Computerspionage — Die „besondere Sicherung gegen unberechtigten Zugang" (§ 202a StGB)

Armin Leicht

A) Überblick

Seit dem Inkrafttreten des zweiten Gesetzes zur Bekämpfung der Wirtschaftskriminalität (2. WiKG) am 1. 8. 1986 ist das „Ausspähen von Daten" in § 202a StGB unter Strafe gestellt. Diese Vorschrift ist erst während der Beratungen des Rechtsausschusses des Deutschen Bundestages in den Katalog des 2. WiKG aufgenommen worden.

Hierzu gaben die Äußerungen von Sieber und Oertel (Nixdorf Computer AG) Anlaß, die in der öffentlichen Anhörung des BT-Rechtsausschusses am 6. 6. 1984[1] einen verstärkten strafrechtlichen Schutz gegen das „unbefugte Abhören und Anzapfen von Datenübertragungssystemen" bzw. gegen den „unbefugten Zugriff auf fremde Datenbanksysteme" forderten. Nach Sieber biete gerade das Anzapfen von Datenübertragungsleitungen größere Möglichkeiten durch die schnellere maschinelle Analyse als das Abhören von Telefongesprächen.

Oertel hielt den strafrechtlichen Schutz vor Computerspionage im Rahmen des UWG für unzureichend, insbesondere im Hinblick auf die erheblichen Schäden, die durch Ausspionierung angerichtet werden können[2].

Mit der Einführung des § 202a, der den Regelungsbereich des § 202 StGB ergänzt, ist der strafrechtliche Schutz vor unbefugtem Zugriff auf alle gespeicherten und im Übermittlungsstadium befindlichen Daten erheblich erweitert worden.

Einschränkungen erfährt der Tatbestand in der Legaldefinition der Daten in Absatz 2: Geschützt sind nur Daten, die nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden. Desweiteren werden diese Daten noch einmal darin eingegrenzt, daß sie nicht für den Täter bestimmt sein dürfen und gegen unberechtigten Zugang besonders gesichert sind.

Die Strafbarkeit des Ausspionierens beginnt auch erst dann, wenn sich der Täter diese Daten „verschafft". Damit bleibt das bloße Eindringen in ein Computersystem (sogen. Hacking) aus allgemeinen strafrechtlichen Erwägungen straflos[3].

B) Rechtsgut des § 202a

Geschütztes Rechtsgut des § 202a ist nicht der persönliche Lebens- oder Geheimbereich, wie seine Eingliederung in den 15. Abschnitt vermuten läßt, sondern das formelle Geheimhaltungsinteresse[4] des Verfügungsberechtigten („Herr der Daten"[5]), der durch seine Sicherung sein Interesse an der Geheimhaltung der gespeicherten oder in Übermittlung befindlichen Daten dokumentiert. Diese Daten müssen keine materiellen Geheimnisse darstellen[6]. Geschäfts- und Betriebsgeheimnisse ohne besondere Sicherung sind ohnehin bereits durch § 17 II Nr. 1 UWG geschützt.

C) Charakter der „besonderen Sicherung gegen unberechtigten Zugang"

Das einschränkende Erfordernis der besonderen Sicherung hat demnach Dokumentations- und Abgrenzungscharakter[7]:

- Wenn es sich schon nicht um materielle Geheimnisse handeln muß, so hat doch der Berechtigte („Herr oder Eigentümer der Daten"[8]) sein Geheimhaltungsinteresse an den Daten der Außenwelt durch erkennbare und geeignete Schutzmaßnahmen zu dokumentieren. Damit erhält nur der sorgsam Handelnde Strafrechtsschutz.
- Gegenüber dem Täter sollen deutliche Schranken gesetzt werden, die ihn sein rechtswidriges Verhalten bei deren Umgehung oder Überwindung erkennen lassen.

Ohne eine besondere Zugangssicherung fehlt es also an einem klar zum Ausdruck gebrachten schutzwürdigen Interesse. Das kann für den Täter auch den Rückschluß zulassen, die Daten seien für ihn bestimmt[9].

D) Maßnahmen und Bedingungen der „besonderen Zugangssicherung"

Aufgrund der existenziellen Abhängigkeit des geschützten Rechtsguts von einer Sicherungsmaßnahme, ist die Beantwortung der Frage entscheidend, welche

[1] Protokoll Nr. 26, 177, 182f
[2] s. Fn. (1)
[3] BT-Drucksache 10/5058, 28, 29; *krit.: Granderath,* DB-Beilage Nr. 18/86, 1, 2
[4] *Möhrenschlager,* Wistra 1986, 128, 140; *Lenckner/Winkelbauer,* CuR 1986, 483, 485
[5] *Lenckner/Winkelbauer,* CuR 1986, 483, 485
[6] BT-Drucksache 10/5058, 29
[7] vgl.: *Lenckner/Winkelbauer,* CuR 1986, 483, 486
[8] vgl. Fn. (5)
[9] Zur Abhängigkeit des Merkmals „besondere Sicherung gegen unberechtigten Zugang" von dem des „Bestimmt-Seins" vgl.: *Lenckner/Winkelbauer,* CuR 1986, 483, 487

Sicherungsmaßnahmen unter welchen Bedingungen das Merkmal der „besonderen Sicherung gegen unberechtigten Zugang" erfüllen. Dies hängt wiederum von den Anforderungen ab, die man an eine solche Sicherung stellt.

I. Auslegung des Tatbestandsmerkmals

Zuvor müssen die Grenzen der Auslegung dieses Tatbestandsmerkmals grob bestimmt werden:

1. Zugang

Ausgehend vom Wortlaut ist unklar, was unter „Zugang" zu den Daten zu verstehen ist. Fraglich ist hierbei, ob damit lediglich die unmittelbare Zugriffsmöglichkeit auf Daten beschrieben wird, oder bereits der physische Zugang zum Rechner (System), oder schon der zu den „Sicherheitsbereichen". Bei extensivster Auslegung des Begriffs könnte bei kleineren Betrieben und Büroräumen von Freiberuflern bereits der Zugang am Eingang zum Betrieb/Büro davon umfaßt sein.

Die Auffassung des Gesetzgebers hierzu kann nicht eindeutig ermittelt werden[10]. Ein Indiz für sein Begriffsverständnis könnte jedoch die Anlage zu § 6 I S. 1 BDSG darstellen, worin Unbefugten bereits der „Zugang zu Datenverarbeitungsanlagen" verwehrt werden soll, um personenbezogene Daten zu schützen.

Nach der Auffassung in der Literatur ist „Zugang" im Interesse größtmöglicher Sicherheit weit auszulegen[11].

Wegen der sehr unterschiedlichen Erfordernisse, finanziellen und technischen Möglichkeiten und örtlichen Gegebenheiten bei Unternehmen, kleinen Betrieben, Freiberuflern und Privaten, ist zunächst der Literaturansicht zu folgen, damit die Möglichkeiten zur Datensicherung nicht schon durch dieses Tatbestandsmerkmal auf eine bestimmte Gruppe beschränkt werden. Einschränkungen werden sich sowieso noch durch den Schutzzweck der Sicherung ergeben.

Zunächst umfaßt damit der „Zugang" zu Daten jede technische und physische Einwirkungsmöglichkeit auf Datenspeicher und den physischen Zugang zum System und Sicherheitsbereich.

2. Der „unberechtigte Zugang"

Das Merkmal des unberechtigten Zugangs ist eng verknüpft mit der Entscheidung des Verfügungsberechtigten, ob die Daten für den Täter bestimmt sind oder nicht[12]. Denn es ist widersprüchlich anzunehmen, der Täter habe berechtigten Zugang zu den Daten, wenn diese nicht für ihn bestimmt sind.

3. Die „besondere Sicherung"

Die bloße Versagung der Zugangsberechtigung reicht für den Rechtsgüterschutz des § 202a allein nicht aus. Durch eine faktische Sicherungsmaßnahme muß der unberechtigte Zugang zusätzlich verhindert oder zumindest erheblich erschwert werden.

a) Ansicht des Gesetzgebers

Nach den Äußerungen des Gesetzgebers soll auf die Regelung des § 202 Abs. 2 und § 243 Abs 1 Nr. 2 StGB zurückgegriffen werden[13]. Die dort aufgeführten körperlichen Gegenstände können Sicherungen von Datenträgern darstellen, sie versagen aber bei chipgespeicherten (ROM, RAM usw.) und per Funk oder Kabel übermittelten Daten. Überdies existieren software- und hardwaremäßige Sicherungsmaßnahmen, die für die §§ 202 Abs. 2, 243 Abs. 1 Nr. 2 StGB untypisch sind, aber gerade im datenverarbeitenden Bereich bessere Schutzmöglichkeiten vor unbefugtem Zugriff bieten und oftmals nur einzig anwendbar sind.

b) Anforderungen an die Sicherheitsmaßnahme

Die von dem Verfügungsberechtigten getroffene Maßnahme zum Schutz seiner Informationen ist für die Tatbestandsmäßigkeit des § 202a vorerst an zwei Kriterien zu messen: an ihrem Sicherungsgrad und dem jeweiligen Schutzzweck.

aa) Sicherungsgrad

Nach bisheriger Literaturansicht seien keine besonders hohen Anforderungen an das Merkmal der „besonderen Sicherung" zu stellen, da jede Maßnahme als Sicherung ausreiche, die dem Schutz vor unberechtigtem Zugang diene[14], bzw. durch die der Verfügungsberechtigte sein Geheimhaltungsinteresse zu erkennen gibt[15]. Desweiteren genüge einerseits, daß die Durchbrechung des Schutzes nicht ohne weiteres möglich sein darf, andererseits sei vollständiger Schutz nicht erforderlich[16].

Hieraus folgt, daß dann z. B. nicht die Anforderungen des § 6 Abs. 1 S.1 BDSG erfüllt sein brauchen. Pawlikowsky versteht hierbei unter Datensicherung die Menge aller Maßnahmen, Einrichtungen und Methoden, mit denen der Datenschutz verwirklicht und der erforderliche Grad an Datensicherheit erzielt werden kann[17]. Diese erhöhten Anforderungen an die Datensi-

[10] vgl.: Fn. (6)

[11] *Lenckner/Winkelbauer,* CuR 1986, 483, 487; *Weck Gerhard,* Datensicherheit: Methoden, Maßnahmen und Auswirkungen (1984), S. 33f; *Dworatschek/Büllesbach/Koch u.a.,* Personalcomputer und Datenschutz (1985), S. 40; *Hoppe Michael,* Straf- und zivilrechtliche Würdigung von Mißbrauchsfällen im EDV-Bereich nichtöffentlicher Unternehmungen, technisch-organisatorische Datensicherungsmöglichkeiten und Entscheidungshilfen zur Auswahl von Sicherungsmaßnahmen, Dissertation Hamburg 1978, S. 83

[12] *Lenckner/Winkelbauer,* CuR 1986, 483, 487

[13] vgl.: Fn. (6)

[14] vgl. Fn. (12)

[15] *Möhrenschlager,* Wistra 1986, 128, 140; *Granderath,* DB-Beilage Nr. 18/86, 1, 2

[16] vgl.: Fn. (12)

[17] *Pawlikowsky,* DuD 1985, 105, 106

cherheit i. S. des BDSG werden in § 202a nicht gefordert.

Jedoch kann der bloße „Dokumentationscharakter" einer Sicherung auch nicht genügen. Dies ergibt sich aus dem Verweis des Gesetzgebers auf die §§ 202 Abs. 2 und 243 Abs. 1 Nr. 2 StGB.

Maßstab für den Sicherungsgrad der zu diesen Vorschriften anerkannten Schutzvorrichtungen[18] ist die erhöhte kriminelle Energie des Täters, die er zu deren Überwindung einsetzen muß. Ein Briefumschlag, der schließlich auch ein gewisses Geheimhaltungsinteresse dokumentiert, reicht nicht aus[19].

Nun ist im Hinblick auf die Komplexität der Datenverarbeitung durch Computer und der Vielzahl technischer Möglichkeiten zu ihrer Manipulation die Überwindung (Durchbrechung) der Sicherungsmaßnahme vom Gesetzgeber nicht in den Tatbestand aufgenommen worden. Dennoch hat sich der Sicherungsgrad der Maßnahme an der vom Täter einzusetzenden erhöhten kriminellen Energie auszurichten. Damit darf es also dem Täter nicht ermöglicht werden, die Sicherung ohne weiteres durchbrechen zu können[20].

bb) Schutzzweck der Sicherung

Zum Schutz von Daten sind die vielfältigsten Sicherungsmaßnahmen entwickelt worden[21]. Wenn nun jede Maßnahme ausreichend ist, die dem Schutz vor unberechtigtem Zugang dient[22] bzw. das formale Geheimhaltungsinteresse erkennen läßt, so ist fraglich, wie weit der geschützte Bereich ausgedehnt werden kann (womöglich sogar bis zum Pförtner am Eingangstor eines großen Unternehmens). Da es hierbei zu Kollisionen mit Schutzbereichen anderer Normen kommen kann, ist auf den primären Schutzzweck der jeweiligen Sicherung abzustellen.

II. Prüfung der Sicherungsmaßnahmen auf ihre Tatbestandsmäßigkeit

Im folgenden soll anhand der zur Zeit bekannten und angewandten Sicherungsarten festgestellt werden, welche Sicherungsmaßnahmen tatbestandsmäßig im Sinne des § 202a sind. Aufgrund dieser Prüfungen ergeben sich möglicherweise neue Abgrenzungskriterien und Erkenntnisse, die eine exaktere Bestimmung der Auslegungsgrenzen des Merkmals der Zugangssicherung fördern können.

Grundsätzlich ist dabei von faktischen Hindernissen auszugehen, also von Schutzvorrichtungen physischer und technischer Art. Die bloß abstrakte Vergabe von Berechtigungen bzw. der Ausspruch von Verboten oder rein personellen Maßnahmen, wie Tätigkeitsverteilung, Hierarchie-Bildung, Job-Rotation, Vier-Augen-Prinzip etc., genügt nicht. Dies leitet sich aus dem Verweis des Gesetzgebers auf die §§ 202 Abs. 2 und 243 Abs. 1 Nr. 2 StGB ab[23].

Weiterhin soll als These gelten, daß eine Schutzmaßnahme umso eher als Sicherung anzusehen ist, je unmittelbarer sie an den fraglichen Daten angebracht ist.

Die Maßnahmen, die möglicherweise dem Schutz der Daten vor unberechtigtem Zugang dienen, können in folgende Gruppen eingeteilt werden:
- baulich-techische Maßnahmen
- betriebsorganisatorische und physische Maßnahmen
- hardware- und softwaremäßige Sicherungen
- Sicherung von Übertragungsverbindungen.

1. Baulich-technische Maßnahmen

Zwar dienen baulich-technische Maßnahmen letztendlich auch der Verhinderung des Ausspionierens von Daten, ihr hauptsächlicher Schutzzweck ist jedoch ein anderer:

a) So dient die Aufteilung eines Rechenzentrums in verschiedene Räumlichkeiten der Erhaltung der Datenträger im Katastrophenfall und der Verhinderung von Sabotage- und Manipulationshandlungen[24]. Es dient somit nicht überwiegend als Hindernis für einen Spionagetäter.

b) Andere Schutzmaßnahmen wie Schranken, abschließbare Gitter am Gebäudeeingang und an Fenstern, Rolläden, Panzerglas, Sicherheitsschlösser, Fernsehüberwachung, Licht-, Ultraschall-, Schwingungs-, Bewegungs- oder Belastungskontakte, Mikrowellen- und Kapazitive Systeme in Verbindung mit Alarmanlagen können schon eher einen Täter vom unberechtigten Zugang abhalten, wobei auch die Dokumentation eines formalen Geheimhaltungsinteresses an den dahinter verborgenen Daten nicht ganz abgeleugnet werden kann.

Sie sind jedoch in erster Linie als Gebäudeschutzmaßnahmen konzipiert bzw. sollen das Eindringen des Täters in das Gebäudeinnere verhindern. Ihr Schutzzweck ist somit aus den §§ 243 Abs. 1 Nr. 1 und 123 StGB abzuleiten.

c) Bildschirmterminals geben elektro-magnetische Strahlung ab, wobei das Videosignal aufgefangen und der aktuelle Bildschirminhalt aus einiger Entfernung noch regeneriert werden kann[25]. Räumlich angeordnete elektro-magnetische Abschirmungen können dies zwar verhindern, als tatbestandliche Sicherungen können sie aber nicht anerkannt werden. Zum einen soll der Austritt der Streustrahlung verhindert werden, um Störungen zu vermeiden, zum anderen fehlt es an der Dokumentation des formalen Geheimhaltungsinteres-

[18] *stellvertr. für viele: Lenckner, Eser,* in: Schönke/Schroeder, Kommentar zum Strafgesetzbuch, 21. Aufl. (1982), § 202 Rdn. 18, § 243 Rdn. 22f

[19] *Samson,* in: Rudolphi/Horn/Samson/Schreiber, Systematischer Kommentar zum StGB, 7. Lieferg. der 3. Aufl. (1985), § 243 Rdn. 19

[20] vgl.: Fn. (12)

[21] *Weck* (s. Fn. 11), S. 77ff, insbes. S. 197ff; *Hoppe* (s. Fn. 11), S. 78ff; *Hellfors/Seiz,* Praxis betrieblicher Datensicherung (1977), S. 81ff; *Arbeitskreis DuD,* DuD 1986, 238, 241; speziell für PC: *Dworatschek/Büllesbach/Koch u.a.* (s. Fn. 11), S. 39ff; für Btx: *Gorn,* DuD 1985, 333ff

[22] wobei „Zugang" möglichst weit auszulegen ist: s. oben D I 1

[23] vgl.: Fn. (6)

[24] *Hoppe* (s. Fn. 11), S. 188

ses, da es sich dabei um gebäudespezifische zumeist versteckt installierte Schutzvorrichungen handelt, die gegenüber dem Täter keinen Dokumentationscharakter entfalten.

d) Da Katastrophenschutzmaßnahmen (gegen Feuer, Wasser, Erdbeben, Krieg) überwiegend diesen Zwekken dienen, stellen sie ebenfalls keine tatbestandlichen Zugangssicherungen dar, obwohl sie zuweilen einen entsprechenden Nebeneffekt haben.

2. Betriebsorganisatorische und physische Maßnahmen

a) Closed-Shop-Betrieb

Hier ist vor allem die sogenannte closed-shop-Sicherung zu nennen, d. h. die Einteilung in Sicherheitszonen. Dabei handelt es sich um räumlich abgetrennte Bereiche, zu denen nur die Mitarbeiter Zutritt haben, die „zutrittsberechtigt" sind. Je nach Größe eines Rechenzentrums werden Sicherheitsbereiche nach Funktion gebildet: z. B. Maschinensaal, Arbeitsvorbereitung, Datenerfassung, Archiv usw. Andererseits können auch mehrere gleichartige Schutzbereiche beim online-Betrieb entstehen. Hierbei steht der Zentralrechner im eigenen Schutzbereich, wobei die einzelnen Terminals außerhalb in den verschiedenen Abteilungen des Betriebs geschützt untergebracht sind.

aa) Kennzeichen

Kennzeichnend für den closed-shop-Betrieb ist die Vergabe von Zutrittsberechtigungen, die durch kombinierte Kontroll- und Sicherheitseinrichtungen überprüft werden. Die Zutrittsbeschränkung wird durchgesetzt anhand von:

— Schlüsseln
— maschinenlesbaren Ausweiskarten
— Systemen, die die Eingabe von Kennziffern bzw. Paßwörtern verlangen
— Analysesystemen zur Identifizierung von Unterschriften, der Handgeometrie, des Fingerabdrucks, der Sprache oder der Augen

in Verbindung mit einem dadurch ausgelösten Türöffner[26].

bb) Zweck der closed-shop-Sicherung

Diese Systeme besitzen zwar den notwendigen Sicherungsgrad zur Dokumentation des „formalen Geheimhaltungsinteresses", das Problem des Schutzzwecks wird aber dann virulent, wenn es sich bei dem so geschützten Bereich nicht um ein Rechenzentrum größeren Ausmaßes handelt, sondern um Büroräume kleinerer Betriebe, von Freiberuflern oder um die Wohnräume Privater. Hier müßte konsequenterweise das Sicherheitsschloß am Büro-/Wohnungseingang ebenso als tatbestandliche Sicherung anerkannt werden.

Damit steht der Schutzzweck der closed-shop-Sicherung in Frage, weil es hierbei offenbar zur Kollision mit § 123 StGB kommt.

Da aber zunächst von einer möglichst weiten Auslegung des Zugangsbegriffs ausgegangen wurde[27], könnte dennoch am closed-shop-Eingang eine Sicherung gegen unberechtigten „Zugang zu Daten" vorliegen[28]. Dem muß jedoch der Verweis des Gesetzgebers auf die Erkenntnisse zu § 202 Abs. 2 und § 243 Abs. 1 Nr. 2 StGB entgegengehalten werden[29]. In beiden Vorschriften werden Gegenstände geschützt, die in einem Behältnis aufbewahrt werden. Nach gesicherter und einhelliger Rechtsauffassung ist eln Behältnis „ein zur Aufnahme von Sachen dienendes und sie umschließendes Raumgebilde, das nicht dazu bestimmt ist, von Menschen betreten zu werden"[30].

Bei der closed-shop-Sicherung handelt es sich aber um eine Zutrittssicherung einer Räumlichkeit, die gerade zum Betreten von Menschen bestimmt ist. Aus der ergänzenden Funktion des § 202a im 15. Abschnitt des StGB, wonach der Schutzbereich des § 202 StGB in Bezug auf Daten erweitert werden soll, und aus dem expliziten Verweis des Gesetzgebers anf § 202 Abs. 2 bzw. § 243 I Nr. 2 StGB folgt demnach, daß Raumsicherungen gerade nicht von § 202a umfaßt werden sollen.

Damit kann der closed-shop-Betrieb als Sicherung gegen unberechtigten Zugang **nicht** anerkannt werden.

b) Physische Sicherungen des Systems/Datenträgers

Bei folgenden Maßnahmen handelt es sich um solche, die typischerweise nach dem Willen des Gesetzgebers erfaßt werden sollen[31]:

- bezüglich des Terminals/Datenstation:
  — Einschließen des Gerätes in ein Behältnis
  — Schließvorrichtung am Gerät, die physischen Zugang verhindert und/oder Stromzufuhr oder Eingabetastatur sperrt:
  — verschließbare Haube
  — Verwendung von Schlüsseln, Ausweislesern, Benutzercode, etc. in Verbindung mit einer elektronischen oder mechanischen Sperre am Terminal
- hinsichtlich der Datenträger:
  — versperrbare Archivschränke, Tresore etc.
  — verschließbare Transportbehälter

[25] *Weck* (s. Fn. 11), S. 96; *Möhrenschlager,* Wistra 1986, 128, 136

[26] vgl.: *Weck* (s. Fn. 11), S. 88 ff; *Hoppe* (s. Fn. 11), S. 83 f; *Pawlikowsky,* DuD 1985, 105, 111

[27] s. oben: D I 1

[28] so: *Lenckner/Winkelbauer,* CuR 1986, 483, 487; wohl auch: *Dreher/Tröndle,* Kommentar zum Strafgesetzbuch, 43. Aufl. (1986), § 202a Rdn. 7

[29] vgl.: Fn. (6)

[30] GrSen BGH 1, 163, 167; *Lenckner, Eser,* in: Schönke/Schroeder (s. Fn. 18), § 202 Rdn. 18, § 243 Rdn. 22; *Dreher/Tröndle,* (s. Fn. 28), § 202 Rdn. 6, § 243 Rdn. 22; *Samson,* in: Rudolphi/Horn/Samson/Schreiber (s. Fn. 19), § 243 Rdn. 19

[31] Detailinformationen zu den Maßnahmen in: *Weck* (s. Fn. 11), S. 165 f; *Hoppe* (s. Fn. 11), S. 86 ff; *Dworatschek/Büllesbach/Koch u.a.* (s. Fn. 11), S. 40, 45; *Arbeitskreis DuD,* DuD 1986, 239, 241; *Pawlikowsky,* DuD 1985, 105, 111 f

Soweit die Schlüssel, Ausweiskarten, Listen von Benutzercodes etc. wiederum auf eben beschriebene Weise geschützt sind, handelt es sich dabei um mittelbare Sicherungen, die ebenfalls anerkannt sind[32].

Nach einer Auffassung[33] soll auch der closed-shop-Betrieb eines Datenverarbeitungszentrums eine mittelbare Sicherung darstellen. Auch hier sind die zur unmittelbaren Sicherung genannten Gründe entgegenzuhalten.

3. Hardware- und softwaremäßige Sicherungen

War die Frage nach dem erforderlichen Sicherungsgrad bei den zuvor beschriebenen Schutzmaßnahmen noch einfach zu beantworten, so stellt sich hier dieses Problem ganz anders, da es um die Sicherung unkörperlicher Informationen geht, die ebenso nicht sichtbar ausgeführt wird. Diese Art von Sicherungen werden zumeist als *logische* Sperren bezeichnet.

a) Besondere Probleme:

aa) Sicherungsgrad

Zweifelhaft ist die Bestimmung des erforderlichen Sicherungsgrades, weil es dem Täter schließlich nicht ganz einfach gemacht werden darf, in ein System einzudringen, sonst wäre das tatbestandliche Erfordernis einer Sicherung überflüssig. Also fragt sich, welcher Maßstab angelegt wird: stellt man auf den Intellekt und das Wissen des Täters ab, oder z. B. auf die technischen Möglichkeiten des System o. ä.

Als Mindestanforderung könnte z. B. das Verwenden einer nicht weit verbreiteten Programmiersprache oder das Einführen individueller Befehle in eine kommerzielle Programmiersprache (z. B. Forth, Pascal) gegenüber einem ungeübten EDV-Amateur durchaus bereits eine Schranke darstellen.

Andererseits braucht der Schutz nicht vollständig zu sein, da der Tatbestand des § 202a eine Überwindung der Sicherung nicht voraussetzt.

Erfahrungsgemäß ist von EDV-Insidern auszugehen[34], so daß die Sicherung so gestaltet sein muß, daß sie auch diesem Täterkreis gegenüber zunächst ein Hindernis bereitet. Der Täter muß gezwungen werden, von der vom Verfügungsberechtigten vorgesehenen und gesicherten „Zugangsart" abzuweichen.

bb) Erkennbarkeit

Weiterhin wird bei dieser Art von Sicherungen das Problem der Erkennbarkeit deutlich, denn das formale Geheimhaltungsinteresse an den Daten muß dem Täter gegenüber dokumentiert werden. Ist eine Sicherung nur versteckt wirksam, d. h. entfaltet sie objektiv keinen Dokumentationscharakter, oder reicht das Wissen eines Amateur-Täters für ihre Erkennbarkeit nicht aus, so ist das formale Geheimhaltungsinteresse nicht *dokumentiert.* Die Sicherung muß also gegenüber jedem Täter das formale Geheimhaltungsinteresse anzeigen.

b) Hardwaremäßige Sicherungen[35]

Diese Sicherungen sollen vor allem den Zugriff auf Haupt-, CPU- und Peripheriespeicher verhindern.

- Bei Multi-Programmierung (gleichzeitige Verarbeitung mehrerer Programme) wird durch Grenz-Register sichergestellt, daß keines der gleichzeitig im Hauptspeicher liegenden Programme auf Daten eines anderen zugreifen kann. Damit wird das Lesen von „fremden" Programmdaten aus dem Hauptspeicher verhindert[36].
- Speicher-Schutz-Schlüssel verhindern unberechtigten Zugriff auf einzelne Speicherbereiche, indem überprüft wird, ob die interne Identifikation eines Programms mit dem Schlüssel eines Speicherbereichs übereinstimmt[37].
- Eine wirkungsvollere Methode besteht in der Segmentierung und/oder im Paging bei virtueller Speicherverwaltung. Hierbei ist der Täter auf indirekte (virtuelle) Adressen angewiesen, denn eine virtuell ausgelegte Hardware verhindert die direkte (reale) Adressierung des Hauptspeichers[38]. Ein darauf aufbauender weitergehender Schutz besteht in der typ-gebundenen Hauptspeicherverwaltung[39].
- Nach einem anderen Verfahren werden die Bitmuster von Programm und Datenstrukturen des Hauptspeichers miteinander nach bestimmten Kriterien verglichen und dementsprechend der Zugriff erlaubt oder versagt[40].

Da diese hardwaremäßigen Sicherungen nicht immer klar erkennbar sind, muß auf den konkreten Einzelfall abgestellt werden. Häufig werden sie jedoch nur zusammen mit anderen deutlicheren Sicherungen eingesetzt, so daß sich hier nur selten Probleme ergeben.

c) Softwaremäßige Sicherungen

Bekannter und verbreiteter sind vor allem bei Verwendung von Mini- und Microcomputern softwaremäßige Sicherungen, da sie flexibler sind und individuell vom Verfügungsberechtigten erstellt werden können.

aa) Prüfung der Voraussetzungen

Wenn nicht gerade in dem abrufbaren ungesicherten Programmlisting dem Täter z. B. das Paßwort frei Haus geliefert wird, kann in der Regel vom erforderlichen Sicherheitsgrad ausgegangen werden. In der überwiegenden Zahl der Fälle sollen diese Sicherungen gerade den Zugang zu den geschützten Daten verwehren, so

[32] vgl.: *Eser,* in: Schönke/Schroeder (s. Fn. 18), § 243 Rdn. 23
[33] *Lenckner/Winkelbauer,* CuR 1986, 483, 487
[34] *Sieber,* Computerkriminalität und Strafrecht, 2. Aufl. (1980), S. 99ff, 119ff; *Rupp,* Computersoftware und Strafrecht, Dissertation Tübingen 1985, S. 32f
[35] Detailinformationen hierzu in: *Weck* (s. Fn. 11), S. 103ff; *Hoppe* (s. Fn. 11), S. 138; *Fischer,* DuD 1985, S. 112ff
[36] *Weck* (s. Fn. 11), S. 106
[37] *Weck* (s. Fn. 11), S. 108
[38] *Fischer,* DuD 1985, 112, 113f; *Weck* (s. Fn. 11), S. 110; *Hoppe* (s. Fn. 11), S. 140
[39] *Weck* (s. Fn. 11), S. 117

daß auch der Schutzzweck gegeben ist. Wird der Abruf der Daten versucht, so erkennt der Täter auch schnell, daß der Verfügungsberechtigte seine Daten schützen will.

Unabhängig vom konkreten Einzelfall erfüllen somit softwaremäßige Sicherungen prinzipiell die Voraussetzungen des § 202a an eine Zugangssicherung.

bb) Sicherungsmethoden

Der Zugang zu Programm und Dateien wird auch hier von Zugangsberechtigungen abhängig gemacht. Diese legen fest, wer auf welche Daten mit welcher Befugnis (Suchen, Lesen, Schreiben bzw. Speichern, Löschen, Ändern, Kopieren) zugreifen darf.

Diese Zugriffsrechte können durch verschiedene Sicherungsmaßnahmen gegenüber dem Benutzer durchgesetzt werden, d. h. im Falle des unberechtigten Zugriffs wird dem Täter ein Hindernis bereitet, das ihm bei seinem Vorgehen eine Schranke setzt: z. B. durch einen Hinweis auf sein unberechtigtes Vorgehen mit gleichzeitiger Sperre des weiteren Zugriffs oder durch Abbruch des Programms.

Beispiele:

1. Bei dem programmierten Frage/Antwort-Verfahren kann nur der rechtmäßige Benutzer die richtigen Antworten geben und damit dem ihm zugewiesenen Pfad folgen.

2. Wird die Eingabe von Benutzerkennummern verlangt, so werden diese mit intern gespeicherten Zugriffsmatrizen oder Zugriffslisten verglichen[41].

3. Die gebräuchlichste und bekannteste Sicherung gegen unberechtigten Zugriff ist die Verwendung von Paßwörtern. Benutzer, die das für den Zugriff vergebene Paßwort nicht kennen, werden abgewiesen. Damit ist auch eine gezielte Vergabe für bestimmte Zugriffsarten (Schreiben, Lesen, Ausführen etc.) möglich.

Ein solches Paßwort kann auch in ein Benutzerprogramm codiert werden, das dann selbständig den Datei-Zugriff ermöglicht, ohne daß der Benutzer von der Existenz des Paßwortes weiß[42]. Überschreitet hierbei der Nutzer die so implementierten Rechte, muß ihm das angezeigt werden.

4. Zuweilen wird das Aufrufen von Programmen und Dateien von einem systemintegrierten Baustein abhängig gemacht, in den eine individuelle Benutzerkennung programmiert ist. Damit wird gewährleistet, daß der Aufruf des Programms oder der Datei nur mit dem dazugehörigen System möglich ist. Dies reicht für eine tatbestandliche Sicherung aus.

5. Eine Möglichkeit der Zugriffssicherung kann auch darin bestehen, daß dem Verwender zwar die Nutzungsmöglichkeit des Programms gestattet wird, aber dennoch die Programmdaten (z. B. Listing des Programms) vor seinem Zugriff gesichert sind. Dies ist z. B. in dem Fall eines berechtigten Nutzers (Angestellter o. ä.) denkbar, der mit dem Programm arbeiten darf, aber die Programmdaten nicht erfahren soll. Hierbei wird also die Sicherung lediglich um eine Stufe zurückgesetzt, d. h. es wird nicht bereits der Aufruf und das Abarbeiten verhindert, sondern lediglich die Kenntnisnahme der Programmdaten. Rückschließend ergibt sich daraus, daß diese Daten für den Nutzer nicht bestimmt sind. Ein „Verschaffen" bleibt damit auch noch möglich[43].

Dasselbe muß für den rechtmäßigen Erwerber gelten, der dem bloßen Nutzer gleichzustellen ist. Nach anderer Auffassung wird dies abgelehnt[44], da ein „Verschaffen" nicht mehr möglich sei. Dies müßte dann konsequenterweise auch für den eben beschriebenen berechtigten Nutzer gelten. Denn auch in seiner Situation wäre damit ein „Verschaffen" nicht mehr möglich.

Gegen diese Auffassung spricht zum einen, daß die Qualität einer Zugangssicherung nicht vom „Verschaffen" abhängig gemacht werden kann, und zum anderen besteht das „Sich-Verschaffen" auch in der Kenntnisnahme, die in diesen Fällen gerade verhindert werden soll — gleichgültig, ob es sich dabei um ein Nutzungs- oder Eigentumsverhältnis handelt.

6. Anders verhält es sich jedoch, wenn der Programmnutzer via Bildschirm oder Drucker die Daten ungehindert aufrufen kann, aber eine Kopiersicherung nur die Übertragung auf einen anderen Datenträger verhindert. Sinn hat eine derartige Maßnahme nur bei sehr umfangreichen Programmen. In dieser Konstellation ist der Schutzzweck der Kopiersicherung nicht darauf gerichtet, den Zugang zu den Daten zu verhindern, denn der ist jederzeit möglich, sondern darauf, eine vom Programmverfasser nicht erlaubte Vervielfältigung durch den Nutzer zu erschweren.

Damit handelt es sich um keine Zugangssicherung im Sinne des § 202a[45].

7. Speziell bei Microcomputern kann die Überprüfung der Benutzerlegitimation und die evtl. Verhinderung des unberechtigten Zugangs durch folgende Maßnahmen erfolgen[46]:

- Schnelladeroutine mit Originalbetriebssystem: beim Laden eines Programms wird die Abweichung von der Soll-Ladezeit gemessen und bei Über- oder Unterschreitung der Toleranzen der Zugriff auf die Daten verhindert
- In Verbindung mit dieser Maßnahme kann auch ein Spezialladealgorithmus für einzelne Bytes programmiert werden
- Bilden von Prüfsummen durch Anfangs- und Endadresse
- ID-Abfrage
- Directory-Manipulation in Verbindung mit softwaremäßigem Schreibschutz
- Floppy-RAM-Abfrage im Interrupt

[40] *Weck* (s. Fn. 11), S. 118
[41] *Weck* (s. Fn. 11), S. 205 ff
[42] vgl.: *Weck* (s. Fn. 11), S. 202
[43] so auch: *Lenckner/Winkelbauer,* CuR 1986, 483, 486; a. A.: *Dreher/Tröndle* (s. Fn. 28), § 202a Rdn. 7
[44] *Dreher/Tröndle* (s. Fn. 28), § 202a Rdn. 7
[45] so auch: *Lenckner/Winkelbauer,* CuR 1986, 483, 486
[46] Diese Aufstellung kann nur eine Auswahl sein!

— Lesen von Bytes auf Track/Sector
— Überprüfung von Schreib-/Lesefehlern auf dem Datenträger
— RESET-Schutz durch Routinen im Cass.-Puffer
— Erkennen von ungewünschten Hardwarezusätzen im Cartridgeport

4. Daten(fern)übertragung (DFÜ)

Problematisch gestaltet sich die Annahme einer Zugangssicherung bei der Datenübertragung per Kabel oder Funk. Gerade dieser Bereich der EDV ist jedoch wegen seiner leichten Zugänglichkeit in öffentlichen Netzen besonders gefährdet.

DFÜ erfolgt durch zwei Übertragungsmodi, wobei die Signale (Daten) mit vertretbarem Aufwand mitgehört werden können:

1. Kabel:

— unterirdisch verlegte Kupferkabel oder Lichtwellenleiter (Glasfaserkabel)
— Überlandleitungen

Signale, die über metallische Kabel transportiert werden, können leicht mittels einer direkten Kabelanbindung oder indirekt über induktive Abkoppelung des Signals abgezapft werden. Das „Abhören" eines Glasfaserkabels gestaltet sich hingegen schwieriger. Dazu muß immer ein Eingriff in das Kabel vorgenommen werden, womit die weitere Datenübertragung erheblich gefährdet wird und dem Täter keinen Nutzen bringt.

2. Funkübertragung:

— Funk
— Richtfunkstrecke
— Nachrichtensatelliten als Relaisstation

Das Mithören der so übermittelten Informationen ist durch geeignete Antennenanlagen möglich.

a) Schutzmaßnahmen

aa) Übertragung mittels Kabel

Jegliche Art der Kabelübertragung (hierzu rechnen auch die Zuleitungen zu den Sende- und Empfangsstationen der DFÜ-Strecken) kann durch physische Maßnahmen gegen Anzapfen/Abhören gesichert werden:

Z. B. durch widerstandsfähige Kabelummantelung, Bleiabschirmung, Hilfsmittel zur Sicherung von Anschlußdosen und Leitungsenden oder durch Abschalten der DFÜ bei zu großen Toleranzen während der automatischen Messung von Leitungsdämpfungen. Letztgenannte Maßnahme kann jedoch nicht als Zugangssicherung anerkannt werden, da sie erst nach erfolgtem Zugang den Zugriff auf weitere Daten verhindert.

Voraussetzung für eine tatbestandliche Sicherung ist ihr primärer Zweck als Zugangssicherung. Dieser ist z. B. bei unterirdischer Verlegung nicht gegeben, da der Hauptzweck in der — für die Umwelt — störungsfreien Leitungsführung liegt[47].

bb) Funkübertragung

Bereits erörterte Schutzmaßnahmen bleiben bei der Funkübertragung weitgehend wirkungslos. Hier wird üblicherweise auf kryptotechnische Verschlüsselungsverfahren zurückgegriffen, die auch bei der Kabelübertragung mehr Sicherheit bieten[48].

1. Verschlüsselungsverfahren

Durch diese Verfahren werden die Ursprungsdaten (Klartext) mittels mathematischer Transformation in andere Daten umgewandelt, d. h. in Daten mit anderem Informationsgehalt (Schlüsseltext)[49].

So kann der Täter zwar den Schlüsseltext empfangen, der Informationsgehalt ist für ihn jedoch nutzlos, da er ohne Kenntnis der Verschlüsselungstechnik die Originaldaten nur mit sehr hohem Aufwand oder überhaupt nicht rekonstruieren kann[50].

Beispiele für Verschlüsselungsmethoden:
— mono- oder polyalphabetische Substitution
— Transposition
— Autokey-Systeme
— Blocksysteme
— Lauftextverschlüsselung etc.[51]

Durch Substitution wird jedes Zeichen eines Klartextes durch ein ihm fest zugeordnetes anderes Zeichen ersetzt.

Bei der Transposition werden die einzelnen Zeichen einer Nachricht durch einen mathematischen Schlüssel untereinander vertauscht; sie ändern also ihre Position innerhalb des Textes.

Substitution und Transposition können auch zusammen angewendet werden.

2. Problem der „Zugangssicherung"

Bei der kryptotechnischen Verschlüsselung versagt die bisherige Auslegung des Merkmals „Zugang"[52], denn zu den verschlüsselten Daten besteht freier „Zugang". Es wird nur der Bedeutungsgehalt der Daten vor Kenntnisnahme geschützt, das aber in § 202a gerade nicht verlangt wird.

Für eine Ablehnung der Verschlüsselungsverfahren als „Zugangssicherung" spricht auch, daß hierbei ein anderer Zeichensatz mit einem — augenscheinlich — vom Klartext völlig verschiedenen Informationsgehalt übermittelt wird. Ihre wahre Bedeutung erhalten die Zeichen des Schlüsseltextes erst durch die abgesprochene Interpretation des Absenders und Empfängers

[47] vgl: Fn. (12)
[48] s. hierzu: *Hellfors/Seiz* (s. Fn. 21), S. 115f; *Weck* (s. Fn. 11), S. 283ff; *Gorn*, DuD 1985, 333, 336; *Heider/Kraus/Welschenbach*, Mathematische Methoden der Kryptoanalyse (1985), S. 1-30
[49] *Weck* (s. Fn. 11), S. 283
[50] zu Entschlüsselungsmethoden: *Heider/Kraus/Welschenbach* (s. Fn. 48)
[51] weiteres bei: *Heider/Kraus/Welschenbach* (s. Fn. 48), S. 1-30; *Weck* (s. Fn. 11), S. 288f
[52] vgl. oben: D I 1

durch Anwendung ihres individuellen Schlüssels. Da somit die Sicherung vor Kenntnisnahme auf intellektueller Ebene im Bereich des Senders und Empfängers erfolgt, grundsätzlich aber faktische Hindernisse gegenüber dem Täter erforderlich sind, könnten Verschlüsselungsverfahren als „Zugangssicherungen" nicht anerkannt werden.

Eine Ausdehnung der tatbestandlichen Zugangssicherung auf kryptotechnische Verfahren erscheint dennoch aus folgenden Gründen unnmgänglich:

Zum einen hat der Gesetzgeber gerade die Übermittlung von Daten in den Schutzbereich des § 202a aufgenommen. Eine Ablehnung würde die Regelung überflüssig machen[53].

Zum anderen besteht bei einigen Übertragungsarten nur die Möglichkeit der Verschlüsselungsverfahren, die eine Kenntnisnahme von den Originaldaten verhindern[54]. Da in § 202a gerade nicht Kenntnisnahme vorausgesetzt wird, ist zweifelhaft, ob eine Zugangssicherung auch eine Sicherung vor Kenntnisnahme einschließt.

Der Gesetzgeber hat jedoch die zu schützenden Daten mit dem weiten Schutzbereich der „Zugangssicherung" umgeben, damit bei komplexen Systemen dem Verfügungsberechtigten ausreichender Spielraum für die Anbringung seiner Sicherungsmaßnahmen bleibt. Dieser weite Bereich umfaßt auch den Schutz vor Kenntnisnahme. Dies wird durch einen Vergleich deutlich:

Der Weg (Zugang) zu einem schutzwürdigen Gegenstand (Datum) wird durch viele Schranken und Hindernisse versperrt, wobei am Ende des Weges der Gegenstand erst nach Überwindung des letzten Hindernisses sichtbar wird. Diese Art von Schranken sind aber bei der DFÜ vielfach nicht einsetzbar.

Das Verschlüsseln eines Datums kann man nun mit dem Überstülpen eines anderen Gegenstandes über den zu schützenden vergleichen, der somit für den Eindringling verborgen bleibt, selbst wenn er die letzte Weg-Schranke überwunden hat.

Diese Betrachtungsweise bestärkt auch die anfangs aufgestellte These[55], wonach eine Schutzmaßnahme umso eher als Sicherung anzuerkennen ist, je unmittelbarer sie an den Daten angebracht ist. Und was ist unmittelbarer, als ein Datum in ein anderes umzuwandeln ..., wobei der ursprüngliche Bedeutuugsgehalt jederzeit rekonstruierbar bleibt?

3. Weitere Voraussetzungen

Der erforderliche Sicherungsgrad ist bei einem Schlüsseltext ebenfalls erreicht, da der Täter nur mit erhöhtem Aufwand die Originaldaten entschlüsseln kann. Desweiteren lassen die „nutzlosen" Daten des Schlüsseltextes dem Täter gegenüber erkennen, daß die Originalinformationen vor ihm verborgen bleiben sollen. Damit sind für kryptotechnische Verschlüsselungsverfahren die Voraussetzungen einer Zugangssicherung erfüllt. Eine Verschlüsselung in diesem Sinne ist jedoch dann nicht gegeben, wenn Schwierigkeiten bei der Rekonstruktion des übermittelten Textes lediglich als — wünschenswerte — Begleiterscheinung einer komplizierten Übertragungstechnik auftreten.

b) Sicherung mittels DFÜ

Ferner bestehen noch Maßnahmen, mittels Datenübertragung Teilnehmer/Nutzer eines (Netz-)Systems zu identifizieren und ihre Rechte zu überprüfen. Sicherung der Daten gegen unberechtigten Zugriff wird z. B. verwirklicht durch[56]:

- Teilnehmer-Nummer
- Modem-Kennwort
- Eingabe-Kennwort
- Rückspiegeln (Echoplexing)
- AIDA-Session PIN/TAN
- Chip-Card
- Sicherheitsabschaltung bei Fehlversuchen

Dabei handelt es sich um Zugangs/Zugriffssicherungen zum System und nicht um solche der Datenübertragung.

E) Im Ergebnis ist festzuhalten:

1. Grundsätzlich ist bei „Sicherungen gegen unberechtigten Zugang" von faktischen Hindernissen auszugehen, also von Schutzvorrichtungen physischer und technischer Art. Hierunter fallen auch die sogen. „logischen" Sperrvermerke.

Zu den tatbestandlichen Zugangssicherungen zählen auch die kryptotechnischen Verschlüsselungsverfahren, die den Bedeutungsgehalt der Daten ändern.

Sicherungsmaßnahmen, die nur den unberechtigten Zutritt zu Räumlichkeiten verhindern sollen, sind keine Zugangssicherungen i.S. des § 202a StGB.

Das Merkmal „unberechtigt" knüpft an das „Bestimmt-Sein" an.

2. Bei der Subsumtion einer Schutzmaßnahme unter den Begriff der „Zugangssicherung", sind folgende Voraussetzungen zu prüfen:

- Schutzzweck der Sicherung? (z. B. nicht überwiegend Gebäude- oder Raumsicherung oder Maßnahme gegen Katastrophenfälle)
- ist Maßnahme eine präventive Sicherung? D. h.: die Maßnahme ist dann keine Sicherung, wenn sie erst nach erfolgtem Zugriff auf Teile der zu schützenden Informationen Wirkung entfaltet, oder den unberechtigten Zugriffsversuch lediglich zu Beweiszwecken protokolliert
- ist erforderlicher Sicherungsgrad erreicht? Mindesterfordernis: Das Hindernis der Sicherungsmaßnahme muß so gestaltet sein, daß es *jeden* Täter zwingt, von der vom Verfügungsberechtigten vorgesehenen gesicherten Zugangsart abzuweichen
- das formale Geheimhaltungsinteresse muß für den Täter erkennbar sein, d. h. die Maßnahme muß Dokumentationscharakter besitzen.

[53] vgl.: Fn. (12)
[54] vgl.: Fn. (12)
[55] vgl. oben: D II
[56] *Gorn*, DuD 1985, 333, 335 f (speziell für Btx)

Literaturverzeichnis

Arbeitskreis Datenschutz und Datensicherung im G.U.I.D.E.: Datenschutz und Datensicherung bei individueller Datenverarbeitung (IDV) DuD 1986, 239
Dreher/Tröndle: Strafgesetzbuch, Kommentar, 43. Aufl., München 1983; zit.: Dreher/Tröndle
Dworatschek/Büllesbach/Koch u. a.: Personalcomputer und Datenschutz, Köln 1985; zit.: Dworatschek
Fischer, J.: Kriterien des Zugriffsschutzes in einem Rechnersystem, DuD 1985, 112
Gorn, Wolfgang: Möglichkeiten des Schutzes und der Sicherung von Btx-Daten, DuD 1985, 333
Granderath, Peter: Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität, DB-Beilage Nr. 18/86
Heider/Kraus/Welschenbach: Mathematische Methoden der Kryptoanalyse, Braunschweig 1985; zit.: Heider/Kraus/Welschenbach
Hellfors, S./Seiz, M.: Praxis betrieblicher Datensicherung, Berlin 1977; zit.: Hellfors/Seiz
Hoppe, Michael: Straf- und zivilrechtliche Würdigung von Mißbrauchsfällen im EDV-Bereich nichtöffentlicher Unternehmungen, technisch-organisatorische Datensicherungsmöglichkeiten und Entscheidungshilfen zur Auswahl von Sicherungsmaßnahmen; Dissertation Hamburg 1978, zit.: Hoppe
Lenckner, Th./Winkelbauer, W.: Computerkriminalität — Möglichkeiten und Grenzen des 2. WiKG (I), CuR 1986, 483
Möhrenschläger, Manfred: Das neue Computerstrafrecht, Wistra 1986, 128
Pawlikowsky, Gerhart J.: Punktation von Grundsätzen der Datensicherung, DuD 1985, 105
Rudolphi/Horn/Samson/Schreiber: Systematischer Kommentar zum StGB, 7. Lieferg. der 3. Aufl., Frankfurt, Juni 1985; zit.: R/H/S-Bearbeiter
Rupp: Computersoftware und Strafrecht, Dissertation Tübingen 1985; zit.: Rupp
Schönke-Schroeder-Bearbeiter: Strafgesetzbuch, Kommentar, 21. Aufl., München 1982; zit.: S-S-Bearbeiter
Sieber: Computerkriminalität und Strafrecht, 2. Aufl., Köln/Berlin/Bonn/München 1980; zit.: Sieber
Weck, Gerhard: Datensicherheit: Methoden, Maßnahmen und Auswirkungen, Stuttgart 1984; zit.: Weck

Für Fotokopien (Reprographien), die zum privaten und sonstigen eigenen Gebrauch von urheberrechtlich geschützten Vorlagen gezogen werden, hat die Urheberrechtsnovelle 1985[1] eine generelle Vergütungspflicht und einen zweigeteilten Vergütungseinzug eingeführt. — Die nachfolgende Untersuchung betrachtet die rechtlichen Voraussetzungen und die wirtschaftlichen Auswirkungen dieser Novellierung (§§ 53, 54 UrhG). Sie geht nicht auf die Strafvorschriften des UrhG und die Einzelheiten des Schiedsverfahrens gem. §§ 14 ff. Urheberrechtswahrnehmungsgesetz (WahrnG) ein.

Die Urheberrechtsvergütung im Fotokopierbereich: Rechtliche und wirtschaftliche Besonderheiten

Teil 1

Günther E. W. Möller/Josef A. Mohr*

Teil 1

A. Darstellung und rechtliche Würdigung der §§ 53, 54[2]

Fotokopien „zum persönlichen Gebrauch" waren nach dem Urheberrechtsgesetz alter Fassung[3] sowohl zustimmungs- als auch vergütungsfrei. Nach § 54 Abs. 1 a. F. galt diese Vergütungsfreiheit grundsätzlich auch für Fotokopien „zum sonstigen eigenen Gebrauch". Sie wurden allerdings gem. § 54, Abs. 2 a. F. vergütungspflichtig, wenn sie zu „gewerblichen Zwecken" hergestellt wurden. Dann hatten die Urheber gem. §§ 54 Abs. 2 und 3 i. V. m. 53 Abs. 5 a. F. gegen den Hersteller und Importeur von Geräten, die zur Vornahme sol-

* Günther E. W. Möller und Josef A. Mohr sind Rechtsanwälte in Frankfurt

[1] Verkündet am 24. 06. 1985, BGBl. I, S. 1137
[2] Paragraphen ohne weitere Angaben beziehen sich auf das Urheberrechtsgesetz
[3] Vom 09. 09. 1965, BGBl. I, S. 1273