Ergebnis

Für die Sowjetunion — wie übrigens auch für andere sozialistische Länder[61] — liegt das Hauptproblem des Softwareschutzes weniger beim Schutz der geistigen Schöpfung *per se* als eher beim Schutz und noch mehr bei der Vergütung der Softwareurheber (als Stimulierung deren schöpferischer Tätigkeit).[62]

Darin kann auch der Grund erblickt werden, daß bis jetzt keine gesetzliche Regelung getroffen wurde, obwohl es im Schrifttum an Vorschlägen nicht fehlt. Die Ablehnung der erfinderrechtlichen (patentrechtlichen) Lösungen zeigt, daß die sowjetischen Fachleute jetzt eher einen Sonderschutz, evtl. einen Urheberschutz zu befürworten scheinen. Die Frage ist aber noch lange nicht gelöst. Wegen der unterschiedlichen politischen und wirtschaftlichen Verhältnisse könnten westliche Lösungen — wenn überhaupt — nur nach äußerst sorgfältiger Untersuchung mit einer evtl. Adaptation übernommen werden.

[61] Statt aller vgl. nur den Fall Ungarn bei *Vida,* Zum Urheberschutz von Rechenprogrammen in Ungarn. GRUR Int. 1987, 769ff.

[62] Vgl. *Vitalier,* Bericht der Sowjetischen Landesgruppe der AIPPI, AIPPI-Annuaire 1987/II 193ff.

Münsteraner Ringvorlesung „EDV und Recht"

Datenveränderung (§ 303a StGB)* — Teil 1

Jürgen Welp

1 Einleitung

1.1 Gesetzgebung

Das *Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität* vom 15.5.1986 (2. WiKG) (1) hat dem Strafgesetzbuch und einigen Nebengesetzen eine Sequenz von Straftatbeständen inkorporiert, deren Kernstück das sog. *Computerstrafrecht* ist. Es enthält Strafdrohungen gegen das Ausspähen von Daten (§ 202a StGB), den Computerbetrug (§ 263a StGB), die Fälschung von Daten (§§ 269, 270 StGB) und gegen die Datenveränderung (§§ 303a, 303b StGB).

Mit der Konzipierung dieser Delikte reiht sich der deutsche Gesetzgeber in die Reihe der Staaten ein, die den vermehrt gemeldeten Mißbräuchen im Bereich der automatischen Datenverarbeitung mit einer Anpassung ihrer Strafgesetzgebung begegnen (2). Zwar ist die Zahl dieser Fälle und ihr Anteil an der registrierten Gesamtkriminalität so gering, daß man geneigt sein könnte, sie vorerst zu vernachlässigen (3). Aber hiergegen spricht, daß alle Prognosen für die Entwicklung dieser Kriminalität negativ sind (4). Nicht nur mit der Vermehrung der Einsatzmöglichkeiten, sondern mehr noch mit der Ausbreitung des Fachwissens über die automatische Datenverarbeitung werden sich die bislang berichteten Einzelfälle aller Voraussicht nach auf längere Sicht zu einem beachtlichen gesellschaftlichen Phänomen steigern.

Dies gilt nicht nur für die *Zahl* der Mißbrauchsfälle, sondern mehr noch für ihre *Struktur* (5). Die vielfache Wiederholung kleinster Arbeitsschritte ist eines der Kennzeichen automatischer Datenverarbeitung. Gelingt es dem Täter daher, einen irregulären Programm-

* Gekürzte Fassung eines Vortrags zu Fragen des „Computerstrafrechts", den Verf. im Rahmen einer Ringvorlesung im Wintersemester 1987/88 an der Universität Münster gehalten hat.

(1) BGBl.I S. 721.

(2) Die rechtsvergleichenden Vorarbeiten sind von Sieber geleistet worden (vgl. OECD, Computer-related Crime: Analysis of Legal Policy, ICCP Bd.10, 1986 sowie Sieber, The International Handbook on Computer Crime. Computer-related Economic Crime and the Infringements of Privacy, 1986). — Darstellungen des „Computerstrafrechts" aus Anlaß der Verabschiedung des 2. WiKG geben Lenckner/Winkelbauer, CR 1986, 483ff, 654ff, 824ff.; Tiedemann, JZ 1986, 865, 868ff; Achenbach, NJW 1986, 1835, 1837f; Granderath, DB, Beilage Nr.18/86; Möhrenschlager, wistra 1986, 128ff; Haft, NStZ 1987, 6ff.; Schlüchter, Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität, 1987, S. 57ff.; Bühler, MDR 1987, 448ff. — Das japanische Gesetz aus dem Jahre 1987 ist von der deutschen Gesetzgebung beeinflußt (Sonoda, wistra 1988, 167, 173).

(3) Haft, NStZ 1987,6.

(4) Sieber, Computerkriminalität und Strafrecht, 2. Aufl. 1980, S. 179ff.

(5) Sieber, Computerkriminalität und Strafrecht, S. 126ff.

teil in einem fremden Rechnersystem zu installieren, so wird die kontinuierliche Tatausführung durch den Ablauf des Programms besorgt. Für den Täter sinkt damit das Entdeckungsrisiko, während sich der Schaden des Opfers summiert. Vielfach wiederholte Überweisungen geringer Beträge, die dauernde Abzweigung von unauffälligen Pfennigbruchteilen oder sich selbst kopierende Virusprogramme sind praktische Beispiele hierfür. Man hat im Bereich des Computermißbrauchs mehr als bei anderen Formen der Kriminalität mit dem Risiko zu rechnen, daß fachkundige Täter ihren „großen Coup" vorbereiten. Die Notwendigkeit qualifizierter Planung wirkt hierbei gelegentlich als Herausforderung und zusätzlicher Antrieb.

Auch die Sensibilität vieler sozialer Bereiche, in denen der Einsatz automatischer Datenverarbeitung realisiert oder geplant ist, spricht für frühzeitige gesetzliche Maßnahmen gegen Computerkriminalität. Ein mit den Mitteln der EDV geführtes Grundbuch oder Bundeszentralregister zum Beispiel ist ohne einen begleitenden Strafschutz ebensowenig vorstellbar wie etwa das „home banking" der Kreditwirtschaft.

Der Begriff der „Computerkriminalität" (6) ist nun zwar populär, für eine juristische Kategorisierung indessen wenig brauchbar. Versteht man darunter alle Fälle, in denen die automatische Datenverarbeitung Objekt oder Mittel der Begehung beliebiger Straftaten (Betrug, Untreue, Bilanz- und Steuerdelikte etc.) ist, so besitzt der begriff der Computerkriminalität keinen größeren Erkenntniswert als etwa der der Kraftfahrzeugkriminalität.

Auch der Begriff des *Computerstrafrechts* ist hiernach für dogmatische Zwecke ohne hinreichende juristische Präzision (7), selbst wenn man ihn den Tatbeständen vorbehält, die das *2. WiKG* geschaffen hat. Der Tatbestand des *Ausspähens von Daten* (§ 202a StGB) schützt das Interesse an der Wahrung ihrer Vertraulichkeit und läßt sich daher als Fall strafbarer Geheimnisverletzung deuten. Der *Computerbetrug* (§ 263a StGB) ist hingegen ein Vermögensdelikt, bei dem die Verwendung unrichtiger Daten Mittel der Herbeiführung eines Vermögensschadens ist. Seine Poenalisierung beruht auf der Annahme, daß Täuschung und Irrtum als Tatbestandsmerkmale des Betruges auf die Beeinflussung maschinell gesteuerter Zahlungsvorgänge nicht anwendbar sind. Der Tatbestand der *Fälschung beweiserheblicher Daten* (§ 269 StGB) gehört demgegenüber in den Zusammenhang der Urkundsdelikte; er schützt das Vertrauen des Rechtsverkehrs in die Echtheit beweiserheblicher Daten. Der Tatbestand der *Datenveränderung* (§ 303a StGB) schließlich zeigt konstruktive Ähnlichkeiten mit dem Delikt der Sachbeschädigung, gewährt seinen Schutz jedoch nicht körperlichen Sachen, sondern unkörperlichen Daten.

Es liegt auf der Hand, daß sich ein solches Sammelsurium von Rechtsgütern keinem übergreifenden dogmatischen Interesse erschließen wird. Betrachtet man die Delikte des „Computerstrafrechts" allerdings unter dem Aspekt der durch sie verletzten *Angriffsobjekte,* so besteht — unter Ausscheidung des Computerbetruges — insofern eine Gemeinsamkeit, als sie sich gegen *Daten* richten. Damit scheinen sich die Konturen eines *Datenstrafrechts,* also eines strafrechtlichen Normenkomplexes abzuzeichnen, der *Datensicherheit* unter den Aspekten der Vertraulichkeit (§ 202a StGB), der Echtheit (§ 269 StGB) und der Integrität (§ 303a StGB) von Daten gewährleistet. Der systematische Gewinn auch einer solchen Betrachtungsweise übersteigt indessen nicht den Wert einer vorgestellten Zusammenfassung von Diebstahl, Unterschlagung, Sachbeschädigung etc. in einem Begriff des „Sachenstrafrechts". Mehr als eine Feststellung der Identität des Angriffsobjekts ist hiervon nicht zu erwarten. -

Der vorliegende Beitrag erörtert mit dem Tatbestand der *Datenveränderung* (§ 303a StGB) dasjenige Delikt des „Datenstrafrechts", das der Erhaltung der *physischen Integrität* von Daten dient.

2 Tatobjekt

2.1 Daten

Die verschiedenen Tathandlungen, die in § 303a StGB unter Strafe gestellt sind, richten sich gegen das gemeinsame *Tatobjekt* der *Daten.*

Zur Bestimmung dieses Begriffs verweist das Gesetz auf die *Legaldefinition* eines anderen Tatbestandes (§ 202a Abs. 2 StGB) und schließt damit jede Modifikation des Datenbegriffs aus, die mit einer besonderen ratio legis des 303a StGB begründet wäre. Daten im Sinne *beider* Tatbestände sind hiernach „nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden".

Offenbar enthält diese Bestimmung lediglich die *Einschränkung* eines vorausgesetzten Datenbegriffs, nicht aber diesen selbst (8). Die juristische Bestimmung eines *technischen* Begriffs wird daher zunächst den technischen Sprachgebrauch zur Kenntnis nehmen (9). Nach DIN 44300 Nr.19 sind Daten solche „Informationen", die auf Grund „bekannter oder unterstellter Abmachungen zum Zwecke der Verarbeitung" durch „Zeichen oder kontinuierliche Funktionen" dargestellt werden (10).

(6) Zu seinen Konturen Lenckner, Computerkriminalität und Vermögensdelikte, 1981, S. 13ff.; Sieber, Computerkriminalität und Strafrecht, S. 184ff., 2/137ff.

(7) Haft, NStZ 1987,6.

(8) Lenckner/Winkelbauer, CR 1986, 484; Lackner, StGB, 17. Aufl. 1987, § 263a Anm. 3a; Jähnke, LK, 10. Aufl. 1988, StGB § 202a Rdn.3; Haft, Strafrecht, BT, 3. Aufl. 1988, S. 70; Maurach/Schroeder/Maiwald, Strafrecht, BT I, 7. Aufl. 1988, S. 280.

(9) Vgl. Samson, SK, StGB § 202a Anm. II 1; Lackner, StGB § 261a Anm. 3 a; Lenckner, Schönke/Schröder, StGB § 202a Rdn. 3.

(10) Auf den in der technischen Norm als weiteres Merkmal genannten *Verarbeitungszweck* kommt es für den Rechtsbegriff des Datums nicht an. Auch das *Ergebnis* einer Datenverarbeitung, das keiner weiteren Verarbeitung bedarf, unterfällt dem Datenbegriff. Vgl. Möhrenschlager, wistra 1986, 128, 132; Lenckner/Winkelbauer, CR 1986, 483, 484; Lenckner, Schönke/Schröder, StGB § 202a Rdn. 3; Lackner, StGB § 263a Anm. 3a; Maurach/Schroeder/Maiwald, Strafrecht, BT 1, S. 226.

Der Datenbegriff besitzt hiernach zwei Ebenen, eine erste der Semantik und eine zweite der Syntax; sie schichten die Bedeutung (Inhalt) eines Datums von seiner Darstellung (Zeichen) ab (11).

Die semantische Ebene betrifft den *Informationsgehalt* des Datums, für den weder der technische noch der juristische Sprachgebrauch irgendeine Einschränkung bereithalten. Information ist daher die Kenntnisbeziehung zu *jedem* realen und irrealen Gegenstand der Welt. Es bedarf keiner „weiten" Auslegung (12) dieses Aspekts, um dem Schutzzweck des Tatbestandes gerecht zu werden; er ist per se grenzenlos. Eine Konkretisierung der mannigfaltigen Dateninhalte kann daher nur in der Warnung vor der irrtümlichen Ausgrenzung bestimmter Informationsgehalte bestehen. Ob der Dateninhalt eine Gedankenerklärung oder ein maschinell erzeugter Code, geheim oder personenbezogen ist, aus einem Zugangscode besteht, Gegenstand, Mittel oder Ergebnis einer Datenverarbeitung ist (13): auf diese und alle anderen inhaltlichen Umstände kommt es offensichtlich deswegen *nicht* an, weil der Informationsgehalt überhaupt kein begrenzendes Kriterium des Datenbegriffs ist (14).

Die Ebene der Syntax betrifft die *Darstellung* der Information durch Zeichen, die auf Grund einer Konvention für den Dateninhalt stehen. Daten sind also der *Code* einer Information. Über dessen Art ergeben sich aus dem Datenbegriff selbst keine weiteren Aufschlüsse (15), wohl aber aus den einschränkenden Kriterien des § 202a Abs.2 StGB.

2.2 Speicherung und Übermittlung von Daten

Diese Norm behält den strafrechtlichen Schutz solchen Daten vor, die „gespeichert sind oder übermittelt werden". Beide Merkmale betreffen die *Objektivierung* (Verkörperung, Fixierung) der codierten Information (16). Sie tragen dem Umstand Rechnung, daß ein Datum als Angriffsobjekt materialisiert sein muß, um einer kriminellen Aktivität zugänglich zu werden.

Den Begriff der *Speicherung* definiert § 2 Abs.2 Nr.1 BDSG als „das Erfassen, Aufnehmen oder Aufbewahren von Daten auf einem Datenträger zum Zwecke ihrer weiteren Verwendung" und bietet damit auch der strafrechtlichen Interpretation einen Anknüpfungspunkt (17). Unter dem Erfassen und Aufnehmen von Daten hat man alle Formen ihrer Verkörperung auf einem Datenträger zu verstehen. Datenträger ist hierbei jedes Medium, das zur Fixierung und zur Wiedergabe von Daten geeignet ist (18). Insoweit stimmen die datenschutzrechtliche und die strafrechtliche Begriffsbildung überein. Eine Übernahme der Verwendungsklausel und der daraus abgeleiteten Folgerungen verbietet sich jedoch (19). Vorgänge von nur „maschineninterner Bedeutung" wie das Einladen von Daten in den Kernspeicher des Rechners mögen für das Datenschutzrecht irrelevant sein (20), weil seine Kautelen nur für eine Datenhaltung „von gewisser Dauer" sinnvoll sind (21). Das Interesse an der Integrität von Daten ist hingegen nicht mit der Dauerhaftigkeit ihrer Speicherung (auf Festspeichern) verbunden, sondern besteht für jede Form ihrer Verkörperung.

Auch für den Begriff der *Übermittlung* enthält das Datenschutzrecht eine Legaldefinition. Nach § 2 Abs.2 Nr.2 BDSG ist darunter „das Bekanntgeben gespeicherter oder durch Datenverarbeitung unmittelbar gewonnener Daten an Dritte" zu verstehen, „in der Weise, daß die Daten durch die speichernde Stelle weitergegeben oder zur Einsichtnahme, namentlich zum Abruf bereitgehalten werden". Offenbar ist diese Begriffsbestimmung, die auf die Schutzbedürfnisse der vom Dateninhalt Betroffenen zugeschnitten ist, für die Interpretation des Straftatbestandes unverwendbar (22). Sie schließt den Datenfluß innerhalb der speichernden Stelle vom Begriff der Übermittlung aus (23), verlangt für die Weitergabe die Vermittlung der Kenntnis vom Dateninhalt (24) und fingiert, daß schon die Bereithaltung der Daten zum Abruf oder zu anderen Formen der Einsichtnahme als Übermittlung anzusehen sei. Keine dieser Folgerungen ist mit dem Schutzzweck eines Strafgesetzes verträglich, das auf die Erhaltung der Integrität von Daten abzielt. Unter Übermittlung ist vielmehr jede — drahtgebundene oder drahtlose — Weiterleitung von Daten zu verstehen, insbesondere der On-line-Verkehr von Rechner zur Rechner innerhalb eines Netzwerks oder über Fernmeldewege. Der Transport körperlicher Datenträger ist hingegen keine Datenübermittlung im Sinne des Gesetzes, da gespeicherte Daten bereits unter die erste Alternative der Einschränkungsklausel fallen. -

(11) Vgl. Ringwald, JZ 1983,291,293.

(12) Lackner, StGB § 202a Anm.3a; Lenckner, Schönke/ Schröder, StGB § 202a Rdn.3; Granderath, Der Betrieb, Beilage Nr.18/86, S. 1.

(13) Samson, SK, StGB § 202a Rdn. 4; Dreher/Tröndle, StGB § 268 Rdn. 4; Lenckner, StGB § 202a Rdn. 3; Lackner, StGB § 263a, Anm.3a; Bühler, MDR 1987, 448, 452.

(14) Die von Lackner (StGB § 263a Anm.3a) vorgeschlagene Exemtion „bestimmter Gruppen von Daten", die außerhalb des „Schutzzwecks" des betreffenden Tatbestandes lägen, kann daher nicht über eine Restriktion des Datenbegriffs erfolgen.

(15) Daß die Daten im Rahmen des § 303a StGB *nicht* „gegen unberechtigten Zugang besonders gesichert" zu sein brauchen (Samson, SK, StGB § 303a Rdn. 9; Stree, Schönke/Schröder, StGB § 303a Rdn. 2), ergibt sich formal bereits aus der Verweisungstechnik des Gesetzes. Das Merkmal hat bei § 202a Abs.1 StGB lediglich die Funktion, den *Geheimhaltungs*willen des Berechtigten zu dokumentieren; Mangel berührt also das in § 303a StGB geschützte Interesse an der *Erhaltung* der Daten nicht.

(16) Simitis/Dammann/Mallmann/Reh, BDSG § 2 Rdn.82.

(17) Dreher/Tröndle, StGB § 202a Rdn. 4; Lenckner, Schönke/ Schröder, StGB § 202a Rdn. 4.

(18) Simitis/Dammann/Mallmann/Reh, BDSG § 2 Rdn. 82; Schweinoch/Geiger, Art.5 Anm. 6; Ordemann/Schomerus, BDSG, 4. Aufl. 1988, § 2 Anm. 2.1.

(19) Vgl. dazu bereits Fußn. 12.

(20) Simitis/Dammann/Mallmann/Reh, BDSG § 2 Rdn. 87; Ordemann/Schomerus, BDSG § 2 Anm. 2.1; Tinnefeld/Tubies, Datenschutzrecht, 1988, S. 44.

(21) Leib, ÖVD 1978,22; Tinnefeld/Tubies, aaO S. 43; Ordemann/Schomerus, BDSG § 2 Anm.2.1.

(22) A.A. Dreher/Tröndle, StGB § 202a Rdn. 5.

(23) Auernhammer, BDSG § 2 Rdn.10; Rückriegel/v.d.Groeben/ Hunsche, aaO Anm.7; Schweinoch/Geiger, Art.5 Anm.6.

(24) Auernhammer, BDSG § 2 Rdn.10.

Der Zuwachs an Merkmalen, den der Datenbegriff durch § 202a Abs. 2 StGB erfährt, besteht also darin, daß die codierte Information in einem Speicher- oder Übermittlungsmedium objektiviert sein muß, um zum Gegenstand strafrechtlichen Schutzes zu avancieren.

2.3 „Wahrnehmbarkeit" von Daten

Den Forderungen der Legaldefinition ist auch damit noch nicht genügt. Vielmehr stellt § 202a Abs. 2 StGB darüber hinaus Ansprüche an die Form der Objektivierung von Daten und verlangt, daß sie *„elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar"* gespeichert sein oder übermittelt werden müßten. Elektronische und magnetische Verkörperungen von Daten sind dabei nach Wortlaut und Sinn des Gesetzes lediglich Beispiele mangelnder unmittelbarer Wahrnehmbarkeit, die nur wegen ihrer besonderen praktischen Bedeutung hervorgehoben sind. Der Tatbestand soll hiermit für andere — bereits verwendete (z.B. CD-ROM) oder im Zuge der technischen Entwicklung erwartbare — Methoden der Speicherung und Übermittlung von Daten offengehalten werden (25).

Daten sind dann unmittelbar wahrnehmbar, wenn ihre Darstellung mit den Sinnen erfaßt (26), also vor allem gesehen oder gehört werden kann. Bedarf es hingegen einer technischen „Umformung" (27), um sie der Sinneswahrnehmung zugänglich zu machen, etwa einer Ausgabe auf Bildschirm, Drucker oder Lautsprecher, so sind sie nicht unmittelbar wahrnehmbar. Die Wahrnehmbarkeit bezieht sich hierbei auf die Syntax der Daten, nicht auf ihre Semantik. Auf eine Wahrnehmbarkeit des Bedeutungsgehalts kommt es daher nicht an (28). Ist das Datum an den Zeichen erkennbar, durch die es objektiviert ist, so entfällt der Schutz des § 303a StGB auch dann, wenn der Informationsgehalt verborgen bleibt. *Lochkarten* oder Lochstreifen beispielsweise enthalten zwar codierte Informationen; da deren Darstellung jedoch sichtbar und damit unmittelbar wahrnehmbar ist, besitzen sie den Schutz des Datenstrafrechts auch dann nicht, wenn der Informationsgehalt unerkennbar bleibt (29).

Die Abgrenzungsprobleme, die diese Bestimmung mit sich bringt, ergeben sich aus der Quantifizierbarkeit des Wahrnehmungsvermögens, wie das Beipiel der visuellen Wahrnehmung zeigt. Sind Daten etwa auf Mikrofilm gespeichert, so bedarf es lediglich einer Vergrößerung, nicht aber einer technischen *Umformung*, um sie der Wahrnehmung zugänglich zu machen. Wollte man dieserhalb bestreiten, daß sie der gesetzlichen Definition entsprechen (30), so hätte man nicht nur das COM/CIM-System (computer output/input on microfilm), sondern jedes optische Aufzeichnungsverfahren aus dem Anwendungsbereich des Gesetzes ausgeschlossen (31).

Man darf daher bezweifeln, ob mit dem Merkmal der unmittelbaren Wahrnehmbarkeit von Daten ein Kriterium gewonnen ist, das dem Schutzzweck des Gesetzes gerecht wird. Es entspräche seiner Logik besser, wenn nur solche Daten als Angriffsobjekt zugelassen wären, die — ohne Rücksicht auf ihre unmittelbare Wahrnehmbarkeit - in einer für die automatische Datenverarbeitung tauglichen Weise codiert sind (32). Auch diese Bestimmung hätte indessen das Bedenken gegen sich, daß die Fortschritte der Scan-Technik im Grundsatz *jedes* Zeichen zu einem für den Rechner lesbaren Datum gemacht haben.

Die erörterten Schwierigkeiten zeigen im übrigen nur, daß der „Wettlauf zwischen Technik und Strafgesetzgeber" (33) von diesem nicht gewonnen werden kann. Es ist auch nicht die Funktion von Strafgesetzen, sozialen Unzuträglichkeiten vorzubeugen, die ihr Dasein einstweilen nur in der technischen Phantasie von Sachverständigen führen. Eine abschließende Enumeration tauglicher Speicher- und Übermittlungsverfahren wäre daher trotz erwartbarer Strafbarkeitslücken die vorzugswürdige gesetzliche Regelung gewesen.

Für die Auslegung des geltenden Rechts wird man sich mit der Konstruktion einer begrifflichen Differenz zwischen den Hilfsmitteln „natürlicher" Wahrnehmung (Brille, Lupe, Hörgerät) einerseits und den Instrumenten „künstlich" erweiterter Wahrnehmungsfähigkeit (Mikroskop, Verstärker, Sensor) andererseits behelfen müssen. Die Unschärfen, die hierdurch entstehen, sind im Gesetz selbst angelegt und nur durch dessen Änderung zu beheben. -

Damit sind die begrifflichen Konturen des Tatobjekts „Daten" ausgezogen.

3 Datenzuordnung

3.1 „Eigene" und „fremde" Daten

Die gesetzliche Deliktsbeschreibung faßt die Tathandlungen des § 303a StGB (Löschen, Unterdrücken, Unbrauchbarmachen und Verändern von Daten) im Begriff der „Datenveränderung" zusammen. Das Verändern von Daten ist nun aber ein *sozialadäquates* Verhalten, mit dem zwar die Tätigkeit ganzer Berufsgruppen, nicht aber kriminelles Unrecht angemessen bezeichnet werden kann. Programmierer und Datentypisten sind gewerbsmäßige Daten*veränderer*. Kein

(25) Dreher/Tröndle, § 202a Rdn. 6;

(26) Vgl. Jähnke, LK, StGB § 202a Rdn. 4.

(27) Samson, SK, StGB § 202a Rdn. 6; Lackner, StGB § 202a Anm. 2; Lenckner, Schönke/Schröder, StGB § 202a Rdn. 4.

(28) Lenckner/Winkelbauer, CR 1986,484; ebenso wohl Lackner, StGB § 202a Anm.2.

(29) Lenckner/Winkelbauer, CR 1986, 484; Lackner, StGB § 202a Anm. 2; Sonoda, wistra 1988, 167, 170. Unklar Schlüchter, aaO S. 60f.

(30) Samson, SK, StGB § 202a Rdn. 7; Jähnke, LK, StGB § 202a Rdn. 4.

(31) Die „Umformung", der die auf einer Compact Disk gespeicherten Daten bedürfen, betrifft die Wiedergewinnung des *Informationsgehalts* aus dem Bitmuster mikroskopisch kleiner Vertiefungen, also die Bedeutungsebene, auf die es für die Frage der Wahrnehmbarkeit nicht ankommt. Die Vertiefungen selbst sind mit geeigneten Hilfsmitteln (Laser, Mikroskop) erkennbar, so daß zu den analog verkleinerten Darstellungen auf einem Mikrofilm unter dem hier erörterten Gesichtspunkt kein Unterschied besteht.

(32) Vgl. auch Dreher/Tröndle, StGB § 268 Rdn. 4; Lenckner, Schönke/Schröder, StGB § 202a Rdn. 3.

(33) Haft, NStZ 1987, 5.

Rechner und kein Programm ist funktionsfähig, ohne daß zumindest die für den Programmablauf notwendigen Daten fortwährend und in großer Zahl „verändert" werden; es ist sinnlos, die Veranlassung dieses Vorgangs als tatbestandsmäßiges Unrecht zu qualifizieren.

Ein Tatbestand, der undifferenziert die Veränderung von Daten unter Strafe stellt, enthält daher keinen *vollständigen* Unrechtstypus (34), sondern bedarf der Ergänzung durch ein (ungeschriebenes) einschränkendes Tatbestandsmerkmal, das den im Gesetz genannten Merkmalen *berichtigend* hinzuzufügen ist (35).

Es steht nun offenbar jedermann frei, mit seinen *„eigenen"* Daten nach Belieben zu verfahren und an ihnen die Handlungen vorzunehmen, die der Wortlaut des Gesetzes verbietet, sie also zum Beispiel zu löschen oder zu verändern. Wenn dem Gesetz daher ein verständiger Inhalt unterlegt werden soll, kann es ernstlich nur so verstanden werden, daß die Verletzung ausschließlich *„eigener"* Interessen an der Integrität von Daten nicht unter Strafe stehen soll (36).

Das formale Defizit des Tatbestandes besteht somit darin, daß er das Verändern von Daten mit Strafe bedroht, ohne auf die Notwendigkeit weiterer Restriktionen auch nur hinzuweisen. Damit bleibt auch die Frage nach den sachlichen Kriterien der *Datenzuordnung* offen. Eine solche Gesetzestechnik steht zu dem Postulat des *nullum crimen sine lege* in offenem Widerspruch und setzt den neuen Tatbestand ernstlichen verfassungsrechtlichen Zweifeln aus (37).

Auch wenn man sie für unbegründet hält, wird mit der Entwicklung der Zuordnungskriterien der Weg in eine ungewisse juristische Zukunft eingeschlagen. Zwar mag es naheliegen, die in § 303 StGB für *Sachen* gegebene Zuordnung auf Daten zu übertragen. Tatbestandsmäßig wäre hiernach nur eine Veränderung solcher Daten, die für den Täter *„fremd"*, also einem anderen Rechtssubjekt zugeordnet sind (38). Ein *„Dateneigentum"*, also ein dem Sachenrecht analoges Zuordnungssystem für *unkörperliche* Daten, gibt es nun aber *nicht* (39). Der Erkenntnisgewinn, der mit der Identifizierung „eigener", „fremder" und „herrenloser" Daten verbunden ist, bleibt daher rein formal, solange die materiellen *Kriterien* nicht definiert sind, die über die Zuordnung von Daten entscheiden.

3.2 Zuordnungskriterien

Als Anknüpfungspunkt für ihre Nominierung bieten sich die zuvor erörterten Eigenschaften des Tatobjekts an. Das Interesse an der Integrität von Daten wird von dem Gesetz erst mit ihrer Verkörperung als schutzwürdig anerkannt, also mit ihrer „Materialisierung" in einem Speicher- oder Übermittlungsmedium. Zuordnungskriterien können sich daher einerseits aus der *Initiierung* von Speicherung oder Übermittlung und andererseits aus der *Beherrschung* des Speicher- oder Übermittlungsmediums ergeben.

Der zuerst genannte Vorgang besteht regelmäßig in einem *„Skripturakt"* oder in einem analog hierzu vorzustellenden Akt der Datenerzeugung, also in der *Eingabe* der zu speichernden oder zu übermittelnden Daten in eine Datenverarbeitungsanlage. Diese kann unmittelbar über die Konsole des Geräts, automatisch durch programmierte Funktionen des Rechners oder durch die selbsttätige Einspeisung anderweit erzeugter Meßwerte (40) oder sonstiger Daten erfolgen.

Nimmt man nun an, daß die Datenzuordnung durch diesen Entstehungsvorgang mitbedingt ist, so wäre „Dateninhaber" zunächst derjenige, der die Daten erzeugt, also ihre Speicherung oder Übermittlung *selbst unmittelbar bewirkt* hat, sei es durch Eingabe der Daten, sei es durch den Start eines selbsttätig speichernden Programms oder durch Bewirkung der Einspeisung externer Daten.

Für diese Annahme spricht — in Ermangelung aller normativen Vorgaben — nichts weiter als eine gewisse Plausibilität. Unter der Voraussetzung, daß Rechte und Interessen Dritter an den gespeicherten oder übermittelten Daten nicht ersichtlich sind, ist der „Skripturakt" das *einzige* Kriterium, das eine Zuordnung der Daten in die Rechtssphäre ihres Urhebers bewirken kann. Würde seine Gültigkeit bestritten, so gäbe es — vorbehaltlich der aus der Beherrschung des Speichermediums zu gewinnenden Kriterien — weder „eigene" noch „fremde" Daten. Denn wenn selbst die urheberschaftliche *Hervorbringung* von Daten keinen tauglichen Zuordnungstatbestand abzugeben vermöchte, könnte der *Veranlassung* dieses Vorgangs im Rahmen von Dienst-

(34) Lenckner/Winkelbauer, CR 1986, 828. Ähnlich Samson, aaO Rdn. 3ff; Lackner, StGB § 303a Anm. 4; Stree, Schönke/Schröder, StGB § 303a Rdn. 3; Frommel, JuS 1987,667; Schlüchter, aaO S. 74.

(35) Diese Annahme setzt voraus, daß der (geschlossene) Tatbestand Träger *aller* unrechtskonstitutiven Merkmale des betreffenden Delikts ist. Folgt man ihr, so ist es eine Frage terminologischen Beliebens, ob man das in § 303a Abs.1 StGB genannte Merkmal „rechtswidrig" als Sitz der einschränkenden Kriterien und damit als Tatbestandsmerkmal (Dreher/Tröndle, aaO Rdn.9; Lackner, aaO Anm.4) oder lediglich als allgemeines Deliktsmerkmal (so m.E. zu Recht Lenckner/Winkelbauer, CR 1986,828f.; Stree, aaO Rdn.6) versteht (vgl. auch Samson, aaO Rdn.5). Insbesondere ist die Verfassungsmäßigkeit der Vorschrift nicht hiervon, sondern von der Bestimmbarkeit und Bestimmtheit der verwendeten materiellen Einschränkungskriterien abhängig.

(36) Ebenso Lackner, aaO Rdn.3; Dreher/Tröndle, aaO Rdn.9; wohl auch Stree (aaO Rdn.3); vgl. ferner Samson, aaO Rdn.7.

(37) Samson, aaO Rdn. 3, 8; vgl. auch Frommel, JuS 1987,667,668.

(38) Auf die explizite Einführung eines Tatbestandsmerkmals der Fremdheit ist, wie Lenckner/Winkelbauer, CR 1986, 828 bemerken, zwar verzichtet worden. Er enthält indessen eine plastische Abbreviatur der sachlichen Zuordnungskriterien, die diesen Begriff konstituieren. Einen Eingriff in eine „fremde" Rechtsposition verlangen zu Recht auch Lackner, aaO Anm.4; Dreher, aaO Rdn.9; Stree, aaO Rdn.3.

(39) Samson, aaO Rdn.7,13.

(40) Der Begriff des Datums setzt bezüglich seines Informationsgehalts — anders als der Begriff der Urkunde — nicht notwendig eine menschliche Gedankenerklärung voraus; vielmehr genügen auch die von dem Rechner gewonnenen oder erhobenen Daten. Die Unterscheidung von Gedankenerklärungen und technischen Aufzeichnungen, die die Grenze zwischen Urkundenfälschung (§ 267 StGB) und der Fälschung technischer Aufzeichnungen (§ 268 StGB) markiert, ist für den Anwendungsbereich des § 303a StGB daher ohne Bedeutung (Samson, aaO Rdn. 11).

oder Auftragsverhältnissen eine solche Wirkung um so weniger zugesprochen werden. Als „Dateninhaber" muß also zunächst derjenige gelten, der die Daten durch Speicherung oder Übermittlung selbst *hervorgebracht* hat.

Allerdings darf dieser Aspekt schon deswegen nicht absolut gesetzt werden, weil sich mit dem *Datenmedium,* das für die Entstehung des Angriffsobjekts nicht weniger notwendig ist als dessen Speicherung oder Übermittlung, ein *zweiter* Bezugspunkt der Datenzuordnung anbietet.

Ist das Speicher- oder Übermittlungsmedium eine körperliche Sache, so ist dessen Zuordnung eine Funktion der *Eigentumsordnung.* Unter der Voraussetzung wiederum, daß Rechte Dritter nicht bestehen, schließt das Vollrecht Eigentum die Befugnis ein, mit dem Medium nach Belieben zu verfahren, sich also vor allem seiner Speicher- oder Übermittlungsfunktionen zu bedienen. Das Eigentum am Datenmedium umfaßt unter der genannten Bedingung daher auch die Befugnis, über Daten zu verfügen, die in ihm gespeichert sind oder von ihm übermittelt werden. Auch der *Medieneigentümer* ist deswegen potentieller Dateninhaber (41).

Erörterungsbedürftig ist nun zunächst das gegenseitige *Verhältnis* beider Zuordnungsfaktoren. Fallen die Vornahme des „Skripturakts" und die Innehabung des Medieneigentums *auseinander,* so wird zu unterscheiden sein, ob der „Skripturakt" mit oder ohne den *Willen* des Medieneigentümers erfolgt. Im zweiten Falle wird das Medium unter Verletzung fremden Eigentums beansprucht. Jede Verfügung über Daten von seiten des „Skribenten" wäre ein weiterer Zugriff auf fremdes Eigentum, zu dessen Duldung der Inhaber nicht verpflichtet ist. Er selbst ist bei einer solchen Konstellation daher alleiniger Dateninhaber (42). Ist er mit der Benutzung hingegen einverstanden (z.B. bei Miete, Leasing, Verkauf unter Eigentumsvorbehalt, Gefälligkeit etc.), so kommt es darauf an, wem die Verfügung über die Daten nach dem Sinn der getroffenen Vereinbarung zustehen soll. Dies ist in aller Regel der „Skribent" als Urheber der Speicherung oder Übermittlung, wenn diese in seinem Interesse erfolgt. In einem solchen Falle ist er Inhaber der Daten, während sie auch für den Eigentümer des Trägermediums „fremd" (43) sind.

Problematischer sind solche Fälle, in denen die Speicherung oder Übermittlung durch einen anderen als denjenigen veranlaßt ist, der diesen Vorgang ausführt. *Auftragsverhältnisse* dieser Art sind bei arbeitsteiligen Funktionsabläufen die Regel. Ihre Beurteilung weist ohne normative Grundlage ein hohes Maß an Beliebigkeit auf. Die Literatur neigt dazu, die „Datenherrschaft" in solchen Fällen dem Auftraggeber zuzusprechen (44). Dies kann jedoch nur unter der Voraussetzung angenommen werden, daß das Datenwerk dem Auftraggeber entweder „abgeliefert" worden oder in allen Einzelheiten nach dessen Weisung bearbeitet worden ist (45).

In der Literatur wird schließlich angenommen, daß eine tatbestandsmäßige Datenveränderung — ohne Rücksicht auf „Skripturakt" und Medieneigentum — auch an solchen Daten vorgenommen werden könne, von deren Inhalt ein Dritter in seinen schutzwürdigen Rechten *betroffen* ist (46). Die Datenzuordnung bezieht sich indessen nicht auf den Dateninhalt, sondern auf dessen *Objektivierung* in gespeicherten oder übermittelten Zeichen. Es genügt daher nicht, daß ein disparates rechtliches Interesse am Dateninhalt, beispielsweise ein Recht auf „informationelle Selbstbestimmung", besteht. Vielmehr kommt es darauf an, wer über die Integrität der *gespeicherten oder übermittelten* Daten zu verfügen hat. Dies ist der vom Dateninhalt Betroffene nur unter der Voraussetzung, daß die Datenhaltung und jeder Vorgang der Datenverarbeitung von seiner Zustimmung abhängig ist. -

Die zuvor erörterten Eigenschaften des Angriffsobjekts Daten sind also um deren Zuordnung zu einer fremden Rechtssphäre zu ergänzen.

3.3 Rechtsgut

Das *Rechtsgut,* das von § 303a geschützt wird, besteht nach einer in der Literatur geläufigen Formulierung in dem „Interesse des Verfügungsberechtigten an der unversehrten Verwendbarkeit der in den gespeicherten Daten enthaltenen Informationen" (47).

Diese Auffassung deckt sich im wesentlichen mit den hier angestellten Überlegungen zur Natur des Angriffsobjekts. Das „Interesse des Verfügungsberechtigten" ist das Recht des Dateninhabers, das dieser durch Erfüllung eines Zuordnungstatbestandes erwirbt. Es besteht in einem Vollrecht über Daten und umfaßt die Befugnis, mit ihnen nach eigenem Willen zu verfahren und Dritte hiervon auszuschließen. Es dient der Erhaltung eines Gegenstandes, von dessen Bestand die Funktionsfähigkeit vielfältiger Abläufe in allen Lebensbereichen abhängt und der aus diesem Grunde einen hohen wirtschaftlichen Wert besitzen *kann* (48). Der

(41) Ebenso Samson, aaO Rdn.14f.; a.A. Tröndle, aaO Rdn.9; undeutlich Stree, aaO Rdn.3.

(42) Ebenso Samson, aaO Rdn. 16.

(43) Samson, aaO Rdn. 15.

(44) Samson, aaO Rdn.17; Tröndle, aaO Rdn.9; Lackner, aaO Anm.4; Stree, aaO Rdn.3.

(45) Nach Ansicht von Lenckner/Winkelbauer, CR 1986,829 genügt den Zuordnungskriterien auch ein *Besitz- oder Nutzungsrecht* (etwa auf Grund eines Mietverhältnisses). Dies kann indessen nicht zugegeben werden, da die genannten Rechte kein Verfügungsrecht über die Integrität der Daten einschließen. Es ist zudem auch kriminalpolitisch kaum plausibel, Nutzungsrechten an Daten strafrechtlichen Schutz zu gewähren, ihn Nutzungsrechten an Sachen aber vorzuenthalten.

(46) Tröndle, Dreher/Tröndle, StGB § 303a Rdn. 9; Lackner, StGB § 303a Anm. 4 (unter der Voraussetzung, daß dem Dritten ein Recht auf Unversehrtheit der Daten zustehe); Möhrenschlager, wistra 1986, 128, 141; Bühler, MDR 1987, 448, 455; abl. Lenckner/Winkelbauer, CR 1986, 829; Haft, NStZ 1987, 6,1 0; Samson, SK, StGB § 303a Rdn. 19; Stree, Schönke/Schröder, StGB § 303a Rdn. 3. Unklar Schlüchter, aaO S. 74.

(47) Stree, Schönke/Schröder, StGB § 303a Rdn. 1; ähnlich Dreher/Tröndle, StGB § 303a Rdn. 2; Lackner, StGB § 303a Anm. 1; Möhrenschlager, wistra 1986, 128, 141; Granderath, DB, Beilage Nr.18/86, S. 2; Bühler, MDR 1987, 448, 445; Frommel, JuS 1987, 667, 668; kritisch Samson, SK, StGB § 303a Rdn. 1.

(48) Tröndle, Dreher/Tröndle, StGB § 303a Rdn. 1.

strafrechtliche Schutz ist hiervon jedoch unabhängig, gilt also auch solchen Daten, die *wirtschaftlich wertlos* sind (49). Dieser Umstand unterscheidet indessen den strafrechtlichen Schutz der Daten nicht von dem des Eigentums und schließt es daher nicht aus, das Verfügungsrecht über Daten als ein *spezialisiertes Vermögensrecht* (50) (Immaterialgüterrecht) zu qualifizieren, dessen Struktur dem Urheberrecht verwandt ist.

Es bleibt hinzuzufügen, daß die gesetzliche Bezeichnung des Tatbestandes als „Datenveränderung" nicht alle unter Strafe gestellten Handlungsalternativen umfaßt, da das „Unterdrücken" von Daten nicht deren „Veränderung" voraussetzt. Tatsächlich besteht der Tatbestand in einer Kumulation von *Datenveränderung und Datenunterdrückung,* die nur durch die Summierung beider Aspekte angemessen zum Ausdruck gebracht werden kann. Die dualistische Struktur des Tatbestandes betrifft indessen nicht das geschützte Rechtsgut, sondern die unter Strafe gestellten Angriffsformen, denen sieh die Erörterung nun zuzuwenden hat.

(wird fortgesetzt)

(49) Frommel, JuS 1987, 667, 668; Bühler, MDR 1987, 448, 455; Jähnke, LK, StGB § 202a Rdn. 3.

(50) So mit Recht Haft, NStZ 1987, 6, 10.

Entscheidungen

Erschöpfungsproblematik beim Vertrieb von Standardprogrammen

OLG München, Urteil vom 14. Januar 1988 (29 U 2036/87)

Nichtamtliche Leitsätze

(1) Die zur Urheberrechtsfähigkeit von Anwendungsprogrammen aufgestellten Grundsätze des BGH (Inkassoprogramm, Urteil vom 9. 5. 1985 — I ZR 52/83) gelten ohne Änderungen auch für die Beurteilung der Urheberrechtsfähigkeit von Betriebssystemen.

(2) Ein Vertrag über die Überlassung von Standardprogrammen hat die Überlassung eines Vervielfältigungsstücks zum Gegenstand (und nicht die Einräumung eines Nutzungsrechts).

(3) Eine Klausel, worin der Lieferant eines Standardprogramms die Weiterveräußerung des Programms von dem Abschluß eines (unentgeltlichen) Überlassungsvertrages mit dem Dritten abhängig macht, begegnet keinen rechtlichen Bedenken.

Paragraphen

§ 17 UrhG

Stichworte

Überlassung von Standardprogrammen — rechtliche Einordnung — Übertragbarkeit des Einsatzrechts an Dritte; Urheberrechtsfähigkeit von Programmen — insb. von Systemsoftware

Tatbestand

„Die Klägerin stellt mittlere und größere Computerhardware und -software her. Die Beklagte handelt mit gebrauchten Computern. ... Sie bot mit ihrem Kundenrundbrief IV/85 in der Sparte ‚Anlagen' ... (Computer) ‚neu-Verkaufspreis auf Anfrage an'. ... In der Zeitschrift ... vom 3. 1. 1986 warb die Beklagte ferner mit einem Inserat, in dem sie Gebrauchtanlagen (der Klägerin) mit einem Nachlaß anbot.

Die Klägerin hat im wesentlichen vorgetragen, mit den Rundbriefen haben die Beklagte nicht nur (ihre) Hardware, sondern auch die Betriebssoftware der Systeme angeboten. ... Die Beklagte sei jedoch nicht berechtigt, die urheberrechtsschutzfähige Betriebssoftware zu veräußern. Die Klägerin hat beantragt, die Beklagte zur Unterlassung zu verurteilen. ..., soweit die bezeichneten Betriebssoftwaresysteme einschließlich Utilities nicht unmittelbar von der Klägerin oder ihren autorisierten Werksvertretern im Rahmen einer Lizenzvereinbarung bezogen worden sind oder die Klägerin nicht der Lizenzierung an die Beklagte zugestimmt hat.

Die Beklagte hat vorgebracht, mit klägerischer Software nicht gehandelt zu haben. Bei ihrer somit nur Hardware der Klägerin betreffenden Tätigkeit habe sie ihre Kunden darauf hingewiesen, daß diese sich die Betriebssoftware bei der Klägerin beschaffen müßten. ... Die Beklagte habe häufig Auftraggeber, die lediglich die Zentraleinheit vertreiben ließen. — Im übrigen komme der klägerischen Betriebssoftware ein Urheberrechtsschutz nicht zu."

Die Klägerin unterlag in beiden Instanzen.

Entscheidungsgründe

„1. Die Beklagte hat nicht entgegen § 17 UrhG ein Werk der Klägerin verwertet, so daß eine Verurteilung unter dem Gesichtspunkt der *Wiederholungsgefahr*