLG Karlsruhe, NStZ 2004, 333 (334), LK/Tiedemann (o. Fn. 5), § 263 a Rdn. 44, Rengier (o. Fn. 17), § 14 Rdn. 14, Lackner/Kühl (o. Fn. 17), § 263 a Rdn. 13, Arzt/Weber/Heinrich/Hilgendorf (o. Fn. 13), § 21 Rdn. 37 f., Wessels/Hillenkamp (o. Fn. 17), Rdn. 609, SK-StGB/Hoyer, § 263 a Rdn. 19 f. und 33, MüKo-StGB/Wohlers, § 263 a Rdn. 44, Sch/Schr/Cramer/Perron (o. Fn. 17), § 263 a Rdn. 9 und Fischer (o. Fn. 5), § 263 a Rdn. 11.

109 NK-StGB/Kindhäuser (o. Fn. 13), § 263 a Rdn. 26 hat zwar eingewandt, eine konkludente Täuschung verlange eine »unausgesprochene Mitteilung«, der Computer könne »Unausgesprochenes« aber nicht verarbeiten. Die konkludente Täuschung beruht jedoch darauf, dass der Getäuschte aufgrund des Täterverhaltens auf einen bestimmten Erklärungswert schließt, der nicht zutrifft. Einem derart falschen Schluss kann durchaus auch ein Computer unterliegen, wie die Tatvariante der »Verwendung unvollständiger Daten« eindrucksvoll zeigt.

110 Vgl. hierzu nur SK-StGB/Hoyer, § 263 a Rdn. 20.

111 So grundlegend Lackner (o. Fn. 12), S. 41 (53) und MüKo-StGB/Wohlers, § 263 a Rdn. 44.

Von hier aus sind die einschlägigen Fallkonstellationen wie folgt zu entscheiden:

aa) »Unbefugt« ist hiernach insbesondere die praktisch häufige Nutzung einer **gefälschten**[112] **Debit-Karte** (Nachfolger der Ende 2001 ausgelaufenen ec-Karte[113]) wie einer Original-Debit-Karte mit PIN am **Geldautomaten**, wenn diese durch **verbotene Eigenmacht oder sonstwie deliktisch erlangt**[114] wurde. Der Täter verwendet mit der Einführung der Karte und der Eingabe der PIN Daten, wirkt jedenfalls mit letzterem auf den Ablauf der Datenverarbeitungsanlage ein und spiegelt diesem so – vergleichbar dem Vorzeigen von Karte und Aufschreiben der PIN gegenüber einem fiktiven Bankmitarbeiter – vor, der Karteninhaber habe ihm zur Geldabhebung eine Vollmacht erteilt[115]. Hierüber »irrt« der Computer durch ein beeinflusstes Datenverarbeitungsergebnis und »verfügt« durch die Herausgabe des abgehobenen Geldes.

Beachte: Hinsichtlich der *gefälschten Karte* kämen subjektive und computerspezifische Ansicht zum gleichen Ergebnis: Die Verwendung der Daten auf der gefälschten Karte widerspricht sowohl dem Willen der Bank wie der des Kontoinhabers und setzt computerinterne Sicherheitsabfragen außer Kraft. Bei der *deliktisch erlangten Karte* würde nur die subjektive Ansicht mit gleicher Begründung zu einer unbefugten Verwendung gelangen, während bei der computerspezifische Auslegung mit der richtigen Karte und PIN die Sicherheitsabfrage nicht umgangen, sondern erfüllt wäre[116].

bb) Gleiches gilt für die Verwendung deliktisch erlangter (z. B. mittels Phishing[117]) **Debit-Karten- oder Kreditkarteninformationen im Internet**[118], etwa zum Online-Banking oder zum Abschluss eines Online-Kaufvertrags oder der Inanspruchnahme einer Online-Dienstleistung (z. B. Betreten einer Sex-Seite), da auch hier eine erteilte Vollmacht zur Nutzung der Bank- oder Kreditkarte vorgespiegelt wird.

cc) Hat der Karteninhaber einem Dritten die **Befugnis zur Verwendung** der Karte und der PIN überlassen, so verstößt dies zwar gegen die jeweiligen Bedingungen für die ec-/Maestro-Karte der Banken[119] (mit der Folge, dass die Nutzung durch den Dritten nach der subjektiven Ansicht »unbefugt« wäre[120]), dieses Verbot dient aber ausschließlich dem Schutz des Karteninhabers selbst. Mit der Überlassung von Karte und PIN erteilt dieser eine wirksame Bank-Außenvollmacht, so dass der Dritte einen fiktiven Bankangestellten nicht über eine von seiner eigenen Person abhängende tatsächliche Wirksamkeitsvoraussetzung (Erteilung der Befugnis) täuschen würde und damit nach der täuschungsäquivalenten Auslegung nicht »unbefugt« handelt[121]. Umstritten ist einzig der Fall, dass die Befugnis im Innenverhältnis ganz oder teilweise beschränkt worden ist. Hierzu der

3. Fall (nach OLG Dresden, StV 2005, 443): Die allein erziehende F lernte eines Tages den A kennen und fasste schnell Zutrauen zu ihm. So überließ sie ihm ihre Debit-Karte nebst Geheimzahl, damit er in ihrem Namen für sie ihr Haushaltsgeld von ihrem Konto abheben konnte. Neben diesen Beträgen, die er vollständig an F weitergab, hob er einmal ohne ihr Wissen 900 € für sich ab, ohne dies an F weiterzugeben und verbrauchte es wie beabsichtigt für sich. Er wusste, dass dieses Geld für den Lebensunterhalt der F und ihrer Kinder gedacht war. Strafbarkeit des A?

Lösung: Da A bei Entgegennahme der Karte noch keine abredewidrige Abhebung vorhatte, scheidet ein *Betrug* durch die Erlangung von Karte und PIN[122] aus. Problematisch ist vielmehr, ob die Abhebung einen *Computerbetrug* darstellt: Da die Abhebung gegen den Willen des Kontoinhabers und der Bank erfolgt (nochmals: Verstoß gegen die Bedingungen für die ec-/Maestro-Karte), würde die *subjektive Ansicht* eine »unbefugte Verwendung« bejahen[123]. Die *computerspezifische* Ansicht würde mangels Überwindung der zulässig passierten internen Sperre bzw. aufgrund der ordnungsgemäßen Bedienung des Automaten einen Computerbetrug ablehnen[124]. Innerhalb der täuschungsäquivalenten Ansicht ist das Ergebnis umstritten:

(1) Teile des Schrifttums[125] bejahen eine »unbefugte Verwendung von Daten«, da der Täter keine Befugnis hinsichtlich der *konkreten* Abhebung gehabt habe (sei es wie im *3. Fall* eine gänzlich unberechtigte Abhebung, sei es die Abhebung eines höheren Betrages) und er so einen fiktiven Bankmitarbeiter über diese Befugnis zur konkreten Abhebung täuschen würde.

(2) Hiergegen spricht jedoch, dass eine Vollmacht im Außenverhältnis trotz Überschreitung des internen Dürfens wirksam bleibt, bis die Vollmacht widerrufen wird (§ 171 BGB) oder die Beschränkung auch im Außenverhältnis erklärt wird. Die generelle Überlassung von Karte und PIN bringt aber bei ihrer Vorlage gegenüber einem fiktiven Bankmitarbeiter keine Be-

112 Vgl. nur BGHSt. 38, 120 (123), LK/Tiedemann (o. Fn. 5), § 263 a Rdn. 48, SK-StGB/Hoyer, § 263 a Rdn. 36, MüKo-StGB/Wohlers, § 263 a Rdn. 45 und Fischer (o. Fn. 5), § 263 a Rdn. 12 a – jeweils m. w. N.; aA Ranft, wistra 1987, 79 (84): es handele sich um eine »unrichtige Gestaltung des Programms«.

113 Beim eurocheque-System (garantierter Scheck) wurde die Einlösung eines Schecks durch einen Garantievertrag zwischen Schecknehmer und Bank gewährleistet, der zwischen dem Schecknehmer und Scheckaussteller abgeschlossen wurde, wobei der Scheckaussteller die Bank nach § 164 Abs. 1 BGB vertrat und sich hierzu mittels ec-Karte auswies. Später wurde die ec-Karte um die Möglichkeit der Geldautomatennutzung (elektronische Debitfunktion) erweitert, international ermöglicht durch Maestro International (unter dem Logo »Maestro«), eine von Europay International und MasterCard International hierfür gegründete Gesellschaft. Das eurocheque-System wurde mangels Bedürfnis garantierter Papierschecks aufgrund der Zunahme elektronischer Zahlungsmöglichkeiten Ende 2001 eingestellt (vgl. hierzu Baier, ZRP 2001, 454), für die globale Debitleistung am Geldautomaten wurden von den Banken inzwischen eigene Karten ausgestellt, wobei die Maestro-Funktion der Abwicklung grenzüberschreitender Transaktionen dient und das nationale Electronic-Cash-Verfahren (»ec« heißt daher heute »Electronic Cash«: ebenso Husemann, NJW 2004, 104 (108)) ergänzt, vgl. Fest/Simon, JuS 2009, 798 (799). Siehe hierzu die Bankbedingungen für den ec-/Maestro-Service, auszugsweise veröffentlicht bei NK-StGB/Kindhäuser (o. Fn. 13), § 263 a Anhang.

114 Vgl. hierzu BGHSt. 47, 160 (162), BGH, NStZ 2005, 213, BGH, NStZ-RR 2004, 333 (335), BayObLGSt. 1986, 127 ff., LK/Tiedemann (o. Fn. 5), § 263 a Rdn. 49, Fischer (o. Fn. 5), § 263 a Rdn. 12 a, Wessels/Hillenkamp (o. Fn. 17), Rdn. 610, SK-StGB/Hoyer, § 263 a Rdn. 37 und MüKo-StGB/Wohlers, § 263 a Rdn. 45 – jeweils m. w. N.

115 Nicht: »er sei bevollmächtigt«, da nur über Tatsachen »getäuscht« werden kann und nicht über Rechte.

116 Ebenso LK/Tiedemann (o. Fn. 5), § 263 a Rdn. 49; für eine »unbefugte Verwendung« dennoch Achenbach (o. Fn. 2), S. 481 (494 f.) und Etter, CR 1988, 1021 (1022 f.).

117 Als »Phishing« werden jene Handlungen bezeichnet, mit Hilfe gefälschter Internet-Adressen bzw. E-Mails an Daten des Internet-Benutzers (insbesondere an dessen Passwörter) zu kommen. Der Begriff selbst ist ein englisches Kunstwort, dass sprachlich an ein »Angeln nach Passwörtern mit Ködern« angelehnt ist. Vgl. zu deren Strafbarkeit Popp, NJW 2004, 3517 (3518) und Graf, NStZ 2007, 129 (130 ff.).

118 Vgl. zu dieser Konstellation die Fallbearbeitung von Laue, JuS 2002, 359 ff.

119 Vgl. Nr. II.6.3 S. 1 der Bankbedingungen für den ec-/Maestro-Service vom 1. 7. 2002 (abgedruckt in Auszügen bei NK-StGB/Kindhäuser (o. Fn. 13), § 263 a Rdn. 65): »Der Karteninhaber hat dafür Sorge zu tragen, dass keine andere Person Kenntnis von der persönlichen Geheimzahl erhält«; ebenso Nr. 7.3 S. 1 der Bedingungen für die Deutsche Bank Card [ist eine Maestro-Karte] oder Nr. 6 S. 2 der Geschäftsbedingungen der Dresdner Bank AG für die Dresdner MaestroCard.

120 Vgl. nur Mitsch, JZ 1994, 877 (882) und NK-StGB/Kindhäuser (o. Fn. 13), § 263 a Rdn. 50.

121 Ebenso OLG Köln, NJW 1992, 125 (126) (mit abl. Anm. Otto, JK 92, StGB § 263 a/5), OLG Düsseldorf, NStZ-RR 1998, 137 (mit abl. Anm. Otto, JK 99, StGB § 263 a/9), LK/Tiedemann (o. Fn. 5), § 263 a Rdn. 50, SK-StGB/Hoyer, § 263 a Rdn. 38 und Meier, JuS 1992, 1017 (1019). Zum gleichen Ergebnis kämen die Anhänger der computerspezifischen Ansicht.

122 Vgl. zum Betrug in dieser Konstellation OLG Jena, wistra 2007, 236 (237) und Fischer (o. Fn. 5), § 263 a Rdn. 13.

123 Vgl. Hilgendorf, JuS 1997, 130 (134) und NK-StGB/Kindhäuser (o. Fn. 13), § 263 a Rdn. 50.

124 Vgl. nur Achenbach, JR 1994, 293 (295 Fn. 28).

125 So Rengier (o. Fn. 17), § 14 Rdn. 20, Arzt/Weber/Heinrich/Hilgendorf (o. Fn. 13), § 21 Rdn. 40, Lackner/Kühl (o. Fn. 17), § 263 a Rdn. 14, Eisele/Fad, **JURA** 2002, 305 (310) und Möhrenschläger, wistra 1986, 128 (133).

schränkung im Außenverhältnis zum Ausdruck, so dass jede Verwendung trotz Überschreiten der internen Beschränkung rechtlich von der Vollmacht gedeckt ist. Aufgrund bestehender Befugnis zum Abhebevorgang kann ein fiktiver Bankmitarbeiter nicht über eine nur angebliche Befugniserteilung getäuscht werden; die Verwendung von Karte und PIN ist nicht »unbefugt«[126].

Im *3. Fall* hat sich A demnach nicht nach § 263 a Abs. 1 Var. 3 StGB strafbar gemacht. Ein *Diebstahl am Geld* (§ 242 Abs. 1 StGB) scheitert an der ordnungsgemäßen Bedienung des Automaten (»Lehre vom bedingten Einverständnis« des Aufstellers am Gewahrsamswechsel) und damit mangels Wegnahme. Hinsichtlich einer *Untreue* (§ 266 Abs. 1 StGB) scheidet zwar der Missbrauchstatbestand mangels rechtsgeschäftlicher Verfügungsmacht aus, da die Möglichkeit einer Abhebung am Geldautomaten bereits bei Einrichtung des Kontos (zumindest per Allgemeinen Geschäftsbedingungen) vertraglich vereinbart wurde. Die einzelnen Buchungsvorgänge des Automaten sind nur Auslöser für die in Anerkennung der AGB getroffenen Verfügungen, so dass die einzelnen Abhebevorgänge daher keine eigenen Verfügungen im Sinne des § 266 I Var. 1 StGB sind[127]. Jedoch wird man bei einer mehrmaligen (ständigen) Abhebebefugnis über eine gewisse Dauer eine Vermögensbetreuungspflicht und damit den Treuebruchstatbestand bejahen können[128]. Hierhinter tritt die *Unterschlagung des Geldes* (§ 246 Abs. 1 StGB) im Wege der formellen Subsidiarität zurück.

dd) Von der Verwendung der Daten durch einen Dritten ist die **missbräuchliche Nutzung durch den Berechtigten** selbst zu unterscheiden:

(1) Hebt der ansonsten vermögenslose Berechtigte am Geldautomaten Geld ab, wobei er seine **Kreditlinie ausschöpft** mit dem Willen, das Geld nicht an die Bank zurückzuzahlen, würde er einen fiktiven Bankangestellten über seinen Rückzahlungswillen täuschen. Über diesen macht sich aber weder der Bankmitarbeiter noch der Computer Gedanken (genauso wenig wie über die sonstige Bonität des Kunden). Geprüft wird stets nur die Berechtigung sowie ob der Verfügungsrahmen (bestimmter Tages- und Wochenbetrag unabhängig von der Kontodeckung) bereits ausgeschöpft wurde. Das Verhalten ist (mangels Irrtums beim fiktiven Angestellten) daher nicht täuschungsäquivalent und somit nicht »unbefugt«[129].

(2) Umstritten ist demgegenüber die Konstellation, dass der Berechtigte mit dem Abheben seinen Kreditrahmen überschreitet. Hierzu der

4. Fall (nach BGHSt. 47, 160 mit Anm. Otto, JK 9/02, StGB § 263 a/13): Die A verschaffte sich einen gefälschten Personalausweis und eröffnete unter dieser falschen Identität bei der B-Bank ein Konto (ohne Kreditrahmen), wobei sie beabsichtigte, unter Verwendung der zugleich erlangten Debit-Karte das Konto zu überziehen, ohne die Salden auszugleichen. So hob sie an einem Geldautomaten der B-Bank mittels der Debit-Karte 500 € ab sowie an einem Geldautomaten der C-Bank 300 €. Strafbarkeit der A?

Lösung: Neben *§ 276 Abs. 1 Nr. 2 StGB* und *§ 263 Abs. 1 StGB* (konkrete Vermögensgefährdung mit der Kontoeröffnung durch Erlangung der Debit-Karte) kann A durch die Abhebungen an den Geldautomaten unter Überschreiten des Kreditrahmens (0 €) »unbefugt« Daten verwendet haben (*§ 263 a Abs. 1 Var. 3 StGB*): Die Anhänger der subjektiven Ansicht bejahen dies, da A gegen den Willen der Bank vertragswidrig handele[130], die Anhänger der computerspezifischen Auslegung verneinen es, da das Programm keine Sicherung gegen Kontoüberziehungen enthalte (der Computer prüfe den Kontostand nicht)[131]. Unter den Anhängern der zutreffenden täuschungsäquivalenten Auslegung herrscht Streit:

Teile des Schrifttums[132] bejahen eine Täuschungsäquivalenz mit der Begründung, ein fiktiver Schalterbeamten dürfe bei Erschöpfung des Kreditrahmens keine Auszahlungen vornehmen und müsse daher den Kontostand prüfen. Um dennoch weitere Zahlungen erreichen zu können, müsse der Kontoinhaber den Schalterbeamten daher über die notwendige Kontendeckung täuschen, so dass die Kontendeckung Geschäftsgrundlage jeder Geldabhebung (am Schalter wie am Computer) sei und hierbei stets konkludent miterklärt werde. Werde aber der fiktive Schalterbeamte konkludent getäuscht, könne für den Bankomaten nichts anderes gelten. Dass der Computer tatsächlich die Kontendeckung beim Geldabheben gar nicht (und auch der Schalterbeamte nicht) prüft, könne hieran nichts ändern, da der Schutzbereich des Betrugs wie Computerbetrugs nicht dadurch verkürzt werde, dass der Getäuschte nicht alle ihm zur Verfügung stehenden Selbstschutzmöglichkeiten wahrnehme[133].

Hierbei würde aber zur Begründung der Täuschungsqualität der Abhebung am Geldautomaten auf einen fiktiven Bankangestellten abgestellt, der die Interessen der Bank umfassend wahrzunehmen hat. Der fiktive Schalterbeamte darf jedoch nicht mehr prüfen als der Computer, würde doch sonst »aus der Parallele zum fiktiven Fall eines Betrugs eine Fiktion«[134]: Da der Geldautomat lediglich die Befugnis (PIN-Abfrage) und ein Einhalten des Verfügungsrahmens prüft (sprich: täglicher oder wöchentlicher Betrag, der nicht überschritten werden dürfe), nicht aber eine ausreichende Kontendeckung, würde auch der fiktive Schalterbeamte dies nicht prüfen, sich hierüber also gar keine Gedanken machen und hierüber auch nicht irren. Mangels Täuschungsäquivalenz ist § 263 a Abs. 1 Var. 3 StGB damit mit der Rechtsprechung[135] und Teilen der Literatur[136] abzulehnen.

Beachte: Sowohl bei der Abhebung vom Automaten der B-Bank wie der C-Bank scheidet ein Missbrauch von Scheck- und Kreditkarten (§ 266 b Abs. 1 StGB) aus, da mit dem Entfallen der ec-Scheckgarantie zum 1. 1. 2002 der Debit-Karte keine für die Tatbestandsmäßigkeit notwendige Garantiefunktion mehr zukommt[137] – der Missbrauch von »Scheckkarten« ist damit gegenstandslos geworden[138].

ee) Beliebte Missbrauchsform in der Praxis ist auch die Nut-

126 Ebenso im Ergebnis BGH, NJW 2005, 213, BGHR StGB § 263 a Anwendungsbereich 1, OLG Köln, NJW 1992, 125 (127), OLG Düsseldorf, NStZ-RR 1998, 137 (mit abl. Anm. Otto, JK 99, StGB § 263 a/9), OLG Dresden, StV 2005, 443, OLG Jena, wistra 2007, 236 f., LK/Tiedemann (o. Fn. 5), § 263 a Rdn. 50, SK-StGB/Hoyer, § 263 a Rdn. 39, MüKo-StGB/Wohlers, § 263 a Rdn. 46, Sch/Schr/Cramer/Perron (o. Fn. 17), § 263 a Rdn. 12 und Fest/Simon, JuS 2009, 798 (800).

127 Vgl. Sch/Schr/Cramer/Perron (o. Fn. 17), § 263 a Rdn. 12.

128 Noch weiter OLG Düsseldorf, NStZ-RR 1998, 137 f. und OLG Hamm, NStZ-RR 2004, 111 (112).

129 Vgl. nur Rengier (o. Fn. 17), § 14 Rdn. 22.

130 Vgl. nur Hilgendorf, JuS 1997, 130 (134 f.) und Otto (o. Fn. 29), § 52 Rdn. 44.

131 So Achenbach, JR 1994, 293 (295 Fn. 28).

132 Lackner (o. Fn. 12), S. 41 (53), Lackner/Kühl (o. Fn. 17), § 263 a Rdn. 14, LK/Tiedemann (o. Fn. 5), § 263 a Rdn. 51, Rengier (o. Fn. 17), § 14 Rdn. 23, Wessels/Hillenkamp (o. Fn. 17), Rdn. 610 a, Otto, wistra 1986, 150 (153) und Möhrenschläger, wistra 1986, 128 (133).

133 Wessels/Hillenkamp (o. Fn. 17), Rdn. 610 a.

134 Altenhain, JZ 1997, 752 (758).

135 BGHSt. 47, 160 (163 f.).

136 Arzt/Weber/Heinrich/Hilgendorf (o. Fn. 13), § 21 Rdn. 42 f., Altenhain, JZ 1997, 752 (758), SK-StGB/Hoyer, § 263 a Rdn. 35, MüKo-StGB/Wohlers, § 263 a Rdn. 39, Mühlbauer, wistra 2003, 244 (251 f.), Krey/Hellmann (o. Fn. 29), Rdn. 513 c, Sch/Schr/Cramer/Perron (o. Fn. 17), § 263 a Rdn. 11, Zielinski, CR 1992, 223 (227), Kudlich, JuS 2003, 537 (540) und Meier, JuS 1992, 1017 (1021).

137 Anders noch in dem Ende 1999 spielenden Fall des BGHSt. 47, 160 ff.: Für diese Fälle hatte der Bundesgerichtshof den § 266 b StGB auf die Fälle im Drei-Partner-System begrenzt, also auf jene Fälle der Abhebung am kreditfremden Automaten. Vor dem 1. 1. 2002 hätte sich A also nach § 266 b Abs. 1 StGB wegen der Abhebung am Automaten der C-Bank strafbar gemacht.

138 Ebenso Sch/Schr/Cramer/Perron (o. Fn. 17), § 263 a Rdn. 11 und Wessels/Hillenkamp (o. Fn. 17), Rdn. 611. § 266 b StGB ist somit auf Kreditkarten und ähnliche Karten mit Garantiefunktion beschränkt. Erledigt hat sich damit zugleich das Argument von BGHSt. 47, 160 ff., der geringere Strafrahmen des § 266 b StGB (bis zu drei Jahre Freiheitsstrafe) gegenüber § 263 a StGB (bis zu fünf Jahren Freiheitsstrafe) zeige, dass der missbräuchliche Einsatz von Bankkarten durch den Berechtigten nicht unter § 263 a StGB fallen könne.

zung der Debit-Karte im point-of-sale Verfahren (»POS« oder »electronic cash«), bei dem der Kunde im Kaufhaus mittels Debit-Karte und seiner PIN an der Kasse bezahlt. Hierzu wird die Debit-Karte in den Terminal eingeführt und der Kunde hat den Rechnungsbetrag zu bestätigen und seine PIN einzugeben. Die auf der Karte gespeicherten Daten werden zusammen mit der eingegebenen PIN und dem Rechnungsbetrag über das Computernetz zum Autorisierungscomputer der kartenausgebenden Bank übermittelt. Dieser prüft lediglich, ob die PIN stimmt, die Karte nicht gesperrt und der (tägliche oder wöchentliche) Verfügungsrahmen nicht überschritten ist, nicht aber, ob das Konto auch eine entsprechende Deckung aufweist. Sind die Voraussetzungen gegeben, erteilt der Computer eine Autorisierung (»wird bezahlt«), die dem Händler übermittelt wird. Hierin liegt zugleich das abstrakte Schuldversprechen (§ 780 BGB) der Bank, das der Händler im Lastschriftverfahren bei der Bank einlösen kann[139]. Wegen der vergleichbaren Prüfinhalte zwischen Autorisierungscomputer und einfachem Geldautomaten können deren Ergebnisse entsprechend übertragen werden:

(1) Nutzt jemand eine **gefälschte oder deliktisch erworbene Debit-Karte**, so begeht er zwar keinen Betrug gegenüber dem Händler, da dieser von der kartenausgebenden Bank unabhängig von der Befugnis des Kunden zur Kartennutzung ein abstraktes Schuldversprechen erhält und sich so über die Befugnis keinerlei Gedanken macht, er über die Befugnis also nicht irrt[140]. Da er aber den Autorisierungscomputer einem Schalterbeamten vergleichbar über seine Befugnis zur Nutzung der Debit-Karte mittels Eingabe der PIN »täuscht«, verwendet er nach der Lehre von der Täuschungsäquivalenz unbefugt Daten (durch die PIN-Eingabe)[141].

(2) Hat der Dritte die Karte **im Auftrag des Inhabers** zum Kaufen einer bestimmten Ware mit PIN erhalten und überschreitet er seine Beschränkung im Innenverhältnis, so scheidet mangels Täuschungsäquivalenz (unbeschränkte Außenvollmacht!) § 263 a Var. 3 StGB aus[142].

(3) Der **berechtigte Karteninhaber** begeht bei einer Überschreitung seines Kreditrahmens durch den Einkauf im POS-Verfahren weder einen Betrug zu Lasten des Händlers (kein Irrtum wegen des abstrakten Schuldversprechens) noch einen Computerbetrug mangels Täuschungsäquivalenz (Zahlungswilligkeit und Bonität werden nicht vom Autorisierungscomputer geprüft, ein fiktiver Schalterbeamte würde hierüber nicht irren)[143].

ff) Davon strikt zu trennen ist das **elektronische Lastschriftverfahren** des Handels (ELV), dass das vergleichbare (Ende 2006 ausgelaufene[144]) POZ-System[145] des Zentralen Kreditausschusses ersetzt hat. Hierbei kauft der Kunde mittels Debit-Karte und Unterschrift ein, indem die Karte an der Kasse in das Terminal gesteckt wird. Dieses sendet die auf der Karte gespeicherten Daten zu einem Zentralrechner, der diese mit der Sperrdatei vergleicht. Ist die Karte nicht gesperrt, druckt das Terminal ein Lastschriftformular mit dem Rechnungsbetrag aus, das der Kunde zu unterschreiben hat. Dieses Verfahren elektronisiert also nur die Lastschriftformular-Erstellung, ermöglicht aber kein elektronisches Bezahlen mit der Folge, dass dies keine Fallgruppe des Computerbetrugs ist. Benutzt jemand diese Bezahlform, der deliktisch die Karte erlangt hat oder der als berechtigter Kartenbesitzer sein Konto überzogen hat, so wird der Händler über die Zahlungswilligkeit und –fähigkeit getäuscht und es liegt ein einfacher Betrug (§ 263 Abs. 1 StGB) vor[146].

gg) **Weitere Fallkonstellationen** der dritten Tathandlungsmodalität sind die Verwendung der Debit-Karte als Geldkarte (Aufladen des in ihnen enthaltenen »Chips« am Geldautomaten sowie deren Nutzung beim Bezahlen kleinerer Beträge, z. B. am Parkautomaten)[147], das Verwenden gefälschter Telefonkarten in der Telefonzelle[148] oder die Nutzung deliktisch erlangter Zugangsdaten zu Pay-TV-Programmen (sog. »Piratenkarten«)[149].

e) Die vierte Tathandlungsmodalität der **sonstigen unbefugten** (sprich: täuschungsäquivalenten) **Einwirkung auf den Ablauf** (als Grundtatbestand) wurde vom Gesetzgeber vor allem geschaffen, um neue Manipulationstechniken zu erfassen, insbesondere Hardware-Manipulationen[150]. Hohe praktische Bedeutung wie Klausurrelevanz erlangt hat diese Variante jedoch durch die ordnungsgemäße Bedienung eines Automaten mit Sonderwissen. Hierzu der

5. Fall (nach BGHSt. 40, 331 ff. mit Anm. *Otto*, JK 95, StGB § 263 a/8): A erwarb von einem Mitarbeiter der N-GmbH illegal ein Computerprogramm, das für den Spielverlauf bei den Geldspielautomaten »Jacky-Jackpot« der N-GmbH maßgebend war. Mit diesem auf einer Diskette gespeicherten Programm und einem Laptop begab er sich in eine Gaststätte, in der ein »Jacky-Jackpot« stand. Er spielte mehrfach, um Daten aus dem laufenden Programm in seinen Computer eingeben zu können und so den Programmverlauf zu berechnen. Dieses Wissen verwendete er dann bei weiteren Spielen, bei denen er durch das Drücken der sog. »Risiko«-Taste (diese ermöglicht es, entweder den Gewinn zu verlieren oder zu vervielfältigen) zu bestimmten Zeitpunkten jeweils ein bestimmtes Gewinnbild erzeugte und so den Automaten leer spielte. Er erlangte 100 €. Strafbarkeit des A?

Lösung: Neben einer Strafbarkeit nach § 17 Abs. 2 UWG (Verschaffen von Geschäftsgeheimnissen) kommt § 263 a Abs. 1 StGB in Betracht: Durch das Drücken der Risiko-Taste während des Spiels hat A jeweils den Programm-Ablauf derart verändert, dass das »normale Spiel« überging in ein Spiel mit erhöhten Gewinn- und Verlust-Chancen, so dass er das »Ergebnis eines Datenverarbeitungsvorgangs« durch eine »Einwirkung auf den Ablauf« beeinflusst hat. Hierbei nutzte er zwar seine Sonderkenntnisse in Form des konkreten Programmablaufs, diese führte er aber nicht in den Automaten ein, so dass er diese Daten vom Programmablauf nicht »verwendete« und § 263 a Abs. 1 Var. 3 StGB ausscheidet[151]. Es verbleibt nur die 4. Var. mit der Frage, ob das ordnungsgemäße Bedienen des Geldspielautomaten »unbefugt« war. Die Anhänger der computerspezifischen Auslegung würden dies verneinen[152], die Anhän-

139 Vgl. zum Ablauf umfassend Altenhain, JZ 1997, 752 m. w. N.

140 Ebenso Rengier (o. Fn. 17), § 14 Rdn. 27.

141 So Altenhain, JZ 1997, 752 (756), LK/Tiedemann (o. Fn. 5), § 263 a Rdn. 52, SK-StGB/Hoyer, § 263 a Rdn. 40, MüKo-StGB/Wohlers, § 263 a Rdn. 48 und Sch/Schr/Cramer/Perron (o. Fn. 17), § 263 a Rdn. 15.

142 Ebenso SK-StGB/Hoyer, § 263 a Rdn. 40, MüKo-StGB/Wohlers, § 263 a Rdn. 48, Sch/Schr/Cramer/Perron (o. Fn. 17), § 263 a Rdn. 13 und Rossa, CR 1997, 219 (221 f.); aA NK-StGB/Kindhäuser (o. Fn. 13), § 263 a Rdn. 53 und Lackner/Kühl (o. Fn. 17), § 263 a Rdn. 14.

143 Ebenso Altenhain, JZ 1997, 752 (758), SK-StGB/Hoyer, § 263 a Rdn. 40, Sch/Schr/Cramer/Perron (o. Fn. 17), § 263 a Rdn. 13, Krey/Hellmann (o. Fn. 29), Rdn. 518 e und Rossa, CR 1997, 219 (221 f.); aA NK-StGB/Kindhäuser (o. Fn. 13), § 263 a Rdn. 53 und Lackner/Kühl (o. Fn. 17), § 263 a Rdn. 14.

144 Vgl. hierzu die Pressemitteilung des Zentralen Kreditausschusses (ZKA: Vereinigung der fünf Spitzenverbände der deutschen Kreditwirtschaft) vom 15. Oktober 2004.

145 »POZ« stand für »*p*oint-of-sale *o*hne *Z*ahlungsgarantie«. Vgl. zu diesem früheren System Altenhain, JZ 1997, 752 (759).

146 Ebenso BGHSt. 46, 146 (153 f.).

147 Vgl. hierzu LK/Tiedemann (o. Fn. 5), § 263 a Rdn. 54, SK-StGB/Hoyer, § 263 a Rdn. 42, MüKo-StGB/Wohlers, § 263 a Rdn. 50 und Sch/Schr/Cramer/Perron (o. Fn. 17), § 263 a Rdn. 13.

148 Hierzu BGH, NStZ 2005, 213, LG Würzburg, NStZ 2000, 374 f. (mit Anm. Otto, JK 00, StGB § 263 a/11) und Hecker, JA 2004, 762 ff.; vgl. auch OLG München, NStZ 2008, 403: Abbruch der Telefonverbindung nach Herstellung de gebührenpflichtigen Verbindung vor Abbuchung als § 263 Abs. 1 Var. 4 StGB.

149 Streitig ist einzig, ob ein unmittelbarer Vermögensschaden vorliegt: bejahend Scheffler, CR 2002, 151 (154 f.), verneinend Beucher/Engels, CR 1998, 101 (104).

150 BT-Drs. 10/5058, S. 30.

151 Ebenso LG Ravensburg, StV 1991, 214 (215), Arloth, **JURA** 1996, 354 (356 f.), MüKo-StGB/Wohlers, § 263 a Rdn. 31 und Sch/Schr/Cramer/Perron (o. Fn. 17), § 263 a Rdn. 8; aA OLG Celle, NStZ 1989, 367 (368) (mit Anm. Otto, JK 90, StGB § 263 a/3) und Arzt/Weber/Heinrich/Hilgendorf (o. Fn. 13), § 21 Rdn. 47; offen gelassen von BGHSt. 40, 331 (334).

152 Vgl. nur OLG Celle, NStZ 1989, 367 (368) und Arloth, CR 1996, 359 (364 f.).

ger einer subjektiven Ansicht wegen Verstoßes gegen den Willen des Automatenaufstellers bejahen.

Nach der täuschungsäquivalenten Auslegung muss man eine Parallele zur Rechtsprechung zum Wettbetrug ziehen: Man stelle sich vor, der Spielablauf erfolge derart, dass der Automatenbetreiber jeweils den Geldeinsatz annimmt und dann die Start- oder Risiko-Taste drückt und den Gewinn auszahlt (vergleichbar dem Roulette im Casino). Der Täter macht nun einen kleinen Gewinn, was ihm die Möglichkeit der Risiko-Option gibt, bei der zwischen dem Automateninhaber, vertreten durch den Mitarbeiter, und dem Täter ein zusätzlicher Wettvertrag abgeschlossen wird. Kennt der Täter aufgrund seiner Kenntnis vom Programmverlauf den Ausgang bereits zuvor, so muss man fragen, ob er mit dem Abschluss der Wette den Mitarbeiter täuschen würde. Mit seiner Fußballwett-Entscheidung hat der 5. Strafsenat (BGHSt. 51, 165 ff.) kürzlich einen normativen Mittelweg gewählt und entschieden, dass es auf die jeweils geschäftstypische Risikoverteilung ankomme[153]: Das Vorhandensein frei zugänglicher leistungsbeschreibender Informationen wie bei Sportwetten von der Mannschaftsaufstellung oder der Verletzung eines Spielers im Training gehöre zum Wettrisiko des Wettanbieters, so dass deren Nichtexistenz beim Vertragsschluss nicht konkludent miterklärt werde[154]. Dagegen überschreite die Kenntnis von Spielmanipulationen das erlaubte Risiko, so dass deren Nichtexistenz beim Vertragsschluss konkludent miterklärt werde und der Wettanbieter hierüber getäuscht werde. Entsprechendes muss gelten, wenn rechtswidrig Insiderinformationen beschafft wurden. Folgerichtig hat BGHSt. 40, 331 (335) entschieden, dass eine »unbefugte« Einwirkung auf den Ablauf jedenfalls dann vorliege, »wenn der Spieler – wie hier – ein Computerprogramm auswertet, das er rechtswidrig erlangt hat«[155]. Hiervon zu unterscheiden ist der

6. Fall (nach OLG Braunschweig, NJW 2008, 1464 mit Anm. *Geppert*, JK 10/08, StGB § 263 a/16): A betankte in 33 Fällen verschiedene Fahrzeuge an einer vollautomatischen Selbstbedienungstankstelle für Beträge zwischen 71 und 80 €, wobei ihr bewusst war, dass Betankungen für mehr als 70 € wegen eines Defekts der Anlage vom System nicht als Treibstoffentnahmen erfasst und dementsprechend auch nicht das Konto der vor dem Tankvorgang einzuführenden Bankkarte belastet wurde. Strafbarkeit der A?

Hatte der Täter im *5. Fall rechtswidrige Kenntnisse* von einem *ordnungsgemäßen Programmablauf*, so verfügte A im *6. Fall* über *rechtmäßige* (die Herkunft der Kenntnisse konnte nicht geklärt werden: vermutlich einfache Beobachtung!) *Kenntnisse* von einem *fehlerhaften Programmablauf*. Legt man auch hier die täuschungsäquivalente Auslegung mit normativer Risikoverteilung zugrunde, so wird man die Verwendung für jedermann zugänglicher Kenntnisse vom Programmablauf einer Datenverarbeitungsanlage normativ dem Automatenaufsteller zuordnen müssen mit der Folge, dass es mangels konkludenter Täuschung eines fiktiven Tankwarts an einer »unbefugten« Einwirkung fehlt. Hierfür spricht auch, dass der Tankautomat bereits vor dem Tankvorgang fehlerhaft funktionierte, ein fiktiver Tankwart also bereits irrte und so sein Irrtum vom Täter nur ausgenutzt (was für § 263 StGB nicht genügt) und nicht hervorgerufen wurde. § 263 a Abs. 1 Var. 4 StGB ist daher zu verneinen[156].

3. Die vom Computer infolge des aufgrund der Täterhandlung beeinflusste Ergebnis des Datenverarbeitungsvorgangs unmittelbar bewirkte Vermögensdisposition muss zu einem nicht durch einen zumindest gleichwertigen Vermögenszuwachs auf der anderen Seite ausgeglichenen **Vermögensschaden** geführt haben, wobei wie beim Betrug der Eintritt einer schadensgleichen konkreten Vermögensgefährdung (z. B. durch eine vom Computer vorgenommene Fehlbuchung) genügt[157]. Infolge des Missbrauchs von Debit-Karten am Bankomaten durch einen Dritten wird stets die kartenausgebende Bank geschädigt, da sie in Höhe des abgehobenen Betrages mangels wirksamer Weisung seitens des Kontoinhabers keinen Aufwendungsersatzanspruch (§§ 675 Abs. 1, 670 BGB) hat; ein Schadensersatzanspruch der Bank wegen einer Obliegenheitsverletzung gegenüber dem Kontoinhaber (z. B. bei verspäteter Schadensmeldung) ändert als unsichere Rechtsposition hieran nichts[158]. Ist in anderen Fällen der Geschädigte nicht der Betreiber der Datenverarbeitungsanlage, so finden die Grundsätze über den Dreiecksbetrug entsprechende Anwendung[159]. Zwar kann man »schwerlich ein Näheverhältnis iSd Lagertheorie zwischen Bankcomputer und Bankkunden konstruieren«[160], da mittels des Computers aber nur Vermögensverfügungen des Betreibers der Datenverarbeitungsanlage automatisiert getroffen werden, ist beim »Computerdreiecksbetrug« auf ein Näheverhältnis zwischen diesem und dem Geschädigten abzustellen[161].

III. Subjektive Tatbestand

Der subjektive Tatbestand des § 263 a Abs. 1 StGB verlangt wie beim einfachen Betrug neben **bedingtem Vorsatz** (mit der Kenntnis aller tatsächlichen Umstände, aus denen sich die Täuschungsäquivalenz des Merkmals »unbefugt« Verhaltens ergibt[162]) sowie die **Absicht** (dolus directus ersten Grades), »sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen«, der mit dem verursachten Schaden stoffgleich sein muss[163]. Beim Missbrauch einer Debit-Karte im POS-System besteht die Stoffgleichheit zwischen dem beabsichtigten Vermögensvorteil und dem Vermögensschaden darin, dass der Täter neben dem Eigentum an der erworbenen Ware die Befreiung von der Verbindlichkeit zur Kaufpreiszahlung (§ 433 Abs. 2 BGB) erlangt, mit der die Bank belastet wird[164].

IV. Sonstige deliktsspezifische Besonderheiten

1. Täterschaft und Teilnahme richten sich nach den allgemeinen Vorschriften. Mittelbarer Täter ist derjenige, der ein gutgläubiges Werkzeug (z. B. eine Sekretärin) dazu benutzt, die Daten in den Computer einzugeben (und damit zu »verwenden«)[165]. Gehilfe ist etwa derjenige, der Dekodierungsdaten für

153 BGHSt. 51, 165 (170 f.); vgl. zur normativen Betrachtungsweise beim Betrug bereits OLG Celle, StV 1994,188 (189), LK/Tiedemann (o. Fn. 5), § 263 Rdn. 30 und SK-StGB/Hoyer, § 263 Rdn. 42 ff.

154 Vgl. auch Kutzner, JZ 2006, 712 (716).

155 Zustimmend LK/Tiedemann (o. Fn. 5), § 263 a Rdn. 61, SK-StGB/Hoyer, § 263 a Rdn. 45 und Sch/Schr/Cramer/Perron (o. Fn. 17), § 263 a Rdn. 17.

156 Ebenso Geppert, JK 10/08, StGB § 263 a/16; anders OLG Braunschweig, NJW 2008, 1464 auf der Grundlage der subjektiven Ansicht.

157 Vgl. hierzu Sch/Schr/Cramer/Perron (o. Fn. 17), § 263 a Rdn. 24 und SK-StGB/Hoyer, § 263 a Rdn. 52; jüngst kritisch zur schadensgleichen Vermögensgefährdung BGHSt. 52, 323 (338) und BGH, ZIP 2009, 1854 (1856 f.: der Begriff sei »missverständlich«).

158 Vgl. BGH, NStZ 2001, 316 und BGH, NStZ 2008, 396 (397).

159 Vgl. zu diesen ausführlich Kraatz, **JURA** 2007, 531 (532 f.).

160 Haft, NStZ 1987, 6 (8), der die Voraussetzungen des Dreiecksbetrugs für nicht erforderlich hält, sei der Computerbetrug doch vom Gesetzgeber bereits strukturell als »Dreiecksbetrug« ausgestaltet.

161 Ebenso Lenckner/Winkelbauer, CR 1986, 654 (659), LK/Tiedemann (o. Fn. 5), § 263 a Rdn. 71, MüKo-StGB/Wohlers, § 263 a Rdn. 64 und Sch/Schr/Cramer/Perron (o. Fn. 17), § 263 a Rdn. 22.

162 Ebenso SK-StGB/Hoyer, § 263 a Rdn. 53.

163 Vgl. LK/Tiedemann (o. Fn. 5), § 263 a Rdn. 76, MüKo-StGB/Wohlers, § 263 a Rdn. 66, Wessels/Hillenkamp (o. Fn. 17), Rdn. 604 und Sch/Schr/Cramer/Perron (o. Fn. 17), § 263 a Rdn. 29.

164 Vgl. zum Stoffgleichheits-Problem in diesem Zusammenhang Altenhain, JZ 1997, 752 (756), MüKo-StGB/Wohlers, § 263 a Rdn. 67 und SK-StGB/Hoyer, § 263 a Rdn. 56; zu einfach daher LK/Tiedemann (o. Fn. 5), § 263 a Rdn. 76, der auf das Eigentum an der erworbenen Ware als Vorteil abstellt.

165 Vgl. nur SK-StGB/Hoyer, § 263 a Rdn. 13.

den unberechtigten Pay-TV-Zugang anderen bereitstellt[166] oder derjenige, der sein Konto zur Verfügung stellt, um darauf durch Phishing erlangtes Geld überweisen zu lassen und das Geld dann dem Täter auszuzahlen[167].

2. Der **Versuch** ist nach §§ 263 a Abs. 2, 263 Abs. 2 StGB strafbar. Ein unmittelbares Ansetzen liegt in den Bankomaten-Fällen bereits mit dem Einführen der Debit-Karte vor[168]. Bereits die **Vorbereitung** durch das zumindest bedingt vorsätzliche Herstellen, Verschaffen, Feilhalten, Verwahren oder Überlassen eines Computerprogramms, »deren (ergänze: alleiniger[169]) Zweck die Begehung einer Tat« nach Absatz 1 ist, ist nach § 263 a Abs. 3 StGB strafbar, allerdings mit der Möglichkeit des persönlichen Strafaufhebungsgrundes einer tätigen Reue nach § 263 a Abs. 4 i. V. m. § 149 Abs. 2 und 3 StGB.

3. Der Computerbetrug wird **qualifiziert** nach §§ 263 a Abs. 2, 263 Abs. 5 StGB bei einer bandenmäßigen Begehung. Nach §§ 263 a Abs. 2, 263 Abs. 3 StGB gelten die dortigen **Regelbeispiele**. Bei geringwertigem Schaden (bis 50 €[170]) ist nach §§ 263 a Abs. 2, 263 Abs. 4, 248 a StGB ein **Strafantrag** erforderlich und ein besonders schwerer Fall scheidet aus (§§ 263 a Abs. 2, 263 Abs. 4, 243 Abs. 2 StGB).

4. Konkurrenzrechtlich besteht zwischen dem Diebstahl einer Debit-Karte und ihrer späteren Nutzung am Bankomaten oder im POS-Verfahren Tatmehrheit, da Geschädigter der Abhebung die kartenausgebende Bank und damit ein anderer Rechtsgutsträger ist[171]. Verwendet ein Täter innerhalb kürzester Zeit eine Debit-Karte mehrfach an einem Bargeldautomaten und hebt er jeweils kleinere Beträge ab, so sind die einzelnen Abhebungen jeweils als eine Tat im materiell-rechtlichen Sinne anzusehen[172]. Lässt sich nicht mehr aufklären, ob Betrug oder Computerbetrug vorliegt (etwa wenn sich nicht aufklären lässt, ob ein konkreter Überweisungsträger menschlich oder computertechnisch bearbeitet wurde), so ist eine Wahlfeststellung möglich[173].

166 So Beucher/Engels, CR 1998, 101 (104).

167 AG Hamm, CR 2006, 70 f.; vgl. hierzu Neuheuser, NStZ 2008, 492 ff.

168 Vgl. LK/Tiedemann (o. Fn. 5), § 263 a Rdn. 79, MüKo-StGB/Wohlers, § 263 a Rdn. 73 und Sch/Schr/Cramer/Perron (o. Fn. 17), § 263 a Rdn. 30.

169 Das Programm muss sich objektiv von zu legalen Zwecken nutzbaren Programmen unterscheiden, vgl. nur SK-StGB/Hoyer, § 263 a Rdn. 59.

170 Vgl. OLG Zweibrücken, NStZ 2000, 536, OLG Hamm, wistra 2004, 34 und OLG Frankfurt a. M., NStZ-RR 2008, 311; für eine Grenze von 25 € dagegen BGHR StGB § 248 a geringwertig 1 (aus dem Jahre 2004).

171 Ebenso BGH, NStZ 2001, 316 (mit Anm. Otto, JK 01, StGB § 263 a/12), Arzt/Weber/Heinrich/Hilgendorf (o. Fn. 13), § 21 Rdn. 52, Wessels/Hillenkamp (o. Fn. 17), Rdn. 614, MüKo-StGB/Wohlers, § 263 a Rdn. 75 und NK-StGB/Kindhäuser (o. Fn. 13), § 263 a Rdn. 64; aA SK-StGB/Hoyer, § 263 a Rdn. 64: § 242 StGB als mitbestrafte Vortat.

172 BGH, wistra 2008, 220 f.

173 So zuletzt BGH, NStZ 2008, 281 f. (mit zust. Anm. Geppert, JK 9/08, StGB § 263 a/15); vgl. zur Postpendenzfeststellung (sicherer Computerbetrug, unsichere betrügerische Scheckeinlösung zuvor) BGH, NStZ 2008, 396 f.