C. Computerbetrug (§ 263a)

Die Strafnorm des § 263a wurde nachträglich in das StGB aufgenommen, um bestehende Strafbarkeitslücken zu schließen, die darin bestanden, daß bei einer mißbräuchlichen Benutzung von Datenverarbeitungsanlagen ein Betrug ausscheidet. Denn der Tatbestand des Betrugs setzt eine Täuschung, also eine Einwirkung auf das intellektuelle Vorstellungsbild eines anderen Menschen mit dem Ziel der Irreführung voraus. Bei dem Ingangsetzen bspw. des Geldausgabemechanismus eines Geldautomaten ist das nicht der Fall, weil hier nicht auf das intellektuelle Vorstellungsbild eines Menschen eingewirkt, sondern nur ein vollautomatisierter Datenverarbeitungsprozeß in Gang gesetzt wird.
Aufgrund der zunehmenden Computerkriminalität hat der Computerbetrug erhebliche **Examensrelevanz** bekommen.

> **Hinweis für die Fallbearbeitung:** Aufgrund des Umstands, daß § 263a Strafbarkeitslücken in bezug auf § 263 schließen soll, empfiehlt es sich in der Fallbearbeitung, mit der Prüfung des § 263 zu beginnen, die Verwirklichung dieses Tatbestands am Merkmal der Täuschung scheitern zu lassen, um sodann auf § 263a einzugehen und diesen Tatbestand durchzuprüfen.

Es empfiehlt sich folgender Prüfungsaufbau:

Computerbetrug (§ 263a)

I. Tatbestand

1. Objektiver Tatbestand

Alle in § 263a I Var. 1-4 genannten Tathandlungen setzen voraus, daß der Täter das Vermögen eines anderen dadurch beschädigt, daß er **das Ergebnis eines Datenverarbeitungsvorgangs beeinflußt**. Dieses Erfordernis tritt bei § 263a an die Stelle von Irrtum u. Vermögensverfügung. Der Begriff des Vermögensschadens ist mit dem des § 263 identisch.

- ⇨ Unter **Daten** sind alle codierten und codierbaren Informationen unabhängig vom Verarbeitungsgrad zu verstehen. Dazu zählen auch der Verarbeitung dienende Programme, weil sie als fixierte Arbeitsanweisungen an den Computer aus Daten zusammengefügt sind.
- ⇨ Unter **Datenverarbeitung** sind die technischen Vorgänge zu verstehen, bei denen durch Aufnahme von Daten und ihre Verknüpfung nach Programmen Arbeitsergebnisse erzielt werden.
- ⇨ Der Täter muß durch seine Tathandlung **das Ergebnis beeinflussen**, d.h. für das Verarbeitungsergebnis zumindest mitursächlich geworden sein.

a. Unrichtige Gestaltung des Programms (Var. 1)

Die 1. Variante erfaßt sog. **Programmanipulationen**. Ein Programm ist eine durch Daten fixierte Arbeitsanweisung an den Computer. „Unrichtig" ist die Programmgestaltung, wenn die Arbeitsanweisung auf betrugsrelevante Tatsachen bezogen ist und wenn sie bewirkt, daß die Daten zu einem Ergebnis verarbeitet werden, das inhaltlich objektiv unrichtig ist.

b. Verwendung unrichtiger oder unvollständiger Daten (Var. 2)

Hier werden Fälle erfaßt, in denen eingegebene Daten in einen anderen Zusammenhang gebracht oder unterdrückt werden, sog. ***Input- oder Eingabemanipulationen***.

- ⇨ **Unrichtig** sind die Daten, wenn die mit ihnen dargestellten Informationen falsch sind, also die Wirklichkeit bzw. den Lebenssachverhalt unzutreffend wiedergeben.

- ⇨ Daten sind **unvollständig**, wenn Informationen über „wahre" Tatsachen pflichtwidrig vorenthalten werden.
- ⇨ **Verwendet** werden Daten, wenn sie in den Datenverarbeitungsprozeß eingeführt werden (dazu näher in Var. 3).

c. Unbefugte Verwendung von Daten (Var. 3)

- ⇨ **Verwendung** von Daten: Während eine weite Auslegung jede Nutzung von Daten genügen läßt, verlangt die (zutreffende) enge Auslegung eine Eingabe von Daten gerade in den Datenverarbeitungsprozeß. Das Befolgen der engen Auslegung führt dazu, daß der Anwendungsbereich des Auffangtatbestandes des § 263a I Var. 4 ausgedehnt wird (vgl. dort).
- ⇨ **Unbefugte** Verwendung von Daten: Auch die Auslegung des Merkmals „unbefugt" ist äußerst umstritten und sehr **prüfungs-** bzw. **examensrelevant**. Folgende Konstellationen müssen sicher beherrscht werden:
  - ⇨ Nach der am weitesten gehenden sog. **subjektivierenden** Auslegung ist jede Datenverarbeitung „unbefugt", die dem wirklichen oder mutmaßlichen *Willen des Rechtsgutsinhabers* (des Berechtigten) widerspricht.
  - ⇨ Vertreter der engen sog. **computerspezifischen** Auslegung stellen darauf ab, ob der einer Datenverwendung entgegenstehende *Wille des Betreibers* im Computerprogramm berücksichtigt ist. Entscheidend ist danach, ob die Befugnis des Verwenders der Daten im Programmablauf Niederschlag gefunden hat, also vom Programm selbst überprüft wird. Diese Überprüfung findet regelmäßig durch eine entsprechende Nachfrage, etwa durch Anforderung und Überprüfung der persönlichen Geheimnummer, der PIN, statt.
  - ⇨ Eine vermittelnde Ansicht, die sog. **betrugsspezifische** Auslegung, orientiert sich an § 263 und verlangt ein täuschungsäquivalentes Verhalten des Täters. Entscheidend ist danach, ob die Verwendung der Daten gegenüber einem Menschen als zumindest schlüssige Vorspiegelung der Befugnis zu deuten wäre. Durch ihre Anlehnung an § 263 entspricht sie dem Zweck des § 263a, lediglich bestehende Strafbarkeitslücken zu schließen, die darin bestanden, daß bei einer mißbräuchlichen Benutzung von Datenverarbeitungsanlagen ein Betrug ausscheidet. Ihr ist daher zu folgen.

d. Sonst unbefugte Einwirkung auf den Ablauf (Var. 4)

Die letzte Tatvariante des § 263a I soll nach Auffassung des Gesetzgebers als **Auffangtatbestand** fungieren und die noch verbleibenden, von den anderen Tatvarianten nicht gedeckten Manipulationen erfassen. Die Reichweite der 4. Variante hängt also maßgeblich davon ab, wie viele der denkbaren Computerdelikte man bereits unter die ersten drei Varianten (insbesondere unter die 3. Variante) subsumieren konnte. Dies wiederum hängt davon ab, ob man für die „Verwendung von Daten" i.S. der 2. und 3. Variante mit der zutreffenden h.M. eine Eingabe in den Datenverarbeitungsprozeß voraussetzt oder jede Nutzung von Daten genügen läßt.

2. Subjektiver Tatbestand

Vorsatz (mindestens *dolus eventualis*) und **Absicht** (*dolus directus* 1. Grades) der rechtswidrigen und stoffgleichen eigen- oder fremdnützigen Bereicherung

II. Rechtswidrigkeit und III. Schuld: Es gelten die allgemeinen Grundsätze.

IV. Strafzumessungsregel (§ 263 III) und Qualifikation (§ 263 V)

Nach § 263a II gilt § 263 II bis VII entsprechend (insbesondere: Strafbarkeit des Versuchs, besonders schwere Fälle und §§ 247, 248a).

I. Tatbestand

1. Objektiver Tatbestand

Alle in § 263a I Var. 1-4 genannten Tathandlungen setzen voraus, daß der Täter das Vermögen eines anderen dadurch beschädigt, daß er **das Ergebnis eines Datenverarbeitungsvorgangs beeinflußt**. Dieses Erfordernis tritt bei § 263a an die Stelle von Irrtum und Vermögensverfügung. Der Datenverarbeitungsvorgang muß also **vermögenserheblich** sein.[1] Der Begriff des Vermögensschadens ist mit dem des § 263 identisch.

- ⇨ Der Begriff der **Daten** ist gesetzlich nicht näher bestimmt. Mit Blick auf den Zweck der Vorschrift ist er aber weit zu verstehen. Nach h.M. umfaßt er alle codierten und codierbaren Informationen unabhängig vom Verarbeitungsgrad (z.B. Eingabe-, Stamm- und Ausgabedaten usw.) und erfaßt daher auch der Verarbeitung dienende Programme, weil sie als fixierte Arbeitsanweisungen an den Computer aus Daten zusammengefügt sind.[2]
- ⇨ Unter **Datenverarbeitung** sind die technischen Vorgänge zu verstehen, bei denen durch Aufnahme von Daten und ihre Verknüpfung nach Programmen Arbeitsergebnisse erzielt werden. Soweit das Gesetz von **Datenverarbeitungsvorgängen** spricht, sind nur die konkreten, dem jeweiligen Ergebnis einer EDV vorausliegenden Vorgänge gemeint.[3]

  Hinweis für die Fallbearbeitung: Obwohl Daten auch in rein mechanisch wirkenden Geräten verarbeitet werden können, dürfen Datenverarbeitungen, die zur Verwirklichung des § 263a führen können, nur in EDV-Anlagen vorkommen; anderenfalls würde die Vorschrift des § 265a (Automatenmißbrauch) funktionslos.[4] Da andererseits aber in nahezu allen Waren- und Leistungsautomaten elektronische Geldprüfvorrichtungen enthalten sind, die das eingeworfene Geld erst aufgrund des Ergebnisses einer Datenverarbeitung akzeptieren, fällt der Mißbrauch solcher Automaten im allgemeinen unter § 263a.

- ⇨ Der Täter muß durch seine Tathandlung **das Ergebnis beeinflussen**, d.h. für das Verarbeitungsergebnis zumindest mitursächlich geworden sein; eine Beeinflussung setzt keinen bereits in Gang befindlichen Datenverarbeitungsvorgang voraus. Vgl. dazu insbesondere das unten auf S. 233 dargestellte Beispiel zum **Leerspielen von Geldspielautomaten**.

Die **Tathandlungen**, die im Verhältnis zu § 263 an die Stelle der Täuschung treten, sind in § 263a I Var. 1-4 **abschließend aufgezählt** und daher nicht durch Analogie erweiterungsfähig.[5]

a. Unrichtige Gestaltung des Programms (§ 263a I Var. 1)

Die 1. Variante erfaßt sog. **Programmanipulationen**. Ein Programm ist eine durch Daten fixierte Arbeitsanweisung an den Computer. „Unrichtig" ist die Programmgestaltung, wenn die Arbeitsanweisung auf betrugsrelevante Tatsachen bezogen ist

[1] Vgl. LK-*Tiedemann*, § 263a Rn 65; *Laue*, JuS **2002**, 359, 363; *Eisele/Fad*, Jura **2002**, 305, 306.
[2] *Lackner/Kühl*, § 263a Rn 3; *Hilgendorf*, JuS **1996**, 509, 511; *Eisele/Fad*, Jura **2002**, 305, 306; *Laue*, JuS **2002**, 359, 362.
[3] *Lackner/Kühl*, § 263a Rn 4.
[4] LK-*Tiedemann*, § 263a Rn 1 u. 22.
[5] Vgl. *Hellmann*, JuS **2001**, 353, 356.

und wenn sie bewirkt, daß die Daten zu einem Ergebnis verarbeitet werden, das inhaltlich objektiv unrichtig ist.[6]

Da sich auch Programme aus Daten zusammensetzen und die Verwendung unrichtiger oder unvollständiger Daten von der 2. Variante erfaßt wird, kann es sich bei der 1. Variante nur um einen Spezialfall der 2. Variante handeln. Der Gesetzgeber wollte die Variante wegen der spezifischen Gefährlichkeit einer Programmanipulation besonders hervorheben.

Beispiel: Der Systemadministrator einer Firma gestaltet im Einvernehmen mit dem Firmeninhaber das Lohnabrechnungsprogramm so, daß die Löhne und Gehälter der Arbeitnehmer niedriger berechnet werden als gesetzlich vorgegeben. Als „Gegenleistung" erhält er von seinem Chef 2.000.- € in bar.
Hier ist das Programm objektiv unrichtig gestaltet, da es den rechtlichen Anforderungen nicht entspricht. Der Systemadministrator ist daher nach § 263a I Var. 1 strafbar, der Chef nach §§ 263a I Var. 1, 26.

b. Verwendung unrichtiger oder unvollständiger Daten (§ 263a I Var. 2)

Mit dieser Tatvariante werden Fälle erfaßt, in denen eingegebene Daten in einen anderen Zusammenhang gebracht oder unterdrückt werden, sog. ***Input- oder Eingabemanipulationen***.

- ⇨ **Unrichtig** sind die Daten, wenn die mit ihnen dargestellten Informationen falsch sind, also die Wirklichkeit bzw. den Lebenssachverhalt unzutreffend wiedergeben.[7]
- ⇨ Daten sind **unvollständig**, wenn Informationen über „wahre" Tatsachen pflichtwidrig vorenthalten werden.[8]
- ⇨ **Verwendet** werden Daten, wenn sie in den Datenverarbeitungsprozeß eingeführt werden (dazu näher in Var. 3).

Beispiele/Gegenbeispiele:

(1) Wenn der Täter mit einer **ec-Karte**[9], deren Kontendaten manipuliert sind, Geld von einem Automaten abhebt, verwendet er unrichtige Daten.

(2) Sonderproblem **Kreditkarten**: Mit Kreditkarten (zum Begriff der Kreditkarte vgl. die Ausführungen zu § 266b unten auf S. 239) kann (bspw. im Internet) bezahlt werden, indem die 16-stellige Nummer und das dazugehörige Gültigkeitsdatum an- bzw. eingegeben wird. Die Eingabe einer PIN wie bei der Benutzung einer ec-Karte ist insoweit nicht erforderlich. Wenn nun der Täter Kreditkartendaten eines anderen ohne dessen Erlaubnis verwendet, stellt sich die Frage, ob er sich wegen Computerbetrugs gem. § 263a Var. 2 strafbar macht. Da ebenfalls eine Strafbarkeit nach § 263a Var. 3 in Betracht kommt, sei insoweit auf die zusammenhängende Darstellung zu dieser Variante verwiesen.

(3) Fraglich ist auch, ob § 263a I Var. 2 verwirklicht ist, wenn der Täter bewußt wahrheitswidrig die Durchsetzung eines (nicht bestehenden) zivilrechtlichen Anspruchs im Wege des **automatisierten Mahnverfahrens** (vgl. § 689 I S. 2 ZPO) beantragt. Da vom Gericht im Mahnverfahren der Wahrheitsgehalt

---

[6] *Tröndle/Fischer*, § 263a Rn 6; *Lackner/Kühl*, § 263a Rn 7; SK-*Günther*, § 263a Rn 14; LK-*Tiedemann*, § 263a Rn 30.
[7] *Tröndle/Fischer*, § 263a Rn 7; SK-*Günther*, § 263a Rn 16; *Laue*, JuS **2002**, 359, 360.
[8] Sch/Sch-*Cramer*, § 263a Rn 7; *Lackner/Kühl*, § 263a Rn 10; *Tröndle/Fischer*, § 263a Rn 7.
[9] „ec" bedeutet nicht etwa „eurocheque", sondern „electronic cash".

der Angaben des Antragstellers zur Schlüssigkeit des Anspruchs nicht (mehr) geprüft wird, scheidet jedenfalls ein Betrug nach § 263 aus. Aber auch ein Computerbetrug nach § 263a I Var. 3 scheidet im Ergebnis aus. Zwar wurde der Computer des Amtsgerichts mit unzutreffenden Angaben „beschickt", infolge der fehlenden Prüfungspflicht des Gerichts würde aber auch eine Strafbarkeit nach § 263 nicht in Betracht kommen (s.o.). Bei einer betrugsspezifischen Auslegung des § 263a kann daher nichts anderes gelten.[10]

c. Unbefugte Verwendung von Daten (§ 263a I Var. 3)

Die Formulierung „**unbefugt**" stellt klar, daß die Daten jedenfalls „richtig" sein müssen, damit eine Strafbarkeit nach § 263a I Var. 3 in Betracht kommt. Im übrigen ist die Auslegung dieser Variante äußerst schwierig und entsprechend umstritten. Eine dem Wortsinn durchaus entsprechende Erstreckung des Tatbestands auf jegliche unbefugte Datenverwendung würde den Tatbestand uferlos machen und möglicherweise dem Verdickt der **Verfassungswidrigkeit** (Verstoß gegen den Bestimmtheitsgrundsatz und gegen das Schuldprinzip) unterstellen. Nach der hier vertretenen Auffassung ist daher bei beiden Tatbestandsmerkmalen eine **restriktive Auslegung** geboten.

- ⇨ **Verwendung** von Daten: Während eine weite Auslegung jede Nutzung von Daten genügen läßt[11], verlangt die (zutreffende) enge Auslegung eine Eingabe von Daten gerade in den Datenverarbeitungsprozeß[12]. Das Befolgen der engen Auslegung führt dazu, daß der Anwendungsbereich des Auffangtatbestands des § 263a I Var. 4 ausgedehnt wird (vgl. dort).
- ⇨ **Unbefugte** Verwendung von Daten: Auch die Auslegung des Merkmals „unbefugt" ist äußerst umstritten und sehr **prüfungs-** bzw. **examensrelevant** (Wann ist die Verwendung von Daten „unbefugt"? Kann auch der berechtigte Karteninhaber selbst seine Kartendaten unbefugt verwenden?). Folgende Konstellationen müssen sicher beherrscht werden:
  - ⇨ Verwendung einer **fremden Kreditkarte** bzw. von deren Daten zwecks **Erlangung von Leistungen aus dem Internet** (dazu sogleich)
  - ⇨ Verwendung einer **fremden ec-Karte** zwecks **Geldabhebung von Geldautomaten** (unten S. 222 ff.)
  - ⇨ Verwendung der **eigenen ec-Karte**, um in **vertragswidriger** Weise **Geld von Geldautomaten** abzuheben (unten S. 226 ff.)
  - ⇨ Verwendung einer **eigenen** oder **fremden ec-Karte** im **electronic-cash-Verfahren** (**point-of-sale-Verfahren**) ⇒ 1. Variante des bargeldlosen Einkaufens mit ec-Karte (unten S. 230 f.)
  - ⇨ Verwendung einer **eigenen** oder **fremden ec-Karte** im **elektronischen Lastschriftverfahren** ⇒ 2. Variante des bargeldlosen Einkaufens mit ec-Karte (unten S. 232 f.)

---

[10] *Lackner/Kühl*, § 263a Rn 20; *Tröndle/Fischer*, § 263a Rn 7; *Rengier*, BT I, § 14 Rn 6; **a.A.** LK-*Tiedemann*, § 263a Rn 39 u. 68; *Otto*, BT, § 52 Rn 37.

[11] So vertreten von BayObLG JR **1994**, 289, 290 f.; *Ranft*, JuS **1997**, 19, 20; *Hilgendorf*, JuS **1997**, 130, 131; *Otto*, BT § 52 Rn 35; offengelassen von BGHSt **40**, 331, 334.

[12] So vertreten von LK-*Tiedemann*, § 263a Rn 4 u. 42-46; *Lackner/Kühl*, § 263a Rn 12; *Rengier*, BT I, § 14 Rn 7; *Tröndle/Fischer*, § 263a Rn 7; *Laue*, JuS **2002**, 359, 362; *Jerouschek/Kölbel*, JuS **2001**, 780, 782.

⇨ Verwendung einer fremden ec-Karte als **Geldkarte** ⇒ 3. Variante des bargeldlosen Einkaufens mit ec-Karte (unten S. 233)

aa. Verwendung einer fremden Kreditkarte bzw. von deren Daten zwecks Erlangung von Leistungen aus dem Internet.

Beispiel[13]: Tankwart T hat sich in einem unbemerkten Moment von der **Kreditkarte** des Kunden K, der die Tankrechnung mit der Kreditkarte bezahlte, die 16-stellige Kreditkartennummer sowie das Ablaufdatum notiert. Am Abend zu Hause surfte er im Internet und rief die von Provider P betriebene Seite *www.girlsfun.com* auf. Von dieser Seite kann man gegen Bezahlung pornographische Bilder herunterladen. Die Bezahlung erfolgt durch das „beleglose Kreditkartenverfahren". Hierzu muß der *user* die 16-stellige Nummer seiner Kreditkarte sowie das Ablaufdatum eingeben. Die Eingabe einer PIN ist nicht erforderlich. Nach Inanspruchnahme der Leistung wird das Entgelt vom Girokonto des Karteninhabers abgebucht. Auch T nahm diese Leistung in Anspruch. Zur Bezahlung verwendete er aber nicht seine eigenen, sondern die Kreditkartendaten des K. Als von dessen Girokonto ein Betrag i.H.v. 420.- € abgebucht wird, meldet K den Schaden sofort dem Kreditkartenaussteller A und läßt die Karte sperren. A bucht den Betrag, den T verbraucht hatte, gem. der rechtlichen Verpflichtung auf das Konto des K zurück. Gleichzeitig wendet A sich an den Anbieter der fraglichen Internetseite P und läßt sich gem. der vertraglichen Ausgestaltung des Kreditkartenvertrags den an diesen zuvor geleisteten Betrag erstatten. P stellt Strafanzeige. Strafbarkeit des T?

1. Handlungsabschnitt: Notieren der Kreditkartendaten in der Tankstelle

a. Ein **Ausspähen von Daten** (§ 202a) kommt nicht in Betracht, da Kreditkartendaten nicht gegen unberechtigten Zugang besonders gesichert sind.

b. Auch liegt im Ergebnis kein **Diebstahl** (§ 242) vor, da T dem K zum einen die Karte nicht weggenommen und zum anderen die Karte – wie von Anfang an geplant – dem K ohne Vermögensverlust wieder zurückgegeben und somit ohne Zueignungsabsicht gehandelt hat.

c. Ein **Betrug** (§ 263) kommt ebenfalls nicht Betracht, weil es zumindest an der Vermögensverfügung durch K fehlte. Denn eine Vermögensverfügung muß unmittelbar zu einer Vermögensschädigung oder zumindest zu einer konkreten Vermögensgefährdung führen. Allein das Notieren der Kreditkartendaten führt noch nicht zu einer konkreten Vermögensgefährdung.

d. Hinsichtlich einer möglichen **Unterschlagung** (§ 246) ist zu beachten, daß T sich weder die Kreditkarte noch deren Sachwert zugeeignet hat.

e. Schließlich ist eine **Untreue** (§ 266) in Betracht zu ziehen. Doch auch dieser Tatbestand ist im Ergebnis nicht verwirklicht, weil T dem K gegenüber keine Vermögensbetreuungspflicht besaß.

2. Handlungsabschnitt: Verwendung der Kreditkartendaten im Internet

a. Eine Strafbarkeit des T wegen **Kreditkartenmißbrauchs gem. § 266b** kommt nicht in Betracht, da dieser Tatbestand die mißbräuchliche Verwendung durch den *Karteninhaber* voraussetzt. T war nicht Inhaber der Kreditkarte, deren Daten er verwendet hat.

[13] Vgl. *Laue*, JuS **2002**, 359 ff.

b. Möglicherweise liegt aber eine Strafbarkeit wegen **Computerbetrugs** gem. **§ 263a I Var. 2** vor. Dazu müßte T unrichtige oder unvollständige Daten **verwendet** haben. Fraglich ist, ob allein die fehlende Berechtigung die verwendeten Daten unrichtig machen.
Die Richtigkeit der Daten kann abstrakt oder konkret, d.h. im Hinblick auf den Verwender, beurteilt werden.

⇨ Bei einer *abstrakten* Betrachtungsweise können Daten einer Originalkarte im Regelfall (also dann, wenn keine zusätzlichen Daten gefordert werden) auch dann nicht unrichtig sein, wenn sie ein Unberechtigter verwendet hat. Denn abstrakt gesehen, werden genau die Daten verwendet, die auf der Originalkarte vorhanden sind.

⇨ Stellt man hingegen auf den *konkreten* Fall ab, bilden die Daten nur in der Hand des Karteninhabers die Wirklichkeit ab. Verwendet sie ein Unberechtigter, sind sie damit unrichtig, weil sie eine nicht mit der Wirklichkeit übereinstimmende Information über Identität und Berechtigung des Verwenders liefern.[14]

Der Wortlaut der Norm läßt beide Möglichkeiten gleichermaßen zu. Berücksichtigt man aber, daß bei der Verwendung der Kreditkarte im beleglosen Zahlungsverkehr (also insbesondere bei Internet-Bestellungen oder -Dienstleistungen) gerade auf die Eingabe einer PIN verzichtet wird, so daß allein die Karte als Identifikations- und Legitimationsmittel dient, scheint die *konkrete* Betrachtungsweise kriminalpolitisch sachgerecht. Allerdings hatte bereits der Rechtsausschuß des Deutschen Bundestages bei der Verabschiedung des Gesetzes Zweifel, ob die unberechtigte Verwendung ansonsten korrekter Kreditkartendaten unter § 263a I Var. 2 subsumiert werden kann, und daher die Aufnahme einer 3. Variante, die „unbefugte Verwendung von Daten" vorgeschlagen.[15] Nachdem der Gesetzgeber diesem Vorschlag gefolgt ist, liegt die abstrakte Auslegung des Merkmals „Verwendung unrichtiger Daten" näher, so daß die Verwendung von Kreditkartendaten durch einen Unberechtigten die Daten nicht „unrichtig" machen.

c. T könnte sich aber wegen Computerbetrugs gem. **§ 263a I Var. 3** strafbar gemacht haben. Dazu müßte er Daten unbefugt verwendet haben. Die Kreditkartennummer und das Ablaufdatum stellen Daten dar. Diese Daten hat T auch verwendet, da er sie gerade in den Datenverarbeitungsprozeß eingegeben hat. Die Verwendung müßte aber auch **unbefugt** erfolgt sein.

⇨ Nach der am weitesten gehenden sog. **subjektivierenden** Auslegung ist jede Datenverarbeitung „unbefugt", die dem wirklichen oder mutmaßlichen *Willen des Rechtsgutsinhabers* (des Berechtigten) widerspricht.[16] Demzufolge hat T sich nach § 263a I Var. 3 strafbar gemacht, da die Verwendung der Kreditkartendaten nicht dem Willen des K entsprach.

⇨ Vertreter der engen sog. **computerspezifischen** Auslegung stellen darauf ab, ob der einer Datenverwendung entgegenstehende *Wille des Betreibers* im Computerprogramm berücksichtigt ist.[17] Entscheidend ist danach, ob die Befugnis des Verwenders der Daten im Programmablauf Niederschlag gefunden hat, also

[14] *Laue*, JuS **2002**, 359, 362.
[15] Vgl. BT-Drs. 10/5058, S. 30.
[16] So vertreten von BGHSt **40**, 331, 334 f.; BayObLG JR **1994**, 289, 291; *Hilgendorf*, JuS **1997**, 130, 131; *Otto*, BT, § 52 Rn 40; *Scheffler/Dressel*, NJW **2000**, 2645; *Mitsch*, JZ **1994**, 877, 883.
[17] So vertreten von OLG Celle NStZ **1989**, 367, 368; *Arloth*, Jura **1996**, 354, 358; *Achenbach*, Jura **1991**, 227 und JR **1994**, 293, 295.

vom Programm selbst überprüft wird. Diese Überprüfung findet regelmäßig durch eine entsprechende Nachfrage, etwa durch Anforderung und Überprüfung der persönlichen Geheimnummer, der PIN, statt. Da beim beleglosen Zahlungsverkehr allein die Eingabe der Kreditkartendaten genügt, um die Identität des Datenverwenders zu überprüfen, und auch im vorliegenden Fall das Computerprogramm des Providers nicht darauf angelegt ist, die Identität des Datenverwenders etwa durch Anforderung der PIN zu überprüfen, hat T sich nach dieser Auslegung *nicht* nach § 263a I Var. 3 strafbar gemacht.

⇨ Eine vermittelnde Ansicht, die sog. **betrugsspezifische** Auslegung, orientiert sich an § 263 und verlangt ein täuschungsäquivalentes Verhalten des Täters. Entscheidend ist danach, ob die Verwendung der Daten gegenüber einem Menschen als zumindest schlüssige Vorspiegelung der Befugnis zu deuten wäre.[18] Hätte T die Kreditkarte des K behalten und einem anderen als Zahlungsmittel vorgelegt, hätte er damit konkludent behauptet, berechtigter Karteninhaber zu sein. Dann hätte T sich wegen vollendeten oder versuchten Betrugs strafbar gemacht. Folgt man dieser Auffassung, hätte T somit die Kreditkartendaten des K unbefugt verwendet und damit den Tatbestand des § 263a I Var. 3 verwirklicht.

Stellungnahme: Fraglich ist, welcher Auffassung zu folgen ist. Der subjektivierenden Auslegung ist entgegenzuhalten, daß sie das Erfordernis einer einschränkenden Auslegung des § 263a verkennt. Die computerspezifische Auslegung schränkt dagegen die Weite des Tatbestands ein, allerdings zu sehr, so daß kriminologisch nicht hinnehmbare Strafbarkeitslücken entstehen. Die vermittelnde Auffassung, die sog. betrugsspezifische Auslegung, teilt die jeweiligen Schwächen gerade nicht. Durch ihre Anlehnung an § 263 entspricht sie zudem dem Zweck des § 263a, lediglich bestehende Strafbarkeitslücken zu schließen, die darin bestanden, daß bei einer mißbräuchlichen Benutzung von Datenverarbeitungsanlagen ein Betrug ausscheidet. Im Ergebnis ist daher der **betrugsspezifischen Auslegung** zu folgen.

d. Da T auch das **Ergebnis eines Datenverarbeitungsvorgangs beeinflußt** und das **Vermögen** des P in entsprechender Bereicherungsabsicht **beschädigt** hat, hat er sich nach § 263a I Var. 3 strafbar gemacht.

bb. Keine geringere Relevanz erlangt die 3. Variante auch beim sog. **Geldautomatenmißbrauch** mit **Codekarten**, insbesondere von **ec-Codekarten**. Folgende examensrelevante Konstellationen sind zu unterscheiden:

⇨ **Abheben von Geld** am Geldautomaten durch einen **unberechtigten Dritten** (dazu sogleich)

⇨ **Überschreiten** der im Innenverhältnis eingeräumten Macht **eines Dritten**, der zur Abhebung eines bestimmten **Maximalbetrags** beauftragt ist (unten S. 225 ff.)

⇨ **Mißbräuchliches Abheben** von Geld am Geldautomaten durch den (berechtigten) **Karteninhaber** (unten S. 226 ff.)

[18] So vertreten von BGH NJW **2002**, 905, 906; BGHSt **38**, 120, 121; OLG Köln NJW **1992**, 125, 126; OLG Düsseldorf StV **1998**, 266 f.; LG Bonn NJW **1999**, 3726; LK-*Tiedemann*, § 263a Rn 44; SK-*Günther*, § 263a Rn 18; *Tröndle/Fischer*, § 263a Rn 8; *Rengier*, BT I, § 14 Rn 8; *Wessels/Hillenkamp*, BT/2, Rn 609; *Laue*, JuS **2002**, 359, 363; *Tiedemann/Waßmer*, Jura **2000**, 533, 536; *Kudlich*, JuS **2001**, 20, 21; *Jerouschek/Kölbel*, JuS **2001**, 780 f.

a.) Abheben von Geld am Automaten durch einen unberechtigten Dritten

In dieser Konstellation hebt der Täter als **nichtberechtigter** Kartenbesitzer unter Verwendung der **richtigen PIN** und der dazu gehörigen Kontendaten (sog. Quell-Code) entweder mit Hilfe einer im Wege **verbotener Eigenmacht** erlangten Codekarte oder mit einer **kopierten** bzw. **gefälschten Codekarte** Geld von einem Geldautomaten ab.

Beispiel 1[19] (Abheben von Geld durch einen unberechtigten Dritten, der die Codekarte im Wege verbotener Eigenmacht erlangt hat):
Die Haushälterin H entdeckt in der Schublade ihres Geschäftsherrn G eine codierte ec-Karte. Die dazugehörige PIN hatte sie zufällig während eines vor kurzer Zeit stattfindenden Gesprächs des G mit dessen Frau mitbekommen. Sie nimmt die Karte, hebt am nächsten Bankautomaten 200.- € ab und legt die Karte anschließend – wie von Anfang an geplant – wieder zurück.

a. Der objektive Tatbestand des § 242 bezüglich der Karte selbst ist erfüllt (und zwar unabhängig davon, ob die Karte dem G oder der Bank gehört). Es fehlte aber an der Zueignungsabsicht. Zwar handelte H mit Aneignungsabsicht, da sie von der Karte Gebrauch machen und sie diese somit wenigstens vorübergehend eigentümerähnlich dem eigenen Vermögen einverleiben wollte. Es fehlte jedoch am Enteignungselement, da sie die Karte nicht dauerhaft aus der Gewahrsamssphäre des G und aus der Eigentümerposition der Bank herauslösen wollte. Nach der Substanztheorie lag somit kein Diebstahl vor. Fraglich ist, ob sich unter Zugrundelegung der Sachwerttheorie etwas anderes ergeben kann. Im Gegensatz zum Sparbuch (vgl. oben S. XX) gelangt sie nicht als „leere Sachhülse" zurück, da sie lediglich als „Schlüssel" zum ständigen Zugriff auf das Konto dient und sich dadurch nicht verbraucht. Die Karte sollte also ohne Verminderung des in ihr verkörperten Wertes zurückgelangen. Auch nach der Sachwerttheorie lag daher **kein Diebstahl**, sondern nur eine straflose Gebrauchsanmaßung vor.[20]

b. H könnte sich aber wegen **Urkundenunterdrückung** aus § 274 I Nr. 1 und 2 strafbar gemacht haben. Eine ec-Karte enthält in ihrer Funktion als Scheckkarte eine verkörperte Gedankenerklärung, die zum Beweis im Rechtsverkehr geeignet und bestimmt ist und die ihren Aussteller erkennen läßt (§ 274 I Nr. 1). Sie ist mithin als Urkunde zu qualifizieren. Die Verfügungsberechtigung über die Karte lag bei G. Die Karte enthält beweiserhebliche Daten i.S.v. § 202 a II (§ 274 I Nr. 2). H hat diese Urkunde mit den auf ihr vorhandenen Daten unterdrückt, indem sie sie dem Gebrauch des verfügungsberechtigten G entzogen hat. Auch ein nur kurzfristiger Entzug genügt. H handelte in der Absicht, G einen Vermögensschaden, mithin einen Nachteil i.S.d. § 274 zuzufügen. Dieser Nachteil sollte aber *nicht* aus der Vereitelung der Beweisfunktion der Karte entstehen, wie es § 274 I Nr. 1 und 2 verlangen, sondern erst aus einer weiteren (mißbräuchlichen) Nutzung der Karte. Daher ist H nicht wegen Urkundenunterdrückung aus § 274 I Nr. 1 oder 2 strafbar.

c. Dagegen kann eine Bestrafung wegen **Datenveränderung** (§ 303a I Var. 2) bejaht werden. H hat Daten unterdrückt, die ihr nicht zustanden.

d. Ausspähen von Daten (§ 202a) scheidet dagegen aus, da H keine besondere Sicherung überwunden hat. Insbesondere stellt die PIN vorliegend keine beson-

[19] Nach BGHSt **35**, 152 ff.
[20] Wie hier *Eisele/Fad*, Jura **2002**, 305, 306.

dere Sicherung dar, da der T diese bekannt war und es somit nichts zu überwinden gab.

e. Ein **Diebstahl** kommt nicht nur bezüglich der Wegnahme der ec-Karte, sondern auch bezüglich der **Entnahme des Geldes** in Betracht. Da das Geld aber unter der Bedingung einer ordnungsgemäßen Bedienung des Bankautomaten übereignet wurde (§§ 929 S. 1, 158 I BGB) und H den Automaten funktionsgerecht bedient hat, war das Geld bei der Entnahme nicht mehr fremd (a.A. vertretbar).[21]

f. Aus demselben Grund liegt auch eine **Unterschlagung** (§ 246) **nicht** vor.

g. Durch die Entnahme des Geldes kommt auch eine Bestrafung wegen **Betrugs** (§ 263) **nicht** in Betracht, da ein Geldautomat nicht getäuscht werden kann.

h. Der Tatbestand des § 265a ist ebenfalls nicht erfüllt, da das **Erschleichen von Leistungen** eine ordnungswidrige Benutzung des Automaten voraussetzt. H hat den Bankautomaten aber funktionsgerecht bedient. Ihr fehlte lediglich die Befugnis, über das Konto zu verfügen.

i. H könnte sich aber wegen **Computerbetrugs** (§ 263a) strafbar gemacht haben. Als Tatvariante kommt § 263a I Var. 3 (die unbefugte Datenverwendung) in Betracht. Dazu hätte sie die Daten **unbefugt** verwenden müssen. Nach der *betrugsspezifischen* Auslegung[22], die sich an § 263 orientiert und ein täuschungsäquivalentes Verhalten des Täters verlangt, ist entscheidend, ob die Verwendung der Daten gegenüber einem Menschen als zumindest schlüssige Vorspiegelung der Befugnis zu deuten wäre. Dies kann vorliegend ohne weiters angenommen werden. Denn H müßte einem Bankangestellten vorspiegeln, Vollmacht über das Konto des G zu haben. Auch sind ein Vermögensschaden auf Seiten des G sowie die Bereicherungsabsicht auf Seiten der H gegeben. Durch die Verwendung der codierten ec-Karte hat H sich deshalb nach § 263a I Var. 3 strafbar gemacht. Sofern entgegen dieser Lösung der Tatbestand des § 246 bejaht wurde, tritt dieses Delikt subsidiär hinter § 263a zurück. Hätte H hinsichtlich der ec-Karte mit Zueignungsabsicht gehandelt, ist nach Auffassung des BGH mit dem späteren Computerbetrug Tatmehrheit anzunehmen.[23] Da dies vorliegend jedoch nicht der Fall ist, hat sich H also nach § 263a I Var. 3 in Tateinheit mit § 303a I Var. 2 strafbar gemacht.[24]

Beispiel 2[25] (Abheben von Geld durch einen unberechtigten Dritten, der die Codekarte kopiert bzw. gefälscht hat):
T besorgt sich Kartenblankette und macht täuschend echt aussehende ec-Codekarten der B-Bank nach. Die zur Abhebung von Geld aus Geldautomaten er-

[21] Wie hier *Eisele/Fad*, Jura **2002**, 305, 306; *Löhnig*, JR **1999**, 362, 364; *Spahn*, Jura **1989**, 513, 517; *Ennuschat*, StV **1990**, 498; *Wessels/Hillenkamp*, BT/2, Rn 164-176; **anders** BGHSt **35**, 152, 161, nach dessen Auffassung das aus dem Automaten entnommene Geld für den Täter fremd bleibt, weil eine interessengerechte Auslegung der einschlägigen Geschäftsbedingungen ergebe, daß ein konkludentes Übereignungsangebot der Bank nur dann vorliege, wenn der Automat von einem Berechtigten bedient werde. Zu beachten ist jedoch, daß die Entscheidung des BGH zu einer Zeit erging, als es den § 263a noch nicht gab, und der BGH ersichtlich bemüht war, die vorhandene Strafbarkeitslücke zu schließen. Nach Einführung des § 263a am 01.08.1986 ist die (zweifelhafte) Annahme des § 242 nicht mehr erforderlich.

[22] In der Klausur müßte an dieser Stelle der komplette Streitstand dargestellt werden. Um Wiederholungen zu vermeiden, wurde vorliegend lediglich die herrschende betrugsspezifische Auslegung wiedergegeben.

[23] Vgl. BGH NJW **2001**, 1508 f.

[24] So auch *Eisele/Fad*, Jura **2002**, 305, 307.

[25] Nach BGHSt **38**, 120 ff. und *Eisele/Fad*, Jura **2002**, 305, 309.

forderlichen Daten wie die PIN, die Kontendaten und den Quell-Code erlangt er dadurch, daß er im Rahmen seines Einzelhandelsgeschäfts ein Kartenlesegerät zum bargeldlosen Zahlungsverkehr einsetzt und etliche Kunden bei ihm mit ec-Karte bezahlen. Durch Eingabe der PIN, die seinem Kunden O zugeordnet ist, hebt er am Geldautomaten 200.- € ab, die dem Girokonto des O belastet werden.

a. Hinsichtlich der Strafbarkeit kann zunächst auf die Ausführungen zu Beispiel 1 verwiesen werden. T macht sich wegen **Computerbetrugs** gem. § 263a I Var. 3 zum Nachteil der B strafbar.

b. Bezüglich des Herstellens der ec-Karte hat T den objektiven Tatbestand des § 152a I Nr. 1 (**Fälschung von Zahlungskarten**) verwirklicht. Insbesondere ist eine codierte ec-Karte eine Zahlungskarte i.S.d. § 152a, wie § 152a IV klarstellt. Subjektiv müßte T vorsätzlich und zur Täuschung im Rechtsverkehr gehandelt haben. Nach § 270 steht die fälschliche Beeinflussung einer Datenverarbeitung im Rechtsverkehr der Täuschung im Rechtsverkehr gleich, so daß auch das Einsetzen gefälschter Scheckkarten am Geldautomaten erfaßt wird.

c. Da die gefälschte ec-Karte eine verkörperte Gedankenerklärung (die von B eingeräumte ec-Kartenfunktion), die zum Beweis im Rechtsverkehr geeignet und bestimmt war, sowie die Garantiefunktion (B war als Ausstellerin der Karte benannt) enthielt, hat T sich auch wegen **Urkundenfälschung** (§ 267 I Var. 1) strafbar gemacht. Die „Unechtheit" ergibt sich daraus, daß Aussteller in Wirklichkeit nicht B, sondern T war.

d. Schließlich liegt eine Strafbarkeit des T wegen **Fälschung beweiserheblicher Daten** (§ 269 I) vor, weil die auf der gefälschten Karte gespeicherten Daten (insbesondere die PIN, die Kontendaten und der Quell-Code) im Falle ihrer Wahrnehmbarkeit eine unechte Urkunde i.S.d. § 267 darstellen würden.

b.) Überschreiten der im Innenverhältnis eingeräumten Macht eines Dritten, der zur Abhebung eines Maximalbetrags beauftragt ist

Diese Konstellation betrifft den Fall, daß der berechtigte Karteninhaber einem nichtberechtigten Dritten Karte und Geheimnummer (PIN) anvertraut und diesen mit der Abhebung eines bestimmten Betrags beauftragt, der **Beauftragte** jedoch einen **höheren Betrag abhebt** und für sich behält.

Beispiel[26]: O sitzt wegen wiederholten Scheckkartenmißbrauchs im Gefängnis. Um sich bestimmte Privilegien zu verschaffen, benötigt er Bargeld. Daher beauftragt er seinen Freund T, der ihn öfter besuchen kommt, mit der ec-Karte, die sich zu Hause im Schreibtisch befindet, 200.- € von einem Geldautomaten der kartenausstellenden B-Bank abzuholen. Die PIN teilt er ihm auch mit. F hebt jedoch 500.- € ab und behält den Rest für sich.
Unstreitig wäre der beauftragte nichtberechtigte Karteninhaber F straflos, wenn er sich im Rahmen des Auftrags bewegt hätte. Entgegenstehende Vereinbarungen zwischen dem berechtigten Karteninhaber und der kartenausstellenden Bank haben lediglich zivilrechtliche Bedeutung. Vorliegend hat F aber den Rahmen seines Auftrags überschritten.

a. In Betracht kommt zunächst eine Strafbarkeit des F wegen **Untreue** (§ 266). Unabhängig davon, ob man einen Mißbrauchs- oder einen Treubruchstatbestand

[26] Nach OLG Köln NJW **1992**, 125 f.; OLG Düsseldorf, NStZ-RR **1998**, 137; *Eisele/Fad*, Jura **2002**, 305, 310; *Jerouschek/Kölbel*, JuS **2001**, 780 ff.; *Hilgendorf*, JuS **1999**, 542 ff.

annähme, verlangt die zutreffende h.M. für beide Alternativen eine Vermögensbetreuungspflicht desselben Inhalts. Eine solche ist anzunehmen, wenn die Pflicht zur Wahrnehmung fremder Vermögensinteressen den typischen und wesentlichen Inhalt des rechtlich eingeräumten oder faktisch begründeten Treuverhältnisses bildet, diese Pflicht also den Hauptgegenstand des Verhältnisses bildet und eine gewisse Eigenverantwortlichkeit des Täters gegeben ist. Vorliegend sollte F strikt nach den Vorgaben des O handeln. Eine gewisse Eigenverantwortlichkeit wurde ihm nicht eingeräumt.

b. Möglicherweise liegt aber eine Strafbarkeit des T nach § 263a I Var. 3 vor. Das OLG Köln geht auf der Grundlage der betrugsspezifischen Auslegung davon aus, daß T nicht unbefugt handelt. Da T zur Benutzung der Daten – Geheimzahl und auf dem Magnetstreifen gespeicherte Informationen – beauftragt sei, komme seinem Handeln kein Täuschungswert zu. Die bloße Eingabe eines überhöhten Betrags sei keine Verwendung von Daten, da es sich nicht um auf dem Magnetstreifen der Karte gespeicherte Informationen handle.[27] Dieser Auffassung wird in der Literatur mit dem Argument widersprochen, daß in der Überlassung der Karte noch nicht die Ermächtigung zur Abhebung von Geld in beliebiger Höhe gesehen werden könne. O hätte nämlich auch für den Fall des Abhebens des Geldes am Bankschalter dem T eine auf einen bestimmten Geldbetrag beschränkte Vollmacht erteilen können. Grundsätzlich könnten bei der Bestimmung des Umfangs einer Innenvollmacht Inhalt und Zweck des Grundgeschäfts mitberücksichtigt werden. T würde dann den Bankangestellten über das Bestehen einer (unbeschränkten) Vollmacht täuschen. Auf der Grundlage der betrugsspezifischen Auslegung sei daher eine unbefugte Verwendung von Daten und damit eine Strafbarkeit nach § 263a I Var. 3 StGB anzunehmen. Dasselbe gelte, wenn T die Karte absprachewidrig mehrfach verwende, um einen höheren Betrag zu erlangen und die Differenz für sich zu verbrauchen.[28] Schließt man sich dieser Auffassung an, hat T sich nach § 263a I Var. 3 strafbar gemacht.

c. Schließlich ist eine Strafbarkeit nach § 269 StGB wegen Fälschung beweiserheblicher Daten in Erwägung zu ziehen. Durch die Eingabe der PIN und des überhöhten Betrags speichert T Daten, die zum Beweis geeignet und bestimmt sind. Dabei muß es sich – die optische Wahrnehmbarkeit unterstellt – um eine unechte Urkunde handeln. Vorliegend hat es den Anschein, als habe Karteninhaber O die Abhebung vorgenommen. Fraglich ist aber, ob O auch tatsächlicher Aussteller im Sinne der Geistigkeitstheorie ist. Dies wäre der Fall, wenn dem O die Erklärung des T im Wege der Stellvertretung zuzurechnen wäre. Doch eine Stellvertretung müßte nicht nur bestanden haben, sondern auch rechtlich zulässig gewesen sein. In diesem Zusammenhang ist zu beachten, daß die Allgemeinen Geschäftsbedingungen der Kreditinstitute vorschreiben, daß die PIN niemandem gegenüber bekannt gegeben werden darf, so daß eine wirksame Stellvertretung ausgeschlossen ist. Kann damit das Handeln des T dem O nicht zugerechnet werden, erscheint T als Aussteller der Urkunde. Aufgrund der damit vorliegenden Täuschung über die Identität ist die Urkunde – würde man diese wahrnehmen können – unecht, so daß T sich auch nach § 269 StGB strafbar gemacht hat.

[27] OLG Köln NJW **1992**, 125 f.; OLG Düsseldorf, NStZ-RR **1998**, 137; LK-*Tiedemann*, § 263a Rn 50.
[28] *Eisele/Fad*, Jura **2002**, 305, 310; *Lackner/Kühl*, § 263a Rn 14; *Hilgendorf*, JuS **1999**, 542, 544.

c.) Mißbräuchliches Abheben von Geld am Geldautomaten durch den berechtigten Karteninhaber

Von den unter a.) und b.) behandelten mißbräuchlichen Abhebungen durch einen (nichtberechtigten) Dritten ist der **Mißbrauch** durch den **berechtigten Karteninhaber** zu unterscheiden. Für die Lösung derartiger Fälle ist entscheidend zu wissen, daß trotz der am 01.01.2002 weggefallenen Scheckgarantie, wonach bis zu einer Höhe von 400.- DM die Einlösung eines Euroschecks auch bei nicht vorhandener Kontodeckung garantiert wurde, die ec-Karte ihre Bedeutung *nicht* verloren hat. Denn die Euroscheckkarte gilt nunmehr als „**Maestro-Karte**" in ihrer Funktion als **Codekarte** fort[29]: Die auf ihr gespeicherten Daten gelten zusammen mit der PIN als **Zugangsschlüssel zum eigenen Girokonto**. Strafbarkeitsfragen bestehen also immer dann, wenn der berechtigte Karteninhaber Geld am Geldautomaten abhebt, obwohl sein Girokonto nicht die nötige Deckung aufweist. Die Beantwortung dieser Fragen wird erleichtert, wenn man die rechtlichen Rahmenbedingungen über das ec-Geldautomatensystem kennt: Nach den Vereinbarungen der Kreditinstitute über das deutsche ec-Geldautomatensystem zieht das automatenbetreibende Kreditinstitut den von seinem Geldautomaten ausgezahlten Betrag bei institutsübergreifenden Verfügungen beleglos per Lastschrift bei dem kartenausgebenden Kreditinstitut ein; eine Rückgabe der Lastschrift wegen fehlender Deckung oder wegen Widerspruchs des Kontoinhabers ist unter den beteiligten Kreditinstituten abbedungen. Hebt also ein ec-Karteninhaber, dessen Konto bereits überzogen ist, mit seiner ec-Karte unter Eingabe der PIN Geld am Automaten eines fremden Kreditinstituts ab, liegt der Schaden stets beim kartenausgebenden Kreditinstitut.

> **Beispiel[30]:** Der vermögenslose T ist wieder einmal knapp bei Kasse. Sein Girokonto bei der B-Bank ist bis zur eingeräumten Kreditlinie überzogen. Wie er es jemals schaffen soll, das Konto auszugleichen, ist ihm völlig schleierhaft. Da er aber dennoch Geld benötigt, hebt er mit seiner (noch nicht gesperrten) ec-Karte Geld am Automaten der C-Bank ab. Hat T sich dadurch strafbar gemacht?
>
> **1. Strafbarkeit des T nach § 263a I Var. 3**
> Durch das Abheben des Geldes könnte T sich wegen **Computerbetrugs** gem. § 263a I Var. 3 strafbar gemacht haben. Dazu müßte er Daten unbefugt verwendet haben.
> T hat die auf dem Magnetstreifen der ec-Karte gespeicherten Daten (Kontonummer, Bankleitzahl, Quell-Code usw.) durch Eingabe in den Geldautomaten „verwendet". Fraglich ist aber, ob er dabei **„unbefugt"** gehandelt hat.
>
> ⇨ Nach der am weitesten gehenden sog. **subjektivierenden** Auslegung ist jede Datenverarbeitung „unbefugt", die dem wirklichen oder mutmaßlichen *Willen des Rechtsgutsinhabers* (des Berechtigten) widerspricht.[31] Demzufolge hat T sich nach § 263a I Var. 3 strafbar gemacht, da die Verwendung der ec-Kartendaten nicht dem Willen des Automatenbetreibers C entsprach.
>
> ⇨ Vertreter der engen sog. **computerspezifischen** Auslegung stellen darauf ab, ob der einer Datenverwendung entgegenstehende *Wille des Betreibers* im Com-

[29] Dies verkennt *Rengier*, BT I, § 19 Rn 1, wenn er konstatiert, § 266b I Var. 1 habe seit dem 01.01.2002 keine Bedeutung mehr. Wie hier BGH NJW **2002**, 905, 906.
[30] Nach BGH NJW **2002**, 905 ff.
[31] So vertreten von BGHSt **40**, 331, 334 f.; BayObLG JR **1994**, 289, 291; *Hilgendorf*, JuS **1997**, 130, 131; *Otto*, BT, § 52 Rn 40; *Scheffler/Dressel*, NJW **2000**, 2645; *Mitsch*, JZ **1994**, 877, 883.

puterprogramm berücksichtigt ist.[32] Entscheidend ist danach, ob die Befugnis des Verwenders der Daten im Programmablauf Niederschlag gefunden hat, also vom Programm selbst überprüft wird. Diese Überprüfung findet regelmäßig durch eine entsprechende Anfrage, etwa durch Anforderung und Überprüfung der persönlichen Geheimnummer, der PIN, statt. Da T diese ordnungsgemäß eingegeben hat, ist er auch nach dieser Auslegung nicht wegen unbefugter Verwendung von Daten strafbar.

⇨ Die herrschende Auffassung, die sog. **betrugsspezifische** Auslegung, orientiert sich an § 263 und verlangt ein täuschungsäquivalentes Verhalten des Täters.[33] Durch ihre Anlehnung an § 263 entspricht sie dem Zweck des § 263a, nämlich lediglich bestehende Strafbarkeitslücken zu schließen, die darin bestanden, daß bei einer mißbräuchlichen Benutzung von Datenverarbeitungsanlagen ein Betrug ausscheidet. Ihr ist daher zu folgen. Ob die Verwendung von Daten durch einen berechtigten Karteninhaber (Kontoinhaber), der – wie hier – Geld am Bankautomaten in der Absicht abhebt, einen ihm damit gewährten Kredit nicht zurückzuzahlen, täuschungsähnlich ist, hängt damit davon ab, ob ein entsprechendes Verhalten gegenüber einem Menschen als schlüssige Vorspiegelung einer Befugnis und damit als Täuschungshandlung i.S.v. § 263 StGB einzustufen ist.

  ⇨ Geht man mit der **h.L.** davon aus, daß ein zahlungsunfähiger bzw. -unwilliger Täter beim Abheben von Geld am Bankschalter einem fiktiven Bankangestellten schlüssig vorspiegelt, sein Konto sei gedeckt oder ein Überziehungskredit werde von ihm zurückgezahlt, ist das Abheben von Geld am Geldautomaten als betrugsähnlich anzusehen.[34]

  ⇨ Der **BGH** hat jüngst anders entschieden. Nach seiner Ansicht wird zur Begründung der Täuschungsqualität der Abhebung am Geldautomaten zwar auf einen fiktiven Bankangestellten abgestellt, der die Interessen der Bank umfassend wahrzunehmen hat, zu Recht werde aber auch darauf hingewiesen, daß eine Vergleichbarkeit nur mit einem Schalterangestellten angenommen werden könne, der sich mit den Fragen befaßt, die auch der Computer prüft.[35] Der Computer prüfe aber nicht die Bonität des berechtigten Karteninhabers, sondern lediglich, ob sich dieser im Rahmen des Verfügungsrahmens bewege. Für die Verneinung des § 263a I Var. 3 spreche zudem, daß der Gesetzgeber durch das 2. WiKG vom 15.5.1986 zugleich mit § 263a StGB auch § 266b StGB eingeführt hat. Diese Vorschrift stelle ein auf den berechtigten Karteninhaber beschränktes Sonderdelikt dar, das die vertragswidrige Bargeldbeschaffung mit einer gegenüber §§ 263, 263a geringeren Strafe bedrohe. § 266b gehe daher auch als lex specialis dem nach der bisherigen Rechtsprechung beim Einsatz einer ec-Karte als Scheckkarte im eigentlichen Sinne verwirklichten § 263 vor. Erfaßte man den Mißbrauch der

[32] So vertreten von OLG Celle NStZ **1989**, 367, 368; *Arloth*, Jura **1996**, 354, 358; *Achenbach*, Jura **1991**, 227 f. und JR **1994**, 293, 295.
[33] So vertreten von BGH NJW **2002**, 905, 906; BGHSt **38**, 120, 121; OLG Köln NJW **1992**, 125, 126; OLG Düsseldorf StV **1998**, 266 f.; LG Bonn NJW **1999**, 3726; LK-*Tiedemann*, § 263a Rn 44; SK-*Günther*, § 263a Rn 18; *Tröndle/Fischer*, § 263a Rn 8; *Rengier*, BT I, § 14 Rn 8; *Wessels/Hillenkamp*, BT/2, Rn 609; *Laue*, JuS **2002**, 359, 363; *Tiedemann/Waßmer*, Jura **2000**, 533, 536; *Kudlich*, JuS **2001**, 20, 21; *Jerouschek/Kölbel*, JuS **2001**, 780 f.
[34] So *Lackner/Kühl* § 263 a Rn 14; *Tröndle/Fischer*, § 263 a Rn 8 a; LK-*Tiedemann*, § 263a Rn 51; *Rengier*, BT I, § 14 Rn 12; *Eisele/Fad*, Jura **2002**, 305, 311. **Anders** SK-*Günther*, § 263a Rn 19; *Zielinski*, CR **1992**, 223, 227; *Hilgendorf*, JuS **1997**, 130, 135 f.
[35] BGH NJW **2002**, 905, 906 unter Bezugnahme auf *Altenhain*, JZ **1997**, 752, 758.

Scheckkarte als Codekarte am Geldautomaten durch ihren berechtigten Inhaber als Computerbetrug nach § 263a, führe dies zu erheblichen Wertungswidersprüchen im Hinblick auf die unterschiedlichen Strafrahmen von § 263a und § 266b und die fehlende Versuchsstrafbarkeit bei § 266b.

Folgt man dieser Auffassung, war T trotz seiner betrügerischen Absicht berechtigter Karteninhaber und zum Einsatz der ec-Karte an Geldautomaten befugt. Er hat seine Befugnis somit nicht täuschungsähnlich vorgespiegelt und daher nicht „unbefugt" i.S.v. § 263a I Var. 3 gehandelt. Ein **Computerbetrug scheidet aus**.

2. Strafbarkeit des T nach § 266b I Var. 1

Möglicherweise hat T sich aber durch den Einsatz der ec-Karte zur Bargeldbeschaffung am Bankautomaten wegen **Mißbrauchs von Scheckkarten** nach § 266b I Var. 1 strafbar gemacht.

T war tauglicher Täter, da ihm durch die Überlassung der ec-Karte die Möglichkeit eingeräumt worden war, die ausstellende B-Bank zu einer Zahlung zu veranlassen. Auch hat er die ihm überlassene ec-Karte i.S.v. § 266b I Var. 1 „mißbraucht", da er die B-Bank im Außenverhältnis zu Dritten (hier der C-Bank) wirksam, im Innenverhältnis jedoch pflichtwidrig zu einer Zahlung veranlaßt hat.

Fraglich ist allerdings, wie es sich auswirkt, daß T seine ec-Karte nicht als Scheckkarte, sondern als Codekarte zur Bedienung von Geldautomaten eingesetzt hat, § 266b I Var. 1 jedoch von „Scheckkarte" und nicht von „Codekarte" spricht.

⇨ Teilweise wird angenommen, § 266b I Var. 1 habe seit dem 01.01.2002 keine Bedeutung mehr, weil mit diesem Tage die Zahlungsgarantie entfallen sei, die bis dahin die Banken bei der Bezahlung mittels Euroscheck und Scheckkarte übernommen hatten. Habe die „Scheckkarte" ihre Funktion verloren, könne es auch den „Scheckkartenmißbrauch" nicht mehr geben. Unerheblich sei, daß die ec-Karte mit ihren – „zufällig" vorhandenen – anderen Zahlungsfunktionen vorläufig – bis zur Einführung der geplanten „Maestro-Karte – erhalten bleibe.[36]

⇨ Dieser Auffassung sind mehrere Argumente entgegenzuhalten: Erstens ist die mit der ec-Karte verbundene Einsatzmöglichkeit als Codekarte keineswegs „zufällig", sondern von den kartenausstellenden Kreditinstituten schon seit langem gewollt, um Schalterpersonal für Barauszahlungen einzusparen.[37] Zweitens setzt sie sich nicht mit dem dieser Konstellation zugrundeliegenden Urteil des BGH vom 21.11.2001 auseinander. Drittens kann sie auch in der Sache nicht überzeugen: Die Verwendung der ec-Karte zur Barabhebung am Geldautomaten einer Drittbank ist mit der (nun weggefallenen) Bareinlösung eines Euroschecks bei anderen Kreditinstituten sehr wohl vergleichbar. Zwar wird die ec-Karte nun nicht mehr als Scheckkarte, sondern nur noch in ihrer Funktion als Codekarte, quasi als „Zugangsschlüssel" zum Abheben von Geld aus Geldautomaten, eingesetzt, diese jetzt alleinige Funktion der ec-Karte steht aber der Anwendung des § 266b nicht zwingend entgegen. Zwar ist richtig, daß die Zahlungsverpflichtung der kartenausstellenden Bank (vorliegend die B-Bank) gegenüber der Drittbank (vorliegend der C-Bank) nun nicht mehr aus der Garantiefunktion der ec-Karte folgt, allerdings ist eine Gleichbehandlung mit der Bareinlösung eines Euroschecks bei einem anderen als dem bezogenen Kreditinstitut schon deshalb

[36] *Rengier*, BT I, § 19 Rn 1.

[37] Insoweit klarstellend BGH NJW **2002**, 905, 906. Gegen die Annahme, die mit der ec-Karte verbundene Einsatzmöglichkeit als Codekarte sei „zufällig", spricht zudem der Umstand, daß „ec" nicht etwa für „eurocheque", sondern für „electronic cash" steht. Allein diese Bezeichnung bringt zum Ausdruck, daß die ec-Karte *bestimmungsgemäß* einen Schlüssel zum eigenen Girokonto darstellt.

gerechtfertigt, weil auch in diesen Fällen das kartenausgebende Institut i.S.v. § 266b zu einer Zahlung „veranlaßt" wird. Die Zahlungsverpflichtung des kartenausgebenden Kreditinstitut ergibt sich dabei aus den bereits genannten Vereinbarungen der Kreditinstitute über das deutsche ec-Geldautomatensystem zur Rückzahlung des vom Geldautomaten ausgezahlten Betrags verpflichtet; eine Rückgabe der Lastschrift wegen fehlender Deckung oder wegen Widerspruchs des Kontoinhabers ist unter den beteiligten Kreditinstituten abbedungen. Damit erlangt das automatenbetreibende Kreditinstitut gegenüber dem kartenausstellenden Kreditinstitut einen schuldrechtlichen Anspruch, der dem aus einem Garantievertrag vergleichbar ist. Hebt also ein ec-Karteninhaber, dessen Konto bereits überzogen ist, mit seiner ec-Karte unter Eingabe der PIN Geld am Automaten eines fremden Kreditinstituts ab, liegt ein Fall des § 266b I Var. 1 vor.[38]

Ergebnis: Nachdem T durch seine Geldabhebung an einem kreditinstitutsfremden Geldautomaten die kartenausstellende B-Bank auch dadurch „geschädigt" hat, daß deren Ersatzansprüche gegen den vermögenslosen T wirtschaftlich wertlos sind, hat er sich wegen Scheckkartenmißbrauchs gem. § 266b I Var. 1 strafbar gemacht. Hinsichtlich der (nicht verwirklichten) §§ 242, 246 und 265a ergeben sich keine Abweichungen zu den Fällen, in denen ein nichtberechtigter Dritter Geld abhebt.

Weiterführender Hinweis: Anders wäre der Fall zu entscheiden gewesen, wenn T ausschließlich Geld an Automaten der **kartenausstellenden** B-Bank abgehoben hätte. Denn nach zutreffender h.M.[39] ist § 266b nur auf Karten im sog. **Drei-Partner-System** (Visacard, Eurocard, Barclaycard, American-Express, Diners usw.), nicht auf Karten im Zwei-Partner-System (sog. Kundenkarten wie IKEA-Family-Card, Lufthansa Air-Plus-Karte usw.) anwendbar (dazu näher unten S. 239 ff.). Allein der Wortlaut des § 266b, der die Veranlassung zu einer „Zahlung" verlangt, spricht für diese Auslegung. Hebt nun der berechtigte ec-Karteninhaber Geld von einem Automaten *des* Kreditinstituts ab, das die Karte selbst ausgestellt hat, verwendet er die Karte – wie von der Bank in diesem Fall gewollt – lediglich zur technischen Erleichterung des Auszahlungsvorgangs, ohne daß eine Zahlungsverpflichtung des Kreditinstituts gegenüber einer anderen Bank entstünde. T wäre also **straflos** geblieben.[40]

Zusammenfassung (Leitsätze des BGH NJW 2002, 905):

1. Der berechtigte Inhaber einer Scheckkarte, der unter Verwendung der Karte und der persönlichen Geheimzahl (PIN) an einem Geldautomaten Bargeld abhebt, ohne zum Ausgleich des erlangten Betrags willens oder in der Lage zu sein, macht sich nicht nach § 263a StGB strafbar.

2. § 266b StGB erfaßt auch die mißbräuchliche Verwendung einer Scheckkarte als Codekarte zur Abhebung an Geldautomaten durch den berechtigten Karteninhaber; dies gilt jedoch nicht bei Abhebungen an Automaten des Kreditinstituts, das die Karte selbst ausgegeben hat.

[38] BGH NJW **2002**, 905, 907.

[39] BGH NJW **2002**, 905, 907; BGHSt **38**, 281, 282; Sch/Sch-*Lenckner/Perron*, § 266b Rn 5; SK-*Samson/Günther*, § 266b Rn 4; LK-*Gribbohm*, § 266b Rn 18 f.; *Lackner/Kühl*, § 266b Rn 4; *Tröndle/Fischer*, § 266b Rn 5; *Zielinski*, CR **1992**, 223, 227; *Eisele/Fad*, Jura **2002**, 305, 311; *Wessels/Hillenkamp*, BT/2, Rn 795. **Anders** *Hilgendorf*, JuS **1997**, 131, 134 f.; *Otto*, JZ **1992**, 1139; *Ranft*, NStZ **1993**, 185 f. (Erstreckung des § 266b auch auf Karten im Zwei-Partner-System).

[40] So ausdrücklich BGH NJW **2002**, 905, 908.

cc. Verwendung einer eigenen oder fremden ec-Karte im electronic-cash-Verfahren (point-of-sale-Verfahren) ⇒ 1. Variante des bargeldlosen Einkaufens mit ec-Karte

Das electronic-cash-Verfahren oder point-of-sale-Verfahren (POS) ermöglicht eine bargeldlose Bezahlung ohne Verwendung von Scheckformularen. Der Kunde steckt seine Karte in das Kartenlesegerät am Terminal der Kasse des Händlers und gibt seine PIN ein. Wie bei dem Bezahlen mit Kreditkarten des Drei-Partner-Systems erhält der Händler aufgrund eines Händlervertrags zwischen ihm und dem Kreditinstitut einen direkten Anspruch gegen das kartenausstellende Kreditinstitut. Die am Terminal eingelesenen Daten und die PIN werden online an eine Autorisierungszentrale bzw. an das jeweilige Kreditinstitut weitergeleitet. Dort werden die PIN und der Verfügungsrahmen des Kunden sowie eine eventuelle Sperrung der Karte überprüft. Ist das Ergebnis der Prüfung positiv, wird die Zustimmung des kartenausgebenden Kreditinstituts zu der Transaktion (sog. Autorisierung) dem Vertragsunternehmen online mitgeteilt. Zwischen dem Kreditinstitut und dem Karteninhaber besteht – neben dem Girovertrag – ein Geschäftsbesorgungsvertrag (§§ 675, 631 BGB), der die Teilnahme des Karteninhabers am electronic-cash-Verfahren regelt.[41]

Auch beim POS sind Straftaten denkbar. Hier sind zwei Konstellation zu unterscheiden: In der ersten setzt der berechtigte Inhaber einer ec-Karte diese trotz überschrittener Kreditlinie im electronic-cash-Verfahren zur Bezahlung von Waren ein, in der zweiten geschieht dies durch einen nichtberechtigten Dritten.

> **Beispiel 1 (Einsatz der ec-Karte durch den berechtigten Karteninhaber):**
> K bezahlt bei V Waren im electronic-cash-Verfahren, obwohl er den Kreditrahmen, den er von seiner kartenausstellenden B-Bank eingeräumt bekommen hat, bereits ausgeschöpft hat.
> Eine Strafbarkeit wegen Betrugs (**§ 263**) kommt bei der Bezahlung im electronic-cash-Verfahren regelmäßig nicht in Betracht, weil sich der Händler aufgrund der mit der Online-Autorisierung verbundenen Garantiefunktion keine Gedanken über die Zahlungsfähigkeit machen muß und daher keinem Irrtum unterliegen kann.
> Auch eine Strafbarkeit nach **§ 266b** scheidet aus, weil K nicht die Möglichkeit besaß, die B-Bank zu einer Auszahlung zu veranlassen. Das „Veranlassen" ist bei § 266b nämlich im Sinne von „Verpflichten" zu verstehen. Beim Einsatz im electronic-cash-Verfahren verpflichtet aber nicht der Karteninhaber das Kreditinstitut im Wege der Stellvertretung, sondern das Kreditinstitut verpflichtet sich letztlich durch die elektronische Autorisation selbst.
> Schließlich kommt eine Strafbarkeit nach **§ 263a I Var. 3** in Betracht. Möchte der berechtigte Inhaber einer ec-Karte trotz überschrittener Kreditlinie mit seiner ec-Karte bargeldlos bezahlen und hat sein Kreditinstitut der Autorisierungszentrale mitgeteilt, es wünsche keine weitere Belastung des Girokontos, wird das Ergebnis der Online-Anfrage negativ sein. Die Bezahlung ist fehlgeschlagen. Möglich ist dann eine Strafbarkeit wegen Versuchs. Wie schon beim Abheben am Bankautomaten kommt es hier darauf an, ob T die Karte unbefugt verwendete, was nach h.L. bei Überschreiten der eingeräumten Kreditlinie zu bejahen ist. Überträgt man jedoch die Rechtsprechung des BGH zum mißbräuchlichen Abheben von Geld aus Geldautomaten durch den berechtigten Karteninhaber, ist auch beim mißbräuchlichen

[41] *Eisele/Fad*, Jura **2002**, 305; *Joecks*, § 263a Rn 25.

Verwenden der eigenen ec-Karte im electronic-cash-Verfahren nicht § 263a Var. 3, sondern § 266b I Var. 1 einschlägig.

Beispiel 2 (Einsatz der ec-Karte durch einen nichtberechtigten Dritten):
Die Haushälterin H entdeckt in der Schublade ihrer Geschäftsherrin G deren codierte ec-Karte. Die dazugehörige PIN hat sie vor einiger Zeit bei einem Gespräch zwischen der G und deren Mann mitbekommen. Sie nimmt die Karte, setzt diese im electronic-cash-Verfahren zur Bezahlung von Waren in einer Boutique ein und legt die Karte anschließend – wie von Anfang an geplant – wieder an ihren Platz zurück.
Ein Diebstahl (**§ 242**) scheitert an der Enteignungskomponente des Zueignungsvorsatzes.
Auch ein Betrug (**§ 263**) zum Nachteil der kartenausstellenden Bank liegt im Ergebnis nicht vor. Zwar hat H durch Vorlage der Karte darüber getäuscht, daß sie zur Teilnahme am electronic-cash-Verfahren berechtigt ist, da sich der Händler aufgrund der mit der Online-Autorisierung verbundenen Garantiefunktion jedoch keine Gedanken über die Berechtigung des ec-Kartenbenutzers zu machen braucht, kann er auch keinem Irrtum unterliegen.
H könnte sich aber wegen Computerbetrugs nach **§ 263a I Var. 3** zum Nachteil der Bank strafbar gemacht haben. Indem sie die ec-Karte nebst PIN in das Händlerterminal eingab, beeinflußte sie das Ergebnis der Datenverarbeitung des Computers der Autorisierungszentrale, wodurch die Bank einen Schaden erlitt. Daß Geschädigter (die Bank) und der Verfügende (das Kassenpersonal der Boutique) nicht personenidentisch sind, ist belanglos, da zwischen den Beteiligten eine vertraglich begründete Nähebeziehung besteht. Insoweit gelten nach h.M. die zu § 263 entwickelten Grundsätze. Diesbezüglich handelte H somit unbefugt. Hinsichtlich der subjektiv neben dem Tatbestandsvorsatz erforderlichen Bereicherungsabsicht muß – ebenso wie beim Betrug – Stoffgleichheit zwischen dem erstrebten Vermögensvorteil und dem Vermögensschaden bestehen. Voraussetzung für die Stoffgleichheit ist, daß Vermögensschaden und Vermögensvorteil auf derselben Vermögensverfügung beruhen und daß der Vorteil aus dem geschädigten Vermögen stammt. Dies ist hier der Fall: Der erstrebte Vermögensvorteil liegt in der Übereignung der Waren bzw. der Befreiung von der Pflicht zur Barzahlung, der Vermögensschaden in der Belastung der kartenausgebenden Bank mit einem entsprechenden Zahlungsanspruch des Händlers.[42]

dd. Verwendung einer eigenen oder fremden ec-Karte im elektronischen Lastschriftverfahren ⇒ 2. Variante des bargeldlosen Einkaufens mit ec-Karte

Auch beim elektronischen Lastschriftverfahren führt der Kunde seine Karte in das Händlerterminal ein. Im Gegensatz zu dem eben dargestellten POS-System gibt der Kunde aber nicht zusätzlich seine PIN ein, sondern unterschreibt (lediglich) eine Ermächtigung zum Lastschrifteinzug. Dadurch kann auch keine Online-Anfrage stattfinden, was wiederum zur Folge hat, daß in Ermangelung eines Garantievertrags ein eigener Anspruch des Händlers gegen das Kreditinstitut nicht besteht. Freilich führt dies zu einem Verlust an Sicherheit. Gleichwohl ist das elektronische Lastschriftverfahren in der Praxis nicht unüblich, da *die Händler* die Kosten für die Onlineabfrage des electronic-cash-Verfahrens zu tragen haben und diese Kosten beim elektronischen Lastschriftverfahren naturgemäß nicht auftreten. Wegen dieser Kostenerspar-

[42] *Eisele/Fad*, Jura **2002**, 305, 308.

nis verzichten viele Händler auf die Sicherheiten, die das electronic-cash-Verfahren bietet.[43] Hinsichtlich möglicher Straftaten ist auch hier zu unterscheiden:

Beispiel 1 (Einsatz der ec-Karte durch den berechtigten Karteninhaber):
X bezahlt bei V Waren im elektronischen Lastschriftverfahren, obwohl er den Kreditrahmen, den er von seiner kartenausstellenden B-Bank eingeräumt bekommen hat, bereits ausgeschöpft hat.
Wird die ec-Karte vom berechtigten Karteninhaber im elektronischen Lastschriftverfahren verwendet, macht er sich wegen Betrugs (**§ 263**) zum Nachteil des Händlers strafbar, da er ihn über die Deckung seines Kontos täuscht. Im Gegensatz zum electronic-cash-Verfahren unterliegt der Händler einem Irrtum, da die kartenausstellende Bank keine Zahlung garantiert. Mit der Übereignung der Waren trifft er auch eine Vermögensverfügung. Einen Vermögensschaden erleidet er dann, wenn sich die Bank mangels Garantieübernahme weigert, die Zahlung vorzunehmen.

Beispiel 2 (Einsatz der ec-Karte durch einen nichtberechtigten Dritten):
Die Haushälterin H geht wie beim letzten Mal vor. Doch da die Boutique nicht am POS-Verfahren, sondern lediglich am elektronischen Lastschriftverfahren teilnimmt, kommt sie nur dadurch zu der Ware, daß sie auf dem Abrechungsbeleg mit G unterzeichnet.
Durch das Unterschreiben des Abrechungsbelegs mit dem Namen der G hat H sich zunächst wegen Urkundenfälschung (**§ 267 I Var. 1 und Var. 3**) strafbar gemacht.
Darüber hinaus hat H den Tatbestand des Betrugs (**§ 263**) zum Nachteil des Boutiqueinhabers verwirklicht. Sie hat diesen bzw. dessen Kassenpersonal über das wirksame Zustandekommen einer Abbuchungsermächtigung zu Lasten der G getäuscht. Diese besteht in Wirklichkeit nicht, da H die G nicht rechtlich bindend verpflichten kann. Auch hat sie beim Kassenpersonal einen Irrtum erregt, da sich dieses aufgrund des Nichtbestehens einer Garantieerklärung sehr wohl Gedanken über die Berechtigung bzw. Zahlungsfähigkeit macht. Hinsichtlich der Vermögensverfügung (die Übergabe und Übereignung der Waren) schadet es wegen der Regelung des § 56 HGB nicht, falls der Boutiqueinhaber nicht selbst an der Kasse gestanden haben sollte. Schließlich erleidet der Boutiqueinhaber auch einen Vermögensschaden, da er im elektronischen Lastschriftverfahren mangels Garantievertrages keinen Anspruch gegen die kartenausstellende Bank besitzt.

ee. Verwendung einer fremden ec-Karte als Geldkarte ⇒ 3. Variante des bargeldlosen Einkaufens mit ec-Karte

Seit einiger Zeit sind ec-Karten mit einem Chip versehen, mit dessen Hilfe die Karte an einem Terminal der kartenausstellenden Bank „aufgeladen" werden kann (meist bis zu einem Wert von 50.- €). Mit dem dann auf der Karte befindlichen Guthaben kann der Karteninhaber – ähnlich einer Telefonkarte – die Karte zur unmittelbaren Bezahlung kleinerer Beträge (beim Bäcker, Blumenladen, Kiosk etc.) einsetzen. Dazu steckt er die Karte in einen Terminal des Händlers, wodurch der geschuldete Betrag vom Kartenguthaben abgezogen wird (ähnlich dem „Abtelefonieren" von Telefonkarten). Die unbefugte Entladung durch einen nichtberechtigten Dritten ist Computerbetrug (§ 263a I Var. 3) zu Lasten des Karteninhabers.[44]

[43] *Eisele/Fad*, Jura **2002**, 305; LK-*Tiedemann*, § 263a Rn 53.
[44] Vgl. dazu LK-*Tiedemann*, § 263a Rn 54.

d. Sonstige unbefugte Einwirkung auf den Ablauf (§ 263a I Var. 4)

Die letzte Tatvariante des § 263a I – die sonstige unbefugte Einwirkung auf den Ablauf – soll nach Auffassung des Gesetzgebers als **Auffangtatbestand** fungieren und die noch verbleibenden, von den anderen Tatvarianten nicht gedeckten Manipulationen erfassen. Die Reichweite der 4. Variante hängt also maßgeblich davon ab, wie viele der denkbaren Computerdelikte man bereits unter die ersten drei Varianten (insbesondere unter die 3. Variante) subsumieren konnte. Dies wiederum hängt davon ab, ob man für die „Verwendung von Daten" i.S. der 2. und 3. Variante mit der zutreffenden h.M. eine Eingabe in den Datenverarbeitungsprozeß voraussetzt oder jede Nutzung von Daten genügen läßt. Folgt man der h.M., kann das **Leerspielen von Geldspielautomaten** allein unter die 4. Variante fallen.

Beispiel (zugleich Abschlußfall zu § 263a): T verschafft sich durch das Kopieren einer Diskette die erforderlichen Informationen über den Programmablauf (insbesondere über die sog. Risikotaste) eines bestimmten **Geldspielautomaten**. Mit diesem Wissen gelingt es ihm, das Gerät so zu bedienen, daß er es „leerspielt". Ist T strafbar ?

1. Durch die Entgegennahme des ausgeworfenen Geldes könnte T sich zunächst wegen **Diebstahls** (§ 242 I) strafbar gemacht haben. Dazu hätte es sich bei dem Geld zunächst um eine fremde bewegliche Sache handeln müssen. Zweifelhaft ist allein das Merkmal *fremd*. Für den Täter ist die Sache fremd, wenn sie nicht in dessen Alleineigentum steht. Folglich ist die Frage zu beantworten, in wessen Eigentum die Münzen standen, als T sie entgegennahm. Sie standen im Eigentum des T, wenn sie ihm wirksam übereignet wurden (§ 929 S. 1 BGB). Im Grundsatz ist davon auszugehen, daß ein genereller Eigentumsübertragungswille des Automatenbetreibers hinsichtlich des ausgeworfenen Geldes besteht. Etwas anderes könnte jedoch im Hinblick darauf gelten, daß T den Automaten mit Hilfe seiner „Spezialkenntnisse" bediente. Der generelle Eigentumsübertragungswille könnte unter dem Vorbehalt der ordnungsmäßigen Bedienung bestehen. Ein solcher Vorbehalt ist jedoch vorliegend objektiv nicht erkennbar. Ein (geheimer) subjektiver Vorbehalt des Betreibers kann nicht genügen. Aber selbst wenn man davon ausgeht, daß der Betreiber eines Geldspielautomaten nur dann mit der Übergabe und Übereignung der in dem Gerät befindlichen und in seinem Eigentum und Gewahrsam stehenden Geldstücken an den Bediener einverstanden ist, wenn dieser den Automaten ordnungsgemäß betätigt, ist dies für den vorliegenden Fall doch anzunehmen. T hat den Automaten äußerlich vollkommen ordnungsgemäß bedient. Daher ist in jedem Fall von einer wirksamen Eigentumsübertragung des Geldes auszugehen. Ein Diebstahl scheidet demnach mangels Fremdheit des Geldes aus.

2. T könnte sich aber wegen **Erschleichens von Leistungen** (§ 265a) strafbar gemacht haben. Bei dem Geldspielautomaten handelt es sich um einen Automaten i.S.d. § 265a I Var. 1. Fraglich ist aber, ob T die Leistung „erschlichen" hat. Darunter wird überwiegend ein ordnungswidriges oder zumindest mißbräuchliches Erreichen einer Leistung verstanden, und zwar durch den *Bedienungsvorgang* der technischen Vorrichtung selbst.[45] T hat den Geldspielautomaten aber äußerlich völlig korrekt bedient. T hat somit die Leistung des Automaten nicht „erschlichen". Darüber hinaus hat T den subjektiven Tatbestand nicht erfüllt, weil dazu die Absicht, das Entgelt nicht zu entrichten vorausgesetzt wird. T ging es aber nicht darum, das Spielentgelt nicht zu entrichten, sondern den

[45] Vgl. dazu Sch/Sch-*Lenckner/Perron*, § 265a Rn 8-11; LK-*Tiedemann*, § 265a Rn 34-57; *Tröndle/Fischer*, § 265a Rn 3; *Lackner/Kühl*, § 265a Rn 6; *Hellmann*, JuS **2001**, 353, 356; *Jerouschek/Kölbel*, JuS **2001**, 780, 784.

Automaten leerzuspielen. Er hat sich somit auch deshalb nicht aus § 265a I Var. 1 strafbar gemacht.

3. Schließlich kommt eine Strafbarkeit wegen **Computerbetrugs** (§ 263a) in Betracht. Dazu müßte T unter Verwirklichung mindestens einer der vier in der Vorschrift genannten Tatvarianten das **Ergebnis eines Datenverarbeitungsvorgangs beeinflußt** haben. **Datenverarbeitung** meint alle technischen Vorgänge, bei denen durch Aufnahme von Daten und ihre programmgesteuerte Verknüpfung Arbeitsergebnisse erzielt werden (Input-Output-Relation).[46] Die Abarbeitung einer Zahlenfolge im Prozessor eines Geldspielautomaten stellt einen solchen Datenverarbeitungsvorgang dar.
Fraglich ist aber, ob T das Ergebnis dieses Vorganges auch **beeinflußt** hat. Wenn man den Begriff der „Beeinflussung" so versteht, daß damit eine programmwidrige Einflußnahme, also eine solche, die zu einem Programmablauf führt, der vom Programm nicht vorgesehen war, gemeint ist, ist das Tatbestandsmerkmal der „Beeinflussung" vorliegend nicht erfüllt. T hätte dann aufgrund der äußerlich ordnungsgemäßen Bedienung keinen programmwidrigen Ablauf herbeigeführt.
Der Begriff der „Beeinflussung" könnte aber auch so ausgelegt werden, daß darunter *jede* Einwirkung zu verstehen ist, die das Ergebnis einer Datenverarbeitung modifiziert.[47] Danach hätte T allein durch die Betätigung der Tasten des Spielautomaten den Datenverarbeitungsvorgang beeinflußt. Für die Auslegung in diesem Sinne sprechen jedenfalls die Semantik dieses Begriffs und der allgemeine Sprachgebrauch. Auch scheint es aus kriminalpolitischer Sicht sachgerecht, den Begriff so zu verstehen. T hat daher den Datenverarbeitungsvorgang des Geldspielautomaten beeinflußt.

T müßte aber auch mindestens eine der vier Handlungsvarianten des § 263 a I verwirklicht haben. In Betracht kommt zunächst eine **unrichtige Gestaltung des Programms (Var. 1)**.
Ein Programm ist eine durch Daten fixierte Arbeitsanweisung an den Computer. „Unrichtig" ist die Programmgestaltung, wenn die Arbeitsanweisung auf betrugsrelevante Tatsachen bezogen ist und sie bewirkt, daß die Daten zu einem Ergebnis verarbeitet werden, das inhaltlich unrichtig ist.[48] Vorliegend hat T nicht auf die Programm*gestaltung* eingewirkt, sondern (lediglich) durch Tastendrucke den Programm*verlauf* beeinflußt. § 263a I Var. 1 scheidet damit aus.

T könnte aber **unrichtige oder unvollständige Daten verwendet haben (Var. 2)**. Mit dieser Tatvariante werden Fälle erfaßt, in denen eingegebene Daten in einen anderen Zusammenhang gebracht oder unterdrückt werden, sog. ***Input- oder Eingabemanipulationen***. **Unrichtig** sind die Daten, wenn die mit ihnen dargestellten Informationen falsch sind, also die Wirklichkeit bzw. den Lebenssachverhalt unzutreffend wiedergeben.[49] Daten sind **unvollständig**, wenn Informationen über „wahre" Tatsachen pflichtwidrig vorenthalten werden.[50] **Verwendet** werden Daten, wenn sie in den Datenverarbeitungsprozeß eingeführt werden (dazu näher in Var. 3).
Aus dieser Definition ergibt sich, daß die Var. 1 lediglich einen Spezialfall der Var. 2 bildet. Aber auch die Var. 2 hat T nicht erfüllt, da er keine Daten eingegeben, sondern nur in Kenntnis des Programmablaufs die Spieltasten bedient hat.

---

[46] *Lackner/Kühl*, § 263a Rn 4; *Jerouschek/Kölbel*, JuS **2001**, 780, 782.
[47] Vgl. zum Begriff der „Beeinflussung" auch LK-*Tiedemann*, § 263a Rn 26; *Tröndle/Fischer*, § 263a Rn 3; Sch/Sch-*Cramer*, § 263a Rn 22; *Jerouschek/Kölbel*, JuS **2001**, 780, 782.
[48] *Tröndle/Fischer*, § 263a Rn 6; *Lackner/Kühl*, § 263a Rn 7; SK-*Günther*, § 263a Rn 14; LK-*Tiedemann*, § 263a Rn 30.
[49] *Tröndle/Fischer*, § 263a Rn 7; SK-*Günther*, § 263a Rn 16; *Laue*, JuS **2002**, 359, 360.
[50] Sch/Sch-*Cramer*, § 263a Rn 7; *Lackner/Kühl*, § 263a Rn 10; *Tröndle/Fischer*, § 263a Rn 7.

Möglicherweise hat T aber **Daten unbefugt verwendet (Var. 3)**. Dazu muß zunächst geklärt werden, was unter dem Merkmal „**Verwenden**" zu verstehen ist. Während eine weite Auslegung jede Nutzung von Daten genügen läßt[51], verlangt die enge Auslegung eine Eingabe von Daten gerade in den Datenverarbeitungsprozeß[52]. Da T keine Daten in den Datenverarbeitungsprozeß eingegeben hat, wäre bei Befolgung dieser Auffassung die Var. 3 zu verneinen und die Var. 4 zu prüfen. Im Ergebnis sind beide Auffassungen gleichermaßen vertretbar.

Folgt man der h.M., ist zu prüfen, ob T **sonst unbefugt auf den Programmablauf eingewirkt** hat (**Var. 4**). Schwierigkeiten bereitet insbesondere die Auslegung des Merkmals „unbefugt" (das im übrigen auch hinsichtlich der Var. 3 zu prüfen gewesen wäre).

- ⇨ Nach der am weitesten gehenden sog. **subjektivierenden** Auslegung ist jede Datenverarbeitung „unbefugt", die dem wirklichen oder mutmaßlichen *Willen des Rechtsgutsinhabers* (des Berechtigten) widerspricht.[53] Demzufolge hat T sich nach § 263a I Var. 3 strafbar gemacht, da die Verwendung von illegal erworbenen Programmkenntnissen kaum dem Willen des Automatenbetreibers entspricht.

- ⇨ Vertreter der engen sog. **computerspezifischen** Auslegung stellen darauf ab, ob der einer Datenverwendung entgegenstehende *Wille des Betreibers* im Computerprogramm berücksichtigt ist.[54] Entscheidend ist danach, ob die Befugnis des Verwenders der Daten im Programmablauf Niederschlag gefunden hat, also vom Programm selbst überprüft wird. Diese Überprüfung findet regelmäßig durch eine entsprechende Nachfrage, etwa durch Anforderung und Überprüfung der persönlichen Geheimnummer, der PIN, statt. Da eine solche zwar bei Geldautomaten, nicht aber bei Geldspielautomaten verlangt wird (Geldspielautomaten stehen für jedermann zur freien Benutzung bereit), ist diese Auslegung für den vorliegenden Fall nicht einschlägig.

- ⇨ Die herrschende Auffassung, die sog. **betrugsspezifische** Auslegung, orientiert sich an § 263 und verlangt ein täuschungsäquivalentes Verhalten des Täters.[55] Durch ihre Anlehnung an § 263 entspricht sie dem Zweck des § 263a, nämlich lediglich bestehende Strafbarkeitslücken zu schließen, die darin bestanden, daß bei einer mißbräuchlichen Benutzung von Datenverarbeitungsanlagen ein Betrug ausscheidet. Gleichwohl bedarf es vorliegend keiner Streitentscheidung, da T auch nach dieser Auslegung den objektiven Tatbestand des § 263a I Var. 4 erfüllt hat. Denn bei der Bedienung des Geräts hat er schlüssig miterklärt, regulär spielen zu wollen und ein spielimmanentes Risiko ohne Sonderwissen vom Spielverlauf einzugehen.[56]

---

[51] So vertreten von BayObLG JR **1994**, 289, 290 f.; *Ranft*, JuS **1997**, 19, 20; *Hilgendorf*, JuS **1997**, 130, 131; *Otto*, BT § 52 Rn 35; offengelassen von BGHSt **40**, 331, 334.

[52] So vertreten von LK-*Tiedemann*, § 263a Rn 4 u. 42-46; *Lackner/Kühl*, § 263a Rn 12; *Rengier*, BT I, § 14 Rn 7; *Tröndle/Fischer*, § 263a Rn 7; *Laue*, JuS **2002**, 359, 362; *Jerouschek/Kölbel*, JuS **2001**, 780, 782.

[53] So vertreten von BGHSt **40**, 331, 334 f.; BayObLG JR **1994**, 289, 291; *Hilgendorf*, JuS **1997**, 130, 131; *Otto*, BT, § 52 Rn 40; *Scheffler/Dressel*, NJW **2000**, 2645; *Mitsch*, JZ **1994**, 877, 883.

[54] So vertreten von OLG Celle NStZ **1989**, 367, 368; *Arloth*, Jura **1996**, 354, 358; *Achenbach*, Jura **1991**, 227 f. und JR **1994**, 293, 295.

[55] So vertreten von BGH NJW **2002**, 905, 906; BGHSt **38**, 120, 121; OLG Köln NJW **1992**, 125, 126; OLG Düsseldorf StV **1998**, 266 f.; LG Bonn NJW **1999**, 3726; LK-*Tiedemann*, § 263a Rn 44; SK-*Günther*, § 263a Rn 18; *Tröndle/Fischer*, § 263a Rn 8; *Rengier*, BT I, § 14 Rn 8; *Wessels/Hillenkamp*, BT/2, Rn 609; *Laue*, JuS **2002**, 359, 363; *Tiedemann/Waßmer*, Jura **2000**, 533, 536; *Kudlich*, JuS **2001**, 20, 21; *Jerouschek/Kölbel*, JuS **2001**, 780, 783.

[56] Vgl. auch BGHSt **40**, 331, 334 f.; *Jerouschek/Kölbel*, JuS **2001**, 780, 783.

Ein **Vermögensschaden** – hier beim Systembetreiber – ist ebenfalls entstanden. Nachdem T auch mit entsprechendem **Tatbestandsvorsatz** und der **Absicht**, sich einen **rechtswidrigen Vermögensvorteil** zu verschaffen, gehandelt hat, ist er im Ergebnis wegen **Computerbetrugs gemäß § 263a I Var. 4 strafbar**.

4. Zur möglichen Strafbarkeit wegen **Hausfriedensbruchs** (**§ 123**), die darin bestehen könnte, daß sich das Einverständnis des Spiel-Center-Inhabers zum Betreten der Räume nur auf redliche Spieler bezieht, vgl. die Ausführungen im BT I auf S. 247.