

# Der Computerbetrug im japanischen Recht aus rechtsvergleichender Sicht

*Marc Dernauer*

- I. Einleitung
- II. Der Tatbestand des Art. 246-2 StrG im Vergleich zu § 263a StGB
  - 1. Die einzelnen Tatbestandsmerkmale des Art. 246-2 StrG
    - a) Schutzgut
    - b) Objekt der kriminellen Handlung
    - c) Tathandlungen
    - d) Kausalität/Vorsatz
    - e) Strafmaß
    - f) Tatvollendung/Versuch der Tat
    - g) Strafverfolgungshindernisse
  - 2. Vergleich mit dem Tatbestand des § 263a StGB
- III. Beispiele aus der japanischen Rechtsprechung für die Anwendung des Art. 246-2 StrG
  - 1. Tathandlung: „Eingeben falscher Daten“
  - 2. Tathandlung: „Eingeben unrichtiger Befehle“
  - 3. Tathandlung: „unbefugtes Verwenden von Daten“
  - 4. Tathandlung: „Verwenden falscher elektromagnetischer Aufzeichnungen“
  - 5. Die Bankautomatenfälle in Japan
- IV. Der Computerbetrug im System der Normen gegen Computerkriminalität im japanischen Strafgesetz
- V. Schlußbetrachtung

## I. EINLEITUNG

Die starke Zunahme des Einsatzes von elektronischen Datenverarbeitungsanlagen und Computern im modernen Wirtschafts- und Rechtsverkehr in den vergangenen Jahrzehnten hat der Organisation von Wirtschaft und Verwaltung ein völlig neues Gesicht gegeben. Viele Arbeits- und Verwaltungsprozesse konnten durch den Einsatz der Technik in großem Umfang rationalisiert werden. Dabei ist von großer Bedeutung, daß nunmehr mit Hilfe von Computern Daten und Informationen wesentlich einfacher verwaltet und mittels vorhandener Computernetzwerke auch über beliebige Entfernungen hinweg in Sekundenschnelle ausgetauscht werden können. Datenspeicherung und Datenaustausch sind daher heute Grundvoraussetzungen einer modernen Verwaltung und Wirtschaftsorganisation geworden.

Bei allem Nutzen, den der technische Fortschritt für die Gesellschaft mit sich gebracht hat, haben sich dadurch jedoch auch neue Möglichkeiten kriminellen Mißbrauchs eröffnet. Entweder ist der Computer selbst zum Angriffsziel geworden, oder aber er wird genutzt, um kriminelle Handlungen auszuführen. Dabei werden Daten gezielt ausgespäht, vernichtet, unerlaubt genutzt oder manipuliert.

Das Phänomen dieser sogenannten Computerkriminalität wird seit Anfang der achtziger Jahre überall auf der Welt beobachtet und kontrovers diskutiert. Es bestand lange Zeit Uneinigkeit über die tatsächliche Bedeutung dieser neuen Form von Kriminalität. So war beispielsweise strittig, ob es zur Bekämpfung der Computerkriminalität einer Reform des Strafrechts bedürfe oder ob das herkömmliche Strafrecht bereits ausreichend Schutz böte.<sup>1</sup>

In Japan wurde man auf die Gefahren durch Computerkriminalität besonders aufmerksam, als im Jahre 1985 deutsche Hacker in ein hochgesichertes Computersystem eines Energieforschungsinstituts in Tsukuba, eines der modernsten Forschungszentren Japans, eindringen (sog. Tristan-Fall).<sup>2</sup> Teilweise wird behauptet, daß dieses Ereignis sogar für eine Sensation in den Massenmedien gesorgt habe.<sup>3</sup> Im gleichen Jahr widmete auch die angesehenen juristische Fachzeitschrift „*Jurisuto*“ eine Ausgabe allein den strafrechtlichen Problemen moderner Datenverarbeitung.<sup>4</sup> Seit 1986 setzten sich Fachausschüsse des japanischen Justizministeriums (*Hômushô*) mit der Bekämpfung der Computerkriminalität auseinander und erarbeiteten einen entsprechenden Gesetzentwurf,<sup>5</sup> der auch vom japanischen Parlament angenommen wurde. Am 22.6.1987 trat dann schließlich das sogenannte „Gesetz zur Änderung von einigen Vorschriften auf dem Gebiet des Strafrechts“ (*Keihô-tô no ichibu o kaisei suru hôritsu*)<sup>6</sup> in Kraft. Dadurch wurden verschiedene Vorschriften geändert und neue ins Strafgesetz<sup>7</sup> aufgenommen, die spezielle Tatbestände der Computerkriminalität enthalten, unter anderem den Tatbestand des sogenannten „Computerbetruges“ (*denshi-keisan-ki shiyô sagi*) in Art. 246-2 StrG.

Damit wurde der Diskussion um die Notwendigkeit neuer Straftatbestände zur Bekämpfung der Computerkriminalität durch den japanischen Gesetzgeber ein Ende bereitet. Es gab jedoch eine Reihe von Kritikern, die zum Teil bis heute daran festhalten, daß eine Reform des Strafrechts zur Bekämpfung der Computerkriminalität nicht nötig gewesen wäre. Sie sei vielmehr nur eine von mehreren Möglichkeiten gewesen, den Erscheinungsformen der Computerkriminalität zu begegnen; man hätte statt dessen

- 
- 1 Vgl. ausführliche Quellenverweise bei M. MÖHRENSCHLÄGER, Das neue Computerstrafrecht: wistra Nr. 4 (1986) 128 ff.; vor allem Fußnoten 13, 14 und 15.
  - 2 A. YAMAGUCHI, Computer Crimes and Other Crimes against Information Technology in Japan, in: U. SIEBER (Hrsg.), Information Technology Crime: National Legislations and International Initiatives (Köln, Berlin, Bonn, München 1994) 307.
  - 3 H. SONODA, Das neue Computerstrafrecht in Japan: wistra Nr. 5 (1988) 168.
  - 4 *Jurisuto* Nr. 846 (1985).
  - 5 *Jurisuto* Nr. 885 (1987) 4.
  - 6 Gesetz Nr. 52/1987, *Hôrei Zensho* (1987/6) 42.
  - 7 *Keihô*, Gesetz Nr. 45/1907 i.d.F.d. Gesetzes Nr. 91/1995; im folgenden StrG abgekürzt. Deutsche Übersetzungen: K. SAITÔ / H. NISHIHARA, Das abgeänderte Japanische Strafgesetzbuch, Sammlung außerdeutscher Strafgesetzbücher in deutscher Übersetzung Nr. 65 (Berlin 1954); S. OBA, Strafgesetzbuch für das Kaiserlich Japanische Reich vom 23. April 1907: ZstW 28 (1908), 205 ff.

ebenso existierende Tatbestände weiter auslegen können.<sup>8</sup> Auch die tatsächliche Bedeutung der Computerkriminalität war lange umstritten. So haben Kritiker den Reformbefürwortern vorgeworfen, daß sie die Gefahren, die von der Computerkriminalität ausgehen, maßlos überschätzten. Übereinstimmung bestand lediglich darin, daß die Anzahl der in Wirklichkeit auftretenden Fälle schwer zu verifizieren sei. Obwohl *Sonoda* in seinem Aufsatz zur Computerkriminalität in Japan nur auf 75 bekanntgewordene Fälle in den Jahren zwischen 1971 und 1986 verweist, geht er gleichwohl davon aus, daß dies nur die Spitze des Eisbergs sei. Seiner Meinung nach sei mit Einführung des Gesetzes ein wichtiger Schritt zur Bekämpfung der Computerkriminalität getan worden.<sup>9</sup> Die Diskussion um die Reform des Strafrechts wurde offensichtlich weniger dadurch ausgelöst, daß sich in konkreten Fällen Strafbarkeitslücken auftraten; man befürchtete vielmehr, daß in Zukunft eine größere Zahl solcher Fälle auftreten könnte, und wollte dieser Gefahr durch neue Tatbestände vorbeugen.<sup>10</sup>

Der Tatbestand des Computerbetrugs (Art. 246-2 StrG) wurde dogmatisch als spezielles Betrugsdelikt verstanden und daher an den Betrugstatbestand (Art. 246 StrG) angehängt. Die Formulierung des Art. 246-2 StrG weist außerdem darauf hin, daß versucht wurde, auch tatbestandlich eine größtmögliche Übereinstimmung mit dem Betrugstatbestand zu erreichen. Somit wurde der japanische Tatbestand des Computerbetrugs dogmatisch in gleicher Weise wie der entsprechende Tatbestand im deutschen Strafgesetzbuch (§ 263a StGB) konstruiert. § 263a StGB trat in Deutschland zusammen mit anderen Vorschriften gegen die Computerkriminalität bereits am 1.8.1986 in Kraft, also etwa ein Jahr früher als Art. 246-2 StrG.<sup>11</sup> Das deutsche Computerstrafrecht scheint bei der Erarbeitung des japanischen Gesetzentwurfes eine Vorbildfunktion gehabt zu haben,<sup>12</sup> was auch die Ähnlichkeit der Dogmatik des Computerbetrugs erklären würde. Beide Normen sind also als spezielle Betrugstatbestände verfaßt worden. Auch im Wortlaut sind die japanische und die deutsche Norm ähnlich, so daß man insgesamt von vergleichbaren Normen ausgehen könnte. Wenn man sich allerdings die offiziellen Kriminalstatistiken anschaut, so ergibt sich ein etwas anderes Bild. In Deutschland wurden im Jahr 1994 20.112 und im Jahr 1995 26.890 Fälle von Computerbetrug

---

8 T. NAKAMURA, *Sagi-zai* [Das Betrugsdelikt], in: J. ABE / H. KAWABATA (Hrsg.), *Keihô-2 kakuron – Kihon mondai seminâ* [Strafrecht, Besonderer Teil – Lehrgang der Grundprobleme] (Tokyo 1992) 128.

9 SONODA (Fn. 3) 168, 173.

10 S. MATOBA, *Konpyûta hanzai ni kan suru keijihô-jô no mondai-ten* [Problempunkte des Strafrechts in Hinsicht auf Computerstraftaten]: *Jurisuto* Nr. 846 (1985) 15.

11 Die neu ins StGB eingefügten Vorschriften wurden zusammengefaßt als „Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität“ (2. WiKG).

12 SONODA (Fn. 3) 173; M. IDA, *Nishi doitsu ni okeru konpyûta hanzai e no taiô* [Reaktionen auf die in Westdeutschland auftretende Computerkriminalität]: *Jurisuto* Nr. 846 (1985) 42 ff.

erfaßt.<sup>13</sup> In Japan hingegen lag die Anzahl der registrierten Fälle deutlich darunter. So waren es im Jahre 1992 nur 31, im Jahre 1993 34 und im Jahre 1994 lediglich 36 Fälle.<sup>14</sup> Auch wenn man berücksichtigt, daß die offizielle Kriminalitätsrate in Japan im allgemeinen deutlich unter der in Deutschland liegt, ist dieser große Zahlenunterschied zunächst doch sehr erstaunlich. Es ist also zu klären, warum die Zahlen für Japan in so deutlicher Weise von den deutschen abweichen.

Ich möchte im folgenden zunächst den Tatbestand des Art. 246-2 StrG darstellen und die Unterschiede und Gemeinsamkeiten zu § 263a StGB aufzeigen. Anschließend sollen einige Beispiele für die Anwendung des Art. 246-2 StrG aus der japanischen Rechtsprechung vorgestellt werden. Schließlich möchte ich die Stellung des Computerbetrugs im System der durch die Reform ins Strafgesetz hinzugekommenen computerstrafrechtlichen Normen darstellen.

## II. DER TATBESTAND DES ART. 246-2 STRG IM VERGLEICH ZU § 263A STGB

Zur Veranschaulichung der Normen erscheint es mir sinnvoll, sie zunächst in deutscher Sprache einander gegenüberzustellen. Bei der Übersetzung des Art. 246-2 StrG kann bereits auf mehrere Übersetzungen in westliche Sprachen zurückgegriffen werden. Auch zwei deutsche Fassungen sind bereits veröffentlicht worden.<sup>15</sup> Diese weichen jedoch so wesentlich voneinander ab, daß nicht ohne weiteres eine Entscheidung zugunsten der einen oder der anderen Fassung getroffen werden kann. Die Schwierigkeit der Übersetzung ergibt sich wohl daraus, daß der japanische Gesetzgeber hier einen sehr komplexen Tatbestand geschaffen hat, der sprachlich nur schwer verständlich ist. Ich möchte hier keinen der beiden Übersetzungsvorschläge übernehmen, sondern einen eigenen dritten der Untersuchung voranstellen. In gewissem Umfang liegt meinem Vorschlag aber die Übersetzung von *Karl-Friedrich Lenz*<sup>16</sup> zugrunde.

### *Art. 246-2 StrG*

Wer außer in den in Art. 246 StrG bezeichneten Fällen

1. einer für die Erledigung geschäftlicher Angelegenheiten verwendeten elektronischen Datenverarbeitungsanlage falsche Daten oder unrichtige Befehle eingibt und dadurch unrichtige elektromagnetische Aufzeichnungen erzeugt, die einen Gewinn, Verlust oder eine Veränderung von Vermögensrechten bewirken, oder

---

13 BUNDESKRIMINALAMT (BKA), Polizeiliche Kriminalstatistik: Berichtsjahr 1995 (Wiesbaden 1996) 250 f.

14 JAPANISCHES JUSTIZMINISTERIUM (*Hômushô*), *Kensatsu tôkei nenpô* [Statistischer Jahresbericht der Staatsanwaltschaft] (Tokyo 1992, 1993 und 1994) 61.

15 SONODA (Fn. 3) 171; K.-F. LENZ/R. HEUSER, *Strafrechtsentwicklung in Japan und der Volksrepublik China* (Freiburg 1995) 15; vgl. auch die englische Übersetzung: YAMAGUCHI (Fn. 2) 315.

16 LENZ / HEUSER (Fn. 15) 15.

2. bei der Erledigung von geschäftlichen Angelegenheiten eines anderen falsche elektromagnetische Aufzeichnungen gebraucht, wodurch ein Gewinn, ein Verlust oder eine Veränderung von Vermögensrechten hervorgerufen wird, und dadurch selbst einen rechtswidrigen Vermögensvorteil erlangt oder einem Dritten verschafft, wird mit Freiheitsstrafe<sup>17</sup> bis zu zehn Jahre bestraft.

### § 263a StGB

(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.

#### 1. Die einzelnen Tatbestandsmerkmale des Art. 246-2 StrG

##### a) Schutzgut

Das Rechts- bzw. Schutzgut des Art. 246-2 StrG ist nach übereinstimmender Ansicht das individuelle Vermögen.<sup>18</sup> Hier wird die Konzeption deutlich, die dem neuen Tatbestand des Computerbetrugs zugrunde liegt. Die neuen Fälle, bei denen es zu einer unrechtmäßigen Vermögensverschiebung durch Mißbrauch der Computertechnologie kommt, sollen als Sonderform des Betrugs und nicht als Eigentumsdelikt behandelt werden.

##### b) Objekt der kriminellen Handlung

Das Objekt der kriminellen Handlung ist eine elektronische Datenverarbeitungsanlage. Das Gesetz präzisiert seine Aussage zwar dahingehend, daß es sich um eine bestimmte Art von Computer handeln muß, nämlich um einen, der "für die Erledigung geschäftlicher Angelegenheiten" verwendet wird. Tatsächlich aber wird dieser Begriff in der japanischen Kommentierung nicht weiter konkretisiert. Übereinstimmend wird vielmehr gesagt, daß an dieses Tatbestandsmerkmal keine allzu hohen Anforderungen gestellt

17 Eigentlich ist die Bezeichnung Freiheitsstrafe ungenau, da es in Japan zwei unterschiedliche Formen der Freiheitstrafe gibt, *chôeki* und *kinko*; hier wird in der japanischen Fassung *chôeki* angeordnet. Um jedoch den Gebrauch von spezifisch deutschen Begriffen zu vermeiden, die nicht mit den japanischen Begriffen in der Sache übereinstimmen, will ich hier den allgemeinen Begriff „Freiheitsstrafe“ verwenden. „*Kinko*“ wird häufig mit „Gefängnisstrafe“ übersetzt, während für „*chôeki*“ häufig „Zuchthaus(-strafe)“ verwendet wird. „*Chôeki*“ ist jedoch inhaltlich nicht identisch mit dem deutschen Begriff „Zuchthaus“.

18 K. NAKAYAMA, *Abusutorakuto chûshaku keihô* [Kurzkommentar zum Strafrecht] (Tokyo 1992) 543; H. KAWABATA, *Keihô kakuron* [Strafrecht, Besonderer Teil] (Tokyo 1993) 166.

werden dürfen. Es gehe beispielsweise nicht um das Kriterium, ob der Computer wegen der Wichtigkeit bestimmter Geschäfte besonders gesichert ist, denn das Schutzgut des Art. 246-2 StrG sei nicht der Computer oder die Daten an sich, sondern lediglich dessen Gebrauch zum finanziellen Schaden eines Dritten.<sup>19</sup> Auch soll sich ein möglicher Mißbrauch keinesfalls nur auf Manipulationen an Datenverarbeitungsanlagen bestimmter Wirtschaftsunternehmen wie z.B. die einer Bank oder bestimmter Kreditinstitute beschränken.<sup>20</sup> Es sei ferner auch nicht von Belang, ob es sich dabei um eine bestimmte Art unternehmerischer, wirtschaftlicher oder rechtlicher Geschäfte drehe oder ob ein besonders großes Vermögen im Spiel sei; es gehe ganz allgemein um jede Art von Datenverarbeitungsanlagen, bei denen die vermögensrechtlichen Angelegenheiten eines anderen mitbetroffen sind.<sup>21</sup> Das Abheben oder das Einzahlen von Geld sowie das Verwalten von Bilanzen jedenfalls werden unproblematisch als „Erledigung geschäftlicher Angelegenheiten“ interpretiert.<sup>22</sup> Bei dem betroffenen „anderen“ kann es sich sowohl um natürliche wie juristische Personen handeln.<sup>23</sup> Außerdem steht es dem direkten Zugriff auf einen fremden Computer gleich, wenn der Täter von zuhause aus mit Hilfe seines privaten Computers in eine fremde Datenverarbeitungsanlage eindringt.<sup>24</sup>

c) *Tathandlungen*

Alle im Gesetz erwähnten tatbestandsmäßigen Handlungen stehen sinngemäß anstelle der Täuschung eines Menschen in Art. 246 StrG. Der Tatbestand des Art. 246-2 StrG ist in zwei Halbsätze unterteilt.

Im ersten Halbsatz werden zwei Handlungsvarianten genannt. Dies sind das „Eingeben falscher Daten“ und das „Eingeben unrichtiger Befehle“. Als Folge beider Formen der Manipulation muß eine unrichtige elektromagnetische Aufzeichnung in der fremden Datenverarbeitungsanlage erzeugt, d.h. gespeichert werden, die ihrerseits eine Veränderung an Vermögensrechten in Dateien bewirkt. Der erste Halbsatz gilt somit für Veränderungen oder Manipulationen an Daten oder Programmen einer Datenverarbeitungsanlage. Das „Eingeben falscher Daten“ meint solche Daten, die den tatsächlichen Zustand an Vermögensrechten so verändern, daß unwahre Aussagen entstehen.

---

19 T. KAMIYAMA, *Nihon no keizai hanzai* [Wirtschaftsbezogene Straftaten in Japan] (Tokyo 1996) 160.

20 KAMIYAMA (Fn. 19) 160.

21 K. YONEZAWA, Art. 246 in: H. Ôtsuka/K. Kawakami/F. Satô (Hrsg.), *Daikonmentaru keihô* [Großkommentar zum Strafrecht] Band 10 (Tokyo 1992) Art. 246-2, Rdnr. 9, 149.

22 K. SHIBAHARA, *Konpyûta-sagi* [Der Computerbetrug] in: Bessatsu Jurisuto – Keihô hanzai hakusen II [Sonderband der Zeitschrift Jurisuto – Auswahl an Delikten II], 3. Auflage (Tokyo 1989) 99.

23 KAWABATA (Fn. 18) 167.

24 YONEZAWA (Fn. 21) Art. 246-2, Rdnr. 11, 150.

Fälle, die unter diese Handlungsmodalität subsumiert werden, seien nachfolgend beispielhaft skizziert:

- Ein Angestellter eines Kreditinstituts gibt wahrheitswidrig in den Zentralcomputer die Information ein, daß auf ein Konto eine Einzahlung getätigt wurde, in der Datei, in der die Bilanzen der Konten gespeichert sind, erscheint zum Nachteil des Kreditinstitutes eine höhere Forderungssumme.<sup>25</sup>
- Die Tat kann auch durch Unterlassen begangen werden, wenn z.B. tatsächlich Geld von einem Konto abgehoben wurde, der Bankangestellte dies jedoch vorsätzlich nicht verbucht oder verhindert, daß diese Auszahlung verbucht wird.<sup>26</sup>
- Ein Angestellter eines Kreditinstitutes nimmt direkt Zugriff auf die Hauptdatei und verändert die Höhe des Kontostandes bzw. des Sparguthabens.<sup>27</sup>
- Ein Bankangestellter tätigt mit Hilfe des Computers unbefugt Überweisungen vom Konto eines Kunden zu dessen Schaden.

Zusammenfassend können die Formen krimineller Handlungen solcher Art als „Eingabemanipulationen“ bezeichnet werden.

Das „Eingeben unrichtiger Befehle“ umfaßt alle Fälle, in denen es zur Verschiebung von Vermögensrechten durch Manipulation an der Software einer Datenverarbeitungsanlage kommt. Die Manipulation kann in der Weise erfolgen, daß ein bereits in der Anwendung befindliches Computerprogramm verändert wird oder auch daß selbstentwickelte Computerprogramme der Datenverarbeitungsanlage eingespeist werden. Fälle, die unter diese Tathandlung subsumiert werden, sind etwa:

- Ein Datenverwaltungsprogramm eines Kreditinstituts wird so verändert, daß es selbständig die Bilanzen auf bestimmten Konten verfälscht, d.h. in der Regel erhöht.<sup>28</sup>
- Ein Datenverwaltungsprogramm eines Kreditinstitutes wird so verändert, daß dadurch auf bestimmten Konten die tatsächlich erfolgte Einzahlungssumme stets um eine Stelle erweitert wird; z.B. statt einer tatsächlich erfolgten Einzahlung von ¥ 10.000 verbucht das Programm automatisch ¥ 100.000.<sup>29</sup>

Fälle dieser Art können mit „Programmanipulationen“ überschrieben werden.

Eine weitere Tatmodalität des Art. 246-2 1. HS StrG ist das „unbefugte Benutzen fremder Daten“. Diese Tathandlung ist eigentlich in Art. 246-2 StrG ausdrücklich in keiner Form erwähnt, wird jedoch allgemein als dem Art. 246-2 StrG zugehörig anerkannt. So werden hier auch Fälle wie die des unbefugten Verwendens gefundener oder entwendeter Codekarten am Geldautomaten erfaßt, deren juristische Behandlung in

---

25 KAWABATA (Fn. 18) 168.

26 KAWABATA (Fn. 18) 168.

27 YONEZAWA (Fn. 21) Art. 246-2, Rdnr. 11, 150.

28 YONEZAWA (Fn. 21) Art. 246-2, Rdnr. 11, 150.

29 KAWABATA (Fn. 18) 168.

Deutschland vor allem bis zur Einführung des § 263a StGB heftig umstritten war. Systematisch gibt es Streit darüber, ob diese Handlung unter „Eingeben falscher Daten“ oder „Eingeben unrichtiger Befehle“ zu fassen ist. Es werden beide Meinungen vertreten;<sup>30</sup> letztendlich ändert dies an der Anwendung aber nichts. Allerdings werden nicht alle Fälle des Codekartenmißbrauchs vom Tatbestand erfaßt, sondern nur die Sonderfälle, in denen jemand am Geldautomaten unberechtigte Überweisungen auf bestimmte Konten tätigt und dadurch den Codekarteninhaber oder die Bank schädigt.<sup>31</sup> Tatsächlich aber ist ein solcher Fall in Japan noch nie aufgetreten. Es wird lediglich befürchtet, daß eine kriminelle Handlung dieser Art zukünftig in Erscheinung treten könnte.<sup>32</sup> Wenn es hingegen zu einer Auszahlung von Bargeld am Automaten kommt, so bleibt nach ganz herrschender Meinung für die Anwendung von Art. 246-2 StrG kein Raum. Hier sei aber der Tatbestand des Diebstahls nach Art. 235 StrG erfüllt.<sup>33</sup> Wenn das „Stehlen“ des Geldes am Geldautomaten dabei mit einer gefälschten Codekarte stattfindet, so wird von der Rechtsprechung regelmäßig Diebstahl (Art. 235 StrG) in Tateinheit mit Datenfälschung bzw. Verwenden gefälschter Daten nach Art. 161 StrG angenommen.<sup>34</sup> Wird eine echte Codekarte zuvor entwendet, so wird entgegen dem Streit in Deutschland das Entwenden der Karte von japanischen Gerichten ohne weitere Erörterung als selbständige Tat bewertet, so daß in solchen Fällen ein zweifacher Diebstahl in Tatmehrheit vorliegt.<sup>35</sup>

Der zweite Halbsatz des Art. 246-2 StrG nennt eine weitere strafbare Handlung. Demnach soll auch das „Gebrauchen falscher elektromagnetischer Aufzeichnungen“ den Tatbestand des Computerbetrugs erfüllen, sofern es dabei zu einer Verschiebung von Vermögensrechten kommt. Gemeint sind damit die Fälle, in denen falsche elektronische Wertkarten verwendet werden, um sich so der Zahlung eines für eine Dienstleistung geforderten Entgelts zu entziehen.<sup>36</sup> Es handelt sich dabei vor allem um die in letzter Zeit zunehmenden Fälle des Gebrauchs falscher Telefonkarten zum Schaden des Telekommunikationsunternehmens. Aber auch der Gebrauch anderer gefälschter Wertkarten, wie z.B. solche von Unternehmen des öffentlichen Nahverkehrs, sollen unter diese Tatmodalität subsumiert werden können.<sup>37</sup> Aufgetreten sind in Japan bisher

---

30 KAMIYAMA (Fn. 19) 160 f.

31 KAMIYAMA (Fn. 19) 164; YONEZAWA (Fn. 21) Art. 246-2, Rdnr. 11, 150.

32 KAMIYAMA (Fn. 19) 164 f.

33 KAMIYAMA (Fn. 19) 164 f.; YONEZAWA (Fn. 21) Art. 246-2, Rdnr. 30, 153.

34 KAMIYAMA (Fn. 19) 165 f.; Urteil des Distriktgerichts (DG) Tokyo vom 17.2.1989, Hanrei Taimusu 700 (1989) 279 ff.; so auch: Urteil des DG Tokyo vom 31.3.1989, Urteil des DG Sapporo vom 27.3.1984.

35 Urteil des DG Tokyo vom 3.3.1980, in: N. NISHIDA, *Hanrei keihô kakuron* [Strafrecht, Besonderer Teil anhand gerichtlicher Fälle] (Tokyo 1993) 232 f.; Urteil des DG Tokyo vom 17.2.1989, Hanrei Taimusu 700 (1989) 279 ff.

36 NAKAMURA (Fn. 8) 129.

37 KAMIYAMA (Fn. 19) 159; YONEZAWA (Fn. 21) Art. 246-2, Rdnr. 26-27, 152.

jedoch nur Fälle des Gebrauchs falscher Telefonkarten.<sup>38</sup> Nicht tatbestandmäßig hingegen sei das Verwenden gefundener oder echter Wertkarten, da es sich dabei nicht um inhaltlich falsche Aufzeichnungen handle und auch bei dem Dienstleistungsunternehmen kein Vermögensschaden entstehe.<sup>39</sup> Als Tatobjekt der Datenverarbeitungsanlage taugt also offensichtlich auch das Fernsprengerät oder im allgemeinen die Maschine, die eine elektromagnetische Wertkarte lesen kann.

Es finden sich in der Literatur auch Vorschläge, wie die Handlungsalternativen des ersten von der Tathandlung des zweiten Halbsatzes durch Oberbegriffe voneinander abgegrenzt werden sollten. Die tatbestandlichen Handlungen des 1. Halbsatzes, also das „Eingeben von falschen Daten“ und das „Eingeben von unrichtigen Befehlen“, werden dabei als *sonaetsuke-gata* bezeichnet, was dafür steht, daß die Daten der Datenverarbeitungsanlage selbst manipuliert werden, wohingegen die tatbestandlichen Handlungen des 2. Halbsatzes *keitai-gata* genannt werden, was auf die Manipulation von tragbaren elektromagnetischen Datenträgern und deren Gebrauch an einem computergesteuerten Datenlesegerät hinweist.<sup>40</sup>

d) *Kausalität/Vorsatz*

Durch das „Eingeben falscher Daten“ oder „unrichtiger Befehle“ muß es zu einer Erzeugung von elektromagnetischen Aufzeichnungen kommen, durch die eine Veränderung von Vermögensrechten bewirkt wird. Desgleichen muß auch der „Gebrauch von falschen elektromagnetischen Aufzeichnungen“ zu einer Veränderung von Vermögensrechten führen. Zudem muß der Täter dadurch selbst einen rechtswidrigen Vermögensvorteil, d.h. einen Vermögensvorteil, der objektiv der Vermögensordnung des Zivilrechts widerspricht, erlangt haben oder diesen rechtswidrigen Vermögensvorteil einem Dritten verschafft haben. Auf all diese Tatbestandsmerkmale muß sich der einfache Vorsatz des Täters erstrecken.

e) *Strafmaß*

Der Täter kann wegen einer rechtswidrigen und schuldhaften Tat nach Art. 246-2 StrG mit Freiheitsstrafe bis zu zehn Jahren bestraft werden. Auch an dieser Strafzumessung sieht man wieder die dogmatische Einbettung des Computerbetrugs in das japanische Strafrecht. Der japanischen Gesetzgeber hat bewußt das gleiche Strafmaß wie beim einfachen Betrug nach Art. 246 StrG angeordnet.

---

38 KAMIYAMA (Fn. 19) 159, 165.

39 YONEZAWA (Fn. 21) Art. 246-2, Rdnr. 28, 152.

40 N. NISHIDA, *Konpyûta no fusei-sôsa to zaisan-zai* [Mißbrauch von Computern und die Vermögensdelikte]: Jurisuto 885 (1987) 18.

f) *Tatvollendung / Versuch der Tat*

Die Tat ist bei den Tathandlungen „Eingeben falscher Daten“ und „Eingeben unrichtiger Befehle“ zu dem Zeitpunkt vollendet, in dem die falsche elektromagnetische Aufzeichnung gespeichert ist und der Täter nach seiner Vorstellung von der Tat den Vermögensvorteil sich oder einem Dritten verschafft hat. Beim Gebrauch falscher elektromagnetischer Aufzeichnungen ist in den bisher ausschließlich in Erscheinung getretenen „Telefonkartenfällen“ die Tat mit Beginn des Telefongesprächs verwirklicht.<sup>41</sup> Gemäß Art. 250 StrG ist auch der Versuch der Tat mit Strafe bedroht. Es ist jedoch sehr umstritten, zu welchem Zeitpunkt der Täter unmittelbar zur Tat ansetzt. Dies gilt vor allem für die Telefonkartenfälle.<sup>42</sup> Dazu wird in der Literatur keine systematische Lösung des Problems aufgezeigt.

g) *Strafverfolgungshindernisse*

Art. 251 StrG verweist auf die Anwendung des Art. 244 StrG, also auf eine besondere Regelung für die Fälle, in denen Täter und Opfer in verwandschaftlicher Beziehung zueinander stehen. Demnach gilt in solchen Fällen, daß für ihre Strafverfolgung ein Strafantrag des Geschädigten erforderlich ist. Zudem gilt, daß der Versuch der Tat nicht verfolgt wird, sofern Täter und Opfer Ehepartner oder miteinander verwandt sind und einen gemeinsamen Hausstand haben.

2. *Vergleich mit dem Tatbestand des § 263a StGB*

Art. 246-2 StrG unterscheidet sich in mehreren Punkten deutlich von § 263a StGB. Der japanische Gesetzgeber hat bei der Fassung keinesfalls nur die deutsche Norm kopiert. Es gibt allerdings auch Gemeinsamkeiten, die sich daraus ergeben, daß beide Normen die gleiche Thematik regeln. Mit den neuen Normen gegen den Computerbetrug in Deutschland und Japan soll das gleiche Rechtsgut, also das persönliche Vermögen, gegen Gefahren geschützt werden, die der fortschreitende Einsatz moderner Computer und deren Mißbrauch mit sich bringt. Die Gesetzgeber beider Länder haben die neue Norm in enger Verbindung zum Tatbestand des herkömmlichen Betrugs konstruiert. So gilt in beiden Fällen, daß das Strafmaß und die Strafverfolgungsvoraussetzungen denen des gewöhnlichen Betrugs entsprechen. Anstatt der sonst beim Betrug erforderlichen Täuschung eines Menschen werden bestimmte Formen strafbarer Computermanipulationen bestimmt, durch die es zu einer widerrechtlichen Verschiebung von Vermögensrechten kommen muß, um dem Taterfolg des Betrugs gleichzukommen.

---

41 KAMIYAMA (Fn. 19) 161; YONEZAWA (Fn. 21) Art. 246-2, Rdnr. 36-38, 154 ff.

42 KAMIYAMA (Fn. 19) 161.

In § 263a StGB werden folgende Handlungsvarianten genannt:<sup>43</sup>

- unrichtige Programmgestaltung (a),
- falsche oder unvollständige Datenverwendung (b),
- unbefugtes Verwenden von Daten (c) und
- sonst unbefugtes Einwirken auf den Ablauf einer Datenverarbeitungslage (d).

Der japanische Tatbestand benennt zwar das gleiche Objekt der Handlung, also eine Datenverarbeitungsanlage, nennt aber ausdrücklich nur drei Handlungsvarianten, nämlich

- das Eingeben falscher Daten (1),
- das Eingeben falscher Befehle (2) und
- den Gebrauch falscher elektromagnetischer Aufzeichnungen (3).

Sachlich entsprechen die beiden Handlungsformen (1) und (2) von Art. 246-2 StrG den Varianten (b) und (a) des § 263a StGB. Es werden also im deutschen und japanischen Recht die Tatformen der „Eingabemanipulation“ und der „Programmanipulation“ durch den Tatbestand des Computerbetrugs erfaßt. Die in Art. 246-2 StrG ungeschriebene Handlungsvariante des „unbefugten Verwendens von Daten“ entspricht nicht der Variante (c) der deutschen Norm, obwohl dies anzunehmen naheliegt. Wie oben bereits festgestellt werden im japanischen Recht nur die Fälle des Codekartenmißbrauchs unter diese Handlungsvariante subsumiert, in denen es zu keiner Bargeldauszahlung an den Täter kommt. Es werden nur die Fälle erfaßt, wo der Täter durch Mißbrauch einer Codekarte am Bankautomaten die Verschiebung von Giralgeld bewirkt. Alle Fälle von Bargeldauszahlung an den Täter werden unter Anwendung der Diebstahlsnorm gelöst. Im deutschen Recht hingegen werden nach herrschender Meinung seit Einführung des § 263a StGB alle typischen Bankautomatenfälle, wo es durch den Mißbrauch einer fremden Codekarte zu einer Bargeldauszahlung an den Täter kommt, als Computerbetrug aufgefaßt. Die §§ 242, 246 StGB sind höchstens noch subsidiär anwendbar.<sup>44</sup> Es wird daneben aber noch die Meinung vertreten, daß im Falle der Verwendung gefälschter Karten weiterhin Raum für die Anwendung der Diebstahlparagrafen 242, 243 StGB bleibe, § 263a StGB dann also nicht anzuwenden sei.<sup>45</sup> Generell gegen die Anwendbarkeit von § 263a StGB auf die Fälle funktionsgerechter, aber mißbräuchlicher Benutzung von Bankautomaten mittels Codekarte ist *Otfried Ranft*, der eine ganze

---

43 Siehe Gliederungspunkt II.

44 P. CRAMER, § 263a StGB, in: A. SCHÖNKE / H. SCHRÖDER, Kommentar zum Strafgesetzbuch, 25. Auflage (München 1997) Rdnr. 18, 26, 41; M. HUFF, Die mißbräuchliche Benutzung von Geldautomaten: NJW (1987) 817; U. WEBER, Probleme der strafrechtlichen Erfassung des Euroscheck- und Euroscheckkartenmißbrauchs nach Inkrafttreten des 2. WiKG: JZ (1987) 216.

45 H. OTTO, Zum Bankautomatenmißbrauch nach Inkrafttreten des 2. WiKG: JR (1987) 225.

Reihe von Einwänden vorbringt.<sup>46</sup> Folgt man in Japan und Deutschland jedoch der herrschenden Meinung, werden die Bankomatfälle, bei der es zu einer Auszahlung von Bargeld kommt, in Deutschland als Computerbetrug, in Japan hingegen als Diebstahl angesehen. Vor der Einführung des § 263a StGB versuchte die Rechtsprechung und Lehre in Deutschland ebenfalls die Bankautomatenfälle unter die herkömmlichen Tatbestände wie den Diebstahl oder die Unterschlagung zu subsumieren.<sup>47</sup> Dies bereitete jedoch beim Diebstahl große Schwierigkeiten, einen Gewahrsamsbruch zu konstruieren; die teilweise angenommene Unterschlagung wurde damit begründet, daß das vom Geldautomaten an den „ordnungsgemäßen“ Bediener herausgegebene Geld, der sich dazu einer gefälschten oder gestohlenen Codekarte bediente, im Eigentum der Bank verbleibe, da kein rechtsgeschäftlicher Übereignungswille anzunehmen sei. Auch diese juristische Konstruktion war höchst umstritten, und einige vertraten die Ansicht, daß solche Fälle weder den Tatbestand des Diebstahls noch den der Unterschlagung erfüllten,<sup>48</sup> mithin der Täter straffrei sein sollte. Die Bedenken gegen eine Anwendung der Vorschrift des Diebstahls in solchen Fällen gibt es in Japan nicht. Hier liegt somit ein großer Unterschied in der Anwendung der deutschen zur japanischen Norm. In Deutschland machen gerade die Bankautomatenfälle den ganz überwiegenden Teil der Anwendungsfälle der Vorschrift über den Computerbetrug aus.<sup>49</sup> Es ist daher festzuhalten, daß der Anwendungsbereich des Art. 246-2 StrG in diesen Fällen gegenüber dem § 263a StGB deutlich eingeschränkt ist.

Für die Tathandlung (d) des § 263a StGB gibt es in der japanischen Norm keine Entsprechung. Die in Deutschland unter dieses Tatbestandsmerkmal fallenden Hardware-Manipulationen oder die Verhinderung des Ausdrucks von Daten<sup>50</sup> werden von Art. 246-2 StrG nicht erfaßt.

Dafür tritt in Art. 246-2 2. HS StrG eine Tathandlung (3) hinzu, die in Deutschland nicht mit dem Computerbetrug in Verbindung gebracht wird. Demnach wird in Japan das Verwenden falscher elektromagnetischer Aufzeichnungen auf einer elektronischen Wertkarte als selbständige Form des Computerbetrugs zum Nachteil des Dienstleistungsanbieters angesehen. Fälle wie diese werden in Deutschland üblicherweise als Erschleichen von Leistungen nach § 265a StGB gewertet.

---

46 O.RANFT, Der Bankautomatenmißbrauch: wistra (1987) 83 f.

47 AG Gießen: NJW (1985) 2283 „einfacher Diebstahl“; OLG Koblenz: wistra (1987) 261 „einfacher Diebstahl“; AG Kulmbach: NJW (1985) 2282 f. „Diebstahl in besonders schwerem Fall“; LG Köln: NJW (1987) 667 ff. „Diebstahl in besonders schwerem Fall“; K. SEELMANN, „Grundfälle zu den Eigentumsdelikten“: JuS (1984) 288 ff. „Diebstahl“; BGHSt 35, 152 „Unterschlagung“; LG Oldenburg: NJW (1987) 667 „Unterschlagung“; G. KLEB-BRAUN, Codekartenmißbrauch und Sparbuchfälle aus volljuristischer Sicht: JA (1986) 249 ff. „Unterschlagung“.

48 OLG Hamburg: NJW (1987) 336; OTTO (Fn. 45) 221 ff.

49 BUNDESKRIMINALAMT (Fn. 13) 250. Ungefähr 85% der Fälle betreffen den Mißbrauch von Codekarten.

50 K. LACKNER, Strafgesetzbuch mit Erläuterungen, 21. Aufl. (1995) § 263a, Rdnr. 15.

Ein weiterer Unterschied zwischen Art. 246-2 StrG und § 263a StGB besteht in der vom Gesetz verlangten Form des Vorsatzes. So verlangt die japanische Norm hinsichtlich aller Tatbestandsmerkmale einfachen Vorsatz. Die deutsche Norm jedoch verlangt hinsichtlich der Verschaffung eines rechtswidrigen Vermögensvorteils eine daraufhin gerichtete Absicht des Täters (*dolus directus* 1. Grades). Für alle anderen Tatbestandsmerkmale reicht einfacher Vorsatz aus.<sup>51</sup>

Obwohl der Tatbestand des Computerbetrugs im deutschen und japanischen Recht vor allem hinsichtlich der dogmatischen Konstruktion ähnlich ist, bestehen wie dargestellt doch große Unterschiede im Anwendungsbereich. Da der japanische Tatbestand die typischen Bankautomatenfälle nicht erfaßt, läßt sich bereits zum Teil erklären, warum in Deutschland § 263a StGB wesentlich häufiger angewendet werden kann.

### III. BEISPIELE AUS DER JAPANISCHEN RECHTSPRECHUNG FÜR DIE ANWENDUNG DES ART. 246-2 STRG

Nachdem der theoretische Anwendungsbereich des Art. 246-2 StrG und die Unterschiede zu § 263a StGB nun ausführlich dargestellt wurden, möchte ich nun die Anwendung der Vorschrift durch die japanische Rechtsprechung anhand von Beispielen erläutern.

#### 1. *Tathandlung: „Eingeben falscher Daten“*

Zum ersten Mal kam Art. 246-2 StrG in einer Entscheidung des Distriktgerichts Osaka aus dem Jahr 1988 zur Anwendung.<sup>52</sup> In dem verhandelten Fall ging es darum, daß eine Bankangestellte auf das Computersystem ihrer Bank zugriff und unbefugt angebliche Überweisungen eines Kunden auf ihr Konto verbuchte. Dadurch erhöhte sich ihr Kontostand zum Schaden des Kunden um ¥ 1.2 Mio. Anschließend fingierte sie auf diese Weise weitere Überweisungen des Kunden auf das Konto ihres Komplizen in Höhe von ¥ 900.000. Schließlich eröffnete sie noch ein Konto bei einer anderen Bank unter falschem Namen, fälschte ein Überweisungsformular, nachdem eine Effektenfirma auf dieses Konto angeblich ¥ 45 Mio. überweisen wollte und gab dieses Formular zur Bearbeitung ihrer davon nichts wissenden Kollegin, die erwartungsgemäß diese Überweisung im Computer verbuchte. Das Gericht verurteilte die Bankangestellte hinsichtlich der selbst getätigten fingierten Überweisungen wegen vollendeten Computerbetrugs in zwei Fällen, da sie durch die Eingabe der sachlich falschen Informationen in den Bilanzdateien der Bank falsche elektromagnetische Aufzeichnungen erzeugt habe. Des weiteren erkannte das Gericht hinsichtlich der Fälschung des Überweisungsformulars und dessen Weitergabe an ihre Kollegin auf Fälschung von Dokumenten und deren

---

51 LACKNER (Fn. 50) § 263a, Rdnr. 24 und 25.

52 Urteil des OG Osaka vom 7.10.1988, Hanrei Jihô 1295 (1989) 151 ff.; zugleich in: SHIBAHARA (Fn. 22) 98 f.

Gebrauch in Tateinheit mit Betrug. Sie wurde zu zwei Jahren Freiheitsstrafe ohne Bewährung verurteilt.

An einer anderen Entscheidung des Obergerichts Tokyo aus dem Jahre 1993 wird deutlich, wie schwer sich japanische Gerichte mit der Einordnung und Anwendung des Art. 246-2 StrG noch tun.<sup>53</sup> Der Sachverhalt läßt sich wie folgt zusammenfassen: Der Angeklagte war seit langem Kunde einer Sparkasse und daher den dort arbeitenden Angestellten persönlich bekannt. Eines Tages füllte er ein Überweisungsformular in Höhe von ¥ 46 Mio. aus, obwohl sein Konto eine solche Summe nicht aufwies. Er versicherte aber gegenüber dem Filialleiter, daß er das Geld bereits am Nachmittag einzahlen werde und bat darum, daß die Überweisung schon vorher erledigt werde. Auf Anweisung des Filialleiters wurden die dazu erforderlichen Daten in das Computernetz eingegeben. Erst am folgenden Tag kam der Angeklagte erneut in die Sparkasse und erklärte gegenüber dem Filialleiter, daß er eine Einzahlungsüberweisung getätigt habe und sich die Buchung etwas verzögere. Er habe aber nun zudem einen derzeit durch sein Konto nicht gedeckten Scheck über ¥ 2.8 Mio. ausgestellt und bat den L darum, daß er bis zum Eintreffen der gesamten Summe zur Einlösung des Schecks schon einmal den Betrag seinem Konto gutschreiben möge. Der Filialleiter entsprach schließlich der Bitte des Angeklagten; die versprochene Überweisung an die Sparkasse ist aber nie getätigt worden. Das Obergericht Tokyo befand, daß sich der Angeklagte wegen Computerbetrugs strafbar gemacht habe. Die Vorinstanz hingegen gelangte zu einer Verurteilung wegen Untreue nach Art. 247 StrG. Diese Urteile lassen vieles unklar. Denn der Angeklagte hat nicht selbst irgendwelche Daten in den Computer eingegeben, was vom Gericht nicht ausreichend berücksichtigt wurde. Vielmehr hat wohl der Filialleiter aufgrund der Täuschung durch den Angeklagten die Eingabe der für die Überweisung erforderlichen Daten veranlaßt. Der Vermögensschaden ist daher letztlich aufgrund dieser Täuschung entstanden, so daß in diesem Fall ein gewöhnlicher Betrug nach Art. 246 StrG einschlägig erscheint. Falls aber vom Gericht eine mittelbare Täterschaft angenommen wurde, was aus dem Urteil nicht hervorgeht, so müßte schließlich der Filialleiter gezwungen gewesen sein, die Daten einzugeben. Er hat aber aus freiem Willen die Vermögensverfügung veranlaßt.<sup>54</sup> Nach Meinung des Gerichts sei aber für die Verurteilung von Bedeutung, daß der Angeklagte durch eigenes Verschulden in die finanzielle Klemme geraten sei und daß er die Einrichtungen der Bank willkürlich mißbraucht habe, um seine Schulden auszugleichen. Durch Ausfüllen der Überweisungsformulare habe er bereits die Ursache für die Eingabe falscher Daten in den Computer bewirkt und so falsche elektromagnetische Aufzeichnungen erzeugt.<sup>55</sup>

---

53 Urteil des OG Tokyo vom 29.6.1993, Hanrei Jihô 1440 (1993) 158 ff.

54 Zur Kritik am Urteil siehe KAMIYAMA (Fn. 19) 168 f.

55 Weitere Fälle dieser Handlungsvariante: Urteil des DG Morioka vom 16.1.1988; Urteil des DG Takamatsu vom 26.4.1989; Urteil des DG Tokyo vom 23.4.1990.

## 2. *Tathandlung: „Eingeben unrichtiger Befehle“*

In dem bislang anscheinend einzigen<sup>56</sup> Fall dieser Tatvariante ging es um das „Erschleichen von Auslandstelefongesprächen“.<sup>57</sup> Der Angeklagte hatte die elektronische Datenübermittlungsanlage des Telekommunikationsunternehmens KDD (*Kokusai Denshin Denwa*) mit Hilfe seines Personalcomputers auf eine Weise manipuliert, daß er ins Ausland telefonieren konnte, ohne dafür eine Gebühr entrichten zu müssen. Dazu imitierte er die Signale einer Amtsleitung und speiste sie in das Telefonnetz der ausländischen Telefongesellschaft ein. Gleichzeitig erzeugte er durch Manipulation des automatischen Gebührenzählprogramms von KDD den Wegfall der automatischen Gebührenzahlung. Durch mehrere Telefonate nach Spanien und Guam entstand KDD ein Schaden in Höhe von ¥ 373.806. Der Angeklagte wurde wegen vollendeten Computerbetrugs zu zwei Jahren und sechs Monaten Freiheitsstrafe verurteilt.

## 3. *Tathandlung: „unbefugtes Verwenden von Daten“*

In der Rechtspraxis ist diese Handlungsvariante bedeutungslos. Es ist noch kein einziger Fall dieser Art aufgetreten.<sup>58</sup> Insbesondere weil die Fälle, in denen jemand mit einer gestohlenen oder gefälschten Codekarte am Geldautomaten Bargeld erbeutet, in Japan nicht unter den Art. 246-2 StrG gefaßt werden, ist diese Handlungsvariante bislang nur von theoretischer Bedeutung.

## 4. *Tathandlung: „Verwenden falscher elektromagnetischer Aufzeichnungen“*

Das für diese Handlungsvariante klassische Fallbeispiel wäre das Verwenden von gefälschten Telefonkarten oder anderen Wertkarten. Theoretisch würde eine solche Tat den Tatbestand des Computerbetrugs erfüllen. Art. 246-2 2. HS StrG wurde auch eigens für diese Fälle konzipiert. Tatsächlich aber wenden die japanischen Gerichte in solchen Fällen grundsätzlich andere Strafvorschriften an, so daß es bisher noch nie zur Anwendung des Art. 246-2 StrG in diesem Zusammenhang gekommen ist.

## 5. *Die Bankautomatenfälle in Japan*

Die Fälle, in denen eine Person durch unbefugten Gebrauch einer gefälschten oder gestohlenen Codekarte am Geldautomaten Bargeld erbeutet, werden wie oben erwähnt nicht durch Anwendung des Art. 246-2 StrG gelöst. Man bedient sich in Japan statt dessen der klassischen Vorschrift über den Diebstahl. Nachfolgend möchte ich der thematischen Vollständigkeit halber ein Beispiel aus der japanischen Rechtsprechung dafür anführen.

---

56 So KAMIYAMA (Fn. 19) 164.

57 Urteil des DG Tokyo vom 13.2.1995, Hanrei Jihô 1529 (1995) 158 ff.

58 KAMIYAMA (Fn. 19) 164.

Dem Fall, der vor dem Distriktgericht Tokyo im Jahre 1989<sup>59</sup> verhandelt wurde, lag folgender Sachverhalt zugrunde. Der Angeklagte hatte die Bankautomatenkarte eines Arbeitskollegen entwendet, sie mit Hilfe eines Computers kopiert und sich daraufhin am Geldautomaten zum Schaden des Arbeitskollegen einen Geldbetrag in Höhe von ¥ 80.000 verschafft. Die Karte gab der Täter nach dem Kopieren wieder an den Arbeitskollegen zurück. Das Gericht erkannte hinsichtlich der Herstellung der unechten Karte auf Datenfälschung nach Art. 161-2 Abs. 1 StrG in Tateinheit mit der Verwendung falscher Daten nach Art. 161-2 Abs. 3 StrG. In Idealkonkurrenz dazu wurde Diebstahl am Geld nach Art. 235 StrG angenommen. Der Täter habe das Geld mit Zueignungsabsicht „weggenommen“. Das Entwenden der Karte wurde vom Gericht daneben als Diebstahl in Tatmehrheit bezeichnet.<sup>60</sup>

#### IV. DER COMPUTERBETRUG IM SYSTEM DER NORMEN GEGEN COMPUTERKRIMINALITÄT IM JAPANISCHEN STRAFGESETZ

Ähnlich wie in Deutschland wurde der Computerbetrug nicht als einzelne Vorschrift ins Strafgesetz aufgenommen. Es wurden daneben wichtige andere Vorschriften erlassen, um umfassend alle möglichen Formen der Computerkriminalität zu erfassen. So wurden mit dem „Gesetz zur Änderung von einigen Vorschriften auf dem Gebiet des Strafrechts“ von 1987<sup>61</sup> mehrere Normen dem StrG hinzugefügt oder verändert, die sich in drei Gruppen von Tatbeständen unterteilen lassen: Normen gegen,

- die Manipulation von Daten (angelehnt an die Urkundendelikte), Artt. 158-161 StrG und Artt. 258-259 StrG,
- betrügerischen Mißbrauch von Computern (Computerbetrug), Art. 246-2 StrG,
- Computersabotage (im Zusammenhang mit der Störung des Wirtschaftsverkehrs), Art. 234-2 StrG.

Für diese Normen gibt es auch im deutschen StGB entsprechende Vorschriften. Nicht strafbar ist in Japan die Datenspionage, so wie dies § 202 StGB in Deutschland vorsieht. Das unbefugte Benutzen von Computern, was manchmal als Zeitdiebstahl<sup>62</sup> bezeichnet wird, ist weder in Deutschland noch in Japan strafbar. In Art. 7-2 StrG hat der japanische Gesetzgeber im Gegensatz zum deutschen den Begriff „elektromagnetische Aufzeichnungen“ definiert. Demnach sind elektromagnetische Aufzeichnungen im Sinne des Gesetzes solche Aufzeichnungen, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar zum Zwecke des Einsatzes in der elektronischen Datenverarbeitung erstellt sind. Dies berücksichtigend ist Art. 246-2 StrG somit als nur ein

---

59 Urteil des DG Tokyo vom 17.2.1989, Hanrei Taimusu 700 (1989) 279 ff.

60 Vergleiche: Urteil des DG Tokyo vom 22.2.1989, Hanrei Jihô 1308 (1989) 161 ff.

61 *Keihôtô no ichibu o kaisei suru hôritsu* (Fn. 9).

62 SONODA (Fn. 3) 168.

Baustein in einem System von Strafvorschriften zur Bekämpfung der Computerkriminalität zu verstehen.

#### V. SCHLUSSBETRACHTUNG

Japan hat also genau wie Deutschland auf die Gefahren der Computerkriminalität durch eine Reform des Strafrechts reagiert. Dadurch sind verschiedene Vorschriften geändert und neue Tatbestände dem Strafgesetz hinzugefügt worden. Dabei wurde auch der Tatbestand des Computerbetrugs geschaffen, der dogmatisch wie der entsprechende deutsche Tatbestand als Sonderform des Betruges konzipiert wurde. Art. 246-2 StrG erfaßt wie § 263a StGB die Eingabe- und Programmanipulationen. Er ist jedoch nicht einschlägig bei den typischen Bankautomatenfällen, die in Deutschland den überwiegenden Teil der Anwendungsfälle bilden, sondern nur in dem speziellen Fall, in dem am Geldautomaten unbefugt Überweisungen getätigt werden. Dafür erfaßt er aber bestimmte Fälle der Leistungerschleichung, die in § 263a StGB nicht geregelt sind.

In der Rechtsprechung allerdings hat Art. 246-2 StrG bisher nur in den Fällen der Eingabemanipulationen gewisse Bedeutung erlangt. Programmanipulationen sind bisher bis auf einen Fall nicht bekannt geworden. Der Sonderfall des Codekartenmißbrauchs, den Art. 246-2 StrG erfaßt, ist bisher ebenfalls nicht aufgetreten. Auch die Tatvariante „Erschleichen von Leistungen“, die der zweite Halbsatz benennt, ist in der Rechtsprechung bisher bedeutungslos, da die Richter den Art. 246-2 StrG hierauf nicht anwenden.

Die praktische Bedeutung des Art. 246-2 StrG in Japan ist also, wie auch die eingangs angeführten Statistiken zeigten, gering. Der japanische Gesetzgeber hat den Computerbetrug als Teil einer der Computerkriminalität vorbeugenden umfangreichen Gesetzesinitiative verstanden und sicherlich erwartet, daß er in der Praxis eine größere Bedeutung erlangen würde. Die Rechtsprechung kommt aber in den meisten Fällen mit der Anwendung klassischer Tatbestände zur Lösung der auftretenden Fälle aus.