Klaus Tiedemann

Wirtschaftsbetrug

Klaus Tiedemann

Wirtschaftsbetrug

Sondertatbestände bei
Kapitalanlage und Betriebskredit, Subventionen, Transport
und Sachversicherung, EDV und Telekommunikation

1999

Walter de Gruyter · Berlin · New York

Erweiterte und aktualisierte Sonderausgabe der Kommentierung der §§ 263 a–265 b in der 11. Auflage des Leipziger Kommentars zum Strafgesetzbuch

Dr. Dr. h. c. mult. *Klaus Tiedemann*, o. Professor für Strafrecht, Strafprozeßrecht und Kriminologie an der Universität Freiburg i. Br., Direktor des Instituts für Kriminologie und Wirtschaftsstrafrecht

Die Deutsche Bibliothek – CIP-Einheitsaufnahme

Tiedemann, Klaus:
Wirtschaftsbetrug : Sondertatbestände bei Kapitalanlage und Betriebskredit, Subventionen, Transport und Sachversicherung, EDV und Telekommunikation [erweiterte und aktualisierte Sonderausgabe der Kommentierung der §§ 263 a–265 b in der 11. Auflage des Leipziger Kommentars zum Strafgesetzbuch] / Klaus Tiedemann. – Berlin ; New York : de Gruyter, 1999
ISBN 3-11-016298-9

Printed in Germany
Satz und Druck: Arthur Collignon GmbH, Berlin
Einbandgestaltung: Thomas Beaufort, Hamburg
Buchbinderische Verarbeitung: Lüderitz & Bauer, Berlin

Den Freunden und Kollegen
der Universität Autónoma de Madrid
in bleibender Verbundenheit

Inhaltsverzeichnis

Einführung und Vorwort

Das deutsche Wirtschaftsstrafrecht, welches die Institutionen und Instrumente des Wirtschaftslebens in der Bundesrepublik Deutschland und in der Europäischen Union schützt, stützt sich auf mehrere rechtliche Pfeiler, die teils im Strafgesetzbuch, teils im Nebenstrafrecht verankert sind: Das StGB regelt – im Insolvenzstrafrecht der §§ 283 ff – das pathologische *Ende*, das Kapitalgesellschaftsrecht (AktG, GmbHG, GenG) bekämpft den kriminogenen *Beginn* unternehmerischer Tätigkeit insbesondere bei anonymen und in der zivilrechtlichen Außenhaftung beschränkten Unternehmenstypen[1]. Die aktive (werbende) Geschäftstätigkeit sowie der Gründungsschwindel außerhalb von Kapitalgesellschaften treffen auf strafrechtliche Schranken vor allem in Gestalt des allgemeinen Betrugstatbestandes (§ 263 StGB), der damit Geschäftspartner, infolge der üblichen Gewährung von Zahlungszielen bei den heutigen Geschäftsbeziehungen also allgemein Geld- und Warenkreditgeber, sowie Abnehmer (Kunden und Verbraucher), aber auch Arbeitnehmer und den Staat umfassend gegen Täuschung schützt. Den Strafschutz der Mitbewerber (Konkurrenten) und zugleich der Verbraucher übernimmt insbesondere § 4 UWG, denjenigen der Erhaltung der Haftungsmasse der (rechtlich selbständigen) Unternehmen der allgemeine Untreuetatbestand (§ 266 StGB)[2].

Der einerseits komplizierte und andererseits pauschale, vom Gesetzgeber auf Zweier- und allenfalls Dreier-Beziehungen zugeschnittene Betrugstatbestand hat sich schon früh – wenige Jahrzehnte nach seiner Ausbildung im liberalen Wirtschaftskapitalismus des 19. Jahrhunderts – als nur teilweise geeignet erwiesen, um den vielschichtigen *Interessenkonflikten* im Verhältnis des Wirtschafters zur Öffentlichkeit und den gestuften *Schutzbedürfnissen* in der arbeitsteiligen Industriegesellschaft gerecht zu werden. Die Exzesse der sog. Gründerzeit führten noch vor der Jahrhundertwende zu den schon erwähnten speziellen Straftatbeständen des Gründungsschwindels, anschließend (im UWG) zu solchen der unlauteren Werbung, der Angestelltenbestechung und der Industriespionage. Nach der Weltwirtschaftskrise zu Beginn der 30er Jahre dieses Jahrhunderts traten mehrfach ausgeweitete Spezialtatbestände gegen Bilanz- und Börsen-(Wertpapier-) Manipulationen hinzu. Nach dem 2. Weltkrieg zwang die zunehmende Internationalisierung der Wirtschaft zu einem

[1] Zum ersteren *Tiedemann* Insolvenz-Strafrecht, 2. Aufl. (1996); zum letzteren *Otto* Aktien-Strafrecht (1997) und *Tiedemann* Kommentar zum GmbH-Strafrecht, 3. Aufl. (1995). Zur *spanischen* Reform im Código penal von 1996, der beide Materien zutreffend innerhalb der zentralen strafrechtlichen Kodifikation regelt, *Rodríguez Mourullo/Barreiro* (Hrsg.), Comentarios al Código penal (1997), Art. 259 ff, 290 ff (*Suárez González*). Grundlegend zum neueren spanischen Wirtschaftsstrafrecht insgesamt *Bajo Fernández* Derecho penal económico aplicado a la actividad empresarial (1978).

[2] Zu § 4 UWG nunmehr klärend *Hernández Basualto* Strafrechtlicher Vermögensschutz vor irreführender Werbung, Diss. Freiburg 1998; zur Untreue allgemein *Schünemann* LK, 11. Aufl. (27. Lieferung 1998) und speziell zur gesellschaftsrechtlichen Untreue *Tiedemann* Kommentar zum GmbH-Strafrecht, Rdn. 11 vor §§ 82 ff (zur entsprechenden neuen spanischen Rechtslage *Suárez González* aaO Anm. zu Art. 295).

speziellen strafrechtlichen Schutz des Außenwirtschaftsverkehrs mit zusätzlichen wirtschaftspolitischen und internationalen Schutzzielen, die in neuerer Zeit durch Akte und Zwecksetzungen der EG (EU) und des Sicherheitsrats der Vereinten Nationen überlagert werden. Daneben wurde schon früh im 19. Jahrhundert das *öffentliche Vermögen* vor allem durch das Steuer- und Zollstrafrecht außerhalb des § 263 StGB speziell geschützt; der Betrug erschien jener Zeit als ein nicht notwendigerweise kriminelles „gemeines Privatdelikt", während die „Defraudation" von Staatsmitteln ein öffentliches oder Staats-Verbrechen war[3].

Diese Ausbildung spezieller Straftatbestände vollzog sich durchweg im Nebenstrafrecht mit seiner typischen Tatbestandstechnik von abstrakten Gefährdungs- und Sonder(pflicht)delikten, welche zudem die Tendenz zur Ausdehnung der Strafbarkeit von der vorsätzlichen Begehung auch in den Bereich grob fahrlässigen (leichtfertigen) Handelns aufweisen. Die Übernahme und Fortführung dieser legislatorischen Entwicklung in der zentralen Kodifikation des StGB veranlaßte die deutsche Strafrechtswissenschaft gegenüber diesem traditionell kaum zur Kenntnis genommenen Modell verständlicherweise zu Kritik, Widerstand und Ablehnung, die sich auch an dem neueren Lehrsatz[4] entzündeten, daß das Wirtschaftsstrafrecht im Verhältnis zum (Wirtschafts-) Verwaltungsrecht bei makroökonomischer Sicht eine geringere Belastung des Wirtschafters und der Wirtschaft darstellen und damit den tradierten *ultima ratio*-Gedanken in sein Gegenteil verkehren kann.

Innerhalb dieses weitgespannten und insgesamt durchaus neuartigen Systems und Instrumentariums des Wirtschaftsstrafrechts[5] kommt dem *Wirtschaftsbetrug* eine zentrale Rolle zu. Der Ausdruck geht auf kriminologisch-kriminalistische Ansätze zurück und orientiert sich daran, daß ein statistisch großer, ja überwiegender Anteil von Betrügereien auf (individuelle oder massenhafte) Wirtschaftsbeziehungen entfällt[6]. Da der auf einfache, plumpe Täuschungen angelegte Betrug im kriminologischen Sprachgebrauch als „Schwindel" aus diesem Begriff ausgeschieden wird, eignet sich der terminus „Wirtschaftsbetrug" vorzüglich zur Kennzeichnung eines erheblichen Teiles der Wirtschaftskriminalität, deren rechtliche Erfassung zu ca. zwei Dritteln auf den Betrug und betrugsähnliche Tatbestände entfällt[7]. Trotz einer nicht zu übersehenden rechtsdogmatischen Abgrenzungsschwäche im allgemeinen umfaßt der Wirtschaftsbetrug jedenfalls die in §§ 264 ff genannten Erscheinungen der Erschleichung von Betriebskrediten und (Wirtschafts-)Subventionen, der Kapitalanlagebetrügerei und des Versicherungsmißbrauchs[8]. Aber auch die neuerdings zuneh-

---

[3] Zusammenfassend dazu *Berger* Der Schutz öffentlichen Vermögens durch § 263 StGB, Diss. Freiburg 1999, mit Nachw.; zum einschlägigen neueren spanischen Strafrecht grundlegend *Rodriguez Mourullo* Presente y futuro del delito fiscal (1974).

[4] *Tiedemann* Tatbestandsfunktionen im Nebenstrafrecht (1969) S. 145 sowie JZ **1986** 865, 866 und Stree/Wessels-Festschrift (1993) S. 527, 530 f mit weit. Nachw., auch zu der übereinstimmenden Stellungnahme der *Association Internationale de Droit Pénal* 1984, des RegE des *2. WiKG* 1986 und der EG-Kommission (1992). Vgl. auch (mit dem historischen Beispiel des im Text genannten Aktienstrafrechts) *Nelles* Untreue zum Nachteil von Gesellschaften (1991) S. 57 mit Nachw.

[5] Entwurfsskizze zu seinem Besonderen Teil bei *Tiedemann* Verh. 49. DJT (1972) Bd. I S. C 3, 59 ff.

[6] *Geerds* Handbuch der Kriminalistik Bd. I, 10. Aufl. (1977) S. 269 ff; *Geisler/Mohr* in: Poerting (Hrsg.), Wirtschaftskriminalität Teil 1 (1983) S. 6 ff; *Lessner* Betrug als Wirtschaftsdelikt (1984) S. 6 ff.

[7] *Kaiser* Kriminologie, 2. Aufl. (1988) § 92 Rdn. 26 mit Nachw.

[8] Vgl. bes. *Eisenberg* Kriminologie, 4. Aufl. (1995) § 47 Rdn. 24; *Tiedemann* LK, 11. Aufl. (24. Lieferung 1997), § 265 Rdn. 2 mit Nachw. (unten S. 123) sowie Nachtrag zu § 265 Rdn. 9.

mende Schädigung der öffentlichen Telekommunikation (z. B. durch Telefonkarten-Simulatoren und Verwendung wieder aufgeladener Original-Telefonkarten[9]) und sonstige vermögensbezogene Computermanipulationen (§ 263 a!), letztlich sogar die Erschleichung der Massenverkehrsbeförderung (§ 265 a!) können unter dem kriminologischen Gesichtspunkt des Mißbrauchs von Instrumenten des modernen Wirtschaftsverkehrs hierzu gerechnet werden. Dabei liegt nach Erkenntnissen der Schwerpunktstaatsanwaltschaften für Wirtschaftsstrafsachen der gegenwärtige Schwerpunkt der Wirtschaftskriminalität beim Kapitalanlage- und Subventionsmißbrauch[10].

Die im folgenden ausführlich dargestellten und auch in ihrer kriminologischen Eigenart und Häufigkeit sowie mit ihrem kriminalpolitischen Hintergrund gewürdigten *Sondertatbestände des Betruges* weisen teilweise – wie der freilich 1998 grundlegend reformierte Straftatbestand des Versicherungsmißbrauchs – ein beträchtliches Alter auf[11]. Überwiegend geht die Einführung dieser Sondertatbestände aber auf das strukturelle Unvermögen des allgemeinen Betrugstatbestandes zurück, den Mißbrauch neuerer technischer und wirtschaftlicher Entwicklungen zu erfassen: Das *Irrtumserfordernis des § 263 StGB* stellt die Täuschung des Computers bzw. der DV-Anlage straflos, auch wenn diese Anlage selbständig eine Vermögensverfügung trifft und hieraus ein Vermögensschaden entsteht; die auch im ausländischen Strafrecht durchweg bestehende Lücke schließt der 1986 eingeführte § 263 a. Entsprechendes gilt für die „Täuschung" von einfachen (Leistungs-) Automaten und für die Inanspruchnahme von Leistungen öffentlicher Kommunikationsnetze sowie anderer Einrichtungen und Veranstaltungen des modernen Massenverkehrs: Der Wegfall menschlicher Kontrollen infolge Vordringens der Automation zwingt auch insoweit zu einer Ergänzung des Betrugstatbestandes (hier: durch den 1935 eingeführten und 1976 durch das 1. WiKG reformierten § 265 a)[12].

Daneben treten – kriminalpolitisch stärker umstritten, da die Lückenhaftigkeit des geltenden Rechts hier weniger evident und je nach Grundüberzeugung nicht unbedingt zwingend ist – *neue Schutzbedürfnisse* in Wirtschaftsbereichen auf, die ebenfalls weitgehend durch die Gesichtspunkte der Massenhaftigkeit und der Interessenvielfalt gekennzeichnet sind. So erfährt der bereits vom Reichsgericht als zentrales volkswirtschaftliches Instrument gekennzeichnete *kaufmännische Kredit*[13] besonderen Schutz durch den 1976 eingeführten Sondertatbestand des § 265 b, dem eine Sonderregelung im früheren Kreditwesengesetz voraufgegangen war; an diese rechtliche Ordnung durch das (heutige) KWG knüpft § 265 b an, so daß von einer *Institution* gesprochen werden kann, die nicht weniger strafschutzwürdig ist als die

[9] *Bundeskriminalamt* Bericht zur IuK-Kriminalität (Kriminalität in Verbindung mit der Informations- und Kommunikationstechnologie) 1997, Mitteilungsblatt **1998** Nr. 1 S. 23 und 34 f; vgl. auch *Tiedemann* LK, 11. Aufl. (27. Lieferung 1998), § 263 a Rdn. 59 mit Nachw. sowie Kaiser-Festschrift (1998) S. 1373 (1374 f).

[10] So das Fazit der Tagung der deutschen Wirtschaftsstaatsanwälte in Erfurt 1998; vgl. FAZ Nr. 117 v. 22.5.1998 S. 10.

[11] Zur Geschichte und zu Vorläufern des § 265 StGB *Wolff* Die Neuregelung des Versicherungsmißbrauchs (§ 265 StGB n. F.), Diss. Freiburg 1999, und *Tiedemann* LK § 265 Rdn. 1 und 2 (unten S. 122 f).

[12] Zur abweichenden Lösung des *französischen* Betrugsstrafrechts, das trotz vergleichbarer gesetzlicher Ausgangslage das Irrtumserfordernis stärker pauschaliert (und ähnlich der deutschen Behandlung des Warenautomaten-Diebstahls auf den Willen des Betreibers abstellt), *Walter* Betrugsstrafrecht in Frankreich und Deutschland, Diss. Freiburg 1999, § 3 II mit Nachw.

[13] RGSt **4** 41, 42; **16** 238, 239; ebenso BVerfGE **48** 48, 61 f; **90** 145, 204; dazu bereits *Tiedemann* Insolvenz-Strafrecht Rdn. 56 vor § 283 und LK § 265 b Rdn. 17 mit weit. Nachw. (unten S. 183).

Rechtspflege, das Urkundenwesen usw.[14] Die *Kapitaleinwerbung* durch Unternehmen und Banken mit Hilfe der Ausgabe von Wertpapieren und Unternehmensbeteiligungen trifft auf ein heute zwar breites, aber weiterhin meist unerfahrenes Anlegerpublikum, dessen Schutz vor Vermögensschäden durch den Betrugstatbestand faktisch zu spät kommt und daher mit dem 1986 eingeführten § 264a schon bei der Werbung ansetzt[15]. Auch wird die *Wirtschaftssubvention* als zentrales wirtschaftspolitisches Lenkungsinstrument wegen seiner Wichtigkeit und Schadensanfälligkeit – auch und besonders im EU-Bereich[16] – durch § 264 besonders geschützt, wobei die damit mögliche Erfassung immaterieller Planungsschäden den allgemeinen Betrugstatbestand von zweifelhaften Konstruktionen wie der der wirtschaftlichen Zweckverfehlung entlastet. Die 1998 aufgrund einer EG-Konvention erfolgte Ergänzung des 1976 eingeführten § 264 ist Teil einer EU-weiten Harmonisierung der strafrechtlichen Erfassung des Mißbrauchs von EG-rechtlichen Subventionen und stellt vor allem auch den durch den Betrugstatbestand von vornherein nicht zu erfassenden (untreueähnlichen) Tatbestand der nachträglichen Zweckentfremdung rechtmäßig erlangter Subventionen deutlich heraus (§ 264 Abs. 1 Nr. 2 n. F.). Das Sozialvermögen und die Institution *Versicherungswirtschaft* schließlich wird nach der heute überholten Beschränkung des speziellen Strafschutzes auf die Feuer- und Seeversicherung seit dem 6. Strafrechtsreformgesetz von 1998 in allen Sparten der Sachversicherung, freilich nicht in anderen vermögensrelevanten Bereichen wie etwa der Lebensversicherung, durch § 265 n. F. geschützt; durch Ablösung von der Betrugsstrafbarkeit und Schutz des Sozialvermögens gegen künstliche Auslösung des versicherten Risikos ist der überindividuell-soziale Aspekt hier zusätzlich verstärkt worden (vgl. unten Nachtrag 2, § 265 n. F. Rdn. 9).

Diese wirtschaftlichen Sondertatbestände des StGB sehen meist von einem *Schadenserfordernis* ab. Soweit hierin ein historischer Rückschritt gegenüber der Ausbildung des modernen Betrugstatbestandes erblickt wird[17], könnte dies allenfalls dann als relevanter Einwand angesehen werden, wenn die Sondertatbestände wirklich besondere Betrugstatbestände, nämlich zumindest betrugsähnliche Delikte, darstellen, wie es die formale Einordnung in den Zweiundzwanzigsten Abschnitt des StGB anzunehmen nahelegen mag. Jedoch orientieren sich diese „Sondertatbestände" des Betruges von vornherein nur teilweise an kommunikativen Täuschungshandlungen (so §§ 264, 264a, 265b) und sind daher nur insoweit betrugsähnlich, nämlich an der Kommunikation ausgerichtet. Andere Sondertatbestände stellen demgegenüber ganz (§§ 265, 265a) oder teilweise (§ 263a 1. und 4. Alt., aber auch 3. Alt.) auf die Manipulation eines Objektes ab und können daher kaum sinnvoll in das Betrugssystem eingeordnet werden; sie sind eher diebstahls-ähnlich[18]. Auch enthält § 263a 3. Alt. mit dem Merkmal unbefugten Handelns eher Elemente der Urkundenfälschung als der

[14] Insoweit zustimmend *Vogel* Legitimationsprobleme im Betrugsstrafrecht (1999); **aA** insbes. *Kindhäuser* in: Schünemann/Suárez González (Hrsg.), Bausteine des europäischen Wirtschaftsstrafrechts – Madrid-Kolloquium für Klaus Tiedemann (1994) S. 125, 129.

[15] *Tiedemann* LK § 264a Rdn. 2 (unten S. 76ff) mit Nachw. (auch zu der – inzwischen weiter verbesserten – *rechtlichen Ordnung* und damit Institutierung des Kapitalanlagemarktes).

[16] Dazu allgemein BTDrs. 13/10425 S. 1 (Begr. zum EG-FinanzschutzG); Einzelangaben zuletzt in: FAZ Nr. 105 v. 7.5.1998 S. 17 (EG-Jahresbericht 1997 über Betrügereien gegen die Finanzinteressen der EG: aufgedeckte [!] Fälle in Höhe von ca. 2,6 Mrd. DM, also knapp 2% des EG-Haushalts); zuvor *Tiedemann* in: Müller-Dietz (Hrsg.), Festschrift 25 Jahre Kolloquien der Südwestdeutschen Kriminologischen Institute (1989) S. 76ff (unter Bezugnahme u. a. auf die Berichte der Rechnungshöfe und auf verwaltungsrechtliche Widerrufsverfahren).

[17] Vgl. nur *Schlüchter* Trusen-Festschrift (1994), S. 573, 589.

[18] *Tiedemann* LK § 263a Rdn. 6, 16 und 44, § 265a Rdn. 16, je mit weit. Nachw.

Täuschung, die somit keineswegs eine durchgehende Klammer der Sondertatbestände des Betrugs darstellt. Die *Legitimation* der täuschungsfreien Sondertatbestände ergibt sich damit nicht aus ihrer größeren oder geringeren Nähe zum Betrugstatbestand und dessen Erfordernis eines Vermögensschadens, sondern aus anderen oder zusätzlichen Überlegungen und Kriterien:

Teilweise geht es bei den Tatobjekten der Sondertatbestände um *immaterielle Leistungen*, die nur deshalb nicht durch §§ 242 ff erfaßt werden, weil sie als nicht-gegenständliche Tatobjekte typischerweise nicht dem sachgebundenen Wegnahme- und Zueignungselement dieser Eigentumstatbestände unterfallen. Die Legitimation dieser Sondertatbestände folgt jedenfalls aus dem Erfordernis des Vermögensschadens, soweit dieser von dem Sondertatbestand vorausgesetzt wird (so § 263 a). Auch bei § 265 a tritt ein Vermögensschaden ein[19], mag dieser auch nicht vom Gesetz als Tatbestandsmerkmal genannt werden: Die Erschleichung einer vermögenswerten Leistung ohne Erbringung der Gegenleistung stellt notwendigerweise einen Vermögensschaden dar.

Soweit die Sondertatbestände dagegen ganz von einem Vermögensschaden absehen, geht es nach einem verbreiteten Sprachgebrauch um Handlungen im *Vorfeld* des Betruges und der Vermögensschädigung. Diese echte Vorverlagerung des Strafschutzes kann unter Gesichtspunkten des Vermögensschutzes nur entweder aus der Massenhaftigkeit der Begehungsweise (sog. Kumulationsdelikt)[20] und im übrigen vor allem aus der besonderen Bedeutung eines neben oder anstelle des Vermögens geschützten institutionellen Rechtsgutes erklärt werden. Die erstere Begründung ist für ein (verfassungsrechtliches) Schuldstrafrecht problematisch, soweit die Einzelhandlungen als solche ungefährlich sind. Anderes gilt für die gemeingefahrähnliche massenhafte Begehungsweise, wie sie sich – als vom Gesetzgeber aufgegriffenes Tatbestands- und Legitimationsmerkmal – in *publikumsschützenden* Sondertatbeständen wie § 264 a, aber auch § 4 UWG und § 82 GmbHG usw., zeigt, wobei mit dem massenhaften Angriff tendenziell eine Verschlechterung der Abwehrmöglichkeiten der potentiellen Opfer verbunden ist; zugleich hängt das Abschneiden des Tatbestandsmerkmals der (auch nur: versuchten) Vermögensbeschädigung hier mit der Formalisierung und Nichtindividualisierung von *Werbung* zusammen und ist bei Postulierung eines individuellen Schadenseinschlages für § 263 geradezu zwangsläufig[21]. Daneben entspricht es dem Verständnis des 20. Jahrhunderts und seiner Verfassungsrechtsprechung[22], daß nicht nur *hoheitliche Vermögensinteressen* heute als besonders gewichtig eingeschätzt werden (§ 264, §§ 370 ff AO!), sondern daß die Übernahme zentraler Funktionen durch Staat und Gesellschaft auch zu deren strafrechtlicher Bewertung als gewichtig führt. Für die einschlägigen Rechtsgüter liefert insbesondere das Wirtschaftsrecht Modelle und Vorentscheidungen, die zwar – anders als weitgehend im Nebenstrafrecht – für den Strafgesetzgeber nicht ohne weiteres bindend sind, von ihm aber als Vorbild gewählt werden können und dann auch im Strafrecht nicht einfach in individuelle Aspekte zerlegt werden dürfen, ohne die Eigenart der (institutionellen) Rechtsgüter und die Schutzzwecke der Norm zu

[19] RGSt **42** 40, 41; *Tiedemann* LK § 265 a Rdn. 15 mit weit. Nachw.; aus zivilrechtlicher Sicht zuletzt *Weth* JuS **1998** 795 ff.

[20] Dazu i. e.S. *Kuhlen* GA **1986** 389 ff; allgemeiner (und unter Wahrung des verfassungsrechtlichen Schuldgrundsatzes) *Tiedemann* Tatbestandsfunktionen S. 119, 124 f.

[21] Näher dazu *Hernández Basualto* aaO, der auch zutreffend darauf hinweist, daß die Täuschungs- oder Irreführungs*eignung* in Sondertatbeständen eine deutliche Qualifikation der Tathandlung im Verhältnis zu § 263 darstellt.

[22] Dazu in diesem Zusammenhang *Appel* Verfassung und Strafe (1998) mit weit. Nachw.

zerstören. So ist die „Kreditwirtschaft" mehr als die Summe der Vermögen der Kreditgeber, und entsprechend ist die Gefährdung der Kreditwirtschaft nicht identisch mit der Gefährdung einzelner Vermögen. Die schon erwähnte enge Anlehnung der Tatbestandsfassung des § 265 b an die rechtliche Garantie des Kreditwesens im KWG indiziert zumindest eine Übereinstimmung der Zweck- und Rechtsgutsbestimmung von KWG und § 265 b StGB. Diese Orientierung an überindividuellen (sozialen) Rechtsgütern des Wirtschaftslebens findet – zusammengefaßt – als strafrechtlicher *Institutionenschutz*[23] eine seit langem anerkannte Parallele bei Straftatbeständen wie §§ 153 ff, 146 ff, 267 ff StGB, also gerade jenen Tatbestandsgruppen, die historisch bis ins 19. Jahrhundert hinein mit dem Betrug eng verbunden waren und nach ihrer Abspaltung von diesem in ihrer Legitimation nicht angezweifelt werden. Wenn Entsprechendes auch für die Sondertatbestände der §§ 264, 264 a, 265, 265 b gilt, wäre es freilich richtiger, diese Tatbestände in anderen Abschnitten des StGB zu regeln oder in einem eigenen Abschnitt zusammenzufassen[24].

Insgesamt kann somit die Systematik des „Betrugsstrafrechts" im StGB nicht ausnahmslos, ja nicht einmal durchgehend, von dem allgemeinen Betrugstatbestand des § 263 her konzipiert und folglich eine diesem Tatbestand ähnliche *Auslegung* der Sondertatbestände nicht ohne vorherige Prüfung ihrer Betrugsähnlichkeit postuliert werden. Die Einzelheiten der jeweiligen Einordnung einschließlich der verfassungsrechtlichen und kriminalpolitischen Problematik und Legitimation sowie die hiermit zusammenhängenden Auslegungsprobleme sind jeweils bei der Kommentierung der Sondertatbestände dargestellt.

Auch die vorläufig abschließende Frage, ob die (zu) pauschal häufig als Vorfeldtatbestände bezeichneten §§ 264 ff durchgehend *abstrakte Gefährdungsdelikte* darstellen, wird ausführlich bei der Erläuterung der einzelnen Tatbestände behandelt. Vorab ist hier nur festzuhalten, daß eine solche Bezeichnung von der h.M. unter dem alleinigen Bezugspunkt des Vermögensschutzes gebraucht wird. In bezug auf überindividuelle Rechtsgüter verliert demgegenüber die Unterscheidung von Verletzungs- und abstrakten sowie konkreten Gefährdungsdelikten weitgehend ihren Sinn: Die Funktionsbedingungen der einschlägigen Institutionen werden durch jede gegen sie gerichtete Straftat verletzt, und eine reale Gefährdung oder Vernichtung der Institutionen wäre ein Tatbestandserfolg, der auch bei §§ 153 ff, 146 ff, 267 ff StGB nicht verlangt wird. Die „abstrakte" Gefährdung dieser Rechtsgüter ist somit in jedem Fall ein *Geltungsschaden*, der nach richtiger Ansicht auch bei den individuellen Rechtsgütern maßgebend ist, selbst wenn diese regelmäßig Tatobjekte betreffen, die real vernichtet, verletzt oder gefährdet werden können. Es darf inzwischen wohl als international herrschende Meinung bezeichnet werden, daß über-individuelle Rechtsgüter ihre typische und zutreffende strafrechtliche Form der Ausgestaltung grundsätzlich in der Figur des abstrakten Gefährdungsdelikts finden, auch wenn diese nicht nur der Vorverlegung der Strafbarkeit und bloßer Beweisverbesserung dienen darf[25]. Strafwürdige Beeinträchtigungen etwa des Weltfriedens (§ 34 AWG!) oder wirtschaftspolitischer Zentralziele (§ 1 StabG!) können – um zwei Beispiele außerhalb des StGB anzuführen – sinnvoll und in verfassungsrechtlich zulässiger, nämlich hinreichend bestimmter, Weise nicht als solche straftatbestandlich erfaßt, sondern

---

[23] Eingehend zu diesem Legitimationsgesichtspunkt *Vogel* aaO.

[24] So für § 264 *Amelung* Rechtsgüterschutz und Schutz der Gesellschaft (1972) S. 376 f; allgemein bereits *Tiedemann* ZRP **1970** 256 ff.

[25] Entschließungen des XIII. Internationalen Strafrechtskongresses in Kairo 1984, ZStW **97** (1985), 736.

müssen als konkretere Handlungen umschrieben oder als Pflichten konstruiert werden. Eine „tatbestandsnahe" Rechtsgutslehre wird insoweit auf Schwierigkeiten stoßen, weil dem geschützten Rechtsgut kein unmittelbares Handlungsobjekt und kein greifbares Opfer entspricht. Deshalb aber Möglichkeit und Existenz abstrakter Gefährdungsdelikte im über-individuellen (sozialen) Wirtschaftsbereich zu leugnen, hieße die Eigenart heutiger Wirtschaft, wie sie im Wirtschaftsrecht entwickelt und anerkannt ist, um einer Ideologie willen verkennen, die so auch im 19. Jahrhundert nicht geherrscht hat.

Bei den im folgenden abgedruckten Kommentierungen der Sondertatbestände habe ich seitens meiner Mitarbeiter tatkräftige Unterstützung erfahren, für die ich auch an dieser Stelle herzlich danke. Zahlreiche inhaltliche Anregungen und technische Hilfen bei der Auswertung von Rechtsprechung und Literatur verdanke ich den Herren Rechtsassessor Dr. Joachim *Vogel* sowie Rechtsreferendaren Dr. Jürgen *Louis* und Dr. Tonio *Walter*. Das umfangreiche Stichwortregister hat mit großer Sorgfalt Herr Rechtsassessor Dr. Martin *Waßmer* angefertigt. Für die genaue Erledigung der Schreibarbeiten habe ich Frau Hildegard *Käppele* zu danken.

Die Gesamtkommentierung befindet sich auf dem Stand der Gesetzgebung von Herbst 1998. Rechtsprechung und Literatur sind bis zu demselben Zeitpunkt berücksichtigt, soweit dies die gestaffelte Drucklegung zuließ. Ausgewertet wurden auch bereits fünf aktuelle, noch ungedruckte Freiburger Dissertationen (*Berger, Hernández, Stein, Walter, Wolff*). Die vor dem Abschluß stehende Habilitationsschrift von *Vogel* leistet eine Vertiefung insbesondere der legitimationstheoretischen Aspekte des Wirtschaftsbetruges.

Freiburg, im November 1998

Klaus Tiedemann

§ 263 a

Computerbetrug

(1) Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, daß er das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf beeinflußt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) § 263 Abs. 2 bis 7 gilt entsprechend.

Schrifttum

Allgemeine Literatur zum 2. WiKG *Achenbach* Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität, NJW **1986** 1835; *Frommel* Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität, JuS **1987** 667; *Granderath* Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität, DB **1986** Beil. Nr 18; *Haft* Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität (2. WiKG), NStZ **1987** 6; *Kolz* Zur Aktualität der Bekämpfung der Wirtschaftskriminalität für die Wirtschaft, wistra **1982** 167; *Mitsch* Rechtsprechung zum Wirtschaftsstrafrecht nach dem 2. WiKG, JZ **1994** 877; *Möhrenschlager* Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität (2. WiKG), wistra **1986** 123; *Möhrenschlager* Der Regierungsentwurf eines Zweiten Gesetzes zur Bekämpfung der Wirtschaftskriminalität, wistra **1982** 201; *Schlüchter* Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität (1987); *Tiedemann* Die Bekämpfung der Wirtschaftskriminalität durch den Gesetzgeber – Ein Überblick aus Anlaß des Inkrafttretens des 2. WiKG am 1. 8. 1986, JZ **1986** 865; *A. Weber* Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität, WM **1986** 1133; *Weinmann* Gesetzgeberische Maßnahmen zur Bekämpfung der Wirtschaftskriminalität: Besteht nach dem 1. und 2. WiKG ein weiterer Regelungsbedarf? Pfeiffer-Festschrift (1986) S. 87.

Spezielle Literatur zum Computerbetrug *Achenbach* Die „kleine Münze" des sog. Computer-Strafrechts – Zur Strafbarkeit des Leerspielens von Geldspielautomaten, Jura **1991** 225; *Altenhain* Der strafbare Mißbrauch kartengestützter elektronischer Zahlungssysteme, JZ **1997** 752; *Arloth* Computerstrafrecht und Leerspielen von Geldspielautomaten, Jura **1996** 354; *Arloth* Leerspielen von Geldspielautomaten – Ein Beitrag zur Struktur des Computerbetrugs, CR **1996** 359; *Bandekow* Strafbarer Mißbrauch des elektronischen Zahlungsverkehrs (1989); *R. Baumann/Bühler* Strafrecht – Die Bankomat-Kriminellen, JuS **1989** 49; *Berghaus* § 263 a StGB und der Codekartenmißbrauch durch den Kontoinhaber selbst, JuS **1990** 981; *Bernsau* Der Scheck- und Kreditkartenmißbrauch durch den berechtigten Karteninhaber (1990); *Bieber* Noch einmal Strafrecht – Die Bankomat-Kriminellen, JuS **1989** 475; *Bieber* Rechtsprobleme des ec-Geldautomatensystems, WM **1987** Beil. Nr. 6; *Bühler* Die strafrechtliche Erfassung des Mißbrauchs von Geldautomaten (1995); *Bühler* Ein Versuch, Computerkriminellen das Handwerk zu legen, MDR **1987** 448; *Bühler* Geldspielautomatenmißbrauch und Computerstrafrecht, MDR **1991** 14; *Bühler* Manipulation von Geldspielautomaten, wistra **1994** 256; *Bühler* Zum Konkurrenzverhältnis zwischen § 263 a StGB und § 266 b StGB beim Scheck- und Kreditkartenmißbrauch, MDR **1989** 22; *Dannecker* Neuere Entwicklungen im Bereich der Computerkriminalität – Aktuelle Erscheinungsformen und Anforderungen an eine effektive Bekämpfung, BB **1996** 1285; *Eck* Die neuen Straftatbestände zur Bekämpfung der Computerkriminalität und ihre Bedeutung für die Datendienste der Deutschen Bundespost, Archiv für Post- und Fernmeldewesen (ArchivPF) **1987** 105; *Ehrlicher* Der Bankomatenmißbrauch – Seine Erscheinungsformen und seine Bekämpfung (1989); *Engelhard* Computerkriminalität und deren Bekämpfung durch strafrechtliche Reformen, DVR **1985** 165; *Engelhard* Neuere Rechtsprechung zu § 263 a StGB, CR **1991** 484; *Etter* Noch einmal: Systematisches Entleeren von Glückspielautomaten, CR **1988** 1021; *Etter* Neuere Rechtsprechung zu § 263 a StGB – Versuch einer systematischen Einordnung, CR **1991** 484; *Frey* Computerkriminalität in eigentums- und vermö-

gensstrafrechtlicher Sicht (1987); *Füllkrug* Manipuliertes Glück – Spiele an Geldspielautomaten, Kriminalistik **1988** 587; *Geßler* Kapitalanlagebetrug und Computerbetrug nach dem 2. WiKG, Kriminalist **1986** 519; *Gogger* Die Erfassung des Scheck-, Kredit- und Codekartenmißbrauchs nach Einführung der §§ 263 a, 266 b StGB durch das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität (1995); *Gutiérrez Francés* Fraude informático y estafa (Madrid 1991); *Haft* Das neue Computer-Strafrecht, DSWR **1986** 255; *Haß* Der strafrechtliche Schutz von Computerprogrammen, in: Lehmann (Hrsg.), Rechtsschutz und Verwertung von Computerprogrammen, 2. Aufl. (1993), S. 467; *Haurand/Vahle* Computerkriminalität, RDV **1990** 128; *Hilgendorf* Grundfälle zum Computerstrafrecht, JuS **1996** 509, 702, 890, 1082, **1997** 130, 323; *Huff* Die mißbräuchliche Benutzung von Geldautomaten, NJW **1987** 815; *Huff* Die Strafbarkeit der mißbräuchlichen Geldautomatenbenutzung durch den Kontoinhaber, NJW **1986** 902; *Huff* Die Strafbarkeit im Zusammenhang mit Geldautomaten, NStZ **1985** 438; *Jungwirth* Diebstahlsvarianten im Zusammenhang mit Geldausgabeautomaten, MDR **1987** 537; *Kleb-Braun* Codekartenmißbrauch und Sparbuchfälle aus „Volljuristischer" Sicht, JA **1986** 249; *Lackner* Zum Stellenwert der Gesetzestechnik – Dargestellt an einem Beispiel aus dem Zweiten Gesetz zur Bekämpfung der Wirtschaftskriminalität, Tröndle-Festschrift (1989) S. 41; *Lampe* Die strafrechtliche Behandlung der sog. Computer-Kriminalität, GA **1975** 1; *Lampe* Erfordert die Bekämpfung der sogenannten Computerkriminalität neue strafrechtliche Tatbestände? in: Bundesminister der Justiz (Hrsg.), Tagungsberichte der Sachverständigenkommission zur Bekämpfung der Wirtschaftskriminalität Bd. XII (1977), Anlage 3 (zit.: Tagungsberichte Bd. XII Anl. 3); *Lenckner* Computerkriminalität und Vermögensdelikte (1981); *Lenckner/Winkelbauer* Computerkriminalität – Möglichkeiten und Grenzen des 2. WiKG, CR **1986** 654; *Lenckner/Winkelbauer* Strafrechtliche Probleme im modernen Zahlungsverkehr, wistra **1984** 83; *Meier* Strafbarkeit des Bankomatenmißbrauchs, JuS **1992** 1017; *Meurer* Die Bekämpfung der Computerkriminalität in der Bundesrepublik Deutschland, Kitagawa-Festschrift (1992) S. 971; *Mitsch* Die Verwendung einer Codekarte durch einen Nichtberechtigten als Diebstahl – AG Kulmbach, NJW 1985, 22, JuS **1986** 767; *Möhrenschlager* Computerstraftaten und ihre Bekämpfung in der Bundesrepublik Deutschland, wistra **1991** 321; *Möhrenschlager* Das neue Computerstrafrecht, wistra **1986** 128; *Neumann* Leerspielen von Geldspielautomaten – Diebstahl und Computerbetrug, CR **1989** 717; *Neumann* Unfaires Spielen am Geldspielautomat – OLG Celle, NStZ 1989, 367, JuS **1990** 535; *Otto* Examinatorium: Probleme des Computerbetrugs, Jura **1993** 612; *Otto* Zum Bankautomatenmißbrauch nach Inkrafttreten des 2. WiKG, JR **1987** 221; *Paul* Gezinkte Karten – Über die vielen Möglichkeiten des Kreditkartenmißbrauchs, NJW-CoR **1994** 284; *Picotti* I reati informatici (Padua 1998); *Ranft* Der Bankomatenmißbrauch, wistra **1987** 79; *Ranft* „Leerspielen" von Glücksspielautomaten – BGHSt. 40, 331, JuS **1997** 19; *Ranft* Zur „betrugsnahen" Auslegung des § 263 a StGB, NJW **1994** 2574; *Richter* Computerkriminalität und Strafrecht, in: Handbuch der modernen Datenverarbeitung (HMD) H. 146 (1989) S. 76; *Richter* Mißbräuchliche Benutzung von Geldautomaten – Verwendung duplizierter und manipulierter Euroscheckkarten, CR **1989** 303; *Richter* Strafbarer Mißbrauch des Btx-Systems, CR **1991** 361; *Rohner* Computerkriminalität (Zürich 1976); *Rossa* Mißbrauch beim electronic cash – Eine strafrechtliche Bewertung, CR **1997** 219; *Sarzana* Informatica e diritto penale (Mailand 1994); *Scheu/Kohler* Der Strafrechtsschutz beim Mißbrauch von computergesteuerten Geldspielautomaten, Der Münzautomat **1987** 56; *Schlüchter* Bankomatenmißbrauch mit Scheckkarten-Blanketten, JR **1993** 493; *Schlüchter* Entschlüsselte Spielprogramme: Schutz für elektronisch gespeicherte geistige Inhalte, CR **1991** 105; *Schlüchter* Zweckentfremdung von Geldspielgeräten durch Computermanipulationen, NStZ **1988** 53; *Schmid* Computer- sowie Check- und Kreditkarten-Kriminalität (Zürich 1994); *Schmidt* Rechtsprechungsübersicht: „Leerspielen" eines Geldautomaten, JuS **1995** 557; *Schmitt* Strafrechtliche Probleme als Folge von Neuerungen im Bankwesen, Jura **1987** 640; *Schulz* Rechtsprechung Strafrecht: Computerbetrug, JA **1995** 538; *Schulz/Tscherwinka* Probleme des Codekartenmißbrauchs, JA **1991** 119; *Schulze-Heiming* Der strafrechtliche Schutz der Computerdaten gegen die Angriffsformen der Spionage, Sabotage und des Zeitdiebstahls (1995); *Sieber* Computerkriminalität und Strafrecht, 2. Aufl. (1980); *Sieber* Der strafrechtliche Schutz der Information, ZStW **103** (1991) S. 779; *Sieber* Informationstechnologie und Strafrechtsreform: Zur Reichweite des künftigen 2. Gesetzes zur Bekämpfung der Wirtschaftskriminalität (1985); *Sieber* The International Handbook on Computer

Crime – Computer-related Economic Crime and the Infringements of Privacy (1986); *Sieg* Strafrechtlicher Schutz gegen Computerkriminalität, Jura **1986** 352; *Sonnen* Wegnahme und Mißbrauch einer codierten eurocheque-Karte, JA **1988** 461; *Spahn* Wegnahme und Mißbrauch codierter Scheckkarten nach altem und neuem Recht, Jura **1989** 513; *Steinhilper* Ist die Bedienung von Bargeldautomaten unter mißbräuchlicher Verwendung fremder Codekarten strafbar? GA **1985** 114; *Steinke* Dem Glück auf die Sprünge geholfen – Überlistung computerisierter Spielautomaten, Kriminalistik **1988** 565; *Steinke* Kriminalität durch Beeinflussung von Rechnerabläufen, NStZ **1984** 295; *Steinke* Mit kleinen Karten an das große Geld – Neue Strafvorschriften zum Schutz gegen moderne Fälscher, Kriminalistik **1987** 62; *Steinke* Verbrecher am Rechner – Was bringen die Gesetze gegen Computer-Kriminalität? Kriminalistik **1987** 73; *Thaeter* Die unendliche Geschichte „Codekarte", JA **1988** 547; *Thaeter* Zur Struktur des Codekartenmißbrauchs, wistra **1988** 339; *Tiedemann* Computerkriminalität und Mißbrauch von Bankomaten, WM **1983** 1326; *Tiedemann* Computerkriminalität und Strafrecht, Kaiser-Festschrift (1998); *Tiedemann* Die deutsche Strafrechtsregelung zur Erfassung der Computerkriminalität im internationalen Vergleich, Fernández Albor-Gedächtnisschrift (Santiago de Compostela 1989) S. 689; *U. Weber* Aktuelle Probleme bei der Anwendung des Zweiten Gesetzes zur Bekämpfung der Wirtschaftskriminalität, Krause-Festschrift (1990) S. 427; *U. Weber* Konkurrenzprobleme bei der strafrechtlichen Erfassung der Euroscheck- und Euroscheckkartenkriminalität durch das 2. WiKG, Küchenhoff-Gedächtnisschrift (1987) S. 485; *U. Weber* Probleme der strafrechtlichen Erfassung des Euroscheck- und Euroscheckkartenmißbrauchs nach Inkrafttreten des 2. WiKG, JZ **1987** 215; *Westpfahl* Strafbarkeit des systematischen Entleerens von Glücksspielautomaten, CR **1987** 515; *Yoo* Codekartenmißbrauch am POS-Kassen-System: Strafrechtliche Überlegungen zur Computerkriminalität (1997).

Einschlägige außerstrafrechtliche Literatur (Auswahl) *Betzel* Sicherung des Rechnungswesens (1974); *Bschorr* Computerkriminalität: Gefahr und Abwehr (1987); *Burhenne/Perband* EDV-Recht (Stand: Juli 1997); *Grosch/Liebl* Computerkriminalität (1994); *Kilian/Heussen* (Hrsg.), Computerrechts-Handbuch – Computertechnologie in der Rechts- und Wirtschaftspraxis (Stand: August 1996); *Poerting/Pott* Computerkriminalität – Ausmaß, Bedrohungspotential, Abwehrmöglichkeiten (1986); *Rossa* Mißbrauch beim electronic cash – Eine zivilrechtliche Bewertung, CR **1997** 138; *Schultz* Computerkriminalität (1993); *Sieber* Computerkriminalität und Informationsstrafrecht, CR **1995** 100; *Sieber* Informationsrecht und Recht der Informationstechnik, NJW **1989** 2569; *Zimmerli/Liebl* (Hrsg.), Computermißbrauch – Computersicherheit (1984).

Materialien

Beschlußempfehlung und Bericht des Rechtsausschusses zu dem Entwurf eines Zweiten Gesetzes zur Bekämpfung der Wirtschaftskriminalität (2. WiKG), BTDrucks. 10/5058 (zit.: Beschlußempfehlung); Bundesminister der Justiz (Hrsg.), Tagungsberichte der Sachverständigenkommission zur Bekämpfung der Wirtschaftskriminalität Bd. XII (1977) (zit.: Tagungsberichte Bd. XII); Protokolle der Sitzungen des Rechtsausschusses, Deutscher Bundestag 10. Wahlperiode Stenographischer Dienst, 26. Sitzung (zit.: Prot.); Regierungsentwurf (RegE) eines Zweiten Gesetzes zur Bekämpfung der Wirtschaftskriminalität, BTDrucks. 10/318 = BRDrucks. 219/82 und BRDrucks. 150/83.

Übersicht

1 **I. Entstehungsgeschichte und kriminalpolitischer Hintergrund; Auslandsrechte.** Der Straftatbestand wurde durch das **2. WiKG** 1986 eingeführt, das zusammen mit weiteren Änderungen (vgl. *Tiedemann* LK § 264 a Rdn. 1) in das StGB das sog. **Computerstrafrecht** einstellte. Dieses betrifft neben dem durch § 263 a geschaffenen Vermögensschutz insbesondere den Schutz der Sicherheit des Beweisverkehrs mit Daten (§ 269), aber auch den Bestand und die Verwendbarkeit (vgl. §§ 303 a, b) sowie die Geheimhaltung von Daten (§ 202 a). Für die letztgenannten Tatbestände wird der Datenbegriff durch § 202 a Abs. 2 im Sinne elektronischer oder magnetischer Speicherung (usw.) legaliter definiert. Eine entsprechende Definition fehlt für § 263 a, allerdings ausweislich der Entstehungsgeschichte nur deshalb, weil hier die Manipulation nicht nur an bereits gespeicherten Daten begangen wird, sondern als sog. Eingabe- oder Input-Manipulation unrichtige Daten in das Verarbeitungssystem eingespeist werden (BTDrucks. 10/5058 S. 30). Bei § 263 a (und § 269) werden daher **Daten** weitergehend als kodierte oder kodierbare (verschlüsselbare) Informationen verstanden (näher und **krit.** unten Rdn. 19 ff). Die bereits durch § 202 a Abs. 2 nahegelegte Weite des Datenbegriffs führt in der Literatur auch zu einer Ausweitung des „klassischen" Begriffs des Computer- oder (E)DV-Strafrechts zum sog. Informationsstrafrecht, das zum Teil noch mit dem „Kommunikationsstrafrecht" zusammengefaßt wird; entsprechend wird im neueren kriminologischen Sprachgebrauch der Begriff „Computer- oder (E)DV-Kriminalität" auch durch „IuK"-(Informations- und Kommunikations-)Kriminalität ersetzt.[1] Jedoch meint § 263 a hauptsächlich Sy-

[1] *BKA* (Hrsg.), Wirtschafts- und Computerkriminalität Mitteilungsblatt Nr. 1/97: Bericht zur IuK-Kriminalität 1996; *Sieber* ZStW **103** (1991) S. 779 (786 ff) und NJW **1989** 2569 ff.

steme der (elektronischen) Datenverarbeitung (unten Rdn. 22) und schließt rein mechanisch wirkende Geräte aus, da sonst § 265 a funktionslos würde.[2] Auch wird die Telekommunikation mittels Netzen, die öffentlichen Zwecken dienen, also die Gesamtheit der öffentlichen Datenübertragungssysteme, von § 265 a 2. Alt. geschützt (*Tiedemann* LK § 265 a Rdn. 24 mit Nachw.), soweit es um die Erbringung der Leistung der Nachrichtenübermittlung geht (näher unten Rdn. 59). Es erscheint daher vorzugswürdig, § 263 a weiterhin – mit seiner Überschrift – als *Computerbetrug* zu bezeichnen und so auf den Einsatz von DV-Systemen zum Zwecke rechtswidriger Erlangung von Vermögensvorteilen, die durch diese Systeme vermittelt werden, abzustellen. Ebenso werden die zugehörigen kriminologischen Erscheinungsformen im folgenden weiterhin als Computer- oder DV-Kriminalität bezeichnet. Diese Terminologie hat rechtlich zugleich den Vorteil, daß nicht die Information und Kommunikation, sondern das **Vermögen** als geschütztes Rechtsgut erscheint (näher dazu unten Rdn. 13 ff).

2 Die Notwendigkeit zur Einführung des § 263 a ergab sich aus dem zunehmenden Einsatz von Datenverarbeitungssystemen in allen Bereichen von Wirtschaft und Verwaltung, insbesondere auch zwecks Abwicklung des Zahlungsverkehrs bei Banken und der Abrechnungsvorgänge bei Versicherungen (vgl. bereits *Sieber* Computerkriminalität S. 16 ff). Derartige Systeme machen menschliche Entscheidungsprozesse ganz oder teilweise überflüssig und entscheiden automatisch, nämlich „selbsttätig" (vgl. AE § 202 Abs. 1). Ähnlich wie bei den mechanischen Leistungsautomaten (und den massenhaften Verkehrsleistungen) nach § 265 a (dazu *Tiedemann* LK Rdn. 2 ff) führt das Fehlen von entscheidungsbefugten oder Kontroll-Personen dazu, daß der allgemeine Betrugstatbestand nicht einzugreifen vermag, da dieser eine Täuschung und den *Irrtum eines Menschen*, also einen psychologischen Sachverhalt voraussetzt, der kausal zu einer Vermögensverfügung des Irrenden führen muß. Dabei kann im einzelnen zumindest zweifelhaft sein, inwieweit bei fehlender Entscheidungsmacht die bloße Kontrolltätigkeit natürlicher Personen noch eine Vermögensverfügung i. S. d. § 263 darstellt, wenn nur Formalien geprüft oder nur Stichproben vorgenommen werden (BTDrucks. 10/318 S. 18 f). Vor allem im Hinblick auf das von der ganz h. M. anerkannte Irrtumserfordernis bei § 263 ging es damit um die Schließung einer echten **Gesetzeslücke**,[3] während andere gesetzgeberische Neuerungen des (1. und des) 2. WiKG eher auf einer Neubewertung von Schutzinteressen beruhten und mehr praktisch als theoretisch bestehende Schwächen des allgemeinen Betrugstatbestandes ausgleichen sollten (vgl. nur *Tiedemann* LK § 264 Rdn. 5, § 264 a Rdn. 2). – Die Eigentumsstraftatbestände (§§ 242 ff) vermögen die beim Betrugstatbestand offenkundige Lücke regelmäßig nicht zu schließen, da Computermanipulationen häufig nichtkörperliche Tatobjekte wie Buch-(Giral-)Gelder, Geschäftsgeheimnisse, know-how oder sonstige Informationen betreffen (*Tiedemann* WM **1983** 1328 f) und diese entgegen *Haft* (DSWR **1979** 46 und **1986** 256) auch im Wege extensiver Auslegung nicht mehr unter den Sachbegriff des StGB gebracht werden können (*Tiedemann*

---

[2] Vgl. nur *Lackner/Kühl* Rdn. 4 mit Nachw.

[3] Begr. RegE BTDrucks. 10/318 S. 18 f; BT-Rechtsausschuß BTDrucks. 10/5058 S. 29; *Arloth* CR **1996** 363 f; *Arzt/Weber* IV Rdn. 65; *Berghaus* JuS **1990** 982; *Bühler* S. 71, 83 f, 97; *Cramer* JZ **1992** 1032; *Frommel* JuS **1987** 667; *Granderath* DB **1986** Beil. Nr. 18 S. 4; *Günther* SK Rdn. 3; *Haurand/Vahle* RDV **1990** 132; *Krey* 2 Rdn. 512 d, 512 h; *Lackner/Kühl* Rdn. 2; *Lenckner* Computerkriminalität S. 26, 34; *Lenckner/Winkelbauer* CR **1986** 654; *Maurach/Schroeder/Maiwald* 1 § 41 VI 1 Rdn. 227; *Otto* BT § 52 III 1 a, JR **1987** 225 und Jura **1993** 612; *Ranft* NJW **1994** 2574; *Richter* in Müller-Gugenberger § 34, 54; *Sch/Schröder/Cramer* Rdn. 1; *Sieber* Informationstechnologie S. 36 f; *Tiedemann* WM **1983** 1329 f und JZ **1986** 869; *Tröndle* Rdn. 1; *A. Weber* WM **1986** 1134 f.

Fernández Albor-Gedächtnisschrift S. 708; vgl. jetzt auch BVerfGE **92** 1, 16 f). Auch der Tatbestand der Untreue (§ 266) scheidet für Datentypisten (früher Locher), Programmierer, Operatoren sowie für betriebsfremde Personen in aller Regel bereits deshalb aus, weil es insoweit an der Selbständigkeit und Eigenverantwortlichkeit wirtschaftlichen Handelns sowie der Verpflichtungs- oder Verfügungsbefugnis fehlt (*Schünemann* LK § 266 Rdn. 109; *Tiedemann* WM **1983** 1330). Im Zuge der weiteren technischen Entwicklung dürfte sich mit der Ausbreitung von Telebanking, Teleshopping usw. sowie der Nutzung globaler Netze (Internet!) eine weitere Zunahme des Kreises externer Täter ergeben. Die Entwicklung hängt vor allem von der Einführung verschlüsselter digitaler Signaturen und sonstigen Fragen gesteigerter Sicherheit der Informationstechnik ab (*Tiedemann* Kaiser-Festschrift 1998).

3 Die Gesetz gewordene Fassung geht auf die Empfehlungen der Sachverständigenkommission zur Bekämpfung der Wirtschaftskriminalität aus dem Jahre 1976 zurück (BTDrucks. 10/318 S. 17) und läßt sich von der Überlegung leiten, daß umfassende wirtschaftsrechtliche Regelungen **präventiver** Art für die betroffenen Wirtschaftskreise nicht akzeptabel sind, nämlich die wirtschaftliche Tätigkeit unangemessen (und schwerer als durch Schaffung von Straftatbeständen) einengen könnten (BTDrucks. aaO S. 16). Diese Sicht des ultima ratio-Prinzips durch den RegE (und *Tiedemann* Tatbestandsfunktionen im Nebenstrafrecht, 1969, S. 145) hat die Zustimmung u. a. des XIII. Internationalen Strafrechtskongresses 1984 gefunden (vgl. *Tiedemann* JZ **1986** 866 u. Stree/Wessels-Festschrift, 1993, S. 530 f; **krit.** *Frey* S. 44 f mit weit. Nachw.). – Entsprechend den Empfehlungen der Kommission (Tagungsberichte Bd. XII S. 76 ff) und dem Vorschlag des RegE (BTDrucks. 10/318) knüpft der Straftatbestand mit seiner ersten und zweiten Alternative an **kriminologische** Einteilungen, nämlich an Programm- und Input-Manipulationen an (BTDrucks. 10/318 S. 18 f; 10/5058 S. 30). Insoweit hat der RegE durch die parlamentarischen Beratungen keine Veränderung erfahren. Die heutige vierte Alternative („sonst unbefugte Einwirkung auf den Ablauf" des DV-Vorgangs) war – ohne das Merkmal „unbefugt" und unter Bezugnahme nur auf den Ablauf des Programms – ebenfalls bereits im RegE enthalten; mit der Gesetz gewordenen Formulierung sollten neue Manipulationstechniken, z. B. Einwirkungen auf den maschinellen Ablauf oder zeitlichen Verlauf, auf den Datenfluß, vor allem auch Konsol- und Hardware-Manipulationen erfaßt werden (BTDrucks. 10/5058 S. 30). Neu eingefügt wurde im Gesetzgebungsverfahren schließlich als dritte Tatbestandsalternative die „unbefugte Verwendung von Daten". Mit ihr sollten wegen Zweifeln, ob insoweit eine Verwendung „unrichtiger" Daten vorliegt, vor allem der Mißbrauch von Geldautomaten (Bankomaten) und die unbefugte Benutzung eines fremden Anschlusses an das Bildschirmtextsystem (Btx-System) inkriminiert werden (BTDrucks. 10/5058 S. 30). – Mit diesen **Ausweitungen** ist allerdings die zunächst im Anschluß an die Vorschläge der Kommission vom RegE gewollte enge Anlehnung des § 263 a an den Tatbestand des Betruges und der alleinige Zweck der Schließung von Lücken, die bei Anwendung des Betrugstatbestandes auftreten würden (BTDrucks. 10/318 S. 19), aufgegeben worden. Zur Sicherstellung einer strikten Anbindung an § 263 und zur Vermeidung einer ungewissen Ausdehnung der Strafbarkeit war zuvor in der Literatur vorgeschlagen worden, anstelle der Schaffung eines neuen Sondertatbestandes nur § 263 selbst zu ergänzen.[4] Diesem Vorschlag ist der Gesetzgeber im wesentlichen deshalb nicht ge-

[4] *Haft* Prot. BT-Rechtsausschuß 10/26 v. 6. 6. 1984 S. 26/164; *Lenckner* Computerkriminalität S. 46 ff; *Sieber* Informationstechnologie S. 37.

folgt, weil neben dem zentralen Irrtumserfordernis auch andere personenbezogene Merkmale des § 263 bei Anwendung auf Computerhandeln einer teilweise anderen Interpretation als bei menschlicher Tätigkeit bedürfen (BTDrucks. 10/5058 S. 30): So „entspricht" der Verfügung nach § 263 bei § 263 a der Datenverarbeitungsvorgang (*Lenckner/Winkelbauer* wistra **1984** 88). Und bereits die „manipulative" Tathandlung löst sich zumindest teilweise von dem Modell inhaltlich unrichtiger Kommunikation, wie es § 263 bei dem Täuschungserfordernis zugrunde liegt (vgl. näher unten Rdn. 16 u. 44). Jedoch soll sich nach Ansicht des historischen Gesetzgebers die Auslegung des § 263 a „zu dessen Eingrenzung an der Auslegung des § 263 StGB ... orientieren" (BTDrucks. aaO).

Die **Kritik** an § 263 a ist insoweit verstummt, als sie sich gegen die grundsätzliche **4** Notwendigkeit einer strafrechtlichen Sonderregelung des Computerbetruges[5] richtete. Im Vordergrund stehen heute Bedenken und Zweifel, die zum einen und vor allem unter dem verfassungsrechtlichen Gesichtspunkt der *Unbestimmtheit* insbesondere der dritten Tatbestandsalternative (zusammenfassend *Lackner/Kühl* Rdn. 12 mit Nachw.), aber auch gegenüber der vierten Alternative (*Arzt/Weber* IV Rdn. 70; *Schl/Schröder/Cramer* Rdn. 12) geäußert werden. Insoweit hatten schon *Lenckner/Winkelbauer* (wistra **1984** 87 f) bei ihrem Vorschlag, die einschlägige Lücke im Vermögensstrafrecht bei der „Verschiebung" von Buchgeld durch Ergänzung des damaligen Entwurfes eines § 263 a zu schließen, auf das Erfordernis hingewiesen, im Gesetz zusätzliche Kriterien anzuführen, um nicht jede Pflichtverletzung im Innenverhältnis zum Grund einer „unbefugten" Datenverarbeitung zu machen (zust. *Schlüchter* S. 89 f). Nachdem der Gesetzgeber diesem Rat nicht gefolgt ist, werden einschlägige Argumente und Kriterien in großer Zahl diskutiert (näher dazu unten Rdn. 40 ff). Mit der Tendenz und Anerkennung einer *restriktiven Auslegung* lassen sie im Ergebnis aber den Vorwurf eines Verstoßes gegen Art. 103 Abs. 2 GG entfallen:[6] Die restriktive Normhandhabung zum Zwecke der Normerhaltung ist ein anerkanntes, wenn auch nicht unbestrittenes Mittel zur Vermeidung des Ergebnisses der Annahme von Normnichtigkeit wegen Unbestimmtheit (*Tiedemann* Tatbestandsfunktionen S. 38 ff, 186 ff mit weit. Nachw.).

Zum anderen wird in *kriminalpolitischer* Hinsicht gerügt, daß § 263 a insofern zu **5** weit geht, als bloße zivilrechtliche Vertragsverstöße berechtigter Kontoinhaber (bei Kontoüberziehung durch Benutzung von Bankomaten, vgl. unten Rdn. 50) in Frage stehen (vgl. bereits *Tiedemann* Fernández Albor-Gedächtnisschrift S. 701). Allerdings ist die Einbeziehung dieses als strafwürdig erachteten Falles (vgl. auch § 266 b!) vom Gesetzgeber ausdrücklich gewollt (*Möhrenschlager* wistra **1986** 133; *Tiedemann* JZ **1986** 869). Die Kritik weitet sich daher auch dahin aus, daß der Straftatbestand nicht einschränkend auf zumutbare *Sicherungsvorkehrungen* der Systembetreiber abstellt, wie es z. B. Art. 148 schweizer. StGB hinsichtlich des Mißbrauchs von Scheck- und Kreditkarten vorsieht (vgl. nur *Frey* S. 283; *Meurer* Kitagawa-Festschrift S. 978). Soweit damit viktimologische Gesichtspunkte eigenverantwortlichen Opferschutzes gemeint sind, kann für ihre Entkräftung auf *Tiedemann* LK § 265 b Rdn. 18 mit Nachw. verwiesen werden. Speziell für § 263 a geht es zu weit, bei Computermanipulationen im Vermögensbereich generell von einem hohen Opfer-Mitverschulden

---

[5] So neben *Haft* aaO vor allem auch *Tröndle* bei *Lenckner* Computerkriminalität S. 24, 37 f; ferner *Sieg* Jura **1986** 362; später *Frey* S. 183 ff.

[6] BGHSt. **38** 120 (122 mit Nachw.); *Bühler* S. 130, 134; *Cramer* JZ **1992** 1032; *Ehrlicher* S. 80 ff, 89; *Berghaus* JuS **1990** 982; *Günther* SK Rdn. 4 a. E.; *Lackner/Kühl* Rdn. 12; *Schlüchter* S. 94; *U. Weber* Krause-Festschrift S. 435; **krit.** aber *Haß* in Lehmann XII, 16; **aA** *Mitsch* JR **1995** 432; *Thaeter* JA **1988** 551.

zu sprechen (so aber *Sieg* Jura **1986** 362). Freilich ist es zutreffend, daß sich vor allem die Hersteller von EDV-Anlagen umfassenden Sicherheitsauflagen des Gesetzgebers widersetzt haben (*Sieber* Computerkriminalität S. 33 f), die aber der RegE vor allem in Form vollständiger Doppelkontrollen aller Daten als unpraktikabel und unökonomisch eingeschätzt hat (BTDrucks. 10/318 S. 16, 18; vgl. bereits oben Rdn. 3). Soweit *Sieber* (Informationstechnologie S. 40 ff) im Gesetzgebungsverfahren hinreichende Sicherung gegen Mißbrauch als Erfordernis des neuen Straftatbestandes forderte und hierfür „die Parallele zum bisherigen Betrugstatbestand" anführte, ist zu bedenken, daß jedenfalls das deutsche Betrugsstrafrecht auch sorglose Opfer schützt (vgl. dazu bereits *Peters* Eb. Schmidt-Festschrift [1961] S. 488 ff). Gerade eine restringierend an § 263 angelehnte Fassung des § 263 a (oben Rdn. 4) muß daher jedenfalls nicht zwingend engere Voraussetzungen der Strafbarkeit aufstellen, mögen solche auch für eine viktimodogmatische Auslegung diskutabel bleiben (vgl. unten Rdn. 14).

6 Unter *dogmatischen* Aspekten wird vor allem bemängelt, daß die vom Gesetzgeber historisch gewollte inhaltliche Anbindung an den allgemeinen Betrugstatbestand mißlungen sei.[7] Nach *Ranft* (NJW **1994** 2574) war es „bereits im Ansatz ein gesetzgeberischer Fehlgriff", eine Entsprechung zur Vermögensverfügung zu konstruieren, da es um einen Vermögensübergang „allein durch einen Zugriff" des Täters gehe. Auch nach *Otto* (BT § 52 III 1 a) unterscheidet sich § 263 a „grundlegend" von § 263, da der Computerbetrug Elemente der Eigentumsdelikte und der Untreue enthalte und folglich nur verbal betrugsähnlich konstruiert sei (zust. *Dannecker* BB **1996** 1288). In ähnlichem, zugleich kriminalpolitisch ausgerichteten Sinne hatte schon *Sieg* (Jura **1986** 362) darauf hingewiesen, daß § 263 a systemwidrig den Schutz des Vermögens gegen bestimmte Angriffsformen (List, Drohung, Vertrauensbruch) durch die bloße „Manipulierung der EDV-Anlage" ergänze. Ähnlich hatte auch *Tiedemann* (Fernández Albor-Gedächtnisschrift S. 708) in einem internationalen Rechtsvergleich gefragt, ob die bloße Tatsache der DV-Speicherung „eine so besondere Schutzbedürftigkeit der Information begründet, wie es das Strafrecht erfordert". Vor allem im praktischen Rechtsanwendungsvergleich zu § 266 wird deutlich, daß Täter unterhalb der für diesen Straftatbestand erforderlichen Schwelle besonderer Treupflichten durch § 263 a erfaßt werden, der damit eine Art „Computeruntreue" darzustellen scheint.[8] – Auf diese Bedenken und Hinweise, die nicht die Geltung, wohl aber die Legitimität und Einordnung des neuen Straftatbestandes in das Betrugssystem in Frage stellen, wird unten Rdn. 16 zurückzukommen sein. An dieser Stelle sei nur daran erinnert, daß auch andere Spezialtatbestände im Umfeld des Betruges nicht ohne weiteres in das Betrugsstrafrecht passen, vor allem weil und soweit dieses Lücken schließt, die aus der Beschränkung des Eigentumsstrafrechts auf körperliche Gegenstände folgen (vgl. *Tiedemann* LK § 265 a Rdn. 16 mit Nachw.). Auch sei schon hier erwähnt, daß der Reformgesetzgeber das Problem keineswegs übersehen hat: Der Bericht des Rechtsausschusses qualifiziert die Computermanipulation als **neue, zusätzliche Angriffsform** im System des Vermögensstrafrechts (BTDrucks. 10/5058 S. 30; näher unten Rdn. 13).

---

[7] *Frey* S. 183 f; *Krey* 2 Rdn. 512 g; *Maurach/Schroeder/Maiwald* 1 § 41 VI 3 Rdn. 236 mit Nachw.; *Ranft* NJW **1994** 2574; *Sch/Schröder/Cramer* Rdn. 2; *Tröndle* Rdn. 1 und 10; auch *Schlüchter* S. 85 f. Vgl. ferner die Angaben im folgenden Text.

[8] *Lenckner/Winkelbauer* wistra **1984** 88; *Sieber* Informationstechnologie S. 40; auch *Frommel* JuS **1987** 667; *Schünemann* LK § 266 Rdn. 110 und 167.

Die **praktische** Bedeutung des § 263 a ist beträchtlich, auch wenn der einschlägige Tatvorwurf in Fällen gleichzeitiger Verwirklichung des § 266 nicht selten über § 154 a StPO in Wegfall kommt. Innerhalb des Computerstrafrechts des StGB ist § 263 a das häufigste Computerdelikt (*Dannecker* BB **1996** 1288 mit Nachw.). Allerdings wird der hohe statistische Ausweis (Polizeiliche Kriminalstatistik 1996 S. 250 f: 32128 Fälle; Strafverfolgungsstatistik 1996: 1742 Verurteilungen) zu mehr als ⅘ (PKS 1996: 26802 Fälle) durch Bankomatenmißbräuche begründet, die jedenfalls seit BGHSt. **38** 120 allein durch § 263 a erfaßt werden (vgl. unten Rdn. 47 ff). Einen erheblichen Anteil der sonstigen Fälle des § 263 a machten bis vor einigen Jahren die Geldspielautomatenmißbräuche aus (*Bühler* S. 9; *Möhrenschlager* wistra **1991** 322, je mit Nachw.). Die Polizeiliche Kriminalstatistik trennt daher zutreffend vor allem die Bankomatenfälle vom „Computerbetrug im engeren Sinne". Zu diesem wird aus Rechtsgründen ebenfalls nicht der – statistisch erhebliche – Mißbrauch von (gestohlenen oder gefälschten) Kreditkarten sowie von Calling Chip-Cards (T-Cards) gerechnet (*Dannecker* BB **1996** 1288 mit Nachw.); der erstgenannte Bereich fällt unter § 263, der zweite unter § 265 a (*Bandekow* S. 295; näher zur strafrechtlichen Einordnung des sonstigen Mißbrauchs von Telekommunikationsanlagen, dem sog. Phreaking, unten Rdn. 59). Die praktisch ebenfalls gewichtige Verfälschung von Computer-Prozessoren stellt im Falle des Vertriebs einen Warenbetrug i. S. d. § 263 dar. Nicht unerheblich, aber von der offiziellen Statistik zu § 263 a wiederum nicht gesondert ausgewiesen sind der Mißbrauch von sonstigen Magnetstreifenkarten (Tankkarten, Kunden- und Devisenkarten usw.) sowie Chipkarten nach Art der bei Banken oder am Heim-PC aufladbaren (z. B. W-Sparkassen-)Multicards („elektronische Geldbörse") und die zum Nachteil der Telekom oder von Telefonkunden erfolgenden Praktiken der Geldschöpfung, z. B. mittels Manipulationen des Telefonnetzes als Mittel zur Abrechnung der Dienstleistungen von Südsee-Sex-Telefonen (*Dannecker* aaO: „neue Welle von Computermanipulationen"). – Für die eigentliche Computerkriminalität sieht *Paul* (NJW-CoR **1995** 42) heute insgesamt zu 99% den Bereich der PCs und der PC-Netze als betroffen an, während früher eher Großrechner und die mittlere Datentechnik im Vordergrund standen. Außerhalb des Bereichs der Bankomatenmißbräuche bezeichnet *Möhrenschlager* (aaO S. 323) als **Täter** überwiegend Angestellte des geschädigten Unternehmens und der geschädigten Verwaltung, und zwar Sachbearbeiter und DV-Personal. Vgl. dazu aber auch oben Rdn. 2 a. E. 7

Ausländische Regelungen und internationale Empfehlungen haben für die Handhabung des § 263 a besonderes Gewicht, weil vor dessen endgültiger Gestaltung durch den Gesetzgeber umfangreiche Erhebungen zu den im Ausland getroffenen oder geplanten strafrechtlichen Regelungen der Computerkriminalität vorgenommen wurden (vgl. nur *Möhrenschlager* wistra **1986** 129 f). Der deutsche Straftatbestand ist also eng in eine zeitlich und sachlich parallele internationale Reformbewegung eingebunden. Die Regelungsmodelle, die sich dabei herausbildeten, lassen die Rechtsnatur, aber auch Vor- und Nachteile des § 263 a deutlicher hervortreten als bei isolierter Betrachtung. – Eine wesentliche Sorge des deutschen Gesetzgebers war es, mit der bloßen Schließung einer Lücke des Betrugstatbestandes nicht alle von der Kommunikationstechnik ermöglichten strafwürdigen Manipulationen zu erfassen; dem stand die Befürchtung gegenüber, durch eine weite Gestaltung des Straftatbestandes auch Fälle einzubeziehen, die nicht strafwürdig sind (vgl. bereits oben Rdn. 3). Diese doppelte Skepsis findet in ausländischen Reformdiskussionen ihre 8

Entsprechung.[9] Übrigens hat die deutsche Regelung des 2. WiKG auch ihrerseits ausländische Reformen angeregt (z. B. § 246–2 **japan**. StGB in der Fassung von 1987, vgl. *Sonoda* wistra **1988** 167 ff mit einer allerdings nicht mangelfreien Übersetzung des japanischen Straftatbestandes; die Bankomaten-Fälle werden in Japan aber weiterhin über den Diebstahlstatbestand erfaßt).

9 Die möglichen Regelungsmodelle werden bereits in den wichtigsten **internationalen** Vorschlägen und Empfehlungen sichtbar. So definiert der **OECD**-Bericht von 1986 den Computerbetrug ohne Erfordernis einer Täuschung, eines Irrtums, einer Vermögensverfügung und eines Vermögensschadens in Anlehnung an die kriminologischen Erscheinungsformen (*Sarzana* S. 59) als Eingabe, Änderung, Löschung und/oder Unterdrückung von Computerdaten und/oder Computerprogrammen in der (bloßen!) Absicht einer rechtswidrigen Übertragung von Geldmitteln oder anderen Vermögensvorteilen.[10] Stärker an kontinentale Vorstellungen vom Betrug angelehnt ist die Empfehlung R (89) 9 des **Europarates** von 1989, die bei identischer Handlungsumschreibung objektiv eine Vermögensschädigung fordert, allerdings für den subjektiven Tatbestand den nationalen Gesetzgebern die Möglichkeit offen hält, anstelle der Absicht, sich oder einem Dritten einen rechtswidrigen wirtschaftlichen Vorteil zu verschaffen, auf die Absicht abzustellen, dem anderen rechtswidrig sein Vermögen zu entziehen.[11] Dem haben sich die Empfehlungen der **Association Internationale de Droit Pénal** (AIDP) von 1994 im wesentlichen, aber unter Betonung des Vorranges eines bestimmt gefaßten objektiven Tatbestandes, angeschlossen.[12]

10 Für die erforderliche legislatorische Umsetzung der überwiegend neutralen Formeln von der Einwirkung auf oder Verwendung von Daten lassen diese internationalen Einschätzungen und Stellungnahmen ansatzweise erkennen, daß zur Erfassung des Computer„betruges" entweder ein **Betrugs- oder** aber ein **Diebstahlsmodell** gewählt werden kann. Ersteres steht vor allem vor der Schwierigkeit, wie die Täuschungshandlung umschrieben bzw. ersetzt werden soll, und nähert sich bei Verwendung von Merkmalen wie „unecht", „unbefugt" usw. (wie z. B. auch in Art. 640*ter italien.* Codice Penale und Art. 147 *schweizer.* StGB, das zusätzlich noch Analogie vorsieht)[13] Zurechnungslösungen aus dem Urkunden- und Untreuestrafrecht an. Das zweitgenannte (Diebstahls-)Modell stellt vor die Notwendigkeit, die Tatobjekte auf nichtkörperliche Gegenstände auszudehnen (wie es das *englische* Strafrecht allgemein schon im Theft Act 1968 Art. 4 statuiert: „Property includes ... intangible property", und es das *US*-Strafrecht teilweise speziell für Computerdaten definiert).[14] Daneben existieren abgewandelte Betrugsmodelle, z. B. in Art. 1 Übereinkommen zum Schutz der finanziellen Interessen der EG von 1995:[15] Die Täuschungshandlung wird – im Sinne unrichtiger Erklärungen – durchaus traditionell gestaltet, dagegen von einem Irrtumserfordernis ganz abgesehen und der Schaden relativiert bzw. normativiert (vgl. *Tiedemann* LK § 264 Rdn. 10). Damit dürfte Art. 1 des Übereinkom-

---

[9] Breite Übersicht in der Sammelveröffentlichung von *Sieber* (Hrsg.), Information Technology Crime – National Legislations and International Initiatives (Köln 1994); ferner *Sarzana* S. 127 ff.

[10] *OECD* Computer-Related Criminality – Analysis of Legal Policy in the OECD-Area (1986).

[11] *Council of Europe* Computer-Related Crime (1990).

[12] *Tiedemann/Möhrenschlager* ZStW **108** (1996) S. 688 (697).

[13] Dazu näher *Hurtado Pozo* Droit pénal Partie spéciale I (3. Aufl. Zürich 1997) § 40, 1058; *Schmid* § 7, 77 ff. Zur Entstehungsgeschichte *Frey* S. 234 f.

[14] *Wise* Revue Internationale de Droit Pénal **1993** 647 (661 f).

[15] ABlEG Nr. C 316/48 v. 27. 11. 1995; dazu bereits *Tiedemann* LK § 264 Rdn. 10 mit weit. Nachw.

mens den Computerbetrug (zum Nachteil von EG-Vermögen) ohne weiteres einschließen, wobei der Verzicht auf das Irrtumserfordernis mit Schwerpunktsetzung bei der Täuschungshandlung englisch-französischer Tradition entspricht (die übrigens auch im *spanischen* Schrifttum vor der Reform von 1995 zu der Frage geführt hatte, ob nicht die Beschränkung des spanischen Betrugstatbestandes auf bloße Täuschungseignung einen eigenen Tatbestand des Computerbetruges überflüssig mache[16]). Als erheblich abgewandeltes Betrugsmodell muß auch Art. 248 Abs. 2 span. Código Penal eingestuft werden, der in unmittelbarem Anschluß an den Betrugstatbestand darauf abstellt, daß die nicht vom Einverständnis (!) des Berechtigten gedeckte Übertragung eines Vermögenswertes erreicht und dadurch eine Person geschädigt wird; Abs. 1 stellt demgegenüber für den allgemeinen Betrugstatbestand darauf ab, daß der Getäuschte eine Verfügung zum eigenen oder zum Schaden eines anderen vornimmt.

Ein zusätzliches Gesetzgebungsmodell wird im anglo-amerikanischen Recht sicht- **11**
bar, wenn als Basisunrecht („baseline offence")[17] der „unauthorized access to computer material" pönalisiert und durch zusätzliche Merkmale – z. B. zum computer fraud – qualifiziert wird (so z. B. der *englische* Computer Misuse Act 1990; zum statute law US-amerikanischer Bundesstaaten *Gutiérrez* S. 128 ff). Hier ist der Computerbetrug Unterfall des Täter**zugriffs** auf fremdes Vermögen, das gegen den Zugriff (nur) dadurch gesichert ist, daß die Daten „held in any computer" sind (Art. 1 litt. a Computer Misuse Act). Der Zusammenhang mit „data privacy" und „data integrity" und damit die Gesamteinordnung in ein Strafrecht zum Schutz von (Persönlichkeits- und Betriebs-)Geheimnissen ist evident. Nach *Wise* wird hier „exclusive access" zum geschützten Rechtsgut und zu „a form of property";[18] *Gutiérrez* (S. 130) sieht dagegen Funktion und Sicherheit der Computeranlagen als geschützt. Unter den kontinentaleuropäischen Rechtsordnungen folgt vor allem *Frankreich* diesem Trend, indem Art. 323–1 ff Code Pénal 1994 den Computermißbrauch völlig vermögens- und schadensunabhängig definieren (*Gutiérrez* S. 185) und damit einen nur indirekten Vermögensschutz etablieren.[19] Art. 323–1 betrifft den „fraudulösen" Zugang zu (und „Aufenthalt" in) einer DV-Anlage, wobei es auf eine Zugangssperre nicht ankommt und auch der sog. Zeitdiebstahl erfaßt wird.[20] Daneben fallen unkörperliche Gegenstände wie z. B. Dienstleistungen zwar nicht unter den Diebstahls-, wohl aber unter den Unterschlagungstatbestand des französischen Rechts.[21]

Das deutsche Computerstrafrecht, das bekanntlich auf einen eigenen Straftatbe- **12**
stand des Eindringens oder *hacking* verzichtet (vgl. aber *Tiedemann* JZ **1986** 868), steht dieser Entwicklung geradezu konträr gegenüber und lehnt sich an die klassischen Straftatbestände des Betruges, der Urkundenfälschung und der Sachbeschädigung an.[22] Dem folgen und entsprechen andere Strafgesetzbücher innerhalb und außerhalb der Europäischen Union, insbesondere in den nordischen Staaten.[23] Eine

---

[16] *Gutiérrez* S. 404 ff; ablehnend insoweit aber das spanische Tribunal Supremo bei *Tiedemann* Lecciones de Derecho Penal Económico (Barcelona 1993) S. 51. Näher zur Täuschungshandlung nach spanischem Recht *Pérez Manzano*, in: Schünemann/Suárez González (Hrsg.), Bausteine des europäischen Wirtschaftsstrafrechts (1994) S. 213 (217 ff).

[17] *Wise* aaO (o. Fußn. 14) S. 661.

[18] *Wise* aaO.

[19] *Francillon* Revue Internationale de Droit Pénal **1993** 291 (306); *Pradel/Danti-Juan* Droit pénal spécial (Paris 1995) Nr. 779 S. 540.

[20] *Pradel/Danti-Juan* Nr. 930 S. 642.

[21] *Pradel/Danti-Juan* Nr. 779 S. 540 mit Nachw. zur Rechtsprechung der Cour de Cassation.

[22] *Lenckner/Winkelbauer* CR **1986** 654 f; *Möhrenschlager* wistra **1991** 325.

[23] Übersicht bei *Sarzano* S. 253 ff und *Sieber* International Handbook S. 197 ff. – Schweden (1986), Norwegen (1987) und Finnland (1990) regeln den Computerbetrug in Abs. (bzw. Nr.) 2 des Betrugstatbestandes, während Dänemark (1985) einen Sondertatbestand eingeführt hat (Text der Straftatbestände bzw. Entwürfe bei *Sarzano* S. 127 f, 131, 293 ff und *Sieber* aaO).

dem Betrug nahe, aber eigenständige Variante bietet Art. 148 a des *österreichischen* StGB, das als „betrügerischen Datenverarbeitungsmißbrauch" die (nicht notwendigerweise: unrichtige, unvollständige oder unbefugte) Programmgestaltung, Eingabe, Veränderung oder Löschung von Daten sowie die Einwirkung auf den Ablauf des Verarbeitungsvorgangs pönalisiert, sofern dies zu einer Ergebnisbeeinflussung und Vermögensschädigung führt. Diese hinsichtlich der Handlungsumschreibung neutrale Formulierung bedarf allerdings einer Konkretisierung im Wege der Interpretation.[24]

13 **II. Geschütztes Rechtsgut und allgemeine Einordnung des Tatbestandes.** Die ganz h. M. sieht entsprechend der Entstehungsgeschichte des § 263 a (oben Rdn. 3) ebenso wie bei § 263 ausschließlich das **Vermögen** als geschütztes Rechtsgut an.[25] Das Allgemeininteresse am Funktionieren und an der Sicherheit der in Wirtschaft und Verwaltung eingesetzten DV-Systeme wird als bloßer Schutzreflex bezeichnet.[26] Dem entspricht es, daß § 269 als selbständige Abspaltung vom strafrechtlichen Vermögensschutz die Sicherheit und Zuverlässigkeit des Beweisverkehrs mit Daten schützt,[27] die überindividuelle Sicherheitskomponente also – wie beim allgemeinen Betrugstatbestand – in das Urkundenstrafrecht verwiesen ist. Die Benutzung von Computern zur Begehung eines Betruges wird bei dieser Sicht zu einer reinen Frage des *Tatmittels*. Dies führt folgerichtig zu einer *Ausweitung der Angriffsformen* des Vermögensstrafrechts von der Täuschung und Drohung (sowie Gewalt und Treuwidrigkeit) auf das Mittel des Einsatzes von DV-Anlagen bzw. von computergespeicherten Daten (BTDrucks. 10/5058 S. 30; BayObLG NJW **1991** 438, 440; oben Rdn. 6). Wenn *Frey* (S. 183) meint, auch bei § 263 a gehe es insgesamt um „List", so ist dies zwar als Aussage richtig oder doch möglich, entkleidet aber dieses Merkmal des bei § 263 unstreitigen kommunikativen Bezuges der Täuschung (!) auf Menschen. Auch die „materielle Unwahrheit" (*Frey* aaO) ist vor allem in Abgrenzung zu den Urkunden-, aber auch Bilanz- und anderen Fälschungsdelikten zu allgemein, um betrugsspezifische Tathandlungen zu kennzeichnen. Die Daten und/oder die ihnen entsprechenden Informationen sind damit – anders als im US-amerikanischen Recht (oben Rdn. 11) – nicht einmal Tatobjekt des § 263 a. Im System des Eigentums- und Vermögensstrafrechts zeigt dies – neben dem Fälschungsschutz des § 269 – der wiederum verselbständigte Bestandsschutz der §§ 303 a, 303 b. Schließlich scheint die Nichtaufnahme des überindividuellen Sicherheitsaspektes in die Rechtsgutsbestimmung des Computerbetrugs auch durch die Annahme gestützt zu werden, daß andernfalls auch beim allgemeinen Betrugstatbestand neben dem Vermögen Verkehrsprinzipien wie das von Treu und Glauben als Schutzgut angesehen werden müßten.

---

[24] *Kienapfel* Strafrecht Bes. Teil II (3. Aufl. 1993) § 148 a Rdn. 20, 22; *Leukauf/Steininger* Kommentar zum StGB (3. Aufl. 1992) § 148 a Rdn. 12, 19 ff mit weit. Nachw.

[25] BGHSt. **40** 331 (334); *Arzt/Weber* IV Rdn. 66; *Frey* S. 183; *Frommel* JuS **1987** 667; *Gössel* 2 § 22, 1; *Gogger* S. 49; *Günther* SK Rdn. 4; *Haft* NStZ **1987** 7; *Haß* in Lehmann XII, 6 S. 469; *Krey* 2 Rdn. 512 c; *Lackner/Kühl* Rdn. 1; *Maurach/Schroeder/Maiwald* 1 § 41 VI 1 Rdn. 227; *Otto* BT § 52 III 1 b; *Ranft* NJW **1994** 2574; *Rengier* 1 § 14, 1; *Schlüchter* S. 85; *Schulz* JA **1995** 540; *Tröndle* Rdn. 2.

[26] *Haß* aaO; *Krey* aaO; *Lackner/Kühl* aaO; *Otto* aaO und Jura **1989** 33; *Tröndle* aaO. – Nach *Otto* (JR **1987** 225) wird der Schutz des **bargeldlosen Zahlungsverkehrs** in § 263 a „miterfaßt, hat aber keine eigenständige Bedeutung neben dem Vermögensschutz" (weitergehend insoweit *Bandekow* S. 301 ff).

[27] *Lackner/Kühl* § 269 Rdn. 1; *Möhrenschlager* wistra **1991** 326; *Sch/Schröder/Cramer* § 269 Rdn. 4; *Tröndle* § 269 Rdn. 2.

Diese Sichtweise wird allerdings dann relativiert, wenn berücksichtigt wird, daß **14** die Lücke bei § 263 nicht nur durch das Fehlen eines Irrtums der DV-Anlage, sondern innerhalb des Eigentums- und Vermögensstrafrechts insgesamt auch und vor allem durch die Nichteinbeziehung nichtgegenständlicher Objekte und Werte in §§ 242 ff bedingt ist. Wenn daher für das Eigentumsstrafrecht anerkannt wird, daß neben dem Eigentum auch der Gewahrsam rechtlich geschützt ist,[28] liegt es jedenfalls bei wertender Herausnahme des § 263 a aus dem Vermögensstrafrecht und Zuordnung zum Eigentumsstrafrecht (dazu sogleich Rdn. 16) nahe, in Anlehnung an die oben Rdn. 11 dargestellte Auffassung des anglo-amerikanischen Rechtssystems die Befindlichkeit der Daten in einer DV-Anlage nicht als zufällig oder nebensächlich anzusehen. Es kommt hinzu, daß entgegen häufigen Formulierungen nicht diese Daten, sondern erst die ihnen zugrunde liegenden Informationen den Tatsachen bei § 263 entsprechen.

Ebenso wie § 263 ist auch § 263 a vom Gesetzgeber als **Erfolgsdelikt** (Vermögens- **15** beschädigung! vgl. nur *Gössel* 2 § 22, 2) und nach wohl überwiegender Auffassung auch als *Vermögensverschiebungs*delikt mit dem Erfordernis der Stoffgleichheit zwischen eingetretenem Schaden und beabsichtigtem Vorteil (unten Rdn. 76) konstruiert (*Arzt/Weber* IV Rdn. 69). Die möglicherweise zusätzlich anzunehmende überindividuelle Schutzkomponente (soeben Rdn. 14) ändert hieran nichts.

Ob § 263 a entsprechend dem Willen des Gesetzgebers ein **betrugsähnliches** Delikt **16** ist, erscheint aus den schon oben Rdn. 6 angeführten Gründen zweifelhaft. Allerdings ist der Untreue-Aspekt auf Täter beschränkt, denen eine Befugnis im Verhältnis zum Vermögensinhaber eingeräumt ist, betrifft also nicht externe Täter, die sich unter Überwindung von Sperren Zugang zu dem Vermögen verschaffen. Daß im ersteren Fallbereich bei entsprechender Höhe und Weite der Befugnis Idealkonkurrenz mit § 266 auftreten kann, stellt keine Besonderheit dar (zutr. *Lenckner/Winkelbauer* CR **1986** 655). Gravierender ist der Einwand, daß die in der Codierung liegende und häufig weiter (z. B. durch Paßwörter oder andere Zugangssperren) qualifizierte Sperre vom – jedenfalls externen – Täter durch Anwendung von List überwunden oder ausgeschaltet wird und damit eher ein „von außen kommender" Zugriff auf fremdes Vermögen als eine (durch List und Verfügung des Computers erreichte) Inempfangnahme von Vermögenswerten vorliegt (*Ranft* NJW **1994** 2574; auch *Mitsch* JZ **1994** 884). Besonders deutlich wird dies, wenn erschlichene Paßwörter dazu benutzt werden, um Leistungen wie z. B. Auskünfte oder Computerprogramme widerrechtlich abzurufen. Ähnlich wie bei § 265 a (dazu *Tiedemann* LK Rdn. 16) erscheint die Tat dann eher als ein Leistungsentziehungs- denn als Betrugsdelikt. Maßgebend für die Strafbarkeit nach § 263 a werden bei einer solchen Sicht Gesichtspunkte des (subjektiven) Willens und Einverständnisses des Systembetreibers, was freilich die Integration der deutlich betrugsähnlichen zweiten Tatbestandsalternative vor Schwierigkeiten stellt.

Überzeugend wäre dies freilich nur, wenn die **Funktion des Computers** auf die eines bloßen Hilfsmittels menschlicher Tätigkeit und einer eher mechanischen Sperre, die als Sphäre gespeicherter Daten das Vermögen gegen fremden Zugriff sichert, beschränkt werden könnte. Davon kann aber nicht die Rede sein. Zwar geht es zu weit, zwischen elektronischer Datenverarbeitung und menschlichen Denk- und

---

[28] *Lackner/Kühl* § 242 Rdn. 1; *Ruß* LK Rdn. 3 vor § 242; *Schl/Schröder/Eser* § 242 Rdn. 2; *Tröndle* § 242 Rdn. 1, je mit weit. Nachw.

Entscheidungsvorgängen technologisch-kybernetisch mehr oder weniger vollständige Parallelen herzustellen (so aber insbesondere *Hilgendorf* JuS **1996** 510, der daher die künftige Existenzberechtigung des § 263 a für zweifelhaft hält). Denn da Computer weder Bewußtsein noch Vorstellung von der Wirklichkeit haben, kann die Beeinflussung des Ergebnisses einer Datenverarbeitung weder ontologisch noch wertungsmäßig mit einem Irrtum gleichgesetzt werden (vgl. auch unten Rdn. 26, 65). Deshalb sind auch Versuche, statt an die Daten*manipulation* und deren *Täuschungs*ähnlichkeit an hypothetische *Irrtums*konstellationen anzuknüpfen (vgl. unten Rdn. 49), ebenso problematisch wie der Versuch, § 263 a auf Einwirkungen auf Datenverarbeitungsvorgänge von besonderer Wichtigkeit zu beschränken, welche dem Hervorrufen eines Irrtums bei einem Menschen vergleichbar sind (vgl. unten Rdn. 22). Gleichwohl gingen Vorstellung und Wille des historischen Gesetzgebers nicht von (primitiven) Sperren, sondern von (hoch)komplexen und wenn auch von Menschen programmierten, so doch selbsttätig wirkenden Anlagen (oben Rdn. 2) aus. Insofern begründet zum einen das äußere Bild einer selbsttätigen Weggabe und einer selbständigen vermögensrelevanten Entscheidung, also die bei § 263 a vorausgesetzte **Verfügungsähnlichkeit** der Computerfunktion, die Betrugsähnlichkeit des § 263 a. Zum anderen beruht die Verfügung auf einer Dateneingabe und -verwendung mit manipulativem Charakter. Insofern ist die **Täuschungsähnlichkeit** des Täterverhaltens der Schlüssel insbesondere für die bei der dritten Alternative erforderliche „restringierende" Auslegung:[29] In hinreichender Loslösung von dem menschlichen Interaktionsprozeß muß die Betrugsähnlichkeit des Gesamtverhaltens gewürdigt werden, wobei auch die Manipulation der sächlichen Umwelt – also die für § 263 irrelevante Objektsveränderung – der Handlung und ihrer Bewertung das Gepräge gibt (näher unten Rdn. 44). Daß dies vor allem im Bereich konkludenter Täuschungen zu Unsicherheiten führt,[30] muß ebenso wie bei § 263 in Kauf genommen, kann aber wie dort durch Heranziehung normativ verfestigter Erwartungen und Berücksichtigung des jeweiligen Geschäftstyps konkretisiert werden. Im übrigen betrifft die „Betrugsäquivalenz" freilich entgegen *Günther* (SK Rdn. 4) und *Sch/Schröder/Cramer* (Rdn. 2) nicht alle Tathandlungen des § 263 a, sondern nur diejenigen, die eine Parallele in dem Täuschungsverhalten gegenüber Menschen finden, also insbesondere nicht die erste und die vierte Alternative (zutr. *Lampe* JR **1988** 438; *Wessels* BT-2 Rdn. 575; dazu unten Rdn. 32). Die übrigen Tathandlungen können demgegenüber gerade wegen ihrer Verselbständigung durchaus zu einer Ausdehnung der Strafbarkeit im Vergleich zu § 263 führen; dies ist Folge der vom Gesetzgeber gewollten Erweiterung des strafrechtlichen Vermögensschutzes um eine zusätzliche Angriffsform. Zugleich muß damit die oben Rdn. 14 diskutierte überindividuelle Schutzkomponente endgültig aus § 263 a ausgeschieden werden: Anders als §§ 264, 264 a, 265, 265 b zielt dieser Straftatbestand – ähnlich wie § 263 und § 265 a – allein auf Vermögensschutz und betont auch nicht den instrumentalen Wert von Computern als heute unerläßlichen Mitteln der Wirtschaft und Verwaltung (weitergehend AE BT § 202 Begr. S. 111): Die „Manipulation" von Daten und Informationen ist Tatmittel und löst sich bei den meisten Tatbestandsalternativen des § 263 a in schlichte Unrichtigkeit oder Unwahrheit auf; die Sicherheit der DV-Anlagen bleibt damit im Sinne der ganz h. M. bloßer Reflex

[29] So vor allem OLG Köln NJW **1992** 125, 126; *Arzt/Weber* IV Rdn. 79; *Günther* SK Rdn. 4 mit Nachw. und Rdn. 5; *Lackner* Tröndle-Festschrift S. 53 ff; *Schlüchter* NStZ **1988** 59; *Sch/Schröder/Cramer* Rdn. 2; *Tröndle* Rdn. 8; *Wessels* BT-2 Rdn. 576. Näher unten Rdn. 40 ff, aber auch Rdn. 49.

[30] *Gössel* 2 § 22, 16; *Hilgendorf* JuS **1997** 132; *Ranft* NJW **1994** 2575.

des Vermögensschutzes in diesem Bereich. Allerdings führt die bereits oben Rdn. 3 a. E. erwähnte und unten Rdn. 44 a. E. näher behandelte sächliche Manipulation (des Programms, der Konsole, der Hardware usw.) zu einem **Handlungsunwert** (zutr. *Wessels* BT-2 Rdn. 580 a. E.), welcher der (ausdrücklichen) Täuschung beim Betrug entspricht.

§ 263 a ist nicht nur materiellrechtlicher *Auffangtatbestand* im Verhältnis zu § 263, **17**
dessen Lücken er schließen soll (vgl. allerdings auch Rdn. 74), sondern – vorbehaltlich des Rdn. 22 erwähnten Unmittelbarkeitsgrundsatzes – zugleich **Sondervorschrift** im Verhältnis zu anderen das Eigentum und Vermögen schützenden Straftatbeständen, die durch den Sondertatbestand ausgeschlossen werden.[31] Greift infolge Täuschung natürlicher Personen der allgemeine Betrugstatbestand (oder z. B. § 264) ein, so tritt § 263 a im Hinblick auf seine Lückenfüllungsfunktion schon aus Tatbestandsgründen zurück. Zweifelhaft kann dies nur in den Fällen sein, in denen zwar ein Mensch getäuscht wird, diese Täuschung aber zu keinem Vermögensschaden führt; in diesen Fällen kann die Manipulation des Computers einen Vermögensschaden des Betreibers begründen, insbesondere wenn dieser dem Getäuschten die Zahlung garantiert (vgl. unten Rdn. 52).

III. Täterkreis. § 263 a ist nach unbestrittener Ansicht **kein Sonderdelikt**. Täter **18**
kann also jedermann sein (vgl. nur *Sch/Schröder/Cramer* Rdn. 39), auch wenn faktisch insbesondere die Programm- und Ablaufmanipulationen der ersten und vierten Alternative regelmäßig nur von Programmierern, Operatoren und anderen Personen mit spezieller Sachkunde und Zugang zu dem DV-System, also gleichsam von innen, begangen werden können (*Tröndle* Rdn. 4). Eine rechtliche Beschränkung auf betriebsangehörige Personen wird aber von keiner Tatbestandsalternative des § 263 a vorausgesetzt (zutr. *Sch/Schröder/Cramer* aaO), so daß auch die bei Entstehung des Straftatbestandes eher im Hintergrund stehende Täterschaft außenstehender Personen rechtlich möglich ist und einschlägig bleibt (*Tiedemann* Kaiser-Festschrift 1998; *Tröndle* aaO). Einzelfragen sind bei den einzelnen Tatbestandsalternativen, z. B. im Hinblick auf die Tathandlung des „Verwendens" unrichtiger oder unvollständiger Daten, zu klären (unten Rdn. 23 ff).

IV. Die Tathandlungen und ihr Gegenstand

1. Daten und Datenverarbeitung. Das Gesetz verwendet beide Begriffe ohne Defi- **19**
nition; diejenige des § 202 a Abs. 2 ist wegen ihrer ausdrücklichen Bezugnahme auf Abs. 1 und der fehlenden Verweisung auf § 202 a in § 263 a (anders § 303 a!) hier nicht anwendbar (vgl. bereits Rdn. 1). Für den Begriff des Datums muß daher auf allgemeine Begriffsbestimmungen zurückgegriffen werden. Die des § 3 Abs. 1 BDSG („Einzelangabe") ist zu weit und betrifft jede Information (*Schulze-Heiming* S. 23 f mit Nachw.). Demgegenüber legt die bereits oben Rdn. 1 mitgeteilte Begr. des RegE jedenfalls eine Anknüpfung an § 202 a Abs. 2 nahe. Auch der technische Sprachgebrauch von DIN-Normen ist für das Begriffsverständnis einschlägig (*Schulze-Heiming* S. 20 ff mit Nachw.).

---

[31] BayObLGSt. **1986** 127, 130; *Arzt/Weber* IV Rdn. 77; *Cramer* JZ **1992** 1032; *Gössel* 2 § 22, 40; *Günther* SK Rdn. 24; *Krey* 2 Rdn. 513 d; *Sch/Schröder/Cramer* Rdn. 26; *U. Weber* JZ **1987** 215 f und Küchenhoff-Gedächtnisschrift S. 488 f; *Wessels* BT-2 Rdn. 584; **aA** insbes. *Ranft* JuS **1997** 22 f.

20 **a) Daten** lassen sich als Darstellungen (Repräsentation) von Informationen kennzeichnen, wobei die Darstellung durch Zeichen oder kontinuierliche Funktionen erfolgt (vgl. DIN-Norm 44300–2, deren Hervorhebung des Verarbeitungszwecks aber für § 263 a nicht zwingend ist und seit der Ausgabe 1988–11 zu nur noch „vorrangig" abgeschwächt wird).[32] Unerheblich ist, ob die Informationen in das Ergebnis des jeweiligen Verarbeitungsvorgangs eingehen sollen oder ob sie für andere Zwecke, z. B. zur Kontrolle der Funktion der DV-Anlage oder zur Abschirmung gegen das Eindringen Unbefugter (z. B. Paßwörter!), bestimmt sind (*Möhrenschlager* wistra **1986** 132; *Lackner/Kühl* Rdn. 3). Auch Computer*programme*, nämlich Arbeitsanweisungen an den Computer (vgl. DIN-Norm 44300–4, Ausgabe 1988–11), sind aus Daten zusammengefügt und daher selbst (ein Inbegriff von) Daten.[33]

21 Erhebliche Bedeutung für die Bestimmung der Strafbarkeit hat die meist nicht ausdrücklich diskutierte (und von BGHSt. **40** 331, 334 offen gelassene) Frage, ob die Daten **kodiert** oder nur **kodierbar** sein müssen. So verneint OLG Köln NJW **1992** 125, 127 (mit Anm. *Otto* JR **1992** 252 ff) den Tatbestand des § 263 a bei auftragswidriger Verwendung einer fremden ec-Karte mit der Begründung, die Eingabe des durch den Bankomaten auszuzahlenden Geldbetrags sei mangels Kodierung und Fixierung der Information auf einem Datenträger keine Verwendung von „Daten" (**aA** z. B. *Huff* NJW **1987** 817); die überwiegende Ansicht sieht hierin dagegen erst eine Frage der Unbefugtheit (der Verwendung von Daten, vgl. Rdn. 50). BayObLG NJW **1991** 438, 440 (mit Anm. *Neumann* JR **1991** 302 ff) erblickt demgegenüber bei dem gezielten Leerspielen von Glücksspielautomaten eine „Verwendung von Daten" in der Auswertung eines sog. Manipulationsprogramms, das den Spieler in die Lage versetzt, die „Risikotaste" in dem Moment zu drücken, in dem dies Gewinn verspricht: Hier sind mit „Daten" ersichtlich die aus dem Manipulationsprogramm stammenden (entkodierten) Informationen gemeint (ebenso *Bühler* S. 101 f). – Die Lösung folgt aus teleologischer Auslegung in Verbindung mit der vom Gesetzgeber gewollten Erfassung einer neuen Angriffsform auf das Vermögen (oben Rdn. 13): Nicht jede Information, die für eine DV-Anlage bestimmt ist, in sie eingeht oder aus ihr stammt, ist ein Datum i. S. d. § 263 a. Mag auch der allgemeine Sprachgebrauch weiter gehen und das Datum mit der Information gleichsetzen, so ist computerspezifisch entsprechend der Rdn. 20 genannten DIN-Norm eine **Darstellung** der Information notwendig, damit der Computer die Information „lesen" kann. Daten sind somit Zeichen, die etwas über Tatsachen aussagen (*Haft* Prot. 26/165) oder sie zumindest „darstellen". Daten sind folglich nur **kodierte Informationen** (*Wessels* BT-2 Rdn. 575; **aA** *Achenbach* Jura **1991** 227; *Bühler* S. 102; *Rengier* 1 § 14, 2). Jedoch ist die Form der Repräsentation gleichgültig, und die Auftragung (Fixierung) auf einen Datenträger ist entgegen *Haft* (DSWR **1986** 256 und NStZ **1987** 8) für den Datenbegriff nicht erforderlich (*Schulze-Heiming* S. 24 ff mit weit. Nachw.). Zum Datum wird die Information damit (auch unter zeitlichen Aspekten) erst, wenn sie von der visuell erkennbaren in die kodierte Form überführt ist, die für die Arbeitsweise der DV charakteristisch ist (zutr. *Gössel* 2 § 22, 5; *Schmid* § 2, 17 u. 25). Die Eingabe kann dabei auch durch Eintippen von Zahlen mittels einer Tastatur (also an einem Termi-

---

[32] *Achenbach* Jura **1991** 227; *Frey* S. 26; *Gössel* 2 § 22, 5; *Lackner/Kühl* Rdn. 3; *Maurach/Schroeder/Maiwald* 1 § 41 VI 2 Rdn. 229; *Meurer* Kitagawa-Festschrift S. 977; *Otto* BT § 52 III 2; *Schulze-Heiming* S. 24 ff; *Sieber* Computerkriminalität S. 6 mit weit. Nachw.

[33] *Günther* SK Rdn. 7; *Lackner/Kühl* aaO, je mit weit. Nachw.; ferner *Gössel* 2 § 22, 20; *Maurach/Schroeder/Maiwald* aaO; *Otto* aaO; *Tiedemann* JZ **1986** 869.

nal) erfolgen (*Schmid* § 2, 28). Bei teleologischer Auslegung bestehen keine Bedenken, eine z. B. erst im Bankomaten kodierte Information als neu entstehendes Datum von dem Zeitpunkt der Kodierung an als Datum anzusehen, das vom Täter „verwendet" wird (zu letzterem Begriff näher Rdn. 36 ff). Auch die nicht kodierte Eingabe des auszuzahlenden Geldbetrages durch Drücken von entsprechenden Zahlenknöpfen führt zu einer Darstellung, die als (kodierte) Zahlenreihe die Information „gewünschter Geldbetrag" verkörpert (*Gogger* S. 64). Es reicht ferner aus, daß die eingegebene Information – wie die persönliche Geheimnummer beim Bankomaten – als sog. Berechtigungsdatum im Computer gespeichert ist. Und bei dem gezielten Leerspielen von Glücksspielautomaten braucht nicht auf die ausgedruckte Liste mit Informationen abgestellt zu werden; vielmehr wird durch Drücken der Risikotaste die Anweisung zur Erhöhung der Gewinn- und Verlustchancen gegeben und dieses im Computer enthaltene Datum verwendet (*Bühler* S. 103; *Neumann* aaO S. 304). Nur wenn man dies alles nicht für ausreichend hält, wirkt der Eingebende immerhin auf kodierte Informationen ein und erfüllt daher bei fehlender Befugnis mit BGH aaO jedenfalls die vierte Tatbestandsalternative (*Wessels* BT-2 Rdn. 583).

b) Der Begriff der **Datenverarbeitung** ist im Ausgangspunkt weit zu verstehen und **22**
meint die technischen Vorgänge, die durch Aufnahme von Daten und ihre Verknüpfung nach Programmen zu Arbeitsergebnissen führen.[34] Jedoch ist damit nicht der gesamte Arbeitsbereich gemeint. Anders als in § 303 b werden nur die konkreten, dem jeweiligen Ergebnis vorausliegenden „Vorgänge" der Datenverarbeitung geschützt (*Hilgendorf* JuS **1997** 131; *Lackner/Kühl* Rdn. 4). Nicht vom Gesetzeswortlaut, wohl aber vom Gesetzeszweck und von der Überschrift her geboten ist ferner die Eingrenzung auf *automatische* Datenverarbeitung (*Lenckner/Winkelbauer* CR **1986** 658; *Möhrenschlager* wistra **1986** 133), praktisch vor allem auf elektronische Datenverarbeitung, also *EDV*-Systeme.[35] Einzubeziehen sind aber auch vergleichbar (z. B. akustisch, optisch, biologisch usw.) arbeitende Medien (*Schmid* § 2, 12 für das schweizer. Strafrecht). Dem Begriff unterfallen auch der Personal Computer (**PC**) und der Mikroprozessor (**Chip**), mögen beide auch nicht (ganz) dem Bild eines Computers entsprechen, das der Gesetzgeber bei Einführung des § 263 a vor sich sah (*Altenhain* JZ **1997** 755 Fußn. 31; auch *Schmid* § 2, 18). Bereits nach der Überschrift des Tatbestandes und wegen der Existenz des § 265 a (oben Rdn. 1) ausgeschlossen sind dagegen rein mechanisch wirkende Geräte, und nach dem Schutzbereich des § 263 a scheidet ferner die menschliche Datenverarbeitung aus (§ 263!). Wenn *Otto* (BT § 52 III 2) auch bloße technische Sicherheitseinrichtungen (Wegfahrsperren!) ausschließen will, so ist ein Abgrenzungskriterium innerhalb der Datenverarbeitungseinrichtungen nicht ersichtlich, zumal es auch etwa auf eine „Anlage" von nicht unerheblicher Größe (§§ 325, 325 a!) nicht ankommt. Auch kann entgegen *Hilgendorf* (JR **1997** 347, 350) nicht entscheidend sein, ob der in Rede stehende Datenverarbeitungsvorgang von besonderer Wichtigkeit ist (abgesehen davon, daß bei Anlegung betrugsparalleler Maßstäbe jeder vermögensrelevante Datenverarbeitungsvorgang, der eine schädigende Vermögensverfügung zur Folge hat, „von besonderer Wichtigkeit" ist). Die Ausgrenzung solcher Sicherheitseinrichtungen ergibt sich vielmehr erst aus dem Unmittelbarkeitserfordernis (unten Rdn. 65 ff): Muß die gesicherte Sache (bei fortbestehendem Gewahrsam) noch weggenommen werden, so sind §§ 242, 243

---

[34] BTDrucks. 10/318 S. 21; *Bühler* S. 72; *Gössel* 2 § 22, 6; *Günther* SK Rdn. 8; *Haß* in Lehmann XII, 17; *Hilgendorf* JuS **1997** 131; *Lackner/Kühl* Rdn. 4; *Rengier* 1 § 14, 2; *Sieber* Computerkriminalität S. 6 ff mit weit. Nachw.; *Tröndle* Rdn. 3; *Wessels* BT-2 Rdn. 575.

[35] *Haß* aaO; *Lackner/Kühl* Rdn. 4; *Lenckner/Winkelbauer* CR **1986** 658.