Computerhacken und materielles Strafrecht
- unter besonderer Berücksichtigung von § 202a StGB -

Dissertation

Rechts-, Wirtschafts- und Verwaltungswissenschaftliche Sektion
Fachbereich Rechtswissenschaft
der
Universität Konstanz

vorgelegt von

Pirmin Schmid

Meinen Eltern

Vorwort

Die vorliegende Arbeit wurde vom Fachbereich Rechtswissenschaft an der Universität Konstanz als Dissertation angenommen. Die mündliche Doktorprüfung fand am 25. April 2001 statt. Literatur und Rechtsprechung konnten bis Mitte November 2000 berücksichtigt werden.

Meinem Doktorvater Prof. Dr. Dr. Eric Hilgendorf danke ich sehr herzlich für die Unterstützung meiner Arbeit. Herr Prof. Dr. Dr. Eric Hilgendorf erstellte auch das Erstgutachten. Für die Erstellung des Zweitgutachtens gilt mein Dank Herrn Prof. Dr. Wolfgang Heinz.

Ganz besonders bedanke ich mich bei meinen Eltern für ihre stets verständnisvolle Unterstützung. Für die Endkorrektur danke ich meiner Schwester Verena Burgbacher und Herrn Dr. Ingo Werner. Ihm ist darüber hinaus besonders zu danken für die vielen fruchtbaren Gespräche zu computerstrafrechtlichen Themen. Schließlich gilt mein Dank allen, die mich bei der schwierigen Aufgabe des Promovierens in persönlicher Hinsicht unterstützt haben.

Berlin, im April 2001

Pirmin Schmid

Gliederung

Kapitel 1: Das Phänomen Hacker: Geschichte und Begriffsbestimmung 10

A. Hacker und Hacken 10

B. Internet 13

C. Strafrechtliche Begriffsbestimmung des Hackens 18

Kapitel 2: Der sog. „Hackerparagraph“: § 202a 22

A. Die Entstehungsgeschichte 22

B. Das Rechtsgut 25

C. Der objektive Tatbestand 52

D. Der subjektive Tatbestand 117

E. Die Rechtswidrigkeit 117

F. Schuld 119

G. Versuch 119

H. Konkurrenzen 119

I. Strafantrag 119

Kapitel 3: Computerhacken und Strafrecht 121

A. Das bloße Eindringen in ein fremdes Computersystem (Hacken i.e.S.) 121

B. Das Hacken im weiteren Sinne 138

C. Untersuchung hackerspezifischer Vorgehensweisen 156

Kapitel 4: Zusammenfassung 178

Inhaltsverzeichnis

Kapitel 1: Das Phänomen Hacker: Geschichte und Begriffsbestimmung 10

A. Hacker und Hacken 10

B. Internet 13

C. Strafrechtliche Begriffsbestimmung des Hackens 18

I. Der Begriff des Gesetzgebers 18

II. Weitere Begrifflichkeiten 19

III. Hackerbegriff in dieser Arbeit 20

Kapitel 2: Der sog. „Hackerparagraph“: § 202a 22

A. Die Entstehungsgeschichte 22

B. Das Rechtsgut 25

I. Bestimmung von strafrechtlichem Rechtsgüterschutz allgemein 25

II. Die in der Literatur vertretenen Meinungen 27

1. Vermögensschutz 27

2. Schutz eines formellen Geheimhaltungsinteresses 28

3. Schutz der Information 29

4. Schutz einer umfassenden Geheimsphäre 29

III. Stellungnahme 29

1. Haft 29

2. Zielinski 30

3. Gössel 31

4. Herrschende Meinung 31

IV. Verfügungsrecht 33

1. Verfassungsrechtliche Bedenken 33

2. Verfügungsbefugnis über Daten in § 202a und § 303a 34

3. Stimmen aus der Literatur 34

4. Anknüpfungspunkte für die Datenzuordnung 35

a) Der Erwerb der Daten 36

b) Das „Betroffensein“ durch den Dateninhalt 36

c) Geistige Urheberschaft am Dateninhalt 36

d) Das Eigentum am Datenträger versus „Skripturakt“ 37

(1) Die Ansicht von Hilgendorf ... 37
(2) Die Ansicht von Welp ... 38
(3) Stellungnahme ... 38
(4) Problematische Konstellationen ... 40
5. Übertragung der Verfügungsbefugnis ... 41
a) Einigung ... 42
b) Übergabe der Daten ... 43
(1) Publizität (Offenkundigkeit) ... 43
(2) Anlehnung an §§ 413, 398 BGB ... 44
(3) Anlehnung an § 929 S. 1 BGB ... 44
(a) Besitz ... 44
(b) Tatsächliche umfassende Zugriffsmöglichkeit über konkrete Daten ... 45
(i) Überlassung von Daten auf einem Datenträger ... 46
(ii) Überlassung ohne Speicherung auf Datenträger im Besitz des Erwerbers ... 46
(c) Problemfall Ursprungsdaten ... 47
c) Zusammenfassung ... 48
6. Ende der Verfügungsbefugnis über Daten ... 48

C. Der objektive Tatbestand ... *52*
I. Daten i.S.d. § 202a Abs. 2 ... 52
1. Computerprogramme als Daten ... 55
2. Datum/Daten ... 56
3. Die einschränkenden Merkmale des § 202a Abs. 2 ... 59
a) Nicht unmittelbar wahrnehmbar ... 59
b) Speicherung von Daten ... 61
c) Übermittlung von Daten ... 64
II. Die Datenbestimmung ... 65
1. Bestimmender ... 65
2. Bestimmung ... 66
3. Einverständnis ... 69
III. Die Datensicherung ... 70
1. Zugang ... 70
2. Besondere Sicherung ... 71
a) Mögliche Schutzvorrichtungen ... 72
b) Voraussetzungen einer besonderen Sicherung ... 73
(1) Dokumentation des Geheimhaltungswillens ... 74
(2) Auslegungsgrenzen der Begriffe „besondere“ und „Sicherung“ ... 75

(a) Sicherung ... 75
(b) „besondere“ ... 75
(3) Sicherungsgrad ... 75
(a) Stimmen aus der Literatur ... 76
(b) Stellungnahme ... 78
(i) Sicherungsgrad des § 243 Abs. 1 Nr. 2 ... 79
(ii) Übertragung des Sicherungsgrads auf § 202a ... 81
(4) Sicherungszweck ... 82
(a) Die Ansichten in der Literatur ... 82
(b) Stellungnahme ... 84
3. „Unberechtigt“ ... 86
a) Meinungsstreit ... 86
(1) Gleichsetzung mit „nicht für den Täter bestimmt“ ... 86
(2) Keine eigenständige Bedeutung ... 87
(3) Umkehrschluß aus „bestimmt“ ... 87
(4) Gedankliche Lückenlosigkeit ... 88
b) Erläuterung am Beispiel des closed-shop-Systems ... 88
(1) Fallkonstellationen ... 89
(2) Lösung nach den verschiedenen Ansichten ... 89
c) Stellungnahme ... 90
4. Sonderproblem: Überwindung der Zugangssicherung ... 92
a) Personalisierte versus nicht-personalisierte Perspektive ... 92
b) Überwindung der Sicherung ... 94
5. Zusammenfassung ... 99
6. Problemfälle ... 99
a) Datenverschlüsselung ... 99
(1) Sicherungsverfahren ... 100
(2) Strafrechtliche Behandlung ... 102
(a) Ansichten in der Literatur ... 102
(b) Stellungnahme ... 103
b) Geheimhaltung ... 104
IV. Tathandlung ... 106
1. Anknüpfungspunkte für die Auslegung ... 106
a) § 259 ... 106
b) § 202 Abs. 1 Nr. 2, § 202 Abs. 2 ... 107
c) § 96 ... 107

2. Auslegung ... 108
a) Fallgruppen ... 108
(1) Materialisierte Daten ... 108
(2) Nicht-materialisierte Daten ... 110
b) Definition ... 110
3. Mehrfache Datensicherung ... 111
4. Problemfall: Datenverschlüsselung ... 112
a) Entschlüsselung ... 112
b) Entschlüsselbarkeit ... 112
c) Keine Anforderungen bei Wegnahme des Datenträgers, sonst Entschlüsselbarkeit ... 113
(1) Materialisierte Datenerlangung ... 113
(2) Nicht-materialisierte Datenerlangung ... 113
d) Keine Anforderungen, wenn vorgeschaltete Sicherung überwunden wurde ... 114
e) Stellungnahme ... 114

D. Der subjektive Tatbestand ... 117

E. Die Rechtswidrigkeit ... 117
I. Das Merkmal „unbefugt“ ... 117
II. Rechtfertigung ... 118

F. Schuld ... 119

G. Versuch ... 119

H. Konkurrenzen ... 119

I. Strafantrag ... 119

Kapitel 3: Computerhacken und Strafrecht ... 121

A. Das bloße Eindringen in ein fremdes Computersystem (Hacken i.e.S.) ... 121
I. Betrachtung der gegenwärtigen strafrechtlichen Situation ... 121
1. Die Subsumtion des Hackens unter § 202a ... 121
2. Ansichten zur Strafbarkeit des Hackens i.e.S. ... 122
a) Ansätze in Nachfolge der Ansicht des Gesetzgebers ... 122
(1) Teleologische Reduktion ... 122
(a) Unterscheidung zwischen Systemzugriffsdaten und Daten *im* System ... 123
(b) Reproduzierbarkeit der Daten oder gesicherte Kenntnis ... 123
(c) Speicherung auf anderem Datenträger ... 124
(2) Andere Ansätze zur Durchsetzung des gesetzgeberischen Willens ... 124

(a) Weiterverwendungsabsicht ... 124
(b) Datennutzung ... 125
b) Ansatz, der sich gegen den erklärten Willen des Gesetzgebers stellt ... 125
3. Stellungnahme ... 126
a) Andeutungstheorie ... 126
b) Datennutzung ... 127
c) Speicherung auf anderen Datenträger ... 127
d) Weiterverwendungsabsicht ... 128
e) Reproduzierbarkeit versus Datendifferenzierung ... 128
II. Betrachtung der kritischen Äußerungen zur Intention des Gesetzgebers ... 131
1. Die Kritikpunkte in der Literatur ... 131
a) Strafwürdigkeit (Rechtsgutsproblematik) ... 131
b) Beweisführung ... 132
c) Argumentation des Gesetzgebers §§ 303a, 303b schütze vor starken Störungen ... 133
2. Stellungnahme ... 133
a) Grundlagen einer Pönalisierung de lege ferenda ... 134
(1) Tatsachenseite ... 134
(2) Strafwürdigkeit (rechtliche Seite) ... 136
b) Ausgestaltung ... 137

B. Das Hacken im weiteren Sinne ... 138
I. Angriffe auf Daten i.S.d. § 202a Abs. 2 ... 138
1. Kenntnisnahme, Kopie oder Wegnahme des Datenträgers ... 138
2. Manipulationen ... 138
a) Datenveränderung, § 303a ... 138
b) Computersabotage, § 303b ... 141
II. Angriffe auf qualifizierte Daten ... 145
1. Kenntnisnahme, Kopie oder Wegnahme des Datenträgers ... 145
a) Industrie- und Wirtschaftsspionage, § 17 UWG ... 145
(1) Geheimnisverrat, § 17 Abs. 1 UWG ... 148
(2) § 17 UWG Abs. 2 ... 149
(a) Betriebsspionage, § 17 Abs. 2 Nr. 1 ... 149
(b) Geheimnishehlerei, § 17 Abs. 2 Nr. 2 UWG ... 152
b) Ausspähung personenbezogener Daten, § 43 BDSG ... 152
2. Manipulationen (§ 43 Abs. 1 Nr. 1 Alt. 2 BDSG) ... 155

C. Untersuchung hackerspezifischer Vorgehensweisen ... 156
I. Paßwortausspähung ... 156

1. Vorgehensweisen ... 156
a) Trial and error ... 156
b) Paßwortknacker ... 157
(1) Lexikon-Angriff ... 157
(2) Brute-Force-Attack ... 158
c) Social Engeneering ... 158
d) „Müllen“ ... 159
2. Strafrechtliche Bewertung ... 159
a) Methoden ... 159
b) Erfolg ... 161
II. Datenreisen ... 163
III. Trojanische Pferde ... 165
1. Aufbau und Funktion ... 165
a) Allgemein ... 165
b) Spoofing-Programme ... 167
c) Aktuelle Beispiele ... 168
2. Strafrechtliche Bewertung ... 169
(1) Installieren des Trojanischen Pferds ... 170
(a) Automatische Änderung ... 170
(b) Änderung des Datenumfeldes ... 171
(2) Ausschnüffeln des Codeworts ... 171
(3) Anschließendes Verwenden des ausgeschnüffelten Paßworts ... 171
IV. Ausnutzen von sog. Wanzen oder sog. Falltüren ... 172
1. Vorgehensweise ... 172
2. Strafrechtliche Bewertung ... 173
V. Adress-Spoofing ... 173
1. Vorgehensweise ... 173
2. Strafrechtliche Bewertung ... 174
VI. Port-Scanner ... 176
1. Arbeitsweise ... 176
2. Strafrechtliche Bewertung ... 176
VII. Packet-Sniffer ... 177

Kapitel 4: Zusammenfassung ... 178

Einleitung

Das Computerhacken nimmt in der polizeilichen Kriminalstatistik (PKS) als Unterkategorie der Computerkriminalität hinsichtlich der Zahl der ermittelten Fälle eine untergeordnete Rolle ein.[1] Dennoch ist allgemein bekannt, daß diese Zahl nicht das eigentliche Aufkommen und die eigentliche Bedeutung des Computerhackens widerspiegelt. Immer wieder waren in den letzten Jahren und gerade in der jüngsten Vergangenheit Einbrüche zumeist jugendlicher Hacker in verschiedenste kommerzielle, wie auch staatliche am Internet angeschlossene Rechner ein Thema, welches auch in der Öffentlichkeit großes Aufsehen erregte.

Die globale Vernetzung nimmt ihren Lauf. Damit einher geht jedoch auch die Gefahr, daß vernetzte Systeme anfällig sind für Einbrüche nicht willkommener Gäste. Das Anschließen eines Rechners an das Internet und damit die Möglichkeit weltweiter Kommunikation und Präsentation bis hin zu kommerziellen Angeboten ist immer ein Drahtseilakt zwischen Öffnung des Systems nach außen und der Sicherung desselben gegen Angriffe von außen. Absolute Sicherheit kann es nicht geben. Daher sind deren Betreiber bei entsprechender Intensität der Beeinträchtigung dieser vernetzten Systeme auch strafrechtlich zu schützen, um den Hackern als den ungebetenen Eindringlingen auch dadurch ein deutliches Signal zu setzen.

Die vorliegende Arbeit versucht, dem Leser einen Überblick über die tatsächlichen Vorgehensweisen der Hacker und deren strafrechtliche Bewertung zu verschaffen. So werden in Kapitel 1 die Grundlagen der Thematik behandelt. Diese sind die Darstellung des Phänomens der Hacker und das Spielfeld derselben, das Internet und anschließend daran die Eingrenzung des gleichsam uferlosen Hackerbegriffs auf einen handhabbaren strafrechtlichen Hackerbegriff.

Großen Raum nimmt dann Kapitel 2 ein. Hier und in Kapitel 3 werden die Grundlagen der strafrechtlichen Behandlung des Computerhackens bearbeitet. Dies erforderte eine eingehende Untersuchung des § 202a[2] (Ausspähen von Daten), der insbesondere mit Abstrichen, wie im Laufe der Untersuchung noch zu sehen sein wird, für die sog. Hakker gedacht war. In Kapitel 3 werden die Definitionen des Hackens aus Kapitel 1 wieder

---

[1] So weist die PKS des Jahres 1999 bundesweit 210, diejenige des Jahres 1998 267 Fälle in der Kategorie „Ausspähen von Daten“ auf. Diese sind nur 0,5% aller in der politischen Kriminalstatistik von 1999 aufgeführten Fälle im Bereich Computerkriminalität. Die PKS ist zu finden unter www.bka.de/pks/

[2] §§ ohne Angabe sind solche des StGB.

aufgenommen und anhand von Differenzierungen zwischen der Art des Angriffs, sowie der Qualität des Angriffsobjekts strafrechtlich untersucht.

Der letzte Teil des Kapitels 3 fasst den Fokus noch etwas enger. Hier werden, in Fallgruppen eingeteilt, spezifische Vorgehensweisen der Hacker im tatsächlichen Bereich auch für den Computerlaien möglichst verständlich dargestellt und daraufhin einer fallgruppenbezogenen strafrechtlichen Untersuchung unterzogen.

In Kapitel 4 werden die Ergebnisse zusammengefaßt.

Kapitel 1: Das Phänomen Hacker: Geschichte und Begriffsbestimmung

A. Hacker und Hacken[3]

Gerade im deutschsprachigen Raum wird das Wort „Hacken“ mit dem aggressiven Bearbeiten einer Computertastatur assoziiert. Der Begriff des „Hack“ und damit auch des Hackers stammt jedoch von einer Gruppe von Studenten der fünfziger Jahre des Massachusets Institute of Technology (MIT), einem technischen Forschungsinstitut der amerikanischen Elite-Universität Harvard in Cambridge, Massachusetts.[4] Ein „Hack“ war in ihrer Sprache eine besonders gelungene Lösung eines komplexen technischen Problems.[5] Dies war zunächst unabhängig von der Verwendung eines Computers. So war einer der ersten großen „Hacks“ die Entdeckung, daß mit Benutzung einer von einem Cornflakes-Hersteller als Beipackgeschenk verteilten Pfeife die Telefonvermittlungen einer amerikanischen Telefongesellschaft dazu veranlaßt werden konnten, Ferngespräche freizuschalten. Der Ton dieser Pfeife hatte genau die dafür notwendige Frequenz von 2600 Hertz. Dies war die Geburtsstunde der sog. „Phreaker“[6]. Im Zuge dessen wurden Apparate gebaut, die diesen und andere Töne erzeugen, um kostenlos das Telefonnetz benutzen zu können.[7]

Diese Hacker der ersten Stunde in den 60er und 70er Jahren entwickelten im Zuge ihren ersten Gehversuche an Großrechnern und der Manipulation der Telefonsysteme eine sog. Hackerethik.[8] Sie ist in einem Katalog von sechs Forderungen formuliert worden:[9]

---

3 Englisch: hacking.

4 *Heine*, Die Hacker, S. 29.

5 Vgl. *Bauerfeld*, JurPC 1989, 211(211).

6 Kunstwort zusammengesetzt aus „Phone“ und „Freak“. Vgl. *Sieber*, Computerkriminalität und Informationsstrafrecht in der internationalen Informations- und Risikogesellschaft, in: Neue Strafrechtsentwicklungen im deutsch-japanischen Vergleich, Kühne/ Miyazawa (Hrsg.), 1995 (ius criminale, Bd. 2), S. 33 (42).

7 Ein Apparat, der den 2600 Hertz-Vermittlungston erzeugen kann, wird „blue box“ genannt. Es gab aber auch die sog. „black box“, die ein fortlaufendes Ertönen eines Freizeichens vortäuschen konnte, sowie die sog. „red box“, mit deren Hilfe Münzfernsprecher kostenlos bedient werden konnten.

8 Dazu auch *Hafner/Markoff*, Cyberpunk, S. 12.

9 Aus *Levy*, Hackers – Heroes of the Computer Revolution.

- Der Zugriff auf Computersysteme – und allen anderen Dingen, die Auskunft darüber geben, wie die Welt funktioniert – muß für jedermann uneingeschränkt möglich sein.
- Alle Informationen sind kostenlos.
- Mißtraue Autoritäten – unterstütze Dezentralisation.
- Hacker sollten nach ihrem Tun und nicht nach Diplomen, Alter, Rasse oder Position beurteilt werden.
- Mit Computern kann auch Kunst und Schönheit geschaffen werden.
- Computer können das Leben zum Besseren verändern.

Auf der Grundlage dieser Grundsätze, deren Basis die Forderung nach einer unbegrenzten Freiheit von Information und Kommunikation ist, entwickelte sich eine Untergrundszene.

Diese Szene unterscheidet selbst zwischen Hackern und Crackern.[10]

- „Hacker“ sind danach Personen, die sich für die geheimnisvollen und verborgenen Arbeitsweisen eines jeglichen Betriebssystems interessieren. Sie sind meistens Programmierer, die sich dadurch ein fortgeschrittenes Wissen über Betriebssysteme und Programmiersprachen erwerben. Hacker können Sicherheitslöcher in Systemen und Gründe dafür entdecken. Hacker sind ständig auf der Suche nach weiterem Wissen, teilen freimütig ihre Entdeckungen mit und würden nie und nimmer absichtlich Daten zerstören.
- „Cracker“ sind in der Sichtweise der Hackerszene solche, die böswillig in die Systemintegrität entfernter Rechner einbrechen, bzw. sie auf andere Weise schädigen. Nachdem Cracker unautorisierten Zugang erhalten haben, zerstören sie wichtige Daten, verweigern Dienste für legitime Benutzer oder verursachen grundsätzliche Probleme im Arbeitsablauf des angegriffenen Rechners.

Grundpfeiler dieser Szene waren vor allem Hackerzeitschriften. Allen voran ist hier die TAP (Technology Assistance Programm, aber auch übersetzt : anzapfen), die insbesondere Spezialwissen zu den Telefonnetzen veröffentlichte, welches dann auch von der Leserschaft allesamt ausprobiert wurden. Weitere wichtige Zeitschriften sind in diesem Zusammenhang die 1984 gegründete „2600: The Hacker Quarterly“ und die sog.

---

[10] Folgende Definition entnommen aus *Anonymous*, Hacker`s guide, S. 84; als Beispiel für zahlreiche, der obigen sehr ähnlichen Begriffsdefinitionen im Internet: www.flyingkorschi.de.

„Phrack“. In diesen werden, neben technischen Themen auch immer wieder politische Anliegen aus der Hackerszene verbreitet.

Ende der 70er Jahre wurden mit der Entwicklung des Personalcomputers und erschwinglichem Datenfernübertragungszubehör diese Printmedien dann von geheimen Mailboxsystemen oder sog. Hacker-Bulletin-Board-Systemen nach und nach abgelöst. Eingeweihte konnten sich hier per Datenfernübertragung in einen Mailboxrechner einloggen und sodann Informationen aller Art austauschen.

Zum eigentlichen **Computer**hacken in der Variante des Eindringens in fremde Datenbereiche mittels Datenfernübertragung kam es im Zuge der Vernetzung von Computersystemen. Hier ist die Schnittstelle der sog. Phone-Phreaks und Computerhackern zu sehen. Damit der Computerhacker in fremde Netze eindringen konnte, mußte er, wenn er von zuhause aus hacken wollte, über das Telefonnetz in Datennetze vordringen. Bei entsprechender Dauer können hierbei hohe Telefongebühren entstehen. Um dies zu vermeiden, wurden zunehmend die Techniken der sog. Telefonhacker attraktiv.

In Deutschland ist der 1984 gegründete Chaos Computer Club (CCC) die führende Institution der klassischen Hackerszene mit Hackerethos.[11] Wichtigstes Ziel des CCC ist ein selbstdefiniertes Menschenrecht auf weltweiten freien Informationsaustausch. Größte Aufmerksamkeit und Popularität erlangte der CCC, als er eine Sicherheitslücke im neuen BTX-System der Bundespost (heute T-Online der Telekom) aufdeckte. Ein Softwarefehler hatte dazu geführt, daß der CCC das BTX-Paßwort der Hamburger Sparkasse erfahren konnte.[12] Durch diese Aktion des CCC wurden der deutschen Öffentlichkeit zum ersten Mal in drastischer Weise die Sicherheitsprobleme von vernetzten Systemen vor Augen geführt.

Der Personenkreis, der sich mit dem Eindringen in fremde Datenbereiche beschäftigt, ist heute jedoch wesentlich größer. So bedienen sich die verschiedensten Personen mit den unterschiedlichsten Motiven der Hackertechniken. Teilweise ist es unter Verwendung der im Internet vielfach angebotenen sog. Hackertools[13] auch mit durchschnittlichem Kenntnisstand möglich, in fremde Datenbereiche vorzudringen. Eine mögliche Einteilung des betreffenden Personenkreises hat *Kyas* vorgenommen.[14] So unterscheidet er 6 Gruppen:

---

11 Zur Hackerethik des CCC, *Schrutzki*, Die Hackerethik, in: Wiekmann (Hrsg.), Das Chaos Computer Buch, S. 168 f.

12 *Bouteiller*, Das Hacker-Hack-Buch, S. 11.

13 Programme, die das Einbrechen in fremde Systeme erleichtern.

14 *Kyas*, Sicherheit im Internet, S. 28.

- Mitarbeiter des eigenen Unternehmens.
- Studenten/Teenager aus dem Universitäts- und Schulumfeld.
- Personen aus dem Konkurrenz- und Wettbewerbsumfeld.
- Hacker/Cracker aus der Computer-Untergrundszene.
- Herkömmliche Kriminelle aus dem Drogen/Mafia-Umfeld.
- Professionelle Hacker/Industriespione.

An dieser anschaulichen Aufzählung ist erkennbar, daß die eigentlichen „Hacker“ der ersten Stunde und ihre „Enkel“ mittlerweile eine von mehreren Gruppen darstellen, die sich derselben Verhaltensweise, des Eindringens in fremde Datenbereiche, zuwenden. Mit der 2. Gruppe wird besonders deutlich, daß das Eindringen in geschützte Bereiche oder zumindest vom Eigentümer nicht für Unbefugte gedachte Bereiche nicht nur über Datenfernübertragung erfolgt, sondern auch sehr häufig direkt vor Ort. Der Betreffende hat zumeist schon einen Zugang zum System, der jedoch auf einzelne Bereiche oder Befugnisse beschränkt ist. In dieser Arbeit ist das Hacken über Datenfernübertragung, sowie auch das Vor-Ort-Hacken Gegenstand der Untersuchung. Denn auch die betreffenden Strafgesetze unterscheiden diesbezüglich nicht, wie später noch zu zeigen sein wird.

Zur letzten Gruppe, der professionellen Hacker, sind die Geheimdienste zu rechnen, die, so wird vielfach kolportiert, gerade im Bereich der Wirtschaftsspionage für nationale Großfirmen mit Hackermethoden die ausländischen Konkurrenzfirmen ausspähen.[15]

B. Internet

Das eigentliche und beliebteste Betätigungsfeld derjenigen Personen, die sich mit dem Eindringen in fremde Datenbereiche beschäftigen, ist heutzutage und auch in Zukunft das Internet. Das Internet ist weltweit bequem über Telefonleitungen erreichbar und fast alle wichtigen Institutionen und Wirtschaftsunternehmen sind daran angeschlossen. Damit stellen die daran beteiligten Systeme ein ideales Angriffsziel für Hacker dar.

Im Folgenden soll daher die Entwicklung des Internet und die Funktionsweise in kurzer Form erläutert werden. Was genau ist das Internet? Das Wort „Internet“ setzt sich aus zwei Teilen zusammen, nämlich aus „inter“ (lateinisch für „zwischen“) und „net“, der

---

[15] Vgl. Der Spiegel, Lauscher im Datenreich, 36/1996, 194 ff.

Abkürzung für „networking“ (englisch für „vernetzen“).[16] Im Computerbereich bedeutet „Internet“ die Vernetzung von Computernetzen. Lokale Netzwerke (LAN[17]), die sich zumeist auf ein Gebäude beschränken oder sich zumindest auf einem Betriebsgelände befinden, werden vernetzt zu Weitbereichsnetzen (WAN[18]). Das Internet ist damit im ursprünglichen Sinn ein sehr großes, weltweites WAN, welches LANs und kleinere WANs verbindet.[19]

Die Ursprünge des Internet sind in der Zeit des Kalten Krieges zu finden. Nachdem man während der Kubakrise 1963 nur sehr knapp einem Krieg entgangen war, wurden in den USA verstärkt Studien über den möglichen Ablauf eines thermonuklearen Krieges und seine Auswirkungen auf Truppen und Zivilbevölkerung in Auftrag gegeben. Besondere Beachtung fand das Problem, wie sich ein Land während und nach einem solchen Krieg organisieren und reorganisieren läßt.

Eine dieser Studien befaßte sich mit der Frage, wie sich die zahlreich über das ganze Land verstreuten Rechner des Militärs und der Zivilverwaltung so miteinander vernetzen ließen, daß es möglich wäre, auch noch nach einer nuklearen Auseinandersetzung der beiden Supermächte über weite Strecken Informationen auszutauschen. Die theoretische Lösung des Problems wurde 1964 veröffentlicht. Die damit verbundenen Vorgaben waren revolutionär:

- Das Netzwerk dürfe keine zentrale Aufsicht haben, sie wäre sofort ein Angriffspunkt des Gegners; mithin müsse jeder Knoten im Netz gleichwertig zu jedem anderen Informationen aussenden, weitergeben und empfangen können.
- Die Netzwerkprotokolle würden von Beginn an so entworfen, als wäre das Netz schon beschädigt und unzuverlässig.
- Die Nachrichten selbst würden in Pakete zerlegt, jedes einzelne mit dem Bestimmungsort versehen und auf den Weg geschickt, ohne daß der genaue Weg des einzelnen Paketes bekannt war.

Nach diesen Prinzipien errichtete man in Großbritannien ein erstes Testnetz. Von diesem ersten Schritt in England angeregt, beschloß das DOD (Department of Defense, Verteidigungsministerium) eine seiner Projektgruppen, die ARPA (Advanced Research

---

16 Anders *Grieser/Irlbeck*, Computerlexikon, S. 461. Diese bezeichnen den Begriff „Internet“ als Abkürzung für „International Network“. Das ist heute im Ergebnis ebenso vertretbar.

17 Abkürzung für „Local Area Network“.

18 Abkürzung für „Wide Area Network“.

19 *Grieser/Irlbeck*, Computerlexikon, S. 461.

Projekt Agency, gegründet 1957 als Reaktion auf die sowjetische Raumsonde Sputnik[20]) bei der Errichtung eines größeren Projektes zu finanzieren. Die damals größten und schnellsten Rechner sollten über ein solches Netz verbunden werden.

Daher plante im Jahre 1966 das zur ARPA gehörige Information Processing Techniques Office, alle Computerzentren der ARPA, die über das gesamte Land verteilt waren, miteinander zu verbinden. Ziel war dabei, auch verschiedenartige Rechner miteinander zu koppeln. Im Herbst 1969 wurde dieses Vorhaben verwirklicht. Das Netz wurde ARPANET genannt und bestand aus vier Knoten[21]: Die University of California in Los Angeles, das Stanford Research Institute, die University of California in Santa Barbara und die University of Utah.

Die beteiligten Rechner waren von verschiedenen Herstellern und verwendeten unterschiedliche Betriebssysteme. Es gelang jedoch, diese Rechner zunächst über speziell angepaßte Netzwerkprogramme zu verbinden, später mit Hilfe eines an die Rechner angeschlossenen Minicomputers, des sog. „Interface Message Processor", der die Kommunikation der Rechner mittels eines einheitlichen Programms übernahm. Hiermit gelang es zum ersten Mal unterschiedliche Rechnersysteme miteinander zu verbinden. Dies war ein großer Schritt in Richtung Internet.

Die ersten beiden Anwendungen des ARPANET, „telnet"[22] und „ftp"[23] wurden nicht übermäßig genutzt. Das änderte sich jedoch mit einer Erfindung im Jahre 1972, einer Software zum Versenden und Empfangen elektronischer Post, die über das ARPANET transportiert wurde: die E-mail, bis heute eine „power application" des Internet.

Das ARPANET wurde beliebt, so daß nach dessen Vorbild weitere Netze entstanden. Auch gab es Netze, die völlig anders aufgebaut waren als das ARPANET. Die ARPA war bestrebt, die technisch unterschiedlichsten Netzwerke miteinander zu verbinden. Das Problem war jedoch, daß Computer und Netze miteinander kommunizieren sollten, ohne eigentlich kompatibel zu sein. Dafür war es notwendig, sich auf ein einheitliches Datenformat und eine einheitliche Methode der Verbindungsherstellung zu einigen. So wurde 1974 das „Transmission Control Protocol / Internet Protocol" (TCP/IP) einge-

---

20 Hier sollte auf den zeitweisen technischen Vorsprung der Sowjetunion reagiert werden.

21 Englisch: nodes.

22 Mit diesem Übertragungsprotokoll kann ein ans Netz angeschlossener Rechner ferngesteuert werden (vgl. *Grieser/Irlbeck*, Computerlexikon, S. 873).

23 Abkürzung für „File Transfer Protocol". Mit diesem Protokoll können Dateien von einem Rechner über das Internet zu einem anderen übertragen werden, unabhängig von deren Betriebssystem oder der Art der Verbindung (vgl. *Grieser/Irlbeck*, Computerlexikon, S. 375).

führt. Aufgrund seiner Zuverlässigkeit und der Tatsache, daß es kostengünstiger als andere Protokolle in ein System integriert werden konnte, wurde TCP/IP zunehmend eingesetzt. Im Jahre 1983 wurde es in verschiedene Versionen des gerade in Netzwerken verbreiteten Betriebssystems UNIX integriert. Da TCP/IP frei verfügbar war, wurde es bald auch auf andere Plattformen portiert, so daß man heute von der Familie der TCP/IP-Protokolle spricht.[24] Verschiedene nationale und internationale Wissenschafts- und Forschungsnetze konnten über TCP/IP verbunden werden. Innerhalb dieser Netzwerke kann sehr wohl ein anderes Protokoll verwendet werden, es muß dann aber eine Schnittstelle[25] vorhanden sein, über die der Datenverkehr mit anderen Netzen abgewikkelt werden kann. Diese Kommunikationsprotokollfamilie stellt bis heute ein Grundpfeiler des Internet dar.

Die meisten der damaligen Netzwerke waren nur zur Verwendung für eine kleine Anzahl von Nutzern gedacht, da sie nur mit bestimmten Absichten gebaut wurden. Nach und nach setzte sich jedoch das Anliegen durch, daß der Netzwerkzugang zumindest allen hochqualifizierten Nutzern gewährt werden sollte, ungeachtet ihres Forschungsbereichs. Im Zuge dieser Entwicklung wurde das ARPANET, welches schon vorher in zwei Teilnetze, ein ziviles und ein militärisches (das sog. Milnet) aufgeteilt worden war, im Jahre 1990 abgeschaltet und durch das Netzwerk der National Science Foundation (NSFNET) ersetzt.

Vorhandene Computernetze außerhalb der USA, wie das deutsche Forschungsnetzwerk WiN, das seit 1990 deutsche Universitäten miteinander verband, schlossen sich nach und nach dem NSFNET an: die ersten waren Kanada, Dänemark, Finnland, Frankreich, Island, Norwegen und Schweden. Ein Jahr später folgten Deutschland, Japan, die Niederlande und das Vereinigte Königreich (UK).

Die Entwicklung des Internet zu einem Massenmedium ist jedoch der Erfindung des WWW[26] zu verdanken. 1991 entwickelte Tim Berners-Lee am Genfer CERN-Institut das *Hyperlink*-System, um Dokumente mit einem Inhalt, der für mehrere Forschungsbereiche interessant sein könnte, allen Interessierten zugänglich zu machen: Internet-Seiten konnten von nun an mit Hyperlinks[27] versehen werden. Durch einen einzigen Tastendruck oder Mausklick konnten Benutzer so von einer Internet-Seite zur nächsten springen und damit durch das gesamte Netz „surfen“. Jede Seite konnte mit jeder belie-

---

24 Es sind ca. 100.

25 In diesem Zusammenhang „Gateway“ genannt.

26 World Wide Web, übersetzt: Weltweites Netz.

27 Elektronische Verweise auf andere Seiten.

bigen anderen verknüpft werden, ungeachtet der Entfernung, bzw. der geographischen Lage des Rechners von dem aus die Seite abgerufen werden sollte, oder anderer Voraussetzungen. Es erlaubte damit den Zugriff auf Dokumente, die auf über die ganze Erde verteilte Rechner gespeichert sind, ohne daß der Anwender sich Gedanken über die Art des Rechners oder dessen Konfiguration zu machen brauchte.

In WWW-Dokumenten können heute nicht nur Texte implementiert werden, sondern jegliche in digitalisierter Form gespeicherte Daten. So können digitalisierte Videos, Sprachdateien und auch animierte Grafiken in WWW-Dokumente integriert werden.[28] Um diese Dokumente aufrufen zu können, muß ein bestimmtes Programm auf den Rechner geladen werden, ein sog. Browser[29]. Er übernimmt die Aufgabe, die angeklickten Seiten zu suchen und diese auf dem Bildschirm des Nutzers aufzubauen und sichtbar zu machen.

Mit Hilfe des WWW erregt das Internet in der Öffentlichkeit ungeahnte Aufmerksamkeit. Private Online-Dienste und Internet Service Provider (ISP) entstehen, die gegen Entgelt einen Zugang zum Internet für die Allgemeinheit über das Telefonnetz anbieten, während die Werbewirtschaft das World Wide Web als ideale Werbeplattform entdeckt. Das Web breitet sich immer mehr aus und entwickelt sich zum wichtigsten Dienst im Internet und überholt im Laufe des Jahres 1996 das Datenaufkommen aller FTP-Verbindungen.

Neueste Entwicklungen führen zu einer weiteren Kommerzialisierung des Internet. So entstehen beispielsweise zahlreiche Internet-Warenhäuser und elektronische Auktionsplattformen oder das sog. Online-Banking, bei dem der Bankkunde seine Geschäfte über das Internet erledigen kann, bis hin zum Ordern von Aktien[30]. Dies kann alles unter den schillernden Begriff des e[31]-Commerce gefaßt werden. Das Internet wird für das tägliche Leben immer wichtiger. Gerade die Sicherheit im Internet ist daher ein gewichtiger Faktor in der heutigen Gesellschaft.

---

28 *Grieser/Irlbeck*, Computerlexikon, S. 988.

29 Englisch;übersetzt: Schmöker- oder Stöberprogramm.

30 Sog. online-brokerage.

31 Abkürzung für „electronic“; „Commerce“ übersetzt: „Handel“.

C. Strafrechtliche Begriffsbestimmung des Hackens

I. Der Begriff des Gesetzgebers

Bei einer strafrechtlichen Begriffsbestimmung des Hackens und des Hackers ist zunächst die Begrifflichkeit des Gesetzgebers heranzuziehen, der sich mit der Hackerproblematik auseinandergesetzt hat. Einen Hinweis auf den Hackerbegriff gibt die Begründung des Rechtsausschusses zum 2. WiKG. (BT-Drs. 10/5058). Hier steht in der Begründung zu § 202a geschrieben: Insbesondere sollen sog. „Hacker", die sich mit dem bloßen Eindringen z.B. in ein Computersystem begnügen, also sich keine Daten unbefugt verschaffen, von Strafe verschont bleiben.[32] In den Vorschlägen zum 2. WiKG war die Pönalisierung des Ausspähens von Daten nicht vorgesehen, so daß diese für den Hackerbegriff nicht herangezogen werden können.

Hauptansatzpunkt des Gesetzgebers ist das bloße Eindringen in Computersysteme. Nun ist zu fragen, was bloßes Eindringen in solche Systeme ist. Bloßes Eindringen kann nur bedeuten, daß die Person an einem Einzelplatzrechner oder über Datenfernübertragung in ein System vordringt, zumeist unter Überwindung oder Umgehung der Sicherungsmaßnahmen, und dann nach dem Knacken der Sicherungsmaßnahmen, oder der Erkenntnis darüber, daß ein System gar nicht oder nur unzureichend vor solchen Angriffen geschützt ist, das System wieder verläßt. Dabei hat er keine (oder nur sehr wenige) Daten zur Kenntnis genommen, keine Daten kopiert, verändert oder zerstört oder sich sonstwie im System umgesehen. Er hat sozusagen lediglich ausprobiert, ob die Tür zum Haus oder zu Räumen eines Hauses ein Schloß hat, ob dieses Haus vollständig gemauert ist, oder welcher Art die Schlösser sind und welchen Standard sie haben. Ist das Fehlen einer Tür oder eines Schlosses festgestellt, oder das an sich wirksame Schloß auf irgendeine Weise geknackt worden, so verschwindet er sofort wieder.

Der Gesetzgeber wollte solche Personen, die er selbst „Hacker" nennt, nicht unter Strafe stellen. Das bloße Eindringen wurde noch nicht für strafwürdig erachtet. Es ist somit von einem positiven oder zumindest neutralen Hackerbegriff des Gesetzgebers auszugehen. Der Hacker ist danach jemand der Sicherheitslücken sucht, findet und gegebenenfalls der Öffentlichkeit bekannt macht.[33] Er ist nicht jemand, der immer weiter in

---

[32] BT-Drs. 10/5058, S. 28.

[33] Vgl. Interview mit Pressesprecher des CCC (Chaos Computer Club), internetworld, 9/1998, 40 ff.

solche Systeme vordringt, sich die dort abgelegten Informationen genau ansieht. Ebensowenig nutzt er das Wissen um diese Informationen dazu, einem Dritten zu schaden, oder sich zu bereichern. Hacken ist danach gleichsam ein „Sport". Der Hacker mißt sich mit den Programmierern und Anwendern von Sicherheitsmaßnahmen in einem sportlichen Wettkampf.[34] Der Hacker ist danach ein Computerexperte, der mit seinem Spezialwissen die Entwicklungen derjenigen testet, die damit Geld verdienen. Der Hackerbegriff des Gesetzgebers ist damit nicht unähnlich dem Begriff der Hackerszene[35] und scheint auch von diesem maßgeblich beeinflußt worden zu sein.

II. Weitere Begrifflichkeiten

Aufbauend auf dem Hackerbegriff des Gesetzgebers wurden in der Strafrechtswissenschaft weitere Unterteilungen von Personengruppen vorgenommen, deren typische Vorgehensweisen auch durch Normen des 2. WiKG unter Strafe gestellt wurden. Der sog. „Datenspion" dringt in Computersysteme oder in bestimmte Bereiche von Systemen ein. Insofern ist sein Vorgehen mit dem des Hackers identisch. Dann jedoch nimmt er Daten zur Kennntis oder kopiert Daten und gibt diese möglicherweise sogar an Dritte weiter.[36] Die Intention des Datenspions ist nicht der Zugang zum System, sondern die in dem System erhaltenen Daten als Information oder in der Funktion der Daten als Programme. Der „Crasher"[37] bedient sich ebenfalls derselben Methoden wie der Hacker, verändert jedoch die Daten im System. Dies kann dazu führen, daß die Daten gelöscht sind oder nicht mehr den gewünschten Informationsgehalt haben, so daß es dem Anwender nicht mehr möglich ist, sachgerecht mit dem System zu arbeiten.[38] Auf „Softwarepiraten"[39], die Computerprogramme raubkopieren und „Cracker"[40], die Kopierschutzmechanismen von Programmen beseitigen, um diese dann vervielfältigen zu können, wird in dieser Arbeit nicht eingegangen. Diese dringen nicht in ein Computersystem ein. Ihre Angriffsobjekte sind Computerprogramme und nicht Computersysteme.

---

34 Vgl. auch *Sieber*, Computerkriminalität und Informationsstrafrecht in der internationalen Informations- und Risikogesellschaft, in: Neue Strafrechtsentwicklungen im deutsch-japanischen Vergleich, Kühne/ Miyazawa (Hrsg.), 1995 (ius criminale, Bd. 2), S. 33 (41 f.).

35 Siehe dazu oben Seite 11.

36 Vgl. *von Gravenreuth*, NStZ 1989, 201 (204).

37 „Crash" übersetzt: abstürzen, krachen(d) fallen.

38 Vgl. *Lenckner*, Computerkriminalität und Vermögensdelikte, S. 19 ff.

39 Näher dazu *Tai* ‚Cracker, Hacker, Datensammler - Softwarepiraten unter der Lupe, S. 14 ff.

40 Englisch; übersetzt: knacken, brechen.

III. Hackerbegriff in dieser Arbeit

In der breiten Öffentlichkeit ist der Begriff „Hacker“ weit negativer, aber auch weiter. Die Personengruppe „Hacker“ wird synonym verwendet für Täter krimineller Akte in Rechnernetzen oder Einzelplatzsystemen. Letztendlich werden die meisten Vorgehensweisen innerhalb der Computerkriminalität den sog. „Hackern“ zugeordnet, wenn damit eine gewisse Intelligenz und insbesondere ausgefeiltes Spezialwissen einhergeht. Der Hackerbegriff der Öffentlichkeit deckt damit weite Teile der Computerkriminalität ab. Es ist daher festzustellen, daß der Hackerbegriff des Gesetzgebers sehr eng ist, der Begriff in der Öffentlichkeit dagegen sehr weit.

Die Begriffsbestimmung in dieser Arbeit will hier zum einen Ausgleich schaffen, zum anderen ein klares Abgrenzungskriterium entwickeln. Der Begriff des Gesetzgebers bietet ein klares Abgrenzungskriterium, nämlich das Eindringen in Rechner, Rechnersysteme, oder in Bereiche von Rechnern und Rechnersystemen. Der Begriff in der Öffentlichkeit berücksichtigt jedoch auch weitere Vorgehensweisen, die unter das Abgrenzungskriterium fallen. So dringen die sog. „Crasher“ und „Datenspione“ ebenfalls in die obengenannten Computersysteme und –bereiche ein. Daß diese weitere Handlungen vornehmen, ändert nichts daran, daß sie in ein System eingedrungen sind. Unterstützung findet dieser Ansatz darin, daß das Verb „hacken“ für jegliches Eindringen in Rechner steht, unabhängig davon, ob danach noch weitere gegebenenfalls strafrechtlich relevante Handlungen vorgenommen werden. Auch der Gesamtvorgang Eindringen und weiteres Vorgehen wird als „Hacken“ bezeichnet.

Ein Hacker ist danach, wer in Computersysteme oder in bestimmte Datenbereiche von Systemen eindringt oder einzudringen versucht. Er ist Oberbegriff für den Hacker im Sinne des Gesetzgebers und aller derjenigen, die über das Eindringen grs. mit den im System gespeicherten Daten nach Belieben verfahren können. Zur strafrechtlichen Untersuchung kann nicht gänzlich auf den Begriff des Gesetzgebers verzichtet werden, da sich darauf die Auslegung der einschlägigen Paragraphen bezieht. Der Begriff des Gesetzgebers wird daher als Hacken oder Hacker im engeren Sinne (i.e.S) bezeichnet. Alle Vorgehensweisen, die das Eindringen zur Grundlage haben, aber danach darüber hinaus gehen, werden als Hacken im weiteren Sinne (i.w.S.) bezeichnet. Dagegen sollten zur klaren Abgrenzung alle Vorgehensweisen in Rechnernetzen oder Einzelplatzsystemen, die nicht das Eindringen in diese Systeme zur Grundlage haben, auch nicht unter den

Begriff des „Hackens“ oder der „Hacker“ gefaßt werden, wie z.B. die in der jüngsten Vergangenheit erfolgten DOS-Attacken gegen führende Internet-Firmen.[41]

Zusammenfassend werden noch einmal die Begrifflichkeiten aufgeführt:

- Hacken i.e.S. ist das bloße Eindringen in Computersysteme oder bestimmte Datenbereiche von Computersystemen.
- Hacken i.w.S. ist das Eindringen in Computersysteme oder bestimmte Datenbereiche von Computersystemen und weiteren Handlungen im Zusammenhang mit den dort gespeicherten Daten.

[41] DOS (denial of service): Angriff auf Rechner im Internet, der dazu führt, daß die angebotene Dienstleistung nicht mehr zur Verfügung steht, bis hin zum Absturz des Systems.

Kapitel 2: Der sog. „Hackerparagraph“[42]: § 202a

Im Rahmen dieses Kapitels wird die für die Thematik dieser Arbeit maßgebliche Vorschrift untersucht.

A. Die Entstehungsgeschichte

Diese neue Vorschrift wurde durch das 2. WiKG vom 14.05.1986, BGBl. I 721 eingefügt. Das 1. WiKG trat am 01.09.1976 in Kraft. Schon im Herbst 1978 wurde ein erster Referentenentwurf für das 2. WiKG verfaßt. Aus dem Bereich der Computerkriminalität waren in diesem Entwurf schon Tatbestände wie der Computerbetrug (§ 263a) und die Fälschung gespeicherter Daten (§ 269) angedacht worden.[43] Nachdem man sich in den anderen Regelungsbereichen des Entwurfs nicht einigen konnte, wurde das Gesetz in der 8. Legislaturperiode nicht verabschiedet. Aufgrund von Neuwahlen konnte es dann auch nicht in der nächsten Legislaturperiode verabschiedet werden. Während der 10. Legislaturperiode haben die Regierung[44] und auch Abgeordnete der SPD[45] jeweils einen Entwurf zum 2. WiKG im Bundestag eingebracht. Eine dem § 202a ähnliche Vorschrift war jedoch in keinem der beiden Vorschläge enthalten.

Wichtigstes Ereignis für die Entstehung des § 202a war eine Sachverständigenanhörung vor dem Rechtsausschuß des Bundestages vom 06.06.1984. Hier wurde den Sachverständigen unter anderem die Frage gestellt, ob bei der Computerspionage oder sogar schon beim unbefugten Eindringen in Datenverarbeitungssyteme über bereits bestehende oder vorgeschlagene Strafvorschriften hinaus (wie §§ 303, 274 in der Fassung des Entwurfs zum 2. WiKG, 17 UWG, 106 UrhG, 41 BDSG) ein Bedürfnis bestehe, diese Handlungen strafrechtlich zu erfassen?[46] Zu dieser Frage taten sich vor allem die Sachverständigen *Sieber*[47] und *Oertel*[48] hervor.

---

42 *Ackermann*, Die aktuellen Tarife fürs Hacken, in: *Wiekmann*, Das Chaos-Computer-Buch, S. 183, bezeichnet § 202a als Anti-Hacker-Gesetz.

43 *Achenbach*, NJW 1986, 1835.

44 BT-Drs. 10/318.

45 BT-Drs. 10/119.

46 BT-Anhörung vom 06.06. 1984, Protokolle S. 26/XII.

47 Damals Professor an der Universität Tübingen, heute an der Universität Würzburg tätig.

48 Vertreter der Firma Siemens Nixdorf Computer, Paderborn.

So forderte *Oertel*[49], die strafrechtliche Erfassung der Datenerlangung nicht allein dem unvollkommenen UWG zu überlassen. Ebenso soll der Programmschutz erweitert werden, wie auch der Schutz von Datenbanken. Erreicht werden könne dies über die Bestrafung von Eindringlingen oder durch strafrechtliche Erfassung des Vorfeldes. Noch weiter geht dann der Vorschlag, das Herstellen und den Gebrauch von Geräten, die in der Lage sind, Sicherungen zu überwinden, unter Strafe zu stellen.[50]

Sieber[51] war der Ansicht, daß zum Schutz der zunehmend an Bedeutung gewinnenden Datenübertragungsnetze sichergestellt werden sollte, daß das unbefugte Anzapfen und Abhören dieser neuen Kommunikationsformen ebenso wie das Abhören von Telefongesprächen strafrechtlich erfaßt werden kann. Das Abhören von Datenübertragungsleitungen stelle einen der wichtigsten Ansatzpunkte der Computerspionage im Bereich datenfernverarbeitender Systeme dar. Es biete weit größere Möglichkeiten als das Abhören von Telefongesprächen, da digital übertragene Informationen mit Hilfe von Computern sehr viel leichter maschinell analysiert werden könnten, als das gesprochene Wort mit Hilfe von Spracherkennungsgeräten. Er zog das Fazit, daß die geltenden Gesetze diesen neuen technischen Möglichkeiten nicht gerecht würden und wollte neben dem unbefugten Anzapfen und Abhören von Datenübertragungssystemen den vorsätzlichen und unter Überwindung von Sicherungsmaßnahmen vorgenommenen unbefugten Zugriff auf fremde Datenverarbeitungs- und Datenspeicherungssysteme strafrechtlich erfassen. Diese Vorschläge von *Sieber* wurden dann fast wörtlich in § 202a übernommen.

Ein weiteres Argument für die Einführung einer derartigen Strafnorm wurde nicht in der Begründung des Rechtsausschusses zum 2. WiKG[52] aufgeführt und kam ebensowenig in der Anhörung zur Sprache. Die Quantität der möglicherweise abgehörten Daten oder digitalisierten Informationen ist wesentlich höher, als die einer sprachlichen Kommunikation per Telefon und stellt auch deswegen ein höheres Gefährdungspotential dar.

Die Lozierung der Norm erfolgte ebenso nach einem Vorschlag *Siebers* in der Position nach den §§ 201, 202.[53] Die Gesetzesbegründung erkennt einerseits einen engen Zusammenhang mit diesen Regelungen; andererseits wird betont, daß § 202a keine Verletzung des persönlichen Lebens- und Geheimbereichs voraussetze.[54] Diese Diskrepanz

---

49 *Oertel*, BT-Anhörung vom 06.06.1984, Protokolle S. 26/ 182 ff.

50 Nixdorf, BT-Anhörungvom 06.06.1984, Anlagen, S. 45.

51 *Sieber*, Informationstechnologie und Strafrechtsreform, S. 51 f. (Dies ist eine leicht überarbeitete Veröffentlichung des Gutachtens von *Sieber* zu besagter Anhörung).

52 BT-Drs. 10/5058, S. 28.

53 *Sieber*, Informationstechnologie und Strafrechtsreform, S. 54.

54 BT-Drs. 10/5058, S. 28.

zwischen dem ausdrücklichen Willen und der Überschrift des 15. Abschnitts wird bei der Bestimmung des Rechtsguts des § 202a relevant.

B. Das Rechtsgut

Der Begriff des Rechtsguts ist einer der am wenigsten geklärten Begriffe der Strafrechtslehre.[55] Zur Bestimmung des Rechtsguts des § 202a ist es zunächst erforderlich, den Begriff und die Funktion des Rechtsguts allgemein zu erörtern.

I. Bestimmung von strafrechtlichem Rechtsgüterschutz allgemein

Strafrecht dient dem Schutz des Rechtsfriedens. Es ist ultima ratio in dem Sinne, daß es besonders schwerwiegende Störungen des gesellschaftlichen Zusammenlebens ahndet, die nach allgemeiner Überzeugung Interessen betreffen, die als besonders wertvoll und schutzwürdig erachtet werden.[56] Diese Interessen werden als Rechtsgüter bezeichnet, wobei dem Strafrecht die Aufgabe zugeordnet wird, subsidiären Rechtsgüterschutz mit bestimmten Mitteln zu verfolgen.[57]

Die Frage nach dem Rechtsgut ist die Frage nach dem sog. materiellen Verbrechensbegriff.[58] Welches Verhalten ist strafwürdig? Was sind sachliche Kriterien für die Ermittlung strafbaren Verhaltens? Diese Fragen gehen der Kodifizierung von Strafnormen voraus. Sie begrenzen den Spielraum des Gesetzgebers und dienen der Kontrolle bestehender Strafgesetze. Folglich ist allgemein anerkannt, daß dem Rechtsgut und dessen Bestimmung bei allen damit zusammenhängenden Schwierigkeiten eine zentrale Bedeutung zukommt.[59] Schon *Armin Kaufmann* hat festgestellt, in der Strafrechtswissenschaft werde der Satz nicht ernsthaft bestritten, daß Rechtsgüterschutz Aufgabe des Strafrechts sei.[60]

---

55 *Gössel*, Das Rechtsgut als ungeschriebenes Tatbestandsmerkmal, in: *Herzberg* (Hrsg.), Festschrift für Dietrich Oehler zum 70. Geburtstag, S. 97 f.; SK-*Rudolphi*, Vor § 1 Rn. 3; *Suhr*, JA 1990, 303 (303).

56 *Maurach/Zipf*, AT 1, § 19 Rn. 4.

57 *Roxin*, AT 1, § 2 Rn. 1.

58 Eingehend dazu *Roxin*, AT 1, § 2 Rn. 1.

59 *Jakobs*, AT, 2. Abschn., Rn. 24; *Jescheck/Weigend*, AT, § 1 III 1.; Lackner/Kühl- *Kühl*, Vor § 13 Rn. 4; *Maurach/Zipf*, AT 1, § 19 Rn. 5, ablehnend nur noch *Amelung*, Rechtsgüterschutz und Schutz der Gesellschaft, S. 393; *Bockelmann/Volk*, AT, S. 11; vorzugswürdig ist die sog. dualistische Lehre vom Rechtsgut, die Rechtsgüter des Individuums, sowie auch der Rechtsgemeinschaft als Staat anerkennt.

60 *Kaufmann*, Die Aufgabe des Strafrechts, S.5; ebenso *Roxin*, AT 1, § 2 Rn. 1.

Es ist danach zu fragen, ob das Rechtsgut ermittelt werden muß, oder ob es gleichsam schöpferisch vom Gesetzgeber über Normsetzung geschaffen werden kann[61]. Damit das Rechtsgut seine oben beschriebene Begrenzungsfunktion für den Gesetzgeber erhält, ist *Jakobs* insofern zuzustimmen, daß nicht die Rechtsordnung das Interesse erzeugt, sondern das Leben, so daß der Rechtsschutz das Lebensinteresse zum Rechtsgut erhebt.[62] Somit ist der Gesetzgeber nicht völlig frei in der Normierung von Strafgesetzen, sondern muß jeweils von einem derartigen Interesse ausgehen bzw. dieses ermitteln. Der Rahmen, in dem aus sozialen Gegebenheiten strafrechtliche Schutzgüter werden können, ist die verfassungsrechtliche Ordnung. Es kann nur das strafrechtlich geschützt werden, was für die verfassungsmäßige Stellung und Freiheit des einzelnen Bürgers und für das im Rahmen der Verfassung bewegende Gesellschaftsleben notwendig ist.[63]

Der Rechtsgutsbegriff dient in der verfassungsrechtlichen und rechtspolitischen Diskussion der Beschränkung auf nicht nur moralisch anstößiges Verhalten. Nur sozialschädliches Verhalten ist strafrechtlich zu ahnden, indem nur die elementaren Lebensinteressen anderer (Individualrechtsgüter) oder der Gesellschaft (Allgemeingüter) anerkannt werden.[64] Der Mensch soll geschützt werden und damit seine freie Entfaltung, die sich in der Möglichkeit zeigt, ihm dienende Objekte zunutze zu machen. Diese Verknüpfung von personalem Element und dem durch in Beziehung zum Menschen tretendes Angriffsobjekt ist eine Funktionseinheit, die jedem Rechtsgut innewohnt.[65] Die Beziehung des Menschen zum Objekt soll geschützt werden. Insofern ist der Rechtsgutsbegriff vom Angriffsobjekt abstrahiert.[66]

Die Gesellschaft ist ständigem Wandel unterworfen. Besonderen Einfluß auf diese Veränderungen hat der technische Fortschritt, der für diese Arbeit von besonderer Relevanz ist. Die Rechtsgüter gehen diesen Technologien voraus, so daß zum Schutz gesellschaftlich wichtiger Neuerungen und dem Interesse der Menschen daran die in der Verfassung vorgegebenen Anknüpfungspunkte für die Rechtsgutsbestimmung maßgeblich sind. Danach gibt es einen sich aus der verfassungsmäßigen Ordnung ergebenden und

---

61 In diesem Sinne wird das Rechtsgut als „Abbreviatur des Zweckgedankens“ bezeichnet von *Grünhut*, Methodische Grundlagen der heutigen Strafrechtswissenschaft, in: Festgabe für Reinhard Frank zum 70. Geburtstag, Bd. I S. 1ff, 8 (sog. methodischer Rechtsgutsbegriff).

62 *Jakobs*, AT, 2. Abschn. R. 13; so auch *von Liszt*, Strafrecht, § 3 I 1.

63 SK-*Rudolphi*, Vor § 1 Rn. 5; so auch *Roxin*, AT 1, § 2 Rn. 9 ff.

64 Schönke/Schröder-*Lenckner*, Vorbem. § 13 Rn. 12.

65 *Otto*, Grundkurs Strafrecht, S. 9; SK-*Rudolphi*, Vor § 1 Rn. 8.

66 *Jescheck/Weigend*, AT, § 26 I. 2.; Schönke/Schröder-*Lenckner*, Vorbem. § 13 Rn. 12. Es wird von einer „Vergeistigung“ gesprochen.

damit aus deren Wandelbarkeit resultierenden akzessorisch dynamischen Rechtsgutskatalog. Der strafrechtliche Schutz technischer Neuerungen hat sich daran zu orientieren.

Neben der Beschränkung des Gesetzgebers aus dem hier vertretenen systemkritischen Ansatz des Rechtsgüterschutzes dient das Rechtsgut insbesondere der Auslegung von Strafrechtsnormen.[67] Des weiteren ergeben sich Anhaltspunkte zur Ermittlung des Rechsgutsträgers, so daß die Frage nach der Dispositionsbefugnis und der Antragsberechtigung beantwortet werden kann. Auch im Rahmen der Konkurrenzen ist das Rechtsgut von Interesse.[68]

II. Die in der Literatur vertretenen Meinungen

Die Bestimmung des Rechtsguts des § 202a ist umstritten und damit auch der von § 202a geschützte Personenkreis. Im Folgenden wird der Streitstand aufgezeigt und anschließend dazu Stellung genommen.

1. Vermögensschutz

Haft[69] stellt darauf ab, daß § 202a solche Daten[70] schützen will, die wie Forschungsdaten, Konstruktionsverfahren, Kalkulationen, Bilanzen, Kundenadressen, Computerprogramme[71] usw. einen wirtschaftlichen Wert haben. Er sieht eine gewisse Analogie zu § 248c, der Entziehung elektrischer Energie, und kommt daher zu dem Schluß, daß die Vorschrift des § 202a dem Diebstahl zuzuordnen sei. Er hält somit die Bezeichnung „Datendiebstahl“[72] für korrekter und bezeichnet die Überschrift „Ausspähen von Daten“ als irreführend. Der Begriff des Vermögens sei in diesem Zusammenhang jedoch weit zu fassen. Geschützt sind danach nur Daten mit Vermögenswert, wie z.B. Datenbanken

---

67 *Suhr*, JA 1990, 303.

68 Suhr, JA 1990, 303.

69 *Haft*, NStZ 1987, 6 (9). Ähnlich, jedoch sich nicht eindeutig festlegend *Bühler*, MDR 1987, 448 (452), ebenso Tröndle/Fischer-*Tröndle*, § 202a Rn. 2.

70 Zum Datenbegriff ausführlich Seite 52 ff.

71 Auch Programme sind Daten, BT-Drs. 5058, S.29; mehr dazu Seite 55 ff.

72 *Haft* hält den Begriff des Datendiebstahls für ungenau, da die Ursprungsdaten beim Kopieren ja erhalten blieben und schlägt dementsprechend den Begriff Informationsdiebstahl vor. Dies ist mit den gleichen Erwägungen ebenso ungenau, da die Information in gleicher Weise dem Berechtigten erhalten bleibt.

von Unternehmen oder Forschungsdaten. Private Daten und Dateien sind nach dieser Meinung dagegen nicht geeignete Angriffsobjekte des § 202a.

2. Schutz eines formellen Geheimhaltungsinteresses

Die h.M. stellt mit unterschiedlicher Nuancierung auf den Schutz eines formellen Geheimhaltungsinteresses ab.[73] Geschütztes Rechtsgut ist, so *Tröndle*, nicht nur der persönliche Bereich und Geheimbereich, sondern außerdem auch das (meist auch wirtschaftliche[74]) Interesse des Verfügungsberechtigten, die in Daten, Dateien oder Datenbanksystemen verkörperten Informationen vor unbefugtem Zugriff zu schützen.[75] Dieses Interesse wird durch die besondere Sicherung i.S.d. § 202a Abs. 1 dokumentiert.[76] Damit erhält nur der sorgsam Handelnde Strafrechtsschutz, was dem ultima-ratio-Prinzip des Strafrechts entspricht.[77] *Lenckner* sieht darin, wie auch in § 202, ein „viktimodogmatisches Element".[78]

Verfügungsberechtigter ist nach dieser Meinung derjenige, der als „Herr der Daten" aufgrund seines Rechts an ihrem gedanklichen Inhalt und damit unabhängig von den Eigentumsverhältnissen am Datenträger darüber bestimmen kann, wem diese zugänglich sein sollen.[79] *Samson* bezeichnet den Verfügungsberechtigten als den Besitzer der Daten.[80]

Kühl sieht auch den vom Dateninhalt Betroffenen als mitgeschützt an, wenn er ein Recht auf Wahrung der Vertraulichkeit gegenüber dem Berechtigten hat.[81]

---

73 *Frommel*, JuS 1987, 667 (668); *Granderath*, 2. WiKG, DB 1986 Beilage Nr. 18, S. 1; *Haß*, Der strafrechtliche Schutz von Computerprogrammen, in: Lehmann (Hrsg.), Rechtsschutz und Verwertung von Computerprogrammen, S. 481 Rn. 20; *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 43 f.; Lackner/Kühl-*Kühl*, § 202a Rn. 1; *Leicht*, iur 1987, 45; *Lenckner/Winkelbauer*, CR 1986, 483 (485); *Möhrenschlager*, wistra 1986,128 (140); *Schlüchter*, 2. WiKG, S. 48; *Schulze-Heiming*, Der strafrechtliche Schutz der Computerdaten, S. 40. Aus der Rspr. OLG Celle CR 1990, 277.

74 Hier wird die Intention des Gesetzgebers (BT-Drs. 10/5058, S. 28) deutlich, nämlich der Schutz wirtschaftlicher Werte in Form von Daten, welches von *Haft* als Rechtsgut gesehen wird.

75 Tröndle/Fischer-*Tröndle*, § 202a Rn. 2.

76 *Möhrenschlager*, wistra 1986, 128 (140).

77 *Leicht*, iur 1987, 45 (45). Zum ultima-ratio-Prinzip eingehend *Roxin*, AT 1, § 2 Rn 28 ff.

78 Schönke/Schröder-*Lenckner*, § 202a Rn. 1.

79 Schönke/Schröder-*Lenckner*, § 202a Rn. 1.

80 SK-*Samson*, § 202a Rn. 1. Dies ist in 2 Richtungen ungenau, da es erstens ein sachenrechtliches Besitzverhältnis über elektrische Zustände gibt, sondern nur in Bezug auf deren Träger, und zweitens der nichtberechtigte „Besitzer" ja gerade der Täter des § 202a ist.

81 Lackner/Kühl-*Kühl*, § 202a Rn. 1; ebenso *Schlüchter*, 2. WiKG, S. 61.

3. Schutz der Information

Als Rechtsgut des § 202a bezeichnet *Zielinski* die Information.[82] Dies wird ohne weitere Auseinandersetzung mit den anderen Ansichten vertreten.

4. Schutz einer umfassenden Geheimsphäre

Gössel[83] hält die h.M. für zu eng. Er beschreibt das Rechtsgut als die umfassende Privat- und Intimsphäre unter Einschluß aller die individuelle Persönlichkeit bestimmenden Umstände ohne Rücksicht auf deren konkreten Inhalt. Die geistige Dimension der geschützten Intimsphäre dürfe nicht auf den der alleinigen faktischen Verfügbarkeit der jeweils betroffenen Person unterliegenden ideellen Raum beschränkt werden. Daher diene § 202a dem Schutz der persönlichen Privat– und Intimsphäre oder einer Quasi-Geheimsphäre des Staates oder sonstiger Personengesamtheiten.

III. Stellungnahme

1. Haft

Die Ansicht von *Haft*, daß das Vermögen Rechtsgut des § 202a sei, ist abzulehnen. Es ist zwar als Versuch der Einschränkung des Schutzbereichs anerkennenswert, jedoch sind aus Wortlaut, Entstehungsgeschichte und Systematik keine zwingenden Anhaltspunkte zu finden. [84] Im Wortlaut der Norm ist zwar von Verschaffen als Tathandlung die Rede. Dies ist jedoch kein spezifisches Merkmal von Vermögensdelikten.[85] Auch fehlen Merkmale, die eindeutig für ein Vermögensdelikt sprechen, wie Bereicherungs- oder Zueignungsabsicht.

Die Gesetzesmaterialien enthalten ebenfalls nur Andeutungen, die auf den gestiegenen Wert von Daten und Datenbanken hinweisen.[86] Mit der Einführung des § 202a soll dem

---

82 *Zielinski*, Der strafrechtliche Schutz von Computersoftware, in: Kilian/Gorny (Hrsg.), Schutz von Computersoftware, S. 115, 118, 121.

83 *Gössel*, BT 1, § 37 Rn. 87.

84 Es verbietet sich eine teleologische Auslegung des Rechtsguts, da das Rechtsgut selbst die Basis der teleologischen Auslegung darstellt (Zirkelschluß).

85 Mit *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 38: Auch in § 96 -Landesverräterische Ausspähung- kommt dieses Merkmal vor.

86 BT-Drs. 10/5058, S. 28.

gestiegenen Wert von Informationen Rechnung getragen werden. *Oertel* forderte in der Sachverständigenanhörung, daß die Strafdrohung für Computerspionage wegen des beträchtlichen Schadens hoch sein müsse.[87] Diese Äußerungen können jedoch bestenfalls als Anlaß, nicht jedoch als Inhalt des Schutzes von Information in Form von Daten angesehen werden.

Der Gesetzgeber hat „wegen des engen Zusammenhangs mit den §§ 201, 202“[88] den § 202a bewußt in den 15. Abschnitt des StGB gestellt. Daß daneben jedoch ausdrücklich vermerkt ist, daß § 202a trotz seiner Stellung nicht die Verletzung des persönlichen Lebens- und Geheimbereichs voraussetzt, ist kein zwingendes Argument für die Ansicht von *Haft*. Die auch aus dieser Äußerung des Gesetzgebers folgende Zuordnung des § 202a zum Diebstahl geht fehl, da § 242 als Eigentumsdelikt auch Sachen schützt, die keinen wirtschaftlichen Wert und damit keinen speziellen Vermögenswert haben.[89] Eine mögliche Nähe zum § 242, was sich auch in der Anlehnung der besonderen Zugangssicherung an § 243 zeigt,[90] spricht dann in letzter Konsequenz für die h.M., die das Verfügungsrecht des Betroffenen im Vergleich zum Eigentum vor „Wegnahme“ der Information, die in Datenform vorliegt, geschützt sieht. *Haft* sieht zudem selbst, daß der Ausschluß des Antragsrechts für den Erben des Verfügungsberechtigten in § 205 Abs. 2 mit seiner Ansicht nicht zu vereinbaren ist.[91]

2. Zielinski

Die Information ist nicht das Rechtsgut des § 202a. Sie ist Essenz des Angriffsobjekts „Daten“ des § 202a, aber nicht dessen Rechtsgut. Ein spezifisches Interesse bzw. ein Herrschaftsverhältnis des Menschen an einem Objekt kann zum Rechtsgut erhoben werden, nicht jedoch das Objekt selbst.[92] Daher ist die Meinung *Zielinskis*[93] abzulehnen.

---

87 *Oertel*, Nixdorf AG, vgl. Protokoll Nr. 26, Anlagen, S. 34 ff.

88 BT-Drs. 10/5058, S. 28.

89 Vgl. *Haß*, Der strafrechtliche Schutz von Computerprogrammen, in: Lehmann (Hrsg.), Rechtsschutz und Verwertung von Computerprogrammen, S. 480 Rn. 20; Schönke/Schröder-*Eser*, § 242 Rn. 4.

90 Vgl. BT-Drs. 10/5058, S. 29.

91 *Haft*, NStZ 1987, 6 (10).

92 Vgl. *Jescheck/Weigend*, AT, § 26 I. 2.; Schönke/Schröder-*Lenckner*, Vorbem. § 13 Rn. 12.

93 *Zielinski*, Der strafrechtliche Schutz von Computersoftware, in: Kilian/Gorny (Hrsg.), Schutz von Computersoftware, S. 115, 118, 121.

3. Gössel

Auch die Ansicht *Gössels* kann nicht überzeugen. Der Schutz einer umfassenden Geheimsphäre, d.h. Privatsphäre in diesem Sinne, umfaßt denselben Bereich, den die h.M. mit dem Verfügungsrecht des Betroffenen an Daten beschreibt, die nicht in irgendeiner Weise z.B. als materielles Geheimnis qualifiziert sein müssen. Daher spricht die h.M. ja gerade von einem „formellen" Geheimhaltungsinteresse.[94] Letztlich liegt hier ein geradezu uferloser Begriff der sog. Privatsphäre vor. Der Privatsphäre sollte im Sinne verfassungsrechtlich gebotener Bestimmtheit diejenigen Daten zugeordnet werden, die persönliche Angaben über eine Person betreffen, wie Geburtsdatum, Adresse, Werdegang usw. So teilt *Hilgendorf* den Schutzbereich in Anlehnung an die h.M. in zwei Bereiche auf: Schutz der Privatsphäre und darüber hinaus Schutz solcher Daten, die nicht mehr dem Bereich der Privatsphäre zugehören, für den Verfügungsberechtigten aber dennoch einen ideellen, wirtschaftlichen oder wissenschaftlichen Wert haben.[95]

4. Herrschende Meinung

Der h.M., die das Verfügungsrecht des Berechtigten an Daten, bzw. ein formelles Geheimhaltungsinteresse als das Rechtsgut des § 202a ansieht, ist zu folgen. Schon der Gesetzgeber läßt diese Rechtsgutsbestimmung anklingen, wenn in den Materialien steht: „Das Strafrecht sollte erst dort eingreifen, wo ein Schaden, oder wenigstens eine Rechtsgutsbeeinträchtigung, wie z.B. die Verletzung des Verfügungsrechts über Informationen bei einer Tat nach § 202a, eingetreten ist."[96] Er schließt die Eingrenzung auf materielle Geheimnisse explizit aus, wenn postuliert wird, daß eine Straftat nach § 202a eine Verletzung des persönlichen Lebens- und Geheimbereichs nicht voraussetzt.[97] Der Wortlaut enthält hinsichtlich einer Einschränkung der geschützten Daten im Sinne eines bestimmten Inhalts der Daten keine Anhaltspunkte. Auch die systematische Auslegung stützt dieses Ergebnis, da dieselbe Schutzrichtung beim § 202 gegeben ist, der die aus dem Recht am gedanklichen Inhalt des Schriftstücks folgende Befugnis schützt, andere von der Kenntnisnahme auszuschließen.[98]

---

94 *Möhrenschlager*, wistra 1986, 128 (140).

95 *Hilgendorf*, JuS 1996, 509 (511).

96 BT-Drs. 10/5058, S. 28.

97 BT-Drs. 10/5058, S. 28.

98 Vgl. *Granderath*, 2. WiKG, DB 1986 Beilage Nr. 18, S. 1.

Problematisch erscheint jedoch, daß Daten als solche keine Körperlichkeit besitzen, so daß eindeutige Zuordnungsmaßstäbe fehlen, wie z.B. der Besitz oder die Eintragung eines Rechts in ein öffentliches Register. Die tatsächliche Sachherrschaft über eine Sache verdeutlicht die Zuordnung derselben zu einer bestimmten Person und kann zivilrechtlich einen Rechtsschein erzeugen, auf den sich Vermutungsregeln wie z.B. § 1006 BGB stützen. Eine solche eindeutige quasi-sachenrechtliche Zuordnung ist für Daten nicht normiert. Dies bereitet auch in der strafrechtlichen Normierung zum Schutze von Informationen in Datenform Probleme. Aus diesem Grund ist das geschützte Rechtsgut aufs engste mit dem Tatbestandsmerkmal der besonderen Zugangssicherung verbunden. Der Verfügungsberechtigte dokumentiert durch einen solchen Zugangsschutz seine Herrschaft über die Daten, wie der Besitzer einer Sache durch seine tatsächliche Nähe- und Sachherrschaftsbeziehung dazu, oft auch in der Form, daß er diese abschließt oder wegschließt und damit besonders sichert. Dies kommt auch in der Formulierung des Rechtsguts von *Jähnke* (mit h.M.) zum Ausdruck, wenn er das Rechtsgut als das Herrschaftsverhältnis an der Information bezeichnet.[99] Die besondere Zugangssicherung dient damit der Eingrenzung des Tatbestandes auf strafwürdiges Verhalten und konkretisiert erst das geschützte Verfügungsrecht an Daten.

[99] LK-*Jähnke*, § 202a Rn. 2.

IV. Verfügungsrecht[100]

Es ist an dieser Stelle zunächst zu klären, wer originär, d.h. direkt nach Herstellung von Daten das Recht daran besitzt. Dieses Geschehen ist mit Herstellung einer Sache aus herrenlosen Rohstoffen vergleichbar. Im Wege der Aneignung oder der Verarbeitung, §§ 958 Abs. 1, 950 Abs. 1 BGB, entsteht an dieser Sache erstmalig ein Eigentumsrecht.

Die Zuordnung des Rechts an Daten ist vor allem zur Ermittlung des Antragsberechtigten nach § 205 und beim Tatbestandsmerkmal der Nichtbestimmung der Daten für den Täter relevant. Hier stellt sich, wie auch bei § 303a, die Problematik, daß die Zuordnung von Daten nicht geregelt ist. Daten sind keine körperlichen Gegenstände, so daß auf sie das Sachenrecht nicht anwendbar ist. Durch die Auslegung des § 202a selbst läßt sich die Frage nach dem Verfügungsberechtigten nicht beantworten. *Tolksdorf*[101] spricht daher im Rahmen des § 303a von „fremden" Daten und davon, daß dieses Merkmal, hier negativ formuliert in dem Sinne, daß der Täter nicht verfügungsbefugt sein darf, zivilrechtsakzessorisch sei. Dies trifft bei § 202a ebenso zu.

1. Verfassungsrechtliche Bedenken

Es ist erstaunlich, daß § 303a von einigen Autoren aufgrund Verstoßes gegen das Bestimmtheitsgebot nach Art. 103 Abs. 2 GG für verfassungswidrig gehalten wird,[102] bei der Prüfung des § 202a dieses Problem jedoch nicht aufgeworfen wird. Der Verstoß gegen das Bestimmtheitsgebot wird damit begründet, daß es keine gesetzlichen Regelungen gibt, welche die Verfügungsbefugnis über Daten regeln. Strafrechtliche Tatbestandsmerkmale müssen jedoch so konkret umschrieben sein, daß die klare Abgrenzung des strafrechtlich Verbotenen vom Erlaubten für jedermann klar erkennbar ist.[103] Dem ist entgegenzuhalten, daß im Strafrecht auch schon andere Rechtsgüter anerkannt wurden, die keine zivilrechtliche Entsprechung haben. Als Beispiel läßt sich der Schutz des Gewahrsams einer Person über eine Sache anbringen. Auch hier gibt es keine exakte Entsprechung im Zivilrecht. Der Gewahrsamsbegriff ist ein rein strafrechtlicher. Mit Bildung von Zuordnungskriterien, Fallgruppen und gefestigter Rechtsprechung ist es

---

100 *Schlüchter*, 2.WiKG, S. 62 verwendet den Begriff Verfügungsbefugnis.

101 LK-*Tolksdorf*, § 303a Rn. 6.

102 SK-*Samson*, § 303a Rn. 7, 8; LK-*Tolksdorf*, § 303a Rn. 7.

103 Vgl. LK-Tolksdorf, § 303a Rn. 7; BVerfGE 29, 269 (285); BVerfGE 78, 374 (382); BVerfGE 80, 244 (256).

allgemeine Meinung, daß § 242 verfassungsgemäß ist. Das Strafrecht kann also auch bestimmte Interessen zu Rechtsgütern und die schutzwürdigen Interessenten zu Rechtsgutsträgern machen, wenn die Beziehung zum Objekt, hier die Daten, noch nicht zivilrechtlich geregelt ist. Insofern kann das Strafrecht auch eine Vorreiterrolle für etwaige zivilrechtliche Regelungen de lege ferenda spielen.

2. Verfügungsbefugnis über Daten in § 202a und § 303a

Es ist nun danach zu fragen, ob die Verfügungsbefugnis über Daten je nach Straftatbestand unterschiedlich oder für alle einheitlich zu behandeln ist. *Samson* beispielsweise spricht im Rahmen des § 202a dem Besitzer der Daten die Befugnis zu, im Rahmen des § 303a dem Eigentümer am Datenträger.[104] Ist die Verfügungsbefugnis nun je nach dem Schutzzweck der Norm zu entwickeln, oder ist analog zu den Eigentumsdelikten eine einheitliche Zuordnung vorzuziehen? Die h.M. zu den Rechtsgütern der §§ 202a, 303a knüpft an das formale Element des Schutzes von Daten an, unabhängig von Inhalt und Qualität des Inhalts. Jedes Datum ist durch § 303a vor Veränderung grs. geschützt, sowie bei § 202a bei besonderer Sicherung auch Daten mit banalsten Inhalten. Daher ist die Verfügungsbefugnis für alle Paragraphen, die an einen formalen Schutz von Daten anknüpfen, richtigerweise einheitlich zu bestimmen.[105]

3. Stimmen aus der Literatur

In der Literatur finden sich zumeist bei der Bearbeitung des Merkmals der „Datenbestimmung“ sehr kurz gehaltene Hinweise auf eine positive Bestimmung des Verfügungsberechtigten. So nennt *Lenckner* die „speichernde Stelle“ als i.d.R. verfügungsbefugt, u.U. jedoch auch ein Dritter unter Angabe eines konkreten Beispiels.[106] So ähnlich auch *Schmitz*, der denjenigen für verfügungsbefugt hält, der die Daten erstellt oder zur weiteren Verfügung erlangt hat.[107] In eine ganz andere Richtung geht *Samson*. Für ihn ist der „Besitzer“ der Daten der Verfügungsberechtigte.[108]

---

104 SK-*Samson*, § 202a Rn. 1.

105 So auch *Hilgendorf*, JuS 1996, 509 (512); *Meinhardt*, Überlegungen zur Interpretation von § 303a StGB, S. 110.

106 Schönke/Schröder-*Lenckner*, § 202a Rn. 6.

107 *Schmitz*, JA 1995, 478 (478).

108 SK-*Samson*, § 202a Rn. 1. Ein Besitz über Daten ist jedoch nicht denkbar im Gegensatz zu der Möglichkeit eines Besitzes an Datenträgern.

Ansonsten spricht die h.M. in Nachfolge von *Lenckner* vom Verfügungsberechtigten als dem „Herrn der Daten", im übertragenen Sinne als dem „Eigentümer" der Daten.[109] Das sei derjenige, der über die Daten verfügen darf, also die Rechtsmacht habe.[110] Dem ist jedoch entgegenzuhalten, daß es „Dateneigentum" im Sinne einer sachenrechtlichen Zuordnung nicht gibt, so daß diese Aussage nicht weiterhilft.[111] Den Verfügungsberechtigten damit zu definieren, daß er verfügungsberechtigt sein muß, ist ein tautologischer Schluß. Negative Abgrenzungen in der Weise, daß die Verfügungsbefugnis unabhängig von den Eigentumsverhältnissen am Datenträger zu bestimmen sei,[112] oder daß § 202a nicht dem Schutz von Geheimhaltungs- oder sonstigen Interessen dessen diene, über den die Daten etwas aussagen (der „Betroffene" i.S.d. BDSG)[113], sind hilfreiche Hinweise. Vom Zwang zu einer positiven Bestimmung der Verfügungsbefugnis befreien sie dennoch nicht.

4. Anknüpfungspunkte für die Datenzuordnung

Die Frage nach dem originären Verfügungsberechtigten ist folglich noch nicht endgültig geklärt.[114] Es sind daher positive Zuordnungskriterien für Daten zu entwickeln. Eingehende Untersuchungen diesbezüglich sind bei *Hilgendorf*[115] und *Welp*[116] im Rahmen der Prüfung des § 303a zu finden. Diese können jedoch auch für § 202a fruchtbar gemacht werden, da systematisch dasselbe Problem gegeben ist.[117] *Hilgendorf*[118] führt folgende Ansatzpunkte ins Feld: den Erwerb der Daten, das „Betroffensein" durch den Inhalt der Daten, das Eigentum am Datenträger, die geistige Urheberschaft am Dateninhalt oder das erstmalige Abspeichern der Daten.

---

109 *Lenckner/Winkelbauer*, CR 1986, 483 (485), Schönke/Schröder-*Lenckner*, § 202a Rn. 1. So auch *Leicht*, iur 1987, 45.

110 LK-*Jähnke*, § 202a Rn. 12.

111 *Welp*, iur 1988, 443 (446).

112 Schönke/Schröder-*Lenckner*, § 202a Rn. 1.

113 Schönke/Schröder-*Lenckner*, § 202a Rn. 1; *Schmitz*, JA 1995, 478.

114 So merkt *Hilgendorf* in JuS 1996, 509 (512) Fn. 50 zutreffend an, daß die Zuordnung der Verfügungsbefugnis über Daten zu den Problemen gehört, die der Gesetzgeber vor Erlaß des 2. WiKG nicht ausreichend geklärt hat.

115 *Hilgendorf*, JuS 1996, 890 (892 f.).

116 *Welp*, iur 1988, 443 (446 f.).

117 So auch *Hilgendorf*, JuS 1996, 509 (512) Fn. 50.

118 *Hilgendorf*, JuS 1996, 890 (892 f.).

a) Der Erwerb der Daten

Der Datenerwerb betrifft die Übertragung der originären Verfügungsbefugnis und demnach die derivative Herrschaft über Daten. Um eine solche bestimmen zu können, ist es notwendig zunächst ein Modell für die originäre Verfügungsbefugnis zu entwickeln.

b) Das „Betroffensein" durch den Dateninhalt

Das „Betroffensein" und damit die Tatsache, daß in den Daten über jemanden etwas ausgesagt wird oder Belange einer Person berührt sind, ist mit der h.M., wie oben schon angesprochen, kein taugliches Kriterium für die Datenzuordnung. Dies wird von *Kühl* bestritten. Er ist der Ansicht, daß der vom Dateninhalt Betroffene mitgeschützt sei, wenn er ein Recht auf Wahrung der Vertraulichkeit gegenüber dem Berechtigten habe.[119] Die h.M. setzt dem zutreffend entgegen, daß diese Interessenlage im nebenstrafrechtlichen § 43 BDSG abschließend geregelt sei.[120] § 202a dient der Datensicherung und nicht dem Datenschutz im engeren Sinne. Nähme man letzteres an, so würde der Schutz von Daten, die über niemanden etwas aussagen, in § 202a wegfallen. Der Gesetzgeber hatte aber gerade mit dem § 202a zum Ziel, Strafbarkeitslücken in Bezug auf § 43 BDSG, 17 UWG und § 106 UrhG zu schließen.[121] Bei einem Schutzgedanken für Daten aller Art kann daher die Qualifizierung des Inhalts, bzw. der Information keine Rolle spielen, genauso wie bei der Zuordnung von Sachen jeglicher Art als Eigentum.

c) Geistige Urheberschaft am Dateninhalt

Es besteht die Möglichkeit auf die geistige Urheberschaft am Dateninhalt abzustellen. Derjenige, der mittels Einsatzes seines Verstandes für den Inhalt der Daten, d.h. für die Information verantwortlich ist, wäre dann Verfügungsberechtigter. Dies ist beispielsweise einleuchtend, wenn jemand Daten auf dem Rechner ablegt, die eindeutig in der Sphäre des „Urhebers" liegen, wie z.B. bei wissenschaftlichen Arbeiten, Briefentwürfen o.ä., oder in dem Fall, daß eine Person einer anderen Daten diktiert, die diese in die DV-Anlage eingibt und abspeichert. Auch hier ist es plausibel, auf den „Urheber" als den Verfügungsberechtigten abzustellen. Probleme bereitet jedoch die Nähe dieser Zuordnung zum Urheberrecht und damit zum Urheberstrafrecht. Das Urheberrecht verlangt

---

119 Lackner/Kühl-*Kühl*, § 202a Rn. 1.

120 *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 43; *Schmitz*, JA 1995, 478.

121 BT-Drs. 10/5058, S. 28.

für die Anerkennung einer geistigen Schöpfung eine gewisse sog. „Werkhöhe“. Es wird geprüft, ob das Werk eine gewisse Individualität und Qualität besitzt. Bei Verneinung dieser Anforderungen entfällt der Schutz durch das Urheberrecht. Werden nun Daten dem „Urheber“ zugeordnet, würde dies den urheberrechtlichen Schutz von Informationen und Werken in Datenform uferlos ausweiten und damit das Urheberrecht aushöhlen. Die §§ 69a ff., 106 ff. UrhG sind als Normen des Nebenstrafrechts insoweit abschließend. Die Zuordnung nach dem Urheber des Dateninhalts ist daher abzulehnen.

d) Das Eigentum am Datenträger versus „Skripturakt“

Es bleiben als taugliche Zuordungsmaßstäbe das Eigentum am Datenträger und die Erzeugung der Daten durch Eingabe und Speicherung übrig. Fraglich ist, welches Kriterium vorzuziehen ist.

(1) Die Ansicht von Hilgendorf[122]

In der ersten Möglichkeit sind dem Eigentümer beispielsweise einer Festplatte alle Daten, die darauf abgelegt sind, diesem zugeordnet, unabhängig davon ob er sie selbst erstellt hat oder eine andere Person.[123] Für diese Ansicht spräche, so *Hilgendorf*, eine große Klarheit und Handhabbarkeit. Gleichzeitig kritisiert er jedoch, daß dies in vielen Fällen zu unhaltbaren Ergebnissen führe, so in dem Fall, daß eine Studentin eine Hausarbeit auf dem Rechner einer Freundin schreibt und damit die Daten der Freundin zuzurechnen wären. Weiterhin führt er an, daß gerade auf Großcomputern und in Netzen häufig Daten erstellt und bearbeitet würden, ohne daß der Bearbeiter Eigentümer der verwendeten Rechenanlage sei. Es würde dem Interesse des Datenverkehrs zuwiderlaufen, wenn den Bearbeitern der Schutz des § 303a (in diesem Zusammenhang kann auch § 202a angeführt werden) versagt würde. Bei Überspielen von Daten auf einen fremdem Datenträger verlöre der Hersteller der Daten konsequenterweise die Verfügungsberechtigung.

Insgesamt lehnt er dieses Kriterium damit ab und ordnet grs. demjenigen Daten zu, der sie als „Skribent“ mittels eines „Skripurakts“[124] erstellt hat. Skripturakt ist die Eingabe und Speicherung von Daten, wobei es im Zweifel auf die Speicherung ankommt. Auch dieser Ansatz sei, so *Hilgendorf*, vom Gesetzgeber nicht gegeben, er scheine aber der

---

122 *Hilgendorf*, JuS 1996, 890 (893).

123 So SK-*Samson*, § 303a Rn. 14.

124 Dieser anschauliche Begriff stammt von *Welp*, iur 1988, 443 (448).

einzige tragfähige Anknüpfungspunkt zu sein, um eine originäre Verfügungsbefugnis zuordnen zu können. Es bestehe auch dann eine Datenzuordnung via Skripturakt, wenn jemand vorsätzlich an einem fremden PC arbeite und dort seine Daten ablege. Der Eigentümer dürfe die ihm nicht zustehenden Daten also nicht einfach löschen (im Rahmen des § 202a: Ausspähen), sondern sei auf seine zivilrechtlichen Beseitigungs- und Unterlassungsansprüche angewiesen.[125]

(2) Die Ansicht von Welp[126]

Welp führt die Kriterien Skripturakt und Eigentum am Datenträger ein und setzt sie in ein Stufenverhältnis. Im Ergebnis gibt er jedoch der Zuordnung nach Eigentum am „Datenmedium", wie er den Datenträger bezeichnet, den Vorzug. Das Vollrecht am Eigentum schließe die Befugnis ein, mit dem Medium nach Belieben zu verfahren, sich also vor allem seiner Speicher- und Übermittlungsfunktion zu bedienen. Fielen die Vornahme des Skripturakts und das Innehaben des Medieneigentums auseinander, so werde, wenn der Eigentümer nicht damit einverstanden sei, das Medium unter Verletzung des Eigentums beansprucht. Jede weitere Verfügung über Daten seitens des Skribenten wäre ein weiterer Zugriff auf fremdes Eigentum, zu dessen Duldung der Inhaber nicht verpflichtet sei. Daher setzt sich nach Ansicht von *Welp* der Eigentümer am Datenträger gegenüber dem Skribenten durch. Bei Abschluß obligatorischer Verträge, z.B. der Eigentümer erklärt sich mit der Benutzung einverstanden, käme es darauf an, die Vereinbarung dahingehend auszulegen, wem die Verfügung über die Daten zustehen soll. Hier wird dann i.S. einer Vermutungsregel dem Skribenten den Vorzug gegeben. Der Skribent soll z.B. bei der Vermietung, Leasing, Verkauf unter Eigentumsvorbehalt, Gefälligkeit in der Regel verfügungsberechtigt sein, wenn die Speicherung oder Übermittlung in seinem Interesse erfolgt.

(3) Stellungnahme

Den Eigentümer des Datenträgers als den grs. Verfügungsberechtigten anzusehen, erscheint problematisch. In der Verbindung mit dem Kriterium des Skripurakts sind zwar plausible Ergebnisse zu erzielen, indem die speichernde Stelle in der Regel bei Vorliegen obligatorischer Beziehungen mit dem Eigentümer des Datenträgers als der dann derivativ Verfügungsberechtigte anzusehen ist. Genau in die entgegengesetzte Richtung geht jedoch die andere Ansicht. Hier ist die speichernde Stelle grs. originär verfügungs-

---

125 A.A. SK-*Samson*, § 303a Rn. 15.

126 *Welp*, iur 1988, 443 ff.

berechtigt. Die Bestimmung, ob ein anderer oder weitere verfügungsberechtigt sind, ist anschließend aus dem zwischen den Beteiligten herrschenden Rechtsverhältnis zu ermitteln.

Im Ergebnis unterscheiden sich evident nur die Ausgangspositionen, so daß bei jeweiliger Auslegung des Rechtsverhältnisses annähernd dieselben Ergebnisse erzielt werden. Nach dieser Feststellung ist es sinnvoll, das Kriterium für die Ermittlung des originär Verfügungsberechtigten zu wählen, welches für die Zukunft die wenigsten Probleme mit sich bringt, um damit Auslegungsschwierigkeiten vorzubeugen. Im Zuge der Vernetzung werden immer mehr Daten auf fremden Datenträgern abgespeichert. Die zentrale Verarbeitung von Daten ganz unterschiedlicher Herkunft auf Großrechnern und Computernetzen gewinnt immer größere Bedeutung. So bieten Internet-Provider auf ihren Servern[127] Kunden Speicherplatz zur Gestaltung einer Homepage an, die dann dort weltweit zum Abruf bereitliegt. Da der Gesetzgeber umfassenden Schutz von Daten anstrebt, ist daher in einer Zukunft, bei der das Eigentum am Träger der Daten mehr und mehr an Bedeutung verliert, das Kriterium des sog. Skripturakts vorzuziehen.

Besonders im Rahmen des § 202a erscheint es problematisch, den Eigentümer an Datenträgern als originär verfügungsbefugt zu qualifizieren. Damit wäre es für diesen straflos, sich mit einem Zugangsschutz versehene Daten zu verschaffen. Die Daten, die mit oder ohne Zustimmung auf einem fremden Träger liegen, wären damit gegenüber dem Eigentümer desselben schutzlos. Hiergegen spricht jedoch das Rechtsgut eines formellen Geheimhaltungsinteresses. Derjenige, der Daten speichert und mit einer Zugangssperre versieht, dokumentiert, daß diese Daten nicht ohne seine Zustimmung gelesen oder kopiert werden dürfen; er will ja gerade nicht, daß „seine“ Daten, die möglicherweise durch andere Personen oder wegen eines Anwendungsfehlers auf der DV-Anlage eines anderen gespeichert sind, von diesem gelesen werden. M.a.W.: Es macht gerade für § 202a keinen Sinn die Verfügungsberechtigung dem Eigentümer am Datenträger zuzurechnen, da die größte Gefahrenlage dann gegeben ist, wenn die Daten auch für andere zugänglich sind, wie in dem Fall, daß sie auf einem fremden Datenträger abgespeichert sind oder sie gerade durch fremde Leitungen übermittelt werden.

Sinn des § 202a ist der Schutz von Daten, die dem Zugriff fremder Personen ausgesetzt sind auch und gerade bei der Übermittlung von Daten. So erscheint es ebenfalls abwegig, in der Übermittlungsphase die Daten dem Eigentümer und Betreiber der Datenleitungen zuzurechnen. Der Schutz des § 202a würde ad absurdum geführt. Somit ist fest-

---

[127] Server, wörtl. „Meß“-Diener, ein Recher, der anderen Rechnern Dienstleistungen zur Verfügung stellt und von dem auch alle netztypischen Vorgänge gesteuert werden.

zustellen, daß gerade im Rahmen des § 202a das Eigentum am Datenträger kein taugliches Kriterium für die originäre Verfügungsbefugnis darstellt. Verfügungsbefugt ist daher unabhängig von den Eigentumsverhältnissen derjenige, der die Daten als erster abspeichert hat. Ob nun dieser oder ein anderer die Daten i.S.d. § 202a besonders gesichert hat, ist nicht von Belang. § 202a verlangt nur, daß eine solche objektiv vorliegt. Ein konsistenter Begriff der Verfügungsbefugnis über Daten, der derselbe bei § 202a wie bei § 303a ist, kann daher nur über das Kriterium des Skripturakts erreicht werden.

(4) Problematische Konstellationen

Bei Skripturakten, die auf Weisung erfolgen, ist die Verfügungsbefugnis dem Auftraggeber zuzurechnen. Nach *Hilgendorf* bedarf es für diese Konstellation der Modifikation des Kriteriums des Skripturakts.[128] Denkbar ist jedoch auch eine Auslegung des Rechtsverhältnisses zwischen dem Weisungsbefugten und dem Skribenten, die ohne Modifikation des hier vertretenen Zuordnungskriteriums auskommt. Wie oben schon angesprochen, ist die Verfügungsbefugnis über Daten zivilrechtsakzessorisch. Bei originärer Befugnis des Skribenten kann das Verhältnis zum Weisungsbefugten dahingehend ausgelegt werden, daß eine antizipierte Übertragung der Befugnis in der „juristischen Sekunde“ nach dem Speicherungsvorgang erfolgen soll. Der Weisungsbefugte hat daher eine derivative Verfügungsbefugnis.

Bei automatisierten Speicherungsvorgängen von möglicherweise vom Computer selbsttätig mittels Programm erstellten Daten, ist der Veranlasser dieses Vorgangs über diese Daten verfügungsbefugt. Er ist bei natürlicher Betrachtungsweise als Skribent der Daten anzusehen.

Gibt jemand Daten zur weiteren Bearbeitung oder zur Auswertung einer anderen Person weiter, so ist strittig, wer über diese bearbeiteten oder ausgewerteten neuen Daten verfügungsberechtigt sein soll.[129] Im Rahmen des § 202a braucht dies jedoch nicht entschieden zu werden, da i.d.R. für denjenigen, der die Daten erhalten hat, diese bestimmt sind i.S. des § 202a. Eine Strafbarkeit kommt für ihn daher nicht in Betracht.[130]

---

128 *Hilgendorf*, JuS 96, 890 (892) in Anlehnung an die Geistigkeitstheorie beim Urkundenstrafrecht.

129 Dies ist vor allem im Rahmen des § 303a von Belang; für Verfügungsbefugnis des Auftraggebers *Hilgendorf*, JuS 1996, 890 (893); des Auftragnehmers LK-*Tolksdorf*, § 303a Rn. 17 unter Berufung auf *Welp*, iur 1988, 443 (448) und *Meinhardt*, Überlegungen zur Interpretation von § 303a StGB, S. 124, 129.

130 Zur Datenbestimmung siehe Seite 65 ff.

5. Übertragung der Verfügungsbefugnis

Es stellt sich nun das Problem, ob und wie das durch Skripturakt entstandene Recht am Datum übertragen werden kann. Nach erstmaliger Abspeicherung von Daten kann die Datenverfügungsbefugnis darüber nur in derivativer, d.h. abgeleiteter Form erworben werden.

Die Datenverfügungsbefugnis ist, wie oben festgestellt wurde, Individualrechtsgut und damit disponibel. Somit könnte die Ausspähung oder Manipulation von überlassenen Daten über die **rechtfertigende Einwilligung** straflos sein. Dies wird jedoch dem Bedürfnis der freien Übertragbarkeit und Handelbarkeit von Daten nicht gerecht. Der Erwerber hat ein Interesse an einer umfassenden Herrschaftsstellung über die erworbenen Daten. Würde man eine Möglichkeit der Übertragung der Herrschaftsmacht der speichernden Stelle verneinen, so müßte jede Weitergabe der Daten und deren Benutzung von dieser genehmigt werden. Ansonsten wäre der „Erwerber" möglicherweise strafbar nach § 202a oder § 303a o.a.. Dies ist nicht im Sinne des Rechtsverkehrs.

Das Interesse an dem Erwerb z.B. eines Programms oder von Datenbanksätzen richtet sich in der Hauptsache auf die Daten. Der Datenträger ist nur als Transportmittel dieser Daten von untergeordnetem Interesse. So sind die Kaufsache eines Softwarevertrages in der Hauptsache die Daten, nicht der Datenträger.[131] Konsequenterweise kann daher, wie auch bei der Beurteilung der originären Datenverfügungsbefugnis, die Übertragung des Eigentums am Datenträger nicht akzessorisch die Wirkung eines Übergangs der Datenverfügungsbefugnis bedeuten. Die Übertragung der Datenverfügungsbefugnis ist daher als eigenständiger Übertragungsakt zu beurteilen.

Nun ist die rechtliche Behandlung des Übertragungsvorgangs von Daten zu erörtern. Problematisch ist, daß im Zivilrecht eine quasi-sachenrechtliche Zuordnung von Daten (bisher) nicht für notwendig erachtet wurde. Im Sinne der Rechtssicherheit gilt jedoch ein sog. numerus clausus für Verfügungsgeschäfte.[132] Es ist allgemeine Ansicht, daß als Verfügungsgeschäfte nur die im Gesetz Normierten in Frage kommen. Eine Verfügung über Daten ist damit zivilrechtlich nicht möglich.[133] So kann auch hier, wie beim origi-

---

131 *Engel*, BB 1985, 1159 (1162), *Meinhardt*, Überlegungen zur Interpretation von § 303a StGB, S. 132.

132 Palandt-*Heinrichs*, Überbl v § 104 BGB, Rn. 16.

133 Die Übertragung von Nutzungs- und Verwertungsrechten urheberrechtlich geschützter Daten, wie Computerprogramme kann nicht als Übertragung von Daten angesehen werden. Hier wird keine eigentümerähnliche Stellung übertragen, sondern übertragbare Rechte am Werk, der geistigen Schöpfung des Urhebers.

nären Verfügungsrecht, ein Verstoß gegen das strafrechtliche Bestimmtheitsgebot angedacht werden. Die strafrechtliche Begriffsbildung ist jedoch von Natur aus eigenständig, so daß bei der Auslegung von Strafgesetzen es allein auf deren Schutzfunktion, nicht aber darauf ankommt, welche Bedeutung das betreffende Tatbestandsmerkmal außerhalb des Strafrechts besitzt.[134] Es muß daher nach Feststellung des Bedürfnisses nach Übertragbarkeit für die genaue Qualifizierung des derivativen Rechtsgutsträgers ein strafrechtliches Modell für die Übertragung einer Datenverfügungsbefugnis entwickelt werden.[135] Im Sinne des Postulats der „Einheit der Rechtsordnung" ist jedoch darauf zu achten, daß das strafrechtliche Modell den zivilrechtlichen Prinzipien und Gegebenheiten nicht entgegenläuft.

Wird das im Strafrecht geschützte Recht an Daten übertragen, so ist im eigentlichen Sinne eine **Verfügung** gegeben. Verfügungen sind Rechtsgeschäfte, die unmittelbar darauf ausgerichtet sind, auf ein bestehendes Recht einzuwirken, es zu ändern, zu übertragen oder aufzuheben.[136] Im strafrechtlichen Schutz von Daten, wie er vor allem durch § 202a und § 303a gewährleistet wird, ist nach herrschender und vorzugswürdiger Ansicht das Recht an Daten absolut; es ist nicht Teil des Eigentums am Datenträger, oder etwa akzessorisch dazu. Soll es übertragen werden, so kann dies im strafrechtlichen Modell daher nur als Verfügung und damit als unmittelbare Rechtsübertragung angesehen werden. Dies wird besonders deutlich bei der tatsächlichen Übertragung von Daten über Datenfernübertragung. In diesem Fall wird eben gerade kein Datenträger mit Sachqualität übergeben, sondern nur die Daten selbst, so daß hier natürlicherweise eine Anknüpfung an die Eigentumsübertragung des Datenträgers erst recht nicht greift.

a) Einigung

Grundlegend für jede Übertragung eines Rechts oder einer Befugnis als Rechtsgeschäft sind in unserem freiheitlichen Rechtssystem zwei aufeinander bezogene Willenserklärungen. Diese müssen sich insofern entsprechen, als der Veräußerer der Befugnis seinen Willen zur Übertragung auf den Erwerber zum Ausdruck bringt und der Erwerber ebenfalls explizit oder konkludent seine Erwerbsbereitschaft zeigt. Die Regelungen in §§ 116 ff. BGB über die Willenserklärung sind hier maßgeblich. So kann nach *Hil-*

---

134 *Wessels/Beulke,*AT, Rn. 58.

135 Was nicht heißen soll, daß eine umfassende zivilrechtliche Regelung im Sinne eines Informationsrechts nicht wünschenswert wäre.

136 BGHZ 1, 304; 75, 226; BGHZ 101, 26; Palandt-*Heinrichs,* Überbl v § 104 BGB, Rn. 16.

gendorf[137] die Verfügungsbefugnis über Daten nach der Verkehrsanschauung durch entsprechende übereinstimmende Willenserklärungen übertragen werden. Dies geschehe tagtäglich etwa beim Verkauf von Software. Wer Daten erwerbe sei, sofern nichts anderes vereinbart werde, uneingeschränkt verfügungsberechtigt. Damit ist die Basis für die gewillkürte Übertragung von Rechten insgesamt gelegt, da unabhängig von der Art des Rechts immer eine Einigung erfolgen muß. So ist dies bei der Eigentumsübertragung von Sachen nach § 929 S. 1 BGB vonnöten, wie auch bei der Übertragung von Forderungen nach § 398 BGB, sowie der Übertragung anderer Rechte nach §§ 413, 398 BGB.

b) Übergabe der Daten

(1) Publizität (Offenkundigkeit)

Fraglich ist dennoch, ob zusätzlich zur Einigung auch ein sog. Publizitätsakt erforderlich ist und wenn, welche Gestalt eine solche Publizität haben müßte. Die Publizität ist eines der Prinzipien des Sachenrechts. Ihr kommen 3 Funktionen zu: (1) Übertragungswirkung, (2) Vermutungswirkung, (3) Gutglaubenswirkung.[138] Offenkundigkeit läßt sich bei beweglichen Sachen über den Besitz herstellen. Sachen sind sichtbar körperlich abgrenzbare Gegenstände, deren Zuordnung durch die tatsächlichen Gegebenheiten nach außen erkennbar wird. So kann vom Besitz über eine Sache -mit einer gewissen Wahrscheinlichkeit- auf das Eigentum und damit auch die Verfügungsbefugnis über diese Sache geschlossen werden.[139] Im Zusammenhang mit der Frage nach der Übertragung der Datenverfügungsbefugnis ist die Übertragungswirkung relevant. Publizität in der Funktion der Übertragungswirkung wird beispielsweise hergestellt durch das Erfordernis des absoluten Besitzverlustes des Veräußerers und der Inbesitznahme des Erwerbers bei der Eigentumsübertragung nach § 929 S. 1 BGB, oder durch die Eintragung in das Grundbuch bei Immobilien, § 873 Abs. 1 BGB.

Sollen nun Daten nur mit einem zusätzlichen Publizitätsakt übertragen werden können oder nicht? Dies ist die Frage nach der Anlehnung der Übertragung von Daten an §§ 413, 398 BGB und damit eine Annäherung an die Regelung für Rechte und Forderungsübertragung, die im Zivilrecht ohne Publizitätsakt auskommt (hier reicht die Eini-

---

137 *Hilgendorf*, JuS 1996, 890 (892).

138 *Bauer/Stürner*, Sachenrecht, § 4 Rn. 9.

139 *Bauer/Stürner*, Sachenrecht, § 4 Rn. 9.

gung aus), oder die Anlehnung an Übertragungsregelungen, die sich auf die Sachübertragung beziehen, welche einen Publizitätsakt fordern, wie § 929 S. 1 BGB.

Hier ist anzumerken, daß Publizität bei Übertragungsakten grs. wünschenswert ist, da sie der Rechtssicherheit dient. Jedoch ist zunächst ein praktikabler Anknüpfungspunkt für Publizität erforderlich und die Anforderungen müssen auch in der Gesamtregelung praktikabel sein.

(2) Anlehnung an §§ 413, 398 BGB

Eine Anlehnung an die Regelungen zur Übertragung von Forderungen nach § 398 BGB oder bei der Übertragung von anderen Rechten nach §§ 413, 398 BGB erscheint unzureichend. Rechte sind geistige Konstrukte ohne eigenes körperliches Wesen. Bei diesen ist eine Übertragung daher ohne tatsächlichen Akt möglich, da ein solcher auch gar nicht denkbar ist. Lediglich eine Mitteilung an den Schuldner einer Forderung[140] oder die Einführung eines Registers könnte Publizitätswirkung entfalten. Diese stellen jedoch zusätzliche Anforderungen dar, die mit der Forderung oder dem Recht als solches nichts zu tun haben. Daten dagegen sind keine geistigen Konstrukte, sondern sind Elemente der realen Welt. Werden Daten übertragen, so ist es ebenso wie bei der Übertragung von Sachen wünschenswert, daß der tatsächliche Übergang der Daten einen Teil des rechtlichen Übertragungsakts darstellt. Allein die Einigung zur Übertragung von Daten kann als solche noch nicht bewirken, daß der Erwerber diese schon innehat. Auch bei Daten ist wie bei Sachen ein in die rechtliche Behandlung eingebundener tatsächlicher Übertragungsakt von Vorteil. Eine Anlehnung an §§ 413, 398 BGB zur Datenübertragung und damit eine Annäherung von Daten an die Regelung für Rechte, die ohne Publizitätsakt auskommen, kann damit letztlich nur einen „Notanker“ darstellen.

(3) Anlehnung an § 929 S. 1BGB

(a) Besitz

Der Besitz von beweglichen Sachen ist ein natürlicher Befund. Er ist vor der Normierung erkannt und für die erwünschte Offenkundigkeit in praktikabler Weise instrumentalisiert worden. Ein Register, wie das Grundbuch für Immobilien, erhöht die Publizitätswirkungen, ist aber nur bei nicht-alltäglichen Rechtsgeschäften, wie die Veräußerung großer, zusammenhängender Vermögenswerte praktikabel, da ansonsten das Wirt-

---

140 Beispiel von *Bauer/Stürner*, Sachenrecht, § 4 Rn. 11.

schaftsleben gelähmt würde. Ein Register für Daten, die alltäglich und ohne oder gegen geringes Entgelt veräußert werden, kommt daher nicht in Betracht.

Es bleibt nun die Prüfung des Besitzes als Anknüpfungspunkt oder die Suche nach einem neuen Anknüpfungspunkt für Publizität bei der Übertragung von „Dateneigentum". Der Besitz nach § 854 ff. BGB ist als Innehaben der tatsächlichen Gewalt über Sachen bestimmt. Der zivilrechtliche Begriff des Besitzes bezieht sich folglich nur auf Sachen. Computerdaten[141] und Computerprogramme[142] sind nach richtiger h.A. jedoch keine Sachen i.S.d. § 90a BGB. Damit kann zivilrechtlich auch kein Besitz über Daten begründet werden, lediglich über den Datenträger.

Weiteres Problem in diesem Zusammenhang ist, daß Sachen eine erkennbare individuelle Existenz innehaben, welche für den Besitz als rechtliches Instrumentarium fruchtbar gemacht wird.[143] Im Gegensatz dazu werden Daten dadurch zum Verkehrsgut, indem sie aus sich selbst heraus kopiert werden. Zunächst kommt vor der Übertragung immer die Vervielfältigung als erster Schritt. Sie haben zwar als konkrete Daten eine individuelle Existenz. Diese ist jedoch kaum erkennbar, da lediglich der konkrete Standort der Speicherung im Datenträger Aufschluß geben könnte, welche Daten nun aus welchen reproduziert sind. Der Standort der Daten ist jedoch nur mit erheblichem technischen Aufwand erkennbar zu machen. Ebenso ungeklärt wäre dann noch der „Datenbesitz" im Datenfernübertragungszustand. In diesem Zustand ist noch nicht einmal ein ermittelbarer Standort von Daten gegeben.

(b) Tatsächliche umfassende Zugriffsmöglichkeit über konkrete Daten

Es erscheint trotz der vorigen Ausführungen ein Kriterium der tatsächlichen umfassenden Zugriffsmöglichkeit über konkrete Daten (im Sinne einer tatsächlichen Gewalt über Daten in Anlehnung an den Besitz) ein möglicher Anknüpfungspunkt für eine Publizität der Datenübertragung zu sein. Werden Daten derart übertragen, daß der Erwerber tatsächliche Gewalt über diese Daten hat, in dem Sinne, daß er auf diese Daten direkt zugreifen und sich diese anschauen und verändern kann, so spricht der Anschein dafür, daß er die Verfügungsbefugnis über diese Daten innehat. Diese tatsächliche Herrschaftsstellung ist zwar nicht so gut sichtbar, wie der Besitz einer Sache und das Her-

---

141 LG Konstanz, NJW 1996, 2662; Palandt-*Heinrichs*, § 90a BGB Rn. 2.

142 *Bormann/Bormann*, DB 1991, 2641 (2642 f.); *Redeker*, NJW 1992, 1739; *Junker*, NJW 1993, 824; Palandt-*Heinrichs*, § 90a BGB Rn. 2; a.A. *König*, NJW 1993, 3121 ff.

143 So bei dem sachenrechtlichen Prinzip der Spezialität, welches bedeutet, daß dingliche Rechte nur an bestimmten, einzelnen Sachen möglich sind, sich also auf sie beziehen müssen (*Bauer/Stürner*, Sachenrecht, § 4 Rn. 17).

ausgeben einer Sache vom Veräußerer an den Erwerber. Die Daten können jedoch sichtbar gemacht werden, was für denjenigen, der diese Daten abrufen kann, kein Problem darstellt. Anhand der Untersuchung der Einigung ist sodann ermittelbar, ob es sich um die Übergabedaten handelt.

Wird eine Anlehnung an die Übertragungsregelungen von Sacheigentum angestrebt, so muß dem Grundsatz der **Spezialität**[144] Rechnung getragen werden. Demzufolge muß eindeutig benennbar sein, welche Daten übertragen werden sollen. Damit ist als Grundvoraussetzung der Übertragung festzulegen, daß die Daten in Dateiform vorliegen; daß also zu übertragende Datenkonglomerate in einem zusammenfassenden Format und unter einer Namensbezeichnung gegeben sind, welche auf einem bestimmten Verzeichnis der Pfadstruktur des Betriebsystems abgespeichert sind. Eine Ausnahme kann davon gemacht werden, wenn die Daten einen eindeutig abgrenzbaren sinnhaften Inhalt haben, wie ein Name oder ein Paßwort.

(i) Überlassung von Daten auf einem Datenträger

Im Falle der Übergabe der Daten mit Hilfe eines Datenträgers oder der Speicherung von Daten über Datenfernübertragung (sog. downloaden) erfolgt die Einräumung der tatsächlichen Gewalt über die konkreten Daten nicht uno actu mit der Besitzüberlassung am Datenträger. Es muß die tatsächliche Gewalt in der Weise eingeräumt sein, daß der Erwerber der Daten vollen Zugriff darauf hat. Wird also der Besitz an einem Datenträger eingeräumt oder sind die Daten per Datenfernübertragung auf den Rechner des Erwerbers geschickt worden, dabei mit einem dem Erwerber nicht bekannten Zugriffsschutz versehen, so hat keine Übertragung der Verfügungsbefugnis stattgefunden.

(ii) Überlassung ohne Speicherung auf Datenträger im Besitz des Erwerbers

Das Kriterium der Einräumung des tatsächlichen uneingeschränkten Zugriffs auf Daten ist auch dann anzuwenden, wenn Daten übertragen werden sollen, ohne daß die Daten auf dem Datenträger des Erwerbers abgespeichert werden. Bietet beispielsweise ein Internet-Provider[145] einen sog. WEB-mail-Dienst an, so hat der Benutzer dieses Systems uneingeschränkten Zugriff auf die Daten, die ihm von anderen zugesandt wurden. Damit ist er, ohne daß sich die Daten auf einem in seinem Besitz stehenden Datenträger befinden, derivativ verfügungsbefugt über diese Daten.

---

144 Zum sachenrechtlichen Grundsatz der Spezialität siehe *Bauer/Stürner*, Sachenrecht, § 4 Rn. 17.

145 Ein Unternehmen, welches den Zugang zum Internet gegen Entgelt zur Verfügung stellt.

(c) Problemfall Ursprungsdaten

Besonderheit bei Daten ist jedoch, daß die Ursprungsdaten bei dem Veräußerer verbleiben, wenn diese nicht nach der Übertragung gelöscht werden, was wohl zumeist auch nicht geschieht. Es findet damit eine „Datenklonierung“ statt, so daß bei der Datenübertragung zumeist nicht von einem totalen „Besitzverlust“ an den Daten mit dem übertragenen Inhalt gesprochen werden kann. Die Einräumung einer tatsächlichen alleinigen Herrschaftsstellung über Daten auf Darstellungs- wie auch Inhaltsebene kann daher nur über zwei tatsächliche Akte erfolgen: Die Kopie der Daten (und Übertragung der tatsächlichen Gewalt über diese konkrete Daten), sowie der Löschung der „Mutterdaten“. Bei Sachen ist nur ein Akt erforderlich, da diese wie oben schon gesagt wurde, nicht duplizierbar sind.

Die beim Veräußerer womöglich verbliebenen, identischen Daten könnten manipuliert werden. Dies tangiert jedoch nicht die Interessen des Erwerbers der Kopie, da diese Daten ja nicht beeinträchtigt werden. Daß diese identischen Daten jedoch ausgespäht werden könnten, ist schon eher eine Gefahr, die auch den Erwerber der Datenkopie tangiert. Seine inhaltlich identischen Daten wären damit nicht mehr geheim und folglich ideell oder wirtschaftlich wertlos. Es ist somit zwischen den konkret zu übertragenden Daten und den tatsächlich nicht übertragenen Daten zu differenzieren. Die konkret übertragenen Daten unterstehen der Verfügungsbefugnis des Erwerbers. Die Ursprungsdaten verbleiben auf dem Datenträger des Veräußerers ohne Einräumung einer tatsächlichen Zugriffsmöglichkeit, so daß eine Übertragung dieser Daten nach dem obigen Modell nicht stattgefunden haben kann.

Auch bei dieser Problematik ist zunächst die Einigung maßgeblich. Sollen nur die konkreten Daten übertragen werden, so verbleibt die Verfügungsbefugnis über die Ursprungsdaten beim Veräußerer. Ist vereinbart, daß die Ursprungsdaten direkt nach oder während des Kopiervorgangs gelöscht werden sollen, so hat der Erwerber ein Interesse daran, auch über die Ursprungsdaten verfügungsbefugt zu sein. Denkbar ist auch eine Vereinbarung dahingehend, daß die Ursprungsdaten oder die konkreten Daten auf dem Datenträger des Veräußerers zwar beim Veräußerer bleiben sollen, der Erwerber jedoch die Verfügungsbefugnis erhält. Hier ist eine Situation gegeben ähnlich der in § 930 BGB, dem sog. Besitzkonstitut. Die Übergabe der Sache wird durch die zusätzliche Vereinbarung ersetzt, daß der Veräußerer für den Erwerber die Sache besitzt. Der Veräußerer fungiert als Besitzmittler. Der Erwerber ist mittelbarer Besitzer i.S.d. § 868 BGB.

Übertragen auf Daten als Verkehrsgut kann bezüglich der Ursprungsdaten oder solchen Daten, die weiterhin im Besitz des Veräußerers des Datenträgers verbleiben sollen, der Übergang der Verfügungsbefugnis dann angenommen werden, wenn vereinbart wurde, daß der Veräußerer mit den Daten im Sinne des Erwerbers verfährt. In Bezug auf Ursprungsdaten bedeutet dies im Falle eines Löschungsinteresses des Erwerbers, daß der Veräußerer im Rahmen der Vereinbarung im Sinne des Erwerbers mit den Daten verfährt und diese daher umgehend löscht. Ist ein Löschungsinteresse nicht gegeben, hat der Veräußerer die Daten im Sinne des Erwerbers zu verwalten. In beiden Fällen hat der Erwerber auch die Verfügungsbefugnis über die Ursprungsdaten. Ist keine solche Vereinbarung getroffen im Sinne des Erwerbers mit den Daten zu verfahren, verbleibt die Verfügungsbefugnis über die Ursprungsdaten beim Veräußerer.

c) Zusammenfassung

- Die Übertragung von Daten ist dann erfolgt, wenn eine Einigung zustande kommt, daß konkrete Daten, die genau bezeichnet sind (Dateiname, Standort in der Verzeichnisstruktur), übertragen werden sollen.
- Hinzu kommt ein tatsächliches Erfordernis, ein sog. Publizitätsakt: Die tatsächliche Einräumung einer umfassenden Zugriffsmöglichkeit auf die konkreten Daten ohne Rücksicht darauf, ob die Daten auf einem im Besitz des Erwerbers stehenden Datenträger gespeichert werden, oder diese sich auf einem Datenträger des Veräußerers oder eines Dritten befinden.
- Die Übertragung von Ursprungsdaten oder Daten, die ohne Vervielfältigung und ohne Einräumung einer umfassenden tatsächlichen Zugriffsmöglichkeit übertragen werden sollen, erfolgt durch eine publizitätsaktersetzende Vereinbarung, daß der Veräußerer im Sinne des Erwerbers mit den Daten zu verfahren hat.

6. Ende der Verfügungsbefugnis über Daten

Im Schrifttum erörtert allein *Hilgendorf*[146] das Problem der Beendigung der Datenverfügungsbefugnis.[147] Wie beim Sacheigentum kann das Interesse des Berechtigten an bestimmten Daten schwinden. Es kann eine derart lange Zeitspanne vergehen, in welcher der Betreffende nicht auf die Daten zugegriffen hat, so daß nicht mehr von „sei-

146 In *Hilgendorf*, JuS 1996, 890 (894) und JuS 1997, 323 (326).

147 In der Rechtsprechung ist diese Problematik noch nicht behandelt worden.

nen“ Daten gesprochen werden kann. Allgemein kann formuliert werden: In den Fällen, in der kein Interesse des dann einstmals Berechtigten an den Daten erkennbar ist, ist auch ein strafrechtlicher Schutz nicht mehr gerechtfertigt. Insofern ist ein strafrechtliches Modell bezüglich der Gründe zur Beendigung einer Datenverfügungsbefugnis für die Bestimmtheit der §§ 202a, 303a unerläßlich. Die Beendigung einer Datenverfügungsbefugnis mittels Übertragung wurde oben abgehandelt und wird daher nicht mehr aufgeführt.

Nach *Hilgendorf* ist eine Datenverfügungsbefugnis in folgenden Fallgruppen beendet (ohne Übertragung):

- Der Berechtigte verzichtet explizit auf sein Recht.[148]
- Der Berechtigte macht über einen längeren Zeitraum sein Recht nicht mehr geltend, obwohl er die Möglichkeit dazu hatte, und der potentielle Rechtsverletzer auf eine weitere Nichtgeltendmachung hoffen darf (Rechtsgedanke der Verwirkung).[149]
- Der Berechtigte hat kein schutzwürdiges Interesse mehr am Fortbestand der Verfügungsberechtigung.[150] Diese sind nach der Terminierung *Hilgendorfs* sog. **freie Daten**.

Die erste Variante ist als Anlehnung an die Dereliktion (Eigentumsaufgabe) gem. § 959 BGB zu erkennen. Eine Sache ist dann derelinquiert und damit herrenlos, wenn zum einen der zur Verfügung über das Eigentum Berechtigte den Willen hat dieses Eigentum aufzugeben, der sog. Verzichtswille[151] (Willensakt), zum anderen der unmittelbare Besitz an der Sache aufgegeben wird oder wurde (Realakt).[152]

Mindestanforderung für die wirksame Aufgabe eines Rechts am Datum stellt ein Willensakt dar: Die ausdrückliche oder konkludente Erklärung eines Verzichtswillens. Fraglich ist jedoch, ob auch bei Daten ein zusätzlicher Realakt zu fordern ist. In diesem Zusammenhang ist kein tatsächliches Moment ersichtlich, welches die Aufgabe des Rechts am Datum dokumentieren könnte. Daher reicht für den Rechtsverzicht am Datum die Äußerung des Verzichtswillens. Bei der „Datendereliktion“ ist zwischen Daten, die auf dem Datenträger des Verzichtenden gespeichert sind und solchen, die auf einem Datenträger eines Dritten abgelegt sind, zu unterscheiden.

---

148 *Hilgendorf*, JuS 1996, 890 (894).

149 *Hilgendorf*, JuS 1996, 890 (894).

150 *Hilgendorf*, JuS 1997, 323 (326).

151 Dies stellt eine einseitige, nicht empfangsbedürftige Willenserklärung dar.

152 *Bauer/Stürner*, Sachenrecht, § 53 Rn. 70.

Sind Daten auf dem im Eigentum des Berechtigten stehenden Datenträger gespeichert, so stellt sich die Frage, ob ein solcher Verzicht überhaupt wirksam sein soll. Grundsätzlich ist das Recht am Datum abstrakt zum Recht am Datenträger.[153] Es erscheint jedoch interessengerecht in diesem Fall das Recht auf Datenverzicht zu verneinen. Daten, die dem Eigentümer des Datenträgers zugeordnet sind, kann dieser ohne weiteres tatsächlich, wie auch rechtlich vom Datenträger entfernen und damit sich dieser entledigen. Im Sinne der Rechtsklarheit ist demnach davon auszugehen, daß dem Eigentümer des Datenträgers zugeordnete Daten nicht „derelinquiert" werden können.[154]

Bei Daten, die auf einem fremden Datenträger abgespeichert sind, ist eine Verzichtsmöglichkeit als sinnvoll zu erachten. Für eine Übertragung fehlt oft der Übertragungswille oder der Trägereigentümer ist nicht erreichbar oder bekannt. Wirkung dieses Verzichts ist jedoch nicht Herrenlosigkeit in Anlehnung an § 959 BGB, da eine solche für Daten abstrakt zum Recht am Datenträger nicht denkbar ist. Verzichtet der Datenberechtigte auf Daten, die auf einem Datenträger eines anderen gespeichert sind, so erwirbt dieser das Verfügungsrecht an diesen Daten. In diesem Fall muß sich das Recht am Datenträger durchsetzen, da ansonsten die Gefahr bestünde, daß Dritte über einen Aneignungsakt die Verfügungsbefugnis auf diese Daten erwerben könnten. Hier hat jedoch das Recht am Datenträger Vorrang, da er ein vorrangiges Interesse daran hat, diese Daten beispielsweise löschen zu können, ohne sich nach § 303a strafbar zu machen.

Die zweite Variante ist eine Anlehnung an die aus § 242 BGB entwickelte Verwirkung.[155] Die Verwirkung stellt jedoch im Zivilrecht eine am Zeitablauf orientierte Rechtsausübungsschranke dar. Sie macht daher nur die Rechtsausübung unzulässig und beseitigt nicht jedoch das Recht selbst.[156] Hier geht es jedoch um eine Beendigung des Verfügungsrechts an Daten, nicht um eine Rechtsausübungsschranke. Die Voraussetzungen der Verwirkung sind daher für das Strafrecht übertragbar, nicht jedoch deren Rechtsfolge. Rechtsfolge dieser „Datenverwirkung" ist damit das Ende des Verfügungsrechts. Auch hier setzt sich, wie in der ersten Variante, das Recht am Datenträger durch. Der Eigentümer des Datenträgers wird verfügungsbefugt über die Daten, an denen das Verfügungsrecht verwirkt wurde.

---

153 *Hilgendorf*, JuS 1996, 890 (893).

154 Ansonsten müßte der Staatsanwalt beweisen, daß Daten, die eindeutig dem Trägereigentümer zugeordnet sind (z.B. aufgrund Skripurakts) nicht von diesem „derelinquiert" wurden.

155 Vgl. *Larenz/Wolf*, Allgemeiner Teil des Bürgerlichen Rechts, § 16 Rn. 46 und 57 ff.

156 *Larenz/Wolf*, Allgemeiner Teil des Bürgerlichen Rechts, § 16 Rn. 63.

Die dritte Variante kann als Auffangtatbestand bezeichnet werden. Daten, die auf einem nicht im Eigentum des Datenverfügungsberechtigten stehenden Datenträger gespeichert sind, können nicht denselben Schutz genießen wie Sachen. Daten können ohne Träger nicht existieren, so daß auch die Interessen des Datenträgereigentümers beachtet werden müssen. In dem Spannungsfeld Recht am Datum und Recht am Träger kann folglich der umfassende Eigentumsschutz an Sachen nicht auf das Datenverfügungsrecht übertragen werden. Es ist z.B. für eine Universitätsverwaltung unzumutbar, zehn Jahre warten zu müssen, wie es beispielsweise die Ersitzung von Sachen gem. §§ 937 ff. BGB vorsieht, bis sie dann mit den auf dem Universitätsnetz abgelegten Daten, an denen der Skribent kein Interesse mehr hat oder diese schlichtweg vergessen hat, straflos nach Belieben verfahren kann.[157]

Der Unterschied der dritten Variante zur Datenverwirkung ist, daß sich das Recht am Datenträger auch dann durchsetzen kann, wenn der ursprünglich Verfügungsberechtigte sein Recht tatsächlich nicht mehr durchsetzen kann, weil er von der Existenz oder dem Standort der Daten keine Kenntnis (mehr) hat. Wann ein schutzwürdiges Interesse nicht mehr vorliegt, ist im Einzelfall zu entscheiden. Anhaltspunkte sind das Rechtsverhältnis zwischen dem Datenberechtigten und dem Trägereigentümer, die Zeitspanne, die seit dem letzten Zugriff des Berechtigten vergangen ist und die (Nicht)-Ermittelbarkeit des Berechtigten.

[157] In den meisten Fällen wird sie die Daten löschen.

C. Der objektive Tatbestand

I. Daten i.S.d. § 202a Abs. 2

Das Tatobjekt des § 202a sind Daten i.S.d. § 202a Abs. 2. Daten i.S.d. § 202a sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert oder übermittelt werden. Der Begriff der Daten wurde damit nicht definiert, sondern im Gegenteil vom Gesetzgeber bewußt offengelassen.[158] § 202a Abs. 2 schränkt den Begriff lediglich auf nicht unmittelbar wahrnehmbare Daten ein.[159] Unmittelbar wahrnehmbare Daten sind nach Ansicht des Gesetzgebers u.a. durch die §§ 201, 202 ausreichend geschützt.[160] Auf diesen eingeschränkten Datenbegriff des § 202a Abs. 2 nehmen die §§ 274 Abs. 1 Nr. 2, 303a und 303b Abs. 1 Nr. 1 Bezug. Der Rechtsausschuß hat sich wohl der Äußerung *Hafts* angeschlossen, daß der Begriff der Daten ein computertechnologischer sei,[161] wenn er darauf hinweist, daß der Datenbegriff offen für neue Technologien sein müsse. Im Folgenden wird das Wesen der Daten und damit der maßgebliche Datenbegriff bestimmt. Der Begriff der „Daten" wird vor allem im Bereich der Computertechnik verwendet. Es kann daher zur näheren Bestimmung zunächst auf die Begriffsdefinitionen aus diesem Bereich eingegangen werden. Danach sind sie auf ihre Übertragbarkeit für das Strafrecht zu untersuchen.

Besonders im Zusammenhang mit § 268 Abs. 2 (Fälschung technischer Aufzeichnungen) wurde auf die Datendefinition der alten DIN 44300 Nr. 19 hingewiesen.[162] Sie lautet: Daten sind durch Zeichen oder kontinuierliche Funktionen aufgrund bekannter oder unterstellter Abmachungen **zum Zwecke** der Verarbeitung dargestellte Informationen, die einer weiteren Verarbeitung in einer Datenverarbeitungsanlage unterliegen. Nach *Jessen* ist diese Definition für § 202a untauglich, da es keine Anhaltspunkte gäbe, daß nur Daten geschützt seien, die einer weiteren Verarbeitung unterlägen.[163] Dem ist zuzustimmen. Es kann nicht auf eine weitere Verarbeitung ankommen, da gerade auch

---

158 BT-Drs. 10/5058, S. 29.

159 So auch LK-*Jähnke*, § 202a Rn. 3; Schönke/Schröder-*Lenckner*, § 202a Rn. 2; *Hilgendorf*, JuS 1996, 509 (511); *Lenckner/ Winkelbauer*, CR 1986, 483 (484); *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 45.

160 BT-Drs. 10/5058, S. 29.

161 *Haft*, BT-Anhörung vom 6.6.1984, Anlagen, S. 208.

162 LK-*Tröndle* (9. Auflg.), § 268 Nr. 13; Schönke/Schröder-*Cramer*, (22. Auflg.), § 268 Rn. 11.

163 *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 47.

die möglicherweise nur zum Ausdruck vorbereiteten Ergebnisse einer Datenverarbeitung für potentielle Täter von Interesse sind.

Einen Schritt in die auch für § 202a richtige Richtung geht die neue DIN 44300 Teil 2-2:1.13, die sich an die Definition der Internationalen Standard Organisation (ISO)[164] anlehnt. Sie bezeichnet Daten als „Gebilde aus Zeichen oder kontinuierlichen Funktionen, die aufgrund bekannter oder unterstellter Abmachung und **vorrangig** zum Zwecke der Verarbeitung Informationen darstellen. Hier ist in der Entwicklung der DIN-Normen erkennbar, daß mehr und mehr auf den Zweck der weiteren Datenverarbeitung verzichtet wird. *Jessen*[165] verkennt hier, daß diese Formulierung auch Raum gibt, Daten zu erfassen, die keiner weiteren Datenverarbeitung mehr unterliegen.

Mit Blick auf die Schutzrichtung des § 202a auf ein formalisiertes Geheimhaltungsinteresse kann nur ein weiter Datenbegriff angenommen werden. Eine Einschränkung durch das Kriterium eines gewissen Verarbeitungsgrads ist untauglich.[166] Mit der Ablehnung einer derartigen Einschränkung bleibt man dennoch die Definition des Begriffs selbst schuldig. Letztlich verbleibt als Anknüpfungspunkt der in allen DIN-Normen auftauchende Begriff der **Information**. Die DIN-Normen sind auch insoweit hilfreich, als sie deutlich machen, daß der Datenbegriff zwei Ebenen enthält,[167] zum einen die Bedeutung, d.h. den Inhalt des Datums: die Information (semantische Ebene), zum anderen die Darstellung der Information (syntaktische Ebene).

Der Inhalt des Datums ist die Information (semantische Ebene). Der Begriff der Information kann definiert werden als jede beliebige Angabe über einen Gegenstand oder Zustand in der realen oder irrealen Welt.[168] Der Satz: **Information ist alles**, läßt sich hier in etwas anderer Bedeutung durchaus anbringen. Alles, was ein Lebewesen mit seiner Sinnesausstattung wahrnimmt, ist Information, so auch Ergebnisse eines automatisierten Datenverarbeitungsvorgangs. Der Begriff der Information ist somit grenzenlos.

---

164 Aus *Möhrenschlager*, wistra 1986, 128 (132) Fn. 39 und 43: Definition der ISO, 2381/1, Data processing- Vocabulary – Part 01: Fundamental terms, 2. Auflg. 1984, 01.04.01: „A sequence of instructions suitable for processing".

165 *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 47.

166 So auch Schönke/Schröder-*Lenckner*, § 202a Rn. 3; *Haurand/Vahle*, RDV 1990, 128 (132); LK-*Jähnke*, § 202a Rn. 3; SK-*Samson*, § 202 Rn. 3; *Schlüchter*, 2. WiKG, S. 60; *Lenckner/Winkelbauer*, CR 1986, 483 (484).

167 So als erster *Welp*, iur 1988, 433 (444); ihm nachfolgend *Schmitz*, JA 1995, 478 (479).

168 Nach *Schmitz*, JA 1995, 478 (479); vgl. auch *Welp*, iur 1988, 433 (444): Information ist „die Kenntnisbeziehung zu jedem realen oder irrealen Gegenstand der Welt".

Die semantische Ebene hilft aufgrund der Uferlosigkeit des Informationsbegriffs für die Bestimmung des Tatbestandsmerkmals Daten nicht weiter.

Die syntaktische Ebene bezieht sich auf die Darstellung einer Information. Eine Information kann dargestellt werden durch die Übereinkunft eines bestimmten „codes". So kann Information über Sprache transportiert werden. Vorher verabredete Einzelbausteine werden zusammengesetzt. Diese Zusammensetzungen symbolisieren Vorgänge und Zustände. So können als Beispiele für solche Konventionen der Binärcode der modernen Datenverarbeitung, das Schriftalphabet, oder Sprachregeln angeführt werden.[169] Die Darstellungsmöglichkeiten von Information sind ebenso wie die Information selbst unbegrenzt.

Es ist festzustellen, daß auch über diesen Weg keine Eingrenzung des Datenbegriffs erfolgt. Der Begriff der Daten wird daher im Sinne eines weiten Datenbegriffs wie folgt definiert: Ein Datum ist die in ihm verkörperte Information[170], oder: Daten sind durch Zeichen codierte Informationen[171], oder einfach: Das Datum als Darstellung einer Information[172]. Letztlich wird der Begriff des Datums mit dem der Information gleichgestellt.[173] Die Information existiert, wie oben angemerkt, ohne das Vorhandensein eines Trägers, eines Mediums (syntaktische Ebene) als solche nicht. Es kann daher bei der Definition des Datenbegriffs auf das Merkmal „Darstellung" verzichtet werden; dies ist in dem Begriff der „Information" enthalten.

Zusammenfassend kann somit definiert werden: Ein Datum ist eine Information. Bejaht man diese Begriffsbestimmung, so wird auf der nächsten Stufe deutlich, daß diese aufgrund ihrer uferlosen Weite für das Strafrecht nicht handhabbar ist. Die Begrenzung kann jedoch über die weiteren Merkmale des § 202a Abs. 2 vorgenommen werden. Es sind nur solche **Informationen** durch § 202a geschützt, die sich im Zustand der Speicherung oder Übermittlung befinden und nicht unmittelbar wahrnehmbar sind. Erst diese Merkmale machen § 202a dann zu einem „Computerstraftatbestand".

Eine andere Ansicht hält jedoch für die Begriffsbestimmung der Daten im Rahmen des § 202a einen funktionalen Zusammenhang der Informationen mit dem Betrieb einer

---

169 Beispiele aus *Schmitz*, JA 1995, 478 (479).

170 *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 50. Hier handelt es sich jedoch um eine problematische Definition, da das Datum als durch das Datum selbst verkörperte Information erachtet wird.

171 *Schulze-Heiming*, Der strafrechtliche Schutz der Computerdaten, S. 26; *Welp*, iur 1988, 434 (444); *Kuhn*, Rechtshandlungen mittels EDV und Telekommunikation, S. 7.

172 *Schmitz*, JA 1995, 478 (479).

173 So auch *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 50.

Datenverarbeitungsanlage für unerläßlich.[174] Letztlich kommen jedoch beide Ansichten zu demselben Ergebnis. Die eine Meinung erhält den funktionalen Zusammenhang und damit Eingrenzung des Datenbegriffs über die datenverarbeitungsspezifischen Merkmale der Speicherung und Übermittlung des § 202a Abs. 2. Die andere erzielt dasselbe Ergebnis über die direkte Einbeziehung des funktionalen Zusammenhangs in den Datenbegriff. Für diese Ansicht können die Merkmale der Speicherung und Übermittlung des § 202a Abs. 2 nur deklaratorischen Charakter haben.

1. Computerprogramme als Daten

Es ist in der Literatur umstritten, ob Computerprogramme unter den Rechtsbegriff der Daten fallen. So wird von der Meinung, die Programme nicht unter den Datenbegriff fassen will, argumentiert, daß in § 263a zwischen den Begriffen Daten und Programme unterschieden wird. Es verstoße daher gegen das Analogieverbot, wenn nun in § 202a der Datenbegriff auch auf Programme angewendet würde.[175] Diese Ansicht kritisiert die Subsumierung von Programmen unter § 202a gerade im Hinblick darauf, daß einfachste Miniprogramme ohne jegliche urheberrechtliche Werksqualität dann unter den Schutz des § 202a fallen würden, wenn sie nur einen Kopierschutz (Zugriffssicherung)[176] hätten. Komplexere Programme ohne Zugriffssicherung und ohne Entsprechung der extrem hohen Anforderungen urheberrechtlicher Art der „Inkassoprogramm-Entscheidung“[177] könnten jedoch straflos kopiert werden.[178]

Die h.M.[179] hat den Gesetzgeber auf ihrer Seite, der ausdrücklich Programme als Daten ansieht[180] und sogar in der Begründung zu § 263a darauf hinweist, daß Programme eine besondere Art von Daten seien.[181] Programme bestehen aus einem Aneinanderfügen einzelner Daten, und die Zusammenfügung mehrerer Daten ändert am Datencharakter des Gesamtausdrucks nichts.[182] Auch der Einwand des Aushebelns der nebenstrafrecht-

---

174 LK-*Jähnke*, § 202a Rn. 3; auch *Haft*, NStZ 1987, 6 (8) und *Hilgendorf*, JuS 1996, 509 (511) fordern die Fixierung auf einen Datenträger.

175 *Von Gravenreuth*, NStZ 1989, 201 (204, 206).

176 Ob Kopiersicherungen überhaupt Zugriffssicherungen darstellen, ist ebenfalls umstritten.

177 BGH, CR 1985, 22 ff.

178 *Von Gravenreuth*, NStZ 1989, 201 (204).

179 Vgl. nur *Hilgendorf*, JuS 1996, 509 (511); Tröndle/Fischer-*Tröndle*, § 202a Rn. 6; Schönke/Schröder-*Lenckner*, § 202a Rn. 3; LK-*Jähnke*, § 202a Rn. 3 (jeweils m.w.N.).

180 BT-Drs. 10/5058, S. 29.

181 BT-Drs. 10/5058, S. 30.

182 *Hilgendorf*, JuS 1996, 509 (511).

lichen Urheberrechtsvorschriften greift nicht. § 202 schützt ein Verfügungsrecht an Daten und nicht eine schöpferische Leistung und hat insofern eine andere, nicht urheberrechtliche Schutzrichtung. Die Befürchtung einer Schutzdiskrepanz zwischen zugriffsgesicherten Miniprogrammen und nicht zugriffsgesicherten komplexeren Programmen kann aus zwei Gründen als unbegründet erachtet werden. Zum einen ist es dem Skribenden des komplexeren Programmes unbenommen auch dieses mit einem Zugriffsschutz zu versehen, zum anderen ist der urheberrechtliche Schutz von Computerprogrammen durch die Neufassung des § 2 Abs. 1 Nr. 1 UrhG und Einführung der §§ 69a – 69g UrhG[183] enorm ausgeweitet worden. Programme fallen daher mit der h.M. unter den Datenbegriff.

2. Datum/Daten

Der § 202a und alle Paragraphen, die den Begriff der Daten aufweisen (z.B. § 268 Abs. 2; auch das BDSG) verwenden die Pluralform. Es stellt sich nun die Frage, ob auch das einzelne Datum Tatobjekt dieser Straftatbestände sein kann.

Problematisch ist zunächst, ob ein Datum als solches überhaupt vorkommen kann. *Jessen* bringt als Beispiel für den Bereich der Computertechnik den auf einem Computer erzeugten Buchstaben „a“, der ein einzelnes Datum darstelle.[184] In einem Computersystem, welcher nur den Binärcode verstehen kann, wird dieser Buchstabe jedoch durch den Binärcode „01100001“ dargestellt. Jede einzelne „0“ oder „1“ ist aber wiederum eine Information kleinerer Einheit und damit ein Datum. Im Rahmen der Computertechnik stellt damit das Bit (0 oder 1; Strom fließt oder Strom fließt nicht) das denkbare einzelne Datum dar. Umformungen von systematischen Aneinanderreihungen (Standard ASCII-Format) von Bits in Schriftsprache (Alphabet) und Sonderzeichen sind daher Datumsmehrheiten und damit schon Daten. Das einzelne Bit als Angiffsobjekt krimineller Handlungen erscheint nicht denkbar, so daß zumindest bei Daten, die durch Binärcode dargestellt werden, die Auseinandersetzung mit der Frage, ob auch das Datum Tatobjekt des § 202a sein kann, wohl rein akademischer Natur ist.

In anderen Bereichen erscheint das Eruieren eines Datums kaum möglich. So ist der geschriebene Buchstabe auf einem Blatt Papier eine Information. Dieser Buchstabe besteht aus einem vom Papier andersfarbigen Material, welches aus Atomen und noch

---

183 Neufassung des § 2 Abs. 1 Nr. 1 UrhG und Einführung der § 69a – 69g (Achter Abschnitt: Besondere Bestimmungen für Computerprogramme) durch Gesetz vom 9.6.1993 (BGBl. I S. 910).

184 *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 49.

kleineren Teilchen besteht. Der Buchstabe ist somit aus den denkbar kleinsten Materialeinheiten der Tinte o.ä. zusammengesetzt, welche selbst wieder u.U. als Information zu qualifizieren sind und kann daher als solches als Datenmehrheit bezeichnet werden. Auch hier erübrigt sich bei dieser Betrachtungsweise die Einbeziehung das Datums in § 202a.

Die nähere Betrachtung dieses Problems führt dazu, daß einige Autoren zu Recht feststellen, daß die Aussage, wann ein Datum oder Daten vorliegen, nicht eindeutig gemacht werden kann.[185] *Schulze-Heiming*[186] schlägt daher die Übertragung der Abgrenzung aus dem BDSG vor. Im Datenschutz sei ein Datum die kleinste, vernünftigerweise für sich zu behandelnde, insbesondere für Entscheidungen zu verwertende Information. So sei z.B. der Name, die Anschrift oder das Geburts**datum** ein einzelnes Datum, welches informationstechnisch Daten bzw. ein Datenfeld wären. Der Gesetzgeber selbst habe auf das BDSG verwiesen, so sei im Ergebnis unter Datum die semantische Sinneseinheit (d.h. das Datenfeld) zu verstehen.

Offen bleibt hier jedoch, was neben den vorgebrachten Beispielen nun denn auch noch als „Datum" zu qualifizieren ist. Ist ein dargestellter Buchstabe keine semantische Sinneseinheit? Wie steht es mit einer durch ein Bit codierten Ja/Nein- Entscheidung oder durch Lautsprecher erzeugte Töne? Auch wenn, was hier bezweifelt wird, ein handhabbarer Datumsbegriff aus dem Bereich des Datenschutzes angenommen werden könnte, so widerspricht dieser dennoch dem Rechtsgut des § 202a, der Verfügungsbefugnis über Daten. Als Abgrenzungskriterium dient im BDSG letztlich der informatorische Inhalt i.S. einer Qualitätsprüfung. Der Inhalt der Daten ist jedoch, wie oben festgestellt wurde, für § 202a irrelevant. Dieser Ansatz ist deshalb abzulehnen.

Gerade bei Annahme einer Übertragung des Datumsbegriffs aus dem Datenschutzrecht ist dann von Interesse, ob das Datum überhaupt Tatobjekt i.S.d § 202a sein kann. Problematisch ist dies im Hinblick auf das aus Art. 103 Abs. 2 GG folgende Analogieverbot (nullum crimen, nulla poena sine lege stricta). Gerade bei Tatbestandsmerkmalen des Besonderen Teils des StGB ist der über die Grenze der Auslegung hinausgehende Analogieschluß verboten.[187] Analogie ist die Übertragung einer rechtlichen Regel auf einen im Gesetz nicht geregelten anderen Fall im Wege des Ähnlichkeitsschlusses.[188]

---

185 *Schulze-Heiming*, Der strafrechtliche Schutz der Computerdaten, S. 27. Sie beruft sich auf *Sondermann*, Die neuen Straftatbestände der Datenveränderung § 303a StGB und § 303b StGB", Diss. Münster 1989, S. 28/29.

186 *Schulze-Heiming*, Der strafrechtliche Schutz der Computerdaten, S. 28.

187 *Roxin*, AT 1, § 5 II. 1. Rn. 8.

188 *Roxin*, AT 1, § 5 II. 1. Rn. 8.

Auslegungsgrenze ist der mögliche umgangssprachliche Wortsinn der Tatbestandsmerkmale.[189] Innerhalb dieses Rahmens erfolgt die Auslegung unter Berücksichtigung der nächstliegenden Wortbedeutung, der Vorstellung des historischen Gesetzgebers und des gesetzessystematischen Zusammenhangs nach dem Zweck des Gesetzes (teleologische Auslegung).

Die ganz h.M.[190] erachtet auch das Datum als Tatobjekt i.S.d. § 202a, da das einzelne Datum ebenso schützenswert anzusehen sei wie die Mehrzahl von Daten.[191] Außerdem stellt *Schulze-Heiming* fest, daß grundsätzlich die Verwendung der Pluralform bei allen Tatbeständen anerkannt sei, die aus praktischen Gründen oder aus der Typizität der Tat heraus in ihrer Fassung den Plural statt den Singular verwenden.[192] Auch aus diesem Grund ist nach dieser Ansicht das Datum Tatobjekt des § 202a und der Paragraphen, die auf § 202a Abs. 2 verweisen.

Aus den Begründungen der h.M. kann ein Argument aus teleologischer Auslegung und ein zweites aus systematischer Auslegung entnommen werden. Eine Überprüfung der Auslegung im Hinblick auf das Analogieverbot ist nicht ersichtlich. Dies erscheint problematisch. Der Wortsinn eines Wortes im Plural kann nicht dahingehend ausgelegt werden, daß auch der Singular damit gemeint ist. Plural und Singular sind im Sprachgebrauch eindeutige Zuweisungen für die Bezeichnung einer bestimmten Anzahl. Es kann daher nicht der Begriff „Daten“ dahingehend ausgelegt werden, daß beim umgangssprachlichen Gebrauch des Begriffs „Daten“ oder irgend eines anderen Begriffs in Pluralform damit auch das singuläre Datum gemeint ist. Der Singular stellt als sprachliche Ausdrucksform nicht ein weniger vom Plural dar, sondern ein aliud. Da der sprachliche Wortsinn die Auslegung begrenzt, schlagen die Argumente teleologischer, so wie systematischer Art der h.M. nicht durch. Die Auslegung der h.M. verstößt damit gegen das Analogieverbot. Nach der hier vertretenen Ansicht ist das einzelne Datum folglich kein Tatobjekt i.S. des § 202a.[193]

---

189 *Roxin*, AT 1, § 5 II. 1. Rn. 28.

190 Tröndle/Fischer-*Tröndle*, § 202a Rn. 6; *Hilgendorf*, JuS 1996, 509 (511); *Schlüchter*, 2. WiKG, S. 60; Schönke/Schröder-*Lenckner*, § 202a Rn. 3.

191 *Schlüchter*, 2. WiKG, S. 60; *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 46.

192 *Schulze-Heiming*, Der strafrechtliche Schutz der Computerdaten, S. 28 unter Berufung auf *Möhrenschlager*, wistra 1982, 201 (204). *Möhrenschlager* selbst beruft sich auf *Sieber*, Computerkriminalität und Strafrecht, (2.Auflg.), S. 41. Dies ist jedoch unzutreffend, da *Sieber* selbst vorschlägt den Singular beim Tatobjekt des § 269 zu verwenden, da sonst das „Datum“ nicht erfaßt sei.

193 Siehe auch *Sieber*, Computerkriminalität und Strafrecht, (2.Auflg.), S. 41. Im Rahmen der Untersuchung des damals noch zu erlassenden § 269 sind Tatobjekt auch „Daten“.

3. Die einschränkenden Merkmale des § 202a Abs. 2

Der uferlose Datenbegriff wird durch die Merkmale des § 202a Abs. 2 erheblich eingeschränkt.[194] Im Folgenden werden diese einschränkenden Merkmale untersucht.

a) Nicht unmittelbar wahrnehmbar

Daten dürfen nach § 202a nicht unmittelbar wahrnehmbar sein. Die Hinweise im Gesetzeswortlaut auf elektronische und magnetische Speicherung sind lediglich Beispiele deklaratorischer Art. Letztlich kommt es nur auf eine nicht unmittelbare Wahrnehmbarkeit der Daten an, so daß, wie es auch dem ausdrücklichen Willen des Gesetzgebers entspricht, § 202a Abs. 2 offen für neue Technologien ist.[195]

Nach Ansicht des Gesetzgebers sind unmittelbar wahrnehmbare Daten u.a. in §§ 201, 202 ausreichend geschützt.[196] Damit ist klargestellt, daß es für die Schutzbereiche des § 202a und der §§ 201, 202 keine Überschneidungen gibt.[197]

Die Wahrnehmbarkeit bezieht sich auf die Darstellung der Daten und damit die Syntax. Dies kann anschaulich gemacht werden durch ein Beispiel, das verschlüsselte Schriftstück. Hier ist der Inhalt der Datensammlung „Schriftstück" nicht wahrnehmbar, da verschlüsselt. Damit liegt auf der Ebene der Semantik nicht unmittelbare Wahrnehmbarkeit vor. Der verschlüsselte Brief ist jedoch klassisches Schutzobjekt der §§ 201, 202. Da sich Schutzbereiche der §§ 201, 202 mit dem des § 202a nicht überschneiden, wird klar, daß sich die fehlende Wahrnehmbarkeit auf die syntaktische Ebene beziehen muß. Ein Datum ist also dann nicht unmittelbar wahrnehmbar, wenn seine Darstellung nicht mit Sinnen erfaßt, also vor allem gesehen oder gehört werden kann.[198] Als Gegenbeispiel dient hier die Lochkarte alter Computersysteme, auf der Daten und Programme gestanzt sind, die dann für den Computer lesbar und abarbeitbar waren. Die Darstellung der Daten in Form gestanzter Löcher auf der Karte ist erkennbar und damit unmittelbar wahrnehmbar. Unerheblich ist, daß der Inhalt der Daten nur von einer Maschine oder einem Spezialisten unmittelbar verstanden werden kann.[199]

---

194 Tröndle/Fischer-*Tröndle*, § 202a Rn. 3.

195 BT-Drs. 10/5058, S. 29.

196 BT-Drs. 10/5058, S. 29.

197 *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 50.

198 *Schmitz*, JA 1995, 478 (479); so auch *Welp*, iur 1988, 443 (446); *Lenckner/Winkelbauer*, CR 1986, 483 (484); *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 51.

199 *Schmitz*, JA 1995, 478 (479).

Streitig ist, ob auch solche Daten nicht unmittelbar wahrnehmbar i.S.d. § 202a sind, die zu ihrer sinnlichen Erfaßbarkeit (z.B. Sichtbarmachung) keine Transformation in eine andere Zeichenkategorie bedürfen.[200] Dies liegt dann vor, wenn die Daten durch reine Vergrößerung sichtbar gemacht werden können, wie z.B. beim Mikrofilm. *Jähnke*[201] fordert, daß von den Daten überhaupt nichts wahrnehmbar sein dürfe. Fehle es bei verkörperten Zeichen, etwa bei Mikrofilmen oder Lochkarten, lediglich an der Lese- oder Deutungsmöglichkeit, läge ein Datum im Sinne des Absatzes 2 nicht vor.

Diese Auslegung erscheint jedoch problematisch. Würde sie zugrunde gelegt, so schieden alle optischen Speichermedien aus. Dies würde dann auch für die weit verbreitete CD-ROM, so wie auch für die wiederbeschreibbare CD[202] gelten.[203] Auch die Übermittlung von Daten mittels Glasfaserkabel würde nicht unter § 202a fallen.[204]

Solche optischen Speicher und Übermittlungsmethoden sind überwiegend in Verbindung mit Daten in Binärform im Einsatz, also den klassischen Computerdaten. Der Schutzzweck des § 202 a bezieht sich jedoch gerade auf solche Computerdaten, so daß mit der h.M.[205] keine Transformation in eine andere Zeichenkategorie zu fordern ist. Der Wortlaut steht dem nicht entgegen, da auch hier die Daten „nicht unmittelbar wahrnehmbar „ im Sinne von „mit Sinnen nicht unmittelbar erfaßbar“[206] sind. Die Darstellung der Daten ist nicht erfaßbar. Der Mensch kann sie ohne bestimmte technische Hilfsmittel nicht wahrnehmen.

Es kann daher definiert werden, daß solche Daten „nicht unmittelbar wahrnehmbar“ i.S.d. § 202a Abs. 2 sind, deren Darstellung ohne technische Hilfsmittel ein mit denkbar

---

200 Eine solche Transformation verlangen SK-*Samson*, § 202a Rn. 7; LK-*Jähnke*, § 202 Rn. 4.

201 LK-*Jähnke*, § 202a Rn. 4

202 Auch CD rewriteable oder CDR genannt

203 Der Laser tastet bei der CD Vertiefungen ab, die ein Bitmuster darstellen. Auch hier ist bei Vergrößerung die Darstellung der Informationen sichtbar.

204 Auch beim Glasfaserkabel, bei dem mittels Lichtimpulsen das Datum dargestellt wird, kann bei entsprechender Vergrößerung (und Verlangsamung des Vorgangs) diese Darstellung sichtbar gemacht werden.

205 *Hilgendorf*, JuS 1996, 509 (511); *Lenckner/Winkelbauer*, CR 1986, 483 (484); *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 51; Tröndle/Fischer-*Tröndle*, § 202a Rn. 6; Lackner/Kühl-*Kühl*, § 202a Rn. 2; *Binder*, RDV 1995, 57 (58); *Schmitz*, JA 1995, 478 (479); *Schulze-Heiming*, Der strafrechtliche Schutz der Computerdaten, S. 48.

206 „Wahrnehmen“ wird definiert mit „als Sinneseindruck aufnehmen“, aus Duden, Das große Wörterbuch der deutschen Sprache, Band 10.

optimalen Sinnen ausgestatteter Mensch nicht erfassen kann. Als Beispiele können hier das Mikroskop, die Lupe oder ein akustischer Verstärker angeführt werden.[207]

b) Speicherung von Daten

Die Merkmale der Speicherung und Übermittlung grenzen die geschützten Informationen weiter ein. In der Literatur werden häufig die Legaldefinitionen aus dem BDSG (§ 3 Abs. 5 Satz 2 Nr. 1 für „Speichern" und Nr. 3 für „Übermitteln") herangezogen.[208] So zitiert *Lenckner* schon im Sinne des § 202a Abs. 2 abgewandelte Definitionen: „Gespeichert sind Daten, wenn sie zum Zweck ihrer weiteren Verwendung erfaßt, aufgenommen oder aufbewahrt sind (§ 3 Abs. 5 Nr. 1 BDSG)".[209] Die Begriffe Erfassen, Aufnehmen, und Aufbewahren decken alle Formen der Verkörperung von Informationen auf einem Datenträger ab.[210] Der Begriff des Datenträgers ist weit auszulegen. Erfaßt ist jedes chemische oder physikalische Medium auf dem Information festgehalten werden kann.[211]

Das BDSG verlangt jedoch darüber hinaus einen Verarbeitungs- und Nutzungszweck. Dies ist im Rahmen des Datenschutzrechts einleuchtend, da dem Datenschutz das Grundrecht auf informationelle Selbstbestimmung zugrunde liegt.[212] Die bloße Existenz vom BDSG geschützter personenbezogener Daten betrifft nicht den Schutzbereich dieses Grundrechts. Erst die drohende Verwendung der Daten tangiert die Betroffenen.[213] Die praktische Bedeutung dieser Klausel ist im Rahmen des Datenschutzes gering, da das Erfassen, Aufnehmen und Aufbewahren von personenbezogenen Daten regelmäßig kein Selbstzweck ist, sondern gerade dazu dient, die Information verfügbar zu halten.[214] Im Bereich des Strafrechts würde dies jedoch relevant werden, da § 202a Abs. 1 sich auf alle denkbaren Daten bezieht. Im Bereich des Strafrechts ist Schutzobjekt die Daten an sich, d.h. die Existenz der Daten. Schutzzweck ist ein formales Geheimhaltungsinter-

---

207 Beispiele von *Welp*, iur 1988, 443 (446).

208 Schönke/Schröder-*Lenckner*, § 202a Rn. 4; Lackner/Kühl-*Kühl*, § 202a Rn. 2; *Haß*, Der strafrechtliche Schutz von Computerprogrammen, in: Lehmann (Hrsg.), Rechtsschutz und Verwertung von Computerprogrammen, S. 481 Rn. 22; Tröndle/Fischer-*Tröndle*, § 202a Rn. 4 bezieht sich nur auf die Definition des Speicherns.

209 Schönke/Schröder-*Lenckner*, § 202a Rn. 4.

210 Vgl. Simitis/Dammann/Geiger/Mallmann/Walz-*Dammann*, § 3 BDSG Rn.121.

211 Vgl. *Schmitz*, JA 1995, 478 (480), der von einem realen („festen") Datenträger spricht.

212 *Ordemann/Schomerus*, § 1 BDSG Anm. 3.3.

213 Vgl. Simitis/Dammann/Geiger/Mallmann/Walz-*Dammann*, § 3 BDSG Rn. 126.

214 Simitis/Dammann/Geiger/Mallmann/Walz-*Dammann*, § 3 BDSG Rn. 126.

esse an Daten unabhängig von ihrer Qualität oder eines dahinter stehenden Motivs. Es kann daher nicht auf einen weiteren Verwendungszweck ankommen. Dieses Kriterium ist für § 202a Abs. 2 untauglich und damit abzulehnen.[215] Eine Speicherung i.S.d. § 202a Abs. 2 ist folglich dann gegeben, wenn Daten auf einem Datenträger fixiert sind.[216]

Eine gewisse, oder bestimmte Zeit der Speicherung ist nicht erforderlich.[217] Das Integritäts- und formalisierte Geheimhaltungsinteresse besteht unabhängig von der Dauer einer Speicherung.[218]

Maßgebliches Kriterium für eine Speicherung stellt für *Jessen* eine eindeutige Adressierung der Daten dar.[219] Für dieses Kriterium finden sich jedoch im Gesetzeswortlaut keine Anhaltspunkte. Lediglich die Feststellung, daß in der computermäßigen Datenverarbeitung regelmäßig eine Adressierung der Daten erfolgt, kann diesem Merkmal nicht diese Bedeutung zukommen lassen. Ist eine Speicherung von Daten auch ohne Adressierung möglich[220], was hier offengelassen werden kann, kann diese kein Abgrenzungskriterium zu einer Nichtspeicherung sein. Als Beispiel für nicht adressierte Daten läßt sich der Mikrofilm anführen.[221] Hier ist lediglich der Standort der Information Hilfe für die Suche danach; eine darüber hinausgehende Adressierung ist nicht gegeben. Auch im Hinblick auf das Rechtsgut der Datenverfügungsbefugnis ist nicht erklärbar, warum gerade Daten ohne Adressierung nicht erfaßt sein sollen. Eine Adressierung der Daten ist somit nicht erforderlich.

---

215 *Welp*, iur 1988, 443 (445). A.A. neben Schönke/Schröder-*Lenckner*, § 202a Rn. 4 auch Tröndle/Fischer-*Tröndle*, § 202a Rn. 4. Es verwundert, daß *Lenckner* und *Tröndle* dieser Ansicht sind, da sie bei der Beurteilung des Datenbegriffs einen weiteren Verarbeitungszweck ablehnen, welches ein parallel gelagertes Problem darstellt.

216 Vgl. *Hilgendorf*, JuS 1996, 509 (512).

217 Ob Speicherung von einer gewissen Dauer erforderlich ist, war im Rahmen des BDSG von 1977 relevant. Siehe dort *Ordemann/Schomerus* in der Vorauflage, § 2 BDSGAnm. 2.1. Dieses Problem ist nunmehr obsolet geworden, da § 1 Abs. 3 Nr. 1 für kurzfristige Dateien eine Ausnahmeregelung trifft. Siehe Ordemann-Schomerus, § 3 BDSG Anm. 8.2.

218 So auch *Welp*, iur 1988, 443 (445). A.A. *Schulze-Heiming*, Der strafrechtliche Schutz der Computerdaten, S. 43 f., die ohne nähere Begründung eine „gewisse Bestandsdauer" für die Speicherung fordert.

219 *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 53 ff.

220 *Jessen* selbst hält sie für möglich.

221 Beispiel von *Schmitz*, JA 1995, 478 (481) in seiner Fn. 31; *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 55, hält auch den Mikrofilm für Tatobjekt des § 202a.

Ebenso ist das von *Schmitz* postulierte Erfordernis eines „Aufbewahrungsstadiums“ der Daten auf einem „festen“ Datenträger abzulehnen.[222] Hier sind zwei Thesen enthalten. Zum einen wird ein wie auch immer gearteter „fester“ Datenträger gefordert, zum anderen, daß die Daten nur dann als gespeichert anzusehen sind, wenn sie sich in einem Aufbewahrungsstadium befinden.

Zur These 1: *Schmitz* geht von der Datenbank i.S. einer dauerhaften Speicherung als Leitbild der gesetzgeberischen Maßnahmen aus. Auf dieser Grundlage wird fälschlicherweise auf einen abgeschlossenen Datenträgerbegriff geschlossen. Eine Datenbank läßt sich wie alle Daten auf jeglichem tauglichen Datenträger festhalten, so daß von dem Leitbild der Datenbank nicht auf spezifische Datenträger geschlossen werden kann. Darüber hinaus war der Gesetzgeber gerade bestrebt, die Norm für zukünftige Speichermedien offen zu gestalten.[223] Auch möglicherweise flüssige oder gasförmige Speicher würden daher unter den weiten Datenträgerbegriff fallen.

Zu These 2: *Schmitz* behauptet, Speichern habe etwas mit aufbewahren für einen späteren Zeitpunkt zu tun. So sind danach Daten, die sich im flüchtigen[224] Arbeitsspeicher befinden und mit denen der Computer gerade arbeitet, nicht gespeichert i.S.d. § 202a Abs. 2. Begründet wird dies damit, daß der Gesetzgeber eine Einschränkung bezüglich des Aggregatzustandes der geschützten Daten vorgenommen habe.[225] Dies ist jedoch nicht ersichtlich, da er wie oben schon angesprochen, § 202a Abs. 2 bewußt für neue Speichertechniken offen gestalten wollte. Auch vom Schutzzweck des § 202a, einer Datenverfügungsbefugnis, ist diese Ansicht nicht haltbar, da für jedwede materialisierte, nicht unmittelbar wahrnehmbare Information ein Schutzinteresse bezüglich ihrer ausschließlichen Verfügbarkeit und ihrer Integrität gegeben ist. Gerade Daten im Arbeitsspeicher sind gegenüber Angriffen Dritter gefährdet, da sie ohne weiteren Ladevorgang gelesen und auf fremden Datenträgern gespeichert werden können.

Wenn *Schmitz* dann doch anmerkt, daß Art und Dauer der Aufbewahrung kein Kriterium für die Speicherung sein können, hebelt er selbst seine Argumentation aus, die vorher noch einen „festen“ Datenträger und ein „Aufbewahrungsstadium“ forderte.[226]

---

222 So *Schmitz*, JA 1995, 478 (480).

223 BT-Drs. 10/5058, S. 29.

224 *Schmitz*, JA 1995, 478 (481).

225 Hier ist darauf hinzuweisen, daß Daten keinen Aggregatzustand haben, sondern nur das Speichermedium.

226 Vgl. *Schmitz*, JA 1995, 478 (481).

Zusammenfassend ist somit Speicherung als Materialisierung und Objektivierung der Daten im Sinne einer physikalischen Zuordnung zu einem Datenträger zu definieren.

c) Übermittlung von Daten

Das „Übermitteln“ wird in § 3 Abs. 5 Nr. 3 BDSG legaldefiniert. So schreibt *Lenckner* in Anlehnung daran, daß Daten übermittelt werden, wenn sie durch die speichernde Stelle weitergegeben oder zur Einsichtnahme, insbesondere zum Abruf bereitgehalten werden.[227] Diese Definition ist jedoch für § 202a Abs. 2 untauglich.[228] Zum einen ist bei der Auslegung des Merkmals der Schutzzweck des § 202a der Datenverfügungsbefugnis zu berücksichtigen, sowie zum anderen die Abgrenzung zur Speicherung. Die Weitergabe von Daten kann sich in Abgrenzung zur Speicherung nur auf die unkörperliche Weitergabe beziehen, da trotz Änderung des räumlichen Aufenthalts des Datenträgers die Daten dort gespeichert sind.[229] Die Verfügungsbefugnis von Daten bezieht sich auch auf Daten, die gerade innerhalb der speichernden Stelle von einem Ort zu anderen gesendet werden, was in der datenschutzrechtlichen Definition nicht berücksichtigt ist.[230] Daten, die zum Abruf bereitgehalten werden, sind gespeicherte Daten i.S.d. § 202a. Der Begriff der Übermittlung ist daher mit der h.M. eigenständig als jede unkörperliche Weiterleitung zu definieren.[231]

---

227 Schönke/Schröder-*Lenckner*, § 202a Rn. 4.

228 Sie kann lediglich zur Verdeutlichung herangezogen werden, so auch *Hilgendorf*, JuS 1996, 509 (512).

229 *Welp*, iur 1988, 443 (445); *Hilgendorf*, JuS 1996, 509 (512).

230 *Welp*, iur 1988, 443 (445); auch Schönke/Schröder-*Lenckner*, § 202a Rn. 4.

231 Vgl. Tröndle/Fischer-*Tröndle*, § 202a Rn. 5; *Hilgendorf*, JuS 1996, 509 (512); *Schmitz*, JA 1995, 478 (481).

II. Die Datenbestimmung

Die Daten dürfen „für den Täter nicht bestimmt sein“. Damit ist § 202a ein negatives Sonderdelikt.[232] Eine Bestimmung von Daten setzt immer einen Bestimmenden voraus. Es muß einen (oder mehrere) Berechtigten geben, der nicht damit einverstanden ist, daß dem möglichen Täter die Daten zugänglich gemacht werden. Bestimmender kann nur derjenige sein, der ein Recht auf die Daten hat. Dies ist der Rechtsgutsträger, der Verfügungsberechtigte über die Daten.[233]

1. Bestimmender

Es ist somit scharf zu trennen zwischen dem Verfügungsberechtigten als dem Bestimmenden und demjenigen, für den die Daten bestimmt sind, was in der Literatur nicht immer durchgehalten wird.[234] Der „Bestimmte“ ist gerade nicht verfügungsberechtigt, auch nicht derivativ, sondern darf im Rahmen der Vorgaben des Berechtigten mit den Daten verfahren. So bedarf es auch nicht dieses Merkmals, wenn ein Verfügungsberechtigter einen anderen mit ihm zusammen zum Verfügungsberechtigten macht. Dies kann in der Weise geschehen, daß beide gemeinschaftlich verfügen dürfen, oder jeder allein und unabhängig von dem oder den anderen. Derjenige, der bei einer gemeinschaftlichen Verfügungsbefugnis allein und ohne Abstimmung handelt, ist nicht verfügungsbefugt.[235] Er ist damit potentieller Täter.[236]

Schlüchter sieht die Möglichkeit einer sog. vertikalen Verfügungsbefugnis im Sinne einer über- und untergeordneten Verfügungsbefugnis.[237] Dies ist jedoch abzulehnen. Der Verfügungsbefugte hat das Vollrecht über die Daten. Er kann damit machen, was er möchte, so auch Zugangs- und Nutzungsrechte in einer bestimmten Weise oder innerhalb eines vorgegebenen Zeitraums vergeben. Eine derivative Verfügungsberechtigung wird jedoch nur erlangt, wenn der ursprünglich Berechtigte seine Herrschaftsmacht

---

232 Tröndle/Fischer-*Tröndle*, § 202a Rn. 7.

233 *Schlüchter*, 2. WiKG, S. 61, weist darauf hin, daß der Verfügungsberechtigte nicht Täter sein kann, was offensichtlich ist, da ja gerade er von § 202a geschützt wird.

234 So z.B. bei *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 61 f.

235 Vgl. *Schlüchter*, 2. WiKG, S. 62.

236 *Schlüchter*, 2. WiKG, S. 62, bezeichnet dies als „horizontale“ Verfügungsbefugnis.

237 *Schlüchter*, 2.WiKG, S. 62.

vollständig aufgibt. Eine vertikale Verfügungsbefugnis ist daher nach dem hier vertretenen Verständnis nicht denkbar.

2. Bestimmung

Im Hinblick auf das Tatobjekt Daten ist festzustellen, daß diese tatsächlich auf verschiedene Weise anderen zugänglich gemacht werden können. Hierzu eine Auflistung der Möglichkeiten:

- Daten können zur Kenntnis überlassen werden, ohne daß mit ihnen gearbeitet werden darf.
- Daten können zur Verwahrung überlassen werden ohne Nutzungs- und Kenntnisnahmerecht.
- Daten können aber auch zur Nutzung überlassen werden, ohne daß der Verfügungsberechtigte deren Kenntnisnahme erlaubt (und dies möglicherweise dokumentiert).
- Daten können zur Kenntnis und zur Nutzung überlassen werden.

Es stellt sich nun die Frage, bei welcher Art der Überlassung eine Datenbestimmung vorliegt. Zur Auslegung des Tatbestandsmerkmals der Datenbestimmung ist das Rechtsgut des § 202a heranzuziehen. Rechtsgut ist ein formalisiertes Geheimhaltungsinteresse des Verfügungsberechtigten. Es wird also ein ausschließliches Recht des Datenherstellers auf die Verfügbarkeit der Daten im Hinblick auf deren Kenntnisgabe geschützt. Der Berechtigte soll bestimmen können, wer, in welcher Weise und wie lange ein anderer die Möglichkeit zur Kenntnisnahme haben soll. Das Recht zur alleinigen Nutzung und Veränderung von Daten wird durch § 303a geschützt. Es ist folglich darauf abzustellen, ob der Täter gegen oder ohne den Willen des Verfügungsberechtigten bezüglich einer Kenntnisgabe der Daten gehandelt hat. Die bloße Überlassung von Daten zur Nutzung ohne Einräumung der Kenntnisnahme ist für die Datenbestimmung nicht ausreichend.

Demgemäß ist eine Definition, die Daten dann für den Täter als nicht bestimmt erachtet, wenn sie nach dem Willen des Verfügungsberechtigten nicht in den Herrschaftsbereich gelangen sollen, abzulehnen.[238] Sie bestimmt allein die willentliche Herausgabe der Daten an den Täter als Datenbestimmung. Dies stellt eine zu starke Anlehnung an das Eigentumsdelikt des § 242 dar. Begibt sich der Gewahrsamsinhaber willentlich des Ge-

---

[238] LK-*Jähnke*, § 202a Rn. 9; Lackner/Kühl-*Kühl*, § 202a Rn. 3; Tröndle/Fischer-*Tröndle*, § 202a Rn. 7.

wahrsams an einer Sache, so liegt keine Wegnahme vor. Hier wird der Gewahrsam über eine Sache mitgeschützt, die regelmäßig im Herrschaftsbereich des Gewahrsamsinhabers verbleiben soll. Das Wesen der Daten ist jedoch bestimmt durch ihre unendliche Reproduzierbarkeit, sowie durch die auf Datenübertragungsleitungen äußerst schnelle Möglichkeit der Versendung. Für die Datenbestimmung ist daher die „Weggabe der Daten" nicht maßgeblich, sondern allein der darüber hinaus gehende Wille des Verfügungsberechtigten, vor dem möglichen Täter die Daten geheim zu halten.

Dies darf jedoch nicht mit dem Merkmal der Zugangssicherung verquickt werden.[239] Es kann nicht automatisch angenommen werden, daß durch eine entsprechende Dokumentation eines Geheimhaltungswillens auch eine Nichtbestimmung der Daten vorläge. Bei einer solchen Auslegung verlöre das Merkmal der Datenbestimmung seine eigenständige Bedeutung. Es kann demnach auch den Fall geben, bei dem eine Datenbestimmung trotz Zugangssicherung gegeben ist. Dazu ein Beispiel:

A versieht eine Datei mit einem Paßwortschutz. Seinen Freund B, der gerade bei ihm zu Besuch ist, läßt er versuchen, diesen Paßwortschutz zu knacken, damit dieser die in der Datei gespeicherten neuesten Witze aus dem Internet lesen kann.

Hier ist dem B ausdrücklich die Kenntnisnahme der Daten erlaubt worden, trotz objektiv gegebener Zugangssicherung. Eine Zugangssicherung kann daher nur als Indiz für eine Nichtbestimmung der Daten angesehen werden. Ebenso ist das Nichtversehen von Daten mit einer Zugangssicherung lediglich Indiz für eine Bestimmung der Daten zugunsten des potentiellen Täters. Letztlich ist der Wille des Verfügungsberechtigten bezüglich einer Einräumung der Kenntnisnahme maßgeblich. Es ist die Bestimmung der Daten folglich zu definieren als das Einverständnis des Verfügungsberechtigten mit der Kenntnisnahme der Daten durch Dritte.[240] Im Sinne der tatbestandlichen Formulierung als negatives Sonderdelikt sind Daten somit dann für den Täter nicht bestimmt, wenn ihm die Kenntnisnahme vom Verfügungsberechtigten nicht gestattet wurde.

Unerheblich sind mit der Einräumung der Kenntnisnahme möglicherweise einhergehende Zweckbestimmungen oder Nutzungsbeschränkungen. Die Daten bleiben trotz Verstoßes gegen derartige Einschränkungen bestimmt i.S.d. § 202a.[241] Somit ist § 202a,

---

239 In diese Richtung *Lenckner/Winkelbauer*, CR 1986, 483 (486); Schönke/Schröder-*Lenckner*, § 202a Rn. 6.

240 So im Ergebnis die h.M: Schönke/Schröder-*Lenckner*, § 202a Rn. 6; *Schlüchter*, 2. WiKG, S. 61 ff.; *Hilgendorf*, JuS 1996, 509 (512); *Schmitz*, JA 1995, 478 (480).

241 *Lenckner/Winkelbauer*, CR 1986, 483 (486).

wie zur Zeit seiner Entstehung oft gefordert wurde,[242] keine Vorschrift zur Bekämpfung der Computerspionage. Die Daten, die dem Spion von seinem Arbeitgeber anvertraut wurden, sind für diesen bestimmt, auch wenn er von diesen Daten für sich selbst eine Kopie anfertigt oder sie an ein Konkurrenzunternehmen oder eine fremde Macht weitergibt. Ohne Bedeutung ist ebenfalls, wenn sich die Daten inhaltlich auf den Täter beziehen, da die Datenbestimmung allein vom Willen des Verfügungsberechtigten abhängt.[243]

Räumt derjenige, für den Daten bestimmt sind, einem Dritten die Möglichkeit der Kenntnisnahme ein, so hängt eine eventuelle Datenbestimmung für diesen von der Vereinbarung des Verfügungsberechtigten mit dem zunächst „Bestimmten" ab.[244] So kann eine Kette derivativer Datenbestimmungen entstehen. Wird einem „Bestimmten" das Recht zur Kenntnisnahme entzogen, verlieren alle, die in der Kette danach kommen, ihre Berechtigung.[245] Hier kann berechtigterweise (im Gegensatz zu einer vertikalen Verfügungsbefugnis) von einer vertikalen Datenbestimmung gesprochen werden.

Samson[246] legt die Tathandlung „Verschaffen" dahingehend aus, daß ein Verschaffen mit Willen des Täters nicht denkbar ist und sieht in einem Verschaffen mit Willen des Berechtigten ein tatbestandsausschließendes Einverständnis i.S. einer Nichterfüllung der Tathandlung. Die Aufgabe des Merkmals der Datenbestimmung sei dann, so *Samson*, denjenigen straflos sein zu lassen, der sich Daten, die er ohnehin erhalten soll, im Vorgriff selbst verschafft. Hier scheint eine Parallele zur „Rechtswidrigkeit der Zueignungsabsicht" in § 242 anzuklingen. Die Zueignungsabsicht ist dann nicht rechtswidrig, wenn der Täter einen Anspruch auf die weggenommene Sache hat. Diese Auslegung ist jedoch abzulehnen. Allein das Sich-Verschaffen mit Willen des Verfügungsberechtigten reicht bei § 202a gerade nicht aus, da für Verschaffen zumindest auch die bloße Erlangung der tatsächlichen Herrschaftsgewalt ausreicht.[247] Vielmehr muß darüber hinaus die Kenntnisnahme der Daten, nicht allein eine Herrschaftsposition, erlaubt sein. Damit

---

242 Anhörung der Sachverständigen vor dem Rechtsausschuß, Protokoll Nr. 26 über öffentliche Anhörung zum 2. WiKG am 6.6.1984, S. 128, 177, 218 und Anlagen dazu; *Sieber*, Informationstechnologie und Strafrechtsreform, S. 49; *Tiedemann*, WM 1983, 1326 (1328); *Liebl/Grosch*, CR 1985, 162 ff.

243 Vgl. *Granderath*, 2. WiKG, DB 1986 Beilage Nr. 18, S. 2.

244 *Hilgendorf*, JuS 1996, 509 (512); *Schmitz*, JA 1995, 478 (481).

245 *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 62.

246 SK-*Samson*, § 202a Rn. 9.

247 Zum Merkmal des Verschaffens, siehe Seite 106 ff.

kann ein Einverständnis nicht allein aus der Tathandlung abgeleitet werden. Ein Merkmal der „rechswidrigen Zueignungsabsicht“ fehlt in § 202a.

3. Einverständnis

Die Tatbestandsmäßigkeit des § 202a ist vom Willen des Berechtigten abhängig. Damit ist in dem Merkmal der Datenbestimmung eine tatbestandsausschließende Einwilligung (Einverständnis) gegeben.[248] *Haß*[249] erschließt daraus zutreffenderweise folgende Konsequenzen für die Datenbestimmung:

- Das Einverständnis kann nur dann den Tatbestand ausschließen, wenn es zur Zeit der Tat vorliegt.
- Es ist anerkannt, daß das Einverständnis bedingt erteilt werden kann.
- Die Datenbestimmung setzt als Einverständnis allein die innerlich gebliebene, natürliche Zustimmung zur Beschaffung der Daten durch den anderen voraus. Damit ist eine Erklärung gegenüber dem die Daten Beschaffenden nicht erforderlich.

Haß[250] lehnt sich an die Voraussetzungen der h.M.[251] für tatbestandsausschließende Einverständnisse an. Die weiteren Konsequenzen dieser Meinung sind:

- Für die Fälle des Einverständnisses ist nur der natürliche Wille maßgeblich, d.h. es ist keine Einsichtsfähigkeit wie bei der rechtfertigenden Einwilligung erforderlich[252]
- Willensmängel (Irrtum, Täuschung, Zwang) sind beim Einverständnis unerheblich[253]

---

248 So ist auch der Hinweis des Gesetzgebers in BT-Drs. 10/5058, S. 29 zu verstehen; Lackner/Kühl-*Kühl*, § 202a Rn. 3; LK-*Jähnke*, § 202a Rn. 9; *Bühler*, MDR 1987, 448 (453); *Möhrenschlager*, wistra 1986, 128 (140). Allgemein zum Einverständnis Schönke/Schröder-*Lenckner*, vor § 32 Rn. 30. A.A. *Schlüchter*, 2. WiKG, S. 68, die die Einwilligung als möglichen Rechtfertigungsgrund anspricht.

249 *Haß*, Der strafrechtliche Schutz von Computerprogrammen, in: Lehmann (Hrsg.), Rechtsschutz und Verwertung von Computerprogrammen, S. 483 Rn. 24 ; auch LK-*Jähnke*, § 202a Rn. 13 ist für die Anwendbarkeit der Regeln der h.M. über das Einverständnis.

250 *Haß*, Der strafrechtliche Schutz von Computerprogrammen, in: Lehmann (Hrsg.), Rechtsschutz und Verwertung von Computerprogrammen, S. 483 Rn. 24.

251 *Geerds*, GA 1954, 262 (266); *Baumann/Weber/Mitsch*, AT, § 17, Rn. 93 ff.; *Blei*, AT, § 37 I 1; *Bockelmann/Volk*, AT, § 15 C I 1 b bb; *Kühl*, AT, § 9, Rn. 9 ff; *Wessels/Beulke*, AT, Rn. 366 ff..

252 So auch BGHSt 23,1.

253 *Wessels/Beulke*, AT, Rn. 368.

III. Die Datensicherung

Weiteres Tatbestandsmerkmal des § 202a ist eine besondere Sicherung gegen unberechtigten Zugang. Hier kommt zum Ausdruck, daß nur solche Daten strafrechtlich geschützt sein sollen, bei denen ein Interesse an der Geheimhaltung nach außen in Erscheinung tritt. Insofern steht dieses Merkmal in engem Zusammenhang mit dem Rechtsgut des § 202a. Das Rechtsgut gewinnt gleichsam durch dieses Merkmal seine Konturen. Es wird nun auf die einzelnen Bestandteile und die sich daraus ergebenden Auslegungsprobleme näher eingegangen.

1. Zugang

Dieses Merkmal ist erstmals in das Strafrecht eingeführt worden und auch in den gesetzgeberischen Materialien finden sich keine Interpretationshinweise.

Der Begriff des Zugangs ist nach Ansicht von *Leicht*[254] weit auszulegen. Zugang zu Daten ist danach jede technische und physikalische Einwirkungsmöglichkeit auf Datenspeicher und den physischen Zugang zum System und Sicherheitsbereich.[255] Dem ist zuzustimmen. Als Beleg dafür kann der Hinweis des Gesetzgebers auf § 243 Abs. 1 Nr. 2 herangezogen werden.[256] Hier wird das Behältnis als Beispiel einer Schutzvorrichtung genannt. Ein Behältnis ist „ein zur Aufnahme von Sachen dienendes und sie umschließendes Raumgebilde, das nicht dazu bestimmt ist, von Menschen betreten zu werden".[257] Es handelt sich damit um eine Vorrichtung zum Schutz vor physischem Zugang zur Datenverarbeitungsanlage und nicht erst zum Schutz vor einem unmittelbaren Datenzugriff.

Auch der Sicherheitsbereich in Form von eigens dafür vorgesehenen Räumen und Anlagen ist vom Begriff Zugang umfaßt. Dieser Sicherheitsbereich besteht jedoch zumeist aus Räumlichkeiten, die auch zum Betreten von Menschen dienen, so daß sie nicht § 243 Abs. 1 Nr. 2 unterfallen, sondern § 243 Abs. Nr. 1. Hierzu ist festzustellen, daß der Gesetzgeber lediglich darauf hinweist, daß zur Auslegung § 243 Abs. 1 Nr. 2 herange-

---

254 *Leicht*, iur 1987, 45 (46) unter Berufung auf *Weck*, Datensicherheit, S. 33 ff. und *Dworatschek/Büllesbach/Koch*, Personalcomputer und Datenschutz, S. 40.

255 So auch Tröndle/Fischer-*Tröndle*, § 202a Rn. 7a.

256 BT-Drs. 10/5058, S. 29.

257 Schönke/Schröder-*Eser*, § 243 Rn. 22; BGHSt 1, 158 (163).

zogen werden „kann".[258] Unter Berücksichtigung des Sinn und Zwecks des § 202a kann es nicht einleuchten, daß eine Schutzvorrichtung eine bestimmte Größe haben soll, so daß es nicht zum Betreten von Menschen dienen kann. Wird also eine Datenverarbeitungsanlage zur Sicherung der Daten weggeschlossen, kann es keinen Unterschied machen, von welcher Art der abgeschlossene Raum ist, und welche Größe er hat. So könnten umschlossene Räume, die zum Betreten von Menschen dienen, wie in § 243 Abs. 1 Nr. 1 beschrieben, unproblematisch unter § 243 Abs. 1 Nr. 2 als andere Schutzvorrichtungen subsumiert werden, müßte man nicht die Nr. 2 von der dann eigentlich überflüssigen Nr. 1 abgrenzen.[259] Der weite Zugangsbegriff gewährleistet dem Dateninhaber, Vorkehrungen jedweder Art zum Schutze der Daten vorzunehmen, die grs. dann auch den gewünschten strafrechtlichen Schutz bringen, wenn sie die weiteren eingrenzenden Voraussetzungen für eine besondere Sicherung erfüllen.[260]

2. Besondere Sicherung

Der Gesetzgeber verweist für den Begriff und die Auslegung der besonderen Zugangssicherung auf die § 243 Abs. 1 Nr. 2 und § 202 Abs. 2.[261] Dies ist jedoch nicht sehr ergiebig, da die dort beschriebenen Sicherungen körperliche Gegenstände schützen durch umhüllende oder mechanisch wirkende Schutzvorrichtungen. Bei § 202a handelt es sich jedoch um das nichtkörperliche Schutzobjekt Daten. Die Träger der Daten, die körperliche Gegenstände darstellen, können zwar im Sinne des Verweises des Gesetzgebers beispielsweise durch Behältnisse geschützt werden. Die Daten können jedoch auch ohne Einwirken auf den körperlichen Datenträger erlangt werden. So sprechen *Lenckner/Winkelbauer*[262] von der Möglichkeit des Abrufens auf einen Bildschirm, des Auffangens von Funksignalen oder Datenströmen. Des weiteren können die Informationen durch „Abhören" der elektromagnetischen Strahlung im Radiofrequenzbereich von Computersystemen und da insbesondere von Monitoren und elektrischen Leitungen verschafft werden.[263] Dies hat auch der Gesetzgeber gesehen und bewußt neben dem

---

258 BT-Drs. 10/5058, S. 29.

259 In diesem Sinne kann auch Tröndle/Fischer-*Tröndle*, § 243 Rn. 23 verstanden werden.

260 So im Ergebnis auch *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 133.

261 BT-Drs. 10/5058, S. 29.

262 *Lenckner/Winkelbauer*, CR 1986, 483 (487).

263 Aufschlußreich hierzu Spiegel 36/1996 S. 194 ff.. „Die elektrischen Signale der Computerelektronik erzeugen elektromagnetische Wellen im Radiofrequenzbereich. Aus den Abstrahlungen läßt sich zum Beispiel ein Monitorbild aus einigen hundert Metern Entfernung ausspähen. Auch Ta-

Begriff „besondere Zugangssicherung“ keine Zusätze wie in § 202 Abs. 2 („verschlossenes Behältnis“) in den Gesetzestext aufgenommen. Es sind daher auch nichtkörperliche Sicherungen (sog. logische Sperren), wie der Paßwortschutz, grs. als Zugangssicherungen i.S.d. § 202a allgemein anerkannt. Zugangssicherungen können daher physikalischer wie auch logischer Art sein.

a) Mögliche Schutzvorrichtungen

Die möglichen Schutzvorrichtungen lassen sich in folgende Kategorien einteilen:

- Verbote und Geheimhaltung

Schon ein Verbot des Berechtigten gegenüber einem Dritten stellt eine Beschränkung des Zugangs dar. Dies ist jedoch schon vom Tatbestandsmerkmal der Datenbestimmung erfaßt.[264] Die Geheimhaltung von Daten durch Verstecken an einem ungewöhnlichen Ort der Dateienstruktur kann möglicherweise eine Zugangssicherung darstellen.[265]

- Schutz des gesamten Computersystems

Hier kommen vor allem mit dem Rechner räumlich verbundene, jedoch hardwareunabhängige[266] Sicherungen in Betracht, so beispielsweise ein Behältnis, in welches das Computersystem weggeschlossen werden kann. Aber auch ein abgeschlossener Raum, den Menschen betreten können oder die Pförtneranlage eines Unternehmens, kann grs. eine Zugangssicherung darstellen. Auch ein sog. closed-shop-Betrieb, bei dem nur bestimmte Personen durch kombinierte Kontroll- und Sicherheitseinrichtungen Zutritt zu den Computerräumen oder einzelnen Computeranlagen haben, stellt in der Praxis eine Methode der Datensicherung dar.

- Hardwaregebundene Sicherung

---

statur und Drucker erzeugen Radiowellen. Verbindungskabel wirken als Sendeantennen. Über die Netzleitung verbreiten sich die Signale über ganze Gebäude“ (S. 197).

264 *Hilgendorf*, JuS 1996, 702 (703).

265 Zur Geheimhaltung als Zugangssicherung siehe Seite 104. Diese wurde von *Hilgendorf*, JuS 1996, 702 (703) als mögliche Zugangssicherung eingeführt und bei bestimmten Voraussetzungen als solche bejaht.

266 Hardware wird in DIN 44.300 definiert als „Gesamtheit oder Teil der apparativen Ausstattung eines Rechnersystems“.

Daten können auch durch direkt mit der Hardware verbundene Zugangsbeschränkungen gesichert sein. Zu nennen sind hier biometrische Erkennungsverfahren[267], Ausweisleser, Benutzercode i.V.m. mechanischer, oder elektronischer Sperre.

- Sicherung softwaremäßiger Art

Daten werden zumeist durch Daten selbst geschützt. Hier sind insbesondere der Schutz von Daten mit Paßwörtern zu nennen, sowie die Verschlüsselung von Daten, welche besonders bei Daten relevant wird, die von einem System zum anderen übermittelt werden.

Zunächst soll geklärt werden, welche Voraussetzungen eine Zugangssicherung allgemein erfüllen muß.

b) Voraussetzungen einer besonderen Sicherung

In der Literatur wird zwischen einer objektiven und einer subjektiven Komponente unterschieden.[268] So schreibt *Lenckner*: „Gegen unberechtigten Zugang besonders gesichert sind sie (d. Verf.: die Daten), wenn Vorkehrungen getroffen sind, die objektiv geeignet und subjektiv nach dem Willen des Berechtigten dazu bestimmt sind, den Zugriff auf Daten auszuschließen oder wenigstens nicht unerheblich zu erschweren. Dies braucht zwar nicht ihr einziger Zweck zu sein, jedenfalls aber muß der Berechtigte durch die Sicherung gerade auch sein spezielles Interesse an der Geheimhaltung dokumentieren."[269] Hieraus ergeben sich zunächst zwei Elemente:

- objektive Eignung
- subjektiver Schutzzweck der Sicherung

Es ist zu prüfen, ob über das objektive Element der Eignung und subjektive Element der Zweckbestimmung hinaus möglicherweise noch ein Drittes hinzutritt: Ein gemischt-subjektiv-objektives Element der Dokumentation des Geheimhaltungswillens.[270]

---

267 Automatische Verfahren zur Erkennung von unverwechselbaren persönlichen Merkmalen, wie z.B. Fingerabdruck zur Identifizierung

268 *Hilgendorf*, JuS 1996, 702 (703).

269 Schönke/Schröder-*Lenckner*, § 202a Rn. 7 unter Hinweis auf BT-Drs. 10/5058, S. 29; ferner Tröndle/Fischer-*Tröndle*, § 202a Rn. 7; LK-*Jähnke*, § 202a Rn. 14; Lackner/Kühl-*Kühl*, § 202a Rn. 3b; *Leicht*, iur 1987, 47 ff.; *Möhrenschlager*, wistra 1986; 128 (140); *Schlüchter*, 2. WiKG, S. 65.

270 Eine gesonderte Prüfung, ob das formale Geheimhaltungsinteresse für den Täter erkennbar ist, d.h. die Maßnahme muß Dokumentationscharakter haben, schlägt *Leicht*, iur 1987, 45 (52) vor.

(1) Dokumentation des Geheimhaltungswillens

Die Anforderungen an die Dokumentation sind umstritten. *Lenckner*[271] sieht die Dokumentation als Gradmesser für die Zweckbestimmung. Dies ist jedoch abzulehnen, da in der Dokumentation eines Interesses ein objektives Element, ein tatsächlicher Vorgang mitenthalten ist. Die Dokumentation eines Geheimhaltungswillens ist daher nicht lediglich subjektiv.

Leicht[272] fordert die äußerliche Erkennbarkeit der Sicherung. *Jähnke*[273] hingegen sieht den Gehalt dieses Elements darin, daß es für eine Dokumentation genüge, wenn sie wirksam sei. Dokumentation bedeute nicht, daß die Sicherung nach außen erkennbar sein müsse. In dieselbe Richtung wie *Jähnke*[274] argumentiert *Tröndle*[275]. Er geht zwar mit *Leicht* von einem Kriterium der Erkennbarkeit aus, bezieht diese jedoch nicht auf die Sicherung selbst, sondern auf das Geheimhaltungsinteresse. Der Täter muß danach nur erkennen können, daß eine Sicherung, deren Art und Grad er nicht kennen muß, eine Sicherungsfunktion bezüglich der Daten erfüllt. Dem ist zuzustimmen. Schon in der Gesetzesbegründung wird die Dokumentation des Geheimhaltungsinteresses hervorgehoben[276] und nicht eine Dokumentation der Sicherung oder Sicherungsart. Der Täter überschreitet die Grenze zum kriminellen Unrecht, wenn er erkennt, daß Daten (wie auch immer) geschützt werden und er sich diese dennoch verschafft.

Damit ist jedoch Dokumentation als eigenständiges Element der besonderen Sicherung abzulehnen.[277] Das Erkennen oder die Erkennbarkeit einer Sicherungsfunktion einer irgendwie gearteten Einrichtung zum Schutz von Daten ist denklogisch nur dann gegeben, wenn eine Sicherung als solche vorliegt. Eine Sicherung ist nur dann als solche zu qualifizieren, wenn sie zumindest für den Dilettanten als Täter wirksam sein kann.[278] Es sind folglich zwei Problemkreise zu unterscheiden. Zum einen ist der erforderliche Grad einer Sicherung zu ermitteln (Sicherungsgrad), zum anderen muß beantwortet werden, welchen Zweck diese Sicherung erfüllen muß (Schutzzweck der Sicherung).[279] Für jede

---

271 Schönke/Schröder-*Lenckner*, § 202a Rn. 7.

272 *Leicht*, iur 1987, 45 (48 f.).

273 LK-*Jähnke*, § 202a Rn. 14.

274 LK-*Jähnke*, § 202a Rn. 14.

275 Tröndle/Fischer-*Tröndle*, § 202a Rn. 7.

276 BT-Drs. 10/5058, S. 29.

277 A.A. *Leicht*, iur 1987, 45 (52).

278 Insofern ist LK-*Jähnke*, § 202a Rn. 14 dann doch zu folgen.

279 Die Begriffe „Sicherungsgrad" (objektive Komponente) und „Schutzzweck der Sicherung" (subjektive Komponente) wurden von *Leicht*, iur 1987, 45 (46) eingeführt.

Sicherung kann in den oben genannten zwei Schritten geprüft werden, ob sie unter das Merkmal der besonderen Zugangssicherung fällt. Vorher werden noch die Auslegungsgrenzen der Begriffe „besondere“ und „Sicherung“ untersucht.

(2) Auslegungsgrenzen der Begriffe „besondere“ und „Sicherung“

Die Auslegung der „besonderen Sicherung“ wird in der Literatur zumeist ohne Anerkennung einer eigenständigen Bedeutung des Attributs „besondere“, oder zumindest ohne dessen Hervorhebung vorgenommen. Vorzugswürdig ist jedoch zu trennen zwischen der Auslegung des Begriffs der Sicherung und dessen Attributes „besondere“.

(a) Sicherung

Der Sicherungsbegriff umfaßt selbst schon die Minimalvoraussetzungen einer objektiven Sicherungswirkung und eines subjektiven Sicherungszwecks. Eine Sicherung muß, um als solche gelten zu können, erstens eine objektive Hürde im Sinne einer erhöhten Anstrengung des die Sicherung Überwindenden darstellen. Zweitens muß der Sichernde das Wissen und den Willen um das Erschweren des Zugangs zu den Daten aufweisen, d.h. einen Zweck zur Sicherung verfolgt haben.

(b) „besondere“

Hieraus ergibt sich, daß der Begriff „besondere“ darüber hinaus im Sinne eines qualitativen Plus gegenüber den allgemein in Frage kommenden Sicherungen auszulegen ist. Da „besondere“ Attribut der Sicherung ist, bezieht sich dieser Begriff auch auf beide Komponenten des Sicherungsbegriffs. Es muß daher in punkto Eignung der Sicherung, sowie in Bezug auf den Sicherungszweck ein qualitatives Plus gegenüber der einfachen Sicherung vorliegen. Dies ist bei Auslegung der objektiven wie subjektiven Komponente zu beachten. Die „besondere“ Zugangssicherung kann folglich weder die objektiv denkbare Mindesthürde sein, noch den denkbar geringsten Datensicherungszweck verfolgen im Sinne eines gänzlich untergeordneten Sicherungsziels. Dies bildet die Untergrenze möglicher Auslegung der besonderen Zugangssicherung.

(3) Sicherungsgrad

Zunächst werden die Äußerungen in der Literatur über die objektiven Anforderungen (die Eignung) dargestellt, die an eine besondere Zugangssicherung zu stellen sind,. Dann wird dazu Stellung genommen.

(a) Stimmen aus der Literatur

Granderath[280] und *Möhrenschlager*[281] verweisen auf die §§ 243 Abs. 1 Nr. 2, 202 Abs. 2. Auch in diesen Vorschriften würden, abgestuft nach dem jeweils geschützten Rechtsgut, keine hohen Anforderungen an die besondere Sicherung gestellt.

Tröndle[282] schreibt, der Täter müsse nur erkennen können, daß eine besondere Sicherung Sicherungsfunktion habe. Vollständigen Schutz setze § 202a, der den Verfügungsberechtigten nicht auf Kosten treiben wolle, nicht voraus. So weist er insbesondere darauf hin, daß der erhöhte Sicherungsgrad des § 9 BDSG nicht erfüllt werden müsse.

Lenckner/Winkelbauer[283] meinen zu den qualitativen Anforderungen an die Sicherung Folgendes: Es gelte nichts anderes als bei § 202 Abs. 2 und § 243 Abs. 2 Nr. 2. Die Sicherung dürfe einerseits nicht lediglich so ausgestaltet sein, daß ihre Durchbrechung ohne weiteres möglich sei, andererseits brauche der Schutz nicht vollständig zu sein. (unter Berufung auf einschlägige Kommentierungen zu § 243) Im Einzelfall sei zu entscheiden, ob die jeweilige Sicherung entsprechend der ratio legis geeignet sei, einerseits das besondere „Geheimhaltungsinteresse" des Berechtigten an den Daten zu dokumentieren und andererseits für den Täter eine eindeutige Grenze zum kriminellen Verhalten zu ziehen.

Hilgendorf[284] will für den Grad der Sicherung ausreichen lassen, daß eine Sicherung den Geheimhaltungswillen des Berechtigten unmißverständlich deutlich macht, auch wenn sie von einem versierten Hacker ohne größere Anstrengung „geknackt" werden könne. Es sei zu bedenken, daß mit hinreichender Geduld und dem nötigen technischen Verständnis praktisch alle Zugangssperren überwunden werden könnten. Insbesondere ließen sich Paßwörter erraten oder mit entsprechenden Programmierkenntnissen umgehen. Dagegen sei das Vorliegen einer Zugangssperre zu verneinen, wenn eine Sicherung bereits von einem Laien ohne besondere Mühe überwunden werden könne.

Jähnke[285] ist der Ansicht, daß der angestrebte Schutz nicht absolut sein könne; unzureichend seien aber Vorkehrungen, die bereits jeder interessierte Laie zu überwinden ver-

---

280 *Granderath*, 2. WiKG, DB 1986 Beilage Nr. 18, S. 1.

281 *Möhrenschlager*, wistra 1986, 128 (140); mit diesem auch *Haß*, Der strafrechtliche Schutz von Computerprogrammen, in: Lehmann (Hrsg.), Rechtsschutz und Verwertung von Computerprogrammen, S. 481 Rn. 22; Lackner/Kühl-*Kühl*, § 202a Rn. 4; *Weber*, WM 1986, 1133 (1135).

282 Tröndle/Fischer-*Tröndle*, § 202a Rn. 7a.

283 *Lenckner/Winkelbauer*, CR 1986, 483 (485).

284 *Hilgendorf*, JuS 1996, 702.

285 LK-*Jähnke*, § 202a Rn. 15.

möge. Da mit Tätern zu rechnen sei, welche eingehende Kenntnisse und Erfahrungen auf dem Gebiet der Datenverarbeitung hätten, müsse die Sicherung auf sie abgestellt und nach der Erfahrung ihnen gegenüber wirksam sein.

Leicht[286] schließt sich zunächst bei der objektiven Komponente *Lenckner/Winkelbauer*[287] an. Er weist darauf hin, daß der Maßstab für den Sicherungsgrad der zu den §§ 243, 202 anerkannten Schutzvorrichtungen die erhöhte kriminelle Energie des Täters sei, die er zu deren Überwindung einsetzen müsse. Als Beispiel führt er einen Briefumschlag an, der auch ein gewisses Geheimhaltungsinteresse dokumentiere, aber für § 243 dennoch nicht ausreiche. Somit habe sich der Sicherungsgrad der Maßnahme an der vom Täter einzusetzenden erhöhten kriminellen Energie auszurichten. Er folgert daraus für den Sicherungsgrad, daß es dem Täter nicht ermöglicht werden dürfe, die Sicherung ohne weiteres zu durchbrechen. Daraufhin erhöht er jedoch den von ihm zunächst geforderten Sicherungsgrad um ein weiteres: Es sei erfahrungsgemäß von EDV-Insidern auszugehen, so daß die Sicherung so gestaltet sein müsse, daß sie auch diesem Täterkreis gegenüber zunächst ein Hindernis bereite.[288]

Jessen[289] übernimmt, ohne sich explizit darauf zu berufen, die Auslegung der besonderen Sicherung von *Lenckner/Winkelbauer* im Hinblick darauf, daß das Merkmal der besonderen Sicherung Ausdruck eines viktimodogmatischen Ansatzes sei. Dies besagt, daß hier Strafrechtsschutz nur demjenigen zuteil werde, der mit seinen Rechtsgütern nicht völlig sorglos verfährt.[290] Er geht von einer Sorgfaltsfunktion des Merkmals aus, die es erlaube, den Sicherungsgrad exakter zu fassen, als es die Ansätze der anderen Autoren vermögen. Maßgebend sei, daß ein Außenstehender dem Rechtsgutsträger bestätige, sorgfältig gehandelt zu haben. Die von ihm getroffenen Maßnahmen müßten nicht dem neuesten Stand der Technik entsprechen. Sie müßten vielmehr nach objektiven und für alle gleichermaßen geltenden Maßstäben ausgesucht, installiert und betrieben werden. Es seien alle wahrscheinlichen Vorgehensweisen des Täters zu berücksichtigen.

---

286 *Leicht*, iur 1987, 45 (46).

287 *Lenckner/Winkelbauer*, CR 1986, 483 (485).

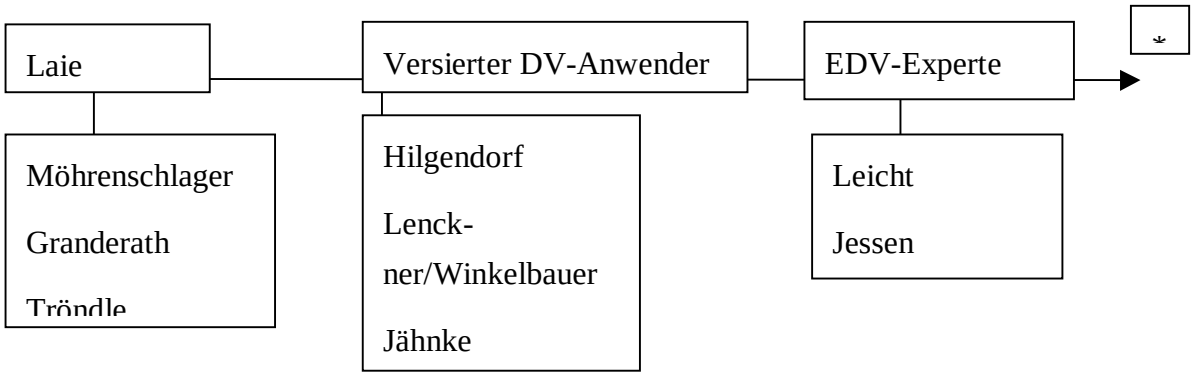
288 *Leicht*, iur 1987, 45 (49).

289 *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 119 ff.

290 *Lenckner/Winkelbauer*, CR 1986 483 (486); *Schönke/Schröder-Lenckner*, § 202a Rn. 1 unter Hinweis auf Hillenkamp, Vorsatztat und Opferverhalten, S. 77 ff.. Auch bei *Leicht*, iur 1987, 45 klingt dies an, wenn er schreibt, daß nur der sorgsam Handelnde Strafrechtsschutz erhalte.

Die untenstehende Abbildung will den verschiedenen Sicherungsgrad (bzw. verschiedene Auslegung der objektiven Eignung als besondere Sicherung), der Literaturmeinungen verdeutlichen.

Abbildung:



* Sicherungsgrad

(b) Stellungnahme

Wie oben dargestellt, gibt es in der Literatur durchaus verschiedene Auslegungen zu dem in § 202a zu fordernden Sicherungsgrad einer Vorrichtung gegenständlicher oder softwaretechnischer Art. Die ersten Äußerungen zu diesem Problem gleich nach Inkrafttreten des 2. WiKG berufen sich auf den Verweis des Gesetzgebers zu §§ 243 Abs.1 Nr. 2, § 202 Abs. 2 zur Auslegung der „besonderen Sicherung".[291] Doch dann wird mehr und mehr eine bestimmte EDV-Fachkunde des Täters gefordert.[292] *Jessen* dreht die Medaille um und fordert stattdessen „Sorgfalt" des Anlagenbetreibers.[293] Die Forderung nach einer bestimmten Fachkunde beim Täter stellt jedoch nichts anderes dar, als die Erstreckung des Strafrechtsschutzes lediglich auf den, der solchen fachkundigen Tätern ein objektives Hindernis entgegenstellt. Fordert man, daß die Sicherung dem fachkundigen Täter das Leben schwer macht, so stellt dies gerade eine Forderung nach Sorgfalt bei Betreiben einer DV-Anlage und der Datensicherung dar. Ein griffigeres und exakteres Kriterium ist mit der „Sorgfaltsfunktion" des Merkmals folglich nicht gefunden worden.

Einziger Anhaltspunkt für den Willen des Gesetzgebers ist der Verweis auf die §§ 243 Abs. 1 Nr. 2 und § 202 Abs. 2.[294] Hieraus kann zunächst für die möglichen physischen

---

291 *Granderath*, 2. WiKG, DB 1986 Beilage Nr. 18, S. 1; *Möhrenschlager*, wistra 1986, 128 (140).

292 *Leicht*, iur 1987, 45 (46).

293 *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 120.

294 BT-Drs. 10/5058, S. 28.

Sicherungen die Auslegung der Literatur und Rechtsprechung direkt übernommen werden, da sich für § 202a bezüglich des Angriffsobjekts „Daten“ nichts anderes ergibt. Diese sind auf körperlichen Trägern gespeichert, welche selbst Angriffsobjekte zumindest auch des § 243 Abs. 1 Nr. 2 sein können. Jedoch ist die Beschränkung auf Behältnisse und sonstige Schutzvorrichtungen, wie Schlösser, für § 202a zu eng. Es kann für den Sinn und Zweck des § 202a keinen Unterschied machen, ob die datenspeichernde Computeranlage durch einen abgeschlossenen, für Menschen begehbaren Raum gesichert ist oder durch ein Behältnis. In beiden Fällen liegt eine Sicherung des Tatobjekts „Daten“ vor. Dies steht auch nicht dem Verweis des Gesetzgebers entgegen, da bei Weglassen der Nr. 1 in Abs. 1 abgeschlossene Räume unproblematisch unter die Nr. 2 als Schutzvorrichtung fallen würden.[295] Es kann daher unterstellt werden, daß der Gesetzgeber dies so ausgelegt wissen wollte, oder er den Verweis auf § 243 Abs. 1 Nr. 1 unbewußt unterlassen hat.

Problematisch sind daher allein die sog. logischen Sperren, d.h. direkt dem System anhaftende Sicherungen softwaremäßiger Art. Auf diese ist der Verweis direkt nicht anwendbar. Angriffsobjekte in § 243 und § 202 sind Sachen, die nur durch andere Sachen vor Wegnahme oder Kenntnisnahme geschützt werden können. Daten sind jedoch nichtkörperlicher Art. Es ist nun zu prüfen, ob der Verweis des Gesetzgebers nicht auch für die Sicherungen nichtkörperlicher Art fruchtbar gemacht werden kann.

Den Ansatz, den Sicherungsgrad des § 243 Abs. 1 Nr. 2 bei den Sperren nichtkörperlicher Art im Rahmen des § 202a anzulegen, verfolgen außer *Jessen*[296] im Prinzip alle Autoren, die diesen Problemkreis behandelt haben, entweder ausdrücklich oder es klingt zumindest in der Argumentation an. Dies ist folgerichtig, da sich aus dem Verweis auch nichts anderes ergeben kann. Auch dem Gesetzgeber war klar, daß der Verweis bei den logischen Sperren, da diese nichtkörperlicher Art sind, sich nur auf den Sicherungsgrad im Allgemeinen beziehen kann. Im Folgenden ist der erforderliche Sicherungsgrad der §§ 243 Abs. 1 Nr. 2, 202 Abs. 2 herauszuarbeiten.

(i) Sicherungsgrad des § 243 Abs. 1 Nr. 2

Der gesetzgeberische Grund für dieses regelmäßig die Strafschärfung auslösende Beispiel des § 243 Abs. 1 Nr. 2 liegt darin, daß der Täter ein erhöhtes Maß von Rücksichtslosigkeit zeigt, weil er sich über eine besondere Sicherung hinwegsetzt, mit wel-

---

295 In diese Richtung auch Tröndle/Fischer-*Tröndle*, § 243 Rn. 23 unter Hinweis auf Bay JZ 73, 324.

296 *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 108.

cher der Eigentümer zu erkennen gibt, daß er auf die Erhaltung gerade dieser Sache Wert legt.[297]

Unter einer Schutzvorrichtung als einer besonderen Sicherung gegen Wegnahme i.S.d. § 243 ist eine von Menschen geschaffene Einrichtung oder Vorkehrung zu verstehen, die –zumindest auch – dazu bestimmt und geeignet ist, die Wegnahme der konkreten Sache, d.h. die Gewahrsamserlangung, **erheblich** zu erschweren.[298] Hier kommt zum Ausdruck, daß das Attribut „besondere" bei § 243 einen erhöhten Sicherungsgrad bedingt. Um als bloße Sicherung gelten zu können, muß eine irgendwie geartete, sowie gegenüber irgendwem wirksame sichernde Wirkung gegeben sein. Eine **besondere** Sicherung erfordert dagegen mehr.[299] Die Sicherung muß gewisse Qualitätsanforderungen erfüllen. So verlangt *Dölling*, daß dieVorrichtung jedenfalls in der überwiegenden Zahl der nach Lebenserfahrung zu erwartenden Vorgehensweisen bei der Ausführung des Diebstahls ein Hindernis gegen die Vollendung der Wegnahme darstellt.[300]

Sicherungen, die nach erfolgter Wegnahme der Wiedererlangung der mit ihr versehenen Sache dienen, wie z.B. ein elektromagnetisches Sicherungsetikett an einem Kleidungsstück, welches sich in einem Kaufladen befindet, stellen keine besondere Sicherungen gegen Wegnahme dar.[301] Die Sicherung muß die Gewahrsamserlangung erheblich erschweren, was das elektromagnetische Sicherungsetikett zumindest bei kleineren, leichteren Gegenständen nicht tut. Es kann damit allgemein von dem Erfordernis einer auch objektiv präventiven Sicherungswirkung gesprochen werden.[302]

Die Anforderungen an den Sicherungsgrad können wie folgt zusammengefaßt werden:

- Strafgrund und damit auch allgemeiner Anknüpfungspunkt für die Auslegung ist das erhöhte Maß an Rücksichtslosigkeit des Täters.
- Die Sicherung muß ein erhebliches Hindernis für den Täter darstellen in der Art, daß sie bei der überwiegenden Zahl der nach Lebenserfahrung zu erwartenden Vorgehensweisen ein Hindernis darstellt.

---

297 LK-*Ruß*, § 243 Rn. 18; BGH NJW 1974, 567; OLG Hamm NJW 1978, 769.

298 *Küper*, Definitionen, S. 227; Lackner/Kühl-*Kühl*, § 243 Rn. 15; *Rengier*, BT 1, § 3 Rn. 14; *Otto*, Grundkurs Strafrecht, § 41 Rn. 17.

299 A.A. *Wessels/Hillenkamp*, BT 2, Rn. 226, die lediglich fordern, daß die Wegnahme durch die Vorrichtung wenigstens erschwert wird.

300 *Dölling*, JuS 1986, 691 (692).

301 OLG Stuttgart NStZ 1985, 76 mit Anmerkung Seier JA 1985, 387; LK-*Ruß*, § 243 Rn. 19.

302 Vgl. *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 120.

- Die Sicherung muß präventiven Charakters sein, d.h. sie muß objektiv vor dem Erlangen des Tatobjekts schützen.

(ii) Übertragung des Sicherungsgrads auf § 202a

Einige Autoren knüpfen für die Auslegung der besonderen Sicherung des Zugangs von Daten an eine erhöhte kriminelle Energie des Täters an.[303] Eine Sicherung ist danach gegeben, wenn der Täter eine erhöhte kriminelle Energie aufwenden muß, um diese zu überwinden. Diese Anknüpfung entspringt offensichtlich der Anlehnung an den Strafgrund des § 243 Abs. 1 Nr. 2. Dies kann jedoch für § 202a nicht zutreffen. Ein erhöhtes Maß setzt immer einen Grundzustand voraus, zu dem sich dieses in Relation setzen kann. § 202a ist jedoch nicht Strafzumessungsnorm oder Qualifikation, sondern einzige Strafnorm gegen das Ausspähen von Daten. Die Auslegung dieses Tatbestandes bestimmt somit die Grenze von nichtkriminellem zu kriminellem Verhalten. Ein Kriterium der erhöhten kriminellen Energie ist daher untauglich, da kein Bezugsgegenstand vorhanden ist.

Dies macht den Verweis des Gesetzgebers jedoch nicht untauglich. Der Sicherungsgrad ist für sich allein genommen ein feststellbarer Umstand. Es ist daher nicht notwendig, auf den Strafgrund der erhöhten kriminellen Energie zur Bestimmung des Sicherungsgrades abzustellen. So kann, auf die Gegebenheiten des § 202a übertragen, der anzulegende Sicherungsgrad wie folgt beschrieben werden:

Auch die nichtkörperliche Sicherung muß ein erhebliches Hindernis für den Täter darstellen in der Art, daß sie bei der überwiegenden Zahl der nach Lebenserfahrung zu erwartenden Vorgehensweisen ein Hindernis darstellt. Die Sicherung muß präventive Wirkung haben. Ein erhebliches Hindernis stellt die nichtkörperliche Sicherung dann dar, wenn die Überwindung der Sicherung nicht ohne weiteres gelingen kann. Der Eindringende muß daher entweder ein erhöhtes Maß an Zeit aufbringen, oder erst durch Einsatz von speziellen Fachkenntnissen oder über Umwegen, wie beispielsweise das Überlisten von Paßwortgeheimnisträgern, die Sicherung überwinden können.

Es wird teilweise geschrieben, daß vollständiger Schutz nicht zu fordern sei.[304] Dies ist grs. richtig, da auch bei § 243 ein solcher nicht gefordert wird. Der Hinweis auf den vollständigen Schutz hilft jedoch nicht weiter, da logischerweise bei Sicherungen, die vollständigen Schutz bieten, Delikte nach § 202a nicht begangen werden könnten.

---

303 Z.B. *Leicht*, iur 1987, 45 (47); *Lenckner/Winkelbauer*, CR 1986, 483 (488).

304 So z.B: Tröndle/Fischer–*Tröndle*, § 202a Rn.7a und *Lenckner/Winkelbauer*, CR 1986, 483 (487).

Richtig an diesen Äußerungen ist jedoch, daß, wie *Hilgendorf* schon bemerkte, mit hinreichender Geduld und dem nötigen technischen Verständnis praktisch alle Zugangssperren überwunden werden könnten. Insbesondere ließen sich Paßwörter erraten oder mit entsprechenden Programmierkenntnissen umgehen.[305] Ist nun für den Meisterdieb das Türschloß eines Autos oder einer Truhe problemlos zu öffnen, jedoch für den Gelegenheitsdieb ein echtes Hindernis, so würde niemand im Rahmen des § 243 auf die Idee kommen, § 243 deshalb zu verneinen, weil das Schloß kein wirklich wirksames Hindernis war. Diese Überlegungen können auf § 202a übertragen werden.

Der Computerexperte kann nicht Maßstab für die Sicherung sein. Wichtigster Ansatzpunkt ist daher die Dokumentation des Geheimhaltungswillens. Ist der Wille zur Geheimhaltung klar erkennbar, so kann objektiv von einer besonderen Sicherung gesprochen werden. Der Geheimhaltungswille ist ausreichend dokumentiert, wenn es für den Computerlaien nicht ohne weiteres möglich, die Sicherung zu überwinden.[306] Hier ist dann für jeden möglichen Täter, für den „Meisterdatendieb" wie auch für den „Gelegenheitsdatendieb", der Wille zur Geheimhaltung unmißverständlich erkennbar.

(4) Sicherungszweck

In Bezug auf die subjektive Komponente werden ebenfalls verschiedene Ansichten vertreten. Die in diesem Zusammenhang möglichen Ansichten können wie folgt klimaktisch aufgegliedert werden.

1. Sicherungszweck kann auch untergeordnetes Nebenziel sein.
2. Sicherungszweck ist zumindest gleichrangiges Ziel eines Motivbündels.
3. Sicherungszweck muß dominierend innerhalb eines Motivbündels sein.
4. Sicherungszweck ist einziges Motiv.

(a) Die Ansichten in der Literatur

Lenckner/Winkelbauer[307] sind der Ansicht, daß Sicherungen, die ausschließlich andere Zwecke verfolgen, sie nennen als Beispiel Feuerschutz, nicht genügen. Deshalb stelle auch die unterirdische Verlegung von Datenfernleitungen keine Zugangssicherung dar, weil diese Verlegeweise nur der störungsfreien Leitungsführung diene. Ebensowenig

---

305 *Hilgendorf*, JuS 1996, 702.

306 So auch *Hilgendorf*, JuS 1996, 702.

307 *Lenckner/Winkelbauer*, CR 1986, 483 (487).

reiche es aus, daß sich die Sicherung lediglich als Nebenwirkung eines komplizierten Betriebssystems darstelle.

Nach *Jähnke*[308] muß die besondere Sicherung den Zweck haben, den Zugang zu verhindern. Anderen Zwecken dienende Maßnahmen, welche nur nebenbei auch den Zugang erschweren, wie feuersichere Türen ohne besonderes Schließsystem, reichten daher nicht aus.

Wenn der Schutz der jeweiligen Daten bloßer Nebeneffekt ist, muß nach *Hilgendorf*[309] eine besondere Zugangssicherung verneint werden. Als Fallbeispiel führt er einen Schuljungen an, der durch ein unzureichend verriegeltes Fenster in die Schule eindringt und sich ein Unterrichtsprogramm vom offen im Klassenzimmer stehenden Schulrechner kopiert. Hier sei nicht der Rechner, sondern die Schule verschlossen gewesen. Es sollten also nicht speziell die Daten geschützt werden, die sich der Schuljunge verschafft hat, sondern das gesamte Gebäude sollte gegen unbefugten Zutritt gesichert werden. Diese allgemeine Zutrittssicherung reiche für § 202a nicht aus.

Diese Äußerungen lassen sich allesamt der 1. Kategorie zuordnen: Der Sicherungszweck muß zumindest untergeordnetes Nebenziel sein.

Jessen[310] sieht eine besondere Sicherung auf der subjektiven Seite dann gegeben, wenn der Berechtigte eine Vorkehrung mit der Zielrichtung installiert, zumindest gleichrangig neben anderen Zielen auch den Schutz von Informationen von einem Verschaffen zu gewährleisten. Dies erschließt er zum einen aus der historischen Auslegung. Hier lehnt er sich stark an die Äußerungen von *Sieber*[311] an. Daneben und das ist sein Hauptargument würde eine Abgrenzung zwischen bloßem Nebeneffekt und nachrangigem Schutzzweck zu erheblichen Abgrenzungsschwierigkeiten führen, die letztlich die Gefahr des Zufalls in sich berge. Die Abgrenzung des nachrangigen Schutzzwecks vom gleichrangigen Schutzzweck ist nach Ansicht von *Jessen* schon praktikabler, da leichter möglich und weniger vom Zufall geprägt. Diese Ansicht läßt sich der zweiten Kategorie zuordnen.

Leicht[312] ist bei der Beurteilung des Sicherungszwecks sehr restriktiv. Er führt an, daß zum Schutz von Daten die vielfältigsten Sicherungsmaßnahmen entwickelt worden sei-

---

308 LK-*Jähnke*, § 202a Rn. 5.

309 *Hilgendorf*, JuS 1996, 702 (703).

310 *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 115, 120.

311 *Sieber*, BT-Anhörung vom 6.6.1984, Anlagen, S. 267.

312 *Leicht*, iur 1987, 45 (47).

en. Wenn nun jede Maßnahme ausreichend sei, die dem Schutz vor unberechtigten Zugang diene, bzw. das formale Geheimhaltungsinteresse erkennen ließe, so sei fraglich, wie weit der geschützte Bereich ausgedehnt werden könne, womöglich sogar bis zum Pförtner am Eingangstor eines großen Unternehmens. Als Eingrenzungskriterium dieser aus seiner Sicht zu weit gehenden Auslegung, führt er an, daß es zu Kollisionen mit Schutzbereichen anderer Normen kommen könne. Folglich will er allein auf den primären Schutzzweck der jeweiligen Sicherung abstellen.[313]

Dies fällt in die 3. Kategorie: Datensicherung als primärer Sicherungszweck. Die 4. Kategorie findet keine Anhänger.

(b) Stellungnahme

Auch hier ist der Verweis des Gesetzgebers für die Auslegung maßgeblich. Bei der subjektiven Komponente gibt es kein Problem im Rahmen der Sicherungen nichtkörperlicher Art. Die Zweckrichtung wird nur vom Verstand gebildet. Sie ist damit unabhängig davon bestimmbar, ob eine körperliche oder nichtkörperliche Einrichtung zu prüfen ist. Dies darf jedoch nicht mit einer rein subjektiven, auf den konkreten Einrichter einer Sicherung abstellenden Sichtweise verwechselt werden. Maßgeblich ist eine Betrachtung der jeweiligen Maßnahme im Sinne eines objektivierten Sicherungszwecks. Zu fragen ist daher, ob die zu prüfende Sicherung auch die Sicherung von Daten bezweckt. Dies ist aus der Sicht eines objektiven Beobachters zu bestimmen. So ist maßgeblich, ob die jeweilige Vorrichtung nach den äußeren Umständen der Datensicherung dient.

Auch bei § 243 Abs. 1 Nr. 2 und § 202 Abs. 2 wird, mit unterschiedlichen Ergebnissen im Einzelfall, lediglich gefordert, daß die sichernde Wirkung nicht bloßer Nebeneffekt ist. Worin bei einer Zweckbündelung der Hauptzweck liegt, ist gleichgültig, sofern dem Sicherungszweck zumindest eine nicht unerhebliche Rolle zukommt.[314] So stellt ein abgeschlossenes Behältnis, in dem sich ein PC befindet, eine besondere Zugangssicherung dar. Daß hier der Hauptzweck die Datensicherung darstellt, kann nicht ohne weiteres behauptet werden. Es kann vielmehr davon ausgegangen werden, daß die Sache PC als solche ebenso oder sogar eher vor Diebstahl als vor Datenausspähung geschützt werden sollte. Die geradezu „klassische“ Sicherung Behältnis nicht als besondere Zu-

---

313 *Schmitz*, JA 1995, 478 (482) ist ebenfalls der Ansicht, daß Vorrichtungen, die nicht in erster Linie den unberechtigten Zugang verhindern sollen, keine Zugangssicherungen seien. Eine Begründung dafür führt er jedoch nicht an.

314 Schönke/Schröder-*Eser*, § 243 Rn. 24; LK-*Ruß*, § 243 Rn. 19; vgl. Hamm, NJW 78, 769.

gangssicherung zu qualifizieren, wegen der Schwierigkeit einen Hauptzweck auszumachen, engt den Tatbestand zu weit ein und erscheint abwegig.

Ob man mit den Vertretern der ersten Kategorie schon einen auch untergeordneten Nebenzweck bejaht, oder nur gleichrangige Ziele für ausreichend erachtet[315], ist im Rahmen der oben dargestellten, von der Einrichtung ausgehenden, objektivierten Ermittlung des Sicherungszwecks schwierig. Wie soll es möglich sein, bei einem abgeschlossenen Computerraum oder einem Behältnis oder selbst einer Paßwortsicherung den objektivierten Sicherungszweck derart scharf abzugrenzen? Der Computerraum schützt eben auch vor dem Eindringen in den Raum selbst und vor Diebstahl; das Behältnis schützt, wie oben schon angemerkt, zumindest auch die Hardware vor Diebstahl; das Paßwort soll auch vor der Datenveränderung oder Datenlöschung schützen. Sind diese Zweckrichtungen innerhalb des Zweckbündels nun gleichrangig oder untergeordnet? Diese Frage kann nicht beantwortet werden, da jede der vorhandenen Sicherungsmöglichkeiten zum Hauptzweck erkoren werden kann, ein objektivierter Hauptzweck ist dagegen nicht per se erkennbar. Folglich ist es der richtige Ansatz, ein besondere Zugangssicherung zu bejahen, wenn ein Datensicherungszweck aus der zu prüfenden Maßnahme erkennbar ist und damit die datensichernde Wirkung nicht bloß gänzlich untergeordneter Nebeneffekt ist.

Die Ansicht *Leichts*[316], die auf einen primären Sicherungszweck abstellt, ist verfehlt. Daß es bei Maßnahmen, die lediglich dem Schutz vor unberechtigtem Zugang dienen, zu Kollisionen mit Schutzbereichen anderer Normen kommen kann, ist unschädlich. Dies wird schon durch das Gesetz selbst widerlegt. In § 243 Abs. 1 Nr. 2 ist von einem Behältnis als Beispiel einer Schutzvorrichtung genannt. Das Behältnis findet sich wieder in § 202 Abs. 2. Beim ersten dient das Behältnis dem Schutz einer Sache vor Diebstahl; das Schutzinteresse ist das Eigentum und der Gewahrsam des Berechtigten. Beim letzteren dient das Behältnis dem Schutz vor Kenntnisnahme einer Information in einem Brief. Hier ist das zugrunde gelegte Schutzinteresse und Rechtsgut das Briefgeheimnis. Ein und dieselbe Maßnahme kann daher bei Einschließen eines Briefes in ein Behältnis dem Eigentumsschutz und dem Schutz des Briefgeheimnisses dienen. Bei Wegnahme und Kenntnisnahme des Inhalts dieses Briefs nach Öffnen des Behältnisses lägen § 202 Abs. 2 und § 243 Abs. 1 Nr. 2 vor. Eine Interessenkollision führt daher nicht dazu, daß die subjektive Komponente auf einen primären Sicherungszweck reduziert werden müßte.

---

315 So *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 115, 120.

316 *Leicht*, iur 1987, 45 (47).

Bei konsequentem Zugrundelegen dieser Ansicht würde letztlich nur noch die Datenverschlüsselung als Zugangssicherung mit primärem Datensicherungszweck übrigbleiben.[317] Bei allen körperlichen Sicherungen kann angenommen werden, daß sie sowohl dem Schutz vor Wegnahme, als auch dem Schutz vor Datenverlust dienen. Bei den übrigen logischen Sicherungen ist der Schutz vor Datenverlust ebenso wichtig, wie der Schutz vor dem Ausspähen der Daten.

Zusammenfassend kann gesagt werden, daß der Datensicherungszweck für einen objektiven Beobachter aus den äußeren Umständen erkennbar sein muß. Dieser kann auch untergeordnet sein. Ein bloß faktischer datensichernder Nebeneffekt ist nicht ausreichend.

3. „Unberechtigt“

a) Meinungsstreit

Zum Merkmal „unberechtigter Zugang“ herrscht einen Meinungsstreit. Dieser soll im Folgenden zur Erläuterung dieses Merkmals dargestellt werden. Anschließend wird dazu Stellung genommen. Der Begriff des Zugangs wurde oben schon geprüft. § 202a spricht jedoch von einem „unberechtigten“ Zugang. Die Bedeutung bzw. Nichtbedeutung dieses Attributs ist streitig.

(1) Gleichsetzung mit „nicht für den Täter bestimmt“

Tröndle[318] ist der Ansicht, daß die Frage, ob der Zugang „unberechtigt“ ist, von der Bestimmung des Verfügungsberechtigten abhängt. Da die Sicherungsmaßnahmen den *„unberechtigen“* Zugang ausschließen müsse, greife § 202a Abs. 1 nur, wenn die Daten für den Täter nicht bestimmt sind **und** die Daten gegen unberechtigten Zugang gesichert sind. In dieselbe Richtung argumentiert auch *Hilgendorf*[319]. Das Gesetz spreche nicht davon, daß die Daten gegen jeden unberechtigten Zugang besonders gesichert sein muß. Erforderlich sei lediglich, daß überhaupt eine Zugangssicherung besteht, und daß sich der Täter die Daten unter Überwindung der Zugangssicherung verschafft.

---

317 So auch *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 99.

318 Tröndle/Fischer-*Tröndle*, § 202a Rn. 7a iVm Rn. 7.

319 *Hilgendorf*, JuS 1996, 702 (704) unter Berufung auf NK-*Jung* (Stand 1995), § 202a Rn. 7.

(2) Keine eigenständige Bedeutung

Jessen[320], der ebenfalls keine eigenständige Bedeutung des Merkmals annimmt, schlägt vor, das Merkmal „unberechtigt" aus dem Gesetzestext zu streichen. Das Merkmal unterstreicht seiner Ansicht nach lediglich die von ihm geforderte Sorgfalt bei der Einrichtung der Sicherungen. Die mögliche Bedeutung des Merkmals ist danach aus seiner Sicht schon im Sicherungsbegriff selbst enthalten.

(3) Umkehrschluß aus „bestimmt"

Lenckner[321] schließt aus der Annahme, daß eine Zugangssicherung per se schon den Zweck hat, Unbefugte auszuschließen, daß in dem Merkmal des „unberechtigten" Zugangs nur eine zusätzliche Einschränkung liegen könne. Er sieht dieses Merkmal im Zusammenhang mit dem zunächst genannten Merkmal, daß die Daten „nicht für ihn (d.Verf.: den Täter) bestimmt" sein dürfen. „Berechtigt" sei der Zugang nur für denjenigen, für den die Daten „bestimmt" seien. Nun folgt der Umkehrschluß, daß dann die Sicherung gegen „unberechtigten" Zugang gegenüber all denjenigen bestehen müsse, für welche die Daten nicht bestimmt seien. Eine Sicherung soll demnach nur tatbestandsmäßig sein, wenn sie jeden abhält, der nicht autorisiert ist. Für das sog. „closed-Shop"-System habe dies zur Folge, daß es nur dann eine besondere Sicherung gegen unberechtigten Zugang darstelle, wenn die ohne weitere Sicherung abfragbaren Daten für alle „closed-shop"-Zugangsberechtigten bestimmt seien; hätten dagegen noch andere Betriebsangehörige ohne weiteres Zutritt, so verlören damit die Daten den Schutz des § 202a auch gegenüber Betriebsexternen. *Lenckner* stellt daraufhin selbst fest, daß eine derartige Auslegung im praktischen Ergebnis darauf hinausläuft, daß der Berechtigte, um den Schutz des § 202a zu erlangen, zu umfassenden Sicherungsmaßnahmen gezwungen ist. Ob dies vom Gesetzgeber so beabsichtigt ist, sei allerdings eine andere Frage.

---

320 *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 141. *Hilgendorf*, JuS 1996, 702 (704) Fn. 18 befürwortet den Streichungsvorschlag.

321 Schönke/Schröder-*Lenckner*, § 202a Rn. 9; *Lenckner/Winkelbauer*, CR 1986, 483 (487). So auch *Meurer*, Die Bekämpfung der Computerkriminalität in Deutschland, in: Festschrift für Kitagawa zum 60. Geburtstag, S. 976; *Schulze-Heiming*, Der strafrechtliche Schutz der Computerdaten, S. 65.

(4) Gedankliche Lückenlosigkeit

Jähnke[322] hingegen sieht im Gegensatz zu *Tröndle*[323]und *Lenckner*[324] keinen Zusammenhang des „unberechtigten" Zugangs mit dem des „Bestimmtseins" der Daten. Zu einem gesicherten Computerzentrum müßten Reinigungskolonnen, Wartungs- und Reparaturdienste, Aufsichts- und Kontrollpersonal Zutritt haben, ohne daß damit die gespeicherten Daten für diesen Kreis bestimmt wären. Mit diesem Merkmal sei vielmehr klargestellt, daß das Sicherungssystem gedanklich lückenlos sein müsse. Es müsse daher nicht bloß Betriebsexterne, sondern auch unberechtigt eindringende Angestellte erfassen. Anderenfalls könnten diese mangels einer tatbestandsmäßigen Handlung, *Jähnke* fordert explizit eine Überwindung der Zugangssicherung[325], nicht belangt werden.

b) Erläuterung am Beispiel des closed-shop-Systems

Der oben dargestellte Meinungsstreit wird unter Anführung der in Unternehmen weit verbreiteten sog. „closed-shop"- Sicherung ausgetragen. Zur Erläuterung der folgenden Ausführungen wird das closed-shop erklärt und sodann die dabei möglichen Fallkonstellationen und die dabei auftretenden Personenkreise aufgezeigt.

Bei einer closed-shop-Sicherung werden EDV-Anlagen in räumlich abgetrennten Bereichen aufgestellt, zu denen dann grs. nur autorisierte Angestellte, für die die betreffenden Daten bestimmt sind i.S.d. § 202a, eine Zutrittsberechtigung haben. Diese Zutrittsbeschränkung wird durchgesetzt mit Schlüsseln, maschinenlesbaren Ausweiskarten, Systemen, welche die Eingabe von Kennziffern bzw. Paßwörtern verlangen, computermäßiger Analyse zur Identifizierung von Unterschriften oder der Analyse der Handgeometrie, des Fingerabdrucks, der Sprache (sog. biometrische Verfahren).[326]

Problematisch sind die durchaus nicht nur „akademischen" Konstellationen, daß der Kreis der Personen, für welche die Daten nicht bestimmt sind, und der, die vom Zugang ausgeschlossen sind, auseinanderfallen. Hierzu ein Beispiel[327]: Ein Unternehmen, welches über ein closed-shop-System verfügt, untersagt den im Sicherheitsbereich mit den Unternehmensdaten arbeitenden Angestellten nach der regulären Arbeitszeit mit den

---

322 LK-*Jähnke*, § 202a Rn. 15.

323 Tröndle/Fischer-*Tröndle*, § 202a Rn. 7a.

324 Schönke/Schröder-*Lenckner*, § 202a Rn. 9.

325 LK-*Jähnke*, § 202a Rn. 15 iVm 7.

326 Vgl. *Leicht*, iur 1987, 45 (48).

327 Angelehnt an Fall 9 in *Hilgendorf*, JuS 1996, 702 (703).

Daten zu arbeiten. Zur Sicherung ändert einer dieser Mitarbeiter (P) jeden Abend den Code der Schließanlage an der Tür zum gesicherten EDV-Bereich. Für diesen gilt das oben genannte Verbot ebenso. Hier hat P auch außerhalb der Arbeitszeit faktische Zutrittsmöglichkeit, ohne daß die Daten für ihn bestimmt wären.

Der Beispielsfall kann nun noch erweitert werden: Zur Reinigung der closed-shop-Räume hat einmal pro Woche das Reinigungspersonal des Unternehmens Zutritt zum gesicherten Bereich. Hier darf das Reinigungspersonal dann die Räume betreten, hat damit berechtigten Zugang zu den Räumen, Daten sind dennoch nicht für sie bestimmt.

(1) Fallkonstellationen

Es kann daher abstrakt zwischen drei Fallkonstellationen unterschieden werden:

Fall 1: Nur Personen, für die die Daten bestimmt sind haben faktische und berechtigte („datenbestimmte") Möglichkeit an die EDV-Anlagen heranzukommen. (Beispiel: EDV-Mitarbeiter mit Rund-um-die-Uhr-Berechtigung)

Fall 2: Personen, für die die Daten bestimmt sind, und solche für die die Daten nicht bestimmt sind, haben Zugangsberechtigung zu den Räumlichkeiten und faktische Zugriffsmöglichkeit auf die Daten (Beispiel: EDV-Mitarbeiter mit Rund-um-die-Uhr-Berechtigung + Reinigungs-und Hardwarewartungspersonal), weitere Personen haben keine faktische Zugangsmöglichkeit

Fall 3: Personen, für die die Daten bestimmt sind, solche die ohne Datenbestimmung berechtigt sind, die Räumlichkeiten zu betreten, und solche, die nicht einmal die Räume betreten dürfen, haben faktisch Zugriffsmöglichkeit auf die Daten (EDV-Mitarbeiter mit Rund-um-die-Uhr-Berechtigung + Reinigungs- oderHardwarewartungspersonal + sonstige Mitarbeite mit Ersatzschlüssel ohne jegliche Berechtigung)

(2) Lösung nach den verschiedenen Ansichten

Nach der „Umkehrschluß-Theorie"[328] *Lenckners* wäre Fall 1 die einzige Konstellation beim Closed-shop-System, bei der eine besondere Sicherung gegen unberechtigten Zugang vorläge. Die Sicherung besteht gegen alle, für die die Daten nicht bestimmt sind. Bei Fall 2 und 3 ist der Kreis derer, die die Möglichkeit zum Zugriff auf die Daten haben, größer als der Kreis derjenigen, für die die Daten nicht bestimmt sind.

---

328 Schönke/Schröder-*Lenckner*, § 202a Rn. 9; *Lenckner/Winkelbauer*, CR 1986, 483 (487); *Meurer*, Die Bekämpfung der Computerkriminalität in Deutschland, in: Festschrift für Kitagawa zum 60. Geburtstag, S. 976; *Schulze-Heiming*, Der strafrechtliche Schutz der Computerdaten, S. 65.

Im Rahmen der „Theorie von der gedanklichen Lückenlosigkeit“[329] wird das Merkmal „unberechtigt“ ohne Bezugnahme zur Datenbestimmung ausgelegt. „Berechtigt“ ist der Zugang als die Möglichkeit zum Zugriff auf Daten dann, wenn die Daten für jemanden bestimmt sind oder der Verfügungsberechtigte willentlich faktische Zugriffsmöglichkeit zu den Daten gibt. Der Verfügungsberechtigte muß danach alle, die nicht „berechtigt“ sind, mit Hilfe der Sicherung von den Daten wirksam fernhalten. Ist „gedanklich lükkenlos“ so zu verstehen, so würde die Konstellation des Fall 3 das Merkmal „unberechtigt“ i.S.d. § 202a Abs. 1 nicht erfüllen.

Aus der Äußerung *Jähnkes*, daß bei einer nicht gedanklich lückenlosen Sicherung im Falle des Eindringens unberechtigter Angestellter, diese mangels einer tatbestandsmäßigen Handlung nicht belangt werden könnten[330], spricht jedoch eher eine konkrete Sichtweise. Gedanklich lückenlos hieße in diesem Fall lediglich, daß der Betriebsinhaber darauf zu achten hat, auch nicht zugangsberechtigte Angestellte wirksam auszuschließen, damit diese sich bei Zuwiderhandlung auch strafbar machen würden. Falls dies so gemeint ist, ergeben sich gegenüber der Ansicht, die „unberechtigt“ mit der Datenbestimmung gleichsetzt, keine anderen Ergebnisse, da auch diese auf die Überwindung der Sicherung im konkreten Fall abstellt.

Bei der „Gleichsetzungs-Theorie“[331] würde auch die Konstellation des Fall 3 eine besondere Sicherung gegen unberechtigten Zugang darstellen, falls ein Betriebsexterner die Sicherungsmaßnahmen zu überwinden trachtet. Für alle Betriebsinternen, die unberechtigterweise faktischen Zugang zu den Daten haben, liegt jedoch eine Sicherung i.S.d. § 202a nicht vor.

c) Stellungnahme

Lenckners Ansicht würde dazu führen, daß der Verfügungsberechtigte zu umfassenden Sicherungsmaßnahmen gezwungen sein würde, um in den Schutz des § 202a zu gelangen.[332] Diese Maßnahmen würden für den Großteil der Betriebsinhaber an die Grenze des Machbaren und Finanziellen gehen. Um dennoch in den Schutz zu gelangen, müßte der verfügungsberechtigte Arbeitgeber allen, die auch nach der Arbeitszeit faktische Zugriffsmöglichkeit zu den Daten haben, auch die rechtliche Zugriffsbefugnis einräu-

329 LK-*Jähnke*, § 202a Rn. 15.

330 LK-*Jähnke*, § 202a Rn. 15.

331 Tröndle/Fischer-*Tröndle*, § 202a Rn. 7a iVm Rn. 7; *Hilgendorf*, JuS 1996, 702 (704).

332 Dieses Ergebnis räumt Schönke/Schröder-*Lenckner*, § 202a Rn. 9 selbst ein.

men, damit eine Zugangssicherung i.S.d. § 202a Abs. 1 vorliegt. Dies ist paradox. Der Betriebsinhaber müßte Befugnisse erteilen, die er logischerweise sonst nicht geben würde. Ein Betriebsinhaber möchte im Allgemeinen nicht, daß viele Personen auch des Nachts ohne Kontrolle an seine Daten herankommen können. Hätten diese Mitarbeiter dann auch noch die Befugnis dazu, so wäre ein arbeitsrechtliches oder schadenersatzrechtliches Vorgehen dagegen ausgeschlossen oder zumindest erheblich eingeschränkt. Er müßte sich folglich eines Teils des zivilrechtlichen Schutzes begeben, um den strafrechtlichen auch gegenüber Betriebsexternen zu erhalten. Es kann nicht angenommen werden, daß ein Betriebsinhaber sich dieses Dilemmas überhaupt bewußt ist, so daß er sich gar keine Gedanken darüber macht, die Sicherungsmaßnahmen auszuweiten, oder sich für den einen oder anderen Schutz zu entscheiden. Damit läge sehr häufig keine Sicherung im Sinne des § 202a Abs. 1 vor, so daß die Norm bei dieser engen Auslegung weitgehend an Bedeutung verlöre.[333] Dies kann nicht im Sinne des Gesetzgebers und auch nicht Sinn der Regelung selbst sein.

Wird die Ansicht *Jähnkes*[334] (gedankliche Lückenlosigkeit) so verstanden, daß die Sicherung, um als solche i.S.d. § 202a gelten zu können, gedanklich alle ausschließen muß, die keinen Zugang zu den Daten haben sollen, so ergeben sich auch hier, zwar nicht ganz so extrem wie bei *Lenckner*, vergleichbare Probleme in der Auswirkung dieser Auslegung. Es müssen alle ausgeschlossen werden, für die die Daten nicht bestimmt sind, oder die keinen sonstigen berechtigten faktischen Zugang zu den Daten haben (z.B. Reinigungspersonal). Auch hier fällt das „Kartenhaus" Sicherung insgesamt zusammen, falls nur eine Person, die nicht einmal in sonstiger Weise Zugang zu den Daten erhalten hat, die vom Verfügungsberechtigten zu verantwortende ungehinderte Möglichkeit zum Zugang zu den Daten hat. Wie oben wäre dann für jeden anderen das Eindringen in geschützte Systeme sogar bei Überwindung der konkret wirksamen Sicherung nicht tatbestandsmäßig. Auch diese Auslegung setzt zu hohe Maßstäbe an die Sicherungsmaßnahmen des Verfügungsberechtigten. Es ist nicht einzusehen, daß ein Betriebsexterner straflos bleibt, für den die Sicherung vornehmlich eingerichtet wurde, nur weil ein Betriebsinterner faktischen Zugang zu den Daten hat.

Der Wortlaut gibt nicht her, daß die Daten gegen **jeden** unberechtigten Zugang besonders gesichert sein müssen.[335] Zweck des § 202a ist es, Unberechtigte von Daten auszuschließen. Besteht gegenüber dem einen Täter eine Sicherung, so kann dieser sich nicht

---

333 So auch *Hilgendorf*, JuS 1996, 702 (704).

334 LK-*Jähnke*, § 202a Rn. 15 iVm 7.

335 *Hilgendorf*, JuS 1996, 702 (704).

darauf berufen, daß sie für einen anderen nicht bestand. Für diesen war zum Zeitpunkt der Tat eine Sicherung vorhanden, die das Geheimhaltungsinteresse des Verfügungsberechtigten dokumentierte. Der Gleichsetzungstheorie ist damit als die dem Wortlaut und dem Zweck des § 202a nächste Ansicht zu folgen.

4. Sonderproblem: Überwindung der Zugangssicherung

Die h.M. fordert, daß die besondere Sicherung gegen unberechtigten Zugang überwunden werden muß, damit § 202a überhaupt erfüllt werden kann. Die Frage nach dem Personenkreis, für den die Sicherung Wirkung entfalten soll, oder entfaltet, beschränkt sich damit offensichtlich nicht auf die Auslegung des Merkmals des „unberechtigten" Zugangs.

a) Personalisierte versus nicht-personalisierte Perspektive

Zunächst ist bei der Beantwortung der Frage, ob die Sicherung überwunden werden muß oder nicht von Interesse, ob das Gesamtmerkmal „besondere Sicherung gegen unberechtigten Zugang" mit Blick auf den konkreten Täter betrachtet werden muß, oder ob auch eine von den Daten ausgehende Sichtweise vertretbar erscheint. Es ist folglich zu entscheiden, ob die Sicherung für den konkreten Täter grs. wirksam sein muß, oder ob es ausreicht, wenn sie als solche funktionsfähig vorhanden ist, gegebenenfalls ohne daß sie auch nur im Geringsten konkrete Wirksamkeit entfaltet. Diese verschiedenen Ansätze werden hier personalisierte oder nichtpersonalisierte Perspektive genannt.

Lenckner führt für seine Ansicht zur Auslegung von „unberechtigt" ins Feld, daß die besondere Sicherung nach Wortlaut des § 202a sich nicht **speziell** gegen den Täter richten müsse, da sonst der Wortlaut „...die **ihm gegenüber** gegen unberechtigten Zugang besonders gesichert..." hätte heißen müssen.[336] Dies sei jedoch im Ergebnis das, was *Tröndle* vertreten würde.[337] Was *Lenckner* mit „speziell für den Täter" gemeint haben könnte, bleibt jedoch im Dunkeln. Er kann damit jedenfalls nicht gemeint haben, daß der eine Sicherung Einrichtende in Kenntnis der Identität des Täters die Sicherung gerade auch für diesen eingerichtet haben muß. *Tröndle* vertritt dies mitnichten. Dieser ist lediglich der Ansicht, daß die Sicherung gegenüber dem jeweiligen Täter eine Sicherungswirkung entfalten muß, und nimmt damit eine Sichtweise ein, die von dem kon-

---

336 Schönke/Schröder-*Lenckner*, § 202a Rn. 9.

337 Schönke/Schröder-*Lenckner*, § 202a Rn. 9.

kreten Täter aus die Sicherung betrachtet.[338] Die Sicherung muß zum Zeitpunkt der Tathandlung gegen den Täter gerichtet und wirksam sein. Es wird damit vom konkreten Täter aus geprüft, ob die Sicherung ihm gegenüber Wirkung entfaltet. Diese Sichtweise soll hier **personalisierte Perspektive** genannt werden.

Möglicherweise könnte nun *Lenckner*[339] ausgehend vom Wortlaut von einer nicht-personalisierten Sichtweise ausgegangen sein, die den Blick auf die Daten richtet, nicht auf den Täter. Ausreichend wäre dann allein das Vorliegen einer Sicherung der Daten gegen Zugang, die das Geheimhaltungsinteresse des Verfügungsberechtigten unmißverständlich zum Ausdruck bringt. Die Sicherung müßte dann jedoch grs. nicht gegenüber dem konkreten Täter wirksam sein. Mindestvoraussetzung wäre dann, daß eine Sicherung als solche auch erkennbar wäre Dies wäre bei einer Paßwortsicherung z.B. auch dann gegeben, wenn das Paßwort zu den Daten auf einem Zettel geschrieben am Bildschirm klebt. Als weitere Konstellation läßt sich der Fall anführen, daß der Täter das Paßwort von einem Dritten erhalten hat. Auch hier wäre eine als Sicherung gedachte Einrichtung noch vorhanden, so daß dem Täter klar würde, daß der Verfügungsberechtigte die nicht unmittelbar wahrnehmbaren Informationen geheim halten möchte.

Eine solche von den Daten ausgehende **abstrakte, bzw. nicht-personalisierte Perspektive** ist vom Wortlaut des § 202a umfaßt. Der Wortlaut verlangt zunächst lediglich, daß eine Sicherung eingerichtet sein muß; daß eine Sicherung als solche vorhanden ist, die den Schutz der Daten verfolgt und diesen auch objektiv fördert. Dies ist grs. vertretbar, ohne gegen das Bestimmheitsgebot aus Art. 103 Abs. 2 GG zu verstoßen, da der Wortlaut des § 202a insoweit offen ist. Jedoch zieht *Lencker* aus der von ihm selbst angedeutete Perspektive keine weiteren Konsequenzen.[340] Seine zu restriktiven Ergebnissen führende Auslegung von „unberechtigt“ führt dazu, daß sich jede Sicherung abstrakt wie auch konkret gegen jeden möglichen Täter richten muß, da der mögliche Täterpersonenkreis identisch ist mit demjenigen, vor dem die Sicherung präventiv schützen muß. Im Ergebnis wäre dasselbe auch mit einer auf den konkreten Täter abzustellenden Sichtweise erzielt worden, so daß dieser Ansatz für die Auslegung *Lenckners* keine Auswirkung hat, da sie sich allein aus dem Merkmal „unberechtigt“ erschließen läßt (Umkehrschluß).

---

338 Tröndle/Fischer-*Tröndle*, § 202a Rn. 7.

339 Schönke/Schröder-*Lenckner*, § 202a Rn. 9.

340 Siehe auch *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 142.

Die faktisch-personalisierte (*Lenckner* und *Jähnke*) oder real-personalisierte (*Tröndle* und *Hilgendorf*) Sichtweise führt dazu, daß die Sicherung zunächst gegenüber dem konkreten Täter wirksam sein muß. Beide Sichtweisen stellen die Forderung nach der Überwindung der Zugangssicherung, welches sich als logische Kehrseite zur Wirksamkeitsforderung darstellt.[341] Wenn der Täter die Sicherung überwinden muß, ist gleichzeitig der Nachweis ihrer Wirksamkeit erbracht.

b) Überwindung der Sicherung

Was „Überwindung der Zugangssicherung" sein soll, wird jedoch nicht definiert. Dies ist insofern problematisch, als logische Datensicherungen immer nur jeweils einen Zugangsweg schützen können. Ist nun allein das Eintippen des vorher ermittelten Paßwortes Überwinden der Sicherung, oder kann das (intelligente) Umgehen der Sicherung auch als „Überwindung" erachtet werden?

Mit der Frage der Umgehung der Sicherung und damit mit dem Ablehnen eines Überwindungserfordernisses setzt sich im Schrifttum bisher allein *Jessen*[342] auseinander. Er fordert lediglich einen erhöhten Sicherungsgrad. Die Sicherung muß die Daten gegen alle wahrscheinlichen Vorgehensweisen durch qualifizierte Maßnahmen schützen. Aus der Einschränkung der Angriffsrichtungen ergebe sich dann zwangsläufig, daß Lücken in der Sicherung der Informationen bestehen können. Dieses Risiko nochmals dem Dateninhaber aufzuerlegen, sei bei der Vielzahl der vorstellbaren Umgehungsmöglichkeiten nicht Sinn und Zweck des § 202a Abs. 1. [343] Ein Überwinden der Zugangssicherung ist danach nicht erforderlich; Umgehen der grs. auch gegenüber dem Täter wirksamen Sicherung reicht aus.

Man könnte auch einen anderen Ansatz wählen. Als Überwinden der Zugangssicherung kann auch deren Umgehen gewertet werden. Die Sicherung, die den Täter zu einem erheblichen Umweg zwingt, der zumindest für den Laien nicht ohne weiteres ersichtlich und machbar ist (Sicherungsgrad), wird durch deren Umgehung „überwunden". Eine Umgehung kann folglich theoretisch auch dem Überwinden der Sicherung gleichgesetzt werden. Die Überwindung der Sicherung eindeutig zu bestimmen, stellt sich somit bei Anschauung des Umgehens der Sicherung als nicht gerade einfach dar.

---

341 Auch *Schmitz*, JA 1995,478 (483) fordert die Überwindung der Zugangssicherung. Ebenso *Celle* CR 1990, 277 mit Anmerkung *Etter*. Bei Tröndle/Fischer-*Tröndle*, § 202a Rn. 9 wird auf das Überwinden der Sicherung nicht explizit eingegangen.

342 *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 121 ff.

343 *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 123.

Des weiteren ist problematisch, wenn jemand die Vorarbeit eines anderen lediglich ausnutzt. So ist fraglich, wie der Fall zu lösen ist, daß jemand ein Paßwort von einem Dritten erhält, der dies vorher „geknackt“ hatte. Ist nun das Eintippen des Paßwortes ein Überwinden der Zugangssicherung? Dies könnte durchaus bejaht werden, denn Überwinden kann auch objektiv ausgelegt werden. Dann wäre es ohne Belang, auf welche Weise der Täter den „Schlüssel“ erhalten hat. Es käme allein darauf an, ob der Täter genau den geschützten Weg zu den Daten nahm, um zu den Daten zu gelangen. Bei subjektiver Auslegung kann von einem Überwinden der Sicherung wohl kaum gesprochen werden. Danach wäre für den konkreten Täter eine geistige oder körperliche „Überwindungs“-Anstrengung zu fordern. Eine solche ist bei Eingabe eines schon bekannten Paßwortes schwerlich zu bejahen.

Jähnke ist explizit der Ansicht, daß es nicht genügt, wenn der Täter eine von anderen geschaffene Lage lediglich für sich ausnutzt. Es bliebe somit straflos, wenn der Täter den versehentlich unverschlossen gebliebenen Computerraum betritt und die Daten abruft, wenn er einem am Datengerät sitzenden Mitarbeiter über die Schulter sieht oder ein Fernglas benutzt.[344] Diese Fallgestaltungen sind jedoch nicht ergiebig, da bei allen die Sicherung zum Zeitpunkt der Tathandlung nicht aktiviert war. Was als solches gar nicht wirkt, kann offensichtlich nicht überwunden werden. Bei dem obigen Paßwort-Fall ist die Sicherung als solche aktiviert. Sie wirkt nur nicht gegenüber dem Täter, der das Paßwort schon erhalten hat. Dieser Täter nutzt aus, daß ein Dritter die Sicherung überwunden hat. Ist dieses Vorgehen bloßes Ausnutzen einer von einem anderen geschaffenen Lage, oder doch Überwinden der Zugangssicherung? Dies erschließt sich jedenfalls nicht auf den ersten Blick.

Man kann aus den obigen Ausführungen ersehen, wie schwer sich die Qualifizierung der Überwindung der Zugangssicherung gestaltet, so daß allein das Postulat einer Überwindung ohne weitere Ausführungen problematisch erscheint. Darüber hinaus ist das Hauptargument der h.M., die eine Überwindung fordert, kritikwürdig. So wird hier argumentiert, daß erst die Überwindung der Zugangssicherung kriminelle Energie manifestiere.[345] Hier stellt sich jedoch die Frage, wer zu bestimmen hat, daß kriminelles Un-

---

344 LK-*Jähnke*, § 202a Rn. 7.

345 LK-*Jähnke*, § 202a Rn. 7; *Lenckner/Winkelbauer*, CR 1987, 483 (486). Unentschlossen *Haß*, Der strafrechtliche Schutz von Computerprogrammen, in: Lehmann (Hrsg.), Rechtsschutz und Verwertung von Computerprogrammen, S. 482 Rn. Rn. 23. *Leicht*, iur 1987, 45 wird von LK-*Jähnke*, § 202a Rn. 7 fälschlicherweise zitiert. Dieser fordert nicht die Überwindung der Sicherung. Er spricht lediglich davon, daß gegenüber dem Täter deutliche Schranken zu setzen sind, die ihn sein rechtswidriges Verhalten bei deren Überwindung oder **Umgehung** erkennen lassen.

recht begründet wird. Zunächst ist hier zu sagen, daß die Frage, was „kriminell“ oder Kriminalität denn eigentlich bedeutet, eine Kernfrage der Kriminologie darstellt. H.M. ist hier der zu bejahende sog. Labeling-Ansatz.[346] Vereinfacht dargestellt wird hier vertreten, daß es kriminelle Handlungen als solche zunächst nicht gibt, sondern daß sie durch den Gesetzgeber erst zu solchen gemacht werden. Der Gesetzgeber definiert, was Kriminalität ist. Wird daher von „kriminell“ und „krimineller Energie“ gesprochen, begibt man sich auf dünnes Eis, gerade wenn es um die Auslegung eines Straftatbestandes, wie § 202a Abs. 1, geht. So kann eben gerade nicht eine Kriminalität mit-definierende Norm tautologisch mit Hilfe der Aussage ausgelegt werden, wann ein entsprechendes Vorgehen „kriminell“ wird, oder sich „kriminelle Energie manifestiert“, so daß ab da der Tatbestand dieser Norm zu bejahen wäre.

Das Parlament hat die Befugnis zu bestimmen, welches Verhalten strafbar ist und welches nicht. Wenn nun entgegen dem Wortlaut des § 202a gesagt wird, kriminelles und damit strafbares Verhalten beginne erst mit der Überwindung der Zugangssicherung, ist dies zwar kein Verstoß gegen den Bestimmtheitsgrundsatz aus Art. 103 Abs. 2 GG (lex stricta), da sich dies zugunsten möglicher Täter auswirkt. Diese Aussage widerspricht jedoch eindeutig dem Willen des Gesetzgebers, der eine solche Überwindung der Sicherung gerade nicht fordert, sondern lediglich ein Verschaffen der Daten.[347] Vorzugswürdig ist daher dem Wortlaut des § 202a zu folgen. Ob die Sicherung im Einzelfall überwunden wurde, ist damit unerheblich.[348]

Der eigene Ansatz wird im Folgenden zusammenfassend erläutert. Bei den physikalischen Sicherungen (z.B. Behältnis) gilt das oben Gesagte.[349] In Anlehnung an § 243 Abs. 1 Nr. 2 sind nur solche körperlichen Sicherungen als solche anzusehen, die die Daten insofern umfassend schützen, als sie nur überwunden werden können und nicht umgangen.

Bei den logischen Sicherungen sind andere Voraussetzungen anzulegen, da diese tatsächlich keinen umfassenden Schutz bieten können. Nach der vorzugswürdigen, nichtpersonalisierten (abstrakten) Sichtweise ist nicht erforderlich, daß die Sicherung zum Zeitpunkt der Tathandlung gegenüber dem Täter wirksam ist. Folglich ist es unerheblich, ob der Täter den geschützten Weg zu den Daten eingeschlagen hat oder einen anderen nicht geschützten, oder ob er den geschützten Weg eingeschlagen hat, der vorge-

---

346 Vgl. *Kunz*, Kriminologie, § 20 Rn. 1 ff. insbesondere Rn. 12.

347 Siehe dazu Seite 106 ff.

348 *Möhrenschlager*, wistra 1986, 128 (140); Lackner/Kühl-*Kühl*, § 202a Rn. 4.

349 Siehe Seite 71 ff.

sehene Schutz jedoch nicht oder nicht mehr auch nur in geringster Weise dem Täter Mühe bereitet.

Unerläßlich ist jedoch, daß eine funktionsfähige Einrichtung als solche zum Zeitpunkt der Tathandlung noch vorhanden ist, so daß damit der Geheimhaltungswille des Verfügungsberechtigten objektiv erkennbar bleibt. Folglich kann auch eine Zugangssicherung im Sinne des § 202a zu bejahen sein, die im konkreten Fall keine Sicherungswirkung erzielt. Für das Erfordernis einer Überwindung der Sicherung ist aus dem Wortlaut des § 202a Abs. 1 nichts zu entnehmen. Tathandlung des § 202a ist das Verschaffen der Daten und nicht die Überwindung der Sicherung, oder das Verschaffen der Daten unter Überwindung der Sicherung.

Jede logische Sicherung kann jeweils nur eine Zugangsart zu den Daten erschweren. Dem Berechtigten ist es unmöglich, alle Wege zu schützen. Damit ist letztlich entscheidend, ob die Sicherung den Geheimhaltungswillen des Berechtigten unmißverständlich zum Ausdruck bringt. Es ist daher nur zu fordern, daß der Berechtigte zumindest die für den Laien üblichen Zugangsarten für diesen wirksam schützt. Auch dem versierten Anwender und Computerspezialisten ist hier der Wille zur Geheimhaltung objektiv erkennbar.

Zur Erläuterung mögen folgende Fallkonstellationen dienen:

Fall 1: A dringt in den Hauptrechner der Firma X ein, welcher mit einem Paßwortschutz versehen wurde. Nun gibt A das Paßwort an seinen Freund B weiter, der sich darauf freut, sich auch einmal ein paar interessante Daten dieser Firma auf seinen Rechner zu kopieren.

B dringt auf dem geschützten Weg in den Hauptrechner ein. Hier ist nun nach h.M. ein Überwinden der Zugangssicherung zu prüfen. Ein „Umgehen der Sicherung“ ist, da er den geschützten Weg zu den Daten nimmt, nicht gegeben. Wie oben schon angemerkt ist auch und gerade in diesem Fall ein Überwinden der Sicherung nicht einfach zu bejahen. Entfaltet die Sicherung überhaupt noch eine Wirkung, wenn der Täter nur noch das von ihm nicht selbst herausgefundene Paßwort einfach eingibt?

Nach der hier vertretenen Ansicht ist eine Sicherung gegen unberechtigten Zugang zu bejahen. Die Einrichtung des Paßwortschutzes ist als solches zum Zeitpunkt der Tathandlung funktionsfähig gewesen. Daß die Daten präventiv gesichert werden sollten, war objektiv erkennbar. Damit dokumentierte die Sicherung den Geheimhaltungswillen des Berechtigten.

Fall 2: A knackt das Sicherungssystem eines kommerziellen Internet-Dienstleisters, der damit gewährleisten möchte, daß nur diejenigen Zugriff auf die eigenen Internet-Seiten haben, die im voraus dafür bezahlen und dann das individuelle Paßwort erhalten. A veröffentlicht die Methode, das System zu knacken auf seiner Homepage. B nutzt dies aus und kann sich auf den entsprechenden Seiten frei bewegen.

Auch hier wählt der Täter den geschützten Zugangsweg. Ob jedoch von einem „Überwinden" der Zugangssicherung gesprochen werden kann, ist fraglich. Die h.A., die ein solches fordert, würde dies wohl bejahen.[350] Dies erscheint im Ergebnis auch richtig zu sein, da es nicht darauf ankommen kann, auf welche Weise der Täter das Know-how zum eigenen Knacken des Schutzes erwirbt. Nach der hier vertretenen Ansicht ist eine Sicherung gegen unberechtigten Zugang wie in Fall 1 gegeben.

Abwandlung 1: A bietet auf seiner Homepage einen Link zu den geschützten Seiten an, die dann von dort aus ohne weitere Zwischenschritte geöffnet werden können. B klickt diesen Link an und gelangt ohne weiteres zu diesen Seiten. Er weiß, daß er nur von den Internet-Seiten des A auf diese Seiten ohne eigene Kenntnis und Eingabe des Paßworts springen kann.

In diesem Fall wäre auch nach der Ansicht von *Tröndle* und *Hilgendorf* § 202a schon der objektive Tatbestand zu verneinen. Die Sicherung entfaltet gegenüber dem konkreten Täter keinerlei Wirkung. Eine solche wird jedoch von dieser Ansicht gefordert. Eine Sicherung i.S.d. § 202a ist danach nicht gegeben. Nach der hier vertretenen Ansicht ist dieser Fall jedoch gleich wie die vorangehenden zu behandeln. Eine grs. funktionsfähige Sicherung ist als solche vorhanden. Sie erstreckte sich gedanklich auch auf den Täter B. Damit war die Sicherung bestimmt und geeignet den Geheimhaltungswillen des Berechtigten zu dokumentieren.

Abwandlung 2: Wie Abwandlung 1, B weiß jedoch von nichts.

Man könnte hier anzweifeln, ob die Sicherung den Geheimhaltungswillen des Berechtigten dokumentiert, da B nichts von der Sicherung weiß. Dies wird jedoch erst auf der Ebene des subjektiven Tatbestandes relevant, da dem B der Vorsatz bezüglich der Sicherung fehlt. Ob die Sicherung ausreichend den Geheimhaltungswillen dokumentiert, ist objektiv zu bestimmen. Bei der gedachten geschützten Zugangsart wäre eine Sicherung als solche klar erkennbar gewesen.

---

350 A.A. *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 154 ff.

Abwandlung 3: A verändert das System derart, daß es keinerlei Sicherungswirkung mehr entfalten kann. A bietet einen Link zu diesen Seiten an. B klickt diesen an. Er weiß, daß diese Seiten gesichert waren.

Die Sicherung ist in diesem Fall zum Zeitpunkt der möglichen Tathandlung nicht mehr vorhanden. Nach allen Ansichten wäre hier § 202a zu verneinen.

5. Zusammenfassung

1.) „Zugang zu Daten" ist jede technische und physikalische Einwirkungsmöglichkeit auf Datenspeicher und den physischen Zugang zum System und Sicherheitsbereich.

2.) Eine besondere Sicherung ist dann gegeben, wenn der erforderliche Sicherungszweck und Sicherungsgrad gegeben ist.

Der Datensicherungszweck muß für einen objektiven Beobachter aus den äußeren Umständen erkennbar sein. Dieser kann auch untergeordnet sein. Ein bloß faktischer datensichernder Nebeneffekt ist nicht ausreichend.

Der erforderliche Sicherungsgrad und damit die Eignung zur Dokumentation des Geheimhaltungswillens ist dann erfüllt, wenn es für den Computerlaien nicht ohne weiteres möglich ist, die Sicherung zu überwinden.

3.) „Unberechtigt" ist ein Zugang, wenn die Daten nicht für den Täter bestimmt sind. Dieses Merkmal korrespondiert damit mit dem Merkmal der Datenbestimmung und ist deklaratorischer Art.

4.) Ob die Sicherung im Einzelfall überwunden oder umgangen wurde, ist nicht erheblich. Eine Sicherung muß als solche mit dem erforderlichen Sicherungsgrad und Sicherungszweck funktionsfähig vorhanden sein.

6. Problemfälle

a) Datenverschlüsselung

Der Gesetzgeber wollte nicht nur gespeicherte Daten, sondern auch solche in den Schutzbereich des § 202a Abs. 1 einbeziehen, die sich im Übermittlungszustand befinden.[351] Der Anteil der im Übermittlungszustand befindlichen Daten nimmt im Zuge der

[351] BT-Drs. 10/5058, S. 28.

Expansion des Internet immer mehr zu. Hier gibt es für Hacker viele Möglichkeiten, diese Daten aufzufangen. Nun stellt sich zunächst auf der tatsächlichen Seite die Frage, wie solche Daten vor „Ausspähung“ gesichert werden können.

(1) Sicherungsverfahren

Besondere Angriffsziele bei der Datenfernübertragung sind frei zugängliche Leitungspunkte wie Erdverkabelungsanschlüsse, Verteilerkästen oder die Telefonanschlüsse in offenen Netzen. Physische Schutzmaßnahmen zur Sicherung gibt es nur eingeschränkt und die möglichen Maßnahmen sind sehr aufwendig.[352] So können Daten, die über metallische Kabel übertragen werden, leicht mit Hilfe einer direkten Kabelanbindung oder indirekt über induktive Abkopplung des Signals abgerufen werden.[353] Hier können sehr aufwendige Maßnahmen, wie Bleiabschirmung gegen das Austreten abhörbarer elektromagnetischer Strahlung oder bessere Kabelummantelungen, die das direkte Anzapfen effektiv verhindern können, eingesetzt werden. Diese sind als besondere Sicherungen i.S.d. § 202a Abs. 1 anzusehen, da sie zumindest auch den Zweck verfolgen, Daten vor unbefugtem Zugang zu sichern. Der datensichernde Effekt bei einer unterirdischen Verlegeweise ist jedoch bloßer Nebeneffekt und damit liegt hier keine besondere Sicherung i.S.d. § 202a vor.[354]

Es bleibt als wohl einzig ökonomisch vertretbare Möglichkeit, die sonst ohne weiteres abzweigbaren Daten auf eine solche Weise zu schützen, daß der Täter mit den erlangten Daten nichts anfangen kann.[355] Der Täter hat im allgemeinen Interesse am Bedeutungsgehalt oder der Funktion der Daten. Werden Daten dahingehend verändert, daß der Bedeutungsgehalt nur dem Absender der Daten und dem Empfänger zugänglich ist, so kann tatsächlich das Datum auf seiner semantischen (d.h. Bedeutungs-) Ebene geschützt werden. Eine solche Veränderung der Daten wird über Datenverschlüsselung erreicht (auch Kryptographie, Chiffrierung).[356] Durch dieses Vorgehen werden die Ursprungsdaten (sog. Klartext) mit Hilfe mathematischer Transformation in andere Daten umge-

---

352 So auch *Weck*, Datensicherheit, S. 282 f.

353 Ausführlich dazu *Leicht*, iur 1987, 45 (51).

354 *Schulze-Heiming*, Der strafrechtliche Schutz der Computerdaten, S. 73.

355 So auch Tröndle/Fischer-*Tröndle*, § 202a Rn. 7a. Auch nach *Hilgendorf*, JuS 1996, 702 (702) Fn. 7 sind Datenverschlüsselungen derzeit offenbar die einzige Möglichkeit, um Daten im Übermittlungszustand wirksam zu schützen.

356 Die Lehre von der Informationsver- und entschlüsselung heißt Kryptologie und ist Oberbegriff der Kryptographie (Verschlüsselungsverfahren) und der sog. Kryptoanalyse. Bei der Kryptoanalyse geht es um die Feststellung der Sicherheit der Verschlüsselung (Entschlüsselungsverfahren).

wandelt, d.h. in Daten mit einem anderen, oder meist keinem Informationsgehalt (sog. Schlüsseltext).[357]

Eine einfache Möglichkeit der Verschlüsselung ist die Festlegung eines Alphabets, bei dem die Zeichen in einer bestimmten Reihenfolge stehen. So kann mit einer Verschiebung des Originalzeichens um eine dem Adressaten bekannten Anzahl der Zeichen ein neuer, dem Nichteingeweihten unverständlicher Text erzeugt und übermittelt werden. Hier wird jedes Zeichen durch ein anderes ersetzt, so daß die absolute Länge der Wörter und des Textes gleich bleibt. Ein solches sog. monoalphabetische Chiffre kann (besonders mit Hilfe von Computern) leicht dechiffriert werden.[358]

Modernere Verschlüsselungsprogramme setzen sich zusammen aus einem komplexen Tauschalgorithmus[359] und einem Schlüssel-Codewort.[360] Das Programm vertauscht oder verschiebt nicht nur die ursprünglichen Symbole innerhalb der Zeichenfolge, sondern verknüpft jedes Zeichen zusätzlich mit der Vorgabe des Codeworts.[361] Damit können derart verschlüsselte Daten nur bei Kenntnis des Tauschalgorithmus, sowie des Codeworts entschlüsselt werden.[362] Hier kann weiter zwischen sogenannten symmetrischen[363] und asymmetrischen[364] Verfahren unterschieden werden.[365]

Das Charakteristikum des symmetrischen Verfahrens ist, daß der Verschlüsselungscode derselbe ist wie der Entschlüsselungscode. Hier stellt sich die Problematik, daß beide Kommunikationspartner beim Nachrichtenaustausch über denselben Schlüssel verfügen müssen. Der Schlüssel muß daher ebenfalls vom Absender oder Dritten dem Adressaten zugesandt werden. Hier ist ebenso für den Schlüssel eine sichere Übertragung notwen-

---

357 *Weck*, Datensicherheit, S. 283; *Leicht*, iur 1987, 45 (51).

358 *Schönleber*, Verschlüsselungsverfahren, S. 71 f.

359 Ein Algorithmus wird in der Informatik eine Anleitung zur Lösung einer Aufgabe (auch nichtmathematischer Art) mit Hilfe eines Computers genannt (aus *Grieser/Irlbeck*, Computerlexikon, S. 50).

360 *Weck*, Datensicherheit, S. 163 und 286 ff.

361 *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 158.

362 Mehr (und durchaus auch für Nicht-Experten verständlich) zu Verschlüsselungsverfahren bei *Schönleber*, Verschlüsselungsverfahren.

363 Solche symetrischen Verfahren sind z.B. DES (Data encryption standard), IDEA (heute in dem vielfach verbreiteten PGP (Pretty Good Privacy) verwendet. Das IDEA-Verfahren gilt als sicher (*Schönleber*, Verschlüsselungsverfahren, S. 95f.).

364 Z.B. das sog. RSA-Verfahren, näher dazu *Schönleber*, Verschlüsselungsverfahren, S. 97 f.; *Weck*, Datensicherheit, S. 297.

365 Anschaulich dazu *Müller-Berg*, DuD 1993, 87 (88 f.).

dig. Dies kann sogar bedeuten, daß der Schlüssel durch einen Kurier überbracht werden muß.[366]

Ein solcher Sicherheits- und Zeitverlust kann bei den asymmetrischen Verfahren vermieden werden, da hier der Verschlüsselungscode für einen bestimmten Adressaten öffentlich ist[367], und dieser allein über den ihm zugeordneten, geheimen Entschlüsselungscode verfügt. Es kann hier somit über ein öffentliches Register der Verschlüsselungscode für den konkreten Adressaten gesucht und eine verschlüsselte Nachricht an diesen ohne vorherige Kontaktaufnahme und Übertragung eines Schlüssels verschickt werden.[368]

(2) Strafrechtliche Behandlung

Ob die Datenverschlüsselung als besondere Zugangssicherung i.S.d. § 202a Abs. 1 angesehen werden kann, erscheint problematisch. Die verschlüsselten Daten sind als solche frei zugänglich. Nur die semantische Ebene der Urinformation, der Bedeutungsgehalt, wird vor Kenntnisnahme geschützt.

(a) Ansichten in der Literatur

Lenckner/Winkelbauer[369] sehen trotz Kenntnis von der Problematik in der Datenverschlüsselung eine Sicherung i.S.d. § 202a. Sie argumentieren damit, daß in den Fällen, in denen die Information verschlüsselt transportiert wird, sich die Kenntnisnahme der verschlüsselten Daten nicht mehr als Zugang zu den Originaldaten darstelle. Der Schlüssel sei eine den einzelnen Daten unmittelbar anhaftende Zugangssicherung. Sie nehmen damit an, daß sog. „Originaldaten" durch die Verschlüsselung geschützt werden. Unterstützt wird dieses Ergebnis mit einer teleologischen Auslegung der Norm.

---

366 *Weck*, Datensicherheit, S. 297.

367 Sog. „public keys". Asymetrische Verfahren werden auch public key-Systeme genannt

368 Ein Verfahren, die Identität des Absenders sicherzustellen, um die Rechssicherheit von Geschäften zu stärken, die über Datennetze abgewickelt werden und entsprechenden Formerfordernissen zu genügen, ist die sog. **Digitale Signatur** (Siehe auch SigG –Signaturgesetz, weiterführend dazu *Roßnagel*, NJW 1999, 1591 ff.). Hier ist der Verschlüsselungscode der digitalen Unterschrift geheim, der Entschlüsselungscode jedoch öffentlich. Der Empfänger der Nachricht kann die dig. Unterschrift entschlüsseln und weiß, daß diese Nachricht nur von dem Absender verschlüsselt werden konnte. Folglich kann mit diesem Verfahren die Authentizität der Nachricht wie bei der konventionellen Unterschrift oder einem Daumenabdruck sichergestellt und beweisbar gemacht werden. Die eigentliche Nachricht muß jedoch, falls erforderlich, für sich verschlüsselt werden, da bei der digitalen Signatur der Entschlüsselungscode jedermann zugänglich ist. (Näher dazu *Kuner*, NJW-CoR 1996, 108 ff.).

369 *Lenckner/Winkelbauer*, CR 1986, 483 (487).

Wenn einerseits das Tatbestandsmerkmal der Zugangssicherung dem Zweck diene, nur den Daten strafrechtlichen Schutz angedeihen zu lassen, „bei denen der Verfügungsberechtigte sein Interesse an der Geheimhaltung dokumentiert hat“ und andererseits im Falle der Datenübertragung nur die Verschlüsselung als Sicherung zu Verfügung stehe, so wäre die Einführung einer Strafvorschrift gegen Computerspionage in einem wichtigen Teilbereich von vornherein ein Schlag ins Wasser, wenn diese Fälle vom Gesetz nicht erfaßt wären.

In dieselbe Richtung geht auch *Leicht*.[370] Er problematisiert, ob eine Zugangssicherung i.S.d. § 202a Abs. 1 auch eine Sicherung vor Kenntnisnahme einschließe, da § 202a gerade nicht die Kenntnisnahme der Daten voraussetze.[371] Dies wird von ihm dahingehend bejaht, daß der weite Schutzbereich der Zugangssicherung auch die Sicherung vor Kenntnisnahme einschließe. So kommt *Leicht* dazu, daß das Verschlüsseln eines Datums nur mit dem Überstülpen eines anderen Gegenstandes über den zu Schützenden verglichen werden könne. Es ist folglich festzustellen, daß nach herrschender Ansicht, teilweise mit unterschiedlichen Ansätzen, die Datenverschlüsselung eine Sicherung i.S.d. § 202a Abs. 1 darstellt.[372]

(b) Stellungnahme

Die obigen Ansichten sind abzulehnen. Die Datenverschlüsselung stellt keine Zugangssicherung i.S.d. § 202a Abs.1 dar.

Rechtsgut des § 202a Abs. 1 ist das formelle Geheimhaltungsinteresse des Berechtigten. Es sind daher jegliche Daten grs. geschützt, ohne daß es auf die Bedeutung der Daten oder deren Qualität ankäme. Damit sind auch unsinnige (oder nur auf den ersten Blick unsinnige) Datenansammlungen im Schutzbereich des § 202a Abs. 1. Werden nun Daten, die sich im Zustand der Übermittlung befinden von, jemandem abgerufen, so sind Tatobjekt dieser möglichen Straftat nach § 202a Abs. 1 exakt die abgerufenen Daten. Diese Daten jedoch sind selbst nicht gegen Zugang geschützt, da sie grs. im Stadium der Übermittlung frei zugänglich sind, unabhängig davon, ob sie verschlüsselt oder unverschlüsselt sind. Wird nun von der Verschlüsselung als einer Sicherung vor Zugang zu den „Originaldaten“ gesprochen, so wird hier verkannt, daß zum Zeitpunkt der mög-

---

370 *Leicht*, iur 1987, 45 (51).

371 Dies ist Ergebnis der Auslegung der Tathandlung „Verschaffen“, siehe Seite 110.

372 So z.B.auch *Schulze-Heiming*, Der strafrechtliche Schutz der Computerdaten, S. 75 f.; Tröndle/Fischer-*Tröndle*, § 202a Rn. 7a; ohne näher darauf einzugehen auch Lackner/Kühl-*Kühl*, § 202a Rn. 4.

lichen Tathandlung Angriffs- und Tatobjekt ausschließlich die verschlüsselten Daten sind und nicht die „Originaldaten“. Die Originaldaten im sog. Klartext werden nicht abgerufen und sind gewöhnlich auf der Festplatte des Absenders gespeichert. Damit ist das von der h.M. angenommene Tatobjekt zum Zeitpunkt der Tat nicht das angegriffene Objekt. Es ist entweder gar nicht existent oder ist am Tatort nicht zugegen. Die h.M. verkennt damit das sog. Simultanitätsprinzip. Hiernach müssen zum Zeitpunkt der Tat alle Tatbestandsvoraussetzungen gegeben sein.

Der h.A. ist zuzugeben, daß der Gesetzgeber ausdrücklich[373] auch die Datenübertragung per Funk und Kabel schützen und dabei nicht auf eine besondere Technologie abstellen wollte[374], folglich es allein Sinn macht, auch solche verschlüsselten Daten strafrechtlich vor Ausspähung zu schützen. Dieses rechtspolitisch wünschenswerte Ergebnis ist jedoch nach dem jetzigen Wortlaut des § 202a nicht haltbar.[375] Daher wird vorgeschlagen, den § 202a Abs. 1 wie folgt zu ergänzen:

Satz 1 unverändert. Satz 2: Ebenso wird bestraft, wer unbefugt verschlüsselte Daten, die nicht für ihn bestimmt sind, entschlüsselt oder sich oder einem Dritten den Schlüssel verschafft.

b) Geheimhaltung

Fraglich ist, ob auch die Geheimhaltung von Daten als besondere Zugangssperre angesehen werden kann. Hierzu hat sich bislang nur *Hilgendorf*[376] geäußert. In seinem Fallbeispiel legt ein Berechtigter bestimmte wichtige Daten nicht bei seinen übrigen Geschäftsdateien ab, sondern versteckt sie in einem anderen Datenverzeichnis und paßt ihren Namen denjenigen der dort befindlichen Dateien an. Diese Daten werden dennoch gefunden und auf eine mitgebrachte Diskette kopiert.

Hilgendorf führt aus, daß eine solche Geheimhaltung u.U. durchaus ebenso effektiv sein könne wie ein Paßwort und ist daher der Ansicht, daß die Geheimhaltung bei dem Täter nicht bloß (wie ein Verbot) zu einer mentalen Schranke führe, die durch einen entsprechenden Willensentschluß überwunden werden könne, sondern sich objektiv als Zugangshindernis auswirke. Deshalb könne auch Geheimhaltung als besondere Zugangs-

---

373 BT-Drs. 10/5058, S. 29.

374 Lackner/Kühl-*Kühl*, § 202a Rn. 7a.

375 Auch *Schulze-Heiming*, Der strafrechtliche Schutz der Computerdaten, S. 76 hält die Argumentation der h.A. für ergebnisorientiert, verweigert ihr dennoch nicht die Anhängerschaft.

376 *Hilgendorf*, JuS 1996, 702 (703).

sperre i.S. von § 202a anerkannt werden, wenn sie eine mehr als nur unerhebliche Sperrwirkung entfaltet. Gerade bei der Geheimhaltung sei jedoch zu verlangen, daß sie den Geheimhaltungswillen des Berechtigten für einen objektiven Betrachter unmißverständlich deutlich macht; das Versteck müsse also zumindest teilweise erkennbar sein.

Es ist *Hilgendorf*[377] darin zuzustimmen, daß eine Geheimhaltung gerade in der von ihm beschriebenen Art ebenso wirksam sein kann wie andere allgemein anerkannte Sicherungen, z.B. die Paßwortsicherung. Die Geheimhaltung ist damit grs. objektiv geeignet, Daten zu sichern. Problematisch ist hier jedoch die zu fordernde objektive Erkennbarkeit des Geheimhaltungswillens. Das Wesen einer solchen Geheimhaltung ist gerade, daß der Täter erst die Gewißheit hat, die gewünschten Daten gefunden zu haben, wenn er die entsprechend versteckte Datei geöffnet hat. Vor dem Verschaffen der Daten ist es ihm aufgrund der Geheimhaltung nicht bewußt, daß sich gerade hier geschützte Daten befinden. Folglich kann die Geheimhaltung nicht als besondere Zugangssicherung i.S.d. § 202a Abs. 1 angesehen werden, da es dem Täter unmöglich ist, vor dem Zugriff auf die Daten den Geheimhaltungswillen des Berechtigten zu erkennen.[378]

---

377 *Hilgendorf*, JuS 1996, 702 (703).

378 LK-*Jähnke*, § 202a Rn. 14 verlangt physische oder technische Voraussetzungen und dürfte daher die Geheimhaltung als Sicherung i.S.d. § 202a Abs. 1 ablehnen.

IV. Tathandlung

Die Tathandlung des § 202a Abs. 1 ist das „Verschaffen“ der Daten für sich oder einen Dritten. Werden die Daten, die sich der Täter schon selbst verschafft hat, zeitlich nachfolgend an einen Dritten weitergegeben, so ist dieses Verhalten eine mitbestrafte Nachtat zum vorangegangenen eigenen Verschaffen.[379]

1. Anknüpfungspunkte für die Auslegung

Der Begriff des Verschaffens kommt auch in den §§ 96, 202 und 259 vor.

a) § 259

Tatobjekt des § 259 ist eine Sache. Eine Sache ist ein körperlicher Gegenstand.[380] Das Tatobjekt des § 202a sind jedoch „Daten“. Diese sind keine körperlichen Gegenstände, sondern von ihrem Träger zu abstrahierende Informationen nichtkörperlicher Art. Werden Datenträger entwendet, um die darauf befindlichen Daten zu erlangen, so liegt scheinbar eine vergleichbare Situation vor. Es kann dennoch nicht an § 259 angeknüpft werden. Denn es erschließt sich nicht von vornherein, daß die „Daten“ immer als „verschafft“ i.S.d. § 202a Abs. 1 anzusehen sind, wenn der Täter sich den körperlichen Datenträger verschafft hat i.S.d. § 259. Sind die Daten auf dem Datenträger verschlüsselt, so erweist sich die Frage des Verschaffens als problematisch.[381] Werden Daten übertragen, wie z.B. durch Kopieren auf einen tätereigenen Datenträger oder durch das reine Auswendiglernen der Informationen, so ist überhaupt keine Vergleichbarkeit zu § 259 mehr vorhanden, da hier die Daten ohne Fixierung auf einem Träger übertragen werden. Somit kann § 259 zur Auslegung der Tathandlung des § 202a Abs. 1 nicht herangezogen werden.[382]

---

379 *Schlüchter*, 2. WiKG, S. 67.

380 Tröndle/Fischer-*Tröndle*, § 242 Rn. 2.

381 *Schlüchter*, 2. WiKG, S. 66 sieht hier jedoch Parallelen zu § 259.

382 So auch *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 142.

b) § 202 Abs. 1 Nr. 2, § 202 Abs. 2

Der Tatbestand der § 202 Abs. 1 Nr. 2 und § 202 Abs. 2 beinhaltet „Kenntnis verschaffen" von wahrnehmbaren Daten auf einem Schriftstück. Der Begriff der „Kenntnis" der Daten ist jedoch in § 202a Abs. 1 bewußt weggelassen worden.[383] Damit soll, so die Begründung des Rechtsausschusses[384], auch der Täter erfaßt werden können, der die Daten ohne eigene Kenntnis einem Dritten verschafft. Der Verzicht auf die Kenntnisnahme ergibt jedoch auch dann Sinn, wenn der Täter diese nur für sich selbst erlangt, diese Daten dann aber ohne Kenntnisnahme weiterverarbeitet und die Ergebnisse der Weiterverarbeitung zu eigenen Zwecken nutzt.[385] Auch dies kann den Verfügungsberechtigen empfindlich treffen. Diese Regelungslücken werden mit dem Verzicht auf die Kenntnisnahme der Daten geschlossen. Folglich sind auch § 202 Abs. 1 Nr. 2 und § 202 Abs. 2 keine tauglichen Anknüpfungspunkte für die Auslegung des § 202a Abs. 1.

Die Überschrift des § 202a „Ausspähen von Daten" ist als verfehlt anzusehen, da sie entgegen dem eigentlichen Willen des Gesetzgebers mindestens Kenntnisnahme, wenn nicht sogar das Verständnis der Information suggeriert. Hier wurde ein im Vergleich zur Tathandlung zu enger und irreführender Begriff gewählt.[386]

c) § 96

Als interessanter und ergiebiger erweist sich § 96[387], da das Tatobjekt „Staatsgeheimnis" nichtkörperlicher Art ist. Hier kann, wie bei § 202a Abs. 1, das Tatobjekt „Staatsgeheimnis" als Information auf einem Träger fixiert sein (auf die Nichtwahrnehmbarkeit kommt es hier nicht an) oder entweder als nichtwahrnehmbare Daten oder auf sonstige Weise (z.B. akustisch) nichtmaterialisiert übertragen worden sein. Verschaffen i.S.d. § 96 wird wie folgt definiert: Ein Verschaffen liegt dann vor, wenn der Täter durch irgendeine finale Handlung entweder ein verkörpertes Geheimnis in seinen Gewahrsam

383 BT-Drs. 10/5058, S. 29.

384 BT-Drs. 10/5058, S. 29.

385 *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 143.

386 *Hilgendorf*, JuS 1996, 509 (511 f.).

387 In diesem Sinne auch Tröndle/Fischer-*Tröndle*, § 202a Rn. 9; Lackner/Kühl-*Kühl*, § 202a Rn. 5; *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 142, 145. Auch in BT-Drs. 10/5058 S. 29 ist ein Hinweis auf § 96 zu finden.

bringt (ohne Rücksicht auf Kenntnis[388]) oder sonst gesicherte Kenntnis von einem Geheimnis erlangt.[389] Es wird somit in zwei Fallgruppen unterteilt:

- Der Täter erlangt das Geheimnis, in dem er die Sache, die das Geheimnis trägt, wegnimmt. Es reicht in diesem Fall aus, daß er Gewahrsam an dem „Geheimnisträger" erlangt. Kenntnis des Geheimnisses selbst ist für die Tatbestandserfüllung nicht erforderlich. Bei dieser Definition wird jedoch die Möglichkeit der computermäßigen Übertragung durch Kopieren von in Datenform vorliegenden Staatsgeheimnissen außer acht gelassen. Kopiert ein Täter Staatsgeheimnisse in Datenform auf einen anderen Datenträger, so hat er keinen Gewahrsam am Geheimnis erlangt. Dennoch ist dieser Fall gleich wie der der Gewahrsamserlangung am Informationsträger zu behandeln, da auch in diesem Fall der Täter oder andere jederzeit vom Geheimnis Kenntnis nehmen können. Folglich ist auch hier keine Kenntnisnahme erforderlich.
- Der Täter erlangt das Geheimnis immaterialisiert durch Sinneswahrnehmung und geistige Verarbeitung. Zumeist geschieht dies durch Lesen von Schriftstücken. Hier handelt es sich somit um Kenntnisnahme. Nicht erforderlich ist es jedoch, daß der Täter das Geheimnis in seiner wahren Bedeutung erfaßt.[390]

2. Auslegung

Ausgangspunkt der Auslegung ist, daß im Gegensatz zu § 202 nicht zwingend Kenntnisnahme erforderlich ist. Es ist nun zunächst zu prüfen, ob bei allen denkbaren Vorgehensweisen die Kenntnisnahme verzichtbar ist oder ob differenziert werden muß.

a) Fallgruppen

Die Tathandlung des § 202a Abs. 1 kann, wie bei § 96, in zwei Fallgruppen unterteilt werden.

(1) Materialisierte Daten

In dieser Fallgruppe erlangt der Täter Gewahrsam am Datenträger oder fixiert die Daten auf einem vom ursprünglichen Träger verschiedenen Medium.

---

388 Lackner/Kühl-*Kühl*, § 96 Rn. 3.

389 Tröndle/Fischer-*Fischer*, § 96 Rn. 2.

390 SK-*Rudolphi*, § 96 Rn. 4.

Für diese Fallgruppe genügt nach h.M. für ein „Verschaffen“ Gewahrsamserlangung des Datenträgers oder die dauerhafte technische Übertragung der Daten (z.B. durch Kopieren auf Diskette) ohne zusätzliche Kenntnisnahme der Information.[391] Die Daten müssen nach einem Übertragungsvorgang auf einem im Gewahrsam des Täters befindliches Medium nicht mehr nicht-wahrnehmbar i.S.d. § 202a Abs. 2 sein. So hat sich der Täter auch die Daten verschafft, wenn er einen mit bloßem Auge sichtbaren Ausdruck von den betreffenden Daten anfertigt oder diese abschreibt.[392] Ein Verschaffen ist nicht gegeben, wenn der Täter sich oder einem anderen nicht die Daten selbst, sondern nur ihre Wiedergabe in wahrnehmbarer Form verschafft, da es sich nicht (oder nicht mehr) um nicht wahrnehmbare Daten i.S.d. § 202a Abs. 2 handelt und es daher am tauglichen Tatobjekt mangelt. [393]

Der h.M. ist grs. zu folgen, da nach allgemeinem Sprachgebrauch man sich eine Sache „verschafft“, wenn man eigene Verfügungsgewalt über sie erlangt.[394] Jedoch ist zu beachten, daß es bei § 202a Abs. 1 nicht um das Verschaffen einer Sache geht, sondern um unkörperliche Daten. Es ist somit danach zu fragen, wann ein Täter die Verfügungsgewalt über Daten erlangt hat. Hat der Täter den Datenträger in Gewahrsam, oder hat er Daten auf ein anderes ihm zur Verfügung stehendes Medium kopiert, so kann es dennoch sein, daß eine besondere Sicherung eingerichtet ist, die den Daten direkt anhaftet, und dem Täter dadurch die Möglichkeit der Kenntnisnahme trotz Gewahrsam des Trägers der betreffenden Daten verwehrt ist. In diesem Fall kann von einer Verfügungsgewalt über die Daten keine Rede sein. Verschafft hat sich der Täter die Daten erst, wenn er die Möglichkeit zur Kenntnisnahme innehat. Es muß ihm möglich sein, die Daten jederzeit abrufen zu können, erst dann hat er die Verfügungsgewalt über die Daten. Auf welche Weise dies geschehen kann, ist jedoch nicht von Belang, insbesondere ist eine Überwindung der Zugangssicherung nicht erforderlich.[395]

---

391 *Hilgendorf*, 1996, 702 (704); Lackner/Kühl-*Kühl*, § 202a Rn. 5; LK-*Jähnke*, § 202a Rn. 6; Schönke/Schröder-*Lenckner*, § 202a Rn. 10; *Bühler*, MDR 1987, 448 (453); *Schlüchter*, 2. WiKG, S. 66; *Schmitz*, JA 1995, 478 (483); Tröndle/Fischer-*Tröndle*, § 202a Rn. 9.

392 LK-*Jähnke*, § 202a Rn. 6; *Hilgendorf*, 1996, 702 (704).

393 *Schmitz*, JA 1995, 478 (483); OLG Celle, wistra 1989, 354 (355); Schönke/Schröder-*Lenckner*, § 202a Rn. 10.

394 *Hilgendorf*, 1996, 702 (704).

395 Siehe dazu Seite 92 ff.

(2) Nicht-materialisierte Daten

In dieser Fallgruppe erlangt der Täter die Daten auf sonstige Weise, d.h. wie auch bei § 96 durch Sinneswahrnehmung.

Bei § 96 war schon erkennbar, daß Informationen, die nicht in technisch reproduzierbarer Weise erlangt werden, einzig durch Sinneswahrnehmung und Aufnahme in das Gedächtnis erlangt werden können (Fallgruppe 2). In diesen Konstellationen handelt es sich nicht um eine rechtliche Fragestellung, ob Kenntnisnahme erforderlich ist, da aus logischen Gründen keine andere Möglichkeit gegeben ist, die Daten zu erlangen. Problematisch hingegen ist jedoch die Qualität dieser Kenntnisnahme, insbesondere im Hinblick auf das Hauptaugenmerk dieser Arbeit, das Computerhacken, da der Gesetzgeber das „Hacking", verstanden als das bloße Eindringen in ein fremdes Computersystem, für straflos erachtete.[396] *Haft*[397] und *Hauptmann*[398] wollen diese Fallgruppe ganz aus dem Anwendungsbereich des § 202a herausnehmen und verlangen eine Übertragung der Daten auf ein vom ursprünglichen Datenträger verschiedenes Medium. Dies ist einer der Versuche, die Problematik des „Hackens" in den Griff zu bekommen.

b) Definition

Eine beide Fallgruppen zusammenfassende Definition nach der h.M. wäre dann: Daten sind dann verschafft, wenn der Täter entweder von den Daten Kenntnis nimmt bzw. einem anderen die Kenntnis ermöglicht oder -ohne Kenntnisnahme- sich oder einen anderen in den Besitz des Datenträgers bringt bzw. die Daten in einem eigenen Datenspeicher ablegt.[399] Hieraus ergibt sich, daß das tragende Kriterium für die Auslegung das Erlangen der Verfügungsgewalt über Daten ist.

Jähnke[400] definiert das Verschaffen i.S.d. § 202a Abs. 1 als den **Wechsel** der Herrschaft über die Information. Dies ist abzulehnen.[401] Ein Herrschaftswechsel über ein Tatobjekt findet bei § 242 statt. Dort ist Tatobjekt eine Sache. Diese eine Sache kann sich nur an

---

396 BT-Drs. 10/5058, S. 28. Zur Problematik des Hackens und der verschiedenen Lösungsansätze siehe Seite 121 ff.

397 *Haft*, NStZ 1987,6 (10).

398 *Hauptmann*, JurPC, 1989, 215 (217f.).

399 Nach *Schmitz*, JA 1995, 478 (483). In diesem Sinne auch *Lenckner/Winkelbauer*, CR 1986, 483 (488); SK-*Samson*, § 202a Rn. 1; Tröndle/Fischer-*Tröndle*, § 202a Rn. 9; *Hilgendorf*, JuS 1996, 702 (704).

400 LK-*Jähnke*, § 202a Rn. 6.

401 So auch *Hilgendorf*, JuS 1996, 702 (704); *Schmitz*, JA 1995, 478 (483) in Fn. 51.

einem Ort befinden. Etwas anderes gilt jedoch bei Daten als Tatobjekt. Bei ihnen besteht die Möglichkeit unendlicher Reproduktion, so daß, wenn jemand die Daten von einem anderen „stehlen“ möchte, zumeist eine Verdopplung dieser Daten stattfindet und beim Opfer eine Kopie verbleibt.

3. Mehrfache Datensicherung

Bei einer mehrfachen Datensicherung, was in der Praxis durchaus oft vorkommen dürfte, ist danach zu fragen, wann sich der Täter die Daten verschafft hat. Mehrfache Datensicherung ist z.B. gegeben, wenn jemand seinen Rechner in einen Schrank einschließt, daneben eine Paßwortsicherung auf BIOS-Ebene[402] hat und dann auch noch einzelne Dateien oder Verzeichnisse mit einem Paßwortschutz versieht.

Auch hier ist das Erlangen der Verfügungsgewalt über die Daten maßgeblich. Hat der Täter den Schrank gewaltsam geöffnet, so kann er die Daten immer noch nicht abrufen, verändern oder kopieren. Er hat somit noch keine Verfügungsgewalt über die Daten auf diesem Rechner. Umgeht oder überwindet er die Sicherung auf BIOS-Ebene, so hat er Verfügungsgewalt über die ungeschützten Daten, jedoch noch nicht auf die Daten, die in nochmals geschützten Dateien oder Verzeichnissen abgelegt sind. Diese Daten sind erst dann verschafft entweder nach erfolgter Kenntnisnahme, wenn er die Daten wahrnehmbar abrufen kann, oder nachdem er sich diese nach Überwindung oder Umgehung der Sicherung abrufbaren Daten kopiert oder er den Datenträger in seinen Gewahrsam bringt. Verfügungsgewalt über Daten ist demnach mit Überwindung oder Umgehung der **letzten Sicherung** gegeben, hinter der Daten **ungeschützt** gespeichert sind und im Fall des nicht-materialisierten Erlangens der Täter (oder ein Dritter) Kenntnis genommen hat oder bei materialisierten Daten diese kopiert wurden oder der Datenträger selbst weggenommen wurde.[403]

---

402 Das BIOS (Basic Input Output System) ist ein Programm, welches das Ausführen elementarer Operationen ermöglicht. Es ist auf einem im Rechner fest verankerten unveränderlichen Speicher (sog. EPROM) gespeichert. (vgl. *Grieser/Irlbeck*, Computerlexikon, S. 130).

403 Zum Spezialfall geschützter, jedoch schon verschlüsselter Daten siehe Seite 116.

4. Problemfall: Datenverschlüsselung

Oben wurde die Datenverschlüsselung als besondere Zugangssicherung abgelehnt. Die folgenden Ausführungen beruhen auf der Annahme, die Datenverschlüsselung sei eine Sicherung i.S.d. § 202a Abs. 1 und sind damit hilfsgutachtlicher Art. Es ist umstritten, wie das Verschaffen im Falle der Datenverschlüsselung[404] zu beurteilen ist.

a) Entschlüsselung

Die engste Ansicht vertritt *Schmitz*[405]. Sie resultiert aus einem konsequenten Verfolgen des auch von ihm geforderten Überwindens der Zugangssicherung. So ist er der Ansicht, falls Daten nur durch ihre Verschlüsselung gegen unberechtigten Zugang gesichert seien, der Täter sie sich erst verschafft habe, wenn er sie (auf der syntaktischen Ebene) entschlüsselt hat.[406] *Schmitz* differenziert nicht zwischen den beiden möglichen Begehungsweisen. Unabhängig von der Frage ob der Täter die verschlüsselten Daten materialisiert oder nicht-materialisiert erlangt hat, liegt ein Verschaffen seiner Meinung nach erst nach Entschlüsselung der Daten vor.

b) Entschlüsselbarkeit

Lenckner[407] fordert für beide Formen des Verschaffens mindestens Entschlüsselbarkeit der Daten. Auch hier ist Anknüpfungspunkt für die Beurteilung der Datenverschlüsselung das auch von ihm vertretene Erfordernis der Überwindung der Zugangssicherung. Sind die Daten durch ihre Verschlüsselung besonders gesichert, so sei zu beachten, daß sie erst mit der Überwindung der Zugangssicherung, d.h. also der Entschlüsselung der Daten, verschafft sind; anders als in § 96 genüge es bei § 202a daher z.B. noch nicht, daß der Täter eine Diskette mit verschlüsseltem Text in seine Verfügungsgewalt bringt, vielmehr liege ein Verschaffen hier erst vor, wenn er die Daten tatsächlich entschlüsselt hat oder jedenfalls auch den Schlüssel in seinen Besitz bringt.[408] Obwohl dies nicht explizit vermerkt ist, ist anzunehmen, daß auch solche Fälle von dieser Meinung miteingeschlossen sind, bei denen der Täter oder der Dritte den Schüssel schon vor dem Ver-

---

404 Siehe dazu auch „Datenverschlüsselung“ als besondere Zugangssicherung, Seite 99 ff.

405 *Schmitz*, JA 1995, 478 (483).

406 *Schmitz*, JA 1995, 478 (483).

407 Schönke/Schröder-*Lenckner*, § 202a Rn. 10.

408 Schönke/Schröder-*Lenckner*, § 202a Rn. 10.

schaffen der verschlüsselten Daten innehatte.[409] *Lenckner* fordert daher unter Zugrundelegung derselben Prämisse wie *Schmitz*, der Überwindung der Zugangssicherung, und ebenso ohne Differenzierung der beiden Tatformen, keine Überwindung der Zugangssicherung „Datenverschlüsselung", sondern nur die Möglichkeit der Überwindung, die Entschlüsselbarkeit der Daten.

c) Keine Anforderungen bei Wegnahme des Datenträgers, sonst Entschlüsselbarkeit

Eine dritte, noch weitere Interpretation[410] differenziert zwischen den beiden möglichen Tatformen.

(1) Materialisierte Datenerlangung

Es wird postuliert, daß Verschaffen auch Erlangen des Besitzes am Datenträger sei. Im Falle von verschlüsselten Daten bedeute dies Folgendes: Erlange der Täter oder der Dritte den Besitz an den Datenträgern, so habe er sich die Daten auch dann verschafft, wenn diese verschlüsselt sind.[411] Es wird hier nicht ausdrücklich noch einmal gesagt, daß von den Vertretern dieser Ansicht eigentlich auch die Überwindung der Zugangssicherung gefordert wird. Folgerichtig können nach dieser Ansicht bei Wegnahme des Datenträgers die verschlüsselten Daten nur dann „verschafft" worden sein, wenn dies unter Überwindung einer tauglichen Sicherung geschah (z.B. Tresor, in dem der Datenträger weggeschlossen war, wird gewaltsam geöffnet).

(2) Nicht-materialisierte Datenerlangung

Im Falle der Kenntnisnahme oder Kenntnisverschaffung genüge die bloße Wahrnehmung des Schlüsseltextes dagegen nicht. Hier liege ein Verschaffen erst dann vor, wenn der Täter den Text entschlüsselt oder einen Schlüssel besitzt oder erlangt; einem Dritten habe der Täter verschlüsselte Daten nur dann verschafft, wenn er ihm neben der Kenntnisnahme der Daten auch die des Schlüssels ermöglicht oder der Dritte bereits im Besitz

---

409 Diese Fallkonstellation ist bei *Lenckner/Winkelbauer*, CR 1986, 483 (486) noch ausdrücklich aufgeführt.

410 *Lenckner/Winkelbauer*, CR 1986, 483 (486) (*Lenckner* hat diese Ansicht in Schönke/Schröder-*Lenckner*, § 202a Rn. 10 explizit aufgegeben); Tröndle/Fischer-*Tröndle*, § 202a Rn. 9; LK-*Jähnke*, § 202a Rn. 6; *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 144.

411 *Lenckner/Winkelbauer*, CR 1986, 483 (486). Über den Fall der materialisierten Datenerlangung durch Verdopplung der Daten auf einem anderen Medium, schweigt sich diese Ansicht aus.

des Schlüssels ist.[412] Bei nicht-materialisierten Daten wird vertreten, daß Entschlüsselbarkeit ausreicht.

Diese Ansicht scheint sich beim Erlangen von materialisierten Daten eng an die Auslegung zu § 96 anzulehnen. Bei dieser Vorschrift ist es anerkannt, daß ein Verschaffen schon dann vorliegt, wenn das Geheimnis in verkörperter, wenn auch möglicherweise verschlüsselter Form erlangt wurde. Die wahre Bedeutung des Geheimnisses, unabhängig von der Art der Beschaffung, ist bei § 96 unerheblich.[413]

d) Keine Anforderungen, wenn vorgeschaltete Sicherung überwunden wurde

Hilgendorf[414] vertritt für die Fallkonstellation, bei der verschlüsselte Daten (in dem von ihm konzipierten Fall werden die Daten materialisiert erlangt) unter Überwindung einer vorgelagerten Zugangssicherung erlangt werden, daß sich der Täter ohne weitere Anforderungen, wie Entschlüsselung oder Entschlüsselbarkeit, die Daten verschafft hat. Zur Begründung führt er aus, daß in der Literatur vertreten werde, ein „Verschaffen" liege erst vor, wenn der Täter die Daten tatsächlich entschlüsselt hat oder zumindest den Schlüssel in seinen Besitz bringt. Diese Ansicht führe jedoch zu der merkwürdigen Konsequenz, daß der Strafrechtsschutz um so geringer ausfalle, je gewissenhafter der Berechtigte seine Daten verschlüsselt. Schon deshalb könne sie nicht überzeugen. Im übrigen seien die meisten verschlüsselten Dateien auch für Unbefugte mit entsprechendem technischem Aufwand wieder entschlüsselbar (zu diesem Zweck existieren eigens entwickelte und sehr leistungsfähige Programme), so daß die Forderung, der Täter müsse sich bei verschlüsselten Programmen auch den Schlüssel vom Berechtigten verschaffen, praxisfremd erscheine.

e) Stellungnahme

Die ersten beiden Ansichten gehen von der gleichen Grundannahme aus, daß die Zugangssicherung überwunden werden muß. Es ist jedoch der Ansicht, die lediglich Entschlüsselbarkeit fordert, Inkonsequenz vorzuwerfen. Ist die Verschlüsselung der Daten die Zugangssicherung, so kann eigentlich erst dann von einer Überwindung der Zugangssicherung gesprochen werden, wenn die Daten entschlüsselt sind. Die Möglichkeit der Überwindung reicht nicht aus. Damit würde entgegen den eigenen Ausführungen

---

412 *Lenckner/Winkelbauer*, CR 1986, 483 (486).

413 Schönke/Schröder-*Stree*, § 96 Rn. 4.

414 *Hilgendorf*, JuS 1996, 702 (705).

die Strafbarkeit gem. § 202a vorverlagert. Fordert man die Überwindung der Zugangssicherung, so ist es demnach vorzugswürdig, ein „Verschaffen“ erst dann zu bejahen, wenn die Daten entschlüsselt sind.

Wird jedoch, wie in dieser Arbeit, vertreten, daß die Zugangssicherung nicht überwunden werden muß, kann sich auch etwas anderes ergeben. Wie oben schon angemerkt, ist tragendes Kriterium für das „Verschaffen“ die Erlangung der nicht notwendig alleinigen Verfügungsgewalt über Daten. Ein solches Erlangen der Verfügungsgewalt über Daten kann auch dann angenommen werden, wenn der Täter oder der Dritte ohne erfolgte Entschlüsselung der Daten den Schlüssel für die konkrete Verschlüsselung der betreffenden Daten besitzt und damit jederzeit die Möglichkeit hat, die Daten zu entschlüsseln. Der Täter oder der Dritte können folglich jederzeit über die unverschlüsselte Information verfügen. Sie haben daher die Verfügungsgewalt über die Daten inne. Entschlüsselbarkeit reicht danach für ein Verschaffen von Daten aus, da es auf eine Überwindung der Sicherung nicht ankommt.

Für die Unterscheidung der Datenverschaffung bei Verschlüsselung nach den verschiedenen möglichen Tatformen gibt es keine Anhaltspunkte. Verfügungsgewalt über die unverschlüsselten Daten ist auch im Falle der Wegnahme des Datenträgers erst gegeben, wenn die Möglichkeit der Entschlüsselung gegeben ist.

Mit *Hilgendorf* [415] könnte ein Verschaffen möglicherweise schon ohne Entschlüsselbarkeit bzw. Entschlüsselung der Daten angenommen werden, wenn die verschlüsselten Daten selbst gesichert waren. In § 202a wird nach h.M. das formelle Geheimhaltungsinteresse des Verfügungsberechtigten geschützt. Tatobjekt ist damit nicht eine nach gewissen Kriterien sinnhafte Information, sondern kann alles sein, was in nicht wahrnehmbarer Weise übermittelt oder gespeichert werden kann (§ 202a Abs. 2). Nun können daher grs. verschlüsselte und damit scheinbar sinnlose Informationen Tatobjekt i.S.d. § 202a sein. Auf der anderen Seite ist die Verschlüsselung, die jedoch den verschlüsselten Daten innewohnt, anerkannt als besondere Zugangssicherung. Kann sich der Täter nun verschlüsselte Daten auch ohne Entschlüsselung „verschaffen“? Dies ist bei zusätzlich mit einer besonderen Sicherung geschützten verschlüsselten Daten zu bejahen. Überwindet oder umgeht der Täter diese Sicherung und dringt er damit zu den verschlüsselten Daten vor, so hat er sich diese auch als Tatobjekt tauglichen verschlüsselten Daten verschafft i.S.d. § 202a.

---

415 *Hilgendorf*, JuS 1996, 702 (705) Fall 11.

Sind die verschlüsselten Daten geschützt, so hat der Verfügungsberechtigte zum Ausdruck gebracht, daß er diese Daten unabhängig von Form und Art geheim halten möchte. Bei Überwindung oder Umgehen der Sicherung ist damit das formelle Geheimhaltungsinteresse des Berechtigten betroffen. In dieser Fallkonstellation sind damit die verschlüsselten Daten ausschließlich Tatobjekt i.S.d. § 202a. Nur wenn die verschlüsselten Daten selbst nicht geschützt sind, ist die Verschlüsselung als Sicherung vorrangig gegenüber der Betrachtung der verschlüsselten Daten als Tatobjekt. *Hilgendorf*[416] ist somit im Ergebnis zu folgen. Bei Sicherung von verschlüsselten Daten brauchen diese für das Bejahen der Tathandlung „Verschaffen" nicht entschlüsselt zu werden, bzw. entschlüsselbar zu sein, wenn die an sich funktionsfähige Sicherung überwunden oder umgangen wurde.

Zusammenfassend ist anzumerken, daß verschlüsselte Daten ohne Differenzierung in materialisiertes oder nicht-materialisiertes Erlangen dann „verschafft" sind i.S.d. § 202a, wenn die Daten zumindest für den Täter oder den Dritten entschlüsselbar sind. Sind verschlüsselte Daten selbst durch eine besondere Zugangssicherung geschützt, so ist ein „Verschaffen" ohne Entschlüsselbarkeit bzw. Entschlüssung mit Überwindung oder Umgehung der Sicherung gegeben.

---

416 *Hilgendorf*, JuS 1996, 702 (705).

D. Der subjektive Tatbestand

Es genügt bei § 202a Abs. 1 dolus eventualis (Eventualvorsatz). Dieser muß sich im Zeitpunkt der Tathandlung „Verschaffen" auf alle Merkmale des objektiven Tatbestandes beziehen.[417] Bei der besonderen Zugangssicherung muß der Täter die Sicherung nicht in allen technischen Einzelheiten wahrgenommen haben. Es genügt, daß er erkennt, daß irgendein funktionsfähiges Zugangshindernis zu den Daten eingerichtet ist. Die Sicherung muß als solche nicht zwingend wahrgenommen werden.[418] Ein subjektives Merkmal mit überschießender Innentendenz (wie z.B. in § 242 Zueignungsabsicht), denkbar wäre hier eine Verwertungsabsicht, ist in § 202a Abs. 1 nicht enthalten.[419] Eine solche Verwertungsabsicht bzgl. der Daten müßte nur dann in den Tatbestand hinein interpretiert werden, wenn man § 202a für ein Vermögensdelikt hält.[420]

E. Die Rechtswidrigkeit

I. Das Merkmal „unbefugt"

Der Täter muß „unbefugt" handeln. Dieses Merkmal kommt in einigen Straftatbeständen vor, so z.B in §202 oder § 263a[421] vor. Es hat keine einheitliche Bedeutung. So wird es zum Teil als gleichbedeutend mit dem allgemeinen Verbrechensmerkmal der Rechtswidrigkeit verstanden (z.B. bei §§ 168, 353b), zum Teil wird ihm eine Doppelfunktion zugeordnet.[422] In diesen Fällen ergibt der Tatbestand ohne Einbeziehung des Merkmals keinen vernünftigen Sinn, so daß es auch als eingrenzendes Element des Tatbestandes dient.[423] Ein Tatbestand ist dann als nicht vernünftig anzusehen, wenn er unter Weglassung des Merkmals „unbefugt" lediglich sozialadäquates Verhalten beschreiben würde.[424] Bei § 202a beschreibt der Tatbestand auch ohne das Merkmal „unbefugt"

---

417 *Hilgendorf*, JuS 1996, 702 (704).

418 A.A. *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 146.

419 Lackner/Kühl-*Kühl*, § 202a Rn. 5 fügen dem § 202a zur Exclusion des Hackens i.e.S. und damit zur Eingrenzung der Tathandlung das ungeschriebene Merkmal einer Weiterverwendungsabsicht hinzu. Siehe dazu Seite 124.

420 So *Haft*, NStZ 1987, 6 (9).

421 Zu § 263a siehe Hilgendorf, JuS 1999, 542 ff.

422 Schönke/Schröder-*Lenckner*, Vor § 13 Rn. 65.

423 Schönke/Schröder-*Lenckner*, Vor § 13 Rn. 65.

424 In dieselbe Richtung auch *Schlüchter*, 2. WiKG, S. 68.

einen sozial inadäquaten Vorgang. Ausschlaggebend ist in diesem Zusammenhang das Merkmal, daß die Daten nicht für den Täter bestimmt sein dürfen. Täter kann damit nur ein solcher sein, der sich ohne erteilte Befugnis durch den Berechtigten die Daten verschaffen möchte. Ein solches Vorgehen ist schon als solches als „unbefugt" und damit als sozialschädliches Verhalten zu bewerten. Folglich ist das Merkmal „unbefugt" mit der ganz h.M.[425] als ein Hinweis deklaratorischer Art, wie auch in allen anderen Tatbeständen des 15.Abschnitts[426], auf das allgemeine Verbrechensmerkmal der Rechtswidrigkeit zu verstehen.

II. Rechtfertigung

Die Einwilligung in das Verschaffen von Daten ist im Tatbestandsmerkmal der Datenbestimmung enthalten und wirkt tatbestandsausschließend. Eine ausdrückliche oder konkludente Einwilligung kommt daher als Rechtfertigungsgrund grs. nicht zum Tragen.[427] Zu beachten ist jedoch, daß die Einwilligung darin, daß ein Dritter die Daten zur Kenntnis nehmen darf, den Täter rechtfertigt, wenn der Täter die Daten ohne Verschaffen der Daten für sich selbst dem Dritten zugänglich macht.[428]

Als Rechtfertigungsgrund kommt in erster Linie die mutmaßliche Einwilligung in Betracht. Insbesondere ist hier die Konstellation zu nennen, bei der die einem Dritten verschafften Daten zwar nicht für den Täter, aber für den Dritten bestimmt sind.[429] Mit *Jähnke* ist jedoch festzustellen, daß solche Fälle praktisch nicht in Betracht kommen. Zur Bejahung einer mutmaßlichen Einwilligung erforderliche Eilsituationen, welche ein Eindringen in fremde Datenanlagen notwendig machen, bevor der Berechtigte befragt werden kann, sind kaum denkbar.[430]

---

425 *Hilgendorf*, JuS 1996, 702 (705); Tröndle/Fischer-*Tröndle*, § 202a Rn 9; Lackner/Kühl-*Kühl*, § 202a Rn. 4; Schönke/Schröder-Lenckner, § 202a Rn. 11; *Schlüchter*, 2. WiKG, S. 68; SK-*Samson*, § 202a Rn. 13; *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 148.

426 Tröndle/Fischer-*Tröndle*, § 201 Rn. 7; Lackner/Kühl-*Kühl*, § 202a Rn. 7 iVm Vor § 201 Rn. 2.

427 A.A. Lackner/Kühl-*Kühl*, § 202a Rn. 7.

428 Vgl. *Lenckner/Winkelbauer*, CR 1986, 483 (488).

429 BT-Drs. 10/5058, S. 29; *Möhrenschlager*, wistra 1986, 128 (140), Tröndle/Fischer-*Tröndle*, § 202a Rn. 9.

430 LK-*Jähnke*, § 202a Rn. 17; zustimmend *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S.149. Anders jedoch BT-Drs. 50/58 S. 29; Tröndle-Fischer-*Tröndle*, § 202a Rn. 9; *Möhrenschlager*, wistra 1986, 128 (140); *Schlüchter*, 2. WiKG, S.68.

F. Schuld

Auf Schuldebene gibt es keine besonderen Probleme bei § 202a Abs. 1. Ein Fall, der als Verbotsirrtum i.S.d. § 17 in Frage kommt, ist der, daß sich jemand, den die Daten betreffen, für befugt hält, diese gesicherten Daten einzusehen.[431] Hier ist jedoch in den meisten Fällen von der Vermeidbarkeit des Irrtums auszugehen.[432]

G. Versuch

Der Versuch ist nicht strafbar.

H. Konkurrenzen

Falls ein Datenträger entwendet wird, ist Tateinheit mit § 242 oder § 246 möglich. Ebenfalls können die §§ 303a und 303b mit § 202a ideal konkurrieren. Hausfriedensbruch (§ 123) und Sachbeschädigung (§ 303) sind keine typischen Begleittaten, so daß Konsumtion ausscheidet.[433] Daher ist auch hier Idealkonkurrenz möglich.[434] Tateinheit mit § 17 UWG, sofern die verschafften Daten Geschäfts- oder Betriebsgeheimnisse enthalten[435], sowie mit § 106 UrhG, sofern gesicherte Programme auch urheberrechtlich geschützt sind, kommt ebenfalls in Betracht. Auch im Zusammenhang mit § 43 BDSG ist Idealkonkurrenz denkbar.[436]

I. Strafantrag

Gem. § 205 Abs. 1 ist bei § 202a Abs.1 ein Strafantrag Prozeßvoraussetzung.[437] Damit sollte nach dem Willen des Gesetzgebers neben der Anwendung von §§ 153, 153a StPO, 47 JGG ein wichtiger Filter zur Verhinderung von unnötigen Strafverfahren eingerichtet werden.[438] Verletzter und damit der originär zur Antragstellung Berechtigte ist

---

431 Fallkonstellation von *Hilgendorf*, JuS 1996, 702 (705).

432 Zu den Anforderungen Nicht-Vermeidbarkeit bei § 17 siehe Tröndle/Fischer-*Tröndle*, § 17 Rn. 7 ff.

433 *Hilgendorf*, JuS 1996, 702 (705).

434 Tröndle/Fischer–*Tröndle*, § 202a Rn. 11; *Hilgendorf*, JuS 702 (705).

435 Zu § 17 UWG siehe Seite 145 ff.

436 So auch *Hilgendorf*, JuS 1996, 702 (705); NKStGB-*Jung*, § 202a Rn. 11. A.A. Lackner/Kühl-*Kühl*, § 202a Rn. 8

437 Der Strafantrag ist geregelt in §§ 77-77d.

438 BT-Drs. 10/5058, S. 29.

der über die Daten Verfügungsberechtigte.[439] In § 205 Abs. 2, S. 1, 2. HS ist für § 202a als Ausnahme zu den §§ 202-204 bestimmt, daß das Antragsrecht bei Tod des Verletzten nicht auf dessen Erben übergeht.[440]

Jessen[441] fordert die Umwandlung des absoluten Antragserfordernisses in ein relatives, nach dem bei Vorliegen eines öffentlichen Interesses auch ohne Strafantrag und damit gegebenenfalls auch gegen den Willen des Verletzten staatsanwaltliche Ermittlungen aufgenommen werden können. Er begründet dies damit, daß die Integrität der Datennetze ein Allgemeingut sei, hinter dem das Interesse des Verletzten, die Tat nicht öffentlich werden zu lassen, im Einzelfall unter Umständen zurücktrete. Die aufwendigen Ermittlungen seien Regulator genug, damit sich die Strafverfolgung auf schwerwiegende Fälle beschränke. Hiergegen ist einzuwenden, daß man dadurch dem in seinem Geheimhaltungsinteresse Verletzten einen zweiten Angriff auf dasselbe zumuten würde, obwohl er der Ansicht ist, daß sein Schaden damit nur vergrößert würde. *Jessens* Ansicht ist daher im Hinblick auf die Schutzrichtung des § 202a abzulehnen.

---

439 Schönke/Schröder-*Lenckner*, § 205 Rn. 4.

440 Kritisch dazu *Haft*, NStZ 1987, 6 (10).

441 *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 216 f.

Kapitel 3: Computerhacken und Strafrecht

A. Das bloße Eindringen in ein fremdes Computersystem (Hacken i.e.S.)

I. Betrachtung der gegenwärtigen strafrechtlichen Situation

1. Die Subsumtion des Hackens unter § 202a

Der Gesetzgeber wollte das Hacken i.e.S. nicht unter Strafe stellen. Dies erscheint insbesondere im Hinblick auf den gewählten Wortlaut der Norm als problematisch.[442]

Fallbeispiel:

Hacker X, der seinen Freunden beweisen will, daß er der Beste ist, schreibt ein Paßwortprogramm zum Ausspähen von Paßwörtern, um das Paßwort seines Vaters für das Firmen-Intranet zu erlangen. Dies gelingt, so daß X die Eingangsseite dieses Intranets[443] auf seinem Bildschirm aufgerufen hat. Im Bewußtsein seines Erfolgs steigt er sogleich wieder aus dem System aus und geht seiner Wege.

Hacker X könnte gem. § 202a strafbar sein. Es liegt eine besondere Sicherung im Sinne des § 202a vor, da der betreffende Intranetzugang mit einem Paßwortschutz versehen war. Die nicht unmittelbar wahrnehmbaren Daten i.S.d. § 202a Abs. 2 des Intranet sind nur für die Personen mit eigenem Zugang bestimmt, so daß auch kein Einverständnis zur Kenntnisnahme der Daten gegeben ist. Fraglich ist nun, ob sich X die Daten auf dem Eingangsbildschirm verschafft hat. Dazu müßte er die nicht notwendig alleinige Verfügungsgewalt über die Daten erlangt haben. Ein verkörpertes Erlangen der Daten über das Kopieren derselben ist im konkreten Fall nicht gegeben. X könnte aber von den Daten auf der Eingangsseite des Intranet Kenntnis genommen haben. Daß er in irgendeiner Weise Kenntnis von den Daten des geknackten Systems genommen hat, ist unumgänglich. Denn sonst hätte er nicht die Gewißheit über den erfolgreichen „Hack“ ge-

---

442 So hält, ohne näher darauf einzugehen, Lackner/Kühl-*Kühl*, § 202a Rn. 5 die Intention des Gesetzgebers für problematisch; kritisch auch *Dannecker*, BB 1996 1285 (1289). Zu den weiteren kritischen Äußerungen zu § 202a gerade auch im Hinblick auf die Nichtbestrafungsintention des Gesetzgebers, siehe Seite 131 ff.

443 Ein Intranet ist ein Netzwerk, welches überregional ist, jedoch nur ausgewählten Personen zur Verfügung steht. So betreibt beispielsweise die Firma IBM ein Intranet, in das sich die Mitarbeiter weltweit einloggen können.

habt. X mußte daher zumindest die Daten, die direkt nach der Sicherung wahrnehmbar gemacht werden, anschauen und diese als die Daten des geknackten Systems identifizieren. Damit hat er sich bei Zugrundelegen des Wortlauts zumindest eine kleine Menge an Daten durch Kenntnisnahme verschafft. Der objektive Tatbestand des § 202a wäre damit gegeben. Die restlichen Prüfungspunkte sind ebenfalls erfüllt. X wäre strafbar nach § 202a.

Aus dem obigen Fallbeispiel ergibt sich, daß beim Hacken das Eindringen in das System und Aufrufen der ersten Daten in einem einzigen Schritt erfolgt, so daß technisch nicht zwischen Eindringen und erstem Datenaufruf differenziert werden kann. In diesem Zusammenhang stellte schon *Hauptmann*[444] die berechtigte Frage, ob nicht möglicherweise wegen der Unwissenheit über diesen Umstand eine wirklichkeitsfremde Auffassung den Beratungen zu § 202a zugrunde gelegen habe. Folglich ist der gesetzgeberische Wille, das bloße Eindringen in fremde Computersysteme straffrei zu belassen, bei der Ausformulierung des Gesetzes nicht berücksichtigt worden.[445]

2. Ansichten zur Strafbarkeit des Hackens i.e.S.

a) Ansätze in Nachfolge der Ansicht des Gesetzgebers

(1) Teleologische Reduktion

Aus der Erkenntnis, daß das Hacken i.e.S. vom Wortlaut des § 202a erfaßt ist, folgt als eine Möglichkeit die teleologische Reduktion der Tathandlung „verschaffen", um dem Willen des Gesetzgebers Genüge zu leisten.[446] Die Lösungsmodelle, die auf einer teleologischen Reduktion des Tatbestands beruhen, sind zum Teil sehr unterschiedlich. Diesen Umstand kritisiert *Schmitz*[447]: „Der Hacker ist bei seinem Eindringen in fremde Datenanlagen darauf angewiesen, zumindest bestimmte Daten zu lesen um damit zur-Kenntnis zu nehmen, um zu wissen, auf welcher Ebene der Datenbank er sich befindet.

---

444 *Hauptmann*, JurPC 1989, 215 (217).

445 *Tiedemann*, JZ 1986, 865 (868); *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 180 f.; *Hilgendorf*, JuS 1997, 702 (704); aus diesem Grund lehnen *Zielinski*, Der strafrechtliche Schutz von Computersoftware, in: Kilian/Gorny (Hrsg.), Schutz von Computersoftware S. 120 und *Welp*, iur 1987, 353 (354) die Lösung des Gesetzgebers ab.

446 So ist Schönke/Schröder-*Lenckner*, § 202a Rn. 10 der Ansicht, daß sich der Wille des Gesetzgebers letztlich nur durch eine teleologische Reduktion des Merkmals „Verschaffen" gewinnen ließe, ohne selbst darauf einzugehen, wie diese Reduzierung der Tathandlung aussehen soll.

447 *Schmitz*, JA 1995, 478 (483).

Will man das reine Zur-Kenntnis-Nehmen der Daten (ohne speichern etc.) nicht grs. aus dem „Verschaffen“ herausnehmen -dann wäre auch straflos, wer Daten am Bildschirm liest und sich aufschreibt- kann, wer den Hacker straffrei stellen will, das Hacking nur durch eine teleologische Reduktion des Tatbestandes aus § 202a herausnehmen. Dann sollte freilich Einigkeit darüber bestehen, bis zu welcher Grenze ein Hacker gehen darf, um sich nicht strafbar zu machen.“ Diese Uneinigkeit soll im Folgenden dargestellt werden.

(a) Unterscheidung zwischen Systemzugriffsdaten und Daten *im* System

Der Vorschlag von *Tröndle*[448] besteht darin, zwischen Systemzugriffsdaten und Systemdaten zu differenzieren. Danach sei beim Computerhacker straflos noch das Ansehen von Daten, soweit es mit dem Zugriff auf das System verbunden ist, strafbar aber das Ansehen von Daten, die *im* System gespeichert sind. Somit ist nach *Tröndle* noch straflos das Ansehen des Eingangsmenüs des Systems, bzw. der Daten, die automatisch nach Eindringen auf dem Bildschirm erscheinen.

(b) Reproduzierbarkeit der Daten oder gesicherte Kenntnis

Nach *Hilgendorf*[449] ist es mit einer weiten Auslegung der Tathandlung, die auch jede Form der Kenntnisnahme als Verschaffen ansieht, jedoch unvereinbar, daß der Gesetzgeber das bloße Hacken, also das unbefugte Eindringen in fremde Rechner ohne Datenveränderung, nicht unter Strafe stellen wollte. Es würde deshalb den gesetzgeberischen Intentionen zuwiderlaufen, wenn man jedes Ansehen fremder Daten unter § 202a subsumieren würde. Um das Hacken nicht gegen den Willen des Gesetzgebers unter Strafe zu stellen, dürfe es deshalb für § 202a nicht ausreichen, daß fremde Daten bloß angeschaut werden; erforderlich sei vielmehr eine teleologische Reduktion der Norm: Der Eindringling müsse imstande sein, den **wesentlichen Informationsgehalt der Daten zu reproduzieren**. Bei großen Datenmengen sei dies nur mittels einer Kopie auf einen anderen Datenträger zu erreichen; in anderen Fällen würde auch die schriftliche Fixierung genügen. Das bloße Lesen reiche nur aus, wenn der Täter die wahrgenommenen Daten oder zumindest deren wesentlichen Gehalt später wiedergeben kann. Diese Anforderungen entsprechen im wesentlichen denen des § 96.

---

448 Tröndle/Fischer-*Tröndle*, § 202a Rn. 9.

449 *Hilgendorf*, JuS 1996, 702 (704).

Jähnke[450] verlangt gesicherte Kenntnis, wie bei § 96, und stellt folglich auf Verwertbarkeit der Kenntnis ab. Dies kann im Ergebnis nichts anderes ergeben, als das Kriterium der Reproduzierbarkeit der Daten.

(c) Speicherung auf anderem Datenträger

Hauptmann[451] will die nicht-materialisierte Variante des Verschaffens aus dem Tatbestand herausnehmen. Zum Eindringen soll noch zusätzlich das Übertragen der Daten auf einen Datenträger zum Ausfüllen der Tatbestandsmerkmals „verschaffen" notwendig sein. Grundlage dieser Auslegung ist die Definition des Hackens als unberechtigtes Eindringen und Umsehen in EDV-Systemen. Strafloses Hacken ist danach, und diese Definition wird auch für die Ansicht des Gesetzgebers zugrunde gelegt, nicht nur das bloße Eindringen in fremde Systeme, sondern auch das „Herumspazieren" im fremden System. Werde dies nun kriminalisiert, würden die Täter in den Untergrund gedrängt. Das Verbreiten der Erkenntnisse und Erfahrungen der Hacker in der Öffentlichkeit werde unterbunden. Das Abspeichern der Daten sei jedoch ein gesonderter Schritt, auf den beim straflosen Hacken verzichtet werden könne.

(2) Andere Ansätze zur Durchsetzung des gesetzgeberischen Willens

Neben der Möglichkeit, das Hacken i.e.S. über eine teleologische Reduktion aus dem Tatbestand herauszunehmen, sind auch andere Ansätze zur Lösung dieses Problems entwickelt worden.

(a) Weiterverwendungsabsicht

Kühl[452] ist bzgl. des Hackens i.e.S. der Ansicht, daß bloße Kenntnisnahme von den fremden Daten aus dem Tatbestand ausscheiden müsse, wenn sie notwendig mit dem Hacking verbunden ist und ihr keine Weiterverwendungsabsicht zugrunde liege. *Kühl* läßt damit dieselbe Lage anklingen, die *Tröndle*[453] schon aus dem Tatbestand herausnimmt. Notwendig mit dem Hacken verbunden ist das automatische Erscheinen der ersten Daten im geknackten System. Nimmt der Hacker von diesen Daten Kenntnis, so ist der Tatbestand nach *Kühl* im Gegensatz zu *Tröndle* jedoch erst dann nicht erfüllt, wenn der Hacker keine Absicht hegt, diese ersten Daten im System weiterzuverwenden.

---

450 LK-*Jähnke*, § 202a Rn. 6.

451 *Hauptmann*, JurPC 1989, 215 (217). Auch *Haft*, NStZ 1987, 6 (10) setzt Verschaffen mit Übertragen auf einen Datenträger gleich; ihm nachfolgend *Frommel*, JuS 1987, 667 (668).

452 Lackner/Kühl-*Kühl*, § 202a Rn. 7a.

453 Tröndle/Fischer-*Tröndle*, § 202a Rn. 9.

Hiermit wird die Tathandlung zunächst teleologisch reduziert, jedoch ebenso ein weiteres ungeschriebenes Merkmal mit überschießender Innentendenz hinzugefügt.

(b) Datennutzung

Auch *Zielinski*[454] sieht zunächst das Bedürfnis nach Restriktion der Tathandlung. Der Hacker müsse gesicherte Verfügungsmacht haben, so daß er sich erst durch Abspeichern auf Diskette oder sonstigem Dauerspeicher strafbar mache. Insoweit ist *Zielinski* noch derselben Ansicht wie *Haft*[455] und *Hauptmann*[456]. *Zielinski* befürchtet jedoch die Folge, daß die sofortige Nutzung oder Verwertung nur im Computer verfügbar gemachter Daten (mangels dauerhafter Speicherung) noch kein „verschaffen" darstellt. Das aber solle nach dem Willen des Gesetzgebers gerade strafbar sein. Daraus zieht er den Schluß, daß neben dem Abspeichern der Daten auch das „Verfügen über die Daten" i.S.v. Nutzen der Daten als Verschaffen zu werten ist.

b) Ansatz, der sich gegen den erklärten Willen des Gesetzgebers stellt

In der Literatur ist nur *Jessen*[457] der Ansicht, daß das Hacken i.e.S. strafbar i.S.d. § 202a ist.[458] Teilweise wird auch von *Gola*[459] angenommen, daß er das Hacking unter § 202a subsumiere.[460] Dies ist jedoch nicht der Fall, da *Gola* nur davon spricht, daß auch die sog. Hacker von § 202a betroffen seien. Dies ist zwar mißverständlich, dennoch kann von dem Begriff Hacker nicht auf die Bejahung der Strafbarkeit von Computerhacken geschlossen werden. Das Hacken ist i.S.d. Gesetzgebers das bloße Eindringen. Der Hacker kann jedoch durchaus auch von Daten Kenntnis nehmen, die sich innerhalb eines Systems befinden. Dann ist er strafbar nach § 202a.

---

454 *Zielinski*, Der strafrechtliche Schutz von Computersoftware, in: Kilian/Gorny (Hrsg.), Schutz von Computersoftware, S. 120.

455 *Haft*, NStZ 1987, 6 (10).

456 *Hauptmann*, JurPC 1989, 215 (217).

457 *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 179 ff.

458 *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 181 behauptet fälschlicherweise, *Möhrenschlager*, wistra 1986, 128 (139) hätte das Hacking unter § 202a subsumiert. Des weiteren merkt er an, dem Verfasser habe offensichtlich die Gesetzesmaterialien gefehlt. Dieser hat jedoch im Gegenteil gesehen, daß der Gesetzgeber bewußt darauf verzichtet hat, schon den bloß unbefugten Zugang zu besonders gesicherten Daten unter Strafe zu stellen.

459 *Gola*, NJW 1987, 1675 (1679).

460 So *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 181; *Binder*, Strafbarkeit intelligenten Ausspähens von programmrelevanten Unternehmensgeheimnissen, S. 42.

Jessen[461] kritisiert die Straflosigkeit des Hackens i.e.S..[462] Er sieht eine eindeutige Subsumierbarkeit des Hackens i.e.S. unter § 202a und knüpft daran die Ansicht, daß der subjektiv-historische Wille des Gesetzgebers seine Grenze finde in der von *Jescheck/Weigend*[463] als Andeutungstheorie bezeichneten Auslegungsmethodik. Diese von der Rechtsprechung[464] und der Literatur[465] gleichermaßen entwickelten und vom Primat der teleologischen Auslegung ausgehende Einschränkung der historischen Auslegung berücksichtige den Willen des Gesetzgebers nur insoweit, „als er in dem Gesetz selbst einen hinreichenden Ausdruck gefunden" habe.[466] Diese Grenze gelte auch unabhängig vom Alter der zu bewertenden Norm. Damit ist nach *Jessen* in Nachfolge der Andeutungstheorie auf Grund des eindeutigen Wortlauts des § 202a und teleologischer Gesichtspunkte, wie der problematischen Beweisführung und der Rechtsgutsverletzung i.S.v. § 202a bei jedem Anzeigen von Informationen, das Hacken i.e.S. entgegen dem ausdrücklichen Willen des Gesetzgebers strafbar.

3. Stellungnahme

a) Andeutungstheorie

Jessen[467] verkennt in der Begründung seiner Ansicht, daß es bei der sog. Andeutungstheorie, die zwischen der subjektiven Theorie, die allein den Willen des historischen Gesetzgebers für maßgeblich hält und der objektiven Theorie, die den objektivierten „Willen des Gesetzes" in den Vordergrund stellt, vermitteln will, sehr wohl auch auf eine zeitliche Komponente ankommt. So soll nach der Andeutungstheorie der wenn auch nur ansatzweise ausgedrückte Willen des Gesetzgebers den Sinngehalt der Norm ausfüllen, wenn nicht zwingende Gründe der Gerechtigkeit, die Entwicklung der Ver-

---

461 *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 179 ff.

462 Mit den Argumenten, die unten auf Seite 131 ff. aufgeführt sind.

463 *Jescheck/Weigend*, AT, § 17 IV 2.

464 Unter Zitierung von BVerfGE 1, 299 (312); BVerfGE 10, 234 (244); BVerfGE 11, 126 (130); BGHSt 1, 74 (76); 11, 52 (53)

465 Von *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, werden hier *Bender*, JZ 1957, 593 (594); *Bockelmann/Volk*, StR-AT, S.21; *Jescheck*, AT, § 17 IV 2 (nun *Jescheck/Weigend*) als Vertreter der Literatur angeführt.

466 *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, zitiert BVerfGE 11, 126 (130).

467 *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 179 ff.

hältnisse oder einfach nur der Geist der Zeit die Wertentscheidung der Vergangenheit als überholt erscheinen lassen.[468]

Besonders zu berücksichtigen dabei ist im Gegensatz zu den Ausführungen *Jessens* das **Zeitmoment**. So zitieren *Jescheck/Weigend* die Formel des Bundesverfassungsgerichts: Neue Gesetze werden eher aus den Materialien auszulegen sein, während bei alten Gesetzen der durch die Rechtsanwendung erarbeitete objektive Bedeutungsgehalt mehr in den Vordergrund tritt.[469] Bei § 202a handelt es sich weder um ein altes Gesetz, da es aus dem Jahre 1986 stammt, noch haben sich die Verhältnisse derart geändert, daß an dem nicht nur andeutungsweise geäußerten Wille des Gesetzgebers nunmehr eine andere Sicht des Hackens i.e.S. zwingend wäre. Bloßes Eindringen bleibt ein solches, auch wenn durch die Entwicklung des Internets die Hackversuche enorm an Zahl und Art zugenommen haben. Dies ändert nichts an möglichen kriminalpolitischen Erwägungen, den § 202a zu reformieren oder das Hacken i.e.S. selbständig unter Strafe zu stellen. De lege lata ist das Hacken i.e.S. straflos.

b) Datennutzung

Das von *Zielinski*[470] eingeführte Kriterium, das bloße Nutzen gespeicherter Daten ohne Übertragung auf andere Datenträger als „verschaffen" von Daten zu werten, ist abzulehnen. Das Nutzen von Daten tangiert nicht das Geheimhaltungsinteresse des Berechtigten, solange von den gespeicherten Daten keine Kenntnis genommen wird. Dies würde bedeuten, daß der sog. Zeitdiebstahl, d.h. die unbefugte Nutzung von Rechenzeiten, durch die Hintertür strafbar würde.[471]

c) Speicherung auf anderen Datenträger

Die Ansicht *Hauptmanns*[472] hat den Vorzug großer Transparenz. So ist der Umstand der Abspeicherung ein Vorgang in der Außenwelt, der leicht ermittelt werden kann. Dennoch ist die gänzliche Herausnahme der nicht-materialisierten Erlangung der Verfügungsgewalt und sogar von Teilen des materialisierten Verschaffens von Daten abzu-

---

468 Vgl. BGHSt 2, 194 (204).

469 *Jescheck/Weigend*, AT, § 17 IV 2; BVerfGE 34, 288 ff.

470 *Zielinski*, Der strafrechtliche Schutz von Computersoftware, in: Kilian/Gorny (Hrsg.), Schutz von Computersoftware, S. 120.

471 Zum sog. Zeitdiebstahl, der eine Parallele zur Gebrauchsanmaßung i.S.d. § 248 b darstellt siehe eingehend *Schulze-Heiming*, Der strafrechtliche Schutz der Computerdaten, S. 15 und 254 ff.

472 *Hauptmann*, JurPC 1989, 215 (217).

lehnen. So kann nicht geleugnet werden, daß beispielsweise das schriftliche Notieren von Daten oder das Photographieren des Bildschirms materialisierte Verfügungsgewalt über Daten und damit erhebliches Gefahrenpotential beinhalten. Hinzu kommt, daß nichtwahrnehmbare Daten i.S.d. § 202a nicht nur Computerdaten sind, sondern beispielsweise auch Daten auf einem Mikrofilm. Diese Daten können nun schwerlich auf einen anderen Datenträger kopiert werden. Bei ihnen kann ein Verschaffen nur durch Photographie oder Kenntnisnahme erfolgen. Nach der Lösung *Hauptmanns* wäre der Mikrofilm nicht mehr durch § 202a geschützt. Die Kenntnisnahme von Daten stellt als nicht-materialisiertes Erlangen der Verfügungsgewalt über Daten (Informationen) eine notwendige Voraussetzung für das Erreichen des Gesetzeszwecks dar. Daten sind eben dann nicht mehr geheim, wenn sie ein anderer unbefugt zur Kenntnis genommen hat. Diese Tatvariante darf daher nicht aus dem Tatbestand herausgenommen werden.

d) Weiterverwendungsabsicht

Die Hinzunahme eines ungeschriebenen Merkmals der Weiterverwendungsabsicht ist abzulehnen. Zunächst hat die Auslegung der vorhandenen Tatbestandsmerkmale im Vordergrund zu stehen. Wenn danach noch ein unweigerliches Bedürfnis zur Konkretisierung eines Tatbestands oder der Abgrenzung eines Tatbestands von einem anderen besteht,[473] kann die Annahme eines ungeschriebenen Tatbestandsmerkmals notwendig sein. Hier ist hingegen ein solches Bedürfnis nicht ersichtlich, wie unten noch zu zeigen sein wird. Darüber hinaus erscheint Weiterverwendungsabsicht als Begriff zu weit. Es ist nicht klar, was damit gemeint sein soll. Soll dies nur Absicht der Datenverwertung wirtschaftlicher Art sein oder sollen auch Motive rein privater Natur ausreichen? Aus diesen Erwägungen folgt, daß dieses zusätzliche Kriterium zur Eingrenzung des Tatbestands des § 202a untauglich ist.

e) Reproduzierbarkeit versus Datendifferenzierung

Nun bleibt nur noch die Untersuchung der beiden verbleibenden Ansichten, die grs. gegenüber den anderen vorzugswürdig erscheinen.

Grundproblem jeden Versuchs teleologischer Reduzierung der Tathandlung ist, daß jegliche Daten i.S.d. § 202a Abs. 2 taugliches Tatobjekt des § 202a Abs. 1 sein können, ohne daß es auf die Art oder Qualität der Daten ankäme. Alle Daten, seien sie noch so simpel oder gar unsinnig, sind, falls sie durch eine besondere Zugangssicherung ge-

---

[473] Wie bei dem allgemein anerkannten ungeschriebenen Merkmal der Vermögensverfügung in § 263.

schützt sind, von § 202a erfaßt. Folglich ist bei der oben dargestellten Tatvariante der Kenntnisnahme das Problem gegeben, daß grs. jede Kenntnisnahme auch nur kleinster Datenmengen den Hacker strafbar machen würde.

Hilgendorf[474] schafft mit dem von ihm eingeführten Kriterium der Reproduzierbarkeit ein griffiges Kriterium zur Abgrenzung des bloßen Lesens, ohne daß sich der Lesende wirklich für den Inhalt der Daten interessiert, wie es beim Hacker der Fall ist, vom Datenspion, den nicht das Eindringen in fremde Systeme interessiert, sondern in erster Linie die Informationen selbst. Es wird die Tatvariante der Kenntnisnahme der Daten richtigerweise nicht aus dem Tatbestand herausgenommen, sondern eine Qualität der Kenntnisnahme der Daten gefordert, die beim bloßen Eindringling (Hacker i.e.S.) nicht vorliegt.

Dieser Ansatz ist jedoch im Hinblick auf die obigen Ausführungen problematisch. Sind jegliche Daten taugliches Tatobjekt, so kann in den meisten Fällen des Hacking davon ausgegangen werden, daß sich der Eindringling auch nur geringste Datenmengen gemerkt hat und diese reproduzieren kann (und wenn es auch nur ein Buchstabe ist), möglicherweise sogar, ohne daß dies absichtlich geschieht. Dann läge aber ein Verschaffen der Daten vor. Der Hacker wäre fast immer strafbar. Daher ist die Qualität der Kenntnisnahme für § 202a kein taugliches Kriterium zur Lösung des Hacking-Problems.

Tröndle[475] hingegen wählt einen anderen Ausgangspunkt. Er nimmt bestimmte Daten, von denen der Hacker unweigerlich nach dem Eindringen Kenntnis nimmt, aus dem Tatbestand heraus. Diese Ansicht hat den Vorzug, daß sie trotz Kenntnisnahme von Daten, die im fremden System gespeichert sind, das Hacken i.e.S. aus dem Tatbestand herausnimmt. Geht es dem Hacker nur um das bloße Eindringen an sich, so ist er sich dessen frühestens dann bewußt, wenn er die Daten zur Kenntnis nimmt, die automatisch beim ersten Schritt in das System aufgerufen werden. Das Eindringen ist damit vollendet. Gibt nun der Hacker weitere Befehle ein, um weiter in das System vorzudringen, spaziert er also im geknackten System herum, so nimmt er unweigerlich Daten wahr und auch nur geringste Datenmengen zur Kenntnis.

Das formelle Geheimhaltungsinteresse des Berechtigen ist nunmehr verletzt. Der Berechtigte wollte gerade nicht, daß Daten, die erst durch weitere Befehle wahrnehmbar gemacht werden, in irgendeiner Weise zur Kenntnis genommen werden. Gibt der Hakker einen Befehl ein, der ihm weitere Daten des Systems anzeigt, so macht er sich daher

---

474 *Hilgendorf*, JuS 702 (704).

475 Tröndle/Fischer-*Tröndle*, § 202a Rn. 9.

strafbar nach § 202a, da er Daten zur Kenntnis nimmt, die mit dem Vorgang des Eindringens nicht unmittelbar und automatisch verbunden sind. Es bleibt ihm lediglich das sofortige Verlassen des Systems. Gibt er diesbezügliche Befehle ein und nimmt er infolgedessen weitere Daten wahr, so ist dies ein mit dem bloßen Eindringen unweigerlich verbundener Vorgang. Wer nur Eindringen will, steigt sofort wieder aus. Das sofortige Verlassen des Systems ist folglich notwendiger Bestandteil des Hackens i.e.S. und damit ebenfalls straflos.

Nach der hier vertretenen Ansicht werden auch Beweisführungsprobleme minimiert. Durch Protokollierung der Vorgänge im System, in der Weise, daß der Hacker nach dem ersten Schritt, dem Eindringen, weitere Schritte im System geht oder vornimmt, wären ein starkes Indiz für die Vollendung einer Straftat nach § 202a Abs. 1.

II. Betrachtung der kritischen Äußerungen zur Intention des Gesetzgebers

Im Folgenden sollen die Argumente gegen die Nichtpönaliserung des Hackens, welche mehrfach unter Kritik stand, gesammelt und dargestellt werden. Daraufhin wird dazu und zu der Thematik insgesamt Stellung genommen.

1. Die Kritikpunkte in der Literatur

a) Strafwürdigkeit (Rechtsgutsproblematik)

Der Gesetzgeber hält das Hacken i.e.S. nicht für strafwürdig. Begründet wird dies damit, daß in den Beratungen zwar darauf hingewiesen wurde, daß mit dem erfolgreichen Eindringen in fremde Datenbanken Integritätsinteressen von Betreibern und Benutzern gefährdet werden könnten und eine zu starke Systembelastung eintreten könne.[476] Insoweit stelle ein solches Verhalten erst eine Gefährdung dar, die für den Rechtsausschuß als Ansatzpunkt für einen neuen Straftatbestand in diesem Bereich nicht ausreicht.[477]

Dieser Standpunkt wurde kritisiert. *Granderath*[478] hält die Begründung des Rechtsausschusses durch die Wirklichkeit schon für überholt. Er beleuchtet dies anhand eines Falles aus der Presse.[479] Mit diesem will er belegen, daß allein schon das Hacking ein immenses Schadenspotential hat. So berichtet er, daß die New Yorker Cornell-Universität aufgrund von Hacking den Teil ihrer Datenverarbeitungsanlagen endgültig abschalten mußte, der internationale Verbindungen zwischen Computersystemen wissenschaftlicher Institute vermittelte. Somit zeige sich an diesem Beispiel, daß durch Hacking volkswirtschaftliche Schäden höchsten Ausmaßes drohen und schon eingetreten seien, deren strafrechtliche Erfaßbarkeit in der Bundesrepublik davon abhänge, ob den Tätern bedingter Schädigungsvorsatz nachgewiesen werden kann (so daß eine Strafbarkeit nach § 303a vorliegt), oder ob sie einfach nur zu dumm gewesen waren, weit genug zu denken.

---

476 BT-Drs. 10/5058, S. 28.

477 BT-Drs. 10/5058, S. 28.

478 *Granderath*, 2. WiKG, DB 1986 Beilage Nr. 18, S. 1 ff.

479 *Granderath* zitiert aus einem Artikel der Rheinischen Post, 27.1.1986.

Lenckner/Winkelbauer[480] sind der Ansicht, daß an der Begründung des Gesetzgebers zwar zutreffend sei, daß Vorfeld- oder Gefährdungstatbestände auf den Bereich hochwertiger Rechtsgüter beschränkt bleiben sollten. Um solche handele es sich – legt man die Strafdrohung (Freiheitsstrafe bis zu drei Jahren oder Geldstrafe) zugrunde – bei den von § 202a geschützten Rechtsgütern zwar nicht. Doch ginge es bei dem fraglichen Vorschlag (d. Verf.: es lag ein Vorschlag des Bundesjustizministeriums vor, welcher das Hacking i.e.S. unter Strafe stellen wollte[481]) auch nicht um einen reinen Gefährdungstatbestand, der sich lediglich gegen Vorbereitungshandlungen zur Datenspionage richtete, vielmehr erfasse der Vorschlag bereits durch das Eindringen in fremde Rechtssphären verwirklichte Unrecht.

Auch *Volesky*[482] hält das Hacken i.e.S. für strafwürdig. Dies folgert er aus einer Untersuchung der Regelungsvorschläge der Law Commission in Groß-Britannien zum Hakken, nach denen das Hacken i.e.S. unter Strafe zu stellen ist.[483] Die bisherigen Vorstellungen (damit meint *Volesky* den Hacking-Begriff des Gesetzgebers[484]) blieben hinter dem tatsächlichen Verhalten der Hacker nach dem heutigen Kenntnisstand zurück. Die Bedrohung durch Hacker, auch wenn diese sich nur mit dem Überwinden der Zugangssicherung begnügen sollten, führe nicht zu einer geringfügigen Systembelastung, sondern zu weitreichenden Konsequenzen. Mit dem Vertrauensverlust in Computersysteme gehe deren eigentlicher Nutzen, der schnelle und weitgehend offene Datenaustausch, in entscheidendem Maße verloren.

b) Beweisführung

Granderath[485] hebt vor allem das Problem der Beweisführung hervor. So ist seiner Ansicht nach zu bedauern, daß eine Strafvorschrift gegen das Eindringen in fremde Datenverarbeitungssysteme (Hacking) nicht verwirklicht worden ist. Angesichts technischer Nachweisschwierigkeiten werde es häufig so sein, daß Strafverfolgungsbehörden schon froh sind, wenn sie überhaupt feststellen können, wer in ein System eingedrungen ist, ohne ihm den Abruf von Daten, den Versuch von betrügerischen Datenveränderungen oder Ähnliches nachweisen zu können. Eine Strafvorschrift gegen Hacking hätte es ver-

---

480 *Lencker/Winkelbauer*, CR 1986, 483 (488).

481 Vgl. *Engelhard*, DVR 1985, 165 (171).

482 *Volesky*, CR 1991, 553 ff..

483 Selbst der Versuch dazu soll hiernach unter Strafe gestellt werden.

484 Siehe dazu Seite 18 ff.

485 *Granderath*, 2. WiKG, DB 1986 Beilage Nr. 18, S. 1 ff.

hindert, daß solche Täter straffrei davonkommen; sie hätte als Vorfelddelikt zu Straftaten nach §§ 202a , 263a , 269 oder 303a eine wichtige Funktion gehabt.

Auch *Lenckner/Winckelbauer*[486] weisen darauf hin, daß durch die Ablehnung der Strafbarkeit des Hackens i.e.S. die Praktikabilität der Norm insgesamt leide. Zwar beschränke sich das „Hacking" in den seltensten Fällen auf den bloßen Zugang, eine Beweisführung dürfte aber bei einer entsprechenden Einlassung nur sehr eingeschränkt möglich sein.

In diesen kritischen Ausführungen wird die Besorgnis deutlich, daß der Hacker, der Daten, die sich auf dem geknackten fremden System befinden, auswendig lernt, um dieselben reproduzieren zu können und damit von diesen Daten sogar gesicherte Kenntnis nimmt (wie bei § 96), sich darauf berufen könnte, sogleich wieder aus dem System ausgestiegen zu sein, ohne die geringste Kenntnis von den Daten genommen zu haben. Das Gegenteil ist ihm nur dann zu beweisen, wenn die „Spaziergänge" des Betreffenden protokolliert sind, oder er auf frischer Tat ertappt wird. Jedoch ist im ersteren Fall immer noch fraglich, ob ihm Kenntnisnahme nachgewiesen werden kann.

c) Argumentation des Gesetzgebers §§ 303a, 303b schütze vor starken Störungen

Auch das Argument des Gesetzgebers, daß §§ 303a, 303b u.U. eingreife, wenn starke Störungen durch das Hacking eintreten, stößt auf Kritik. So hält *Jessen*[487] dies für nicht stichhaltig, da es den Hackern oft am entsprechenden Vorsatz mangele oder dieser oft nicht nachweisbar sei. Hacker, die sich mit dem Eindringen in ein Computersystem begnügen, wollen gerade nicht das betreffenden System belasten oder Daten verändern. Ihnen fehlt der Vorsatz für § 303a oder § 303b.

2. Stellungnahme

Zunächst ist bei der Erörterung der Frage, ob das unbefugte Eindringen in Computersysteme oder Datenbereiche unter Strafe zu stellen ist, ein Strukturieren der Problembereiche erforderlich. So ist in einem ersten Schritt die Erforderlichkeit einer strafrechtlichen Sanktionierung zu prüfen. Diese Erforderlichkeit kann dann weiter in zwei Untergruppen aufgeteilt werden. Zum einen ist die Tatsachenseite zu prüfen: Feststellung der Beeinträchtigung von Interessen und deren Erheblichkeit und tatsächliche Möglichkeit der

---

486 *Lenckner/Winkelbauer*, CR 1986, 483 (488).

487 *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 183 unter Berufung auf *Granderath*, 2. WiKG, DB 1986 Beilage Nr. 18, S. 2.

Verhinderung von Hackerattacken. Zum anderen ist die rechtliche Seite zu berücksichtigen: Die Strafwürdigkeit dieses Verhaltens in Form der Feststellung eines neuen Rechtsgutes oder der Einbindung in ein schon (an-) erkanntes Rechtsgut. Sind diese Fragestellungen im Sinne einer Pönalisierung de lege ferenda beantwortet, ist nach der Ausgestaltung einer neuen Norm oder der Anpassung des § 202a im Wortlaut zu fragen.

a) Grundlagen einer Pönalisierung de lege ferenda

(1) Tatsachenseite

In Frage steht hier die Bestrafung des bloßen Eindringens. Das Interesse, welches mit diesem Verhalten gefährdet wird, ist ein Integritätsinteresse an Daten, Computersystemen und Dienstleistungsangeboten, die für Nichtautorisierte nicht zugänglich sein sollen. Zu diesem Zweck werden dafür regelmäßig Hindernisse gegenständlicher oder datenmäßiger Art eingerichtet, um zum einen dem Unberechtigten zu signalisieren, daß er „draußen" bleiben soll, und zum anderen ihn auch tatsächlich abzuhalten. Diese Sicherungen können jedoch nicht alle abwehren, sondern sie können mit entsprechendem Spezialwissen oder unter Anwendung spezieller Programme überwunden oder umgangen werden. Dringt nun ein Hacker in ein System ein und verschwindet sofort wieder, so sind die Integritätsinteressen des Systembetreibers tangiert, da der Zugang zu den Daten jederzeit befürchtet werden muß.

Werden nach einem Hackerfolg Sicherheitslücken publik gemacht, so profitiert die Allgemeinheit von dieser Information. Sie kann einschätzen, wie sicher solche Systeme sind, bei denen der Einzelne möglicherweise seine Kreditkartennummer speichern läßt oder bei denen er Online-Banking nutzt. Der Systembetreiber jedoch hat grs. kein Interesse an der Veröffentlichung einer Hackerattacke, da er dadurch einen enormen Imageverlust zu erwarten hat. Hieraus erklärt sich auch, daß eine Strafanzeige wegen Verhaltens i.S.d. § 202a höchst selten gestellt wird, da insbesondere in einem anschließenden Strafprozeß Öffentlichkeit hergestellt werden würde.[488]

Festzustellen ist daher eine paradoxe Situation. Auf der einen Seite würde eine strafrechtliche Sanktionierung des Eindringens zu einer Stärkung des Integritätsschutzes von Daten und Systemen führen, andererseits scheuen gerade die möglichen Profiteure einer solchen Stärkung die Inanspruchnahme strafrechtlichen Schutzes. Aus der Perspektive

---

[488] Diesen Umstand hob der Abteilungsleiter des Referats für Computerkriminalität beim LKA Stuttgart bei einem Gespräch am 28.10.1999 mit dem Verfasser hervor.

der Nutzer von Netzdienstleistungen wäre eine strafrechtliche Sanktionierung wohl nicht von Interesse, da die „sportlichen“ Hacker davon abgehalten würden, weiter zu hacken oder die Hackergebnisse zu veröffentlichen.

Die Interessenlage der möglichen Rechtsgutsinhaber (hauptsächlich Systembetreiber) ist jedoch im Ergebnis im Sinne einer Pönalisierung zu beurteilen. Zum einen spricht dafür, daß eine Bestrafung des Eindringens die Täter abhalten könnte, zum anderen kann gerade nach dem Schließen einer Sicherheitslücke das Interesse bestehen, gegenüber dem Hacker, der vorher ins System eingedrungen ist, ein deutliches Signal zu setzen, indem er bei den Ermittlungsbehörden angezeigt werden kann. Dies kann auch ohne Entstehung eines Imageschadens ablaufen, wenn die Sicherheitslücke nach dem Eindringen wirksam geschlossen werden konnte. Die Verletzung des Integritätsinteresses an Systemen und Datenbereichen ist auch in den meisten Fällen nicht nur unerheblich, da die Systembetreiber aufgrund von Hackerangriffen immer größeren personellen und finanziellen Aufwand betreiben müssen. Der „sportliche“ Angriff kann, während er abläuft, gerade nicht von dem Angriff, bei dem eine Schädigung des Angegriffenen oder eine Bereicherung des Angreifers zu befürchten ist, unterschieden werden. Zumal auch beim Hacken i.e.S. eine unvorsätzliche Schädigung nicht ausgeschlossen werden kann.

Die Einteilung des Gesetzgebers in solche Verhaltensweisen, die sich in einem bloßen Eindringen in Computersysteme oder Datenbereiche erschöpfen und solchen, die darüber hinaus auch noch ein Datenverschaffen darstellen, erscheint lebensfremd. Auch der gutwillige Hacker, der sich der sog. Hackerethik[489] verschrieben hat, wird sich zumindest die Verzeichnisstruktur der im gehackten System gespeicherten Daten ansehen und auch darüber hinaus ausgewählte Daten aufrufen und zur Kenntnis nehmen. Ein datenbezogener „coitus interruptus“ ist praktisch auszuschließen. Will man Hacker i.S.d. Eigendefinition der Hackerszene von sog. Crackern unterscheiden[490] und die einen straffrei stellen und jene nicht, so ist nach einem anderen Unterscheidungskriterium zu suchen. Dies zeigt sich übrigens auch darin, daß das bloße Eindringen im Wortlaut des § 202a enthalten ist. Auf Tatsachenseite spricht daher vieles für eine Bestrafung des bloßen Eindringens in geschützte Computersysteme und Datenbereiche.

---

489 Zur Hackerethik siehe Seite 10.

490 Zur Unterscheidung von Hackern und Cracken siehe Seite 11.

(2) Strafwürdigkeit (rechtliche Seite)

Der damalige Gesetzgeber erachtete das Hacken i.e.S für nicht strafwürdig. Jedoch klingt in der Gesetzesbegründung selbst schon an, was *Lenckner/Winckelbauer* richtigerweise bemerkt haben. So heißt es in Begründung: Für eine Kriminalisierung ist zwar schon darauf hingewiesen worden, daß mit dem erfolgreichen Eindringen in fremde Datenbanken Integritätsinteressen von Betreibern und Benutzern gefährdet werden können und eine starke Systembelastung eintreten kann.[491] Bis dahin kann den Ausführungen ohne weiteres gefolgt werden. Mit *Lenckner/Winckelbauer*[492] ist jedoch festzustellen, daß mit Eindringen in ein geschütztes Computersystem oder in einen geschützten Datenbereich nicht lediglich eine Gefährdung von Integritätsinteressen vorliegt, sondern diese vielmehr schon als verletzt zu erachten sind. Die eigentlich nicht für den Hacker zur Benutzung oder zur Kenntnisnahme bestimmten Daten liegen diesem nach dem Eindringen gleichsam zu Füßen. Die faktische Möglichkeit zur Manipulation oder zur Kenntnisnahme reicht für die Verletzung der Datenintegrität aus.

Damit ist mit den Ausführungen zur Strafwürdigkeit[493] festzustellen, daß das Vertrauen in die Integrität und Verläßlichkeit vernetzter Computersysteme als Rechtsgut für einen Straftatbestand, der Hacken i.e.S. unter Strafe stellt, durchaus in Frage kommt. Ausgehend von dieser Annahme ist es dann nicht mehr weit zu einem Vergleich des Eindringens in fremde Computersysteme mit dem unbefugten Eindringen in die Wohnung, in die Geschäftsräume oder in das befriedete Besitztum eines anderen nach § 123. Das Hacking stellte danach einen „elektronischer Hausfriedensbruch“[494] dar.[495] Rechtsgut wäre dann ein elektronisches oder virtuelles[496] Hausrecht. Dies stellte dann eine Komponente des Verfügungsrechts über Daten, welches zum einen in § 202a und zum anderen in §§ 303a, 303b schon geschützt ist, in der Ausprägung eines Rechts auf Integrität der Daten und des Vertrauens in tatsächlich geschützte Systeme oder Datenbereiche dar.

---

491 BT-Drs. 10/5058, S. 28 f.

492 *Lenckner/Winckelbauer*, CR 1986, 483 (488).

493 Siehe Seite 131.

494 Begriff schon zu finden in „recht“, Informationen des BMJ 1985, 56.

495 *Goldmann/Stenger*, CR 1989, 543 (546) mahnen auf Grund dieser Überlegung an, daß die Frage nach der Strafbarkeit des bloßen Umschauens in fremden Datenbanken vom Gesetzgeber noch einmal aufgegriffen wird. Zur möglichen Strafbarkeit des Umschauens de lege lata siehe Seite 163.

496 Virtuell heißt nicht physikalisch vorhanden, sondern gedacht, vo rgespiegelt, nachgebildet (vgl. *Grieser/Irlbeck*, Computerlexikon, S. 948); in diesem Zusammenhang wird die Software, die den Zugang zum Internet bietet und sonstige Dienstleistungen als künstliches Haus angesehen, welchem dann auch ein Hausrecht zugeordnet wird.

b) Ausgestaltung

Bei der Ausgestaltung einer Pönalisierung bieten sich zwei Varianten an. Die ausdrückliche Aufnahme des Eindringens in den Tatbestand des § 202a als Handlungsalternative, oder die eigenständige Normierung einer Strafnorm in Anlehnung an § 123. Den Versuch bei § 202a unter Strafe zu stellen, würde das gewünschte Ziel nicht erreichen, da auch hier die teleologische Reduktion des Verschaffens von Daten zum Ergebnis hätte, daß bei bloßem Eindringen der Vorsatz zum Verschaffen von Daten fehlt.

Anzudenken ist bei der Entscheidung für die eine oder andere Variante, daß bei Anlehnung an § 123 ein neues Tatobjekt in Form des elektronischen oder virtuellen Hauses oder Geschäftsraums[497] entwickelt werden könnte, so daß sich die Strafbarkeit des bloßen Eindringens auch nur auf solche Computersysteme oder Datenbereiche erstrecken würde, die ein erhöhtes Integritätsinteresse oder ein erhöhtes Vertrauen ihrer Benutzer benötigen. Damit wäre den tatsächlichen Anforderungen am besten gedient. Hier wären vor allem ans Internet angeschlossene virtuelle Geschäftsräume und ebenso private Homepages als Tatobjekt zu schützen. Die zweite Variante, die Anlehnung an den Hausfriedensbruch (§ 123) wird daher im Sinne einer sinnvollen Begrenzung der Strafbarkeit als vorzugswürdig erachtet. Damit das Interesse an der Integrität der Daten und zum Ausdruck kommt, ist auch hier das Erfordernis einer besonderen Sicherung einzufügen.

---

497 Sog. e-commerce.

B. Das Hacken im weiteren Sinne

Wie oben[498] schon angedeutet, ist die Grundsituation des Hackens i.w.S. die, daß der Hacker in das geschützte System eingedrungenist oder Zugang zu geschützten Daten innehat, dann aber nicht sofort das System verläßt oder die geschützten Daten unbehelligt läßt. In diesem Fall nimmt er entweder von Daten, die geschützt werden sollten, Kenntnis, kopiert solche Daten auf einem in seinem Gewahrsam befindlichen Datenträger oder manipuliert die Daten, womöglich auch die Hardware des Computersystems selbst. Es wird im Folgenden nach der Qualität der angegriffenen Daten differenziert. Innerhalb dieser Einteilung wird weiter zwischen verschiedenen Angriffsarten unterschieden.

I. Angriffe auf Daten i.S.d. § 202a Abs. 2

1. Kenntnisnahme, Kopie oder Wegnahme des Datenträgers

Diese Handlungen stellen Varianten des „Verschaffens“ von Daten gem. § 202a Abs. 1 dar. Der Hacker macht sich in diesen Fällen nach § 202a strafbar. Bei der Variante der Kenntnisnahme ist dies jedoch erst dann gegeben, wenn er Daten zur Kenntnis genommen hat, die er durch einen ersten Schritt nach Eindringen in das geschützte System zur Kenntnis genommen hat.

2. Manipulationen

Nimmt der Hacker Manipulationen an den geschützten Daten vor, so kann er sich nach § 303a oder § 303b strafbar machen.

a) Datenveränderung, § 303a

Geschütztes Rechtsgut des § 303a ist nach der h.A. das Verfügungsrecht über Daten in der speziellen Ausprägung des Interesses an der uneingeschränkten und unversehrten Verwendbarkeit derselben.[499] Das Vermögen[500] kann wegen der nicht nur systemati-

---

498 Siehe Seite 20 ff.

499 Schönke/Schröder-*Stree*, § 303a Rn. 1; Tröndle/Fischer-*Fischer*, § 303a Rn. 2; *Welp*, iur 1988, 443 (448); *Tiedemann*, JZ 1986, 865 (870); *Hilgendorf*, JuS 1996, 890.

schen Nähe zu § 303, der das Verfügungsrecht über Sachen schützt und zwar unabhängig von deren Wert[501], nicht als Rechtsgut angesehen werden.

Tatobjekt sind Daten i.S.d. § 202a Abs. 2.[502] Eine besondere Sicherung der Daten, wie in § 202a, ist nicht erforderlich. § 303a enthält vier Tathandlungsvarianten, das Löschen, das Unterdrücken, das Unbrauchbarmachen sowie das Verändern von Daten. Der von *Hilgendorf* postulierten trennscharfen Abgrenzung der Varianten ist zu folgen.[503]

Das Löschen von Daten ist dann gegeben, wenn sie vom Datenträger entfernt oder unwiederbringlich unkenntlich gemacht werden.[504] Wird jedoch beispielsweise im verbreiteten Betriebssystem Windows eine Datei „gelöscht", so wird lediglich der Icon, der für den Aufruf der Datei zuständig ist, in den sog. Papierkorb verschoben (sog. logisches Löschen). Die Datei bleibt damit physikalisch erhalten. Auch das „Löschen" aus dem Papierkorb erzeugt lediglich eine Markierung der Daten und dadurch die Freigabe zum Überschreiben derselben. Mit einem Hilfsprogramm können solche Daten vielfach wieder gefunden werden. Folglich ist hierdurch noch kein „Löschen" i.S.d. § 303a gegeben. Das Formatieren[505] eines Datenträgers ist unzweifelhaft ein „Löschen" i.S.d. § 303a. Allerdings fällt unter das Löschen von Daten auf einem Datenträger auch die Beschädigung desselben i.S.d. § 303, da dessen Funktion als Träger dieser Daten verloren geht.[506]

Daten werden dann i.S.d. § 303a unterdrückt, wenn sie ohne Löschen dem Zugriff des Berechtigten auf Dauer oder zeitweilig entzogen werden.[507] *Hilgendorf*[508] nennt als Beispiele das oben angesprochene logische Löschen, die Entwendung oder Unterschlagung des Datenträgers, die Vorschaltung eines unbekannten Paßworts oder das Umbenennen von Dateien.

---

500 So aber *Haft*, NStZ, 1987 6 (10) und *Welp*, iur, 1988, 443 (448), die das „Vermögen in seiner spezialisierten Ausprägung in Daten" als Rechtsgut annehmen.

501 In diesem Zusammenhang wird wieder fehlende gesetzliche Ausgestaltung des Verfügungsrechts Daten relevant; eingehend dazu *Hilgendorf*, JuS 1996, 890 (892 f.).

502 Zum Datenbegriff siehe Seite 52 ff.

503 *Hilgendorf*, JuS 1996, 890.

504 *Bühler*, MDR 1987, 448 (455); Tröndle/Fischer-*Fischer*, § 303a Rn. 5.

505 Ein Datenträger wird dabei in eine bestimmte Anzahl von Spuren und Sektoren eingeteilt, die dem Betriebssystem das Speichern und Auffinden der Daten ermöglichen. Bereits gespeicherte Daten werden beim Formatieren gelöscht (vgl. *Grieser/Irlbeck*, Computerlexikon, S. 360).

506 Vgl. *Müller*, Aktuelle Probleme des § 263a StGB, S. 62.

507 BT-Drs. 10/5058, S. 35; Schönke/Schröder-*Stree*, § 303a Rn. 4; *Hilgendorf*, JuS 1996, 890 (891).

508 *Hilgendorf*, JuS 1996, 890 (891).

Unter Unbrauchbarmachen ist die Aufhebung der bestimmungsgemäßen Verwendbarkeit der Daten in anderer Weise als durch Löschen (Var. 1) oder Unterdrücken (Var. 2) zu verstehen.[509] Ein Verändern der Daten ist nicht erforderlich. Eine Beeinträchtigung des Datenträgers oder des die Daten verarbeitenden Programms in der Weise, daß diese nicht mehr ordnungsgemäß verarbeitet werden können, reicht aus. Daneben kommt insbesondere das Hinzufügen weiterer Daten[510] oder die inhaltliche Umgestaltung[511] von Daten in Betracht.

Der Gesetzgeber sieht in der Tatbestandsalternative „Verändern" jede Funktionsbeeinträchtigung von Daten, die den Informationsgehalt oder den Aussagewert der Daten ändert.[512] Zur klaren Abgrenzung zu den obigen Tatvarianten ist jedoch zum einen nur die konkrete Einwirkung auf Daten über eine Eingabe- oder Veränderungsschnittstelle (z.B. Tastatur) zu fordern, zum anderen nur die Beeinträchtigung, nicht die Aufhebung der Verwendbarkeit der Daten. So fallen unter „Verändern" inhaltliche Modifikationen von Daten, wie die Änderung der Abfolge von Daten. Eine „Veränderung" liegt ohne Änderung des Informationsgehaltes, wie z.B. das Ersetzen von Klartext durch Code oder der Übersetzung in eine andere Programmiersprache nicht vor.[513] Eine Einbeziehung dieser Varianten widerspricht der eindeutigen Aussage des Gesetzgebers, daß für „Verändern" der Informationsgehalt von Daten und nicht die syntaktische Ebene geändert werden müsse. Diese Fälle können jedoch bei entsprechender Erheblichkeit im Einzelfall als Unterdrücken oder Unbrauchbarmachen von Daten qualifiziert werden.

Problematisch an der Auslegung dieser Tatvariante ist jedoch, daß sie durch den Informationsgehalt von Daten bestimmt wird. Tatobjekt ist aber, wie beim § 202a, „Daten" irgendwelcher Art, nicht aber Dateien oder Datenansammlungen, die als solche in ihrer Gesamtheit einen eigenen Informationsgehalt haben. Werden Daten verändert (auch nur geringste Datenmengen), so wird deren eigener Informationsgehalt jeweils geändert (Beispiel: Ein „A" wird durch ein „U" ersetzt). Eine Datenveränderung läge damit vor. Dies würde jedoch bei jeder Einwirkung auf Daten zu einer Erfüllung des Merkmals „Verändern" führen. Aus diesem Grund ist auf die Änderung des Informationsgehalts des logisch zusammenhängenden Datenfeldes abzustellen. Nur wenn dieser erheblich

---

509 Tröndle/Fischer-*Fischer*, § 303a Rn. 5, jedoch ohne die Ausschlußklausel in Bezug auf die Varianten 1 und 2, wie sie von *Hilgendorf*, JuS 1996, 890 (891) eingeführt wurde.

510 *Granderath*, 2. WiKG, DB 1986 Beilage Nr. 18; S. 3.

511 *Lenckner/Winkelbauer*, CR 1986, 825 (829).

512 BT-Drs. 10/5058, S. 35; so auch Schönke/Schröder-*Stree*, § 303a Rn. 4; *Möhrenschlager*, wistra 1986, 128 (141).

513 Dagegen *Mühle*, Hacker und Computerviren im Internet, S. 97.

von dem abweicht, der vor der Einwirkung gegeben war, liegt ein „Verändern“ von Daten vor.

In dem Kopieren von Daten und der Veränderung dieser kopierten Daten liegt keine tatbestandsmäßige Handlung i.S.d. § 303a. In diesem Fall ist das Rechtsgut des § 303a nicht betroffen, da die Daten des Verfügungsberechtigten selbst nicht manipuliert wurden.[514] Auch objektiv vorteilhafte Veränderungen an Daten sind tatbestandsmäßig i.S.d. § 303a. Maßgeblich ist allein die Abweichung von dem Zustand, den der Verfügungsberechtigte wollte.[515]

Das Merkmal „rechtswidrig“ ist mit der h.M. als Tatbestandsmerkmal zu interpretieren.[516] Anderenfalls wäre jede Veränderung von Daten, die jemand auf seinem eigenen Rechner vornimmt, tatbestandsmäßig.[517] „Rechtswidrig“ ist eine „Datenveränderung“ dann, wenn sie von jemandem vorgenommen wird, der nicht Verfügungsberechtigter über die betreffenden Daten ist, oder wenn der Verfügungsberechtigte nicht damit einverstanden ist (tatbestandsausschließendes Einverständnis).[518]

§ 303a ist wie § 303 und § 303b Antragsdelikt mit Offizialvorbehalt. Der Versuch ist nach Abs. 2 strafbar.

b) Computersabotage, § 303b

Das Rechtsgut des § 303b ist das Interesse von Wirtschaft und Verwaltung am störungsfreien Ablauf der Datenverarbeitung.[519] Tatobjekt des 303b ist die „Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist“. Damit sind sog. „Normalbürger“ nicht im Schutzbereich des § 303b. Taterfolg ist das Stören einer Datenverarbeitung. Der Tatbestand ist in zwei Tathandlungsvarianten gegliedert. § 303b Abs. 1 **Nr. 1** ist **softwarebezogen** und wird

---

514 *Hilgendorf*, JR 478 (479); vgl. auch LK-*Tolksdorf*, § 303a; *Meinhardt*, Überlegungen zur Interpretation von § 303a StGB, S. 166 f.. A.A. AG Böblingen, CR 1989, 308 mit zust. Anmerkung von *Richter* CR 1989, 303 (306).

515 Vgl. *Hilgendorf*, JuS 1996, 890 (891).

516 Lackner/Kühl-*Kühl*, § 303a Rn. 4; *Granderath*, 2. WiKG, DB 1986 Beilage Nr. 18, S. 3; *Frommel*, JuS 1987, 667; *Hilgendorf*, JuS 1996, 890 (892).

517 *Hilgendorf*, JuS 1996, 890 (892).

518 Zum Verfügungsrecht über Daten siehe Seite 33 ff.

519 So die h.M., Schönke/Schröder-*Stree*, § 303b Rn. 1; Tröndle/Fischer-*Fischer*, § 303b Rn. 2; *Volesky/Schulten*, iur 1987, 280; *Hilgendorf*, JuS 1996, 1082. A.A. *Achenbach*, NJW 1986, 1835 (1838) der als „überindividuelles Rechtsgut“ den störungsfreien Ablauf einer Datenverarbeitungsanlage schützen will. *Haft*, NStZ 1987, 6 (10) sieht auch hier „Vermögen“ als das Rechtsgut an.

durch ein Stören einer Datenverarbeitung nach den Handlungsvarianten des § 303a erfüllt. Diese Variante ist damit eine Qualifikation zu § 303a.[520] § 303b Abs. 1 **Nr. 2** ist **hardwarebezogen** und ist dann verwirklicht, wenn Datenverarbeitungsanlagen oder Datenträger manipuliert werden. Diese Variante ist ein selbständiger Tatbestand, da auch der Eigentümer der Hardware Täter des § 303b sein kann.[521] Maßgeblich ist allein, wem das Verfügungsrecht über die gestörte Datenverarbeitung von wesentlicher Bedeutung zusteht. So ist beispielsweise der Eigentümer einer Datenverarbeitungsanlage, auf der Datenverarbeitungen von wesentlicher Bedeutung für einen fremden Betrieb laufen, Täter i.S.d. § 303b Abs. 1 Nr. 2, wenn er diese z.B. zerstört und damit den fremden Betrieb stört.[522] Es kommt nicht darauf an, daß es sich hier möglicherweise auch um eine Vertragsverletzung handelt. Das Rechtsgut des § 303b ist auch in diesen Fällen verletzt. Daher ist *Hilgendorf* zu folgen, wenn er schreibt, daß aus einem Plus an Rechtsverletzung kein Minus an strafrechtlichem Schutz folgen kann.[523]

Tathandlungsvarianten des § 303b Abs. 1 Nr. 2 sind das Zerstören, Beschädigen, Unbrauchbarmachen, Beseitigen und Verändern von Datenverarbeitungsanlagen oder Datenträgern. Der Begriff der Datenverarbeitungsanlage ist gleichbedeutend mit dem in der Computerpraxis verwendeten Begriff der „Hardware“[524]. Dazu zählen die gesamte maschinentechnische Ausstattung, z.B. das zentrale Steuer- und Rechenwerk[525], sowie alle Peripheriegeräte und deren Verbindungen zum Rechner.[526] Kabel eines internationalen Netzwerkes können keiner Datenverarbeitungsanlage zugeordnet werden und sind damit nicht Bestandteile einer Datenverarbeitungsanlage i.S.d. § 303b.[527] Als Datenträger kommen insbesondere Festplatten, Disketten, CD-ROMs, DVD, und Magnetbänder in Betracht.

Die ersten beiden Handlungsvarianten lehnen sich an § 303 an.[528] Wegen der Existenz der Variante „Unbrauchbarmachen“ setzt ein „Beschädigen“ immer eine Substanzver-

---

520 Tröndle/Fischer-*Fischer*, § 303b Rn. 11.

521 Der Gesetzgeber (BT-Drs. 10/5058, S. 36) hat den § 303b bewußt nicht als qualifizierte Sachbeschädigung ausgestaltet.

522 A.A. *Lenckner/Winkelbauer*, CR 1986, 825 (831); Schönke/Schröder-*Stree*, § 303b Rn. 8; *Schulze-Heiming*, Der strafrechtliche Schutz der Computerdaten, S. 215.

523 *Hilgendorf*, JuS 1996, 1082 (1083); so im Ergebnis auch Lackner/Kühl-*Kühl*, § 303b Rn. 4 und 5.

524 Siehe Seite 72.

525 Englisch: CPU (central processing unit).

526 Vgl. Schönke/Schröder-*Stree*, § 303b Rn. 13.

527 LK-*Tolksdorf*, § 303b Rn. 23.

528 BT-Drs. 10/5058, S. 36.

letzung der Hardware voraus. Die bloße Veränderung des Zustands eine Datenverarbeitungsanlage/Datenträger stellt kein „Beschädigen“ dar,[529] da anderenfalls den Merkmalen des Unbrauchbarmachens und Veränderns kein eigenständiger Regelungsbereich zukäme. Die Auslegung von „Beschädigen“ ist bei § 303b folglich im Gegensatz zu § 303 „nach unten“ begrenzt.[530]

Ein Unbrauchbarmachen ist dann gegeben, wenn die Gebrauchsfähigkeit der Hardware nicht unerheblich eingeschränkt ist.[531] Verändern ist als das Herbeiführen eines Zustands zu verstehen, der vom Ursprünglichen abweicht.[532] Eine Beseitigung i.S.d. § 303b Abs. 1 Nr. 2 ist dann gegeben, wenn Datenverarbeitungsanlagen oder Datenträger aus dem Verfügungsbereich entfernt werden.[533] Dies hat aufgrund der natürlichen Wortlautgrenze von „Beseitigen“ durch Ortsveränderung zu geschehen.[534]

Fremd ist ein Unternehmen oder ein Betrieb, wenn der Täter nicht selbst Inhaber oder Repräsentant ist.[535] Der Begriff der Datenverarbeitung ist weit auszulegen. Er umfaßt den gesamten Arbeitsbereich, der sich auf die Speicherung und Verarbeitung von Daten mittels EDV bezieht.[536] Tatobjekt ist daher die Datenverarbeitung im Ganzen, nicht der einzelne Datenverarbeitungsvorgang.[537] Die Manipulation eines einzelnen Datenverarbeitungsvorgangs ist nur dann tatbestandsmäßig, wenn die Datenverarbeitung in ihrer Gesamtheit gestört ist.

Von wesentlicher Bedeutung ist die Datenverarbeitung dann, wenn ihr Ausfall zur Folge hat, daß der betroffene Betrieb, das Unternehmen oder die Behörde seine Tätigkeiten nicht mehr oder nur unter erheblichem Kosten- und Zeitaufwand weiterführen.[538] Positiv formuliert muß die Datenverarbeitung die für die Funktionsfähigkeit von Betrieben zentralen Informationen enthalten. Dies ist z.B. der Fall bei grundlegenden Daten und Arbeitsvorgänge in Rechenzentren, aber auch bei dem einzigen Rechner eines kleineren

---

529 Im Gegensatz zu § 303, bei dem die sog. Zustandsveränderungstheorie vielfach vertreten wird, dazu Lackner/Kühl-*Kühl*, § 303 Rn. 6.

530 *Hilgendorf*, JuS 1996, 1082.

531 BT-Drs. 10/5058, S. 36.

532 BT-Drs. 10/5058, S. 36; wie Zustandsveränderungstheorie bei § 303.

533 BT-Drs. 10/5058, S. 36

534 So auch SK-*Samson*, § 303b Rn. 7; *Hilgendorf*, JuS 1996, 1082.

535 Lackner/Kühl-*Kühl*, § 303b Rn. 2. Eingehend *Schulze-Heiming*, Der strafrechtliche Schutz der Computerdaten, S. 198 ff.

536 *Hilgendorf*, JuS 1996, 1082 (1083); BT-Drs. 10/5058, S. 35.

537 So auch LK-*Tolksdorf*, § 303b Rn. 4, 15. A.A. Tröndle/Fischer-*Fischer*, § 303b Rn. 3.

538 LK-*Tolksdorf*, § 303b Rn. 6; Schönke/Schröder-*Stree*, § 303b Rn. 7; *Lenckner/Winckelbauer*, CR 1986, 824 (830).

Unternehmens.[539] Damit scheiden in aller Regel untergeordnete Datenverarbeitungsvorgänge, wie die eines Taschenrechners oder einer elektronischen Schreibmaschine aus dem Anwendungsbereich aus.[540] Es reicht aus, wenn ein wesentlicher Teil eines Betriebs, Unternehmens oder Behörde auf die funktionsfähige Datenverarbeitung angewiesen ist.[541]

Der Taterfolg, das Stören der qualifizierten Datenverarbeitung, ist nach h.M. dann gegeben, wenn der reibungslose Ablauf der Datenverarbeitung nicht nur unerheblich beeinträchtigt ist.[542] Eine bloße Gefährdung der Datenverarbeitung reicht nicht aus.[543] Die Tathandlung muß für die Störung der Datenverarbeitung kausal und objektiv zurechenbar sein.[544] Die Auslegung der Erheblichkeit der Störung korrespondiert mit der Auslegung zu der „wesentlichen Bedeutung" einer Datenverarbeitung. So ist die Störung dann nicht unerheblich, wenn sie sich nicht ohne großen Kosten- und Zeitaufwand wieder beseitigen läßt.[545] Auf die Dauer der Störung selbst kommt es dagegen nicht an.[546] Es ist jedoch einzig die Störung der Datenverarbeitung tatbestandsmäßig. Eine Störung des Betriebes ist, wie etwa in § 316 b, nicht erforderlich.[547] Werden jedoch Datenverarbeitungen mit „wesentlicher Bedeutung" gestört, so kann i.d.R. dies auch unter eine „Betriebsstörung" subsumiert werden, so daß dies praktisch keine Auswirkungen hat.[548]

§ 303b ist wie § 303a Antragsdelikt mit Offizialvorbehalt. Der Versuch ist nach Abs. 2 ebenfalls strafbar.

Für den Hacker kommt in erster Linie § 303b Abs. 1 Nr. 1 in Betracht, da er in ein System über die Software und zumeist über Datenfernübertragung eindringt. So kann er die Hardware direkt nicht stören. Für § 303b Abs. 2 Nr. 2 kommen jedoch Hardwareangriffe in Frage, die über Eingriffe in Programm- und Betriebssystemabläufe erfolgen.

---

539 *Möhrenschlager*, wistra 1986, 128 (142); Tröndle/Fischer-*Fischer*, § 303b Rn. 4.

540 Vgl. BT-Drs. 10/5058, S. 35.

541 *Schlüchter*, 2. WiKG, S. 78; Schönke/Schröder-*Stree*, § 303b Rn. 7.

542 BT-Drs. 10/5058, S. 35; LK-*Tolksdorf*, § 303b Rn. 11; *Lenckner/Winckelbauer*, CR 1986, 824 (831); *Volesky/Schulten*, iur 1987, 280 (283 f.); Tröndle/Fischer-*Fischer*, § 303b Rn. 5; *Hilgendorf*, JuS 1996, 1082 (1083).

543 BT-Drs. 10/5058, S. 35.

544 Vgl. *Haß*, Der strafrechtliche Schutz von Computerprogrammen, in: Lehmann (Hrsg.), Rechtsschutz und Verwertung von Computerprogrammen, S. 502 Rn. 65.

545 Schönke/Schröder-*Stree*, § 303b Rn. 10.

546 Schönke/Schröder-*Stree*, § 303b Rn. 10.

547 In diese Richtung möglicherweise jedoch SK-*Samson*, § 303b Rn. 12.

548 Vgl. *Hilgendorf*, JuS 1996, 1082 (1083).

II. Angriffe auf qualifizierte Daten

1. Kenntnisnahme, Kopie oder Wegnahme des Datenträgers

Daten sind auch je nach ihrer Art und Qualität in Sondertatbeständen speziell geschützt, wobei das Tatobjekt nicht auf Daten i.S.d. § 202a Abs. 2 beschränkt sein muß, sondern diese Tatobjekte auch in Datenform tatbestandsmäßig angegriffen werden können. So sind Daten, welche Betriebs- und Geschäftsgeheimnisse enthalten, durch § 17 UWG besonders geschützt. Die Ausspähung personenbezogener Daten wird in § 43 BDSG unter Strafe gestellt.

a) Industrie- und Wirtschaftsspionage, § 17 UWG

Dringt ein Hacker in das geschützte Computersystem eines Unternehmens ein, so wird er dort zumeist Informationen vorfinden, die für das Unternehmen äußerst wichtig sind. Diese Informationen können die Grundlage des Unternehmens darstellen, so z.B. bei einer Chemiefirma die Formel zur Herstellung des wichtigen Produktes, oder bei einer Softwarefirma die Idee und der Ablauf eines neuen Programms. Der Hacker, der diese Informationen zur Kenntnis nimmt, kopiert oder an Dritte mitteilt, kann sich gem. § 17 UWG strafbar gemacht haben.

Rechtsgut des § 17 UWG ist das Interesse eines Unternehmers, einen Geheimbereich in seinem Unternehmen aufzubauen und zu unterhalten. Dies soll den Unternehmer davor schützen, daß Konkurrenten oder andere, die ihn schädigen oder sich bereichern wollen, wichtige Informationen erhalten und verwerten.[549] Daneben ist jedoch auch das überindividuelle Interesse an der Funktionsfähigkeit und Reinhaltung der Wettbewerbsordnung als geschütztes Rechtsgut anzusehen.[550]

Im Gegensatz zu § 202a Abs. 1, dem ein durch eine Sicherung dokumentierter, formeller Geheimnisschutz zugrunde liegt, werden in § 17 UWG **materielle Geheimnisse** geschützt. Schutzobjekt sind nicht Daten i.S.d. § 202a Abs. 2, sondern das Betriebs- und Geschäftsgeheimnis, unabhängig in welcher Form es aufbewahrt wird, ob wahrnehmbar oder nicht, oder dieses nur über das Gedächtnis einer Person abgerufen werden kann. Eine besondere Sicherung, wie in § 202a Abs. 1, ist nicht erforderlich.

---

549 Vgl. *Baumbach /Hefermehl*, § 17 UWG Rn. 6.

550 *Rupp*, WRP 1985, 676; *Otto*, wistra 1988, 125 (126). A.A. wohl *Schlüchter*, 2. WiKG, S. 130.

Zentrales Merkmal des § 17 UWG ist das Betriebs- und Geschäftsgeheimnis.[551] Dies ist nach h.M. eine Tatsache, die nach dem erkennbaren Willen des Betriebsinhabers geheimgehalten werden soll, die ferner nur einem begrenzten Personenkreis bekannt und damit nicht offenkundig ist und hinsichtlich der Betriebsinhaber deshalb ein berechtigtes Geheimhaltungsinteresse hat, weil eine Aufdeckung der Tatsache geeignet wäre, dem Geheimnisträger wirtschaftlichen Schaden zuzufügen.[552] In dieser Definition wird deutlich, daß kumulativ eine subjektive Komponente, der Wille des Berechtigten zur Geheimhaltung, und eine objektive Komponente, ein nachweisbares berechtigtes Interesse an der Geheimhaltung, gegeben sein muß.[553] Geschäftsgeheimnisse betreffen die kaufmännische Sphäre (z.B. Bilanzen, Investitionsplanungen, Kundendatenbanken); Betriebsgeheimnisse betreffen den technischen Bereich eines Unternehmens (z.B. Konstruktionspläne, Rezepturformeln, aber auch Computerprogramme). Die Beurteilung als Betriebs- oder Geschäftsgeheimnis ist unabhängig von der Art der Aufbewahrung des Geheimnisses. Geheimnisse können daher auch auf einem Datenträger gespeichert sein.[554] Als Gegensatzbegriff zu einer geheimen und damit durch § 17 UWG möglicherweise geschützten Tatsache, wird der Ausdruck der **offenkundigen** Tatsache verwendet.[555] Offenkundig und damit nicht oder nicht mehr geheim ist eine Tatsache dann, wenn sie allgemein bekannt ist. Allgemein bekannt ist sie, wenn verständige Menschen regelmäßig Kenntnis haben oder sich aus verläßlichen Quellen ohne besondere Fachkunde sicher unterrichten können.[556]

Besonders relevant im Zusammenhang mit Hacken ist, daß auch **Paßwörter**, die Unberechtigte von Rechnern oder bestimmten Datenbereichen von Unternehmen fernhalten sollen, i.d.R. Geheimnisse i.S.d. § 17 UWG darstellen.[557] Der Geheimhaltungswille des Unternehmers bzgl. der Paßwörter ist offensichtlich (subjektive Komponente). Sie sind normalerweise einem eingegrenzten Personenkreis bekannt und damit nicht offenkundig. Deren Aufdeckung birgt die Gefahr, daß andere Geheimnisse sowie die Datenverarbeitung des Unternehmens zugänglich werden. Dies kann zu erheblichem wirtschaftli-

---

551 Beide Varianten werden gleich behandelt, so daß auch als Oberbegriff von einem „Unternehmensgeheimnis“ gesprochen wird (Erbs/Kohlhaas-*Diemer*, § 17 UWG Rn. 5).

552 BGHSt 41, 140 (142); *Haß*, Der strafrechtliche Schutz von Computerprogrammen, in: Lehmann (Hrsg.), Rechtsschutz und Verwertung von Computerprogrammen, S. 484 Rn. 28.

553 Sog. „Vereinigungstheorie“ vereinigt sog. „Interessentheorie“ mit sog. „Willenstheorie“.

554 Vgl. *Rupp*, WRP 1985, 676 (677).

555 So schon RGSt 29, 426 (430); vgl. auch Erbs/Kohlhaas-*Diemer*, § 17 UWG Rn. 6.

556 BGHSt 6, 292 (293); BGHSt 26, 56 (59).

557 Vgl. auch *Binder*, Strafbarkeit intelligenten Ausspähens von programmrelevanten Unternehmensgeheimnissen, S. 71 f.

chen Schaden führen, bis hin zum Verlust der Unternehmensgrundlage[558] (objektive Komponente).[559]

§ 17 UWG ist ein Tatbestand mit überschießender Innentendenz. In beiden Absätzen ist eine Handlung nur dann tatbestandsmäßig, wenn eines oder mehrere der subjektiven Tatbestandsmerkmale erfüllt sind. Dazu gehören: zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Geschäftsbetriebs Schaden zuzufügen. Zu dem Vorsatz auf die objektiven Merkmale muß folglich ein absichtliches Handeln i.S. dieser Merkmale in der Qualität des dolus directus 1.Grades[560] hinzutreten.[561] Zu Zwecken des Wettbewerbs wird eine Handlung dann vorgenommen, wenn sie die eigene oder fremde Wettbewerbsposition zum Nachteil eines anderen Gewerbetreibenden fördern soll.[562] Aus Eigennutz handelt, wer sich einen Vorteil jedweder Art verspricht.[563] Neben der Schädigung des Betriebsinhabers kann der Täter auch andere Ziele verfolgt haben.[564] Der Schaden kann auch immaterieller Art sein.[565] Durch das 2. WiKG ist das Merkmal „zugunsten eines Dritten“ eingefügt worden. Dies ist dann gegeben, wenn der Täter das Ziel verfolgt, einem Dritten materiellen oder immateriellen Vorteil zu verschaffen. Damit sollen nach dem Willen des Gesetzgebers auch Täter erfaßt werden können, die weder wettbewerbliche Interessen fördern wollen, noch aus Eigennutz oder in Schädigungsabsicht handeln, sondern z.B. aus ideologischen Motiven im Interesse eines anderen Staates handeln.[566]

Das Merkmal „unbefugt“ ist in beiden Absätzen nach der vorzugswürdigen h.M. wie auch in den §§ 201-204 kein Tatbestandsmerkmal, sondern Hinweis auf die Rechtswidrigkeit als allgemeines Verbrechensmerkmal.[567]

---

558 So z.B., wenn alle Daten des Unternehmens unwiderbringlich gelöscht worden sind.

559 Zur Strafbarkeit des Ausspähens des Unternehmenspaßworts siehe Seite 151.

560 Dazu eingehend *Kühl*, AT, § 5 Rn. 28 ff.

561 Vgl. *Baumbach/Hefermehl*, § 17 UWG Rn. 19 ff.; Erbs/Kohlhaas-*Diemer*, § 17 UWG Rn. 24.

562 Erbs/Kohlhaas-*Diemer*, § 17 UWG Rn. 25.

563 GK-*Otto*, § 17 UWG Rn. 46.

564 RGSt 51, 184 (194).

565 *Baumbach/Hefermehl*, § 17 UWG Rn. 22.

566 BT-Drs. 10/5058, S. 40.

567 Erbs/Kohlhaas-*Diemer*, § 17 UWG Rn. 20, 37; *Otto*, wistra 1988, 125 (128); Bay ObLG NJW 1991, 438 (440). A.A. *Rupp*, WRP 1985, 676 (679).

(1) Geheimnisverrat, § 17 Abs. 1 UWG

Täter des § 17 Abs. 1 UWG können nur abhängig Beschäftigte sein. Auch der Hacker, der in geschützte Bereiche vordringt, muß damit, um nach § 17 Abs. 1 UWG strafbar sein zu können, bei dem betroffenen Unternehmen abhängig beschäftigt sein. Dem Hacker darf das Geheimnis nicht anvertraut worden sein, da er sonst kein Grund zum Hacken hätte. Es reicht jedoch aus, wenn das Geheimnis ihm vermöge des Dienstverhältnisses zugänglich geworden ist. Unter den Begriff des Zugänglichwerdens fällt alles, was dem Beschäftigten auf irgendeine Weise während seines Dienstverhältnisses bekannt wird, so auch dann, wenn er sich das Geheimnis selbst zugänglich gemacht hat (z.B. Bestechen eines anderen Beschäftigten[568] oder Veranlassung der Mitteilung des Geheimnisses durch andere Beschäftigte[569]) Das Bestehen des Dienstverhältnisses muß damit für die Kenntniserlangung kausal sein.[570] Gewinnt der Hacker durch Eindringen in Datenbereiche auf Rechnern des Geschäftsbetriebs, für die er keine Berechtigung hat, Kenntnis, so ist das Dienstverhältnis kausal für das Zugänglichwerden der Daten geworden. Kann der abhängig beschäftigte Hacker auch an seinem eigenen Rechner über Datenfernübertragung an tatbestandsrelevante Geheimnisse gelangen, so ist i.d.R. die Kausalbeziehung Dienstverhältnis – Zugänglichwerden gegeben. Denn auch der Hacker an seinem Rechner hat infolge seiner Beschäftigung bessere Kenntnis über den Aufbewahrungsort und die Art des Geheimnisses erworben. Erlangt der Hacker zufällig Kenntnis, so ist diese nur dann nicht tatbestandsmäßig, wenn der Zufall auch ohne das Dienstverhältnis zu der Kenntnis geführt hätte.[571]

Tathandlung ist nicht die eigentliche Hackerhandlung, sondern das Mitteilen der erlangten Geheimnisse. Folglich ist die bloße Kenntnisnahme noch nicht strafbar i.S.d. § 17 Abs. 1 UWG. Mitteilen ist jede beliebige Art der Bekanntgabe einer geheimzuhaltenden Tatsache, welche ihre Ausnutzung in irgendeiner Form ermöglicht.[572] Es ist nicht erforderlich, daß der Empfänger das Geheimnis auch verwertet.[573] Ebensowenig ist notwendig, daß der Empfängers das Geheimnis versteht, oder er die Fähigkeit hat, es

---

568 RGSt 33, 354 (356).

569 BGH NJW 1984, 239 (240).

570 *Haß*, Der strafrechtliche Schutz von Computerprogrammen, in: Lehmann (Hrsg.), Rechtsschutz und Verwertung von Computerprogrammen, S. 487 Rn. 32.

571 RGSt 33, 354 (356).

572 *Baumbach/Hefermehl*, § 17 UWG Rn. 16.

573 RGSt 51, 185 (189).

zu nutzen. Er muß es lediglich behalten und weitergeben können.[574] Es ist ausreichend, wenn eine das Geheimnis verkörpernde Sache, wie z.B. eine Diskette, in schlüssiger Form übergeben wird.[575]

(2) § 17 UWG Abs. 2

In Bezug auf Hacker ist der Abs. 2 des § 17 UWG wesentlich relevanter. Dieser ist im Zuge des 2. WiKG neu formuliert worden. Täter kann im Gegensatz zu Abs. 1 jedermann sein. Abs. 2 ist daher im Gegensatz zu Abs. 1 kein Sonderdelikt. Auch der Beschäftigte kann Täter sein.[576] Abs. 2 ist selbst wiederum in zwei Varianten aufgeteilt. Nr. 1 regelt die sog. Betriebsspionage, Nr. 2 die sog. Geheimnishehlerei.

(a) Betriebsspionage, § 17 Abs. 2 Nr. 1

In der Variante der Betriebsspionage muß sich der Täter das Betriebs- und Geschäftsgeheimnis unter den oben genannten Motiven (Eigennutz usw.) verschafft oder gesichert haben. Der Begriff des Verschaffens lehnt sich an § 96 und § 202a an.[577] Zum einen ist Kenntnis des Geheimnisses „verschaffen", zum anderen fällt das Erlangen des Geheimnisses in verkörperter Form darunter. Ein Durchdringen und Verstehen des Geheimnisses ist nicht erforderlich, sondern lediglich die Fähigkeit zur Wiedergabe.[578] Bei verkörperten Geheimnissen braucht der Täter keine Kenntnis wie bei § 202a zu erlangen. Es genügt hier die technische Möglichkeit der Wiedergabe. Durch die Tathandlungsvariante „sichern" will der Gesetzgeber sicherstellen, daß auch derjenige bestraft wird, der das Geheimnis zwar schon kennt, sich jedoch eine genaue und bleibende Kenntnis schafft[579], damit er jederzeit darauf zurückgreifen kann.[580] Dies ist z.B. dann der Fall, wenn ein Täter sich ein Computerprogramm oder sonstige große Datenmengen aus-

---

574 RGSt 51, 185 (189).

575 *Haß*, Der strafrechtliche Schutz von Computerprogrammen, in: Lehmann (Hrsg.), Rechtsschutz und Verwertung von Computerprogrammen, S. 487 Rn. 32; vgl. auch RGSt 33, 6 (7).

576 GK-*Otto*, § 17 UWG Rn. 81.

577 BT-Drs. 10/5058, S. 40.

578 *Haß*, Der strafrechtliche Schutz von Computerprogrammen, in: Lehmann (Hrsg.), Rechtsschutz und Verwertung von Computerprogrammen, S. 488 Rn. 34.

579 BT-Drs. 10/5058 S. 40.

580 Vgl. *Schlüchter*, 2.WiKG, S. 131.

druckt, damit er dann leichter davon Gebrauch machen kann.[581] Eine Verwertung der verschafften Geheimnisse durch den Verschaffenden ist nicht erforderlich.[582]

Zur Beschränkung der Strafbarkeit hat der Gesetzgeber zusätzliche Merkmale eingeführt. Es sollten nur typische und besonders gefährliche Erscheinungsformen der Betriebsspionage unter Strafe gestellt werden, in denen der Taterfolg nur unter Einsatz bestimmter „Verkörperungen" und oder mit anderen technischen Mitteln geschieht.[583] Erste Variante des Verschaffens ist die unter „Anwendung technischer Mittel" (§ 17 Abs. 2 Nr. 1 a UWG). Hierunter fallen alle im weitesten Sinne technischen Vorrichtungen, die zum Verschaffen oder Sichern der Geheimnisse verwendet werden. Der Gesetzgeber zählt hier beispielhaft den Einsatz von Ablichtungsgeräten, Fotoapparaten, Filmkameras, Abhörvorrichtungen, Kleinsende- oder Empfangsgeräten auf.[584] Liest der Hacker Daten, die ein Geheimnis i.S.d. § 17 UWG darstellen, vom Bildschirm ab[585], oder stellt er eine Kopie der Daten her[586], wendet er technische Mittel an.

Zweite Variante ist das Verschaffen oder Sichern durch die „Herstellung einer verkörperten Wiedergabe des Geheimnisses" (§ 17 Abs. 2 Nr. 1 b UWG). Dieses Merkmal überschneidet sich in weiten Bereichen mit dem obigen Merkmal. Unter den Begriff der verkörperten Wiedergabe fällt jede verkörperte Festlegung der Geheimnisse.[587] Das Aufrufen von Daten auf einem Bildschirm ist keine verkörperte Wiedergabe.[588] Drittes Merkmal ist das Verschaffen oder Sichern unter Wegnahme einer das Geheimnis verkörpernden Sache (§ 17 Abs. 2 Nr. 1 c UWG). Diese Variante kommt jedoch für den Hacker nicht in Frage, da er sich nur Daten per Datenverarbeitung verschafft, nicht aber deren ursprüngliche Verkörperungen (Datenträger).

Beschränkt der Hacker sich lediglich auf das Verschaffen eines Geheimnisses zur Dokumentation seines Hackerfolgs, so ist danach zu fragen, ob hier schon **Eigennutz** angenommen werden kann. Das Bestreben des Hackers ist in diesem Fall der „sportliche" Erfolg, wieder einmal ein System geknackt zu haben. Das wird sein Selbstbewußtsein stärken und er kann sich bei anderen Hackern damit brüsten. Vorteil ist jedoch nur, was

---

581 *Rupp*, WRP 1985, 676 (680).

582 *Haß*, Der strafrechtliche Schutz von Computerprogrammen, in: Lehmann (Hrsg.), Rechtsschutz und Verwertung von Computerprogrammen, S. 489 Rn. 35.

583 BT-Drs. 10/5058, S. 40.

584 BT-Drs. 10/5058, S. 40.

585 *Rupp*, WRP 1985, 676 (680).

586 Bay ObLG NJW 1991, 438 (439).

587 *Baumbach/Hefermehl*, § 17 UWG Rn. 27.

588 GK-*Otto*, § 17 UWG Rn. 71.

eine Person in Bezug auf andere Mitmenschen in eine günstigere Situation bringt. Damit scheidet das Stärken des Selbstbewußtseins als Eigennutz aus. Dieses liegt allein in der Person des Hackers. Kann der Hacker jedoch seine Position innerhalb der Hackerszene aufbessern, so hat er gegenüber anderen, die diesen Erfolg nicht vorzuweisen haben einen Prestigegewinn und damit einen Vorteil im weitesten Sinne. Daß ein solches Vorgehen den Tatbestand des § 17 Abs. 2 Nr. 1 UWG erfüllt, steht nicht im Widerspruch zu der Intention des Gesetzgebers, das Hacken straflos sein zu lassen. Nimmt der Hacker in der Weise Kenntnis von den Geheimnissen oder kopiert er sich diese, daß er seinen Erfolg dokumentieren kann, so liegt kein bloßes Eindringen in ein geschütztes System mehr vor. Ein Hacken i.e.S. liegt hier vor.

Problematisch ist jedoch, wenn sich der Hacker lediglich das **Paßwort eines Unternehmens verschafft** hat. Unternehmenspaßwörter können i.d.R. als Geheimnisse i.S.d. § 17 UWG angesehen werden.[589] Das Verschaffen eines geheimen Paßwortes ist nach teleologischer Reduktion nicht als strafbar gem. § 202a anzusehen.[590] Fraglich ist, ob sich dies auch auf den § 17 Abs. 2 Nr. 1 UWG auswirkt. Der Gesetzgeber wollte das Hacken i.e.S. straflos stellen.[591] Ermittelt ein Hacker dieses Paßwort, so ist dies eine vorbereitende Handlung für das eigentliche Eindringen, dem anschließenden Verwenden des Paßworts. Ist noch nicht einmal ein strafloses Hacken i.S.d. Gesetzgebers gegeben, so könnte man vertreten, daß dann eine Strafbarkeit nach § 17 UWG des Herausfindens des Paßworts im Widerspruch zum Willen des Gesetzgebers steht.[592]

Dagegen sprechen jedoch gewichtige Gründe. Die Kenntnis oder eine sonstige Aufbewahrung eines Unternehmenspaßwortes stellt eine ähnliche Gefährdungslage dar, wie in dem Fall eines Verschaffens einer Produktformel o.ä.. Kommt dieses Paßwort in die falschen Hände, so können weitere Geheimnisse ausgespäht, bzw. die Datenverarbeitung manipuliert werden. Es kann folglich jederzeit auf das Unternehmen eingewirkt werden. Das Rechtsgut des § 17 UWG ist somit mit dem Verschaffen eines Paßworts betroffen.

Würde man den Argumenten pro Strafbarkeit gem. § 17 UWG folgen, so wären weite Bereiche des Hackens i.e.S. strafbar nach § 17 UWG, da gerade auch Unternehmen die Möglichkeit der weltweiten Abrufbarkeit von Informationen insbesondere für Mitar-

---

589 Siehe Seite 146.

590 Siehe unter Seite 156 ff.

591 BT-Drs. 10/5058, S. 28.

592 In diesem Sinne vgl. *Binder*, Strafbarkeit intelligenten Ausspähens von programmrelevanten Unternehmensgeheimnissen, S. 73.

beiter nutzen wollen und sich zumeist mit Paßwortabfrage vor Eindringlingen schützen. Diese Einrichtungen sind klassische Angriffsziele von Hackern. Damit wäre Hacken dann doch durch die Hintertüre wieder strafbar und nicht erst das eigentliche Eindringen, sondern schon die Ermittlung eines Paßwortes mit technischen Mitteln oder die verkörperte Aufwahrung des zuvor ermittelten Paßwortes. Eine Strafbarkeit § 17 UWG ist im Ergebnis aufgrund des insoweit eindeutigen Willens des Gesetzgebers zum Hakken i.e.S. abzulehnen. Unternehmenspaßwörter sind daher aus systematischen Erwägungen (im Hinblick auf § 202a) nicht durch § 17 UWG vor Kenntnisnahme geschützt. Würde man das Hacken i.e.S. unter Strafe stellen, so wäre eine Strafbarkeit der Ausspähung des Unternehmenspaßworts gem. § 17 UWG zu bejahen.

(b) Geheimnishehlerei, § 17 Abs. 2 Nr. 2 UWG

Bei der sog. Geheimnishehlerei ist Tathandlung das Verwerten oder Mitteilen eines Geheimnisses, welches vorher entweder schon gem. § 17 Abs. 1 UWG, oder durch eigene oder fremde Handlungen nach § 17 Abs. 2 Nr. 1 UWG, oder sonst unbefugt sich verschafft oder gesichert wurde. Dieser Tatbestand kommt jedoch für Hacker nicht in Frage, da das Hacken kein Verwerten oder Mitteilen eines schon erlangten Geheimnisses darstellt. § 17 Abs. 2 Nr. 2 UWG ist folglich für Hacker nicht einschlägig.

Der Versuch ist gem. § 17 Abs. 3 strafbar. Gem. § 22 Abs. 1 UWG ist § 17 UWG ein Antragsdelikt mit Offizialvorbehalt.

b) Ausspähung personenbezogener Daten, § 43 BDSG

Das Rechtsgut des § 43 BDSG ist das Persönlichkeitsrecht des Betroffenen im Umgang anderer mit seinen Daten.[593] Im Gegensatz zu § 202a ist nicht die Verfügungsbefugnis des Skribenden oder eine derivative Verfügungsberechtigung über Daten geschützt.[594] Der Tatbestand ist als Blankettnorm formuliert, da sich der Tatbestand und die Rechtswidrigkeit erst in der Gesamtschau der den Datenumgang regelnden Normen ergibt.[595] Trotz teilweise berechtigter Kritik[596] genügt auch die Novellierung der Strafnormen des BDSG den Anforderungen an die Bestimmtheit und dem Übermaßverbot.[597]

---

593 Simitis/Dammann/Mallmann/Reh-*Dammann*, § 43 BDSG Rn. 2.

594 Simitis/Dammann/Mallmann/Reh-*Dammann*, § 43 BDSG Rn. 2.

595 Erbs-Kohlhaas-*Ambs*, § 43 BDSG Rn. 4.

596 Siehe z.B. *Tiedemann*, NJW 1981, 945 ff.; *Herb*, Verweisungsfehler im Datenschutz-Strafrecht.

597 Simitis/Dammann/Mallmann/Reh-*Dammann*, § 43 BDSG Rn. 6f.; Erbs/Kohlhaas-*Ambs*, § 43 BDSG Rn. 4.

Täter des § 43 BDSG kann jedermann sein.[598] Tatobjekt sind die vom BDSG geschützten personenbezogenen Daten, die nicht offenkundig sind. Die Eingrenzung auf vom BDSG geschützte Daten ist ein Hinweis darauf, daß es auch personenbezogene Daten gibt, die durch landesrechtliche Normen geschützt werden. Diese sind vom Strafrechtsschutz des § 43 BDSG nicht erfaßt.[599] Welche Daten geschützt sind, ergibt sich insbesondere aus dem in § 1 BDSG bestimmten und in § 12 BDSG und § 27 BDSG präzisierten Schutzbereich des BDSG.[600] Aus der Subsidiarität des BDSG gegenüber anderen Vorschriften des Bundes über den Datenschutz gem. § 1 Abs. 4 BDSG ergibt sich, daß auch die unter besondere bundesrechtliche Regelungen zu subsumierende Daten durch § 43 BDSG geschützt sind.[601] Offenkundig sind Daten, die einer beliebig großen Anzahl von Menschen bekannt sind oder über die man sich ohne besondere Anstrengung, etwa durch die Benutzung allgemein zugänglicher und zuverlässiger Quellen unterrichten kann.[602] Bloße Gerüchte sind nicht als offenkundige Daten zu werten, solange sie noch weiterer Bestätigung bedürfen.[603]

Im Zusammenhang mit dem Computerhacken sind Abs. 1 Nr. 3 und Abs. 2 Nr. 1 von Bedeutung. In Abs. 1 Nr. 3 ist das Abrufen oder das Verschaffen geschützter Daten für sich oder einen anderen aus Dateien unter Strafe gestellt. Der Dateien-Begriff wird in § 3 Abs. 2 BDSG legaldefiniert. Besonders interessant ist, daß im Zuge der Novellierung des BDSG vom Jahre 1990 mit Abs. 2 Nr. 1 eine Norm eingeführt wurde, die speziell gegen Hacker schützen sollte. Nach der Begründung zum Regierungsentwurf soll durch Tathandlung des Erschleichens der Übermittlung geschützter Daten durch unrichtige Angaben die Datenbeschaffung durch Hacker erfaßt werden.[604]

Der Begriff des „**Abrufens**“ ist entnommen aus der Legaldefinition der Übermittlung in § 3 Abs. 3 Nr. 3 b BDSG. Abrufen ist die Herstellung der Verfügungsmacht über personenbezogene Daten i.S.d. BDSG, die in einer automatischen Datenverarbeitungsanlage gespeichert sind und zwar durch Eingabe oder Aktivierung von Programmbefehlen.[605]

---

598 *Ordemann/Schomerus/Gola*, § 43 BDSG Anm. 2.1.

599 Vgl. *Dammann*, NJW 1978, 1906 (1906); a.A. LG Kreuznach, NJW 1978, 1931.

600 Simitis/Dammann/Mallmann/Reh-*Dammann*, § 43 BDSG Rn. 10.

601 *Ordemann/Schomerus/Gola*, § 43 BDSG Anm. 2.2; Simitis/Dammann/Mallmann/Reh-*Dammann*, § 43 BDSG Rn. 11.

602 BGHSt 6, 292; *Schaffland/Wiltfang*, § 43 BDSG Rn. 5; Erbs/Kohlhaas-*Ambs*, § 43 BDSG Rn. 3.

603 Erbs-Kohlhaas-*Ambs*, § 43 BDSG Rn. 3; Simitis/Dammann/Mallmann/Reh-*Dammann*, § 43 BDSG Rn. 14.

604 BT-Drs. 11/4306; *Ordemann/Schomerus/Gola*, § 43 BDSG Anm. 3.5.

605 Vgl. Simitis/Dammann/Mallmann/Reh-*Dammann*, § 43 BDSG Rn. 23.

Die Verfügungsmacht wird, wie beim „Verschaffen“ in § 202a Abs. 1 entweder durch Kenntnisnahme oder durch Herstellen einer Datenkopie gewonnen. Ausgenommen ist die Wegnahme des ursprünglichen Datenträgers, auf den der Täter nicht vorher die gewünschten Daten durch Programmbefehle überspielt hat.[606] Hauptkriterium des Abrufens ist damit das Erlangen der Daten mit Hilfe von Programmbefehlen. Das physikalische Anzapfen von Leitungen ist somit nicht durch den Begriff des Abrufens abgedeckt.[607] Die Daten müssen nicht zum Abruf bereitgehalten worden sein, da zum einen auch in automatisierter Form gespeicherte Daten abgerufen werden können, die nicht zum Abruf vorgesehen wurden, zum anderen in § 3 Abs. 5 Nr. 3 b BDSG das Bereithalten nicht Bestandteil des Begriffes des Abrufens ist.[608] Es ist ebenso unerheblich, ob der Täter grs. abrufberechtigt ist und nur seine Befugnisse überschreitet, oder ob er sich unabhängig von seiner Befugnis Zugang zu den Daten verschafft, wie es beim Hacken regelmäßig der Fall ist.[609]

Das „Verschaffen aus Dateien für sich oder einen anderen“ stellt als Tathandlungsalternative das Auffangmerkmal zum „Abrufen“ dar. Die Daten müssen hier nicht in automatisierter Form vorliegen und auch nicht über Programmbefehle abgerufen werden. So ist der Begriff „verschaffen“ zu definieren als die Kenntnisnahme oder die sonstige Herstellung einer Verfügungsmacht über die geschützten Daten.[610] Im Gegensatz zu § 202a müssen die Daten nicht in nicht-wahrnehmbarer Form vorliegen. Diese Handlungsalternative ist jedoch für Hacker nicht relevant, da der Hacker immer nur Daten in automatisierter Form ausspäht und dazu Programmbefehle benutzt. Das Hacken fällt damit unter die im Handlungsbereich gegenüber dem „Verschaffen“ speziellere Tathandlungsalternative „Abrufen“.[611] Damit ist das Hacken i.w.S. auch dann nach § 43 BDSG als Abrufen von Daten strafbar, wenn diese nicht aus Dateien i.S.d. § 3 Abs. 2 BDSG stammen.

Das „Erschleichen unter Angabe unrichtiger Angaben“ soll nach der Begründung zum Regierungsentwurf die Datenbeschaffung durch Hacker erfassen.[612] Dies wäre jedoch in

---

606 Simitis/Dammann/Mallmann/Reh-*Dammann*, § 43 BDSG Rn. 23; Erbs/Kohlhaas-*Ambs*, § 43 BDSG Rn. 5.

607 Simitis/Dammann/Mallmann/Reh-*Dammann*, § 43 BDSG Rn. 25; a.A. Erbs/Kohlhaas-*Ambs*, § 43 BDSG Rn. 5.

608 Erbs-Kohlhaas-*Ambs*, § 43 BDSG Rn. 5; Simitis/Dammann/Mallmann/Reh-*Dammann*, § 43 BDSG Rn. 23; *Ordemann/Schomerus/Gola*, § 43 BDSG Anm. 3.4.

609 *Ordemann/Schomerus/Gola*, § 43 BDSG Anm. 3.4.

610 Simitis/Dammann/Mallmann/Reh-*Dammann*, § 43 BDSG Rn. 29.

611 So wohl auch *Ordemann/Schomerus/Gola*, § 43 BDSG Anm. 3.4.

612 BT-Drs. 11/4306.

diesem speziellen Fall nicht notwendig gewesen, da das Hacken i.w.S. schon unter „Abrufen“ oder „Verschaffen“ gem. Abs. 1 Nr. 3 subsumierbar ist. Die Eingabe eines gültigen Paßworts ist für sich genommen keine unrichtige Angabe. Der Eingebende erklärt jedoch damit auch die Identität des berechtigten Paßwortinhabers zu haben. Die Angabe des Hackers ist unrichtig. Findet der Hacker zumeist unter Ausnutzung von Sicherheitsmängeln jedoch andere Wege zu den Daten, so macht er keine unrichtigen Angaben und ist damit nicht gem. § 43 Abs. 2 Nr. 1 BDSG strafbar.

Handelt der Täter gegen Entgelt oder um sich zu bereichern oder einen anderen zu schädigen, so ist die **Qualifikation** nach Abs. 2 einschlägig, welche mit § 203 Abs. 5 wortgleich ist. „Entgelt“ ist legaldefiniert in § 11 Abs. 1 Nr. 9 und damit „jede in einem Vermögensvorteil bestehende Gegenleistung“. Die Absicht der Bereicherung muß auf einen Vermögensvorteil gerichtet und „rechtswidrig“ sein. Rechtswidrig ist die Bereicherungsabsicht dann, wenn der Täter keinen Rechtsanspruch auf den Vermögensvorteil innehat.[613] Die Schädigungsabsicht muß sich nicht auf einen Vermögensschaden beziehen.[614]

Nach Abs. 4 ist § 43 BDSG Antragsdelikt. Antragsberechtigt ist allein der Betroffene[615] als Verletzter i.S.d. § 77, im Gegensatz zu § 202a, bei dem grs. der Skribent antragsberechtigt ist. Der Versuch ist nicht strafbar.

2. Manipulationen (§ 43 Abs. 1 Nr. 1 Alt. 2 BDSG)

Manipulationen an qualifizierten Daten sind, außer in dem Fall des Veränderns von personenbezogenen Daten nach § 43 BDSG[616] nicht besonders unter Strafe gestellt. Insoweit gelten auch hier für den Fall, daß Daten manipuliert werden, die auch solche i.S.d. § 202a Abs.2 sind, die §§ 303a, 303b.

---

613 BGHSt 19, 206 (216).

614 Wie bei § 203; siehe dazu Schönke/Schröder-*Lenckner*, § 203 Rn. 74.

615 Siehe Legaldefinition § 3 Abs. 1 BDSG

616 Siehe zum Begriff des „Veränderns“ die Erläuterungen zu § 303a auf Seite 140. Der Begriff ist gleich auszulegen.

C. Untersuchung hackerspezifischer Vorgehensweisen

I. Paßwortausspähung

1. Vorgehensweisen

Die häufigste Ursache für erfolgreiche Einbrüche in Computersysteme sind die unzureichenden Vorkehrungen für die Authentifikation. Hier wird der Name des Benutzer und die damit verbundenen Nutzungsrechte, für die dieser autorisiert ist, abgefragt. Diese Authentifikation wird zumeist dadurch erreicht, daß eine Benutzeridentifikation und das dazugehörige Paßwort abgefragt wird. Authentifikation ist damit Autorisierung plus Identifikation. Der Computer, auf den zugegriffen werden soll, vergleicht die Eingaben mit identischen Daten, die zumeist verschlüsselt dort abgelegt sind. Stimmen die eingegebenen Daten mit den im Computer gespeicherten überein, wird der Zugang zum Rechner mit dem für den Benutzer entsprechenden Rechten ermöglicht.[617]

Hat der Hacker Kenntnis von Benutzeridentifikation und Paßwort, kann er in das System eindringen. Die (Netz-)Betriebsysteme[618] haben oft Standardkennungen für voreingestellte Benutzer wie „guest“ oder „sysop“, für die vom Hersteller ein Ursprungspaßwort vergeben wird, welches nach Installation geändert werden sollte. Die Änderung wird aber des öfteren unterlassen. Ist eine Benutzeridentifikation bekannt, muß das Paßwort herausgefunden werden. Im folgenden werden die verschiedenen Arten der Paßwortbeschaffung erläutert.

a) Trial and error

Augenfälligste Methode, Paßwörter herauszufinden, ist, das zur Zugangskennung (Login) passende Paßwort zu erraten. Hier helfen vor allem Kenntnisse über die Vergabepraxis von Paßwörtern. Variationen des Login Namens (Vor- und Zuname) und anderer persönlicher Daten aus der /etc/passwd-Datei[619], häufige Namen, Namen von be-

---

617 Andere, zumeist sicherere Zugangssysteme sind Smartcards oder biometrische Verfahren, wie Fingerabdrucktest, oder Augentest.

618 Zumeist UNIX, immer öfter jedoch auch Windows NT.

619 Standard-Datei im bei Netzrechnern am häufigsten verwendeten Betriebssystem unix, in dem unteranderem die Benutzerkennung und die dazugehörenden Paßwörter abgespeichert sind. Die Paßwörter sind verschlüsselt mit dem DES-Verfahren (dazu mehr unter Seite 100 f.).

kannten Personen, Namen und Orte aus Filmen, von Sportereignissen und aus der Bibel, gebräuchliche Schimpfwörter und Wörter aus Fremdsprachen, verschiedene Variationen dieser Wörter, wie z.B. Umwandlung Groß-Kleinschreibung, Einfügen von Sonder- und Kontrollzeichen, Umkehrung der Buchstabenreihenfolge, wiederholte Buchstaben (z. B. aaabbb) oder häufige Abkürzungen (z. B. rggbv für die Farben des Regenbogens) und Paare aus zwei kurzen Wörtern.[620]
Dieses systematische Paßwortraten kann durch die Begrenzung der Anzahl von Zugriffsversuchen bekämpft werden.

b) Paßwortknacker

Paßwortknacker sind Computerprogramme, die Paßwortsicherheitsmaßnahmen umgehen, indem sie Paßwörter aufdecken, die vorher verschlüsselt[621] wurden.[622] Zumeist werden die Paßwörter durch die Paßwortknacker jedoch nicht entschlüsselt, da die meisten Paßwörter und insbesondere Unix-Paßwörter mit starken Einmal-Verschlüsselungsverfahren verschlüsselt wurden, die im Prinzip nicht entschlüsselbar sind. Die Paßwortknacker bedienen sich daher eines anderen Verfahrens. Dieses soll am Beispiel von Unix-Paßwörtern erläutert werden.

Die Paßwörter in einem Unix-System sind in der Datei /etc/passwd mit dem Verschlüsselungsverfahren DES[623] einwegverschlüsselt abgespeichert. Bestimmte, scheinbar unsinnige Zeichenfolgen ergeben damit ein Paßwort, welches im Klartext z.B. „Mausi“ lautet. Diese Verschlüsselung kann in einem vertretbaren Zeitrahmen nicht entschlüsselt werden. Einfacher ist es da, selbst Klartextwörter, die möglicherweise das Paßwort darstellen, mit demselben Verschlüsselungsverfahren zu verschlüsseln und diese dann mit den im Erfolgsfall identischen Einträgen in der Paßwortdatei zu vergleichen. Dies erfolgt mittels der obengenannten Paßwortknacker. Innerhalb dieser Programme kann dann weiter zwischen zwei verschiedenen Vorgehensweisen unterschieden werden.

(1) Lexikon-Angriff

Der sog. Lexikon-Angriff[624] kann als höhere Form des trial and error-Vorgehens bezeichnet werden. Mit der Erkenntnis, daß viele Anwender ähnliche und sehr häufig so-

---

620 Vgl. www.bsi.de/gshb/deutsch/g/g548.htm.

621 Zur Verschlüsselung siehe Seite 100.

622 *Anonymous*, Hacker`s guide, S. 224.

623 Abkürzung für Data Encryption Standard.

624 Englisch: dictionary cracking.

gar dieselben Paßwörter wählen, entstanden Wörterbücher mit häufigen Paßwörtern. Solche Wortlisten sind in großer Zahl im Internet verfügbar. Paßwortknacker in dieser Variante haben solche Wortlistendateien implementiert.[625] Sie können jedes einzelne Wort , wie z.B. das obige Wortbeispiel „Mausi“, aus der Wortliste mit dem gleichen Verschlüsselungsalgorithmus wie das zu findende Paßwort verschlüsseln und dann einen Vergleich mit diesem ausführen. Diese Programme können zumeist auch unter Anwendung verschiedener Regeln Wörter aus der Wortliste verschlüsseln, da der Anwender oft auch kleine Veränderungen an denselben Klartextpaßwörtern vornimmt. So wird beispielsweise dasselbe Wort in Groß- und Kleinschreibung, von hinten nach vorne oder unter Anfügung der Zahl 1 zum Anfang oder Ende des Wortes verschlüsselt. Der automatisierte Lexikonangriff hat sich als eine sehr effektive Methode zur Paßwortbeschaffung gezeigt.[626]

(2) Brute-Force-Attack[627]

Die zweite Variante der Paßwortknacker benutzt die sog. Brute-Force-Methode. Hier werden aus einer bestimmten Sammlung von Zeichen, beispielsweise aus den 26 Zeichen des Alphabets und den Ziffern 0-9, Zeichenketten gebildet, welche dann mit dem Paßwortverschlüsselungsverfahren verschlüsselt und mit den Paßwörtern verglichen werden. Nacheinander werden dann alle möglichen Kombinationen aus dem gewählten Zeichensatz gebildet und ausgewertet.[628]

c) Social Engineering

Eine etwas andere Methode der Paßwortbeschaffung ist das sog. „Social Engineering“.[629] Ziel ist es, durch geschicktes Vorspiegeln falscher Identitäten und Funktionen oder Tatsachen dem nichtsahnenden Geheimnisträger die Zugangsdaten zu entlocken. Das Social Engineering kann z.B. durch einen Telefonanruf erfolgen, bei dem sich

---

625 Sie können zumeist auch neue Wortlisten in das Programm einbinden.

626 Ein verbreites, frei verfügbares Lexikon-Paßwortknackprogramm ist das sog. Crack, welches Unix-Paßwörter aufdeckt. Es soll laut Erfinder dazu benutzt werden Unix-Netzwerke auf schwache Paßwörter zu untersuchen. Erhältlich ist es unter www.users.dircom.co.uk/~crypto/.

627 Dieselbe Bezeichnung hat die computerbasierte Entschlüsselung eines Verschlüsselungsalgrithmus durch Ausprobieren aller möglichen Schlüssel.

628 Ein Beispiel für ein Programm, welches diese Methode anwendet (es unterstützt jedoch ebenso den Lexikon-Angriff) ist das sog. 10phtCrack 2.0, welches Windows NT-Paßwörter aufdeckt. Es ist zu finden unter: www.10pht.com/10phtcrack/ (Hinweis entnommen aus *Anonymous*, Hacker´s guide, S. 233).

629 Die folgenden Beispiele sind entnommen aus www.bsi.de (Bundesamt für die Sicherheit in der Informationstechnik).

jemand als Sekretärin ausgibt, deren Vorgesetzter schnell noch etwas erledigen will, aber sein Paßwort vergessen hat und es jetzt dringend braucht. Beliebt ist auch, als Administrator aufzutreten, der wegen eines Systemfehlers anruft und zur Fehlerbehebung noch das Paßwort des Benutzers benötigt. Weitere Variante ist, als falscher Telefonentstörer anzurufen, der einige technische Details wissen will, z. B. unter welcher Rufnummer ein Modem angeschlossen ist und welche Einstellungen es hat. Weitere Möglichkeit ist auch, sich als Externer zu erkennen zu geben, der gerne Herrn X sprechen möchte, der aber nicht erreichbar ist. Die Information, daß Herr X drei Tage abwesend ist, sagt dem Anrufer gleichzeitig, daß der Account von Herrn X in dieser Zeit nicht benutzt wird, also unbeobachtet ist.

Eine andere, zumeist in den Anfängen des Hackens sehr erfolgreiche Methode, war der Besuch von Computermessen. Hier wurde zum Teil grob fahrlässig mit Paßwörtern umgegangen. So konnte der findige Hacker oft Merkzettel, auf denen die Paßwörter notiert waren, an sich nehmen, oder dem Mitarbeiter während eines inszenierten Beratungsgesprächs einfach beim Einloggen ins System beobachten und dabei die Zugangsdaten ausspähen.

d) „Müllen“

Als besonders effektiv zeigt sich auch das Stöbern im Müll des anvisierten Einbruchsopfers. Dort können wichtige Infomationen über die Funktionsweise des Systems bis hin zu Paßwörtern und sonstigen Einbruchsmöglichkeiten erfahren werden.

2. Strafrechtliche Bewertung

a) Methoden

Die jeweils angewandte Methode der Paßwortausspähung spielt für die strafrechtliche Bewertung bzgl. § 202a keine Rolle. Die Art und Weise des Vorgehens könnte jedoch beim „Müllen“ und beim „Social Engineering“ neben § 202a anderweitig strafrechtlich relevant sein.

Für die Methode des „Müllens“ kommt § 242 und § 123 in Betracht.[630] Dringt der Hakker beispielsweise in ein Firmengelände eines Unternehmens ein, um wertvolle Informationen insbesondere im Müll desselben zu erhalten, so macht er sich gem. § 123 des

[630] Zu der Problematik des Paßwortausspähens bei § 17 UWG siehe Seite 146 und Seite 151.

Hausfriedensbruchs strafbar. Ob er sich bei Entwendung weggeworfener Papiere gem. § 242 strafbar macht, ist Tatfrage. Entscheidend ist, ob der Eigentümer die weggeworfene Sache derelinquiert hat i.S.d. § 959 BGB und diese damit herrenlos geworden ist. Herrenlos wird eine Sache durch Besitzaufgabe mit Eigentumsverzicht.[631] Ist die Sache noch nicht zur Abholung durch die Müllabfuhr bereitgestellt, liegt noch keine Besitzaufgabe vor. Bei Bereitstellung zur Abholung auf dem Firmengelände ist diese Voraussetzung ebenfalls nicht erfüllt. Der Besitzwille ist immer noch vorhanden, da bewußt eine Abholung auf dem firmeneigenen Gelände vorgesehen ist. Der Hacker würde sich in diesen Fällen gem. § 242 strafbar machen. Ein Diebstahl in einem besonders schweren Fall gem. § 242 iVm § 243 kann bei entsprechendem Vorgehen (z.B. der Hacker steigt über den Zaun des Unternehmens) ebenfalls einschlägig sein.

Im Bereich des Social Engineering können die §§ 263, 263a, 265a angedacht werden. Der Hacker ruft beispielsweise bei einem Internetnutzer an und gibt sich als Systemadministrator dessen Internet-Service-Providers aus. Er bittet um das Paßwort des Angerufenen, da aufgrund eines Computerfehlers alle Paßwörter wieder neu eingerichtet werden müßten. Der Angerufene buchstabiert dem „Systemverwalter“ das Paßwort. Der Hacker geht dann sofort mit Hilfe dieses Paßworts ins Internet. Die für die Nutzung entstandenen Kosten werden dem bereitwillig Auskunft gebenden in Rechnung gestellt. § 263 ist nicht einschlägig, da die Herausgabe des Paßworts nicht unmittelbar zu einer Vermögensminderung führte und es insofern an der Unmittelbarkeit der Vermögensverfügung fehlt. In Bezug auf die Eingabe des Paßworts fehlt es an einer Täuschungshandlung gegenüber einem Menschen.

Mit Benutzung des Paßworts erhält der Hacker die Möglichkeit, auf Kosten eines anderen das Internet zu nutzen. Durch die Eingabe des Paßworts und der Nutzung der Service-Provider Dienstleistung macht er sich nach § 263a strafbar. Die Paßwortdaten hat er unbefugt i.S.d. § 263a Abs. 1 Var. 3 verwendet. Die Unbefugtheit ergibt sich daraus, daß der Hacker nicht Vertragspartner des Service-Providers war.[632] Die Authentifikation durch das Paßwort und die Nutzungsmöglichkeit der Dienstleistungen sind Ergebnis eines Datenverarbeitungsvorgangs. § 265a ist ebenfalls gegeben in der Variante des Erschleichens von Leistungen eines Automaten (§ 265a Abs. 1 Var. 1).[633] Automat ist der Rechner des Service-Providers. Dessen entgeltliche Leistung ist der Zugang zum Internet. Erschlichen ist diese Leistung, da der Hacker unter Vortäuschung einer ord-

---

631 Tröndle/Fischer-*Tröndle*, § 242 Rn. 8.

632 Hilgendorf, JuS 1997, 323 (327); zu § 263a siehe auch Hilgendorf, JuS 1999, 542 ff.

633 Eingehend dazu *Hilgendorf*, JuS 1997, 323 (327).

nungsgemäßen Benutzung gehandelt hat. Der subjektive Tatbestand, Vorsatz und Absicht das Leistungsentgelt nicht zu entrichten, sind ebenfalls erfüllt. § 265a tritt hinter § 263a zurück.[634]

b) Erfolg

Für alle Methoden soll in Bezug auf den Erfolg (das Herausfinden des Paßworts) ein Fallbeispiel dazu dienen, die Strafbarkeit der Paßwortausspähung gem. § 202a zu prüfen.

Fall: Hacker H wird auf das alleingelassene Notebook des Doktoranden D aufmerksam. Ihn interessiert brennend die dort abgelegte Doktorarbeit des D. Sogleich schaltet er den Rechner an. Nun wird er jedoch aufgefordert das Boot-Paßwort[635] des D einzugeben. Mit Eingabe des Vornamens der Freundin wird der Rechner hochgefahren.

Fraglich ist, ob das Herausfinden und damit auch die Kenntnisnahme des Codeworts unter § 202a subsumiert werden kann. Das Paßwort ist taugliches Tatobjekt, da es Informationen beinhaltet, die in nicht wahrnehmbarer Form gespeichert sind. Auch das Paßwort ist von § 202a grs. als Daten geschützt.[636] Das Paßwort ist auch nicht für den Hacker H bestimmt. Ein Einverständnis bzgl. der Verfügbarkeit der Daten für Hacker H ist nicht gegeben.

Bühler[637] ist der Ansicht, daß auch schon das Beschaffen eines Code-Worts (Paßwort) ein Sich-Verschaffen von Daten ist, weil das Code-Wort ja auch nur über Programme etc. herausbekommen werden könne und bejaht in diesem Fall die Strafbarkeit nach § 202a. Diese Argumentation ist jedoch nicht nachvollziehbar, da zum einen Paßwörter auch durch Ausprobieren geknackt werden können[638], zum anderen der Hinweis auf Programme, die das Paßwort herausfinden, auch nicht weiterhilft. Das „Verschaffen" solcher Paßwörter ist durchaus zu bejahen. Vorher ist jedoch zu klären, ob das Paßwort selbst durch eine besondere Zugangssicherung geschützt ist, was für die Bejahung des § 202a zwingend notwendig ist. Hierzu schweigt sich *Bühler* jedoch aus.

---

634 Siehe § 265a Abs. 1 a.E.

635 Paßwortschutz auf BIOS-Ebene eines Rechners, der vor dem eigentlichen Start-(Boot-)vorgang wirksam wird. Er schützt alle Daten, die auf dem Rechner abgelegt sind. Das BIOS (Basic Input Output System) steuert das Ausführen elementarer Operationen, wie Eingabe über Tastatur, Ausgabe über Bildschirm und Drucker.

636 *Möhrenschlager*, wistra 1986, 128 (140).

637 *Bühler*, MDR 1987, 448 (453).

638 Vgl. *Binder*, RDV 1995, 57 (59 f.).

Auch *Lenckner*[639] stellt fest, daß, falls die Überwindung der Zugangssicherung die Kenntnis der Daten des Zugangscodes voraussetze, deren Ausspähen allerdings auch nach § 202a strafbar sein könne.[640] Ist hier Ausspähen im Sinne des § 202a gemeint (**Ausspähen von Daten** ist die amtliche Überschrift von § 202a), so ist dies eine richtige Aussage. Sie hilft dennoch für die Lösung des Problems nicht weiter, da Ausspähen von Daten i.S.d. § 202a auch nur an solchen Daten erfolgen kann, die ihrerseits besonders gesichert sind. Auf die Sicherung, die durch das Paßwort selbst erfolgt, kann nicht abgestellt werden, da diese Zugangsschranke nur andere Daten und Dateien vor dem Zugriff schützt, nicht aber sich selbst.[641]

Hilgendorf[642] nennt in diesem Zusammenhang die Geheimhaltung[643] des Paßworts als besondere Sicherung i.S.d. § 202a. Anders als das bloße Verbot habe die Geheimhaltung eines Paßwortes durchaus objektive Wirkung; die Möglichkeit eines Zugriffs werde durch sie ebenso zuverlässig verhindert wie durch eine softwaretechnische Sicherung. Dem ist grs. zu folgen. Im Falle der Geheimhaltung eines Paßworts ist der Geheimhaltungswille des Berechtigten unmißverständlich erkennbar. Der Hacker befindet sich auf der Ebene des login-Prozesses[644], bei dem die Eingabe eines Paßworts gefordert wird. Er weiß damit um die Geheimhaltung als solche, welche ihn objektiv hindert, das Paßwort herauszufinden. Verschafft er sich dieses Paßwort, so ist dieses Vorgehen unter § 202a subsumierbar.

Nun taucht jedoch wieder die Problematik auf, daß der Gesetzgeber das Hacken i.e.S. und damit das bloße Eindringen in geschützte Datenbereiche für straflos hielt.[645] Würde man nun das Verschaffen von Paßwörtern unter § 202a subsumieren, so wäre genau die klassische Vorgehensweise des Hackens, das Knacken von Paßwörtern, unter Strafe gestellt, welche der Gesetzgeber für straflos erachtete. Um dem Willen des Gesetzge-

---

639 Schönke/Schröder-*Lenckner*, § 202a Rn. 10 unter direkter Bezugnahme auf *Bühler*, MDR 1987, 448 (453).

640 Auch *Haurand/Vahle*, RDV 1990, 128 (132) sprechen von der Strafbarkeit des Ausspähens von Paßwörtern nach § 202a; so auch *Koch*, RDV 1996, 123 (126).

641 Vgl. *Hilgendorf*, JuS 1997, 323 (324); *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 180 Fn. 11; in diesem Sinne auch *Binder*, Strafbarkeit intelligenten Ausspähens von programmrelevanten Unternehmensgeheimnissen, S. 49.

642 *Hilgendorf*, JuS 1997, 323 (324).

643 Zur Problematik der Geheimhaltung durch Verstecken von Daten in ungewöhnlichem Verzeichnis siehe Seite 104.

644 Beim LOGIN identifiziert sich der Benutzer bei dem Rechner oder dem Datenbereich, zu dem er Zugang erhalten möchte, und gibt das dazugehörige Paßwort ein.

645 BT-Drs. 10/5058, S. 28.

bers Geltung zu verschaffen, ist somit auch das Tatbestandsmerkmal der besonderen Zugangssicherung um die Geheimhaltung des Codeworts teleologisch zu reduzieren. Hacker H hat sich demnach im obigen Fall wegen des Herausfindens des Paßworts nicht nach § 202a strafbar gemacht.

II. Datenreisen

Fallbeispiel: Hacker H hat sich vorgenommen, von einem System zum nächsten zu springen, um sich so gegenüber seinen Hacker-Kollegen als Datenreisender auszuzeichnen. Er verschafft sich Zugang zu dem paßwortgeschützten Rechner einer großen Computerfirma, welche mit vielen anderen Rechnern vernetzt ist. Von diesem Rechner aus verschafft er sich Zugang zu weiteren geschützten Rechnern. Sobald er Zugang zu einem neuen Rechner hat, wiederholt er das Spiel, so daß er von einem Rechner zum nächsten „hoppen" kann, die sich an den verschiedensten Orten befinden.[646] Ist H nach § 202a strafbar?

Beim Datenreisen kommt es in erster Linie darauf an, ob dies noch als Hacken i.e.S. gewertet werden kann. In diesem Zusammenhang stehen sich wiederum die Ansichten von *Hilgendorf* und *Tröndle* gegenüber. So erachtet *Hilgendorf*[647] *Tröndles* Differenzierung von Daten, die mit dem Zugriff auf das System verbunden sind und solchen, die im System gespeichert sind, als überaus problematisch. Der typische Hacker dringe in einen Rechner ein, um seinen Einfallsreichtum und seine Fertigkeiten unter Beweis zu stellen. Der Zugriff auf das System sei geglückt, wenn die im System befindlichen Zieldaten seinem Zugriff unterliegen. Der Hacker werde sich also in aller Regel erst dann zufrieden geben, wenn die im fremden System gespeicherten Daten ungeschützt vor ihm liegen; erst dann wüßte er ja auch, daß keine weiteren Sicherungen zu überwinden sind.

Nach dieser Ansicht wird folglich das Hacken i.e.S. weit interpretiert. Hacking ist damit das Eindringen in Systeme, ohne Kenntnis von Daten zu nehmen in der Weise, daß diese sicher reproduzierbar sind. Der Hacker kann danach durch das System spazieren, um weitere Anschlüsse an andere vernetzte Rechner zu suchen, und von dort in diese durch Überwindung oder Umgehung der Zugangssicherungen (zumeist Paßwortschutz) einzudringen, um möglicherweise von dort aus „weiterzureisen". Im Gegensatz dazu ist der

---

646 So auch bei dem berühmten KGB-Hack (nachzulesen bei *Stoll*, Kuckucksei, die Jagd nach den deutschen Hackern, die das Pentagon knackten, Frankfurt/Main 1990), bei dem ein gewisser M. H. in den Rechner der Lawrence Berkeley Laboratories (LBL) eindrang, um von dort aus sich Zugriff zu weiteren vernetzten Rechnern zu verschaffen.

647 *Hilgendorf*, JuS 1996, 702 (704).

„Datenreisende“ nach Ansicht *Tröndles*[648] strafbar, da er notwendigerweise das System nach Portalen zu weiteren Systemen suchen muß und damit Daten aufruft, die **im** System gespeichert sind.

Die Entscheidung zwischen diesen verschiedenen Ansätzen hat sich am gesetzgeberischen Willen auszurichten. Der Gesetzgeber spricht davon, daß sog. „Hacker“, die sich mit dem bloßen Eindringen in ein Computersystem begnügen, von Strafe verschont bleiben.[649] Der Eindringling überwindet die Sicherung zum System, freut sich über seine gedanken-sportliche Leistung und verschwindet sofort wieder. Gerade dies macht jedoch der Datenreisende nicht. Er ist geradezu darauf angewiesen, das System zu durchsuchen, um nach Möglichkeiten Ausschau zu halten, weiter zu reisen. Dies beeinträchtigt das Rechtsgut des § 202a. Von einer Geheimhaltung der Daten kann bei dem im System umherschweifenden Hacker nicht mehr die Rede sein. Bei dieser Suche nimmt der Eindringling unweigerlich Daten wahr, die er danach differenziert, ob sie solche sind, die ihn zu einem weiteren Rechner bringen. Daher ist die Ansicht *Tröndles* vorzuziehen. Sie berücksichtigt in ihren praktischen Auswirkungen am ehesten die Vorstellung des Gesetzgebers vom straflosen Hacken.

Die Tathandlung „Verschaffen“ ist daher in der Form der Kenntisnahme von Daten gegeben. Die übrigen Tatbestandsmerkmale sind ebenfalls erfüllt. Auf Vorsatz, Rechtswidrigkeit und Schuld braucht nicht näher eingangen zu werden. „Datenreisender“ H ist damit strafbar gem. § 202a.

---

[648] Tröndle/Fischer-Tröndle, § 202a Rn. 9.

[649] BT-Drs. 10/5058, S. 28.

III. Trojanische Pferde[650]

1. Aufbau und Funktion

a) Allgemein

Sogenannte „Trojanische Pferde“ sind Programme mit versteckten Nebenwirkungen. Die Bezeichnung „Trojanisches Pferd“ wurde der griechischen Sagenwelt entnommen.[651] Das Trojaner-Programm bedient sich, wie das aus der griechischen Mythologie überlieferte Pferd, einer List. Es erbringt zwar einerseits seine spezifizierte Leistung (z.B. als Spiel-Programm), darüber hinaus jedoch beinhaltet es noch unzulässige, vom Konstrukteur oder Manipulierer beabsichtigte und nicht dokumentierte Nebenwirkungen.[652] Sie werden von dem Konstrukteur oder Verwender an eine bestimmte Stelle in ein Rechnersystem eingebracht und bleiben dort, falls nicht weiter von außen auf sie eingewirkt wird. Das trojanische Pferd vermehrt sich anders als die sog. Viren[653] grs. nicht.[654] Von dem gewählten Standort aus, ist es Hauptfunktion des Trojanischen Pferdes, Systeme und deren Anwender auszuspionieren. Sie können Sicherheitslücken erkunden, Hintertüren[655] im System öffnen oder bestehende Infrastrukturen zerstören.

---

650 Englisch: trojan horse; auch oft nur „Trojaner“ genannt.

651 Kleiner Exkurs: Nach zehnjähriger erfolgloser Belagerung Trojas bauten die Griechen ein großes hölzernes Pferd, in dessen Bauch sich die besten Soldaten versteckten. Das griechische Heer zog ab, nur das hölzerne Pferd stand immer noch vor den Toren Trojas. Die Trojaner hielten das schöne Werk für eine Opfergabe und zogen es in die Stadt. In der darauffolgenden Nacht verließen die griechischen Soldaten ihr Versteck, öffneten die Stadttore und benachrichtigten mit Feuerzeichen die eigene Flotte. Mit dieser List gelang dann die Eroberung von Troja.

652 Vgl. *Oppliger*, Computersicherheit, S. 94.

653 Ein Computervirus ist ein nicht-selbständig ablauffähiges Programm, oder ein Programmteil, das sich in einem sog. Wirtsprogramm enthalten ist (*Pohl/Weck*, DuD 1993, 18 (20)). Der Virus hat zwei grundlegende Eigenschaften und Funktionen. Erstens, er enthält ein Unterprogramm für die Infektion eines Wirtsprogramms (Vermehrung), zweitens ein Unterprogramm für die Funktion, welches die verschiedensten Schadensroutinen sein können (z.B. Formatieren der Festplatte) (vgl. *Dierstein*, NJW-CoR 1990, 8 (10)).

654 Ein Spezialfall stellen trojanische Pferde dar, die in sog. Würmer integriert sind. Würmer sind selbstreproduzierende (sich selbst kopierende), selbständig ablaufende Programme. Der Wurm ist ein Programm, das auf einem oder mehreren Rechnern leben kann und aus verschiedenen Segmenten, die sich auf verschiedenen Systemen zu installieren suchen und miteinander kommunizieren.

655 Englisch: backdoor.

Als Träger für Trojanische Pferde lassen sich alle möglichen Anwenderprogramme benutzen. Auch Scriptsprachen, wie z.B. Postscript[656], die vom jeweiligen Betriebssystem oder Anwenderprogramm interpretiert werden, können für Trojanische Pferde mißbraucht werden. Zumeist jedoch werden Trojanische Pferde als Tarnung an Shareware, Freeware, oder Public-Domainprogramme[657] angehängt. Der Internetnutzer lädt nichtsahnend ein Programm und startet es. Auch wenn diese Programme gleich wieder gelöscht oder deinstalliert werden, hat sich das trojanische Pferd schon unbemerkt installiert. Trojanische Pferde sind meistens kleine Programme, die „lediglich" einen Eintrag in der Windows-Registry[658] vornehmen. Doch dieser Eintrag hat gravierende Folgen: Er öffnet bestimmte Ports[659] eines Rechners und läßt ihn bei der nächsten Internetverbindung vor Hackern absolut ungeschützt. Wenn der infizierte Rechner[660] online geht, benötigt der Rechner des Hackers lediglich die IP-Adresse[661] des infizierten Rechners und schon hat er vollen Zugriff.[662] So kann er z.B. Dateien kopieren oder löschen.
Die für einen Hacker interessanteste Funktion liegt in der unbemerkten Protokollierung von Codewörtern, die Zugang zu geschützten Systemen und Datenbereichen zulassen. Paßwörter werden (und sollten)[663] zumeist nach Vergabe einwegverschlüsselt[664] abge-

---

656 PostScript ist eine von der Firma Adobe 1985 vorgestellte Programmiersprache, die dazu dient die Ausgabe von Text und Bildern auf einer auszugebenden Seite an einen Laserdrucker oder Belichter zu steuern (*Grieser/Irlbeck*, Computerlexikon, S. 707).

657 Als „Freeware" werden Computerprogramme bezeichnet, die unentgeltlich für private Zwecke genutzt werden dürfen. Sie sind jedoch urheberrechtlich geschützt und dürfen daher nicht verändert werden. „Public-Domain-Software" ist ebenfalls unentgeltlich für private Zwecke nutzbar und kann, da auf urheberrechtlichen Schutz verzichtet wurde, auch gänzlich uneingeschränkt benutzt und verändert werden. „Shareware" kann ebenfalls genutzt (jedoch nicht verändert) und auch weitergegeben werden. Es darf jedoch nur für eine bestimmte Zeit getestet werden. Sobald man es auf Dauer nutzen will, muß man sich beim Programmautor als Anwender regisitrieren lassen und eine Registrierungsgebühr entrichten.

658 „Registry" ist die englische Bezeichnung für eine Konfigurationsdatenbank eines Betriebssystems.

659 Port ist im Internet die Nummer, die nach Doppelpunkt in einer URL auftaucht. Es gibt Standard-Portnummern für Standarddienste im Internet, z.B. 80 für HTTP 25 für SMPT.

660 In diesem Zusammenhang „server" genannt; Ein „server" (wörtlich: „Meß"-Diener) ist ein Rechner, der für andere Rechner Dienstleistungen zur Verfügung stellt und von dem zumeist auch zentral das Netzwerk gesteuert wird.

661 Die IP-Adresse ist eine numerische Adresse zur Identifizierung von Rechnern in einem TCP/IP-Netz. Das Internet basiert auf den Kommunikations-Protokollen TCP und IP. Das IP (Internet Protokoll) ist für die Adressierung und Weiterleitung der Daten zuständig. Das TCP (Transmission Control Programm) sorgt beim Empfänger für die Sortierung der übermittelten Datenpakete in die richtige Reihenfolge und sichert die Kommunikation durch Betätigung des Paket-Empfangs ab.

662 *Luckardt*, c`t 4/2000, 208 (210).

663 Beispiele: Beim Finanzprogramm „Quicken" wurden bis in die vorletzte Version Paßworte unverschlüsselt abgelegt. Der Datenschutzbeauftragte von Baden-Württemberg, Werner Schneider, rügte die Universität Tübingen wegen unzulänglicher Sicherheitsmaßnahmen nach einem äußerst

legt. Die zur Authentifizierung eingegebene Ziffernfolge wird dann nach derselben Einwegverschlüsselung mit dem abgelegten Paßwort verglichen. Diese einwegverschlüsselten Codes sind äußerst schwer entschlüsselbar. Wird nun die Paßworteingabe vor Verschlüsselung im Klartext abgefangen, protokolliert und abgerufen, so hat der Hacker im Falle der Kenntnis der entsprechenden Benutzerkennung Zugriff zum System. Somit kann dadurch sehr elegant die Sicherungswirkung der Verschlüsselung umgangen werden.

b) Spoofing-Programme

Bei Hackern sind die sog. Spoofing-Programme[665] besonders beliebt, welche eine bestimmte Unterart eines Trojaners darstellen. Sie stellen Vorschaltprogramme dar, die zumeist in den Hauptspeicher des betroffenen Rechners geladen werden.[666] Das Spoofing-Programm wird aktiviert, wenn der Nutzer Zugang zu einem gesicherten Bereich, oder zu einem Netz haben möchte. Um dies zu erreichen, muß er einen login-Prozeß abarbeiten. Mit dessen Hilfe wird die Identität des Benutzers festgestellt und entschieden, ob dieser Benutzer Zugang zum System erhält. Zunächst wird die nicht geheime Benutzerkennung[667] eingegeben. Dies dient der Identifikation des Benutzers.[668] Darauf muß der Rechner feststellen können, ob auch der richtige Benutzer, der die user-ID zulässigerweise verwenden darf, sich Zugang verschaffen möchte. Dies wird dadurch erreicht, daß zumeist ein geheimes Paßwort eingegeben werden muß, welches mit der user-ID verknüpft ist. Dies erscheint selbst nicht im Klartext auf dem Bildschirm, sondern zumeist versteckt durch Platzhalter (z.B. ******).[669]

Das Spoofing-Programm simuliert nun diesen LOGIN-Prozeß.[670] Der Benutzer meint das echte LOGIN-Programm vor sich zu haben und gibt ahnungslos user-ID und Paß-

---

erfolgreichen Hackerangriff. Insbesondere wurden Paßwörter unverschlüsselt übertragen. (Südkurier vom Donnerstag, den 09.03.2000, S. 25).

664 Einwegverschlüsselung ist eine Gruppe von Verschlüsselungsverfahren, die auch bei Kenntnis des Schlüssels nicht (oder nur schwer) entschlüsselt werden können; eingehend dazu Kersten, Sicherheit in der Informationstechnik, S. 43 f.

665 Spoofing heißt „Vortäuschen, Vorgaukeln"; Spoofing-Programme werden auch „Namensvettern" genannt (vgl. *Dierstein*, NJW-CoR 4/1990, 8 f.).

666 *Paul*, NJW-CoR 1/1996, 62.

667 Englisch: user-ID.

668 Englisch: identification.

669 Englisch: authentication.

670 *Kersten*, Sicherheit in der Informationstechnik, S. 249, nennt als Oberbegriff für ein derartiges Vorgehen die Maskerade: Manipulationsmethode, bei der sich eine Instanz als eine andere ausgibt.

wort ein. Daraufhin meldet ihm das Spoofing-Programm eine Falscheingabe des Paßworts, protokolliert die Eingaben in eine Referenzdatei, deaktiviert sich und aktiviert das echte LOGIN-Programm. Der immer noch ahnungslose Benutzer versucht es ein zweites Mal und gelangt dann natürlich problemlos in den geschützten Bereich. Der Hacker sieht das erlangte Paßwort direkt am Rechner ein, oder läßt sich diese Daten übers das Netz zukommen.

c) Aktuelle Beispiele

Die beiden bekanntesten und gebräuchlichsten trojanischen Pferde sind wohl „Netbus" und „Back Orifice"[671]. „Back Orifice" kann an ein beliebiges Programm angehängt werden und ist außerdem stark modifizierbar, was es zu einem der gefährlichsten Trojanerprogramme macht. Es besteht aus einem Server[672]- und einem Client[673]-Programm, welches zur Fernbedienung[674] von Rechnern in einem Netzwerk eingesetzt werden kann. Da es sich selbst installieren und an andere Programme angehängt werden kann, erfolgt die Verbreitung unter Umständen unbemerkt. „Back Orifice" wird in der Task-Liste[675] nicht angezeigt und wird beim Hochfahren des Rechners unter einem beliebigen Namen gestartet. Während der Client auf allen möglichen Betriebssystemen lauffähig ist, funktioniert der Server nur auf Windows 95/98. Back Orifice ist nunmehr auch in der verbesserten und noch gefährlicheren Version, genannt Back Orifice 2000, verfügbar.

Die erste Version des Trojaners „NetBus"[676] wurde Mitte März 1998 veröffentlicht. Die Funktionalität von Netbus ist der von „Back Orifice" vergleichbar. Jedoch hat es eine

---

Als weiteres Beispiel führt er an, daß sich eine Person ihre Arbeitsstation in einem LAN (local area network; Netzwerk von Rechnern, welches sich auf einen betimmten begrenzeten Raum beschränkt, z. B. in Bürogebäude einer Firma, oder Behörde) als LAN-server ausgibt, um auf diese Weise an die user-IDs und Paßwörter der anderen Benutzer zu gelangen.

671 „Back Orifice" wurde von der Hackergruppe „cult of the dead cow" (cDc) geschrieben und ist seit dem 03.08.1998 im Internet verfügbar; übersetzt: Hintere Öffnung.

672 Siehe Fußnote auf Seite 39.

673 „Clients" (oder „Klienten") sind Arbeitsplatzrechner oder Programme, die Dienstleistungen von Servern in Anspruch nehmen. So können Rechner in Netzen gemeinsame Betriebsmittel oder Dienste mit anderen Arbeitsplatzrechnern teilen.

674 Englisch: remote.

675 Diese zeigt in Betriebssystemen an, welche Dateien und Programme gerade gleichzeitig aktiv sind und in den Hauptspeicher des Rechners geladen wurden.

676 Netbus wurde von dem Schweden Carl-Frederik Neikter geschrieben.

bessere Client-Oberfläche mit der Folge, daß es von den Hackern auch am häufigsten benutzt wird.

Ist eines dieser Programme erst einmal auf dem mit dem Internet oder einem anderen Netz, auf das der Hacker Zugriff hat, verbundenen Rechner eines ahnungslosen Anwenders installiert, so kann der Hacker damit beispielsweise Tastatureingaben aufzeichnen, Web-Seiten ansteuern, Anwendungen auf dem attackierten Rechner starten, Manipulationen am Dateiensystem vornehmen, wie Kopieren, Löschen, Umbenennen oder Suchen. Daneben kann er auch Up- und Downloads[677] von Daten aus dem und ins Internet vornehmen oder sogar den Rechner dazu veranlassen, wieder hochzufahren[678].

2. Strafrechtliche Bewertung

Bei der strafrechtlichen Beurteilung von Trojanischen Pferden in der Variante des Spoofing-Programms ist zwischen dem Installieren des (Server-)Programms, dem Ausschnüffeln des Paßworts und dem anschließenden Verwenden des Codeworts und dem Eindringen in den geschützten Bereich zu unterscheiden.

Beispielsfall:

A surft gerade im Internet und ist auf der Seite des Hackers B angelangt. Dort wird ihm ein Programm namens whackjob.exe[679] angepriesen und zum Download angeboten. A speichert das Programm auf seiner Festplatte und ruft es auf. A merkt nicht, daß der Trojaner NETBUS aktiviert wird. Dieser protokolliert beim nächsten Einloggen das Paßwort, welches A für den Zugriff auf eine Partition der Festplatte vergeben hat, in der A für ihn wichtige Daten gespeichert hat. B kopiert dann mit Hilfe des Trojaners und des Paßworts Dateien aus dieser Partition auf seinen Rechner.

---

677 „Upload“ wird genannt, wenn der angeschlossene Rechner Daten zum Abruf für das Netzwerk bereitstellt. „Download“ wir genannt, wenn ein Benutzer sich Daten, die von einem Netzwerk abrufbar sind, schicken läßt, so daß er damit arbeiten kann oder auf einem Festspeicher (zumeist Festplatte) abspeichert.

678 Englisch: reboot.

679 In einer im Internet zum Download angebotenen Anwendung dieses Namens war der Trojaner NETBUS integriert.

(1) Installieren des Trojanischen Pferds

Da der Internetnutzer[680] ahnungslos ist, ist hier der Hacker B möglicherweis mittelbarer Täter (§ 25 Abs. 1 Alt. 2) des § 202a. Er hat Tatherrschaft in Form der Wissensherrschaft. Er weiß um den Trojaner, der Tatmittler A nicht. Dennoch ist bei der Installation des Trojanischen Pferds § 202a nicht einschlägig. Der Hacker hat lediglich Daten hinzugefügt und zumindest zu diesem Zeitpunkt keine Daten zur Kenntnis genommen oder kopiert. Des weiteren kann die Installation oder die Aktivierung des Trojaners nur in ungesicherter Datenumgebung vorgenommen worden sein. Der Hacker B möchte ja gerade erst in diese Bereiche eindringen. § 202a i.V.m. § 25 Abs. 1 Alt. 2 ist somit nicht einschlägig. Gäbe es eine Versuchsstrafbarkeit des Ausspähens von Daten, so könnte die Installation eines Trojaners als Versuch gewertet werden.

Fraglich ist, ob § 303a gegeben ist. Überschreibt der Trojaner andere auf dem Datenträger gespeicherte Daten, um sich besser tarnen zu können, da er dann nicht durch Datenvermehrung auffällt, so liegt ein Löschen i.S.d. § 303a vor. Zumeist jedoch installieren sich Trojaner auf nicht belegten Speicherplätzen, so daß lediglich eine Datenvermehrung stattfindet. Fraglich ist, ob hiermit ein Verändern von Daten i.S.d. § 303a gegeben ist. Anknüpfungspunkte sind das automatische Ändern von Daten bei der Installation und die Änderung des Umfelds der ursprünglichen Daten durch die mit der Installation erfolgten Datenvermehrung.

(a) Automatische Änderung

Jäger ist der Ansicht, daß jeder Hacking-Angriff Daten in irgendeiner Form, sei es durch eine Protokollierung der Zugriffsdaten auf dem Server[681], sei es durch Veränderung der Daten im RAM[682] oder im Speicher der Grafikkarte, Daten i.S.d. § 303a verändere.[683] Dies ist abzulehnen. Jeder Zugriff auf den Hauptspeicher oder jeder Befehl, der dem Speicher einer Grafikkarte gilt, verändert Daten im tatsächlichen Sinne. Hier wird der Blick jedoch auf jedes einzelne Bit gelenkt. Jeder Befehl, der auf einem Rechner ausgeführt wird, verändert automatisch einzelne Bits und Bytes eines Rechners, insbesondere im flüchtigen Speicher (Hauptspeicher). Eine solche Auslegung würde

---

680 Bloße Internetanwender ohne großes technisches Wissen werden von Hackern „Loser“ genannt (*Paul*, NJW-CoR 1996, 62), neuerdings jedoch in Anspielung auf einen Werbespot „Ich-bin-schon-drin-Surfer“ (Südkurier vom 10.03.2000, S. 3).

681 Siehe Fußnote auf Seite 39.

682 Random Access Memory: Flüchtiger Speicher in den Daten zur Verarbeitung geladen werden.

683 *Jaeger*, c`t 9/1999, 174 (174) ebenso in c`t 4/2000, 232 (233).

jedoch die Strafbarkeit zu weit ausdehnen. Sie würde gar dazu führen, daß eine „datenbezogene Gebrauchsanmaßung“ durch die Hintertüre strafbar wäre.[684] Daher ist der h.M. zu folgen, die auf die Änderung des Informationsgehalts von Daten abstellt.[685] Es sind somit Datenfelder voneinander abzugrenzen, die einen bestimmten Informationsgehalt haben, welcher dann unter Umständen verändert werden könnte. Entscheidend ist in diesem Zusammenhang somit die semantische Ebene des Datenfelds und nicht die bloße Veränderung der syntaktischen Ebene der Daten.

(b) Änderung des Datenumfeldes

Die Datenvermehrung durch die Installation des Trojaners könnte darin liegen, daß das Umfeld der eigenen Daten des A verändert wurde. Die bloße Vermehrung des Datenbestandes verändert jedoch nicht den Inhalt der ursprünglichen Daten. Die zusätzlichen Daten sind sozusagen auf einem anderen Parkplatz. Eine veränderte Verknüpfung der neuen Daten mit denen des A, welche eine inhaltliche Umgestaltung der Daten des A darstellen würde[686], hat ebenfalls nicht stattgefunden. Folglich ist das Interesse des A an der unversehrten Verwendbarkeit seiner Daten und damit das Rechtsgut des § 202a nicht tangiert.[687]

Die Installation eines Trojaners durch B ist demzufolge straflos.

(2) Ausschnüffeln des Codeworts

Der Hacker B hat im obigen Fall das Paßwort zu den geheimen Daten des H erhalten. Das Erlangen des Paßworts ist, wie oben schon geprüft, nicht strafbar.[688]

(3) Anschließendes Verwenden des ausgeschnüffelten Paßworts

Mit dem Kopieren der geschützten Daten auf seinen Rechner hat sich B gem. § 202a strafbar gemacht. Somit hat das Verwenden von Trojanern keine Änderung der Beurteilung der Strafbarkeit des Hackens zur Folge. Die Ansicht *Jessens*[689], daß das Verwenden von vorher straflos erlangten Paßwörtern straflos sei, und das sogar bei Einsatz

---

684 Vgl. *Schulze-Heiming*, Der strafrechtliche Schutz der Computerdaten, S. 254 ff.

685 Siehe Seite 140.

686 *Hilgendorf*, Anmerkung zu Bay ObLG 1993, 486 ff., JR 1994, 478.

687 Vgl. *Hilgendorf*, JuS 1997, 322 (324); *Binder*, Strafbarkeit intelligenten Ausspähens von programmrelevanten Unternehmensgeheimnissen, S. 76 f.

688 Siehe Seite 156 ff.

689 *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 198 und S. 154 ff.

von Trojanern, ist abzulehnen. Es kommt allein darauf an, daß die Sicherungswirkung als solche erkennbar war, und damit bei grundsätzlicher Wirksamkeit den Geheimhaltungswillen unmißverständlich deutlich macht. Eine besondere Sicherung i.S.d. § 202a ist gegeben, so daß sich auch derjenige strafbar macht, der zufällig Kenntnis von einem Paßwort erlangt und dieses anschließend zum Ausspähen der Daten verwendet.

IV. Ausnutzen von sog. Wanzen[690] oder sog. Falltüren[691]

1. Vorgehensweise

Wanzen sind Programmierfehler. In jedes umfangreichere Programm und damit auch in jedes Betriebssystem schleichen sich bei der Programmierung Fehler ein.[692] Diese Fehler führen zu Lücken im Sicherheitskonzept des Programms. Das Herausfinden solcher Fehler und deren Ausnutzung ist eine der Hauptbeschäftigungen versierter Hacker.

Falltüren sind Pfade in einem Programm, die in der Konzeption des Programms nicht vorgesehen waren, aber durch den Programmierer zu Testzwecken oder in manipulativer Absicht eingebaut wurden.[693] Als Teil eines Sicherheitssystems können solche Programmteile, z.B das Login-Programm, zur Umgehung aller Sicherheitsmaßnahmen eingesetzt werden.[694] Das Programm kann den Programmierer oder den Hacker, der Kenntnis von dieser Falltüre besitzt, anhand einer sonst nicht vorkommenden User-ID oder eines speziellen Paßworts erkennen, ggf. auch durch eine spezielle Tastenkombination (Hot Key).[695] Ist eine solche Falltür auch nur zu Wartungszwecken programmiert worden, so besteht dennoch die Gefahr, daß außenstehende Hacker diese entdecken und möglicherweise dieses Wissen verbreiten und ausnützen.

---

690 Englisch: bugs; siehe auch *Oppliger*, Computersicherheit, S. 94.

691 Englisch: trapdoors; siehe auch *Oppliger*, Computersicherheit, S. 94.

692 So müssen Softwarefirmen die Programme laufend nachbessern und den Anwender informieren, wie Fehler berichtigt oder umgangen werden können. Oftmals kann auch über das Internet das entsprechende Programm auf den neuesten Stand gebracht werden.

693 *Kersten*, Sicherheit in der Informationstechnik, S. 62.

694 Vgl. *Oppliger*, Computersicherheit, S. 94.

695 *Kersten*, Sicherheit in der Informationstechnik, S. 62.

2. Strafrechtliche Bewertung

Dringt ein Hacker über Falltüren oder über Ausnutzung von Wanzen in ein ansonsten gesichertes System ein, so ist dies nach h.A.[696] nicht nach § 202a strafbar. Nur die Überwindung der konkreten Zugangssicherung führt zur Strafbarkeit. Bei Zugang über Falltüren nutzt der Eindringling Sicherheitslücken aus, die völlig unabhängig von der eigentlichen Sicherung sind. Nach der hier vertretenen Ansicht ist hingegen eine Strafbarkeit gem. § 202a zu bejahen. Ist dem Täter die Sicherung als solche erkennbar geworden, ist der Geheimhaltungswille ausreichend für den konkreten Täter dokumentiert. Dringt er dennoch, auf welchem Weg auch immer in das geschützte System ein, so macht er sich nach § 202a strafbar.

V. Adress-Spoofing

1. Vorgehensweise

Adress-Spoofing ist eine Angriffsmethode, bei der gefälschte Adressangaben einer Netzwerkschnittstelle eines Rechners dem Zielrechner vorgaukeln, der Rechner des Angreifers sei ein anderer, bekannter und als vertrauenswürdig eingestufter Rechner.[697] Gelingt dieses Vorgaukeln einer vertrauenswürdigen Adresse, so erhält der Angreifer Zugang zum damit geknackten System.
Voraussetzung für diese Angriffsmethode ist, daß eine Authentifizierung in Netzwerken oft über Eintragung in den Rechnern als vertrauenswürdig erfolgt. Diese Identifikation der Rechner erfolgt über deren einzigartige Adresse im jeweiligen Netz. Haben zwei Rechner in einem Netz jeweils die Adresse des anderen als vertrauenswürdig eingetragen, so erfolgt die Authentifikation über das Senden dieser Adresse und der Vergleich mit dem Eintrag. Bei Übereinstimmung wird der Zugang freigegeben.
Als Beispiel soll das sog. **IP-Spoofing** dienen. Jeder mit dem Internet verbundene Rechner hat eine ihm zugewiesene, einzigartige sog. IP-Adresse[698]. Bei vielen Protokollen der TCP/IP-Familie[699] erfolgt die Authentisierung der kommunizierenden Sy-

---

696 Siehe dazu Seite 92 ff.

697 Eingehend dazu *Anonymous*, Hacker`s guide, S. 592 ff.

698 Siehe Fußnote auf Seite 166.

699 Siehe Fußnoten auf Seite 15 und Seite 166.

steme nur über die IP-Adresse, die aber leicht gefälscht werden kann.[700] Eine IP-Spoofing-Attacke erfolgt vereinfacht nach dem folgenden Schema: Der Hacker mit Rechner A sucht sich einen anzugreifenden Rechner B im Netz aus. Er hat vorher herausgefunden, daß zwischen Rechner B und einem Rechner C im Netz eine Vertrauensbeziehung besteht.[701] Nun muß der Hacker Rechner A als Rechner C bei dem Zielrechner B ausgeben. Damit Rechner C diesen Vorgang nicht stören kann, muß dieser für diese Zeit außer Gefecht gesetzt werden.[702] Eigentliches Problem dieser Angriffsform ist dann nach erfolgter Vorspiegelung der IP-Adresse des vertrauenswürdigen Rechners C, daß beim Kommunikationsaufbau bestimmte sog. Sequenznummern hin und her geschickt werden. Diese Nummern werden jedoch über bestimmte Algorithmen erzeugt, so daß nach Analyse vorher abgefangener Sequenznummern des Zielrechners B die für den konkreten Kommunikationsvorgang erforderliche Sequenznummer herausgefunden werden kann. Der Hacker, der über diese Methode in ein System eingebrochen ist, wird dann versuchen dieses in der Weise zu konfigurieren, daß er beim nächsten Zugang ohne Adress-Spoofing auskommt.

Adress-Spoofing in der Variante des IP-Spoofing kann heute recht einfach betrieben werden. Es kursieren frei im Internet abrufbare Programme, die das Spoofing erheblich erleichtern.[703]

Die anderen Varianten des Adress-Spoofing sind das sog. ARP-Spoofing und das DNS-Spoofing.[704] Die obigen Ausführungen sind vom theoretischen Ablauf auf diese Angriffsformen grs. übertragbar.

2. Strafrechtliche Bewertung

Das zumindest zeitweise Außergefechtsetzen des anderen Rechners ist nach der hier vertretenen Definition kein Computerhacken, da es nicht zu einem Eindringen in fremde Computersysteme oder Datenbereiche führt.

---

700 Zu der Angriffsform IP-Spoofing, siehe www.bsi.de/gshb/deutsch/g/g548.htm.

701 Die Authentifikation erfolgt damit nur über die IP-Adressen der Rechner.

702 Dies wird zumeist durch einen sog. Denial-of-Service-Attack (übersetzt: Dienstverweigerung) erreicht, bei dem der angegriffene Rechner über eine Unmenge von Anfragen und Zugangsversuchen dauerhaft beschäfigt wird. Dies kann sogar zu einem Absturz des gesamten Systems führen.

703 So z.B. ipspoof oder rbone. Das erste ist nach *Anonymous*, Hacker`s guide, S. 600, unter www.rootshell.com/archive-j457nxiqi3gq59dv/199707/ip.spoof.c erhältlich, das zweite unter www.net-security.sk/network/spoof/rbone.tar.gz.

704 Nähere Informationen dazu unter www.bsi.de/gshb/deutsch/g/g548.htm.

Dringt jemand in ein Computersystem mittels Adress-Spoofing ein, so könnte dies gem. § 202a strafbar sein. Problematisch ist jedoch, ob die Authentifikation zwischen zwei Netzrechnern über vertrauenswürdige Adressen als besondere Sicherung i.S.d. § 202a angesehen werden kann. Eine besondere Sicherung ist dann gegeben, wenn es für den Computerlaien nicht ohne weiteres möglich ist, die Einrichtung zu überwinden (Sicherungsgrad) und durch diese nicht lediglich in einem bloßen Nebeneffekt Daten gesichert werden (Sicherungszweck).

Da die Adressen eines Rechners im Netz einzigartig sind, sind die Adressen prinzipiell dazu geeignet, wie die vertraute, unverwechselbaren Stimme eines Anrufers per Telefon, diesen Rechner als vertrauenswürdig einzustufen. Eine Authentifikation i.S. einer eindeutigen Zuordnung des Einlaß Begehrenden ist damit möglich. Verglichen mit der Paßwortidentifikation kann die Adress-Authentifikation einerseits sicherer sein, da sie nicht durch menschliches Versagen im Falle der schlechten Auswahl des Paßworts angreifbar ist. Andererseits sind jedoch diese Adressen nicht geheim, so daß jeder grs. die Möglichkeit hat, mittels Adress-Spoofing unberechtigten Zugang zu erlangen. Dies erfordert jedoch erhebliches Spezialwissen, da das Spoofing eine recht komplizierte Angriffsart ist. Daher erfüllt der Sicherheitsgrad der Adress-Authentifikation die Anforderungen des Merkmals der besonderen Sicherung, da für den Computerlaien ein deutliches Hindernis gesetzt wurde. Der Sicherungszweck zielt hauptsächlich auf den Schutz der Daten und ist damit ebenfalls erfüllt.

Etwas anderes ergibt sich auch nicht daraus, daß Programme im Internet erhältlich sind, die solche Angriffe erleichtern. Wer solche Programme erfolgreich verwendet, der ist zum einen kein Computerlaie, zum anderen ist auch hier das Geheimhaltungsinteresse ausreichend dokumentiert, da ansonsten solche Hilfsprogramme auch nicht zur Anwendung kommen müßten. Die Adress-Authentifikation ist daher eine besondere Sicherung i.S.d. § 202a. Liegen die übrigen Tatbestandsvoraussetzungen vor, d.h. der Hacker beschränkt sich nicht lediglich auf das Eindringen, sondern verschafft sich darüber hinaus Daten, ist eine Strafbarkeit nach § 202a gegeben. Dies gilt auch, wenn man mit der h.M. eine Überwindung der Sicherung fordert, da hier konkret die Datensicherung über Adress-Authentifikation überwunden wird.

VI. Port-Scanner[705]

1. Arbeitsweise

Scanner sind Computerprogramme, die es einem Hacker ermöglichen, bei einem anvisierten Rechner in einem Netzwerk nach fehlerhaften Konfigurationen und Diensten zu suchen.[706] Sie senden Anfragen an den Zielrechner und zeichnen dessen Antwort auf. So werden aufschlußreiche Informationen zusammengetragen, die dann einen Einbruch vorbereiten und erleichtern können. Mit Scannern können folglich über das Internet von jedem Ort der Welt Sicherheitslücken an einem entfernten Server aufgedeckt werden.
Scanner werden oft auch von Sicherheitsadministratoren von Netzwerken zur Fehleranalyse eingesetzt. In den Händen eines Hackers stellen sie jedoch eine Bedrohung für die Sicherheit von Netzwerken dar. Prominentester Vertreter von Scanner-Programmen ist das 1995 vorgestellte sog. SATAN[707]. Neuester, weitverbreiteter Scanner ist Nessus, der seit 1998 kostenlos im Internet erhältlich ist.[708]

2. Strafrechtliche Bewertung

Das Austesten von Sicherheitslücken an Netzrechnern ist grs. nicht strafbar.[709] Die Anfragen an den mit dem Netz verbundenen entfernten Rechner lösen bei diesem für die Beantwortung solcher Fragen vorgesehene Programmroutinen aus. Jedem Zugriff auf Dienstprogramme (z.B. sendmail als E-Mail-Dienstprogramm eines Unix-Rechners) geht eine Anfrage u.a. über Verfügbarkeit oder Konfiguration voraus. Es werden dadurch keine Daten verändert, da die Anfrage lediglich eine Vermehrung der Daten und Entsendung der Antwortdaten auslöst. § 303a ist damit nicht einschlägig.

Die Anfragen erfolgen im Vorbeitungsstadium des eigentlichen Eindringens in den fremden Rechner. Wenn selbst das bloße Eindringen nicht nach § 202a Abs. 1strafbar

---

705 Zu Port siehe Fußnote auf Seite 166. Scanner heißt „Abtaster“.

706 Ausführlich in *Anonymous*, Hacker`s guide, S. 188 ff.

707 SATAN (Security Administrator´s Tool for Analyzing Networks).

708 Dokumentation zu finden unter www.nessus.org. Das Programm steht www.gnu.org zum download bereit.

709 Führen die Anfragen aufgrund ihrer Anzahl zu einer Blockade oder dem Absturz des anvisierten Rechners, könnte § 303b einschlägig sein.

ist, kann erst recht das diesen Eingriff vorbereitende Scannen nicht nach § 202a strafbar sein.[710]

VII. Packet-Sniffer[711]

Sniffer sind Rechner oder Programme, die Datenpakete in Netzwerken abfangen. Sie versetzen die Netzwerkschnittstelle des benutzten Rechners in einen bestimmten Modus[712], der dazu führt, daß alle oder bestimmte Datenpakete zur Weiterverarbeitung empfangen werden und erst nach Protokollierung und Auswertung an den eigentlichen Zielort weitergesendet werden. Hierbei können sie beispielsweise **Paßwörter** oder sonstige vertrauliche, womöglich auch wirtschaftlich wertvolle Daten abfangen und dem Hacker zur Verfügung stellen. Mit den erhaltenen Informationen über angrenzende Netzwerke, insbesondere Zugangsdaten, können Sniffer entscheidend dazu beitragen, daß der Angreifer Sicherheitsvorkehrungen überwindet oder umgeht und infolgedessen in das Netz eindringen kann.
Mit Sniffern können Daten verschiedenster Art abgefangen werden. Wird ein Paßwort abgefangen, so ist dies nach der hier vertretenen Ansicht straflos.[713] Das Abfangen von personenbezogenen Daten oder von Unternehmensgeheimnissen in Datenform wird aufgrund der oben angesprochenen Tatbestände relevant.[714]

---

710 Im Ergebnis auch *Jäger*, c`t 4/2000, 232 (233).

711 Packet (englisch) übersetzt: Datenpaket; Sniffer (englisch) übersetzt: Schnüffler

712 Sog. Promiscuous Mode.

713 Siehe Seite 156 ff.

714 Siehe zu personenbezogenen Daten Seite 152 ff.. Zu Unternehmensgeheimnissen in Datenform siehe Seite 145 ff.

Kapitel 4: Zusammenfassung

1. Computerhacken wird eingeteilt in die Fallgruppen:

- **Computerhacken i.e.S.** als das bloße Eindringen in Computersysteme und/oder Datenbereiche.
- **Computerhacken i.w.S.** als das Eindringen in Computersysteme und/oder Datenbereiche plus Vornahme weiterer Handlungen im System oder in Datenbereichen

2. Zu § 202a:

- **Rechtsgut** des § 202 ist das Verfügungsrecht über Daten in der Ausprägung eines Geheimhaltungsinteresses des Berechtigten.
- Der **Datumsbegriff** ist gleichzusetzen mit dem Begriff der Information. Tatobjekt sind Daten, das einzelne Datum ist von § 202a nicht geschützt. Eine Änderung des Wortlauts des § 202a ist daher angebracht.
- **Programme** sind Daten i.S.d. § 202a Abs. 2.
- **Datenbestimmung** ist gegeben, wenn der Verfügungsberechtigte die Kenntnisnahme der Daten einräumt. Dies ist eine tatbestandsausschließende Einwilligung (sog. Einverständnis).
- **Zugang** zu Daten ist jede technische und physikalische Einwirkungsmöglichkeit auf Datenspeicher und den physischen Zugang zum System und Sicherheitsbereich.
- Eine **besondere Sicherung** gegen Zugang ist gegeben, wenn eine Vorkehrung objektiv dazu geeignet ist, zumindest für den Computerlaien den gebräuchlichsten Weg zu den Daten zu verwehren (Sicherungsgrad) und der Schutz der Sicherung in Bezug auf die Daten nicht nur bloßer Nebeneffekt ist (Sicherungszweck).
- Das Merkmal „**unberechtigt**“ hat gegenüber der Datenbestimmung keine eigenständige Bedeutung. Sind die Daten für den Täter nicht bestimmt, so ist der Zugang zu den Daten für diesen „unberechtigt“.
- Eine **Überwindung der Sicherung** ist nicht zu fordern. Bei Schutz der Daten körperlicher Art ist der Zugang zu den Daten lediglich faktisch Überwindung dieser Sicherung. Bei allen anderen Schutzvorrichtungen kann immer nur der von diesen zu schützende Zugangsweg gesichert werden. Daher reicht hier eine funktionsfähige Sicherung aus, die den Computerlaien wirksam von den Daten fernhält. Ob die Sicherung, die dann als solche eindeutig den Geheimhaltungswillen des Berechtigten dokumentiert, überwunden oder umgangen wird, ist unerheblich.

- Die **Datenverschlüsselung** ist keine besondere Zugangssicherung, da die verschlüsselten Daten Angriffsobjekt sind. Das Tatobjekt, nämlich die Daten im Klartext, ist zum Zeitpunkt der Tat nicht vorhanden oder zugegen. Die verschlüsselten Daten sind im Übertragungszustand selbst zumeist nicht gesichert. Der Wortlaut des § 202a ist daher um die Datenverschüsselung zu ergänzen. Satz 1 unverändert. Satz 2: Ebenso wird bestraft, wer unbefugt verschlüsselte Daten, die nicht für ihn bestimmt sind, entschlüsselt, oder sich oder einem Dritten den Schlüssel verschafft.
- Die Tathandlung des „**Verschaffens**“ von Daten ist dann gegeben, wenn der Täter entweder von den Daten Kenntnis nimmt bzw. einem anderen die Kenntnis ermöglicht oder -ohne Kenntnisnahme- sich oder einem anderen in den Besitz des Datenträgers bringt bzw. die Daten in einem eigenen Datenspeicher ablegt.
- **Mehrfach gesicherte Daten** sind mit Überwindung oder Umgehung der letzten Sicherung hinter der Daten ungeschützt gespeichert sind „verschafft“, wenn im Fall des nicht-materialisierten Erlangens der Täter (oder ein Dritter) Kenntnis genommen hat oder im Falle des materialisierten Erlangens die geschützten Daten kopiert wurden oder der Datenträger selbst weggenommen wurde.
- Verschlüsselte Daten sind, folgt man der Ansicht die Datenverschlüsselung sei eine besondere Sicherung i.S.d. § 202a Abs. 1, dann verschafft, wenn die Daten **entschlüsselt** werden oder der Täter (oder ein Dritter) den Schlüssel zur Entschlüsselung innehat (**Entschlüsselbarkeit**). Sind verschlüsselte Daten selbst gesichert, ist keine Entschlüsselung oder Entschlüsselbarkeit zu fordern.

3. Computerhacken i.e.S.

- Das **Computerhacken i.e.S.** ist nicht strafbar. Der Tatbestand des § 202a Abs. 1 ist daher teleologisch zu reduzieren. Straflos ist die Kenntnisnahme der Daten, die direkt nach dem Eindringen ins geschützte System oder in einen geschützten Datenbereich automatisch der Wahrnehmung zugänglich sind. Jedes weitere Vorgehen nach dem Eindringen ist strafbar, da dann eine Kenntnisnahme von Daten im System erfolgt.
- Es wird eine Strafnorm de lege ferenda vorgeschlagen, die in Anlehnung an den Hausfriedensbruch (§ 123) das Eindringen in wichtige elektronische, bzw. virtuelle Aufenthaltsorte (insbesondere Internet-Marktplätze) unter Strafe stellt. Das Erfordernis der besonderen Sicherung ist entsprechend § 202a Abs. 1 einzufügen.

5. Computerhacken i.w.S.

- Das Computerhacken i.w.S. kann über den § 202a Abs. 1 hinaus insbesondere nach §§ 303a, 303b, § 17 UWG und § 43 BDSG strafbar sein.
- Paßwörter von Rechnersystemen von Betrieben, Unternehmen oder Behörden sind grs. als Unternehmensgeheimnisse i.S.d. § 17 UWG anzusehen.
- Werden diese Paßwörter herausgefunden, so ist § 17 UWG dennoch nicht einschlägig. Im Hinblick auf § 202a soll das Computerhacken i.e.S. entgegen dem Willen des Gesetzgebers nicht durch § 17 UWG wieder in weiten Bereichen unter Strafe gestellt werden.

6. Fallgruppen des Computerhackens:

- Das Herausfinden eines **Paßwort**es ist nicht strafbar.
- Das **Datenreisen** (Eindringen in ein System von einem zuvor schon „gehackten" System aus) ist strafbar nach § 202a Abs. 1, da man sich dabei zwangsläufig nicht mit dem bloßen Eindringen in das erste System begnügt.
- Die Installation von **Trojanischen Pferden** ist straflos.
- Das Eindringen und Umsehen in geschützten Systemen über die Ausnutzung von **Wanzen** (Programmierfehlern) oder **Falltüren** erfüllt § 202a, obwohl die eigentliche Sicherung (z.B. Paßwortsicherung) nicht überwunden wird.
- Das sog. **Adress-Spoofing** überwindet die Sicherung von vernetzten Rechnern durch Adressen-Authentifikation und ist damit bei zusätzlichem Datenverschaffen strafbar gem. § 202a Abs. 1.
- Das Verwenden von sog. **Port-Scannern** in Netzen ist straflos.
- Bei sog. **Packet-Sniffern** ist das bloße Herausfinden eines Paßworts straflos. Werden Daten im Klartext abgefangen, so ist eine Strafbarkeit nur nach § 43 BDSG bei personenbezogenen Daten und nach § 17 UWG bei Unternehmensgeheimnissen denkbar.

Literaturverzeichnis

Achenbach, Hans	Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität, NJW 1986, 1835 ff.
Ackermann, Stephan	Die aktuellen Tarife fürs Hacken, in: Das Chaos-Computer-Buch, hacking made in Germany, Chaos Computer Club, Wiekmann, Jürgen (Hrsg.), Reinbek bei Hamburg 1988
Amelung, Knut	Rechtsgüterschutz und Schutz der Gesellschaft, Frankfurt am Main 1972
Anonymous	Hacker`s guide - Sicherheit im Internet und im lokalen Netz, Haar bei München 1999
Bauer, Jürgen/ Stürner, Rolf	Sachenrecht, 17. Auflg., München 1999
Bauerfeld, Wulf-Dieter	Hier wird gehackt, JurPC 1989, 210 ff.
Baumann Jürgen/ Weber, Ulrich/ Mitsch, Wolfgang	Strafrecht Allgemeiner Teil, 10. Auflg., Bielefeld 1995
Baumbach, Adolf/ Hefermehl, Wolfgang	Wettbewerbsrecht, 21. Auflg., München 1999
Bender, Bernd	Zur Methode der Rechtsfindung bei der Auslegung und Fortbildung gesetzten Rechts, JZ 1957, 593 ff.
Binder , Jörg	Computerkriminalität und Datenfernübertragung - Teil 1, RDV 1995, 57 ff.
ders.	Strafbarkeit intelligenten Ausspähens von programmrelevanten DV- Informationen, Dissertation, Marburg 1994
Blei, Herrmann	Strafrecht Allgemeiner Teil, 18. Auflg., München 1983
Bockelmann, Paul/ Volk, Klaus	Strafrecht Allgemeiner Teil, 4. Auflg., München 1987

Bormann Friedrich W./ Bormann, Michael	Rechtsnatur und Rechtsschutz der Software, DB 91, 2641 ff.
Boutellier, Roger	Das Hacker-Hack-Buch, Moers 1985
Bühler, Christoph	Ein Versuch, Computerkriminellen das Handwerk zu legen: Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität, MDR 1987, 448 ff.
Dammann, Ulrich	Erste Erfahrungen mit dem Bundesdatenschutzgesetz, NJW 1978, 1906 ff.
Dannecker, Gerhard	Neuere Entwicklungen im Bereich der Computerkriminalität: Aktuelle Erscheinungsformen und Anforderungen an eine effektive Bekämpfung, BB 1996, 1285 ff.
Dierstein, Rüdiger	Von Viren, trojanischen Pferden und logischen Bomben, NJW-CoR 4/1990, 8 ff.
Dölling, Dieter	Diebstahl in einem besonders schweren Fall bei Ausschaltung einer Alarmanlage in einem Kaufhaus? - (OLG Stuttgart, NStZ 1985, 76), JuS 1986, 691 ff.
Duden	Das große Wörterbuch der deutschen Sprache, Band 10, 3. Auflg., Mannheim Leipzig Wien Zürich 1999
Dworatschek, Sebastian/ Büllesbach, Alfred/ Koch, Hans-Dietrich	Personalcomputer und Datenschutz, 5. Auflg., Köln 1993
Engel, Friedrich-Wilhelm	Mängelansprüche bei Software-Verträgen, BB 1985, 1159 ff.
Engelhard, Hans A.	Computerkriminalität und deren Bekämpfung durch strafrechtliche Reformen, DVR 1985, 165 ff.
Erbs, Georg/ Kohlhaas, Max	Strafrechtliche Nebengesetze, Band 1, 4, 136. Ergänzungslieferung, Stand: März 2000, München 2000, (zit.: Erbs/Kohlhaas-*Bearbeiter*)

Etter, Eberhard	Anmerkung zu OLG Celle CR 1990, 276 f., CR 1990, 277
Frommel, Monika	Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität, JuS 1987, 667 ff.
Geerds, Friedrich	Einwilligung und Einverständnis des Verletzten im Strafrecht, GA 1954, 262 ff.
Gola, Peter	Zur Entwicklung des Datenschutzrechts im Jahre 1986, NJW 1987, 1675 ff.
Goldmann, Günter/ Stenger, Hans-Jürgen	Unbefugtes Eindringen in Computersysteme - eine Betrachtung aus polizeilicher Sicht, CR 1989, 543 ff.
Gössel, Karl-Heinz	Strafrecht Besonderer Teil, Band 1, Heidelberg 1987
ders.	Das Rechtsgut als ungeschriebenes Tatbestandsmerkmal - zugleich ein Versuch über das Verhältnis von Rechtsgut, Tatbestand und Norm, in: Festschrift für Dietrich Oehler zum 70. Geburtstag, Herzberg, Rolf (Hrsg.) S. 97ff. , Köln 1985
Granderath, Peter	Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität, DB 1986 Beilage Nr. 18, S. 1 ff.
Gravenreuth, von	Computerviren, Hacker, Datenspione, Crasher und Cracker - Überblick und rechtliche Einordnung, NStZ 1989, 201 ff.
Grieser, Franz/ Irlbeck, Thomas	Computerlexikon, München 1995
Großkommentar zum UWG	§§ 16 -21, 3. Lieferung, Berlin New York 1991, (zit.: GK-*Bearbeiter*)
Grünhut, Max	Methodische Grundlagen der heutigen Strafrechtswissenschaft, in: Festgabe für Reinhard Frank zum 70. Geburtstag, Band 1, Neudruck der Ausgabe Tübingen 1930, Aalen 1969

Hafner, Katie/ Markoff, John	Cyberpunk, Düsseldorf Wien 1993
Haft, Fritjof	Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität (2. WiKG), NStZ 1987, 6 ff.
Haß, Gerhard	Der strafrechtliche Schutz von Computerprogrammen, in Lehmann Michael (Hrsg.), Rechtsschutz und Verwertung von Computerprogrammen, 2. Auflg., Köln 1993
Hauptmann, Peter-Helge	Zur Strafbarkeit des sog. Computerhackens - die Problematik des Tatbestandsmerkmals „Verschaffen“ in § 202a StGB, JurPC, 1989, 215 ff.
Haurand, Günter/ Vahle, Jürgen	Computerkriminalität, RDV 1990, 128 ff.
Heine, Werner	Die Hacker - von der Lust in fremden Netzen zu wildern, Reinbek bei Hamburg 1985
Herb, Armin	Verweisungsfehler im Datenschutzstrafrecht, Braunschweig Wiesbaden 1986
Hilgendorf, Eric	Grundfälle zum Computerstrafrecht, JuS 1996, 509 ff., JuS 1996, 890 ff., JuS 1997, 323 ff.
ders.	Anmerkung zu BayObLG, JR 1994, 476 ff., in JR 1994, 478 ff.
ders.	Entscheidungsbesprechung zu OLG Düsseldorf, NStZ-RR 1998, 137, in JuS 1999, 542 ff.
Hillenkamp, Thomas	Vorsatztat und Opferverhalten, Göttingen 1985
Jaeger, Stefan	Risiken und Nebenwirkungen - Rechtsunsicherheit bei Trojaner-Angriffen, c`t 9/1999, 174 ff.
ders.	Gesetze und Lücken - Rechtliche Schritte gegen Angriffe im Netz, c`t 4/2000, 232 ff.
Jakobs, Günther	Strafrecht Allgemeiner Teil, 2. Auflg., Berlin New York 1991
Jescheck, Hans-Heinrich/ Weigend, Thomas	Lehrbuch des Strafrechts, Allgemeiner Teil, 5. Auflg., Berlin 1996

Jessen, Ernst	Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, Dissertation, Frankfurt a.M. 1993
Junker, Abbo	Entwicklung des Computerrechts in den Jahren 1991 und 1992, NJW 93, 824 ff.
Kaufmann, Armin	Die Aufgabe des Strafrechts, Opladen 1983
Kersten, Heinrich	Sicherheit in der Informationstechnik, München Wien 1995
Koch, Frank	Aspekte des technischen und strafrechtlichen Zugriffsschutzes von EDV-Systemen, RDV 1996, 123 ff.
König, Michael	Software (Computerprogramme) als Sache und deren Erwerb als Sachkauf, NJW 1993, 3121 ff.
Kühl, Kristian	Strafrecht Allgemeiner Teil, 2. Auflg., 1997
Kuhn, Matthias	Rechtshandlungen mittels EDV und Telekommunikation, München 1991
Kuner, Christopher	Digitale Unterschriften im Internet-Zahlungsverkehr: Rechtliches in Deutschland und USA, NJW-CoR 1996, 108 ff.
Kunz, Karl-Ludwig	Kriminologie, 2. Auflg., Bern Stuttgart Wien 1998
Küper, Wilfried	Strafrecht Besonderer Teil - Definitionen mit Erläuterungen, 3. Auflg., Heidelberg 1999
Kyas, Othmar	Sicherheit im Internet, Bergheim 1996
Lackner, Karl/ Kühl, Kristian	Strafgesetzbuch mit Erläuterungen, 23. Auflg., München 1999, (zit.: Lackner/Kühl-*Bearbeiter*)
Larenz, Karl/ Wolf, Manfred	Allgemeiner Teil des Bürgerlichen Rechts, 8. Auflg., München 1997
Leicht , Armin	Computerspionage - Die „besondere Sicherung gegen unberechtigten Zugang“ (§ 202a StGB), iur 1987, 45 ff.

Leipziger Kommentar	Strafgesetzbuch, Band 5 (§§ 185 bis 262), 10. Auflg., Berlin New York 1989 §§ 302-311c in der 11. Auflg., Berlin New York 1993, (zit.: LK-*Bearbeiter*)
Lenckner, Theodor	Computerkriminalität und Vermögensdelikte, Heidelberg Karlsruhe 1981
Lenckner, Theodor/ Winckelbauer, Wolfgang	Computerkriminalität - Möglichkeiten und Grenzen des 2. WiKG (II), CR 1986, 483 ff.
dies.	Computerkriminalität - Möglichkeiten und Grenzen des 2. WiKG (I), CR 1986, 825 ff.
Levy, Steven	Hackers - Heroes of the Computer Revolution, Double Day and Company 1984
Liebl, Karlhans/ Grosch, Olaf	Datendiebstahl als Form der Computerkriminalität, CR 1985, 162 ff.
Liszt von, Franz	Lehrbuch des deutschen Strafrechts, Berlin 1921
Luckardt, Norbert	Windows für Einsteiger - der Weg zum sicheren PC, c`t 2000, Heft 4, 208 ff.
Maurach, Reinhart/ Zipf, Heinz	Strafrecht Allgemeiner Teil, Teilband 1, 7. Auflg., Heidelberg 1987
Meinhardt, Lars	Überlegungen zur Interpretation von § 303a StGB, Dissertation, Pfaffenweiler 1991
Meurer, Dieter	Die Bekämpfung der Computerkriminalität in Deutschland, in: Festschrift für Zentaro Kitagawa zum 60. Geburtstag, Berlin 1992
Möhrenschlager, Manfred	Der Regierungsentwurf eines 2. WiKG, wistra 1982, 201 ff.
ders.	Das neue Computerstrafrecht, wistra 1986, 128 ff.
Mühle, Kerstin	Hacker und Computerviren im Internet - eine strafrechtliche Beurteilung, Dissertation, Passau 1998

Müller, Wulf	Aktuelle Probleme des § 263a StGB, Dissertation, Frankfurt am Main Berlin Bern NewYork Paris Wien 1999
Müller-Berg, Michael	Sicherheitsmaßnahmen und rechtliche Anforderungen im Rahmen des elektronischen Datenaustauschs, DuD 1993, 87 ff.
Nomos Kommentar	Kommentar zum Strafgesetzbuch , Baden-Baden 1995, (zit.: NK-*Bearbeiter*)
o.V.	Interview mit Pressesprecher des CCC (Chaos Computer Club), internetworld, 9/1998, 40 ff.
o.V.	Lauscher im Datenreich, Spiegel 36/1996 S. 194 ff.
o.V.	„recht“, Informationen des BMJ 1985, 56
o.V.	Alarmplan nach Hackerangriff, Südkurier, 09.03.2000, S. 25
o.V.	Zeitenwende im Internet, Südkurier, 10.03.2000, S. 3
Oppliger, Rolf	Computersicherheit: Eine Einführung, Braunschweig Wiesbaden 1992
Ordemann, Hans-Joachim/ Schomerus, Rudolf/ Gola, Peter	Kommentar zum Bundesdatenschutzgesetz, 5. Auflg., München 1992
Otto, Harro	Verrat von Betriebs- und Geschäftsgeheimnissen, wistra 1988, 125 ff.
ders.	Grundkurs Strafrecht, 5. Auflg., Berlin New York 1998
Palandt, Otto	Bürgerliches Gesetzbuch, 59. Auflg., München 2000, (zit.: Palandt-*Bearbeiter*)
Paul, Werner	NJW-CoR-Hackerreport: Aus dem Wörterbuch des Onliners, NJW-CoR 1/1996, 62
Pohl, Hartmut/ Weck, Gerhard	Stand und Zukunft der Informationssicherheit, DuD 1993, 18 ff.

Redeker, Helmut	Wer ist Eigentümer von Goethes Werther, NJW 1992, 1739 ff.
Rengier, Rudolf	Strafrecht Besonderer Teil 1, 3. Auflg., München 1999
Richter, Hans	Anmerkung CR 1989, 303 ff. zu AG Böblingen CR 1989, 257
Roßnagel, Alexander	Das Signaturgesetz nach zwei Jahren, NJW 1999, 1591 ff.
Roxin, Claus	Strafrecht Allgemeiner Teil, Band 1, 3. Auflg., München 1997
Rupp, Wolfgang	Strafrechtlicher Schutz von Computersoft- und Orgware nach §§ 17 ff. UWG unter Berücksichtigung der Reformentwürfe zum UWG, WRP 1985, 676 ff.
Schaffland, Hans-Jürgen/ Wiltfang, Noeme	Bundesdatenschutzgesetz (BDSG), Stand: Januar 2000, Berlin 1977
Schlüchter, Ellen	Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität, Heidelberg 1987
Schmitz, Roland	Ausspähen von Daten, § 202a StGB, JA 1995, 478 ff.
Schönke, Adolf/ Schröder, Horst	Strafgesetzbuch - Kommentar, 25. Auflg., München 1997, (zit.: Schönke/Schröder-*Bearbeiter*)
Schönleber, Claus	Verschlüsselungsverfahren, Poing 1995
Schrutzki, Reinhard	Die Hacker-Ethik, in Wieckmann, Das Chaos Computer Buch, S. 168 f., Reinbek bei Hamburg 1988
Schulze-Heiming, Ingeborg	Der strafrechtliche Schutz der Computerdaten gegen die Angriffsformen der Spionage, Sabotage und des Zeitdiebstahls, Dissertation, Münster New York 1995

Seier, Jürgen	Der Schutz vor Ladendiebstahl durch Sicherungsetiketten JA 1985, 387 ff., zugleich Anmerkung zu OLG Stuttgart NStZ 1985, 76
Sieber, Ulrich	Informationstechnologie und Strafrechtsreform, Köln Bonn Berlin München 1985
ders.	Computerkriminalität und Informationsstrafrecht in der internationalen Informations- und Risikogesellschaft, in: Neue Strafrechtsentwicklungen im deutsch-japanischen Vergleich, Hrsg.: Kühne/Myazawa, ius criminale, 1995, Band 2, S. 33 ff.
ders.	Computerkriminalität und Strafrecht, 2. Auflg., Köln Berlin Bonn München 1980
Simitis, Spiros/ Dammann, Ulrich/ Geiger, Hansjörg/ Mallmann, Otto/ Walz, Stefan	Kommentar zum Bundesdatenschutzgesetz, 4. Auflg, 30. Lieferung Mai 1999, Baden-Baden 1992, (zit.: Simitis/ Dammann/Geiger/Mallmann/Walz-Bearbeiter)
Stoll, Clifford	Kuckucksei, die Jagd nach den deutschen Hackern, die das Pentagon knackten, Frankfurt am Main 1989
Suhr, Christian	Zur Begriffsbestimmung von Rechtsgut und Tatobjekt im Strafrecht, JA 1990, 303 ff.
Systematischer Kommentar	Band I, Allgemeiner Teil (§§ 1 bis 79 b) Band II, Besonderer Teil (§§ 80-358), 5. bzw. 6. Auflg, Stand: 49. Lieferung (Oktober 1999), (zit.: SK-*Bearbeiter*)
Tai, Thomas	Cracker, Hacker, Datensammler - Softwarepiraten unter der Lupe, Heidelberg 1986
Tiedemann, Klaus	Die Bekämpfung der Wirtschaftskriminalität durch den Gesetzgeber, JZ 1986, 865 ff.
ders.	Computerkriminalität und Mißbrauch von Bankomaten, WM 1983, 1326 ff.

ders.	Datenübermittlung als Straftatbestand, NJW 1981, 945 ff.
Tröndle, Herbert/ Fischer Thomas	Strafgesetzbuch, 49.Auflg., München 1999, (zit.: Tröndle/Fischer-*Bearbeiter*)
Volesky, Karl-Heinz	Strafbarkeit und Strafwürdigkeit nach englischem Recht, CR 1991, 553 ff.
Volesky, Karl-Heinz/ Schulten, Hansjörg	Computersabotage - Sabotageprogramme, Computerviren - Rechtliche Probleme des § 303b StGB, iur 1987, 280 ff.
Weber, Ahrend	Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität WM 1986, 1133 ff.
Weck, Gerhard	Datensicherheit: Methoden, Maßnahmen und Auswirkungen, Stuttgart 1984
Welp, Jürgen	Datenveränderung (§ 303a StGB) - Teil 1, iur, 1988, 443 ff.
Wessels, Johannes/ Beulke, Werner	Strafrecht Allgemeiner Teil, 29. Auflg., Heidelberg 1999
Wessels, Johannes/ Hillenkamp, Thomas	Strafrecht Besonderer Teil/2, 21. Auflg., 1999
Zielinski, Diethart	Der strafrechtliche Schutz von Computersoftware, in: Kilian, Wolfgang/ Gorny, Peter (Hrsg.), Schutz von Computersoftware - Technische und rechtliche Aspekte, S. 115 ff., Darmstadt 1987