Convention on Cybercrime (ETS 185)

Ein Vergleich mit dem deutschen Computerstrafrecht in materiell- und verfahrensrechtlicher Hinsicht

Dissertation
zur Erlangung des Doktorgrades
der Juristischen Fakultät
der Universität Regensburg

vorgelegt von
Christian Spannbrucker

Erstberichterstatter:	Prof. Dr. Henning Ernst Müller
Zweitberichterstatter:	Prof. Dr. Bernd von Heintschel-Heinegg
Tag der mündlichen Prüfung:	29.11.2004

Die vorliegende Dissertation lag der juristischen Fakultät der Universität Regensburg im Sommersemester 2004 vor. Literatur, Rechtsprechung und Gesetzeslage konnten bis Mitte 2004 berücksichtigt werden.

Meinem Doktorvater, Herrn Prof. Dr. Henning Ernst Müller, möchte ich für seine tatkräftige Unterstützung besonders danken. Darüber hinaus danke ich Herrn Prof. Dr. Bernd von Heintschel-Heinegg für die schnelle Erstellung des Zweitgutachtens.

Mein persönlicher Dank gebührt meinen Eltern, Frau Ute Küspert, Herrn RA Adnan Sen sowie Herrn Horst Schatz, deren vielseitige Unterstützung zum Gelingen dieser Arbeit beitragen hat.

Inhaltsverzeichnis

INHALTSVERZEICHNIS V

ABKÜRZUNGSVERZEICHNIS XI

1 EINLEITUNG 1

1.1 EINE NEUE BEDROHUNG? 1
1.2 FUNKTIONEN UND AUFGABEN DES EUROPARATS 2
1.3 ENTSTEHUNG DER KONVENTION 3
1.4 DER RECHTSCHARAKTER DER KONVENTION 5
1.5 ÜBERBLICK ÜBER DIE KONVENTION UND DEN GANG DER DARSTELLUNG 6
1.6 „CYBERCRIME“ UND COMPUTERKRIMINALITÄT 8
1.7 PHÄNOMENOLOGIE DER NETZWERKKRIMINALITÄT 11
1.7.1 Vertraulichkeitsverletzungen 11
1.7.1.1 „Hacking“ 12
1.7.1.1.1 Ausnutzen menschlicher Schwächen 13
1.7.1.1.2 Sicherheitslücken im Betriebssystem 13
1.7.1.1.3 Gefahren von Außen 14
1.7.1.1.4 Schwachstellen in den Netzwerkprotokollen 15
1.7.1.2 Cookies 19
1.7.1.3 Echelon 19
1.7.2 Integritätsverletzungen 20
1.7.2.1 Viren, Würmer, Hoaxes und Trojaner 20
1.7.2.2 0190-Dialer 22
1.7.3 Beeinträchtigungen der Verfügbarkeit 22
1.7.4 Rechtswidrige Inhalte 24
1.7.4.1 „Filesharing“ und Urheberrechte 24
1.7.4.2 Extremistische, rassistische und pornografische Inhalte 26
1.8 STATISTIK 27

2 BEGRIFFSBESTIMMUNGEN 31

2.1 ARTIKEL 1 LIT. A) – COMPUTERSYSTEM 31
2.1.1 Datenverarbeitungsanlage im StGB 33
2.1.2 Vergleich 33
2.2 ARTIKEL 1 LIT. B) – COMPUTERDATEN 34
2.2.1 Datenbegriff des StGB 34
2.2.2 Vergleich 37
2.3 ARTIKEL 1 LIT. C) – DIENSTANBIETER 38
2.3.1 Dienstanbieter im deutschen Strafrecht 38
2.3.1.1 §§ 100a f. und §§ 100g f. StPO 39
2.3.1.2 §§ 3 Nr. 1 TDG und 3 Nr. 1 MDStV 40
2.3.2 Vergleich 42
2.4 ARTIKEL 1 LIT. D) – VERBINDUNGSDATEN 43
2.4.1 Verbindungsdaten nach § 100g Abs. 3 StPO und § 206 Abs. 5 Satz 2 2. Halbsatz StGB 43
2.4.2 Vergleich 45

3 MATERIELLES STRAFRECHT 47

3.1 ARTIKEL 2 – RECHTSWIDRIGER ZUGRIFF 47
3.1.1 Anwendungsbereich 47
3.1.2 Tatbestand 48
3.1.3 Vorsatz 49
3.1.4 Unbefugt 49
3.1.5 Art. 2 Satz 2 – Einschränkungen im Anwendungsbereich 50
3.1.6 Vergleichbare Tatbestände im deutschen Strafrecht 51
3.1.6.1 § 202a StGB – Ausspähen von Daten 51
3.1.6.1.1 Rechtsgut 51
3.1.6.1.2 Tathandlung 52
3.1.6.1.3 Ergebnis zu § 202a StGB 53

3.1.6.2 § 17 Abs. 2 Nr. 1 UWG (Betriebsspionage) ... 54
3.1.6.2.1 Rechtsgut und Tatbestand ... 54
3.1.6.2.2 Ergebnis zu § 17 Abs. 2 Nr. 1 UWG ... 55
3.1.7 Bewertung Art. 2 ... 55
3.2 ARTIKEL 3 – RECHTSWIDRIGES ABFANGEN ... 57
3.2.1 Anwendungsbereich ... 57
3.2.2 Tatbestand ... 57
3.2.3 Unbefugt ... 58
3.2.4 Art. 3 Satz 2 – Einschränkungen ... 59
3.2.5 Vergleichbare Tatbestände im deutschen Strafrecht ... 59
3.2.5.1 § 202a StGB – Ausspähen von Daten ... 59
3.2.5.1.1 Datenbestimmung ... 60
3.2.5.1.2 Die Datensicherung ... 61
3.2.5.1.3 Ergebnis zu § 202a StGB ... 64
3.2.5.2 § 17 Abs. 2 Nr. 1 lit. a) UWG (Betriebsspionage) ... 65
3.2.5.2.1 Tatbestand ... 65
3.2.5.2.2 Ergebnis zu § 17 Abs. 2 Nr. 1 UWG ... 65
3.2.5.3 § 206 StGB – Verletzung des Post- oder Fernmeldegeheimnisses ... 66
3.2.6 Bewertung Art. 3 ... 66
3.3 ARTIKEL 4 – EINGRIFFE IN DATEN ... 67
3.3.1 Anwendungsbereich ... 67
3.3.2 Tatbestand ... 67
3.3.3 Unbefugt ... 67
3.3.4 Art. 4 Abs. 2 – Vorbehalt ... 68
3.3.5 Vergleichbare Tatbestände im deutschen Strafrecht ... 68
3.3.5.1 § 303a StGB – Datenveränderung ... 68
3.3.5.1.1 Tatbestand ... 69
3.3.5.1.2 Rechtswidrigkeit ... 70
3.3.5.1.3 Ergebnis zu § 303a StGB ... 72
3.3.5.2 § 303 StGB – Sachbeschädigung am Datenträger bzw. Löschen eines Programms ... 72
3.3.6 Bewertung Art. 4 ... 72
3.4 ARTIKEL 5 – EINGRIFFE IN DAS SYSTEM ... 73
3.4.1 Anwendungsbereich ... 73
3.4.2 Tatbestand ... 73
3.4.3 Unbefugt ... 74
3.4.4 Vergleichbare Tatbestände im deutschen Strafrecht ... 74
3.4.4.1 § 303b StGB – Computersabotage ... 74
3.4.4.2 Tatbestand ... 74
3.4.4.3 Ergebnis zu § 303b StGB ... 76
3.4.5 Bewertung Art. 5 ... 77
3.5 ARTIKEL 6 – MISSBRAUCH VON VORRICHTUNGEN ... 79
3.5.1 Anwendungsbereich ... 79
3.5.2 Tatbestand ... 80
3.5.3 Art. 6 Abs. 2, Abs.3 – Einschränkung und Vorbehalt ... 81
3.5.4 Vergleichbare Tatbestände im deutschen Strafrecht ... 81
3.5.4.1 § 4 ZKDSG ... 81
3.5.4.2 Tatbestand ... 81
3.5.4.3 Ergebnis § 4 ZKDSG ... 82
3.5.5 Bewertung Art. 6 ... 82
3.6 ARTIKEL 7 – COMPUTERURKUNDENFÄLSCHUNG ... 85
3.6.1 Anwendungsbereich ... 85
3.6.2 Tatbestand ... 85
3.6.3 Unbefugt ... 86
3.6.4 Einschränkung nach Satz 2 ... 86
3.6.5 Vergleichbare Tatbestände im deutschen Strafrecht ... 86
3.6.5.1 § 267 StGB – Urkundenfälschung ... 86
3.6.5.1.1 Tatbestand ... 86
3.6.5.1.2 Ergebnis zu § 267 StGB ... 87
3.6.5.2 § 268 StGB – Fälschung technischer Aufzeichnungen ... 88
3.6.5.2.1 Tatbestand ... 88
3.6.5.2.2 Ergebnis zu § 268 StGB ... 90
3.6.5.3 § 269 StGB – Fälschung beweiserheblicher Daten ... 91
3.6.5.3.1 Tatbestand ... 91
3.6.5.3.2 Tathandlung ... 93
3.6.5.3.3 Ergebnis zu § 269 StGB ... 93

3.6.5.4 § 270 StGB – Täuschung im Rechtsverkehr bei Datenverarbeitung ... 94
3.6.6 Bewertung Art. 7 ... 94
3.7 ARTIKEL 8 – COMPUTERBETRUG ... 95
3.7.1 Anwendungsbereich ... 95
3.7.2 Tatbestand ... 95
3.7.3 Vergleichbare Tatbestände im deutschen Strafrecht ... 96
3.7.3.1 § 263a StGB – Computerbetrug ... 96
3.7.3.2 Taterfolg ... 96
3.7.3.3 Tathandlung ... 97
3.7.3.4 Subjektiver Tatbestand ... 99
3.7.3.5 Ergebnis zu § 263a StGB ... 99
3.7.4 Bewertung Art. 8 ... 99
3.8 ARTIKEL 9 – STRAFTATEN IN BEZUG AUF KINDERPORNOGRAFIE ... 101
3.8.1 Anwendungsbereich ... 101
3.8.2 Tatbestand ... 102
3.8.3 Tathandlungen ... 102
3.8.4 Unbefugt ... 103
3.8.5 Subjektiver Tatbestand ... 103
3.8.6 Abs. 4 – Vorbehalt ... 103
3.8.7 Vergleichbare Tatbestände im deutschen Strafrecht ... 104
3.8.7.1 § 184b StGB n.F. – Verbreitung, Erwerb und Besitz kinderpornografischer Schriften ... 104
3.8.7.1.1 Tatbestand ... 105
3.8.7.1.2 Tathandlungen ... 108
3.8.7.1.3 Vorsatz ... 109
3.8.7.1.4 Ergebnis zu § 184b n.F. StGB ... 109
3.8.7.2 § 184c StGB n.F. – Verbreitung pornografischer Darbietungen durch Rundfunk, Medien- oder Teledienste ... 109
3.8.7.3 Strafnormen im Jugendschutzrecht ... 110
3.8.7.3.1 § 23 Jugendmedienschutz-Staatsvertrag ... 111
3.8.7.3.2 Ergebnis zu § 23 JMStV ... 112
3.8.8 Bewertung Art. 9 ... 112
3.9 ARTIKEL 10 – STRAFTATEN IN ZUSAMMENHANG MIT VERLETZUNGEN DES URHEBERRECHTS UND VERWANDTER SCHUTZRECHTE ... 113
3.9.1 Anwendungsbereich ... 113
3.9.2 Tatbestand ... 114
3.9.2.1 Art. 10 Abs. 1 – Urheberrecht ... 114
3.9.2.1.1 RBÜ ... 114
3.9.2.1.2 TRIPs ... 115
3.9.2.1.3 WCT ... 116
3.9.2.2 Art. 10 Abs. 2 – Verwandte Leistungsschutzrechte ... 116
3.9.2.2.1 RA ... 117
3.9.2.2.2 WPPT ... 117
3.9.3 Subjektiver Tatbestand ... 118
3.9.4 Rechtswidrigkeit ... 118
3.9.5 Art. 10 Abs. 3 – Vorbehalt ... 118
3.9.6 Vergleichbare Tatbestände im deutschen Strafrecht ... 118
3.9.6.1 §§ 106, 108a UrhG – Unerlaubte Verwertung urheberrechtlich geschützter Werke ... 118
3.9.6.1.1 Tatbestand ... 119
3.9.6.1.2 Tathandlungen ... 120
3.9.6.1.3 Schranken ... 122
3.9.6.1.4 Ohne Einwilligung des Berechtigten ... 122
3.9.6.1.5 § 108a UrhG – Gewerbsmäßigkeit ... 122
3.9.6.1.6 Ergebnis zu §§ 106, 108a UrhG ... 123
3.9.6.2 §§ 108, 108a UrhG – Unerlaubte Eingriffe in verwandte Schutzrechte ... 123
3.9.6.2.1 Tatbestand ... 123
3.9.6.2.2 Schranken ... 124
3.9.6.2.3 Ohne Einwilligung des Berechtigten ... 124
3.9.6.2.4 § 108a UrhG – Gewerbsmäßigkeit ... 125
3.9.6.2.5 Ergebnis zu §§ 108, 108a UrhG ... 125
3.9.6.3 § 108b – Unerlaubte Eingriffe in technische Schutzmaßnahmen und zur Rechtewahrnehmung erforderliche Informationen ... 125
3.9.7 Bewertung Art. 10 ... 125
3.10 ARTIKEL 11 – VERSUCH UND BETEILIGUNG ... 127
3.10.1 Anwendungsbereich ... 127
3.10.2 Abs.1 – Beteiligung ... 127

3.10.3 Abs. 2, 3 – Versuch *127*
3.10.4 Teilnahme und Versuch im deutschen Strafrecht *128*
3.11 ARTIKEL 12 – VERANTWORTLICHKEIT JURISTISCHER PERSONEN 129
3.11.1 Anwendungsbereich *129*
3.11.2 Tatbestand *130*
3.11.3 Vergleichbare Normen im deutschen Strafrecht *130*
3.11.3.1 Geldbuße gegen juristische Personen und Personenvereinigungen – § 30 OWiG 131
3.11.3.1.1 Tatbestand 131
3.11.3.1.2 Ergebnis zu § 30 OWiG 132
3.11.3.2 Verletzung der Aufsichtspflicht in Betrieben und Unternehmen – § 130 OWiG 132
3.11.3.2.1 Tatbestand 133
3.11.3.2.2 Ergebnis zu § 130 OWiG 134
3.11.4 Bewertung Art. 12 ..... *134*
3.12 ARTIKEL 13 – SANKTIONEN UND MAßNAHMEN 135
3.12.1 Anwendungsbereich *135*
3.12.2 Rechtsfolgen der Tat im deutschen Strafrecht *135*

4 VERFAHRENSRECHT 137

4.1 ARTIKEL 14 – GELTUNGSBEREICH VERFAHRENSRECHTLICHER BESTIMMUNGEN 137
4.1.1 Anwendungsbereich *138*
4.1.2 Einschränkungen *138*
4.1.3 Vergleichbare Befugnisnormen im deutschen Strafverfahrensrecht *139*
4.1.4 Bewertung Art. 14 ..... *140*
4.2 ARTIKEL 15 – BEDINGUNGEN UND GARANTIEN 141
4.2.1 Anwendungsbereich *141*
4.2.2 Schutzmechanismen *141*
4.2.3 „Bedingungen und Garantien" im Grundgesetz *142*
4.2.3.1 Schutz der Privatsphäre 143
4.2.3.1.1 Art. 10 Abs. 1 GG – Fernmeldegeheimnis 143
4.2.3.1.2 Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG – Recht auf informationelle Selbstbestimmung 145
4.2.3.2 Art. 5 Abs. 1 Satz 1 GG – Meinungs- und Informationsfreiheit 145
4.2.3.3 Verhältnismäßigkeitsgrundsatz (Übermaßverbot) 147
4.2.3.4 Justizgrundrechte – Art. 19 Abs. 4, 101 und 103 GG 147
4.2.4 Bewertung Art. 15 ..... *148*
4.3 ARTIKEL 16 – BESCHLEUNIGTE SICHERUNG GESPEICHERTER COMPUTERDATEN 149
4.3.1 Anwendungsbereich *149*
4.3.2 Beschleunigte Sicherung von Daten *149*
4.3.3 Sicherungszweck *150*
4.3.4 Dauer der Sicherung *150*
4.3.5 Adressat der Sicherungsanordnung *151*
4.3.6 Grenzüberschreitende Sachverhalte *151*
4.3.7 Vergleichbare Befugnisnormen im deutschen Strafprozessrecht *151*
4.3.7.1 § 94 StPO – [Sicherstellung von Beweisgegenständen] 151
4.3.7.2 Gegenstände als Beweismittel 152
4.3.7.3 Ablauf 154
4.3.7.4 Beschlagnahmezweck 155
4.3.7.5 Dauer 156
4.3.7.6 Verhältnismäßigkeit 156
4.3.7.7 Beschlagnahmeverbote 157
4.3.7.8 Ergebnis zu § 94 StPO 157
4.3.8 Bewertung Art. 16 ..... *157*
4.4 ARTIKEL 17 – BESCHLEUNIGTE SICHERUNG UND TEILWEITERGABE VON VERBINDUNGSDATEN 159
4.4.1 Anwendungsbereich *159*
4.4.2 Verbindungsdaten *159*
4.4.3 Beschleunigte Sicherung und Teilweitergabe *161*
4.4.4 Sicherungszweck und Sicherungsdauer *162*
4.4.5 Adressaten der Sicherungsanordnung *162*
4.4.6 Vergleichbare Befugnisnormen im deutschen Strafprozessrecht *162*
4.4.6.1 § 94 StPO – [Sicherstellung von Beweisgegenständen] 162
4.4.6.2 § 100g Abs. 1 Satz 1 StPO – [Auskunft über Telekommunikationsverbindungsdaten] 162
4.4.6.2.1 Telekommunikationsverbindungsdaten 163
4.4.6.2.2 Umfang der Auskunftserteilung 163
4.4.6.2.3 Verdacht einer Straftat 165
4.4.6.2.4 Zeitlicher Rahmen 165

4.4.6.2.5 Adressaten der Auskunftsanordnung ... 165
4.4.6.2.6 Datenschutzbelange und Zeugnisverweigerungsrechte ... 166
4.4.6.2.7 Ergebnis zu § 100g Abs. 1 Satz 1 StPO ... 166
4.4.7 Bewertung Art. 17 ... 167
4.5 ARTIKEL 18 – HERAUSGABEANORDNUNG ... 169
4.5.1 Anwendungsbereich ... 169
4.5.2 Computerdaten und Kundendaten ... 169
4.5.3 Besitz oder Kontrolle ... 170
4.5.4 Bedingungen und Garantien ... 171
4.5.5 Vergleichbare Befugnisnormen im deutschen Strafprozessrecht ... 171
4.5.5.1 § 95 StPO – [Herausgabepflicht] ... 171
4.5.5.1.1 Gegenstände der vorbezeichneten Art ... 171
4.5.5.1.2 Gewahrsam des Herausgabepflichtigen ... 172
4.5.5.1.3 Beschränkungen im Anwendungsbereich von § 95 StPO ... 173
4.5.5.1.4 Verhältnismäßigkeit ... 174
4.5.5.1.5 Ergebnis zu § 95 StPO ... 174
4.5.5.2 § 89 Abs. 6 TKG – Abfrage von Bestandsdaten ... 174
4.5.6 Bewertung Art. 18 ... 174
4.6 ARTIKEL 19 – DURCHSUCHUNG UND BESCHLAGNAHME GESPEICHERTER COMPUTERDATEN ... 177
4.6.1 Anwendungsbereich ... 177
4.6.2 Abs. 1 und 2 – Durchsuchung ... 178
4.6.2.1 Durchsuchungsobjekte ... 178
4.6.2.2 Durchsuchungshandlung ... 179
4.6.3 Abs. 3 – Beschlagnahme und Sicherstellung in ähnlicher Weise ... 179
4.6.4 Objekte der Beschlagnahme ... 179
4.6.5 Abs. 4 – Erteilung von Auskünften ... 180
4.6.6 Vergleichbare Befugnisse im deutschen Strafprozessrecht ... 181
4.6.6.1 §§ 102 ff. StPO – [Durchsuchung] ... 181
4.6.6.1.1 Durchsuchungsobjekte ... 181
4.6.6.1.2 Einschränkungen ... 184
4.6.6.1.3 Ergebnis zu §§ 102 ff. StPO ... 184
4.6.6.2 § 94 StPO – [Sicherstellung von Beweisgegenständen] ... 185
4.6.6.3 §§ 48 ff StPO – [Zeugenpflichten] ... 185
4.6.6.4 Ergebnis zu §§ 48 ff. StPO ... 187
4.6.6.5 Auskunftserteilung durch andere Personen ... 187
4.6.7 Bewertung Art. 19 ... 188
4.7 ARTIKEL 20 – ECHTZEIT-ERHEBUNG VON VERBINDUNGSDATEN ... 191
4.7.1 Anwendungsbereich ... 191
4.7.2 Verbindungsdaten ... 192
4.7.3 Erheben oder Aufzeichnen ... 192
4.7.4 Bestimmte Kommunikationen ... 192
4.7.5 Einschränkungen im räumlichen Anwendungsbereich ... 193
4.7.6 Verhältnis von Abs. 1 zu Abs. 2 ... 193
4.7.7 Abs. 3 – Vertraulichkeit ... 194
4.7.8 Vorbehalt nach Art. 14 Abs. 3 ... 194
4.7.9 Vergleichbare Befugnisse im deutschen Strafprozessrecht ... 194
4.7.9.1 §§ 100g f. StPO – [Auskunft über Telekommunikationsverbindungsdaten] ... 196
4.7.9.1.1 § 100g Abs. 1 Satz 3 StPO – Auskünfte über zukünftige Verbindungsdaten ... 196
4.7.9.1.2 Zeitlicher Rahmen ... 197
4.7.9.1.3 Datenschutzbelange ... 197
4.7.9.1.4 Überwachung eines abgegrenzten Netzwerks (LAN) ... 198
4.7.9.1.5 Vertraulichkeit der Überwachung ... 198
4.7.9.1.6 Ergebnis zu § 100g Abs. 1 Satz 3 StPO ... 198
4.7.9.2 §§ 100a, 100b StPO – [Überwachung der Telekommunikation] ... 199
4.7.10 Bewertung Art. 20 ... 199
4.8 ARTIKEL 21 – ABFANGEN VON INHALTSDATEN ... 201
4.8.1 Anwendungsbereich ... 201
4.8.2 Inhaltsdaten ... 202
4.8.3 Vorbehalt nach Art. 14 Abs. 3 ... 202
4.8.4 Vergleichbare Befugnisse im deutschen Strafprozessrecht ... 202
4.8.4.1 §§ 100a und 100b StPO – [Überwachung der Telekommunikation] ... 202
4.8.4.2 Begriff der Telekommunikation ... 202
4.8.4.3 Überwachung und Aufzeichnung ... 205
4.8.4.4 Verdacht der Begehung einer Katalogstraftat ... 205
4.8.4.5 Adressaten der Überwachungsanordnung ... 206

4.8.4.6 Subsidiaritätsprinzip 207
4.8.4.7 Überwachung eines abgegrenzten Netzwerks (LAN) 207
4.8.4.8 Ergebnis zu § 100a StPO 207
4.8.5 Bewertung Art. 21 ..... *208*
4.9 ARTIKEL 22 – GERICHTSBARKEIT 209
4.9.1 Anwendungsbereich *209*
4.9.2 Abs. 1 lit. a) – Territorialitätsprinzip *209*
4.9.3 Abs. 1 lit. b) und c) – Flaggenprinzip *210*
4.9.4 Abs. 1 lit. d) – Personalprinzip sowie Grundsatz der stellvertretenden Strafrechtspflege *210*
4.9.5 Abs. 2 – Vorbehalt; Abs. 3 – „aut dedere aut judicare“ *210*
4.9.6 Abs. 4 und Abs. 5 ..... *211*
4.9.7 Deutsches Strafanwendungsrecht *211*
4.9.7.1 §§ 3 und 4 StGB – Territorialitäts- und Flaggenprinzip 211
4.9.7.2 §§ 5 und 7 StGB 211
4.9.7.3 § 9 StGB – Ort der Tat 212
4.9.7.4 Ergebnis zum internationalen Strafanwendungsrecht 213
4.9.8 Bewertung Art. 22 ..... *213*
5 ZUSAMMENFASSUNG DER ERGEBNISSE 215
LITERATURVERZEICHNIS 221

Abkürzungsverzeichnis

BMI	Bundesministerium des Innern
BMJ	Bundesministerium der Justiz
BMWA	Bundesministerium für Wirtschaft und Arbeit
ETS	European Treaties Series
EIM	European Institute for the Media
ER	Explanatory Report des Europarats
EuR	Europarat
EuRatS	Satzung des Europarats
IP	Internet Protocol
ISO	International Standard Organisation
ISP	Internet Service Provider
iVm	in Verbindung mit
jP	juristische Person
LAN	Local Area Network
MDStV	Staatsvertrag über Mediendienste
mwN	mit weiteren Nachweisen
OSI	Open Systems Interconnection
PV	Personenvereinigung
RA	Abkommen von Rom
RegE	Gesetzentwurf der Bundesregierung
RegTP	Regulierungsbehörde für Telekommunikation und Post
RBÜ	Berner Übereinkunft zum Schutz von Werken der Literatur und Kunst in der Pariser Fassung vom 24. Juli 1971
TCP	Transmission Control Protocol
TDG	Teledienstegesetz
TDDSG	Gesetz über den Datenschutz bei Telediensten
TDSV	Telekommunikations-Datenschutzverordnung
TK	Telekommunikation
TKG	Telekommunikationsgesetz

TKÜV	Telekommunikations-Überwachungsverordnung
TRIPs	Agreement On Trade Related Aspects of Intellectual Property Rights
UNRISD	United Nations Research Institute for Social Development
WAN	Wide Area Network
WCT	WIPO Copyright Treaty
WIPO	World Intellectual Property Organization
WPPT	WIPO Performances and Phonograms Treaty

1 Einleitung

1.1 Eine neue Bedrohung?

„Als sich die Köpfe der Weltwirtschaft im Januar 2001 im schweizerischen Davos zum „World Economic Forum“ trafen, sorgten 4000 Polizisten für Sicherheit – glaubten sie. Denn während die Staatsmacht den Tagungsort hermetisch abriegelte, bedienten sich Hacker in Seelenruhe in den Konferenz-Computern. Dort verschafften sie sich die Daten der 3200 Teilnehmer des Gipfels, einschließlich 1400 Kreditkarten- sowie die Handynummern von Palästinenserführer Jassir Arafat und der ehemaligen US-Außenministerin Madeleine Albright.[...][1]“ Mit diesen Zeilen beginnt ein Artikel der „Financial Times Deutschland“ vom 31.08.2001 über die von der Computerkriminalität ausgehenden Gefahren und führt so eindrucksvoll die Risiken vor Augen, die die neuen Medien neben zahlreichen Gebrauchsvorteilen mit sich bringen.

Wirtschaft und Politik zeigen sich in gleichem Maße über die Sicherheit im Cyberspace besorgt. Laut weltweiter Umfragen und Statistiken nimmt die Computerkriminalität in alarmierendem Maße zu.[2] Ein Hauptgrund besteht darin, dass die modernen Kommunikationstechnologien Einzug in nahezu alle Lebensbereiche der modernen Informationsgesellschaft gehalten und auf diese Weise neue Möglichkeiten für kriminellen Missbrauch eröffnet haben. Sensible Daten werden in großen Mengen elektronisch erfasst, oftmals ohne der IT-Sicherheit die gebührende Aufmerksamkeit zu schenken. Vor allem die rasante Vernetzung der globalen Computersysteme und die massenhafte Nutzung des WWW-Dienstes im Internet schufen eine verwundbare Angriffsfläche für kriminelle Aktivitäten jeder Couleur.

Die Angst vor Angriffen aus dem Netz wurde durch die terroristischen Anschläge vom 11. September 2001 noch weiter verstärkt. US-Präsident George W. Bush hat zum Schutz vor neuen Formen des Terrors seinen Stab um einen Sonderberater für Computersicherheit erweitert. Eine der ersten Aufgaben Richard Clarkes ist die Entwicklung eines Plans für ein eigenes, vom Internet getrenntes Computernetz der Regierung und Behörden. Das „Govnet“ solle vor Hacker- oder terroristischen Angriffen schützen, berichtete „Die Welt“[3].

Daher muss die Frage aufgeworfen werden, inwieweit die Computerkriminalität eine „neue Bedrohung“[4] darstellt, die legislatorische Schritte erfordert. Die Antwort darauf hat nicht nur Bedeutung für die Sicherheit der modernen Informationsgesellschaft, sondern auch für den Umfang der Freiheitsrechte des Einzelnen. Je höher der Gesetzgeber das Gefährdungspotential im Bereich von Computernetzen einschätzt, desto rigider werden Maßnahmen zu dessen Eindämmung ausfallen und desto mehr werden Bürgerrechte beschränkt werden. Genau in dieses Spannungsfeld stößt auch die „Convention on Cybercrime“[5] (**E**uropean **T**reaties **S**eries No. 185) des Europarats. Dabei handelt es sich um einen Vertragsentwurf des Ministerkomitees auf dem Gebiet des Computerstrafrechts, der nach Abschluss des mehrstufigen völkerrechtlichen Vertragsschlussverfahrens auch in Deutschland geltendes Recht darstellen wird. Von den Sicherheitsbehörden hoch gelobt hat das Übereinkommen Datenschützer und Bür-

[1] „Financial Times Deutschland“ vom 31.08.2001, *Lizenz zum Schnüffeln*, Tillmann Prüfer
[2] Siehe dazu Kapitel 1.8
[3] „Die Welt“ vom 04.04.2002, *Die Angst vor dem Terror aus dem Internet wächst*, Oliver Tessmer
[4] Ein „Bedrohungspotential“ sieht auch die Bundesregierung in ihrer Antwort auf eine große Anfrage aus dem Bundestag zum wirksamen Schutz vor Computerattacken vom 20.06.2001, BT-Drs. 14/6321, S. 2 ff.
[5] Da die Amtssprachen des Europarats Englisch und Französisch sind, existiert keine amtliche Übersetzung ins Deutsche. In der vom BMJ veröffentlichten „Arbeitsübersetzung“, die auch den weiteren Ausführungen zu Grunde gelegt wird, wird der Ausdruck mit „Übereinkommen über Datennetzkriminalität“ wiedergegeben.

gerrechtler zu heftigen Protesten veranlasst. Nicht umsonst tituliert die „Financial Times Deutschland“ den zitierten Artikel *Lizenz zum Schnüffeln* und nimmt damit Bezug auf die umfassenden Befugnisse, die der Vertrag den Ermittlungsbehörden geben soll.

Die vorliegende Arbeit untersucht, inwieweit die materiellrechtlichen und prozessualen Vorgaben des Übereinkommens von geltenden Strafnormen in Deutschland abweichen. Soweit die vertraglichen Vorgaben über das deutsche Recht hinausgehen, werden Möglichkeiten und Grenzen – vor allem im Hinblick auf die grundgesetzlichen Freiheitsrechte – einer Anpassung des nationalen Rechts aufgezeigt.

1.2 Funktionen und Aufgaben des Europarats[6]

Der Europarat (EuR) entstand im Jahre 1949[7] als Reaktion der westeuropäischen parlamentarischen Demokratien auf die Blockbildung der kommunistischen Staaten Osteuropas. Er war der erste sichtbare Ausdruck der europäischen Idee. Seine Aufgabe besteht darin „[...] eine engere Verbindung zwischen seinen Mitgliedern zum Schutze und zur Förderung der Ideale und Grundsätze, die ihr gemeinsames Erbe bilden, herzustellen und ihren wirtschaftlichen und sozialen Fortschritt zu fördern“, Art. 1 lit. a) EuRatS. Dies soll gem. Art. 1 lit. b) EuRatS realisiert werden „durch Beratungen von Fragen von gemeinsamem Interesse, durch den Abschluss von Abkommen und durch gemeinschaftliches Vorgehen auf wirtschaftlichem[8], sozialem, kulturellem und wissenschaftlichen Gebiet und auf den Gebieten des Rechts und der Verwaltung sowie durch den Schutz und die Fortentwicklung der Menschenrechte und Grundfreiheiten“. Als große, allgemeinpolitische Organisation Europas, die zunächst primär den Frieden im Nachkriegseuropa sichern sollte, stellte er ein wichtiges europäisches Forum dar und wird insofern zu Recht als „Keimzelle“ der europäischen Gemeinschaften bezeichnet.[9] Gemäß Art. 1 lit. d) EuRatS wurden Fragen der Verteidigung aus dem Zuständigkeitsbereich des EuR ausgenommen, um den neutralen Staaten Europas (Schweden, Schweiz, Österreich) die Mitgliedschaft zu ermöglichen. Zentrale Bedeutung für den EuR und seine Mitgliedsländer haben das Rechtstaatsprinzip, die Menschenrechte sowie die grundsätzlichen Freiheitsrechte, vgl. Art. 3 EuRatS. Als eine seiner bedeutendsten Leistungen ist in diesem Zusammenhang die Erarbeitung der „Europäischen Menschenrechtskonvention“ im Jahre 1950 hervorzuheben, die von allen Mitgliedsstaaten ratifiziert wurde. Seinen Sitz hat der Rat in Straßburg, Frankreich. Die Bundesrepublik Deutschland ist am 13.07.1950 assoziiertes und am 02.05.1951 Vollmitglied geworden.[10]

Mit dem Ende des Kalten Krieges und der Blockbildung in Europa besteht eine neue Aufgabe des EuR in der Stabilisierung der osteuropäischen Demokratien. Diese sollen schrittweise an die demokratischen und rechtsstaatlichen Standards der übrigen Länder Europas herangeführt werden. In diesem Licht sind die Beitritte der jüngsten Mitglieder Armenien und Aserbaidschan am 25.01.2001 sowie Bosnien und Herzegowina am 24.04.2002 zu sehen. Der Europarat zählt mittlerweile 45 Mitgliedsstaaten; darunter alle 15 Mitgliedsstaaten der EGen. Beobachterstatus im Ministerkomitee haben Kanada, der Heilige Stuhl, Japan, Mexiko sowie die USA; Beobachterstatus in der Parlamentarischen Versammlung Kanada, Israel und Mexiko. Mitglied kann auf Einladung des Ministerkomitees jeder europäische Staat werden, Art. 4

[6] Im WWW: http://www.coe.int/
[7] Unterzeichnung der Satzung am 05.05.1949, BGBl. 1950 I, S. 263
[8] Primäre Aufgabe der 1948 gegründeten OEEC (*Organization for European Economic Cooperation)*, heutige OECD (*Organization for Economic Cooperation and Development*)
[9] Oppermann, Europarecht, § 2, Rn. 61
[10] Gesetz über den Beitritt der Bundesrepublik Deutschland zum Europarat vom 08.07.1950, BGBl. 1950 I, S. 263 ff. iVm der Bekanntmachung vom 16.09.1953, BGBl. 1953 II, S. 558

EuRatS, der die in Art. 3 EuRatS niederlegten Grundsätze respektiert.

Nach Art. 10 EuRatS besitzt der EuR zwei Organe, das Ministerkomitee und die Parlamentarische Versammlung. Durch das parlamentarische Organ hebt er sich von der typischen Struktur anderer internationaler Organisationen ab. Beide Einrichtungen werden unterstützt durch das Sekretariat, Art. 10, 36 ff. EuRatS, sowie durch den „Congress of Local and Regional Authorities of Europe", der auf die Wiener Erklärung der Staats- und Regierungschefs der Europaratsstaaten zurückgeht.

Die „Convention on Cybercrime" stellt ein Abkommen im Sinne von Art. 1 lit. b) EuRatS dar[11], über das das Ministerkomitee nach Art. 15 lit. a) EuRatS beschloss, nachdem es der Parlamentarischen Versammlung zum Zweck der Beratung zugeleitet worden war, Art. 22 EuRatS. Es dient der Aufgabenerfüllung nach Art. 1 lit. b) EuRatS. Neben den Mitgliedsstaaten wurde die Konvention bislang von Kanada, Japan, Südafrika und den USA unterzeichnet.[12] Insbesondere der Beitritt der Vereinigten Staaten ist zu begrüßen, da ein Großteil der internationalen Datenübertragungen wegen der hohen Transportkapazitäten über das Staatsgebiet der USA erfolgt[13] und daher ihrer Strafgewalt unterliegen.

Das strafrechtliche Engagement des Europarats war seit jeher groß. Bereits im Jahre 1957 hat das Ministerkomitee den europäischen Ausschuss für Strafrechtsprobleme (ECCP) ins Leben gerufen, um die Arbeit auf diesem Gebiet zu intensivieren. Von einer Harmonisierung der materiellen Strafrechte im europäischen Bereich kann jedoch noch keine Rede sein. Zwar laufen seit 1984 Bestrebungen, sämtliche strafrechtlichen Instrumente des Europarats zu einem „zusammenfassenden Übereinkommen" zu verschmelzen; der Ausgang dieses ehrgeizigen Projekts ist zum gegenwärtigen Zeitpunkt jedoch noch nicht absehbar.[14] Im Augenblick stellt die „Cybercrime Convention" das 25. Abkommen des EuR auf dem Gebiet des Strafrechts dar.[15]

1.3 Entstehung der Konvention

Die Konvention ist ein Resultat jahrelanger, internationaler Bemühungen zur Verbesserung der Bekämpfung der Computerkriminalität. Neben dem Europarat findet eine länderübergreifende Zusammenarbeit auch auf der Ebene der Vereinten Nationen, der OECD, der G8 und der Europäischen Union statt.[16] Bislang stellt die Konvention das weitest reichende und konkreteste Ergebnis dieser Bemühungen dar.

Die Ausarbeitung der Konvention wurde durch eine Entscheidung des Lenkungsausschusses für Strafrecht (*„European Committee on Crime Problems", CDPC)* im November 1996[17] angeregt. Darin wurde die Absicht bekundet, einen Sachverständigenausschuss (*„Committee of Experts on Crime in Cyber-space"*, PC-CY) einzusetzen, der sich mit den Fragen der Datennetzkriminalität auseinandersetzen sollte. Als Ergebnis der Ausschussarbeit sollte ein Vertragsentwurf entstehen, „[…] der Fragen des materiellen Strafrechts, des Verfahrensrechts und Möglichkeiten internationaler Zusammenarbeit sowie internationaler Verträge […]" be-

[11] In den beiden Amtssprachen Englisch und Französisch.
[12] Überblick auf den WWW-Seiten des EuR unter: http://conventions.coe.int/Treaty/EN/cadreprincipal.htm (01.03.2004)
[13] Das Windows Programm *„tracert"* erlaubt beispielsweise eine Rekonstruktion der Datenwege.
[14] Jescheck/Weigend, Strafrecht AT, § 18, S. 182 ff.
[15] Übersicht über die Abkommen zwischen 1957 und 1990 bei Vogler JURA 1992, 586 ff.
[16] Germann, Gefahrenabwehr und Strafverfolgung im Internet, S. 42 f. mwN
[17] CDPC/103/211196

handelt.[18] Im Gegensatz zu einer bloßen Empfehlung bevorzugte der EuR diese Handlungsform wegen ihrer größeren rechtlichen Verbindlichkeit.

Der Sachverständigenausschuss wurde durch eine Entscheidung[19] des Ministerkomitees vom 04.02.1997 eingerichtet und nahm seine Arbeit im April 1997 mit dem Ziel auf, bis zum 31.12.2000 einen Entwurf vorzulegen. Der Ausschuss konnte dabei an vorhandene Dokumente des Europarates anknüpfen. Die Empfehlung Nr. R (88) 2[20] behandelt Probleme der Piraterie auf dem Gebiet des Urheberrechts und anderer Rechte, die Empfehlung Nr. R (89) 9[21] Richtlinien für die Definition bestimmter Computerdelikte und die Empfehlung Nr. R (95) 13[22] Probleme des Strafprozessrechts, die im Zusammenhang mit den Informationstechnologien auftauchen.

Der Auftrag an den Sachverständigenausschuss wurde auf folgende drei Themenkreise konkretisiert:[23]

1. In materieller Hinsicht auf diejenigen Computerdelikte, die in oder durch Netzwerke, z.B. dem Internet, begangen werden. In Betracht kommen rechtswidrige Geldtransfers, das Anbieten rechtswidriger Dienste, Verletzungen der Menschenwürde und Delikte gegen die Rechte Minderjähriger. Darüber hinaus sollten Fragestellungen des materiellen Strafrechts überall dort beleuchtet werden, wo ein gemeinsames Vorgehen zum Zwecke internationaler Zusammenarbeit geboten ist, z.B. bei der Erarbeitung von Definitionen, Festlegung von Sanktionen und Verantwortungsbereichen für die Beteiligten in Datennetzen, einschließlich der Anbieter von Diensten im Internet.

2. Was das Verfahrensrecht betrifft, war beabsichtigt, die Anwendbarkeit von Eingriffsbefugnissen auf die neuen Informations- und Kommunikationstechnologien zu prüfen, auch und vor allem im grenzüberschreitenden Bereich, beispielsweise das Abhören von Telekommunikationseinrichtungen und die elektronische Überwachung von Informationsnetzwerken, z.B. dem Internet, die Durchsuchung und Beschlagnahme gespeicherter Daten (einschließlich Internetseiten), die Einziehung illegaler Materialien und die Verpflichtung von Anbietern, bestimmte Vorschriften zu beachten. Dies sollte unter Berücksichtigung der Probleme geschehen, die sich durch Methoden der Datensicherheit ergeben, wie z.B. durch Verschlüsselungsverfahren und der Frage, welche Rechtsordnung bei Delikten im Bereich der Informationstechnologie zur Anwendung kommt. Notwendig dazu ist eine Regelung zur Bestimmung des Tatorts (*locus delicti*), von dem der Gerichtsstand abhängt, eine Regelung zum Problem des *ne bis in idem* für den Fall, dass mehrere Gerichte sich für zuständig halten und Regelungen zur Frage positiver und negativer Zuständigkeitskonflikte.

3. Darüber hinaus war die Behandlung von Fragen der internationalen Zusammenarbeit bei der Ermittlung im Bereich von Computerdelikten Gegenstand der Ausschussarbeit.

[18] Explanatory Report (ER) Ziff. 10, EuR: http://conventions.coe.int (01.03.2004); zur Bedeutung des Explanatory Report siehe im folgenden vor allem Kapitel 1.5 (letzter Absatz)
[19] Nr. CM/Del/Dec (97) 583
[20] *Recommendation on Measures to Combat Piracy in the Field of Copyright and Neighbouring Rights*; Online: http://cm.coe.int/ta/rec/1988/88r2.htm (01.03.2004)
[21] *Recommendation on Computer-Related Crime;* Europarat, Computer-Related Crime, S. 7; Online: http://cm.coe.int/ta/rec/1989/89r9.htm (01.03.2004)
[22] *Recommendation of the Committee of Ministers to Member States Concerning Problems of Criminal Procedural Law Connected with Information Technology*; Online: http://cm.coe.int/ta/rec/1995/95r13.htm (01.03.2004)
[23] ER Ziff. 11

Für diese drei Gebiete wurde die Erstellung eines Entwurfs hinsichtlich rechtlicher Handlungsmöglichkeiten erwartet, der für die Unterzeichner verbindlich sowie einen möglichst umfassenden Handlungsspielraum eröffnet sollte. Das besondere Augenmerk galt der Berücksichtigung internationaler Fragen und der Möglichkeit begleitender Empfehlungen bezüglich spezifischer Fragen. Der Sachverständigenausschuss hatte darüber hinaus ein Vorschlagsrecht in Angelegenheiten, die technologische Entwicklungen betreffen.

Während der mehr als drei Jahre dauernden Arbeit des PC-CY brachten sowohl die europäischen Justizminister als auch die Mitgliedsstaaten der EU mehrmals ihre unterstützende Haltung zum Ausdruck.[24] Gleichzeitig forderten sie die verhandelnden Parteien auf, ihre Bemühungen mit dem Ziel fortzusetzen, Möglichkeiten zu finden, damit eine möglichst große Zahl von Nationen die Konvention unterzeichnen könne, um auf diese Weise eine wirksame und effektive internationale Zusammenarbeit im Kampf gegen die Datennetzkriminalität zu gewährleisten. Nach dem Ablauf seines Mandats hielt der Ausschuss unter der Schirmherrschaft des CDPC drei weitere Sitzungen, um den Entwurf eines „Erläuternden Berichts (*Explanatory Report*)“ fertig zu stellen und den Konventionsentwurf unter Berücksichtigung der Stellungnahme der Parlamentarischen Versammlung zu überarbeiten. Das Ministerkomitee forderte die Parlamentarische Versammlung im Oktober 2000 zu einer Stellungnahme auf, die sie im zweiten Teil ihrer Vollversammlung im April 2001 verabschiedete.

Auf der Grundlage einer Entscheidung des Sachverständigenausschusses PC-CY waren frühere Konventionsentwürfe im April 2000 deklassifiziert und veröffentlicht worden, gefolgt von weiteren Entwürfen nach jeder Vollversammlung. Auf diese Weise sollte den an den Beratungen beteiligten Staaten die Möglichkeit gegeben werden, betroffene Interessengruppen frühzeitig in den Entscheidungsprozess mit einzubeziehen, wenn auch erst drei Jahre nach Aufnahme der Ausschussarbeit.[25] Wie umstritten die Konvention war (und ist), zeigt sich daran, dass 26 Entwürfe benötigt wurden, bis alle Beteiligten sich auf die endgültige, 27. Fassung, einigen konnten.

Der überarbeitete und vervollständigte Konventionsentwurf und der „Erläuternder Bericht“ wurden dem CDPC zum Zwecke der Zustimmung auf seiner 50. Vollversammlung im Juni 2001 übergeben. Im Anschluss daran ging der Entwurf dem Ministerkomitee zur Beschlussfassung und Unterzeichnung zu. Die Konvention wurde in ihrer endgültigen Fassung am 08.11.2001 vom Ministerkomitee des Europarats auf seiner 109. Sitzung in Budapest verabschiedet und am 23.11.2001 auf der Internationalen Konferenz zum Thema „Cybercrime“ zur Unterzeichnung eröffnet. Etwa ein Jahr später kam es zum Beschluss des ersten Zusatzprotokolls, das der Bekämpfung fremdenfeindlicher Inhalte im Zusammenhang mit Computersystemen, vor allem dem Internet, gewidmet ist.[26] Das Zusatzprotokoll wurde in der vorliegenden Arbeit nicht untersucht.

1.4 Der Rechtscharakter der Konvention

Wie bereits im vorigen Kapitel angedeutet, besitzt der Europarat (EuR) als internationale Organisation keine hoheitliche Befugnis für eine überstaatliche Rechtssetzung, wodurch er sich grundlegend von den supranationalen EGen unterscheidet. Diese können gemäß Art. 249 des

[24] Explanatory Report (ER) Ziff. 12; ABl. EG. L 142, S. 1, CELEX Nr. 31999F0364
[25] Zu Recht kritisch daher: Bäumler DuD 2001, 348 (349)
[26] „Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems“ (ETS 189); am 28.01.2003 zur Unterzeichnung eröffnet.

EG-Vertrags sowohl Verordnungen und Entscheidungen mit unmittelbarer Wirkung für die Bürger ihrer Mitgliedsstaaten erlassen als auch Richtlinien mit verpflichtendem Umsetzungsauftrag für die Mitgliedsstaaten.

Die legislatorischen Möglichkeiten des EuR erschöpfen sich dagegen in der Vorbereitung von völkerrechtlichen Verträgen, deren Annahme einer bestimmten Gruppe von Staaten, in erster Linie den Mitgliedsstaaten des Europarats, vorgeschlagen wird. Die Ausarbeitung und Verabschiedung der „Convention on Cybercrime" durch das Ministerkomitee entfaltete daher noch keinerlei rechtliche Wirkung, sondern stellte lediglich die erste Stufe im mehrphasigen völkerrechtlichen Vertragsschlussverfahren dar (sog. Authentifizierung). Beschlossen wurde nur, den Mitgliedsstaaten die Annahme des in diesem Beschluss verkörperten Vertragsentwurfes gemäß den verfassungsrechtlichen Vorschriften der einzelnen Staaten zu empfehlen.[27]

Völkerrechtlich verbindliche Wirkung entfaltet die Konvention, sobald fünf Staaten, unter denen sich mindestens drei Mitgliedsstaaten des EuR befinden müssen, den Vertragsentwurf unterzeichnet und die Ratifikations-(bzw. Annahme- bzw. Genehmigungs-)urkunden beim Generalsekretär des Europarats hinterlegt haben, Art. 36 Abs. 1-3 der Konvention.[28] Nach der Ratifikation durch Litauen am 18.03.2004, der bereits die Annahmen durch Albanien, Kroatien, Estland und Ungarn vorausgegangen waren,[29] trat die „Convention on Cybercime" am 01.07.2004 in Kraft. Da der Europarat selbst nicht mit eigener Rechtspersönlichkeit wie die EGen nach Art. 281 EG-Vertrag ausgestattet ist, wird er nicht Vertragspartei.

Die Konvention stellt daher einen multilateralen, völkerrechtlichen Vertrag zwischen denjenigen Staaten dar, die unterzeichnet und ratifiziert haben (im Folgenden: Unterzeichnerstaaten).[30] Die Einbeziehung von Völkerrechtssubjekten, die den Vertrag nachträglich annehmen, richtet sich nach Art. 36 Abs. 4. Über Art. 37 wird denjenigen Staaten, die nicht im Europarat vertreten sind und nicht an der Ausarbeitung des Abkommens teilhatten, der Beitritt zur Konvention ermöglicht.

Um die unmittelbare Geltung im Hoheitsgebiet der BRD herbeizuführen, ist auf nationaler Ebene darüber hinaus ein Zustimmungsgesetz des Bundestages erforderlich, Art. 59 Abs. 2 GG, das den Vertragsinhalt in die innerstaatliche Rechtsordnung einfügt (sog. generelle Transformation). Kommt das Übereinkommen völkerrechtlich nicht zu Stande, erlangt auch das transformierende Gesetz keine Rechtskraft. Bislang hat die BRD die Konvention zwar am 23.11.2001 unterzeichnet, jedoch weder eine Ratifikationsurkunde hinterlegt noch ein Zustimmungsgesetz verabschiedet[31], so dass noch keine vertragliche Bindung und damit auch keine Verpflichtung zur Umsetzung entstanden ist.

1.5 Überblick über die Konvention und den Gang der Darstellung

Die Konvention ist in vier Kapitel (*chapter)* unterteilt, die wiederum aus mehreren Abschnitten (*section*) und Titeln (*title*) bestehen können und die einzelnen Artikel (*article*) enthalten.

Die vier Kapitel tragen folgende Überschriften:

[27] Seidl-Hohenveldern/Stein, Völkerrecht, Rn 251 ff. (292)
[28] Im Folgenden beziehen sich alle Artikel ohne Gesetzesangabe auf die „Convention on Cybercrime".
[29] Eine Übersicht über den Status des Abkommens befindet sich auf der Homepage des EuR: http://conventions.coe.int/Treaty/EN/cadreprincipal.htm (01.03.2004)
[30] Explanatory Report (ER) Ziff. 304 ff.; Kugelmann DuD 2001, 215 (215)
[31] Siehe die Übersicht auf der Homepage des Europarats: Fn 29

(I) Definition von Begriffen *(Definitions)*

(II) Maßnahmen, die auf nationaler Ebene zu treffen sind *(Measures to be taken at the national level)* – materielles Recht und Strafverfahrensrecht.

(III) Internationale Zusammenarbeit *(International co-operation)*

(IV) Schlussbestimmungen *(Final provisions)*

Der 1. Abschnitt in Kapitel II behandelt Fragen des **materiellen Rechts**. Die Konvention geht anders als das deutsche StGB nicht vom Allgemeinen zum Besonderen Teil, sondern definiert zunächst neun Delikte, um im Anschluss daran allgemeine Bestimmungen zu Versuch und Beteiligung, sowie Sanktionen und Maßnahmen zu treffen. Die Delikte wurden in vier Gruppen zusammengefasst, denen jeweils ein Titel entspricht. Titel 1 enthält Tatbestände, die den unerlaubten Zugang zu Computersystemen – sog. Hacking – (*Illegal Access*), Art. 2, Eingriffe in nichtöffentliche Datenübertragungen (*Illegal Interception*), Art. 3, und gespeicherte Daten (*Data Interference*), Art. 4, sowie Manipulationen an Computersystemen (*System Interference*), Art. 5, sanktionieren. Eine Sonderstellung nimmt Art. 6 ein, der den Umgang mit bestimmten Vorrichtungen (*Illegal Devices)* – sog. „Hacker-Tools" – ächtet. Titel 2 beschreibt Tatbestände zur Computerdatenfälschung (*Computer-related Forgery*), Art. 7, und zum Computerbetrug (*Computer-related fraud*), Art. 8. Die nächsten beiden Titel sind Straftaten in Zusammenhang mit Kinderpornografie (*Offences related to child pornography*), Art. 9, sowie Urheber- und Verwandten Rechten (*Offences related to Copyright and related rights*), Art. 10, gewidmet. Art. 11 bis einschließlich 13 enthalten Normen zu Nebenformen der Verantwortlichkeit und Sanktionen.

Der 2. Abschnitt in Kapitel II enthält Bestimmungen zum **Verfahrensrecht**, die nach dem Willen der Verfasser nicht nur auf die im 1. Abschnitt definierten Tatbestände zur Anwendung kommen sollen, sondern auf alle Delikte im Zusammenhang mit Computern und Beweisen in elektronischer Form.[32] In einem vorangestellten allgemeinen Teil werden zunächst der Geltungsbereich der verfahrensrechtlichen Bestimmungen (*Scope of procedural provisions*), Art. 14, sowie Bedingungen und Garantien (*Conditions and Safeguards*), Art. 15, definiert. Im Anschluss daran bestimmt Titel 2 Befugnisse zur Beschleunigten Sicherung von Computerdaten (*Expedited preservation of stored computer data*), Art. 16, und der Beschleunigten Sicherung und Teilweitergabe von Verbindungsdaten (*Expedited preservation and partial disclosure of traffic data*), Art. 17. Titel 3 regelt in Art. 18 die Voraussetzungen der Herausgabeanordnung (*Production order*); Titel 4 die der Durchsuchung und Beschlagnahme gespeicherter Computerdaten (*Search and seizure of computer data*), Art. 19. Eingriffe in Verbindungsdaten (*Real time collection of traffic data*) und Inhaltsdaten (*Interception of content data*) während der Übermittlung werden von den Art. 20 und 21 geregelt. Kapitel II endet mit Bestimmungen zum Internationalen Strafrecht (*Jurisdiction*), Art. 22.

Kapitel III (Art. 23 bis 35) enthält Vorschriften zur Internationalen Zusammenarbeit und Rechtshilfe sowohl in Bezug auf die in der Konvention definierten Tatbestände als auch auf weitere, sofern Beweise in elektronischer Form erhoben werden sollen. Behandelt werden Situationen eines Rechtshilfeersuchens mit anwendbaren völkerrechtlichen Übereinkünften sowie Fälle ohne derselben. Die Rechtshilfe bezieht sich im Prinzip auf alle in Kapitel II definierten Befugnisse. Darüber hinaus sind Vorschriften enthalten zum grenzüberschreitenden Zugriff auf gespeicherte Daten ohne Rechtshilfeersuchen und zur Errichtung eines 24 (Stun-

[32] Art. 14 Abs. 2 lit. b) und c)

den)/7 (Tage) Netzwerkes für eine schnelle wechselseitige Hilfeleistung.

Kapital IV (Art. 36 bis 48) enthält lediglich Schlussbestimmungen, die nicht von denjenigen in anderen Konventionen des Europarates abweichen.

Die weiteren Ausführungen untersuchen die materiell- und verfahrensrechtlichen Vorgaben der Konvention (Art. 1 bis einschließlich 23). Dazu werden die einzelnen Artikel der Konvention zunächst erläutert und anschließend vergleichbare Normen des deutschen Strafrechts dargestellt. In einem dritten Schritt werden Unterschiede und Gemeinsamkeiten ermittelt und abschließend nach nationalen rechtlichen Gesichtspunkten bewertet. Die Erläuterung der Konvention erfolgt in erster Linie anhand des Wortlauts[33] sowie ergänzend mit Hilfe des am 08.11.2001 veröffentlichten „Explanatory Reports" (ER).[34] Dieser Erläuternde Bericht stellt zwar keine amtliche Kommentierung der einzelnen Konventionsbestimmungen dar, er wurde jedoch vom Europarat in einem formellen Verfahren mit der Maßgabe verabschiedet, die Umsetzung der vertraglichen Vorgaben in nationales Recht zu erleichtern.[35] Insofern ist er eine unverzichtbare Hilfe bei der Auslegung. Aus Gründen des besseren Verständnisses wurde der weiteren Darstellung die deutsche „Arbeitsübersetzung" des Normtextes durch das BMJ zu Grunde gelegt.[36] Auf den englischen bzw. französischen Wortlaut[37] wurde nur an den Stellen zurückgegriffen, wo es zur Erfassung des Norminhalts als unverzichtbar erschien. Von einer Bearbeitung des dritten und vierten Kapitels wurde Abstand genommen, da sie thematisch nicht mehr dem Kernbereich des Strafrechts angehören und insoweit abgrenzbar sind. Nicht zuletzt auch aus Platzgründen soll die Untersuchung der Internationalen Zusammenarbeit und Rechtshilfe in Strafsachen einer gesonderten wissenschaftlichen Bearbeitung vorbehalten bleiben.

1.6 „Cybercrime" und Computerkriminalität

Die amtliche Überschrift des Vertragsentwurfes lautet in der englischen Fassung „Convention on Cybercrime". Wenn man von dem Titel auf den Anwendungsbereich der Konvention schließt, so findet eine Einschränkung dahingehend statt, dass nicht die Computerkriminalität im Allgemeinen (engl. *computer crime*), sondern nur der Teil, der dem „Cyber"-Bereich zugeordnet werden kann, Gegenstand des Übereinkommens sein soll. Diese auf den ersten Blick nachvollziehbare Eingrenzung erweist sich jedoch auf Grund der inhaltlichen Unschärfe des „Cyber"-Begriffs als wenig aussagekräftig. Selbst im englischen Sprachraum wird der Ausdruck nicht einheitlich verwendet und beschreibt eine unbestimmte Vielzahl von Sachverhalten, die mit Computern im weiteren Sinne zu tun haben. Zu diesem Ergebnis kam eine Studie des „Europäischen Medieninstitutes" (EIM) im Auftrag der Friedrich-Ebert-Stiftung.[38]

In etymologischer Hinsicht setzt sich der Begriff „Cybercrime" aus den Bestandteilen „Cyber" und „Crime" zusammen. Während der zweite Wortbestandteil ohne weiteres etwa mit „Verbrechen, Delikt, Untat" wiedergegeben werden kann, fällt die Interpretation von „Cyber" deutlich schwerer. Dabei handelt es sich um kein eigenständiges Wort, sondern lediglich um

[33] Zu den Grenzen der Wortlautauslegung mangels einer internationalen Rechtssprache: von Weber ZStW 1953, 334 (345)

[34] Allgemein zur Auslegung internationaler Übereinkommen am Beispiel der EMRK: Echterhölter JZ 1956, 142 (142); Mattil JR 1965, 167 ff.; Meyer NJW 1974, 1175 (1176)

[35] ER Ziff. II

[36] Zu beziehen über das Bundesministerium der Justiz (BMJ), http://www.bmj.de/ (01.03.2004)

[37] BGH NJW 1966, 1021 (1024); Echterhölter JZ 1956, 142 (143); Herzog JZ 1966, 657 (657 f.); Meyer-Goßner Art 4 MRK Rn 5

[38] EIM, Twilight Zones in Cyberspace: Crimes, Risk, Surveillance and User-Driven Dynamics, S. 17

einen Wortteil, der ursprünglich dem englischen *„cybernetics"* (dt. Kybernetik) entlehnt wurde. Während unter „Kybernetik" die Wissenschaft der Systematik von Steuer- und Regelmechanismen in Technik, Biologie und den Gesellschaftswissenschaften[39] zu verstehen ist, hat der Begriff durch die Abkopplung und Neukombination des Morphems „Cyber" in den letzten Jahren einen Bedeutungswandel erfahren.

Die erste Neukombination, in der der Wortbestandteil „Cyber" verwendet wurde, war der englische Ausdruck *„Cyberspace"*. Dabei handelt es sich um ein Kunstwort, das der kanadische Sciencefiction-Autor William Gibson 1984 in seinem Roman „Neuromancer" kreierte. Es leitet sich ab von griechisch *„kybernetike techne"*, zu Deutsch „Steuermannskunst" und englisch „*space*", zu Deutsch „Raum". Gibson bezeichnete damit eine virtuelle Landschaft, die nur in den weltweit vernetzten Computern besteht, also eine digitale Scheinrealität. Die Umgangssprache verwendet den Begriff und auch das Morphem „Cyber" mittlerweile quasi als Synonym für das Internet. „Cyber" wird dementsprechend mit verschiedenen Begriffen kombiniert, je nachdem, in welchem Gesamtkontext es verwendet wird.

Wie schon Gibson, so sieht auch das EIM unter Bezugnahme auf ein Gutachten im Auftrag des UNRISD[40] den „Cyberspace" im „[…] nicht physischen Raum in den weltweiten Datennetzen, in dem, unabhängig von Zeit, Ort und Distanz, Inter- und Transaktionen zwischen Menschen untereinander, zwischen Menschen und Computern und zwischen Computern untereinander stattfinden."[41] Neben dem Internet erfüllen auch andere Netzwerke diese Kriterien, wie beispielsweise bei voll automatisierten Transportsystemen (Zügen, Flugzeugen, usw.), Überwachungssystemen in der industriellen Produktion, Robotern, Funknetzwerken (z.B. Mobiltelefone,...) und in anderen Bereichen.

„Cybercrime" bezeichnet demnach im engeren Sinne lediglich kriminelle Aktivitäten in Datennetzen.[42] Diese begriffliche Beschränkung in der Überschrift des Übereinkommens setzt sich in den einzelnen Bestimmungen der Konvention jedoch nicht fort. Wie sich bereits aus der Präambel und Art. 2 Satz 2 sowie vor allem Art. 14 Abs. 2 für den Bereich des Verfahrensrechts ergibt, ist die Konvention nicht nur der Bekämpfung der „Internetkriminalität" gewidmet, sondern jeder Form von Straftaten in Verbindung mit Computern. Dies sogar ohne grenzüberschreitenden internationalen Bezug. Der Sachverständigenausschuss ist damit weit über seinen vom Europarat erteilten Arbeitsauftrag hinausgegangen.[43] In der Literatur wird daher zu Recht kritisiert, dass das Übereinkommen einen unbegründeten Eingriff in die nationale Regelungshoheit im Bereich des Strafrechts darstelle und darüber hinaus im Rahmen der EU auf die Vereinbarkeit mit Art. 29 und 31e des EU-Vertrags zu überprüfen sei.[44] Auch die deutsche „Arbeitsübersetzung" des BMJ, die den Begriff mit „Datennetzkriminalität" wiedergibt, ist somit in Bezug auf die inhaltliche Reichweite der Konvention missverständlich. Richtigerweise wäre der Vertragsentwurf mit „Übereinkommen zur Computerkriminalität" zu überschreiben.

Selbst diese Präzisierung vermag den Kreis der erfassten Sachverhalte nur wenig einzugrenzen. Der Ausdruck „Computerkriminalität" wird im deutschen Strafrecht als ein kriminologischer Sammelbegriff für eine Vielzahl strafwürdiger, nicht unbedingt strafbarer Verhaltens-

[39] Langenscheidts online Fremdwörterbuch, http://www.langenscheidt.aol.de/ (01.03.2004)
[40] Hamelink, *New Information and Communication Technologies, Social Development and Cultural Change.*
[41] EIM, Twilight Zones in Cyberspace: Crimes, Risk, Surveillance and User-Driven Dynamics, S. 19
[42] Beispielsweise im „Internet". Auf eine Darstellung der technischen Grundlagen internationaler Computernetze wird im Folgenden verzichtet, da dies an anderer Stelle schon in erschöpfender Weise erfolgt ist.
[43] Siehe Kapitel 1.3 „Entstehung der Konvention"
[44] Bäumler DuD 2001, 348 (350)

weisen verwendet, denen gemeinsam ist, dass Computer entweder als Tatobjekte oder -werkzeuge behandelt werden.[45] Mit Ausnahme der durch das 2. WiKG[46] im Jahre 1986 eingefügten Tatbestände der §§ 202a, 263a, 269, 270, 303a, und 303b StGB weist das Kernstrafrecht keine Normen im Zusammenhang mit Computern auf. Ein „Allgemeiner Teil", der grundlegende Begriffe definieren könnte (z.B. „Daten"), steht bis heute aus. Nach derzeitiger Ansicht[47] lassen sich folgende Deliktsgruppen unterscheiden:

- Computermanipulation: Verändern von Daten, ohne diese zu beschädigen oder zu zerstören, mit dem Ziel, den Ausgang eines Datenverarbeitungsvorgangs zu beeinflussen
- Computerspionage: Ausforschen von Daten
- Computersabotage: Beschädigen oder Zerstören von Daten
- Computermissbrauch/Zeitdiebstahl: unberechtigte Nutzung fremder Rechenleistung und -kapazität

Insgesamt handelt es sich um ein sehr heterogenes Deliktsfeld. Eine Zuordnung zur Wirtschaftskriminalität, wie dies Teile der Literatur[48] vornehmen, lässt sich höchstens historisch nachvollziehen. Anders als in den Anfängen des Computerzeitalters sind PCs mittlerweile Massenware, die nicht mehr – u.a. wegen des hohen Anschaffungswertes, enormen Platzbedarfs, usw. – exklusiv zur Kontrolle von Wirtschaftsabläufen eingesetzt werden. In der modernen Informationsgesellschaft hat der Computer einen alltäglichen Stellenwert erhalten und wird neben beruflichen auch in gleichem Maße für private Zwecke eingesetzt. Daher wird auch verständlich, dass durch Delikte im Zusammenhang mit Computersystemen die unterschiedlichsten Rechtsgüter gefährdet und verletzt werden können. Eine weitere Unterteilung des Deliktsfelds, dessen einziges Bindeglied die Verwendung eines Computers in irgendeiner Art und Weise ist, entspricht nicht der Realität.

An Stelle des Blickwinkels des Täters wählt die Konvention für eine Systematisierung der Computerkriminalität den der Opfer. Bedroht durch Delikte im Zusammenhang mit Computern sind danach in erster Linie die Vertraulichkeit, die Integrität und die Verfügbarkeit der Computersysteme, Netze und Computerdaten.[49] Diese Kriterien entsprechen weitgehend dem heutigen Verständnis der IT-Sicherheit.[50] Daneben wird bisweilen auch die Verbindlichkeit von Informationen dazugezählt, die von der Konvention allerdings unerwähnt bleibt. Verletzungen – und auch Gefährdungen – der Vertraulichkeit, Integrität und Verfügbarkeit von Computersystemen, Netzen und Computerdaten bezeichnet die Konvention als „neue Formen" der Computerkriminalität.[51] Sie bedrohen oder behindern den ungestörten Informationsaustausch. Daneben können Computer auch als Werkzeuge zur Begehung herkömmlicher Delikte benutzt werden,[52] etwa der Verbreitung pornografischer, extremistischer oder sonstiger von einer Rechtsordnung geächteter Inhalte.

[45] Hilgendorf JuS 1996, 509 (510); Lampe GA 1975, 1 ff.; Sieg Jura 1986, 352; Welp IuR 1988, 443 (444)
[46] BGBl. 1986 I, S. 721 ff.
[47] Bereits Lampe GA 1975, 1 ff.; ebenso: Hilgendorf JuS 1996, 509 (510); Sieg Jura 1986, 352 sowie Winkelbauer CuR 1985, 40 (41)
[48] Etwa Hoeren/Sieber – *Sieber* 19 Rn 29 ff. in Bezug auf Hacking, Computerspionage, -sabotage und -manipulation.
[49] Vgl. Präambel der Konvention sowie ER Ziff. 8; ebenso: Antwort der Bundesregierung auf Große Anfrage, BT-Drs. 14/6321, S. 4 ff.
[50] Hilgendorf JuS 1996, 509 (510)
[51] ER Ziff. 5
[52] ER Ziff. 8

Damit schließt sich der Kreis zur Einteilung der Computerkriminalität nach deutschem Verständnis. Wie bereits *Lampe*[53] 1975 feststellte, können Computer entweder Mittel (seitens der Täter) oder Ziel (seitens der Opfer) der Einwirkung auf einen Datenverarbeitungsvorgang sein. Eine weitere Unterteilung der Computerkriminalität ist wegen der Vielzahl der bedrohten Rechtsgüter nicht zweckmäßig. Allenfalls in technischer Hinsicht bietet sich eine weitere Untergliederung an. In der Literatur wurden die Begriffe der Netzwerk- (z.B. Internet) und der Multimediakriminalität geprägt.[54] Gemeint sind damit Delikte, die sich in erster Linie im Umfeld von Netzwerken bzw. in dem Bereich ereignen, in dem mehrere Medien sich überschneiden und zusammenwachsen.

1.7 Phänomenologie der Netzwerkkriminalität

Wie bereits im vorangegangenen Kapitel dargestellt, geht die Konvention weit über den Bereich der Netzwerkkriminalität in einem internationalen Umfeld hinaus. Stattdessen erfasst sie eine Vielzahl strafwürdiger Sachverhalte im Zusammenhang mit Computern, wie im Folgenden noch zu zeigen sein wird. Dennoch kommt den Datennetzen – allen voran dem „Internet" – im Bereich der Computerkriminalität eine besondere Bedeutung zu. Seit seiner Entstehung[55] hat sich das Internet als ein zentrales Medium bei der Übermittlung von Informationen etabliert[56] und wesentlich zu einem „Paradigmenwechsel im Bereich der Rechtsobjekte"[57] beigetragen. In gleichem Maße wie das Informationszeitalter zusehends das Industriezeitalter ablöst, hat der Wert unkörperlicher Informationen zugenommen. Die „modernen Datenautobahnen" stellen Plattformen für den Informationsaustausch dar, bergen gleichzeitig jedoch schwer überschaubare Risiken. Die Strafrechtswissenschaft hat dies in den letzten Jahren erkannt und ist seither bemüht, den Schutz unkörperlicher Informationen an den körperlicher Objekte (Sachen) anzupassen sowie strafwürdige Verhaltensweisen in Zusammenhang mit den neuen „Informations- und Kommunikationstechnologien" zu definieren. Um die Anforderungen an die zukünftige Strafgesetzgebung nachvollziehen zu können sowie auf Grund der besonderen Bedeutung des Internets für die moderne Informationsgesellschaft, geben die folgende Darstellungen einen kurzen Überblick über ausgewählte Formen der Internetkriminalität, untergliedert nach den von der Konvention unterschiedenen Angriffsrichtungen Vertraulichkeit, Integrität und Verfügbarkeit von Computersystemen und Daten. Die Ausführungen erheben keinen Anspruch auf Vollständigkeit. Vernetzte Rechner können ebenso wie nicht an ein Netzwerk angeschlossene Computer Ziel und Medium krimineller Aktivitäten sein. Das Gefährdungspotential ist jedoch wegen der technischen Komplexität dieser Systeme und ihrer geografischen Reichweite ungleich größer.

1.7.1 Vertraulichkeitsverletzungen

Vertraulichkeitsverletzungen zielen nach dem natürlichen Wortsinn auf die Verletzung einer fremden Geheimsphäre ab. Diese umfasst bei Einzelplatzrechnern die lokal gespeicherten

[53] Lampe GA 1975, 1 ff.
[54] Eingehend dazu Hoeren/Sieber – *Sieber* 19 Rn 19 ff.
[55] Die Geburtsstunde des Internet im heutigen Sinne wird gemeinhin am 01.01.1983 erblickt, als das ARPANET das NCP-Protokoll durch die TCP/IP-Protokollfamilie ersetzte. Konstitutives Kriterium für das Internet ist nach diesem Verständnis die Verbindung von Computern auf der Basis der TCP/IP Protokolle. Ein fortlaufend aktualisierter Überblick über die Entwicklung des Internets seit dem Jahr 1957 findet sich bei „*Hobbes Internet Timeline*" unter der URL: http://www.zakon.org/robert/internet/timeline/ (01.03.2004). Dieses Dokument wurde von der Internetgemeinde 1998 als Standard RFC (engl. *Request for Comments*) 2235 veröffentlicht.
[56] Vor allem seit der Entwicklung des WWW am CERN in Genf, 1991.
[57] Hoeren/Sieber – *Sieber* 19 Rn 10

Daten; bei vernetzten Rechnern darüber hinaus die Verbindungen zu entfernten Systemen, etwa TCP/IP-basierten Datenübertragungen im Internet.

1.7.1.1 „Hacking“

Der aus dem Englischen stammende Begriff des „Hacking“ – zu Deutsch „Hacken“ – wird im allgemeinen Sprachgebrauch sowie in der strafrechtlichen Literatur in unterschiedlicher Bedeutung verwendet. Zum Teil werden Hacker mit Datenspionen bzw. Saboteueren gleichgesetzt[58], denen es auf die Erlangung der Herrschaft über fremde Daten ankommt, um sich beispielsweise geldwerte Betriebs- und Geschäftsgeheimnisse zu verschaffen oder sonstige Schäden anzurichten. Nach anderer Ansicht[59] handelt es sich um „Computerfreaks“, die aus sportlichem Ehrgeiz die Sicherheitsmechanismen fremder Computersysteme überwinden, ohne weitergehende Interessen an den freigelegten Daten zu verfolgen. Bei den Beratungen zu § 202a StGB verstand auch der Rechtsausschuss des Bundestags unter „Hacken“ das bloße Eindringen in ein fremdes Computersystem ohne die Verursachung von Beeinträchtigungen an den Daten oder dem System.[60]

Historisch betrachtet hat der Begriff „Hacker“ einen mehrfachen Bedeutungswandel erfahren. Er leitet sich vom englischen Verb „*to hack*“ ab, womit das Hineinhacken im Sinne von Tippen auf einer Tastatur gemeint ist. In den 1960er Jahren wurden erstmals diejenigen als Hacker bezeichnet, die sich intensiv mit der neuen EDV-Technik befassten, indem sie beispielsweise Computerprogramme schrieben und diese in die Tastatur hackten. Eine Hochburg war damals (wie heute) das „Massachusetts Institute of Technology“ (MIT)[61] in Boston, USA. Als wenig später die ersten Computernetze entstanden – zunächst in wissenschaftlichen und militärischen, später auch in für die Allgemeinheit zugänglichen Bereichen –, etablierte sich ein neuer Begriff des Hackers. Nicht mehr das Programmieren von Einzelplatz-Computern, sondern das Beschaffen von Zugangsrechten, insbesondere Passwörtern, zu räumlich entfernten Rechnern, die über ein Netzwerk erreichbar waren, stand nunmehr im Vordergrund. Die damals noch überschaubare Hackergemeinde fühlte sich jedoch einem ungeschriebenen Ehrenkodex verpflichtet und verzichtete auf die Verursachung von Schäden.[62]

Die negative Konnotation, die dem Begriff heutzutage beigemessen wird, resultiert aus dem Umstand, dass viele Hacker es bald nicht mehr dabei bewenden ließen, fremde Systeme aus schierem sportlichen Ehrgeiz zu kompromittieren, ohne diese zu beeinträchtigen. Mit der zunehmenden Verbreitung von EDV-Anlagen in allen Lebensbereichen befanden sich bald immer größere Mengen sensibler Daten im Netz, die für kriminelle Zwecke missbraucht werden konnten. Dieser Versuchung konnte auch ein Großteil der ehemals harmlosen Hacker nicht widerstehen[63] und fühlte sich dem ursprünglichen Ehrenkodex nicht mehr verpflichtet.

„Hacken“ mit dem „bloßen Eindringen in ein Computersystem“ gleichzusetzen, ist für eine strafrechtliche Bewertung zu undifferenziert. Hinter dem beschriebenen Erfolg verbirgt sich eine Vielzahl zweifelhafter Methoden, die oft nicht nur dem Hacker Zugang zu dem System

[58] Winkelbauer CuR 1985, 40 (44)
[59] Eingehend zum Begriff „Hacken“ Hauptmann JurPC 1989, 215 f.; zum Bedeutungswandel des Begriffs: Hoeren/Sieber – *Sieber* 19 Rn 30; Mühle, S. 17
[60] BT-Drs. 10/5058, S. 28
[61] http://web.mit.edu/ (01.03.2004)
[62] Siehe beispielsweise die „Hackerethik“ des Chaos Computer Clubs in Deutschland: http://www.ccc.de/hackerethics (01.03.2004)
[63] Eingehend zum Bedeutungswandel Frech, Der Bedeutungswandel des Begriffs „Hacker“ seit seiner Entstehung zu Beginn der 60er Jahre

und den Daten verschafft, sondern diese für eine breite Öffentlichkeit, etwa nach einem provozierten Systemabsturz, offen legt. Gängige Methoden lassen sich wie folgt systematisieren:

1.7.1.1.1 Ausnutzen menschlicher Schwächen

Gerade in der Anfangszeit der Computer benutzten viele Anwender Standardpasswörter (1234567..., Geburtsdatum, Name der Frau, usw.), die einfach zu erraten waren. Kamen potentielle Eindringlinge mit bloßem Raten nicht weiter, unternahmen sie Trickanrufe, in denen sie sich als Kollegen, Netzwerkadministratoren, usw. ausgaben (engl. *social engineering*) und die entsprechenden Kennungen unter dem Vorwand der Berechtigung erfragten. Mit steigender Rechenleistung wurden ganze Wörterbücher eingescannt, die unter Verwendung kleiner Hilfsprogramme vollautomatisch alle denkbaren alphanumerischen Kombinationen abfragten (engl. *brute force attack,* dt. Attacke mit roher Gewalt).

1.7.1.1.2 Sicherheitslücken im Betriebssystem[64]

Wann immer Rechner an Netzwerke angeschlossen werden, kommen sie mit anderen – im Falle des Internets mit einigen Millionen anderen – Computern in Berührung. Probleme können in diesem Fall durch Programm- und Konfigurationsfehler der Betriebssysteme entstehen. Dies beginnt bereits bei der Neuinstallation eines Computers, der vernetzt werden soll. Anders als der Laie es erwartet, enthalten viele Systeme keine vorkonfigurierten Sicherheitseinstellungen. Oftmals sind beispielsweise Standardzugänge und Standard-Passwörter (Wartungs- und Gast-Accounts, Router-Passwörter, Demo-User, usw.) enthalten, die von potentiellen Eindringlingen zweckentfremdet werden können. In diesem Stadium resultieren darüber hinaus Gefährdungen aus der Installation von Standarddiensten (z.B.: FTP-Server oder Apache-Webserver bei „Linux“, Datei- und Druckerfreigabe unter „Windows“, usw.), aus mitinstallierten und dann „vergessenen“ Diensten und aus der mangelnden Eignung vieler so genannter „netzwerkfähiger“ Softwareprodukte, die für kleine lokale Netze, nicht jedoch für große WANs (engl. *Wide Area Network*) geeignet sind.

Neben der mangelhaften Installation durch den Benutzer weist auch die Programmierung mancher Betriebssysteme Defizite auf. Ein typischer Fehler dieser Art ermöglicht die sog. Buffer-Overflow Attacke:

Puffer	**angrenzender Speicher**	
123	Programmdaten	Leerer Puffer
12345678901234567	Programmdaten	Puffer voll
12345678901234567	89012345679Progra	Puffer-Überlauf (Buffer-Overflow)
12345678901234567	890/bin/sh	Einschleusen des Shell Aufrufs

Abbildung bei Plate/Holzmann, Sicherheit in Netzen, 2.6.

[64] Fuhrberg, 3 ff., Plate/Holzmann, Sicherheit in Netzen, 2.3.; Wolf/Häger/Schorn, 3.3

Dabei lässt ein Angreifer eine bestimmte Datenmenge an ein Serverprogramm übertragen, das nicht prüft, ob der dafür vorgesehene Zwischenspeicher (Puffer) mit der Länge der übermittelten Zeichenkette übereinstimmt. Gelingt es dem Eindringling, eine überlange Zeichenfolge zu senden, wird der Speicher des Server-Programms überflutet und angrenzende Bereiche überschrieben. Das Server-Programm stürzt ab und hinterlässt das aufrufende Programm, das meist mit Administratoren-Berechtigung läuft. Im Anschluss kann der Aufruf einer „Shell“[65] (z.B.: /bin/sh) übertragen werden, wodurch der Angreifer Zugriff auf alle Funktionen des Betriebssystems erlangt.

Neben den Sicherheitsmängeln bei der Installation und Programmierung von Betriebssystemen, die oben dargestellt wurden, existieren zahlreiche weitere Lücken in diesem Bereich, die auf einschlägigen WWW-Seiten nachgelesen werden können.

1.7.1.1.3 Gefahren von Außen

Hat der Benutzer die Sicherheitseinstellungen seines Betriebssystems aktualisiert, ist er noch lange nicht sicher, sondern kann Zielscheibe zahlreicher weiterer Angriffe aus dem Netz werden. Je nach System kommen folgende Methoden zur Anwendung:

Trojanische Pferde sind Programme, die einerseits die gewünschte bzw. „offizielle“ Funktion bewirken, aber andererseits gleichzeitig die vom Manipulanten beabsichtigte Nebenwirkung ausführen. Während des Anmeldevorgangs (engl. *login*) eines berechtigten Nutzers imitieren sie beispielsweise den Prozess der Passwortabfrage, um dieses dann, unbemerkt für den Benutzer, abzuspeichern und/oder weiterzuleiten. Trojaner lädt sich der Benutzer in der Regel selbst aus dem Internet herunter, wobei er über die wahre Funktion des Schadprogramms getäuscht wird, dadurch dass es beispielsweise in ein Softwarepaket eingebunden ist, um sich dann unbemerkt im Hintergrund zu installieren oder unter dem Namen eines nützlichen Programms zu „verstecken“.

Viren dienen eigentlich nicht der Zugangserlangung, sondern bedrohen vor allem die Integrität und Verfügbarkeit von Daten (dazu weiter unten). Es sind jedoch auch Fälle bekannt, in denen Viren nach Infektion eines Systems vertrauliche Daten sammelten und in codierter Form nach außen weiterleiteten.[66]

Trapdoors (dt. Falltüren) sind Programmfunktionen, die einen nicht autorisierten Zugang zum System ermöglichen. Dies muss nicht in böser Absicht geschehen. Auch Programmteile, die zur Fehlersuche dienten und dann in der Verkaufsversion nicht entfernt wurden, oder Wartungszugänge, können zu unbeabsichtigten Hintereingängen werden. Das bekannteste Programm dieser Kategorie für Rechner unter Windows ist wohl „Back Orifice 2000” (BO2K) von der Hackergruppe „Cult of the Dead Cow“. Es ist frei im Internet erhältlich und ermöglicht einen vollständigen Zugriff auf alle Daten und Systempasswörter einschließlich des Zugangs zu Netzwerken. „Wer einen Multimedia-Computer mit Kamera und Mikrofon sein Eigen nennt, liefert dem Angreifer eine Überwachungsstation mit Bild und Ton“.[67]

[65] Unter „Shell“ (dt. Schale) versteht man die Benutzeroberfläche eines zeichenbasierten Betriebssystems, über die der Nutzer mit dem Rechner kommuniziert. Vorrangige Aufgabe ist das Übernehmen von Befehlen und die Ein- und Ausgabe von Meldungen des Systems. Unter MS-DOS ist „command.com“ gebräuchlich, unter Linux ist die „Standard-Shell“ beispielsweise „bash“.

[66] Hoeren/Sieber – *Sieber* 19 Rn 44 mwN

[67] Plate/Holzmann, Sicherheit in Netzen, 7.8

In Netzen gibt es dann noch Formen der **Tarnung**[68] (engl. *spoofing*), bei der ein Rechner vorgibt, „ein anderer zu sein“. Dies soll im folgenden Kapitel noch näher erläutert werden. In vielen Betriebssystemen existiert der Begriff des „*trusted host*“. Vereinfacht gesprochen sind dies Rechner, denen der eigene Computer auf Grund besonderer Voreinstellungen, die vor allem historisch bedingt sind, vertraut und deren Berechtigung nicht gesondert überprüft wird. Tarnt sich ein fremder Rechner als vertrauenswürdiger Host, wird das Eindringen erleichtert.

Auch diese Liste lässt sich beliebig fortsetzen. Eine Übersicht über etwa 50 gängige Trapdoors und Trojaner findet sich bei „The Trojans Removal Database“.[69]

1.7.1.1.4 Schwachstellen in den Netzwerkprotokollen[70]

Die TCP/IP-Protokollfamilie, die Standard„sprache“ für Datenübertragungen im Internet, wurde vor etwa 20 Jahren entwickelt. Damals wurden Computernetze nahezu ausschließlich für wissenschaftliche Zwecke eingesetzt, so dass die Entwickler Sicherheitsaspekte getrost zu Gunsten von Fehlertoleranzeigenschaften vernachlässigen konnten. Heutzutage dominieren kommerzielle Inhalte das Internet, deren Übertragung verstärkte Sicherheitsmaßnahmen erfordert. Die wesentliche Anforderung an Datenübertragungen in großen Netzwerken besteht darin, plattformunabhängig (Hard- und Software) Verbindungen zwischen unterschiedlichen Hosts zu ermöglichen. Um dies zu gewährleisten, erfolgt eine Schematisierung und Gliederung des Kommunikationsprozesses in wohl definierte, hierarchische Ebenen.[71] Die einzelnen Kommunikationsfunktionen werden bestimmten logischen Schichten zugeordnet. Änderungen auf einer Schicht haben daher keine Auswirkungen auf die anderen Ebenen. Angriffe sind grundsätzlich über alle Schichten denkbar und sollen deshalb in dieser Reihenfolge systematisiert werden. Daher zunächst ein Überblick über die TCP/IP-Netzwerkprotokolle anhand des siebenschichtigen ISO-Referenzmodells:

Application Layer Schichten 5- 7 WWW, Email, etc.
Transport Layer Schicht 4 TCP, UDP
Network Layer Schicht 3 IP
Data Link Layer Schicht 1 und 2 LLC, Hardwareinterface

Abbildung bei Plate/Holzmann, Sicherheit in Netzen, 2.6.

[68] Beschreibung der Funktionsweise von IP-, DNS- und Webspoofing bei Hoeren/Sieber – *Sieber* 19 Rn 36-38
[69] http://www.multimania.com/ilikeit/ (01.01.2004)
[70] Fuhrberg, Sicherheit im Internet, 3 ff., Plate/Holzmann, Sicherheit in Netzen, 2.3.; Wolf/Häger/Schorn, 3.3
[71] Sog. 7-Schichten-Modell der „International Standard Organisation“ (ISO)

Auf der hierarchisch niedrigsten Ebene erfolgt die physikalische Verbindungserstellung (engl. *physical layer*). Hierfür müssen Parameter für die Bit-Übertragung festgelegt werden, wie beispielsweise Pegel, Verkabelung, Stecker, usw. In TCP/IP wird diese Ebene gewöhnlich mit der Sicherungsschicht (engl. *data link layer)* zusammengefasst. Diese ist für die Herstellung einer funktionierenden Verbindung zwischen zwei benachbarten Stationen verantwortlich.[72] Dazu stellt sie einen definierten Rahmen für den Datentransport zur Verfügung und übernimmt die Fehlererkennung und Datensynchronisation. Informationen werden in Blöcke geeigneter Länge zerlegt, die als Datenrahmen (engl. *frames*) bezeichnet und mit einer Prüfinformation für die Fehlererkennung und -korrektur versehen werden.[73] In der hierarchisch nächst höheren Schicht (engl. *network layer*) wird Sorge getragen für die Übertragung der in Schicht 2 erstellten Datenpakete. Dafür werden Datenwege gewählt (engl. *routing*), Verbindungen vor Überlastung geschützt (Flusskontrolle) sowie eine nochmalige, auf die in Schicht 2 aufbauende, Überprüfung einer fehlerfreien Übertragung vorgenommen.[74]

Auf dieser dritten Ebene können komplette Datenübertragungen, einschließlich (unverschlüsselter) Passwörter, durch sog. **Sniffing** (dt. schnüffeln) mitgelesen werden. Ein (Packet-) Sniffer ist ein Programm, das den Datenverkehr im Netzwerk abhört. Technisch wird dies dadurch ermöglicht, dass Datenpakete in Netzwerken grundsätzlich an alle Rechner geschickt werden. Diejenigen Rechner, an die der Datenstrom nicht adressiert ist, verwerfen jedoch die nicht für sie bestimmten Pakete. An dieser Stelle können „Sniffer" ansetzen. Sie speichern die verworfenen Daten und ermöglichen unter Zuhilfenahme entsprechender Filter, ganze Verbindungen zu protokollieren. Auf diese Weise können Passwörter abgehört und fremde Emails mitgelesen werden, sofern diese unverschlüsselt übertragen werden. Sniffer sind nicht etwa obskure Hacker-Tools, sondern gehören bei vielen Betriebssystemen zum Lieferumfang, da sie zum Test und der Fehlersuche in Netzwerken notwendig sind. Bekannte Vertreter sind z.B. „SniffIt", „Etherload", „Netman", „LinkView" oder „LANWatch". Abhilfe kann, wie bereits angedeutet, durch Verschlüsselung (Kryptographie) geschaffen werden.

Die Transportschicht erfüllt – wie der Name schon sagt – eine reine Transportfunktion. Damit alle Datenpakete den richtigen Empfänger erreichen, stellt Schicht 4 eine Datenverbindung zwischen zwei Partnern her, übernimmt den Datentransport, die Flusskontrolle, die Fehlererkennung und Korrektur. Diese Schicht verbirgt die Charakteristika des Netzes (LAN, WAN, usw.) vor den darüber liegenden Schichten. Bei einer Forderung nach höherem Datendurchsatz kann die Transportschicht mehrere Verbindungen zum Partner aufbauen und die Daten in Teilströmen leiten (engl. *splitting*/*combining*).[75]

Auf dieser Ebene können Kommunikationspartner über die Identität ihres Gegenübers getäuscht werden. Beim sog. **IP-Spoofing** (*to spoof,* dt. hereinlegen) werden IP-Adressen der beteiligten Rechner gefälscht. IP-Adressen (engl. *internet protocol address*) sind eindeutige viergliedrige Zahlen, die jedem mit dem Internet verbundenen Rechner vom Zugangsanbieter (z.B. T-Online, AOL, Universitäten, usw.) zugewiesen werden. Dadurch kann er von anderen Rechnern im Netz zweifelsfrei lokalisiert werden, so dass man von einer „elektronischen Hausnummer" sprechen kann. Beim IP-Spoofing wird die ungenügende Überprüfung des Kommunikationspartners unter TCP/IP ausgenutzt, um mit gefälschten IP-Adressen einem Rechner falsche Informationen unterzuschieben. Ermöglicht wird dies durch einen Konzeptionsfehler im TCP/IP-Protokoll, der bereits 1985 entdeckt wurde.[76] Oft werden diese Attacken

[72] Taschenbuch der Informatik – *Löffler*, Kap. 6, S. 208 ff., 216
[73] Taschenbuch der Informatik – *Löffler*, Kap. 6, S. 168, 184, 208, 216
[74] Plate, Grundlagen Computernetze, 1.2
[75] Plate, Grundlagen Computernetze, 1.2
[76] Morris, A Weakness in the 4.2BSD UNIX TCP/IP Software, S. 2 ff.

benutzt, um falsche Routing Informationen an ein System weiterzugeben. Aber auch bei einzelnen Verbindungen kann das Fälschen von IP-Adressen Anwendung finden, wie z.B. beim **Hijacking** (vgl. weiter unten). Dem Eindringling ermöglicht diese Attacke, sich in eine fremde Verbindung „einzuklinken", indem er eine falsche Identität vortäuscht. Ganze Verbindungen können, sofern sie unverschlüsselt erfolgen, abgehört werden.

Beim sog. **Route-Spoofing** versucht ein Angreifer, den Weg der Datenpakete in einem Netzwerk zu beeinflussen. Routing (dt. senden, steuern) bezeichnet das Senden von Datenpaketen über bestimmte Wege im Netzwerk vom Sender zum Empfänger. Gelingt es einem Hacker falsche Informationen an einen Router (Gerät, das den Datenfluss steuert) zu übermitteln, dann kann er Verbindungen auf seinen oder einen anderen Rechner umleiten. Technisch möglich ist die vor allem durch Manipulationen des ***R**outing **I**nformation **P**rotocol* (RIP) und das ***I**nternet **C**ontrol **M**essage **P**rotocol* (ICMP).[77]

DNS-Spoofing zielt auf Manipulationen am Namenssystem des Internets ab. Durch einen ***D**omain **N**ame **S**erver* erfolgt die Übersetzung des Trivialnamens eines Hosts im Internet in die weltweit eindeutige numerische IP-Adresse (z.B. hat der WWW Server der Uni Regensburg die IP Adresse 132.199.1.205, die man statt http://www.uni-regensburg.de in die Adresszeile des Browsers eingeben kann). Bei jedem Zugriff im Internet liefert der DNS die dem symbolischen Namen entsprechende numerische Kennung der Rechner. Gelingt es einem Hacker die Kommunikation zwischen Client und DNS abzuhören, kann er versuchen, dem anfragenden Rechner eine falsche IP-Adresse zukommen zu lassen und so die Verbindung auf eine andere Seite umzulenken. Es ist aber auch möglich, dass der Eindringling die Kontrolle über einen DNS erlangt, beispielsweise durch eine **Denial of Service**-Attacke (mehr dazu weiter unten).[78]

Hijacking (dt. Entführung) stellt eine Kombination der Sniffing- und Spoofing-Angriffe dar. Dabei werden bestehende Verbindungen – im Unterschied zum Spoofing, die auf neue „gefälschte" Verbindungen abzielen – zwischen zwei Rechnern „entführt", d. h. der Angreifer übernimmt die Stelle eines Kommunikationspartners innerhalb einer Verbindung. Da bei einer solchen Übernahme einer Verbindung keine Authentifizierung des Gegenübers mehr durchgeführt wird, kann ein Angreifer großen Schaden anrichten.[79]

Im siebenschichtigen ISO/OSI-Schema bezeichnet die Anwendungsschicht (engl. *application layer)* nur die oberste Ebene. Im TCP/IP-Modell werden die obersten drei Schichten unter dieser Bezeichnung zusammengefasst.[80] Dies bedingt funktionell jedoch keine Unterschiede. Schicht 7 stellt die Verbindung zur jeweiligen Anwendung (Applikation) dar und ist für den Dialog mit den Programmen verantwortlich. Daraus wird deutlich, dass es sich bei dieser Ebene – trotz der missverständlichen Namensgebung – nicht selbst um ein Programm handeln kann, sondern lediglich um eine funktionelle Einheit in einem Kommunikationsschema.[81] Eine Standardisierung ist aber bislang noch in weiter Ferne. Die Anwendungsebene bietet vielfältige Möglichkeiten für Angreifer in ein (geschütztes) Netzwerk einzudringen. Sicherheitslücken ergeben sich sowohl aus Mängeln in der Konzeption und Implementation als auch aus Fehlern in der Konfiguration einzelner Anwendungen.[82]

[77] Taschenbuch der Informatik – *Löffler*, Kap. 6, S. 167, 184 ff.; Plate/Holzmann, Sicherheit in Netzen, 2.7
[78] Hoeren/Sieber – *Sieber* § 19 Rn 36 ff.; Plate/Holzmann, Sicherheit in Netzen, 2.7
[79] Plate/Holzmann, Sicherheit in Netzen, 2.7
[80] Plate, Grundlagen Computernetze, 8; Taschenbuch der Informatik – *Löffler*, Kap. 6, S. 217 f.
[81] Plate, Grundlagen Computernetze, 1.2; Taschenbuch der Informatik – *Löffler*, Kap. 6, S. 210, 212 ff.
[82] Plate/Holzmann, Sicherheit in Netzen, 2.7; Taschenbuch der Informatik – *Plate/Henning*, Kap. 21, S. 710 ff.

Gefahren resultieren vor allem aus der Nutzung aktiver Komponenten im Web, wie z.B. CGI-Skripten, ActiveX, Java, usw.[83] WWW-Seiten können aus passiven (z.B. Text, Grafik, Sound, usw.) wie aktiven Inhalten (Programme, die entweder auf dem WWW-Server oder dem Browser ausgeführt werden) bestehen. Vor letzteren wird in der Presse und Literatur zu Recht gewarnt, da sie schon mehrfach für missbräuchliche Zwecke eingesetzt wurden. Auf Serverseite entstehen Sicherheitsrisiken vor allem bei der Verwendung von CGI-Skripten.[84] Dadurch, dass diese nicht beim Anwender, sondern auf dem Server ausgeführt werden, besteht die Gefahr, dass ein Hacker in der Position eines Benutzers Zugriffsrechte auf den Server bekommt. Auf Anwenderseite bereitet vor allem das Microsoft Produkt „ActiveX" Probleme. Diese Technologie wurde nicht primär für den Einsatz im Internet entwickelt, sondern ist eine Art Nebenprodukt zu *Microsofts* „Component Objekt Model" (COM) Entwicklung, die eine wichtige Komponente in der Windows-Architektur geworden ist. Teile dieser Technologie (z.B. OLE) werden von den meisten Windows-Anwendern, ohne dass sie es wüssten, fast tagtäglich eingesetzt. „**O**bjekt **L**inking and **E**mbedding" ist ein von *Microsoft* entwickeltes Verfahren, das es erlaubt, Dokumente – wie z.B. Excel-Sheets – in Microsoft Office Dokumente einzufügen. „ActiveX"-Elemente werden derzeit nahezu ausschließlich von Microsoft Windows Plattformen in Verbindung mit dem Microsoft Internet Explorer unterstützt. Mit Hilfe von Plug-Ins kann „ActiveX" mittlerweile auch mit Netscape-Browsern genutzt werden. Die von „ActiveX" ausgehenden Gefahren hat der Chaos Computer Club (CCC) bereits 1997 medienwirksam vor Augen geführt. Dazu gingen Vertreter des CCC wie folgt vor:

> *Zunächst wurde auf einem WWW-Server mit dem sinnigen Titel „Millionär in fünf Minuten" ein manipuliertes ActiveX-Control installiert. Betrachtete ein Anwender diese Seite mit dem Internet Explorer und hatte er die Homebanking-Software „Quicken" auf seinem Rechner installiert, so startete das Control diese im Hintergrund und schleuste unbemerkt einen Überweisungsauftrag ein. Bei der nächsten Sammelüberweisung mit „Quicken" wurde das Konto dann um DM 20,- erleichtert.*[85]

„Java" überzeugt im Gegensatz dazu mit fundierteren Überlegungen zum Thema Sicherheit. Dies ist auch nicht weiter verwunderlich, denn im Gegensatz zu „ActiveX" handelt es sich um eine Programmiersprache, die speziell zur Erzeugung interaktiver Inhalte im Internet entworfen wurde.[86] Darüber hinaus wird die von *Netscape* entwickelte Script-Sprache „JavaScript" zur Erzeugung interaktiver Web-Inhalte benutzt. Sie hat mit dem von *Sun* entwickelten Java im Grunde nur einen Namensbestandteil gemeinsam und erreicht keinen vergleichbaren Sicherheitsstandard. „JavaScript" wird nicht kompiliert[87], sondern zur Laufzeit interpretiert. Das erleichtert zwar das Programmieren, schafft jedoch auch Risiken, da keine Fehlerprüfung im Kompilierungslauf erfolgt, durch die sich schwere Programmfehler, die zum Systemabsturz führen können, entdecken ließen.

---

[83] BSI, „Ausführbare Inhalte – Sicherheitsrisiken und Lösungen", http://www.bsi.bund.de/taskforce/literatur/aktivinh.htm#Ausblick; Informationen des CCC zu ActiveX, http://www.ccc.de/activex/ (01.03.2004); Mack DuD 1999, S. 192 ff.; Sicherheitsinfos auf der Homepage von Sun: http://java.sun.com/products/jdk/1.1/knownbugs/index.html (01.03.2004); Sicherheitsratschläge des Rechenzentrums der Universität Münster, http://www.uni-muenster.de/WWW/Sicherheit.html (01.03.2004)

[84] „Common Gateway Interface"*:* Standardisierte Programmierschnittstelle zum Datenaustausch zwischen Browser und Programmen auf dem Webserver. Diese Programme sind überwiegend in „Perl" geschrieben und dienen hauptsächlich der Auswertung von HTML-Formularen.

[85] Die ursprüngliche CCC Pressemitteilung befindet sich auf folgender Mirror-Seite: http://www.iks-jena.de/mitarb/lutz/security/activex.html (01.03.2004)

[86] Ausführliche Darstellung bei Mack DuD 1999, 192 ff.

[87] Ein Kompiler (von engl. *compile*) ist ein Programm, das den Quelltext eines anderen Programms, das in einer bestimmten Programmiersprache vorliegt, in eine für den Computer verständliche Zeichenfolgen übersetzt.

1.7.1.2 Cookies[88]

Cookies (dt. Kekse) können ähnlich wie die Aktivitäten von Hackern den individuellen Geheimbereich verletzen. Es handelt sich um kleine Datenpakete, die beim Besuch einer Website zunächst im Arbeitsspeicher des heimischen Computers gespeichert werden. Übersteigt ihre programmierte Lebensdauer die Dauer der Verbindung mit der besuchten Seite, so werden sie als Textdatei auf die Festplatte geschrieben (sog. persistente Cookies). Mit Hilfe von Cookies können Besucher einer Webseite identifiziert werden, was die Bereitstellung von Komfortfunktionen, wie beispielsweise individualisierte „Warenkörbe", ermöglicht.[89] Sie wurden von Netscape[90] entwickelt und erstmals im Browser „Navigator 1.0" verwendet.

Strafrechtliche Relevanz erlangen vor allem persistente Cookies, die ohne Wissen und Wollen des Betroffenen auf der Festplatte deponiert werden und die Erhebung und Sammlung personenbezogener Daten in großem Umfang ermöglichen (engl. *data mining*). Unternehmen wie „DoubleClick"[91], „Adfly"[92] usw. haben sich darauf spezialisiert, detailliert Kundenprofile zu erstellen und diese gegen Entgelt an Dritte zu überlassen. Dazu werden vor allem kommerzielle Webseiten so präpariert, dass der Browser eines Besuchers Cookies von „Doubleclick" usw. anfordert, ohne die Webseiten jener Unternehmen jemals besucht zu haben. Aus den Cookies können „DoubleClick" usw. auf die Identität und das Konsumverhalten des Betroffenen schließen und diese Informationen an Werbeunternehmen verkaufen.[93] Bedenklich an dieser Praxis ist, dass personenbezogene Daten ohne Wissen und Wollen der Betroffenen und ohne Rücksicht auf Belange des Datenschutzes erhoben, verarbeitet und weitergegeben werden.

Bei der Entwicklung der neusten Browser Generation wurde diese Problematik erkannt. Der Benutzer kann beispielsweise ab dem MS IE 6.0 Sicherheitszonen definieren und Cookies nach programmierter Lebensdauer, Anbieter usw. annehmen oder verweigern. Die neueren Mozilla Browser enthalten einen eigenständigen „Cookie Manager", der die Kontrolle und Verwaltung eines jeden einzelnen Cookies ermöglicht. In Unix/Linux Systemen genügt es, die Leseberechtigung des Browsers in Bezug auf die Cookie-Dateien aufzuheben.

1.7.1.3 Echelon

Die Kommunikation über die weltweiten Datennetze ist nicht nur durch private Eindringlinge, sondern auch von staatlicher Seite gefährdet. Unter dem Codewort **Echelon** betreiben die Unterzeichnerstaaten der sog. *UKUSA*-Vereinbarung von 1948, die USA, Kanada, Großbritannien, Australien und Neuseeland, das wohl größte weltweite Satellitenabhörsystem. Bis vor kurzem wurde sowohl die Existenz des zu Grunde liegenden Vertragswerkswerks als auch die des Abhörsystems in der Öffentlichkeit vehement bestritten. Das Europaparlament setzte schließlich nach jahrelangem Drängen verschiedener Bürgerrechtsvereinigungen einen nichtständigen Ausschuss ein, dessen Berichterstatter Gerhard Schmid am 11.07.2001 seinen knapp 200 Seiten umfassenden Abschlussbericht[94] vorlegte. Als Ergebnis des Berichts bleibt

[88] Weiterführende Informationen unter: http://www.cookiecentral.com/ (01.03.2004)
[89] Taschenbuch der Informatik – *Plate/Henning*, Kap. 21, S. 702; Plate/Holzmann, Sicherheit in Netzen, 7.3
[90] http://www.netscape.com/ (01.03.2004)
[91] http://www.doubleclick.com/ (01.03.2004)
[92] http://www.adfly.com/ (01.03.2004)
[93] Mayer-Schönberger, http://www.cookiecentral.com/content.phtml?area=2&id=1 (01.03.2004); Plate/Holzmann, Sicherheit in Netzen, 7.3
[94] Europaparlament; http://www.europarl.eu.int/tempcom/echelon/rrechelon_en.htm (01.03.2004)

festzuhalten, dass „Echelon“ nunmehr von offizieller Seite bestätigt existiert[95], dass „wahrscheinlich“ Art. 8 EMRK[96] sowie Europa- und Völkerrecht verletzt werden[97], die jährlichen Spionageschäden sich auf ca. 7 Milliarden US $[98] belaufen und dass von staatlicher Seite Aufforderungen[99] an die Betreiber des Spionagesystems ausgesprochen wurden, bis zu deren Umsetzung sich die Betroffenen besser selbst schützen[100] sollen.

1.7.2 Integritätsverletzungen

Nach dem Wortlaut erfassen „Integritätsverletzungen“ Handlungen, die die Unversehrtheit eines Systems oder von Daten beeinträchtigen. Dabei handelt es sich um Fälle der Computermanipulation und -sabotage. Exemplarisch für die zahlreichen Fallgestaltungen soll an dieser Stelle auf die Phänomene „Computerviren“ sowie „0190-Dialer“ eingegangen werden.

1.7.2.1 Viren, Würmer, Hoaxes und Trojaner

Computerviren sind eine Erscheinung, die Mitte der 1980er Jahre zum ersten Mal auftrat. Der Begriff im engeren Sinne geht zurück auf den amerikanischen Wissenschaftler Lenn Adleman von der Universität von Südkalifornien. Die erste umfangreichere Untersuchung stammt von Fred Cohen vom selben Institut, der im Rahmen seiner Dissertation[101] Pionierarbeit auf dem Gebiet leistete. Man vermutet, dass das erste Virus („*Brain*“) von zwei Brüdern aus Pakistan stammt, die frustriert von dem Umstand der Piraterie an ihrer Software ein Programm erstellten, das eine Kopie von sich selbst und einen Copyrightvermerk auf jeder kopierten Diskette erstellte. Mittlerweile haben sich Viren – vor allem über Emails – epidemisch verbreitet. Kommerzielle Schutzprogramme[102] geben an, über ein Archiv von etwa 75.000 Viren, Würmer und Trojaner zu verfügen. Es vergeht fast kein Tag, an dem nicht vor neuen Schadprogrammen „*in the wild“ (ITW)* gewarnt wird.[103] Eine aussagekräftige Statistik hierzu führt das Rechenzentrum der Universität Bern. Ein- und ausgehende Emails werden auf dem zentralen Mailserver gescannt und die Ergebnisse werden im 15-Minuten-Takt aktualisiert im Internet publiziert.[104] Allein im Mai 2002 wurden auf diese Weise über 8.100 Viren entdeckt und unschädlich gemacht.

Nach der auf Cohen zurückgehenden Definition ist ein „Computervirus“ in Anlehnung an sein Pendant aus der Biologie „*[...] a program that can infect other programs by modifying them to include a possibly evolved version of itself.*“ Diese Definition besitzt auch heute noch Gültigkeit und wurde nur geringfügig modifiziert: Unter einem „Computervirus“ versteht das Bundesamt für Sicherheit in der Informationstechnik (BSI) „*[...] eine nicht selbständige Programmroutine, die sich selbst reproduziert und dadurch vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vor-*

[95] Abschlussbericht siehe Fn 94, lit. A), S. 14
[96] Abschlussbericht siehe Fn 94, lit. H), I), J) und K), S. 15 f.
[97] Abschlussbericht siehe Fn 94, lit. F), G), S. 15
[98] Abschlussbericht siehe Fn 94, lit. S), S. 17
[99] Abschlussbericht siehe Fn 94, lit. AA), Ziff. 11 ff., S. 20 ff.
[100] Abschlussbericht siehe Fn 94, lit. AA), Ziff. 27 ff., S. 21 ff.
[101] Cohen, *Computer viruses: theory and experiments*, Ph. D. dissertation, U. of Southern California, 1984
[102] Beispielsweise Sophos Anti-Virus, Version 3.59, Stand 01.06.2002
[103] Sehr gründliche und aktuelle Auswertungen von Viren *itw* bei *The WildList Organization International*, http://wildlist.org/ (01.03.2004)
[104] Informatikdienst der Universität Bern, http://www.id.unibe.ch/network/stats/email/viri/index.shtml (01.03.2004)

nimmt.“[105]

Entscheidend für ein Computervirus ist, dass es wie sein Verwandter aus der Biologie einen Träger benötigt (z.B. Bootsektor, Makro, Programmteil, usw.), um sich zu verbreiten. Darin liegt der wesentliche Unterschied zum **Wurm**, der sich ohne Wirt verbreiten kann, indem er von sich selbst Kopien erstellt. Die Übergänge sind allerdings fließend, da sich manche Viren wie Würmer verhalten, indem sie sich selbst per Email an andere Anwender weiterleiten (z.B. VBS/Kakworm und VBS/LoveLet-A).[106] **Hoaxes** (dt. Scherz, Schabernack) sind keine Schadprogramme, sondern gefälschte Virenmeldungen, die den Anwender meist dazu auffordern, Systemdateien zu löschen, bei denen es sich angeblich um Viren, etc. handelt. Der gute Glaube des Anwenders führt dazu, dass er sich auf diese Weise selbst Schaden zufügt. Der Begriff des **Trojanischen Pferdes** – bzw. Trojaners – wurde bereits in Kapitel 1.7.1.1.3 erläutert. Eine der unerwünschten Nebenfunktionen kann neben dem Öffnen einer „*backdoor“* auch das Einschleusen eines Virenprogramms sein.

Die Schätzungen der von Viren verursachten Schäden gehen weit auseinander. Das EMI gibt unter Berufung auf eine von den ICSA Labs[107] durchgeführte Studie folgende Zahlen an:

Virus	Jahr	Typ	Zeitraum innerhalb dessen „der weltweit am weitesten verbreitete“ Virus	Schäden
Jerusalem, Cascade, Form, etc.	1990	.exe File, Boot Sector	3 Jahre	Für alle Viren im Zeitraum von 5 Jahren US $ 50 Mio.
Concept	1995	Word Makro	4 Monate	US $ 50 Mio.
Melissa	1999	Email, Word Makro	4 Tage	US $ 93- 385 Mio.
Love Bug	2000	Email, VBS	5 Stunden	> US $ 700 Mio.

Quelle: EMI, „Twilight Zones in Cyber Space“, S. 52

Weniger konservative Schätzungen[108] beziffern die Schäden noch weit höher, ohne jedoch die Grundlagen für ihre Erhebungen offen zu legen. Im Mai 2002 wurde der Schöpfer des Virus „Melissa“, David Smith, im US-Bundesstaat New Jersey zu einer Haftstrafe von 20 Monaten sowie zu einer Geldbuße von US $ 5.000,- verurteilt. Nach Angaben des US-Justizministeriums wurde allein durch den „Melissa“-Virus Schäden in Höhe von US $ 80 Mio. verursacht.[109]

[105] BSI, http://www.bsi.bund.de/av/virbro/kap1/kap1_2.htm (01.03.2004)
[106] Oldfield, Von Viren, Würmern und Trojanern, Sophos Plc, http://www.sophos.de (01.03.2004)
[107] ICSA (International Computer Security Association) Labs, http://www.icsalabs.com/html/communities/antivirus/iloveyou/testimony.shtml (01.03.2004)
[108] Computer Economics: *Economic Impact of Malicious Code Attacks*, http://www.computereconomics.com/article.cfm?id=936 (01.03.2004)
[109] U.S. Department of Justice, CCIPS, http://www.cybercrime.gov/cccases.html (01.03.2004)

1.7.2.2 0190-Dialer[110]

Webdialer – darunter fallen auch die 0190-Dialer – sind Programme, die ursprünglich dafür gedacht waren, Internetnutzern die Erstellung einer DFÜ-Verbindung sowie die Abrechnung kostenpflichtiger Netzangebote zu erleichtern. Zu diesem Zweck sollten sie mit Wissen und Wollen des Benutzers eine neue Wählverbindung (nicht möglich bei DSL) zu einem 0190-, 0180-, 0800- oder 118xx-Mehrwertdienst einrichten, über den der jeweilige Anbieter die anfallenden Kosten für den genutzten Service festlegen kann. Die Abrechnung übernimmt der Netzbetreiber (z.B. die Deutsche Telekom AG), der die Sondergebühren über die Telefonrechnung einzieht. Legitime Einsatzzwecke für Dialer sind z.B. der Download kostenpflichtiger Software, Produktsupport und andere Hilfeleistungen im Internet, Nachrichtendienste, Erotikangebote, usw.

Seriöse Anbieter halten sich dabei, wie auch von der Regulierungsbehörde für Telekommunikation und Post (RegTP) gefordert wird, an einen vom *Freiwillige Selbstkontrolle Telefonmehrwertdienste e.V. (FST)*[111] erarbeiteten Verhaltenskodex. Dieser verpflichtet die Anbieter unter anderem dazu, Angaben über Gebühren, Dienstanbieter, vollständige Rufnummer, usw. zu machen. Darüber hinaus ist ein sog. „*opt-in*"-Verfahren für die Einrichtung eines Dialers vorgesehen, d.h. dass sich derartige Programme nur nach ausdrücklicher Bestätigung durch den Benutzer installieren dürfen. Während der Benutzung des kostenpflichtigen Dienstes muss der Tarif je Kanal permanent sichtbar sein; nach Verlassen des entgeltlichen Service darf der Dialer die Verbindung – jedenfalls nicht ohne Wissen und Wollen des Nutzers – aufrechterhalten.[...] [112]

Damit sind auch schon die gängigen Verstöße der unseriösen Anbieter aufgezählt. Dialer installieren sich unbemerkt im Hintergrund, vor allem nach dem Öffnen von „ActiveX"- und „Java"-Elementen (siehe 1.7.1.1.4), geben falsche Tarife an, errichten neben einer bestehenden DSL-Verbindung unbemerkt eine kostenpflichtige Wählverbindung, unterbrechen die Verbindung nach Verlassen des kostenpflichtigen Angebots nicht, usw. Sie modifizieren also im Wesentlichen die DFÜ-Einstellungen und verletzen daher die Integrität des benutzten Systems. Bei Dialern handelt es sich um ein relativ junges Phänomen, das seine Anfänge etwa um die Jahreswende 2000/2001 hatte und seinen Höhepunkt mittlerweile überschritten hat, da die breite Öffentlichkeit gewarnt ist. Am 15.08.2003 ist das Gesetz zur Bekämpfung des Missbrauchs von 0190er-/0900er-Mehrwertdienstenummern[113] vom 09.08.2003 in Kraft getreten.

1.7.3 Beeinträchtigungen der Verfügbarkeit

Von einer Beeinträchtigung der Verfügbarkeit kann man in Anlehnung an die Begriffsbestimmung der „Abteilung für Computerkriminalität und geistiges Eigentum" des US-Justizministeriums (CCIPS) dann sprechen, wenn ein berechtigter Benutzer von rechtzeitigem und sicherem Zugriff auf Daten oder ein System abgehalten wird.[114] Die wohl bekanntesten

[110] Weitergehende Informationen bei http://dialerschutz.de, http://dialerhilfe.de (01.03.2004) und http://trojaner-info.de (01.03.2004)
[111] http://www.fst-ev.org/ (01.03.2004)
[112] http://www.fst-ev.org/ger/verhaltenskodex.html (01.03.2004)
[113] BGBl. 2003 I, S. 1590 ff.
[114] Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division of the U.S. Department of Justice, http://www.cybercrime.gov/ (01.03.2004). Die Seite enthält aktuelle Urteile und Materialien zum Thema Computerkriminalität aus den USA.

Vertreter dieser Fallgruppe sind **DoS-** und **DDoS-**Attacken[115], die im Folgenden näher betrachtet werden.

DoS-Attacken existieren seit den Anfängen des Internets. Ihr unmittelbares Ziel ist es, die Verfügbarkeit bestimmter Rechner und/oder Dienste drastisch einzuschränken. Darüber hinaus sind sie oft Ausgangspunkt für weiterreichende Angriffe. Spätestens seit populäre Webseiten wie *Yahoo*, *Amazon*, *ebay*, *CNN* und andere im Februar 2000[116], sowie *Microsoft* am 16.08.2003[117], Ziele derartiger Sabotageakte wurden, ist der Begriff auch hier zu Lande bekannt. Die betroffenen Rechner waren stundenlang nicht funktionsfähig, so dass Schäden in schwer bezifferbarer Höhe entstanden. *Reine DoS-Angriffe verfolgen nicht die Absicht, vertrauliche Daten zu stehlen oder Benutzer-Authentifizierungs-Mechanismen zu umgehen, sondern Dienstanbieter lahm zu legen.*[118] *Daneben werden sie jedoch auch eingesetzt, um Computersysteme „teilweise" abstürzen zu lassen, wodurch Sicherheitsmechanismen ausgehebelt werden können.*

Bei einer DoS-Attacke wird ausgenutzt, dass jeder Rechner nur begrenzte Ressourcen (Speicher, Rechenzeit, usw.) hat. Schafft man es, eines dieser Elemente, die zum ordnungsgemäßen Systembetrieb erforderlich sind, zu überlasten, so kann das ganze System damit lahm gelegt werden. Die Clients werden nicht mehr bedient und „nichts geht mehr". Derselbe Effekt kann darüber hinaus durch gezielte Manipulation an Schwachstellen in Betriebssystemen und Netzwerkprotokollen erzielt werden.

Einer **DDoS**-Attacke liegt das gleiche Prinzip zu Grunde. Dabei bemächtigen sich die Angreifer einer Anzahl fremder Computer – beispielsweise durch Verbreitung von Schadprogrammen – und lassen von dort vollautomatisch gewaltige Datenmengen an den Zielrechner schicken. Dieser ist der Datenflut in der Regel nicht gewachsen und stellt entweder jegliche Kommunikation mit der Außenwelt ein oder, was noch schlimmer ist, die attackierten Dienste stürzen ab und das verbleibende System gibt dem Hacker vollen (Administratoren) Zugriff. Bei DDoS-Attacken ist das Zielsystem in wenigen Sekunden einem Datenverkehr ausgesetzt, wie ihn kleine Webseiten in einem Jahr nicht erfahren. Im Falle von Yahoo gehen Schätzungen von 1 Gbit/s aus.[119]

Die Begriffe „DoS" und „DDoS" stellen eine Sammelbezeichnung für eine Vielzahl von Angriffsvarianten dar. Gängige Techniken verbergen sich hinter klangvollen Namen wie „Ping of Death", „Smurf" oder „Out of band".[120] Ihre große Popularität in den letzten Jahren ist darauf zurückzuführen, dass bis heute die Sicherheitsstandards der Betriebssysteme und Netzwerkprotokolle nur wenig verbessert wurden. Wie bereits eingangs erwähnt, ist dies auch nicht weiter verwunderlich, da das Internet als Wissenschaftsnetz nicht zum Transport kommerzieller Inhalte konzipiert war. Für die Sicherheit vor DoS/DDoS-Attacken hat daher bis auf weiteres jeder Anwender individuell zu sorgen.

[115] Siehe auch: Überblick des CERT (*Computer Emergency Response Team*) Coordination Centers vom 02.10.1997, http://www.cert.org/tech_tips/denial_of_service.html
[116] Meldung bei „heise online" vom 11.02.2000, http://www.heise.de/newsticker/data/chr-11.02.00-002/default.shtml
[117] Siehe Microsoft Security Bulletin MS03-026, http://www.microsoft.com/germany/ (01.03.2004)
[118] Informationsbulletin des DFN (Deutsches Forschungsnetz) CERT vom 05.06.2000 zu DDoS Attacken, http://www.cert.dfn.de/infoserv/dib/dib-2000-01.html
[119] Vogel, DDoS, 1.2.1, S.8
[120] Ausführlich und mit technischen Details: Ruef, DoS, Kap. 2 ff.

1.7.4 Rechtswidrige Inhalte

Neben technologiespezifischen, neuen Formen der Kriminalität werden die modernen Medien auch zur Begehung bereits bekannter Delikte benutzt. Als populäre Beispiele werden Tauschbörsen im Internet (engl. *filesharing)* sowie die Verbreitung pornografischer, rassistischer und extremistischer Inhalte erläutert.

1.7.4.1 „Filesharing“[121] und Urheberrechte

Das wohl bekannteste Beispiel im Filesharing-Bereich stellt die Musiktauschbörse „Napster“ dar. Nach zahlreichen Klagen der RIAA (*Recording Industry Association of America*)[122] wegen Urheberrechtsverletzungen musste das Unternehmen zwar am 04.06.2002 Gläubigerschutz nach Chapter 11 des US-Konkursrechts beantragten. Seit dem 29.10.2003 ist die Tauschplattform jedoch mit anderem Inhalt und Konzept unter dem Namen „Napster 2.0“ wieder online.[123]

Die Idee hinter der Napster-Software geht zurück auf den damals 19-jährigen Studenten Shawn Fanning aus Boston, USA. Ende 1999 präsentierte er der Welt eine revolutionäre Möglichkeit, Musikdateien komfortabel über das Internet zu tauschen. Die von ihm entwickelte Software fungierte dabei als elektronische Kleinanzeigenseite, die zwischen Angebot und Nachfrage teilnehmender Musikliebhaber vermittelte. Benutzer der „Napster Community“ gaben mithilfe eines schlichten Clientprogramms Bereiche auf ihrer Festplatte frei, von denen andere Teilnehmer Musikdateien – in der Regel im Platz sparenden MP3-Format[124] – herunterladen konnten. Im Gegenzug stellten jene wiederum Titel auf ihren Computern bereit, so dass alle Beteiligten wechselseitig voneinander profitierten. Um ein bestimmtes Musikstück im Napster-Netzwerk zu lokalisieren, schickte das Client-Programm eine Anfrage an einen der Napster-Server, die ein fortlaufend aktualisiertes Verzeichnis aller vorhandenen Titel beherbergten. Die Austauchbeziehung wurde danach unmittelbar zwischen den Benutzern aufgenommen. Die Napster-Server waren daran nicht beteiligt, bildeten jedoch wegen ihrer zentralen Rolle beim Auffinden von Musikstücken, das virtuelle Rückrat einer globalen, dezentralisierten Musikbibliothek. Der Erfolg dieses Modells basierte im Wesentlichen auf dem Fortschritt der Computer-Technologie, der eine qualitativ hochwertige Digitalisierung von Musiktiteln erlaubte, die mithilfe moderner Komprimierungsverfahren (beispielsweise MP3)[125] Platz sparend verkleinert und über moderne Breitbandnetze global ausgetauscht werden konnten.

Das Napster-Netzwerk ist zunächst explosionsartig gewachsen. Im Jahr 2000 berichteten die Internet Service Provider (ISP), dass der Begriff „Napster“ der am häufigsten in ihre Suchmaschinen eingegebene Terminus war. 2001 gab es nach Schätzungen 70 Millionen registrierte Benutzer (was allerdings zweifelhaft ist, da jeder User mehrere Benutzerkonten einrichten

[121] Zu Deutsch sinngemäß: *Tauschbörse*

[122] Verband der US-Plattenindustrie *RIAA* (*Record Industry Association of America*), dem weltweit agierende Medienkonzerne wie *Seagram/Universal*, die Bertelsmann Tochter *BMG* und *Sony Music* angeschlossen sind,

[123] Napster Pressemeldung vom 29.10.2003: http://www.napster.com/press_releases/pr_031029.html; Meldung bei „heise online“ vom gleichen Tag: http://www.heise.de/newsticker/result.xhtml?url=/newsticker/meldung/41511&words=Napster%202%200

[124] Abkürzung für MPEG Layer 3. Am „Fraunhofer Institut“ entwickeltes Komprimierungsverfahren, das es erlaubt, digitale Audiodateien nahezu ohne Qualitätsverlust auf ein Zehntel ihrer ursprünglichen Größe zu verkleinern.

[125] Gampp GRURInt 2003, 991 (991); Hänel, JurPC Web-Dok. 245/2000, Abs. 2; Heghmanns MMR 2004, 14 (14)

konnte), die monatlich bis zu 2,8 Milliarden Dateien (Höhepunkt Februar 2001) heruntergeladen.[126] Dieser phänomenale „Erfolg" von Napster blieb der Musikindustrie nicht verborgen, da der „kostenlose" Tausch zwischen den Mitgliedern der Napster-Community zumeist ohne Rücksicht auf fremde Urheber- und Nutzungsrechte erfolgte.[127] Zwar wurde auch der Austausch analoger Tonträger, der vor der Filesharing-Ära praktiziert wurde, von der Musikindustrie nicht begrüßt. Jedoch war er aus technischen Gründen vorwiegend auf den Familien- und Freundeskreis beschränkt und damit überschaubar.[128]

Der Verband der US-Plattenindustrie *RIAA* (*Record Industry Association of America*), dem weltweit agierende Medienkonzerne wie *Seagram/Universal*, die Bertelsmann Tochter *BMG* und *Sony Music* angeschlossen sind, erreicht schließlich auf gerichtlichem Weg, dass Napster zunächst eine Filtersoftware implementieren musste, um alle geschützten Werke aus dem Netzwerk zu entfernen. Die Zahl der Downloads fiel daraufhin auf 400.000 Dateien pro Monat, was einer Abnahme der Nachfrage von knapp 99,99 % in weniger als sechs Monaten entsprach.[129] Die Werbeeinnahmen blieben aus, so dass Napster Unterstützung bei der Bertelsmann Mediengruppe suchte. Nach einer strategischen Allianz, die bereits am 31.10.2000 geschlossen worden war, wurde das Unternehmen am 18.05.2002 vollständig in die Bertelsmann Mediengruppe eingegliedert. Dies konnte den Niedergang jedoch nicht abwenden und Napster musste, wie bereits dargestellt, im Sommer 2002 Gläubigerschutz beantragen.

Mit dem Fall von Napster sind die Filesharing-Plattformen jedoch keineswegs aus dem Internet verschwunden. Ganz im Gegenteil wurde das Vakuum, das der wohl bekannteste Dienst hinterließ, nicht nur rasch aufgefüllt, sondern die Nachfolger verfügen nunmehr über neue Charakteristika, die ihre Verfolgung in tatsächlicher und juristischer Hinsicht zum Teil erheblich erschweren. Die Vertreter der zweiten Generation der P2P-(*peer to peer*, dt. gleich zu gleich bzw. Person zu Person) Netzwerke sind weitgehend dezentral aufgebaut[130] und teilweise als *Open Source Software* (dt. offener Quellcode) konzipiert[131], d.h. für jedermann frei veränderbar, so dass es nahezu unmöglich ist, einen bestimmten Rechtsträger für die urheberrechtlichen Folgen des Programms verantwortlich zu machen. Bekannte Netzwerke sind beispielsweise „eDonkey", „Overnet", „FastTrack" und „Gnutella". Sie basieren zum Teil auf proprietären Protokollen und Clientprogrammen – wie beispielsweise Napster und „eDonkey" – können jedoch auch als interoperable (z.B. „FastTrack"[132]) oder offene Netzwerke (z.B. „Gnutella"[133]) konzipiert sein. Die Vielzahl der Netzwerke und Clientprogramme wurde in den letzten Jahren nahezu unüberschaubar.[134]

Die neuen Filesharing-Plattformen brachten nicht nur technische, sondern auch inhaltliche Änderungen. Neben Audiodateien im MP3 Format werden mit stetig steigender Tendenz komplette Filme getauscht. Ermöglicht wurde dies, ähnlich wie zuvor in Bezug auf Audiodateien, durch die Digitaltechnologie, verbesserte Datei-Kompressionsverfahren[135] sowie die

[126] EIM, Twilight Zones in Cyberspace: Crimes, Risk, Surveillance and User-Driven Dynamics, S. 63
[127] Hänel, JurPC Web-Dok. 245/2000, Abs. 3 f.
[128] Gampp GRURInt 2003, 991 (991)
[129] EIM, Twilight Zones in Cyberspace: Crimes, Risk, Surveillance and User-Driven Dynamics, S. 63
[130] Hänel, JurPC Web-Dok. 245/2000, Abs. 28; Heghmanns MMR 2004, 14 (14 f.)
[131] Beispielsweise das „Gnutella"-Netzwerk. Die Client-Programme heißen etwa „BearShare", „Morpheus", „LimeWire", usw.. Detaillierte Informationen auf der Homepage, http://www.gnutella.com/news/4210 (01.03.2004)
[132] Detaillierte Informationen auf der Homepage des australischen Unternehmens „Sharmann Networks", das seit Januar 2002 den „FastTrack" Client „KaZaA" entwickelt und vertreibt, http://www.sharmannetworks.com/ (01.03.2004)
[133] Siehe Fn 131
[134] Grundlegend zum Ganzen: http://www.kefk.net/P2P/Website/Language/index_de.asp (01.03.2004)
[135] Beispielsweise „DivX", „OpenDivX", „XviD", usw.

steigenden Bandbreiten privater Internetanschlüsse (beispielsweise T-DSL). Die Spielfilme werden entweder im Kino mit Digitalkameras abgefilmt oder gelangen als Vorabversion (engl. *screener*) durch Mitarbeiter der Produktions- und Schneidefirmen usw. in den Verkehr.[136] Verbreitet ist auch das „Rippen“[137] von DVDs, die vor allem in den USA früher erscheinen als in anderen Teilen der Welt.

Die Internationalen und Nordamerikanischen Verbände der Spielfilmindustrie *MPA*[138] *MPAA*[139] schätzen die jährlichen Verluste, die durch Filmpiraterie in den USA entstehen, auf über 3 Mrd. US $.[140] Welcher Anteil davon auf Filesharing-Dienste im Internet entfällt, lässt sich nicht beziffern. Nach Schätzungen des *IFPI*[141], einer internationalen Dachorganisation der Plattenindustrie, der etwa 1400 Unternehmen in 70 Ländern angehören, benutzten im Mai 2002 ca. 3 Mio. User P2P-Dienste und konnten auf ca. 500 Mio. Musikdateien zugreifen, von denen 99 % unter Verstoß gegen Bestimmungen des Urheberrechts in das Internet gelangt waren.[142] Insbesondere die Ausweitung des Filesharing auf Hollywoodfilme und Software hat zu einer massiven Ausweitung gerichtlicher Verfahren gegen Benutzer und Programmierer entsprechender Software geführt.

1.7.4.2 Extremistische, rassistische und pornografische Inhalte

Auf Grund der einzigartigen Möglichkeiten des Internets, kostengünstig, schnell und anonym[143] mit einer breiten Weltöffentlichkeit zu kommunizieren, wurde und wird es in großem Umfang zur Verbreitung rechtswidriger Inhalte eingesetzt.

Eine behördliche Inhaltskontrolle ist nahezu unmöglich. Dies hat das Ermittlungsverfahren gegen die linksradikale Zeitschrift „Radikal“ deutlich vor Augen geführt. Auf Initiative des deutschen Generalbundesanwaltes sperrten verschiedene deutsche Zugangsanbieter die Netzadressen des niederländischen Webhosters „XS4ALL“, „www.xs4all.nl“ und „www.serve.com“, der auf seinen Servern eine digitale Ausgabe (Nr. 154) des in Deutschland verbotenen Druckwerks bereit hielt. Als Konsequenz konnten alle von „XS4ALL“ vermittelten Webseiten (ca. 6000), unabhängig vom jeweiligen Inhalt, in Deutschland nicht mehr abgerufen werden, während die beanstandete Zeitschrift in kürzester Zeit auf 36 anderen WWW- und FTP-Servern gespiegelt (engl. *mirror server*), d.h. als Kopie bereit gehalten wurde. Der renommierte DFN-Verein[144], der wie die anderen Zugangsanbieter am 11.04.1997 eine Sperrung der Adressen vorgenommen hatte, hob diese daher als erster bereits am 21.04.1997 wieder auf. Als Begründung gab die Pressestelle an, dass durch die festgestellte anderweitige Verbreitung der gesperrten Seite der Beweis erbracht worden sei, dass sich einzelne Informa-

[136] Ein populäres Beispiel ist der Hollywood-Streifen „The Hulk“, der noch vor dem offiziellen Kinostart in den USA im Internet war. Der für die Weitergabe der Kopie Verantwortliche wurde identifiziert und zu sechs Monaten Hausarrest sowie einer Geldstrafe verurteilt, „heise online“, 28.09.2003, http://www.heise.de/newsticker/result.xhtml?url=/newsticker/meldung/40655&words=Gonzales%20Hulk; Weitergabe von Vorabversionen durch Mitglieder der „Oscar“-Jury: „heise online“, 23.01.2004, http://www.heise.de/newsticker/result.xhtml?url=/newsticker/meldung/43935&words=DVD%20Oscar

[137] Bitweise Kopie von einem Datenträger auf die Festplatte eines Computers. Dadurch können beispielsweise Kopierschutzmechanismen umgangen werden.

[138] *Motion Picture Association*

[139] *Motion Picture Association of America*

[140] http://www.mpaa.org/anti-piracy/ (01.03.2004)

[141] *International Federation of the Record Industry*

[142] IFPI, IFPI Music Piracy Report June 2002, S. 10, http://www.ifpi.org/ (01.03.2004)

[143] Gegebenenfalls durch die Verwendung sog. Anonymisierungsdienste, z.B. http://www.anonymiser.com/ (01.03.2004)

[144] Betreiber des deutschen Forschungsnetzes G-WIN, http://www.dfn.de/ (01.03.2004)

tionen nicht sperren ließen und dass die Sperrung daher nicht mehr zumutbar sei.[145] Eben sowenig wie sich linksradikales Gedankengut aus dem Internet entfernen lässt, gelingt dies mit rechtsextremistischen WWW-Seiten. 2002 beobachtete das Bundesamt für Verfassungsschutz allein 1000 Homepages aus dem rechtsradikalen Spektrum, die von Deutschen betrieben wurden (2001: 1.300).[146] Die Seiten liegen zum großen Teil auf Servern im Ausland, um sie dem Zugriff deutscher Behörden und Gerichte zu entziehen.

Da sich bestimmte Inhalte durch behördliche und polizeiliche Maßnahmen kaum aus den globalen Netzen entfernen lassen, bleibt daher allein die freiwillige Selbstkontrolle durch die Anbieter. In Deutschland entstand 1997, in etwa gleichzeitig mit dem Inkrafttreten des TDG, der „Freiwillige Selbstkontrolle Multimedia Diensteanbieter e.V. (FSM e.V.)“[147], dem zahlreiche ISP und Interessenverbände angehören. Auf europäischer Ebene wurde als Dachorganisation „The Association of Internet Hotline Providers in Europe (INHOPE)“ gegründet.[148] Bei einer Beschwerde wird zunächst Kontakt mit dem Anbieter aufgenommen verbunden, mit einer Bitte um Stellungnahme, wodurch sich nach Angaben des FSM-Vorstandes, Arthur Waldenberger, bereits 80 % der Beschwerden von selbst erledigen.[149] Schafft der Anbieter keine Abhilfe und liegt der Verdacht einer Straftat vor, schaltet der FSM die Behörden ein, die freilich nur gegen inländische Anbieter vorgehen können.

Eine andere Form der Inhaltskontrolle wird durch die „Internet Content Rating Association (ICRT)“, hinter der die Bertelsmannstiftung steht, angestrebt. Per Fragebogen gibt der Webautor eine Beschreibung seiner Seite ab, die daraufhin von der *ICRT* eingestuft wird. Abhängig von der Bewertung wird eine Art „elektronisches Etikett“ erstellt, das der Autor auf seiner Seite anbringt. Diese mit bloßem Auge unsichtbare Kennzeichnung wird in der XML-(Extensible Markup Language) Sprache „PICS“ (*Platform for Internet Content Selection*) auf der Webseite angebracht und von jedem neueren Browser erkannt. Eltern können durch dieses Verfahren eine graduelle Abstufung derjenigen Inhalte vornehmen, die sie ihren Kindern zugänglich machen wollen. Die Nachteile liegen darin, dass die Bewertung dem Anstands- und Sittengefühl der ICRT überlassen bleibt und dass dieses Verfahren zwingend die Kooperation der Webautoren erfordert.

1.8 Statistik

Das Phänomen „Computerkriminalität“ ist zahlenmäßig nur schwer zu erfassen, da eine Begriffsdefinition (vgl. Kapitel 1.7) bislang noch aussteht. Die den deutschen Ermittlungsbehörden bekannt gewordenen Straftaten werden in der jährlich geführten Polizeilichen Kriminalstatistik (PKS) erfasst.[150] Darin erscheinen die Fälle, die der Polizei im Rahmen von Ermittlungsverfahren hinreichend bekannt geworden sind, d.h. es müssen überprüfbare Anhaltspunkte für Tatbestand, Zeitpunkt, Ort, Beteiligte, usw. vorliegen.[151] Auf eine Verurteilung

[145] Pressemitteilung des DFN vom 21.04.1997, http://www.dfn.de/service/ra/archiv/sperrung.html; Hoeren/Sieber – *Sieber* 19 Rn 107 ff., 201 ff.; „heise online“, 09.09.1996, http://www.heise.de/newsticker/result.xhtml?url=/newsticker/data/un-09.09.96-000/default.shtml&words=radikal; 17.04.1997 http://www.heise.de/newsticker/result.xhtml?url=/newsticker/data/un-17.04.97-000/default.shtml&words=radikal

[146] Verfassungsschutzbericht 2002, S. 107 ff.

[147] http://www.fsm.de/ (01.03.2004)

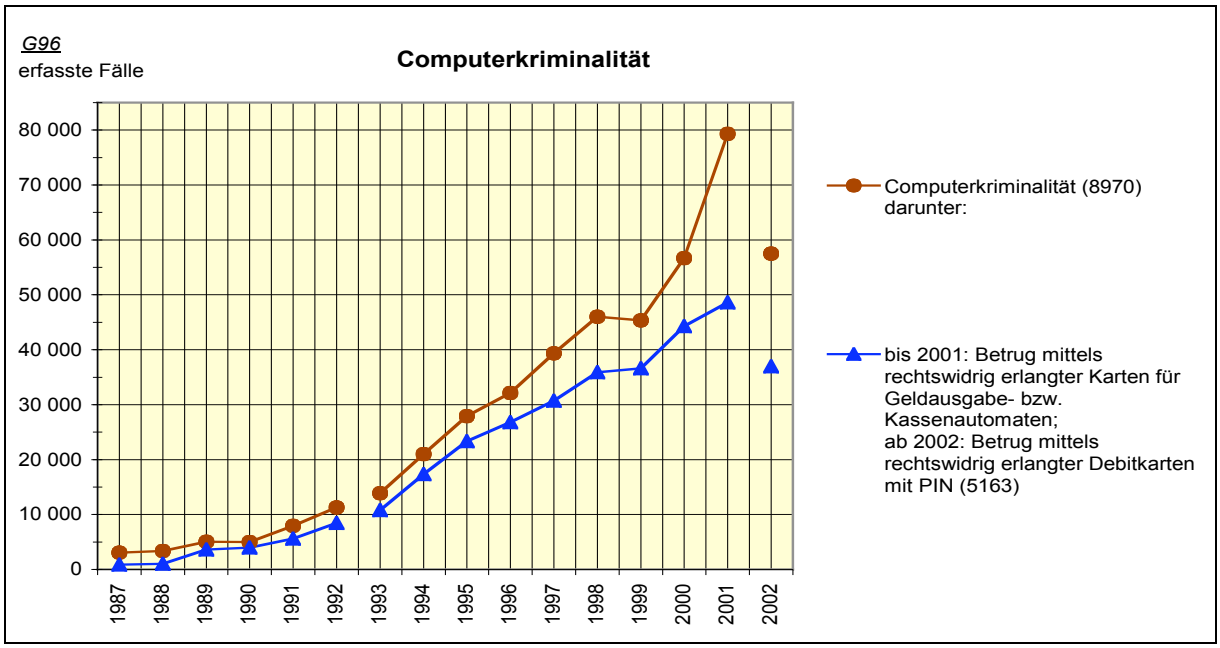
[148] http://www.inhope.org/ (01.03.2004)

[149] Krempl “telepolis” 09.03.2001, http://www.heise.de/tp/deutsch/inhalt/te/7103/1.html

[150] Elektronische Version über die Homepage des BKA verfügbar, http://www.bka.de/ (01.03.2004)

[151] PKS 2002, Vorbemerkung, lit. D, S. 19 ff.

kommt es nicht an. In Bezug auf die Aussagekraft dieser Statistik wird in der PKS zu Recht darauf hingewiesen, dass auf Grund eines schwer abschätzbaren Dunkelfeldes bei den Ermittlungen „kein getreues Bild der Kriminalitätswirklichkeit gegeben werden kann, sondern nur eine mehr oder weniger starke Annäherung an die Realität.“[152] Eine Differenzierung zwischen Datennetz- und sonstiger im Zusammenhang mit Computern stehender Kriminalität erfolgt in der PKS nicht. Unter dem Stichwort „Computerkriminalität“ wurden folgende Delikte erfasst: Betrug mittels rechtswidrig erlangter Debitkarten mit PIN, Computerbetrug (§ 263a StGB), Betrug mit Zugangsberechtigung zu Kommunikationsdiensten, Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung (§§ 269, 270 StGB), Datenveränderung, Computersabotage (§§ 303a, 303b StGB), private und gewerbliche Softwarepiraterie. Betrug mittels Scheck-/Kreditkarten ohne PIN (Lastschriftverfahren) wurden im Jahr 2002 erstmals nicht mehr als Computerkriminalität erfasst. Vor allem dadurch lässt sich der starke Rückgang im Jahr 2002 erklären. Insgesamt fällt auf, dass Betrug mittels Debitkarten in der PKS die überwiegende Mehrheit von Computerdelikten ausmacht. Bemerkenswert ist darüber hinaus, dass es im Bereich der Softwarepiraterie und Datenveränderung/Computersabotage starke prozentuale Zunahmen im Vergleich zum Vorjahr gab.



Hinweis:
1987 – 1990: alte Länder
1991 – 1992: alte Länder mit Berlin
ab 1993: Bundesgebiet insgesamt
1998: Wegen zusätzlicher Aufnahme von Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten (Schlüssel: 5179) ist ein Vergleich der Computerkriminalität (8970) zum Vorjahr beeinträchtigt.

Quelle: BMI, Polizeiliche Kriminalstatistik 2002, S. 238

Neben amtlichen Statistiken liefern zunehmend private Umfragen aussagekräftige Zahlen. In diesem Bereich ist beispielsweise die Studie der Zeitschrift für „Kommunikations- und EDV Sicherheit“ (KES) zu nennen, die alle zwei Jahre Unternehmen und Behörden in Deutschland, Österreich und der Schweiz befragt.[153] Die letzte Studie wurde 2002 in Zusammenarbeit mit

[152] PKS 2002, Vorbemerkung, lit. A, S. 7 ff.
[153] Lagebericht zur IT-Sicherheit, KES 2002 Nr. 3 und Nr. 4; online verfügbar unter http://www.kes.info/studie2002/index.htm

der Wirtschaftsberatung *KPMG* durchgeführt. Insgesamt machten 260 Teilnehmer aus Wirtschaft und Verwaltung Angaben zum Thema IT-Sicherheit. In Bezug auf das Internet gaben 63 % der Befragten an, Ziel von Angriffsversuchen gegen die Verfügbarkeit, Vertraulichkeit und Integrität ihrer Daten und Systeme gewesen zu sein. Spitzenreiter bei den Nennungen waren Hack-Versuche sowie DoS-Attacken. Bei den Webservern kam auf den vorderen Plätzen die Entstellung von Webseiten, (engl. *defacement*) hinzu. Die Dunkelziffer lässt sich allerdings nur schwer abschätzen, da die meisten Unternehmen über keine „Intrusion Detection Systeme“ verfügen, so dass Angriffe teilweise (noch) nicht bemerkt wurden.

Aus dem Mutterland der Computertechnologie verdient vor allem die seit 1995 jährlich durchgeführte Studie des „Computer Security Institute (CSI)“[154] und der „Computer Intrusion Squad“ der US-amerikanischen Bundespolizei FBI besonderes Augenmerk. In der Umfrage wird unter anderem versucht, die Kosten der Computerkriminalität zu erfassen. Spitzenposition nehmen danach der Diebstahl geschützter bzw. geheimer Informationen (engl. *proprietary information*) sowie DoS-Angriffe ein. Der geschätzte Schaden stieg von ca. 100 Millionen US $ 1997 zunächst auf über 455 Millionen US $ im Jahr 2002 an, um 2003 wieder auf ca. 200 Millionen US $ zu fallen. Unklar an dieser Studie bleibt, anhand welcher Methoden die Betroffenen die Schadenshöhe feststellten.

[154] http://www.gocsi.com/ (01.03.2004)

2 Begriffsbestimmungen

Kapitel I der Konvention enthält in Art. 1 Begriffsbestimmungen mit Geltung für das gesamte Übereinkommen. Es stellt daher einen „allgemeinen Teil“ mit einheitlichen Definitionen dar, der im deutschen Strafrecht bislang keine Entsprechung findet. Bei den vier Begriffsbestimmungen in Art. 1 der Konvention kommt es dem Sachverständigenausschuss des Europarats (PC-CY)[155] ausweislich des Erläuternden Berichts[156] nicht darauf an, die Unterzeichner zu einer wörtlichen Übernahme in nationales Recht zu verpflichten. Es genügt vielmehr, wenn die Grundsätze in einer mit der Konvention zu vereinbarenden Weise übernommen werden.[157]

Artikel 1 – Begriffsbestimmungen[158]

Im Sinne dieses Übereinkommens bedeutet

a) „Computersystem“ eine Vorrichtung oder eine Gruppe verbundener oder zusammenhängender Vorrichtungen, die einzeln oder zu mehreren auf der Grundlage eines Programms die automatische Datenverarbeitung durchführen;

b) „Computerdaten“ jede Darstellung von Fakten, Informationen oder Konzepten in einer für die Verarbeitung in einem Computersystem geeigneten Form einschließlich eines Programms, das geeignet ist, ein Computersystem zur Durchführung einer Funktion zu veranlassen;

c) „Dienstanbieter“

- *i) jede öffentliche oder private Organisation, die Nutzern ihres Dienstes ermöglicht, mit Hilfe eines Computersystems zu kommunizieren;*
- *ii) jede andere Organisation, die für diesen Kommunikationsdienst oder für Nutzer dieses Dienstes Computerdaten verarbeitet oder speichert.*

d) „Verbindungsdaten“ alle Computerdaten in Zusammenhang mit einer Kommunikation mit Hilfe eines Computersystems, die von einem Computersystem, das Teil der Kommunikationskette war, erzeugt wurden und aus denen Ursprung, Bestimmung, Leitweg, Uhrzeit, Datum, Umfang oder Dauer der Kommunikation oder die Art des Trägerdienstes hervorgehen.

2.1 Artikel 1 lit. a) – Computersystem[159]

Art. 1 lit. a) versteht den Begriff des „Computersystems“ aufbauend auf dem Konzept der Digitaltechnik in einem weiten Sinn. Es setzt sich zusammen aus der Summe elektronischer Bauteile (Hardware) und nichtkörperlicher Programme (Software), die gemeinsam der automatischen Datenverarbeitung dienen. Hard- und Software werden auf Grund ihrer wechselseitigen Abhängigkeit als Funktionseinheit betrachtet. Mit Datenverarbeitung werden alle Operationen bezeichnet, die mit Hilfe von Computerprogrammen an digitalen Daten durchgeführt werden. Computerprogramme stellen eine Abfolge von Befehlen dar, die einen Computer veranlassen, bestimmte Vorgänge durchzuführen. Sofern diese Verarbeitungsprozesse ohne direkte menschliche Beteiligung erfolgen, handelt es sich um eine automatische Datenverar-

[155] Siehe Kapitel 1.3 „Entstehung der Konvention“.
[156] Zur Bedeutung des Erläuternden Berichts (engl. *Explanatory Report*) siehe Kapitel 1.5 „Überblick über die Konvention und den Gang der Darstellung“ a.E.
[157] Explanatory Report (ER) Ziff. 22
[158] Der deutsche Wortlaut entspricht der Arbeitsübersetzung des BMJ vom 25.05.2001; siehe auch Fn 36.
[159] ER Ziff. 23-24

beitung. Im Bereich der Hardware werden sämtliche Bauteile erfasst, die an der Durchführung dieser Operationen beteiligt sind, sowie alle Arten von Ein-/Ausgabe- und Speichergeräten. Der Begriff des „Computersystems" im Sinne der Konvention stellt daher eine Sammelbezeichnung für alle an einer automatischen Datenverarbeitung beteiligten Geräte, Bauteile und Programme dar. Er geht über den umgangssprachlichen Computerbegriff hinaus, der sich in Zusammenhang mit der massenhaften Verbreitung von Personal Computern (PCs) herausbildete. Danach wird üblicherweise unterschieden zwischen Computer im Sinne des „Kastens", der Hauptplatine, CPU, Grafik-, Soundkarte sowie sonstige Bauteile, beherbergt, und Peripherie im Sinne unselbstständiger Ein- und Ausgabegeräte wie Drucker, Scanner, usw. Diese Abgrenzung lässt sich heutzutage nicht mehr aufrechterhalten. Als Beispiel seien marktübliche Fotodrucker genannt, die – ohne an eine Zentraleinheit angeschlossen zu sein –, „Flash Memory"-Speicherkarten[160] auslesen und digitale Bilder drucken können. Ermöglicht wird dies durch eigenständige Mikroprozessoren und Speicherelemente im Drucker. Von „unselbstständiger Peripherie" kann daher nicht ohne weiteres die Rede sein, sondern es ist eine Einzelfallbetrachtung geboten. Die Definition des Computersystems in Art. 1 lit. a) der Konvention ist jedenfalls flexibel genug, um auch derartige technische Neuerungen berücksichtigen zu können.[161]

Unklar an der Begriffsbestimmung des Abs. 1 lit. a) bleibt, inwieweit neben Einzelplatzrechnern ohne Netzwerkanschluss auch die Summe aller in einem LAN[162] vernetzten Einzelrechner als ein Computersystem betrachtet werden. Letzteres wird im Wortlaut von Art. 1 lit. a) angedeutet und in den Erläuterungen zu Art. 19 ausdrücklich ausgesprochen.[163] Danach erlaube Art. 19 Abs. 1 die Durchsuchung eines Computersystems (engl. „[…] *one distinct computer system* […]", worunter neben PC und Peripherie auch „lokale Netzwerke" fallen sollen. Art. 19 Abs. 2 beziehe sich hingegen auf überregionale Netze (WAN[164]), die öffentliche Telekommunikationsnetze als Übertragungswege involvieren. Die Erläuterungen zu Abs. 1 legen den Schluss nahe, dass „ein" Computersystem im Sinne des Übereinkommens nicht nur eine Funktionseinheit (Computer und Peripherie) umfasst, sondern darüber hinaus aus einer unbestimmten Vielzahl vernetzter Einzelrechner bestehen kann, solange die Verbindung ohne die Benutzung öffentlicher Übertragungsstrecken erfolgt. Gegen diese Schlussfolgerung spricht, dass Art. 1 lit. a) von „einem" Programm ausgeht. „Mehrere" Computer würden mit „mehreren" Programmen arbeiten. Darüber hinaus würden sich einerseits erhebliche Konsequenzen für die sachliche und persönliche Reichweite von Ermittlungsbefugnissen ergeben, da ein lokales Netzwerk eine unbestimmte Vielzahl einzelner Rechner und dahinter stehender Personen repräsentieren kann. Andererseits kann den Verfassern der Konvention und der erläuternden Materialien unterstellt werden, dass sie die Unterschiede zwischen vernetzten Rechnern und Einzelrechnern kennen. Festzuhalten bleibt daher, dass der Begriff „Computersystem" hierdurch an Trennschärfe verliert, worauf im Rahmen der einzelnen Normen näher einzugehen sein wird.

Die technische Verwirklichung der Vernetzung kann im Übrigen dahinstehen, so dass kabelgebundene wie drahtlose (z.B. Funk, Infrarot, usw.) Verbindungen gleichermaßen zu „verbundenen oder zusammenhängenden Vorrichtungen" im Sinne von Art. 1 lit. a) führen.

---

[160] Bei „Flash-Memory" handelt es sich um einen Typ nicht-flüchtigen Speichers (ROM), d.h. Daten können unabhängig vom Anliegen elektrischer Spannung aufbewahrt werden. Im Unterschied zum ROM-Speicherchip handelt es sich um ein wiederbeschreibbares Medium. Grundsätzlich kann zwischen dem „CompactFlash" und dem „SmartMedia" Standards unterschieden werden, innerhalb derer wiederum eine Vielzahl verschiedener Normierungen anzutreffen sind.

[161] ER Ziff. 23

[162] Engl. *Local Area Network*. Örtlich begrenztes Netzwerk ohne öffentliche Übertragungsstrecken.

[163] ER Ziff. 188; Art. 19 Abs. 1 und Abs. 2

[164] Engl. *Wide Area Network*

2.1.1 Datenverarbeitungsanlage im StGB

Der Begriff des „Computers“ findet sich im deutschen Kernstrafrecht bislang nur in den amtlichen Überschriften zu § 263a StGB, Computerbetrug, sowie § 303b StGB, Computersabotage. Beide Normen wurden durch das 2. WiKG vom 15.05.1986 eingefügt. Im Normtext spricht das StGB von „Datenverarbeitungsvorgängen“ (§ 263a StGB) und „-anlagen“ (§ 303b Abs. 1 Nr. 2 StGB), was verdeutlicht, dass die Begriffe „Computer“ und „Datenverarbeitungsanlage“ synonym verwendet werden. Weder im StGB noch in den Materialien zu §§ 263a und 303b StGB findet sich eine Begriffsbestimmung. In der Kommentarliteratur wird unter einer Datenverarbeitungsanlage eine Funktionseinheit maschinentechnischer Vorrichtungen verstanden, die der Datenverarbeitung dient.[165] Erfasst werden neben den zentralen Bestandteilen (Prozessor, Speicher, usw.) auch die Eingabe- (z.B. Tastatur, Scanner, usw.) und Ausgabegeräte (z.B. Bildschirm, Drucker, usw.), sog. Peripheriegeräte[166], nicht jedoch die Software. Ebenso wenig werden die Übertragungskabel eines lokalen Netzwerkes unter den Begriff „Datenverarbeitungsanlage“ subsumiert.[167] Der Datenverarbeitungsbegriff wurde im Regierungsentwurf zum 2. WiKG bewusst offen gelassen.[168] Jedoch wurde die Formel geprägt, dass „[…] Datenverarbeitung alle technischen Vorgänge umfasse, bei denen durch die Aufnahme von Daten und ihre Verknüpfung nach Programmen Arbeitsergebnisse erzielt werden […]“. Wie wenig aussagekräftig diese Definition ist, zeigt sich daran, dass die Kommentarliteratur den Gesetzeszweck heranzieht, um den Begriff weiter einzuschränken.[169] Daraus soll sich ergeben, dass nur die automatische (im Sinne von elektronischer) Datenverarbeitung gemeint ist sowie nur „konkrete“ Verarbeitungsvorgänge, die dem Ergebnis unmittelbar zu Grunde liegen. Die „menschliche“ Datenverarbeitung beurteilt sich nach § 263 StGB. Auf eine Definition nach technischen Kriterien wurde verzichtet. Das deutsche Strafverfahrensrecht enthält bislang keine Definition des Begriffs „Datenverarbeitungsanlage“.

2.1.2 Vergleich

Die Begriffe „Computersystem“ im Sinne der Konvention und „Datenverarbeitungsanlage“ im Sinne des deutschen StGB unterscheiden sich insofern, als ersterer auch die Software mit einbezieht.

Unklarheiten ergeben sich nach Art. 1 lit. a) hinsichtlich der räumlichen Ausdehnung eines Computersystems in einem LAN. Der Netzwerkbegriff wird im deutschen Strafrecht nicht näher erläutert.

In Bezug auf die Hardware stellt die Konvention konstitutiv auf die Verwendung elektronischer Digitaltechnik ab. „Datenverarbeitungsanlagen“ im deutschen StGB sind dagegen nicht auf bestimmte technische Systeme festgelegt, insbesondere nicht auf die Verwendung digitaler Technologien. Erst unter Heranziehung des Gesetzeszwecks und durch eine Abgrenzung zu § 263 StGB lässt sich eine Einschränkung auf EDV-Systeme vornehmen.

[165] Sch/Sch – *Stree* § 303b Rn 13; Tröndle/Fischer § 303b Rn 4
[166] SK – *Hoyer* (6. Aufl.) § 303b Rn 6
[167] LK – *Tolksdorf* § 303b Rn 23
[168] BT-Drs. 10/318, S. 21
[169] Lackner/Kühl – *Kühl* § 263a Rn 4; LK – *Tiedemann* § 263a Rn 22 sowie Lenckner/Winkelbauer CR 1986, 654 (658), die ausführen, dass der Begriff „Datenverarbeitung“ zwar auf die EDV abziele, diese Einschränkung dem Gesetz jedoch nicht zu entnehmen sei.

2.2 Artikel 1 lit. b) – Computerdaten[170]

Art. 1 lit. b) definiert den Begriff „Computerdaten“ im Anwendungsbereich der Konvention. „Daten“ sind danach eine Art der Darstellung von Fakten, Informationen oder Konzepten. Zu „Computerdaten“ werden sie, wenn sie Inhalte in einer Form verkörpern, die für die Verarbeitung in einem Computersystem geeignet ist. Mit dieser Definition haben sich die Verfasser an ISO-Standards zum Datenbegriff angelehnt. Die ISO-Norm 2382/1 (1993) definiert „Daten“ beispielsweise als „[...] *reinterpretable representation of information in a formalized manner suitable for communication, interpretation, or processing* [...].“ Dieser Erläuterung sind auch Strafvorschriften in den USA und Kanada[171] nachgebildet. Sowohl der Wortlaut von Art. 1 lit. b) als auch die Erläuterungen stellen auf eine direkte Verarbeitbarkeit der Daten durch ein Computersystem ab. Damit werden „menschliche“ Verarbeitungsvorgänge (z.B. Datenerfassung, -eingabe, usw.) ausgeschlossen. Für den „Aggregatzustand“ der Daten bedeutet dies, dass sie nur in digitaler, binärer Codierung „Computerdaten“ im Sinne der Konvention darstellen, da die Verwendung von (elektronischer) Digitaltechnik konstitutives Kriterium für ein „Computersystem“ nach Art. 1 lit. a) ist.

2.2.1 Datenbegriff des StGB

Der deutsche Gesetzgeber sah weder bei den Beratungen zu § 268 StGB[172] im Rahmen des 1.[173] und 2. StrRG[174] noch später bei der Ausarbeitung der einschlägigen Computerdelikte[175] durch das 2. WiKG[176] die Notwendigkeit, den Datenbegriff zu definieren. Eine allgemeine Begriffsbestimmung wird auch im Verfahrensrecht nicht vorgenommen. § 202a Abs. 2 StGB enthält ausweislich des eindeutigen Wortlauts keine Legaldefinition, sondern lediglich Beschränkungen in zweierlei Hinsicht mit Wirkung für die §§ 202a Abs. 1, 274 Abs. 1 Nr. 2, 303a und 303b StGB. Diese gelten nicht für den Datenbegriff der §§ 263a, 268 und 269 StGB, da anders als in der erstgenannten Gruppe von Tatbeständen ein Verweis auf § 202a StGB fehlt. Daraus folgt, dass das StGB wenigstens zwischen zweierlei Arten von Daten unterscheidet.[177] Daten im Sinne der Tatbestände, die auf § 202a Abs. 2 StGB Bezug nehmen und andere, bei denen ein entsprechender Verweis fehlt (§§ 263a, 268 und 269 StGB). Erstere sind nur solche, die „[…] elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übertragen werden.“, § 202a Abs. 2 StGB. Letztere unterliegen nicht der soeben genannten Einschränkung. § 202a Abs. 2 StGB trifft demnach keine Aussage über den Wesensgehalt von Daten, sondern begrenzt lediglich einen vorher nicht definierten allgemeinen Datenbegriff im Rahmen einer Gruppe von Tatbeständen.

In formaler Hinsicht ergibt sich kein Anknüpfungspunkt aus dem Begriff der „Datenverarbeitungsanlage“. Wie im vorigen Kapitel gezeigt, wird der Ausdruck im StGB nicht ausschließlich in Bezug auf EDV-Anlagen verwendet. Erst der Normzusammenhang und -zweck veranlasste die Kommentarliteratur zu einer Einschränkung auf Anlagen, in denen elektronische Verarbeitungsvorgänge stattfinden. Im Übrigen kommen grundsätzlich auch Vorrichtungen in

[170] ER Ziff. 25
[171] Vgl. Canadian Criminal Code, R.S.,c.C-34, s. 342.1 [2]: “[…] *“data” means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer system*[…].”
[172] Erster Schriftlicher Bericht des Sonderausschusses für die Strafrechtsreform, BT-Drs. V/4094, S. 37
[173] BGBl. 1969 I, S. 645 ff.
[174] BGBl. 1969 I, S. 717; in Kraft seit dem 01.01.1975
[175] Beschlussempfehlung und Bericht des Rechtsausschusses: BT-Drs. 10/5058, S. 29
[176] BGBl. 1986 I, S. 721 ff.
[177] Sch/Sch – *Lenckner* § 202a StGB Rn 3 mwN

Betracht, die analoge Daten erarbeiten. Ausgehend von der Hardware kann daher – wenigstens unter Heranziehung formaler Wortlautkriterien – kein Rückschluss auf die zu verarbeitenden Daten unternommen werden.

Historisch gesehen wurde der Datenbegriff das erste Mal im StGB in § 268 StGB verwendet. Bei den Beratungen im Rahmen des 1. und 2. StRG – etwa 20 Jahre vor dem 2. WiKG – wurde der Begriff „Daten" auf den Vorschlag der „Physikalisch-Technischen Bundesanstalt" in Braunschweig in den Tatbestand eingefügt, weil man befürchtete, dass ansonsten das Merkmal der „technischen Aufzeichnungen" zu sehr eingeengt würde.[178] Nach dem damaligen Erkenntnisstand sollten Daten in Anlehnung an einen Entwurf einer DIN-Norm, „[…] durch Zeichen[179] oder kontinuierliche Funktionen[180] auf Grund bekannter oder unterstellter Abmachungen zum Zweck der Verarbeitung dargestellte Informationen […]" sein.[181] Unter „Verarbeitung" versteht die Informationstechnologie die Durchführung mathematischer, umformender, übertragender und speichernder Operationen. Es sollten vor allem speicherbare Informationen erfasst werden, „[…] die der weiteren Verarbeitung in einer Datenverarbeitungsanlage unterliegen […]."[182] Die Begriffe „Daten" und „Rechen- und Messwerte" wurden ursprünglich durch das Kriterium „zum Zwecke der Verarbeitung" unterschieden.[183] Jedoch wurde bald klar, dass auch Daten als Ergebnis der Datenverarbeitung – also nicht nur final zu deren Zweck – zur Vermeidung von Strafbarkeitslücken unter den Schutz der Vorschrift fallen sollten, so dass der Datenbegriff erweitert und verallgemeinert werden musste.[184] In diesem Zusammenhang wurde auch die DIN-Norm 44300 flexibler formuliert, indem durch die Einfügung des Wortes „vorrangig" die Verarbeitung in einer Datenverarbeitungsanlage kein konstitutives Element des (neuen) Datenbegriffs mehr darstellte.[185] Diese Begriffsbestimmung wurde im Rahmen des 2. WiKG nicht weiterentwickelt. Der Gesetzgeber begnügte sich mit dem Hinweis, dass er „[…] wie seinerzeit bei der Einführung des § 268 (Absatz 2) StGB […] keine Notwendigkeit gesehen habe, den Datenbegriff näher zu bestimmen […]."[186] Dieser historische Datenbegriff ist sehr weit. Erfasst werden digitale (Zeichen) wie analoge (kontinuierliche Funktionen) Daten. Es findet keine Beschränkung auf binäre Zeichenfolgen statt, die von modernen PCs und EDV-Anlagen vorausgesetzt werden. Daten im Sinne dieser Definition sind daher beispielsweise auch Computerausdrucke (Abfolge digitaler Zeichen), die von einer EDV-Anlage, anders als die zu Grunde liegenden Dateien, nicht mehr unmittelbar verarbeitet werden können. *Puppe* ist daher darin zuzustimmen, dass dieser Datenbegriff darauf hinausläuft, dass die klassische Urkunde nur ein Sonderfall der Datenspeicherung ist.[187]

In der neueren Literatur wird versucht, den Datenbegriff weiter zu abstrahieren und von der technischen, an den einschlägigen ISO- und DIN- Normen orientierten Betrachtungsweise, zu lösen. Es findet sich vielfach die Definition, dass das einzelne Datum aus einer semantischen und einer syntaktischen Ebene bestünde. Auf der ersten – der semantischen – Ebene befinde sich die Information im Sinne einer Angabe über einen Gegenstand oder Zustand der realen oder irrealen Welt.[188] Die zweite – syntaktische – Ebene übernehme die Darstellung durch

[178] BT-Drs. V/4094, S. 37
[179] Digitale Daten.
[180] Analoge Daten.
[181] BT-Drs. V/4094, S. 37; Entwurf der DIN-Norm 44300, Nr. 16, 1968, „Informationsverarbeitung"
[182] BT-Drs.V/4094, S. 37
[183] BT-Drs. V/4094, S. 37
[184] Sch/Sch – *Cramer* § 268 Rn 11
[185] DIN 44300, Nr. 19 (1988); Möhrenschlager wistra 1986, 128 (132)
[186] BT-Drs. 10/5058, S. 29
[187] NK – *Puppe* § 269 Rn 20
[188] Näher zur Entwicklung des Informationsbegriffs Sieber NJW 1989, 2569 ff.

konventionell festgelegte Zeichen[189], d.h. auf digitale Weise. Warum diese zweite Ebene auf Zeichen beschränkt sei, wodurch analoge Darstellungsformen ausgeschlossen würden, wird von den Anhängern dieser Ansicht nicht näher erläutert. Im Ergebnis wäre dieser Datenbegriff enger als der oben dargestellte historische, da er ausschließlich digitale Daten erfasst. Damit sind jedoch noch keine Computerdaten im Sinne der Konvention beschrieben, denn diese erfordern neben der digitalen eine binäre Kodierung, um unmittelbar durch Computer lesbar zu sein.[190]

Wenn diese Literaturmeinung auch eine engere Beschreibung von Daten erlaubt, als die historische Begriffsbestimmung, die dem § 268 StGB zu Grunde gelegt wurde, ist sie dennoch abzulehnen, da sich keinerlei unterstützende Anhaltspunkte im Wortlaut des Gesetzes finden. Allenfalls Normzusammenhang und -zweck legen – wie schon beim Begriff der Datenverarbeitungsanlage – eine Beschränkung auf einen computerspezifischen Kontext nahe.[191] Selbst in diesem Zusammenhang stellt sich dann jedoch die Frage, ob es sich um unmittelbar computerlesbare Daten handeln muss, d.h. digital-binäre Zeichenfolgen, oder ob auch analoge Daten in Betracht kommen, die über entsprechende Peripherie (beispielsweise Scanner) mittelbar für EDV-Anlagen lesbar werden. *De lege lata* lässt sich diese Frage nicht entscheiden. Wie bereits *Puppe* feststellte, bleibt es daher dabei, dass selbst die klassische Urkunde nur ein Sonderfall der Datenspeicherung ist.[192] Daten im Sinne des StGB sind beliebige Informationen in einer beliebigen Kodierung, d.h. Darstellung.

Wie bereits eingangs dargestellt, enthält § 202a Abs. 2 StGB keine Legaldefinition des Datenbegriffs, sondern lediglich Einschränkungen für § 202a Abs. 1 StGB, sowie diejenigen Tatbestände, die auf ihn verweisen. Aufgrund der untechnischen Formulierung von § 202a Abs. 2 StGB ist in der Literatur umstritten, welche Daten durch diese Vorschrift ausgeschlossen werden. Die Adjektive „elektronisch“ und „magnetisch“ deuten zunächst auf alle nicht computerspezifischen Daten hin, da diese üblicherweise in den genannten Zustandsformen weder „gespeichert“ noch „übertragen“ werden. Allerdings heißt es dann in Abs. 2: „[…] oder sonst nicht unmittelbar wahrnehmbar […], was beispielsweise auch für Aufzeichnungen auf Mikrofiche zutrifft, die keinen Computerbezug haben. Ein Teil der Literatur hat die Defizite in der Formulierung von § 202a Abs. 2 StGB erkannt und fordert, dass eine unmittelbare Wahrnehmbarkeit nur dann nicht vorliege, wenn eine Umsetzung der Daten in andere Zeichen erforderlich sei.[193] Im Ergebnis würde dies für Informationen auf Mikrofiche bedeuten, dass sie keine Daten im Sinne von § 202a Abs. 2 StGB darstellten, da zu ihrer Wahrnehmung keine Transformation, sondern lediglich eine Vergrößerung erforderlich ist. Eine Umwandlung würde jedoch stets bei binären Computerdaten erfolgen müssen, um sie am Bildschirm in einer lesbaren Zeichenfolge darstellen zu können. Dieser Ansatz könnte zwar zu einer brauchbaren Beschreibung des Datenbegriffs führen, ist jedoch mangels Anhaltspunkten im Gesetz abzulehnen. Darüber hinaus kann er keine Erkenntnisse für den Datenbegriff der Tatbestände liefern, die nicht auf § 202a Abs. 2 StGB verweisen.[194]

Die Software fällt nach dem ausdrücklichen Willen des Gesetzgebers[195] jedenfalls unter den

[189] Erstmals bei: Welp IuR 1988, 443 (445); dann bei: LK – *Schünemann* § 202a Rn 3 sowie Schulze-Heimig, S. 20 ff.
[190] Ebenso: Schulze-Heimig, S. 21, 25
[191] Siehe dazu Kapitel 2.1.1.
[192] Siehe Fn 187
[193] LK (10. Auflage) – Jähnke § 202a Rn 4; Sch/Sch – *Lenckner* § 202a Rn 4; SK – *Samson* (6. Aufl.) § 202a Rn 7; aA: SK – *Hoyer* (7. Aufl.) § 202a Rn 4
[194] Lackner/Kühl – *Kühl* § 202a Rn 2; Schmitz JA 1995, 480; Sch/Sch – *Lenckner* § 202a Rn 4
[195] BT-Drs. 10/5058, S. 29

historischen Datenbegriff. Die gegenteilige Argumentation[196] überzeugt nicht, denn auch Programmdaten sind, wenn sie in kompilierter Form vorliegen, nichts anderes als eine durch einen Code (im Sinne einer Programmiersprache) definierte Abfolge kleinster digitaler Informationseinheiten (Bits), die von der CPU abgearbeitet – verarbeitet – werden müssen, damit ein Datenverarbeitungsvorgang gestartet und kontrolliert werden kann.

2.2.2 Vergleich

Der technische Datenbegriff der Konvention ist sowohl enger als der historische als auch der in der Literatur entwickelte Datenbegriff des deutschen StGB. Selbst die Einschränkungen des § 202a Abs. 2 StGB reduzieren das umfassende Verständnis von Daten, dass dem deutschen Strafrecht zu Grunde liegt, nicht auf den in der Konvention verwendeten Begriff.

Historisch gesehen wurden bei der Einführung von § 268 Abs. 2 StGB zwar ebenso wie bei Art. 1 lit. b) der Konvention Anleihen aus der Informationstechnologie geholt. Es hat sich im StGB jedoch kein auf elektronische Systeme beschränkter Datenverarbeitungs- und damit auch kein entsprechender Datenbegriff etabliert. Der Grund dafür liegt darin, dass der Gesetzgeber technologieoffene Tatbestände schaffen wollte, die freilich de facto fast ausschließlich auf EDV-Systeme zur Anwendung kommen. In Bezug auf den von der Literatur entwickelten Datenbegriff bleibt festzuhalten, dass auf seiner Grundlage zwar analoge Daten ausgeschieden werden können, jedoch nicht klar wird, mit welcher Begründung. Im Ergebnis muss dieser Definitionsversuch daher abgelehnt werden. Es bleibt somit bei der Erkenntnis, dass Daten im deutschen Strafrecht beliebige Informationen in einer beliebigen Darstellung, d.h. Kodierung, sind.

Die Einschränkungen des § 202a Abs. 2 StGB vermögen dieses Ergebnis nicht zu verändern. Zum einen handelt es sich ausweislich des klaren Wortlauts um keine Legaldefinition des Datenbegriffs. Ein solcher wird vielmehr vorausgesetzt. Zum anderen lassen sich aus Abs. 2 keine allgemeinen Charakteristika für einen strafrechtlichen Datenbegriff herleiten, da dieser Absatz nur auf einen Teil der Tatbestände Anwendung findet, die auf das Tatbestandsobjekt „Daten“ abstellen.

[196] Z.B. von Gravenreuth NStZ 1989, 201 (205) mwN

2.3 Artikel 1 lit. c) – Dienstanbieter[197]

Aus Art. 1 lit. c) ergibt sich, dass „Dienstanbieter“ derjenige ist, der auf Grund eines eigenen Dienstes die Kommunikation mit Computern in einem umfassenden Sinne ermöglicht oder erleichtert. Da „Kommunikation“ bereits nach dem natürlichen Wortsinn den Austausch von Informationen, Daten, Nachrichten, usw. zwischen mindestens zwei Personen bzw. Computern betrifft, spielt der Begriff nur in Mehrbenutzersystemen und in Netzwerken eine Rolle. Die Art des Netzes kann nach den Erläuterungen zu Art. 1 lit. c) dahinstehen, so dass sowohl die Ermöglichung bzw. Erleichterung des Zugangs zu einem LAN als auch zu einem größeren Netz, wie beispielsweise dem Internet, erfasst werden. In einem LAN kann von einem Dienstanbieter freilich erst dann gesprochen werden, wenn einer der Beteiligten ein gewisses Maß an Infrastruktur bzw. Dienstleistung im Sinne eines „Dienstes“ nach Art. 1 lit. c) i) anbietet. Sehr kleine Netzwerke unter gleichberechtigten Benutzern scheiden daher aus.

Lit. c) i) und ii) wählen einen umfassenden Ansatz und schließen im Bereich des Internets lediglich den bloßen Anbieter von Inhalten (engl. *Content Provider*[198]) als Dienstanbieter aus. Umgekehrt bedeutet dies, dass angefangen vom Leitungsanbieter (engl. *Network Provider*) über Zugangs- (engl. *Access-)*, Host-Service- und Online-Dienstanbieter[199] alle Dienstleister als „Dienstanbieter“ im Sinne der Konvention eingestuft werden. Dieser Kreis von Personen wird vor allem durch lit. c) ii) noch erweitert, indem Hilfsdienste sowohl für die Anbieter als auch die Nutzer dieser Kommunikationsdienste erfasst werden. Die Begriffsdefinition ist daher, mit Ausnahme der bloßen Inhaltsanbieter, eine Sammelbezeichnung für alle Anbieter von Dienstleistungen im Zusammenhang mit Datenübertragungen zwischen Computern.

2.3.1 Dienstanbieter im deutschen Strafrecht

Das StGB verwendet den Begriff des „Dienstanbieters“ nicht. Die StPO spricht im Zusammenhang mit Maßnahmen zur Überwachung der Telekommunikation, §§ 100a, 100b sowie §§ 100g, 100h StPO) von „[…] denjenigen, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken […]“. Außerhalb des materiellen Kernstrafrechts und des Verfahrensrechts definieren §§ 3 Nr. 1 TDG und 3 Nr. 1 MDStV den „Diensteanbieter“ als natürliche oder juristische Person, die eigene oder fremde Teledienste (Mediendienste) zur Nutzung bereithalten oder den Zugang zur Nutzung vermitteln. Nach wohl herrschender Meinung wird die Strafbarkeit eines Anbieters durch die §§ 8 ff. TDG bzw. §§ 6 ff. MDStV begrenzt. Die zitierten Normen statuieren eine abgestufte Verantwortlichkeit des Providers, je nachdem welche Dienste er im Einzelnen offeriert. Aufgrund der Neuartigkeit dieser Vorschriften, die zumindest dem Wortlaut nach nicht auf bestimmte Rechtsgebiete beschränkt sind, ist ihre dogmatische Einordnung bislang ungeklärt. Die wohl herrschende Meinung geht davon aus, dass die dargestellten Normen wie ein „Filter“ vor die Prüfung der in den anderen Rechtsgebieten geltenden Maßstäbe treten sollen.[200] Die Gegenansicht argumentiert, dass dem deutschen Strafrecht eine Filterfunktion in dogmatischer Hinsicht fremd sei.[201] Im Ergebnis sprechen der Wortlaut sowie die Einzigartigkeit der §§ 8 ff. TDG bzw. §§ 6 ff. MDStV in der

[197] ER Ziff. 26 und 27
[198] Zum Begriff: Hoeren/Sieber – *Sieber* 1 Rn 17
[199] Zu den Begriffen: Hoeren/Sieber – *Sieber* 1 Rn 17. Statt „Leitungsanbieter“ sollte allerdings vom „Netzwerk-“ oder „Übertragungsanbieter“ gesprochen werden, da Datenübertragungen nicht notwendigerweise leitungsgebunden sind.
[200] BGHSt 47, 55 (56); Engel-Flechsig/Maennel/Tettenborn NJW 1997, 2981 (2984); Roßnagel – *Spindler* 2 § 5 TDG Rn 33 ff. mwN
[201] LG München, Urteil vom 17. November 1999, 20 Ns 465 Js 173158/95 (CompuServe-Berufung)

deutschen Rechtslandschaft für die herrschende Meinung. Der im TDG und im MDStV verwendete Begriff „Diensteanbieter“ erlangt dadurch, wenigstens mittelbar, Wirkung für das materielle Strafrecht. Zu den im Folgenden zu klärenden Einzelfragen in TDG und MDStV zählt hingegen, ob es sich dabei um den Leitungs- (engl. *Network*-), Zugangs- (engl. *Access*-) oder sonstigen Anbieter handelt.

2.3.1.1 §§ 100a f. und §§ 100g f. StPO

Die StPO erlaubt Überwachungsmaßnahmen gemäß §§ 100a f. und 100g f. StPO in Bezug auf „geschäftsmäßige Anbieter von Telekommunikationsdiensten“. Maßgeblich ist daher, was unter „Telekommunikation“ im Sinne der StPO zu verstehen ist. Außer in § 3 Nr. 16 TKG wird der Begriff an keiner Stelle im Gesetz legal definiert. Im Sinne des Telekommunikationsrecht wird er beschrieben als „[…] der technische Vorgang des Aussendens, Übermittelns und Empfangens von Nachrichten jeglicher Art in der Form von Zeichen, Sprache, Bildern oder Tönen mittels Telekommunikationsanlagen (§ 3 Nr. 17 TKG).“ Diese Begriffsbestimmung hat sich von der klassischen Sprachtelefonie gelöst und umfasst nunmehr funktionsbezogen und unabhängig von der spezifischen Nutzung jede Art von Datenübertragung über Telekommunikationsnetze. Bedenken an einer Übernahme dieser Definition in das Strafprozessrecht ergeben sich jedoch aus den unterschiedlichen Regelungsbereichen der beiden Gesetze.[202] Während § 100g StPO zu Grundrechtseingriffen ermächtigt, zielt das TKG auf eine Regulierung der Telekommunikationsmärkte ab, die den Wettbewerb fördern, eine angemessene und flächendeckende Versorgung mit Dienstleistungen sichern sowie eine Frequenzordnung festlegen soll, § 1 TKG. Allerdings besteht Einigkeit[203], dass auf die Begriffsdefinition in § 3 Nr. 16 TKG zumindest zurückgegriffen werden kann. Darüber hinaus bietet vor allem das Begleitgesetz zum TKG (BegleitG)[204] Grund zur Annahme, von synonymen Begrifflichkeiten auszugehen. In der Gesetzesbegründung[205] wird ausgeführt, dass das BegleitG die Terminologie harmonisieren (der bis dato in §§ 100a f. StPO verwendete Begriff des „Fernmeldeverkehrs“ wurde durch „Telekommunikation“ ersetzt), materiell-rechtliche Strafbarkeitslücken schließen sowie die Überwachung der Telekommunikation durch die dazu berechtigten Stellen sicherstellen soll. Dazu wurden durch Art. 2 und 3 BegleitG zahlreiche Verzahnungen zwischen TKG, StGB, StPO sowie den anderen Gesetzen eingeführt, die auf Telekommunikation Bezug nehmen. Als Beispiel sei die Durchführung von Überwachungsmaßnahmen genannt, gestützt auf das G-10 Gesetz, das AWG sowie die StPO, die einheitlich durch Art. 88 TKG normiert wird. Ebenso macht der Verweis in § 100g Abs. 1 Satz 1 StPO auf § 3 Nr. 3 TKG zur Definition des Begriffs „Endeinrichtungen“ nur Sinn, wenn beiden Gesetzen derselbe Telekommunikationsbegriff zu Grunde liegt. Bei genauer Betrachtung stehen selbst die abweichenden Anwendungsgebiete von TKG und StPO einer Übernahme der Legaldefinition aus § 3 Nr. 16 TKG in das Strafverfahrensrecht nicht entgegen. Die Begriffsbestimmung erfolgt ohne Bezug zur Regulierungsintention des Telekommunikationsrechts allein anhand funktioneller Kriterien. Dadurch dürfte sich vor allem die Diskussion um die Reichweite des „Fernmeldebegriffs“, der bis zum Erlass des TKG und des BegleitG in §§ 100a f.[206] verwendet wurde, erledigt haben. Erst durch die „Direktruf“-Entscheidung[207] des BVerfG wurde der historische Fernmeldebegriff über den Bereich der analogen Sprachtelefonie auf digitale Nachrichtenübermittlungen erweitert. Die Definition des Telekommunikati-

[202] Kritisch für den Begriff des „Fernmeldeverkehrs“: Bär, S. 303 ff. sowie Eisenberg/Nischan JZ 97, 74 (77 ff.)
[203] KK – *Nack* § 100a Rn 4; Meyer-Goßner § 100a Rn 2
[204] BGBl. 1997 I, S. 3108 ff.
[205] BT-Drs. 13/8016, S. 1
[206] §§ 100g StPO wurden als Nachfolgeregelung zu § 12 FAG mit Wirkung ab dem 01.01.2002 eingeführt, (BGBl. 2001 I, S. 3879)
[207] Bär, S. 304 ff.; BVerfG 46, 120 ff.

onsbegriffs in § 3 Nr. 16 TKG hat diese Rechtsprechung weitergeführt.

Zusammenfassend kann daher festgehalten werden, dass TKG und StPO einen weitgehend übereinstimmenden Telekommunikationsbegriff verwenden.[208] Es ergeben sich darüber hinaus aus dem Wortlaut, der Entstehungsgeschichte sowie der Gesetzessystematik konkrete Anhaltspunkte dafür, von kongruenten Begrifflichkeiten auszugehen. Für die Einordnung der Anbieter im Internet bedeutet dies: Telekommunikationsdienste werden sowohl vom Leitungs- (z.B. Arcor, T-Com usw.) als auch vom Zugangsprovider (z.B. T-Online, AOL usw.) erbracht. Der eine stellt die Übertragungswege zur Verfügung (in der Regel öffentliche Telefonnetze), während der andere als „Vermittlungsstelle" auf seinem Server (Computer) Daten entgegennimmt und diese an andere miteinander verbundene Server weiterleitet. Inhalts- (engl. *Content*), Speicherplatz- (engl. *Host Service*) und sonstige Anbieter (z.B. Email, News usw.) setzen mit ihren Diensten auf die beschriebenen Übertragungsleistungen auf. Sie sind daher nicht als „Anbieter von Telekommunikationsdiensten" zu qualifizieren.

2.3.1.2 §§ 3 Nr. 1 TDG und 3 Nr. 1 MDStV

TDG und MDStV gehören zwar nicht dem Kernstrafrecht an, entfalten jedoch wenigstens bzgl. ihrer Verantwortlichkeitsnormen für Dienstanbieter Wirkung für das materielle Strafrecht (siehe oben 2.3.1). Beide Gesetze entstanden 1997, als Bund und Länder sich veranlasst sahen, einen einheitlichen Regelungsrahmen für die neuen „Multimediadienste"[209] zu schaffen. Aus der Sicht der Länder handelte es sich um eine mit dem Rundfunk verwandte Materie, für die sie die Gesetzgebungskompetenz nach Art. 70 GG beanspruchten. Der Bund stützte sich auf Art. 73 Nr. 7 GG und ordnete den Bereich dem Telekommunikationsrecht zu. Auf diese Weise entstanden der MDStV[210] der Länder und das IuKDG[211] des Bundes. Das IuKDG ist ein Artikelgesetz, das in den ersten drei Artikeln neue Gesetze enthält, die Multimedia-Dienste ermöglichen und absichern sollen (TDG, TDDSG, SigG) sowie in sechs weiteren Artikeln bestehende Gesetze (StGB, OwiG, GjSM, UrhG, Preisangabengesetz sowie die Preisabgabeverordnung) den neuen Anforderungen anpasst. Die Abgrenzung von „Telediensten" und „Mediendiensten", die sich wegen § 2 Abs. 4 Nr. 3 TDG gegenseitig ausschließen, ist anhand der Legaldefinitionen in § 2 Abs. 1 TDG und § 2 Abs. 1 Satz 1 MDStV abstrakt nicht durchführbar. Dies liegt vor allem daran, dass das TDG und der MDStV bei der Begriffsbestimmung einen unterschiedlichen Blickwinkel gewählt haben. § 2 Abs. 1 TDG spricht von einer „individuellen Nutzung" und § 2 Abs. 1 Satz 1 MDStV von einem „an die Allgemeinheit gerichteten Angebot" von „Informations- und Kommunikationsdiensten". Im TDG wurde die Perspektive des Nutzers und im MDStV die des Anbieters gewählt. Problematisch daran ist, dass eine Vielzahl von Diensten in Computernetzen an eine beliebige Öffentlichkeit gerichtet sind und gleichzeitig individuell genutzt werden können. Als Beispiel sei eine banale HTML-Seite genannt. Auf einem Web-Server gespeichert, richtet sie sich an eine globale Weltöffentlichkeit und wird vom Betrachter individuell am Bildschirm aufgerufen. Nach den Legaldefinitionen in TDG und MDStV handelt es sich sowohl um einen Tele- als auch einen Mediendienst, obwohl sich beide Regelungen gegenseitig nach § 2 Abs. 4 Nr. 3 TDG ausschließen. Die Kommentarliteratur schlägt daher eine von Fall zu Fall gesonderte Beurteilung

[208] Begründung zum BegleitG BT-Drs. 13/8016, S. 26; Eisenberg/Nischan JZ 1997, 74 (77); KK – *Nack* § 100a Rn 4; SK/StPO – *Wolter* § 100g Rn 18

[209] Roßnagel – *Roßnagel* 1 Einf Rn 4 ff. Die Terminologie ist wenig prägnant. Gebräuchlich ist auch: Informations- und Kommunikations-, Tele-, und Mediendienste, usw. Dahinter verbergen sich vor allem das Internet sowie digitales Fernsehen und andere Breitbandtechnologien.

[210] Staatsvertrag über Mediendienste; Bayern: BayGVBl. 1997, S. 226

[211] Informations- und Kommunikationsdienste Gesetz; BGBl. 1997 I, S. 1870 ff.

anhand der „Regel"-Beispiele in beiden Gesetzen vor.[212]

Die Art des Dienstanbieters richtet sich grundsätzlich nach dem Typus des angebotenen Dienstes, denn Dienstanbieter im Sinne von TDG und MDStV ist, wer „[…] eigene oder fremde Teledienste/Mediendienste zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt", §§ 3 Nr. 1 TDG, 3 Nr. 1 MDStV. Für Dienstleitungen im Zusammenhang mit dem Internet liefert § 2 Abs. 2 Nr. 3 TDG Anhaltspunkte hinsichtlich der Anwendbarkeit des TDG, indem „[…] das Angebot zur Nutzung des Internets und weiterer Netze" als Teledienst beschrieben wird. Da TDG und MDStV sich gegenseitig ausschließen, kann es sich nicht gleichzeitig um einen Mediendienst handeln. Liest man beide Definitionen zusammen, so ist derjenige, der das Angebot zur Nutzung des Internets und weiterer Netze bereit hält oder den Zugang zur Nutzung vermittelt, Dienstanbieter im Sinne von § 3 Nr. 1 TDG. Dieses auf den ersten Blick schlüssige Zwischenergebnis lässt sich jedoch nicht mit der Legaldefinition eines Teledienstes in § 2 Abs. 1 TDG vereinen. Darin heißt es, dass Telediensten eine „[…] Übermittlung mittels Telekommunikation zugrunde […]" liege. Teledienste bauen demnach auf Telekommunikationsdienste auf und sind nicht mit diesen identisch. Wer jedoch den Zugang zum Internet usw. bereit hält oder vermittelt, übernimmt gerade selbst die Übermittlung von Nachrichten jeglicher Art in Form Zeichen, Bildern usw. und damit die Telekommunikationsdienstleistung im Sinne von § 3 Nr. 16 TKG. Es handelt sich bei diesem Anbieter typischerweise um den Leitungs- bzw. Zugangsproviders, was in § 2 Abs. 2 Nr. 3 TDG korrekt beschrieben wird und sich in den Verantwortlichkeitsregelungen der §§ 8 ff. TDG so wieder spiegelt. Nur passt für den Fall der Internetdienste die Legaldefinition eines Teledienstes in § 2 Abs. 1 Nr. 1 TDG nicht zu den „Regel"-Beispielen.

Die Auflösung dieses Widerspruchs läuft auf eine grundsätzliche Abgrenzung zwischen Telekommunikation und Telediensten hinaus, die wegen der universellen Definition des Telekommunikationsbegriffs in § 3 Nr. 16 TKG sowie dem übergreifenden Charakter des TDG auch für andere Rechtsgebiete Wirkung entfaltet[213]. Ein Teil der Literatur[214] betrachtet § 2 Abs. 2 Nr. 3 TDG als Redaktionsversehen und argumentiert, dass der Gesetzgeber mit der Formulierung „Angebote zur Nutzung des Internets" nicht die Übermittlung von Daten, sondern die inhaltliche Erschließung der Angebote des Internets meinte, wie z.B. Suchmaschinen, usw. Dann stellt sich jedoch wiederum die Frage, warum der Anbieter von Suchmaschinen „[…] fremde Daten übermitteln […] oder den Zugang zu ihnen vermitteln […]" soll, wie § 9 TDG formuliert. Eine Suchmaschine – wie Google, Yahoo, Lycos, usw. – durchsucht nur ein bestehendes Angebot, übermittelt jedoch weder fremde Daten noch vermittelt sie den Zugang zu ihnen. Dies ermöglicht nur der Zugangsanbieter im technischen Sinne. Ein Ausweg aus diesem Widerspruch bestünde darin, von einem unterschiedlichen Begriff des Zugangsanbieters in § 2 Abs. 2 Nr. 3 und § 9 TDG auszugehen. Im Hinblick auf die Einheit der Rechtsordnung wäre eine einheitliche Terminologie, zumindest innerhalb eines Gesetzes, erstrebenswert.

Schmitz[215] hat einen anderen Lösungsansatz entwickelt und will Teledienste von Telekommunikation anhand der technischen Realisierung der Datenübertragungen abgrenzen. Er zieht dazu das ISO-Referenzmodell, in der durch die Verwendung der TCP/IP-Protokollfamilie modifizierten Fassung (siehe Kapitel 1.7.1.1.4) heran und führt aus, dass sich die insgesamt sieben (logischen) Schichten in vier Transport- und drei Anwendungsebenen unterteilen lie-

[212] Engel-Flechsig/Maennel/Tettenborn – Tettenborn § 2 Rn 40 ff.
[213] Vor allem in Bezug auf die sog. Verbindungsdaten. Dazu mehr im folgenden Kapitel.
[214] Engel-Flechsig/Maennel/Tettenborn – *Tettenborn* § 2 Rn 77, allerdings mit unklarem Begriff des „Access Providers" (dt. Zugangsanbieter); Hoeren/Sieber – *Sieber* 19 Rn 6
[215] Hoeren/Sieber – *Schmitz* 16.4 Rn 8 ff. 8 (13)

ßen. TCP, das auf der vierten Ebene angesiedelt ist, bilde demnach die letzte Stufe der Übermittlung und sei daher dem Telekommunikationsbereich zuzuordnen, während alle höheren Protokolle – HTTP, SMTP, FTP, usw. – der Anwendungsschicht Teledienste darstellten.[216] Diese Ansicht kann nicht überzeugen. Der Verfasser übersieht, dass letztlich alle Protokolle des ISO-Referenzmodels für die Übermittlung von Daten eingesetzt werden. Das Modell ist nur ein gedankliches Gebilde, das versucht, den technisch einheitlichen Übertragungsvorgang von Daten im Internet weiter zu strukturieren. Die Protokolle der Anwendungsebene haben nichts mit der inhaltlichen Gestaltung bestimmter „Dienstleistungen" im Sinne des TDG zu tun. Sie repräsentieren lediglich bestimmte Funktionen im Internet (technische Dienste). Als Beispiele seien das SMTP- und IMAP-Protokoll genannt, die beide den Transport von Emails übernehmen bzw. das HTTP-Protokoll, das die komfortable Übertragung von Bildern und Tönen ermöglicht und so den (technischen) Dienst des WWW für die breiten Massen zugänglich gemacht hat. Mit Telediensten im Sinne des TDG hat das WWW jedoch nichts zu tun, da es nicht per se für bestimmte Inhalte und Dienstleistungen steht, sondern lediglich deren Übermittlung übernimmt. Der Ansatz von *Schmitz* ist daher abzulehnen.

Als vorzugswürdiges Ergebnis bleibt an einem „Redaktionsversehen" des Gesetzgebers im Rahmen von § 2 Abs. 2 Nr. 3 TDG festzuhalten. Danach sind Teledienste und Telekommunikation anhand von § 2 Abs. 1 TDG abzugrenzen. „Telekommunikation" betrifft ausschließlich die Übertragung von Nachrichten; „Teledienste" bauen darauf auf und stellen besondere Dienstleistungen und Inhalte dar. Konsequenterweise beschreibt daher nur § 9 TDG den Zugangsanbieter im technischen Sinne, § 2 Abs. 2 Nr. 3 TDG dagegen „Suchmaschinen" und ähnliche Dienstleistungen. Für die Dienstleister im Internet bedeutet dies, das Leitungs- und Zugangsanbieter dem Telekommunikationsbereich zugeordnet werden. Darüber hinausgehende Dienste gehören den Tele- bzw. Mediendiensten an.

2.3.2 Vergleich

Der in der Konvention definierte Begriff des „Dienstanbieters" ist umfassend und differenziert nicht nach einzelnen Funktionen bei Datenübertragungen in Computernetzen. Den Verfassern ging es in erster Linie um die lückelose Erfassung aller an der Kommunikation mit Computern Beteiligten. „Dienstanbieter" in Art. 1 lit. c) stellt eine Sammelbezeichnung dar, die nur den Inhaltsanbieter (engl. *Content Provider*) ausnimmt.

Der deutsche Gesetzgeber differenziert grundsätzlich zwischen den Anbietern von Telekommunikationsdiensten sowie Tele- bzw. Mediendiensten. Die Einordnung der Beteiligten bei Datenübertragungen in Computernetzen wird durch die wenig geglückte Abgrenzung zwischen den einzelnen Diensten erschwert. Unterschiedliche Gesetzgebungskompetenzen im diffusen „Multimediabereich" haben zu einem Regelungsdickicht geführt, das nur anhand der klaren Definition des § 3 Nr. 16 TKG entzerrt werden kann. Leitungs- und Zugangsanbieter, die beide Übertragungsdienste erbringen, gehören danach dem Telekommunikationsbereich an. Alle anderen Anbieter im Internet erbringen wahlweise Tele- bzw. Mediendienste, je nachdem ob man den Blickwinkel der Anbieter oder den der Nachfrager wählt so wie es die Legaldefinitionen in §§ 2 Abs. 1 TDG/MDStV vorsehen (siehe Kapitel 2.3.1.2). Reformbedarf besteht nur im Bereich des TDG bzw. des MDStV auf Grund der unklaren Abgrenzung der Tele- von den Mediendiensten. Das TKG erlaubt eine klare Bestimmung des Dienstanbieters.

[216] Hoeren/*Sieber* – *Schmitz* 16.4 Rn 13 ff.

2.4 Artikel 1 lit. d) – Verbindungsdaten[217]

Bei Verbindungsdaten im Sinne der Konvention handelt es sich um diejenigen Daten, die von einem Computer im Rahmen eines Kommunikationsvorgangs erzeugt werden, um Inhaltsdaten vom Ausgangs- an den Zielort leiten zu können. Sie nehmen daher bei jeder Kommunikation eine dem Austausch von Inhalten untergeordnete Hilfsfunktion wahr. In rechtlicher Hinsicht kommt ihnen besondere Bedeutung dadurch zu, dass sie die Rückverfolgung einer Datenübertragung an ihren Ursprungsort und damit das Auffinden von Beweismitteln ermöglichen bzw. selbst als Beweismittel fungieren können. Verbindungsdaten fallen beim jeweiligen Dienstanbieter an und stehen daher in einem engen Zusammenhang zu diesem.

Lit. d) nimmt eine abschließende Aufzählung der Verbindungsdaten im Sinne der Konvention vor. Nicht alle genannten Angaben werden technisch immer zur Verfügung stehen, von dem Dienstanbieter zur Verfügung gestellt werden können oder für eine strafrechtliche Ermittlung erforderlich sein. Der „Ursprung" bezieht sich auf eine Telefonnummer, eine Internet Protokoll (IP) Adresse oder eine andere, ähnliche Identifikation einer Kommunikationsvorrichtung, für die ein Dienstanbieter Leistungen bereitstellt. Die „Bestimmung" betrifft vergleichbare Kommunikationsvorrichtungen am Zielpunkt der Datenübertragung. Der Begriff des „benutzten Dienstes" beschreibt einzelne technische Dienste in Computernetzen, beispielsweise WWW, FTP, Email oder Instant Messaging.

Der Grund, warum Verbindungsdaten besonders hervorgehoben wurden, besteht ausweislich der Erläuterungen zu lit. d) darin, auf die unterschiedliche Sensibilität von Verbindungs- und Inhaltsdaten hinzuweisen. Eingriffe in Inhaltsdaten wiegen im Allgemeinen schwerer als solche in Verbindungsdaten. In Abhängigkeit von der Eingriffsintensität variiert der Schutz, den die Unterzeichnerstaaten ihren Bürgern auf Grund von Art. 15 zu gewähren haben. Dadurch, dass die Konvention einzelne Daten aus der Gesamtheit der Computerdaten herausgreift, konnten graduell abgestufte Befugnisse geschaffen werden, die den Unterzeichnerstaaten bei der Transformation in nationales Recht einen Handlungsspielraum eröffnen. Abschließend bleibt kritisch anzumerken, dass die Abgrenzung zu den Kundendaten in Art. 18 Abs. 3 lit. a) die erforderliche Trennschärfe vermissen lässt.

2.4.1 Verbindungsdaten nach § 100g Abs. 3 StPO und § 206 Abs. 5 Satz 2 2. Halbsatz StGB

Die StPO spricht in Zusammenhang mit den zum 01.01.2002[218] eingeführten §§ 100g und 100h StPO von „Telekommunikationsverbindungsdaten", ohne einen expliziten Bezug zu Datenübertragungen mit Hilfe von Computern herzustellen. Im StGB wird der Begriff der „Verbindungsdaten" nicht verwendet. Allerdings definiert § 206 Abs. 5 Satz 2 2. Halbsatz StGB[219], dass neben den Inhalten einer Telekommunikation auch „[…] ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war", dem Fernmeldegeheimnis unterliegen. Inhaltlich weist diese Umschreibung Ähnlichkeit zu Art. 1 lit. d) auf, ohne jedoch ausdrücklich auf Computerdatenübertragungen bezogen zu sein. In den Datenschutzgesetzen definiert § 2 Nr. 4 Telekommunikationsdatenschutzverordnung (TDSV) den Begriff der „Verbindungsdaten" für den Bereich der Tele-

[217] ER Ziff. 28-31

[218] Gesetz zur Änderung der Strafprozessordnung vom 20.12.2001, BGBl. 2001 I, S. 3879

[219] Trat im Zuge der Postreform an die Stelle des alten § 354 StGB (Begleitgesetz zum Telekommunikationsgesetz , BGBl. 1997 I, 3108 ff.). Nach der Privatisierung der Deutschen Bundespost stellen Eingriffe in das Fernmeldegeheimnis keine Amtsdelikte mehr dar.

kommunikation, § 6 Abs. 1 Teledienste Datenschutzgesetz (TDDSG) den „Nutzungsdaten“ in Bezug auf die Teledienste nach dem TDG. Die TDSV und das TDDSG sind allerdings – wie alle Datenschutzgesetze – auf personenbezogene Daten beschränkt. Da Art. 1 lit. d) eine Begriffsbestimmung für strafrechtliche Zwecke intendiert, scheinen nur §§ 100g Abs. 3 StPO und 206 Abs. 5 StGB unmittelbar mit Art. 1 lit. d) vergleichbar.

Im Anwendungsbereich der StPO werden diejenigen Daten, über die Auskunft zu erteilen ist, durch § 100g Abs. 3 StPO anhand allgemeiner Kriterien bestimmt und abschließend aufgezählt.[220] Uneinigkeit besteht vor allem in Bezug auf die Einbeziehung von IP-Adressen, die für die Rückverfolgung einer Datenübertragung im Internet von besonderer Bedeutung sind. Sie werden bei der Einwahl in ein TCP/IP-basiertes Netzwerk (z.B. Internet) durch den Zugangsanbieter erteilt und fungieren als „elektronische Hausnummer“, anhand derer ein Computer zweifelsfrei identifiziert werden kann. Namentlich werden IP-Adressen in §§ 100g und 100h StPO nicht genannt. In der Begründung zum Gesetzentwurf der Bundesregierung heißt es hierzu, dass sie ebenso wie die elektronische Kennung von Mobiltelefonen (sog. IMEI-Nummern) vom Begriff der „Kennung“ in Abs. 3 Nr. 1 umfasst würden. Nicht erfasst würden dagegen die Namen der Nutzer, die hinter einer IP-Adresse stünden.[221] Diese könnten nach § 89 Abs. 6 TKG ermittelt werden.[222] Zweifel an der Einbeziehung von IP-Adressen unter den Begriff der „Telekommunikationsverbindungsdaten“ ergeben sich jedoch aus einem Umkehrschluss zu § 8 Abs. 8 BVerfSchG, § 10 Abs. 3 MADG und § 8 Abs. 3a BNDG ein. Diese Vorschriften gestatten ähnlich wie § 100g StPO den Zugriff auf Telekommunikationsverbindungsdaten, beziehen darüber hinaus jedoch auch die sog. „Teledienstenutzungsdaten“ namentlich mit ein. Aus dem fehlenden Hinweis auf Teledienstenutzungsdaten in § 100g StPO folgert *Wolter*[223], dass solche Daten nicht Gegenstand einer strafprozessualen Auskunft sein können. Die Gefahr eines solchen *e contrario* Schlusses sah auch der Rechtsausschuss in seiner Beschlussempfehlung bzgl. §§ 100g, 100h StPO und schlug vor, „[…] zu Klarstellungszwecken einen Hinweis, dass sich das Auskunftsbegehren auch auf Daten der Teledienste erstrecke […]“, aufzunehmen.[224] Ein solche Ergänzung wurde allerdings in der geltenden Fassung nicht umgesetzt.

Für die Entscheidung der Frage, ob IP-Adressen den Teledienstenutzungs- oder Telekommunikationsverbindungsdaten zuzuordnen sind, kommt es auf eine Abgrenzung der Tele- von den Telekommunikationsdiensten an. Insoweit kann auf die Ausführungen oben, Kapitel 2.3.1.2, verwiesen werden, die wegen der übergreifenden Geltung des TDG, wenigstens in Bezug auf die Regelungen zur Verantwortlichkeit, auch auf die StPO übertragen werden können. Als Ergebnis wurde dort festgestellt, dass Leitungs- und Zugangsanbieter zum Internet dem Telekommunikationsbereich angehören, alle sonstigen Anbieter Tele- bzw. Mediendienste erbringen. Überträgt man diese Erkenntnisse auf IP-Adressen, können diese nur „Telekommunikationsverbindungsdaten“ darstellen, da sie in einem untrennbaren Sachzusammenhang mit Datenübertragungen in TCP/IP-Protokoll basierten Netzwerken wie dem „Internet“ stehen. Dazu werden sie vom Zugangsprovider aus dem ihm zugeteilten Adresspool jedem Nutzer für die Dauer einer Verbindung zum Internet zugeteilt (sog. dynamische Adressvergabe). Mit Inhalten oder Dienstleistungen, die über die bloße Übertragung von Daten hinausgehen (Tele- bzw. Mediendienste), haben sie nichts zu tun. Der von *Wolter*[225] gezogene Umkehrschluss kann daher aus systematischen Gründen nicht überzeugen und ist daher abzu-

[220] Meyer-Goßner § 100g Rn 4; SK/StPO – *Wolter* § 100g Rn 17
[221] BT-Drs. 17/7008, S. 7
[222] SK/StPO – *Wolter* § 100g Rn 10
[223] SK/StPO – *Wolter* § 100g Rn 10
[224] BT-Drs. 14/7679, S. 7
[225] SK/StPO – *Wolter* § 100g Rn 10

lehnen. Verbindungsdaten, die beim Leitungs- oder Zugangsanbieter anfallen, können zu den Telekommunikationsverbindungsdaten im Sinne von § 100g Abs. 3 StPO gezählt werden.

§ 206 Abs. 5 Satz 2 2. Halbsatz StGB definiert die strafrechtliche Weite des Fernmeldegeheimnisses. Die Norm trat im Rahmen von Art. 2 XIII Nr. 6 BegleitG[226] an die Stelle von § 354 StGB. Der Wortlaut ist nunmehr identisch mit dem des § 85 Abs. 1 TKG. Statt von „Fernmeldeanlagen" spricht der Gesetzestext von „Telekommunikation" und „Telekommunikationsanlagen". Auf Grund der einheitlichen Terminologie und der Entstehungsgeschichte erscheint die Übernahme der Definition des Telekommunikationsbegriffs aus § 3 Nr. 16 TKG in das StGB als gerechtfertigt.[227] Konsequenterweise muss dies auch für die Abgrenzung zu den Tele- und Mediendiensten gelten. Der materiellrechtliche Begriff der Verbindungsdaten unterscheidet sich daher nicht vom verfahrensrechtlichen, so dass auf die Ausführungen zu § 100g Abs. 3 StPO verwiesen werden kann.

2.4.2 Vergleich

Der Begriff der „Verbindungsdaten" steht in engem Zusammenhang zur Definition des Dienstanbieters, denn dort fallen diese Daten üblicherweise an. Die Konvention unterscheidet anders als der deutsche Gesetzgeber nicht zwischen dem Telekommunikationsbereich und den sonstigen Dienstleistungen (Tele- und Mediendienste) in Computernetzen. Daher werden die Begriffe „Dienstanbieter" und „Verbindungsdaten" als Sammelbezeichnung für alle Anbieter und Dienste verwendet, die in Datenübertragungen zwischen Computern involviert sind. Konsequenterweise unterscheidet die Konvention auch nicht zwischen Telekommunikationsverbindungsdaten und Teledienstenutzungsdaten, sondern verwendet den Begriff „Verbindungsdaten" stattdessen als Sammelbezeichnung für alle Hilfsdaten, die bei einer Datenübertragung zwischen Computern anfallen, egal aus welchem Bereich sie stammen.

[226] Begleitgesetz zum TKG, BGBl. 1997 I, S. 3108 ff.

[227] Ebenso: Sch/Sch – *Lenckner* § 206 Rn 6; Anhaltspunkte dafür auch in der Gesetzesbegründung, die von einem identischen Adressatenkreis in § 206 Abs. 1 und § 85 Abs. 2 TKG ausgeht, was nur bei einem ebenfalls identischen „Telekommunikationsbegriff" Sinn macht, BT-Drs. 13/8016, S. 29

3 Materielles Strafrecht

An die Begriffsbestimmungen in Kapitel I der Konvention schließt sich Kapitel II an, das mit „Maßnahmen auf nationaler Ebene“ überschrieben ist. In drei Abschnitte unterteilt werden Normen zum materiellen Strafrecht (Abschnitt 1), Verfahrensrecht (Abschnitt 2) sowie zur Gerichtsbarkeit (Abschnitt 3) definiert. Abschnitt 1 beinhaltet insgesamt zwölf Artikel, die sich wie folgt untergliedern lassen: Art. 2 bis 6 enthalten Tatbestände, die die ungestörte Kommunikation mit Hilfe von Computersystemen schützen (Informationsdelikte[228]), wobei Art. 6, der bestimmte Vorbereitungshandlungen kriminalisiert, eine Sonderstellung einnimmt. Titel 1 lautet daher: „Straftaten gegen die Vertraulichkeit, Integrität und Verfügbarkeit von Computerdaten und Systemen“. Titel 2 bezieht sich „Computerstraftaten“ und definiert Tatbestände zu Urkundenfälschung und Betrug in Zusammenhang mit Computern. Titel 3 beinhaltet als „Inhaltsbezogene Straftaten“ solche in Bezug auf Kinderpornografie. „Straftaten in Zusammenhang mit Verletzungen des Urheberrechts und verwandter Schutzrechte“ sind Gegenstand von Titel 4. Im 5. und letzten Titel in Abschnitt 1 werden „Nebenformen der Verantwortlichkeit und Sanktionen“ beschrieben.

In diesem Kapitel werden die materiell-rechtlichen Normen der Konvention erläutert, wobei – dem Aufbau des Übereinkommens folgend – die Bestimmungen zur Gerichtsbarkeit und das internationale Strafrecht bzw. Strafanwendungsrecht nach dem verfahrensrechtlichen Teil dargestellt werden.

3.1 Artikel 2 – Rechtswidriger Zugriff[229]

Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um den unbefugten Zugriff auf ein Computersystem als Ganzes oder auf einen Teil davon nach ihrem innerstaatlichen Recht als Straftat festzulegen, wenn die Handlung vorsätzlich begangen wird. Eine Vertragspartei kann als Voraussetzung vorsehen, dass die Straftat durch Verletzung von Sicherheitsmaßnahmen, in der Absicht, Computerdaten zu erlangen, oder in anderer unredlicher Absicht oder in Zusammenhang mit einem Computersystem, das mit einem anderen Computersystem verbunden ist, begangen worden sein muss.

3.1.1 Anwendungsbereich

Die Vorschrift zielt auf den Schutz der Vertraulichkeit von Daten und Systemen ab und etabliert gleichzeitig eine Art „virtuelles“ Hausrecht[230] im elektronischen Herrschaftsbereich des Berechtigten. Insofern besteht eine gewisse Ähnlichkeit zu § 123 StGB in Bezug auf körperliche Schutzobjekte. Ein Vergleich mit dieser Vorschrift erweckt sogleich Bedenken hinsichtlich der zu schützenden Sphäre. Während § 123 StGB auf Räumlichkeiten verweist, die wenigstens zum Teil grundrechtlichen Schutz genießen (Art. 13 GG, Unverletzlichkeit der Wohnung)[231], beabsichtigt Art. 2 diesen Schutz auf Bereiche auszudehnen, deren besondere

[228] Bzw.: Kommunikationsdelikte, Preuße, S. 18
[229] ER Ziff. 44-50
[230] LG Bonn, Az. 10 O 457/99, in Bezug auf die Rechtsposition eine „Chatroom“-Betreibers, der einen ungebetenen Besucher von der Teilnahme ausschließen wollte.
[231] Sch/Sch – *Lenckner* § 123 Rn 1

Schutzwürdigkeit vom deutschen Gesetzgeber bislang verneint wurde[232] und die zum Teil nur virtuell[233] existieren. Nach Auffassung der Verfasser der Konvention stellt das „bloße Eindringen“ in ein Computersystem – auch als „Hacken“ bzw. „Cracken“[234] bezeichnet – jedoch eine Vorbereitungshandlung für weitere Angriffe gegen die Sicherheit von Computersystemen und Daten dar und ist daher als strafwürdig zu beurteilen. Neben der unmittelbar eintretenden Vertraulichkeitsverletzung werden zumeist auch das Integritäts- und Verfügbarkeitsinteresse gefährdet. Ist ein Hacker erst einmal in ein System eingebrochen, besteht die Gefahr, dass er es nicht dabei bewenden lässt, sondern sich oder Dritten vertrauliche Daten (z.B. Passwörter, Codes, usw.) verschafft, das kompromittierte System unentgeltlich nutzt oder manipuliert. Es drohen weitere Straftaten im Zusammenhang mit Computern, wie etwa Computerbetrug oder Computerurkundenfälschung. Obwohl nach nahezu einhelliger Ansicht die wirksamsten Methode im Kampf gegen Eindringlinge in der Implementierung technischer Sicherheitsmaßnahmen besteht, können strafrechtliche Bestimmungen nach Ansicht des Europarats bereits im Vorfeld abschreckende Wirkung entfalten und auf diese Weise zusätzlichen Schutz für die bedrohten Systeme und Daten bieten.[235] In Bezug auf gängige Methoden, mittels derer in ein Computersystem eingedrungen werden kann, wird auf die Ausführungen in Kapitel 1.7.1 verwiesen.

3.1.2 Tatbestand

Tatobjekte sind Computersysteme nach Art.1 lit. a). Unter „Zugriff“ versteht die Konvention das „Eindringen“ in ein Computersystem als Ganzes oder einen Teil davon (Hardware, Peripherie, gespeicherte Daten, Verzeichnisse, Verbindungs- und Inhaltsdaten).[236] Was damit im Einzelnen gemeint ist, ließen die Verfasser der Konvention ebenso wie der deutsche Gesetzgeber offen.[237] Durch einen Umkehrschluss aus Art. 2 Satz 2 a.E. lassen sich grundsätzlich zwei Szenarien beschreiben, in denen auf ein Computersystem im Sinne der Konvention zugegriffen wird:

Einerseits erfasst Art. 2 den Zugriff über Netzwerkverbindungen auf den Datenbestand eines Computers. Diese Variante wird umgangssprachlich als „Hacking“ bezeichnet. Die Täter befinden sich üblicherweise an einem anderen Ort als das beeinträchtigte Computersystem und greifen auf die unkörperlichen Inhalte des Zielsystems zu. Von diesem Begriffsverständnis ließ sich auch der deutsche Gesetzgeber bei seinen Beratungen zu § 202a StGB leiten.[238]

Andererseits versteht die Konvention auch den körperlichen Zugriff auf die Hardware eines Computersystems als Zugriff im Sinne von Art. 2. Dies wird aus einem Umkehrschluss zu Art. 2 Satz 2 a.E. deutlich, der besagt, dass die Vernetzung eines Rechners von den Unterzeichnerstaaten als einschränkendes Tatbestandsmerkmal bei der Umsetzung von Art. 2 vorgesehen werden könne, d.h. der Tatbestand des „Rechtswidrigen Zugriffs“ nicht auf Netzwerke beschränkt sei.

Bedenklich an diesem Verständnis des „Zugriffs“ ist, dass der Tatbestand eine überaus große

[232] Beschlussempfehlung und Bericht des Rechtsausschusses: BT-Drs. 10/5058, S. 29: Im Zusammenhang mit § 202a StGB heißt es dort, dass das sog. „Hacking“, das sich im „bloßen Eindringen“ in ein Computersystem erschöpft, straflos bleiben soll.
[233] Beispielsweise „Chatrooms“. Allgemein zum Begriff der elektronischen Scheinrealitäten Kapitel 1.6.
[234] Die Begriffe werden uneinheitlich verwendet; Definitionsversuch bei von Gravenreuth, NStZ 1989, 201 (204ff.)
[235] ER Ziff. 45
[236] ER Ziff. 46
[237] Siehe Fn 232.
[238] Siehe Fn 232.

Reichweite erlangt und an Bestimmtheit verliert. Vor allem in Bezug auf unkörperliche Zugriffe auf die Daten eines Computers wird nicht deutlich, wann qualitativ die Schwelle zur Strafbarkeit überschritten wird. Nach dem Wortlaut der Vorschrift wäre bereits das Einschalten eines Computers, sofern es mit dem Vorsatz des Zugriffs erfolgt, strafbar. Dies gilt selbst dann, wenn der Rechner nach dem Einschalten nicht bootet, sich keine vertraulichen Informationen darauf befinden bzw. das System besonders gesichert ist. Fraglich ist insbesondere auch, wann in einem echten Mehrbenutzersystem (z.B. Unix/Linux, Novell NetWare usw.) von einem Zugriff gesprochen werden kann. Für alle Benutzer und Dateien existieren differenzierte Rechte. Solange ein Eindringlich sich nicht entsprechend gegenüber dem Computersystem authentifiziert, werden ihm bestimmte Dateien und Verzeichnisse überhaupt nicht angezeigt.[239] Es besteht keine Zugriffsmöglichkeit, obwohl der Täter in einen Teilbereich des Computersystems eingedrungen ist. Eine Beeinträchtigung des Systems oder der Daten droht erst dann, wenn der Eindringling Administratorenrechte erlangt. Gerade darauf zielen Hacker etwa mit „*Buffer Overflow*“ (siehe Kapitel 1.7.1.1.2) oder „*DDoS/DoS“*-Attacken (siehe Kapitel 1.7.3) ab.

Ebenfalls fraglich erscheint, was die Verfasser der Konvention mit dem Eindringen in die Hardware eines Computers meinen.[240] Weder aus dem Tatbestand noch aus den Erläuterungen wird deutlich, ob damit Sabotagehandlungen beschrieben werden, oder ob bereits das Öffnen eines Druckers genügt, um den Toner zu ersetzen oder das Papier aufzufüllen. Derartige Handlungen, die bereits auf den ersten Blick nicht strafwürdig erscheinen, müssten über das Merkmal der „Unbefugtheit“ ausgeschieden werden, da die Beschreibung der Tathandlung keinen besonderen Unwertgehalt enthält.

Insgesamt erweckt der Tatbestand den Eindruck als hätten die Verfasser versucht, eine Hacking-Strafbarkeit zu begründen, ohne über eine wirksame Begrenzung des Tatbestandes nachgedacht zu haben, um Bagatellfälle auszuschließen.

3.1.3 Vorsatz

In subjektiver Hinsicht erfordert Art. 2, wie alle anderen Tatbestände der Konvention, Vorsatz. Welche Anforderungen an die subjektive Seite des Tatbestandes zu stellen sind, wird in den Erläuterungen nicht näher beschrieben.

3.1.4 Unbefugt

Der Täter muss „unbefugt“ handeln. Dabei handelt es sich um ein Merkmal, das sich durch Art. 2 bis Art. 9 zieht und eine zentrale Stellung im materiell-rechtlichen Teil der Konvention einnimmt.[241] Auch das StGB verwendet das Tatbestandsmerkmal an verschiedenen Stellen, unter anderem in §§ 107a, 132, 132a, 168 StGB sowie in allen Tatbeständen des 15. Abschnitts §§ 201 ff. StGB, der dem Schutz des persönlichen Lebens- und Geheimbereichs dient. Die dogmatische Einordnung ist dort noch nicht vollends geklärt[242]. Zum Teil begrenzt es den Tatbestand; teilweise ist es auch als Hinweis auf die allgemeine Rechtswidrigkeit zu verstehen bzw. nimmt sogar eine Doppelfunktion wahr.[243] Im Rahmen der Konvention lässt sich keine allgemeine Zuordnung vornehmen. Das Merkmal der Rechtswidrigkeit wird daher

[239] Taschenbuch der Informatik – *Federrrath/Pfitzmann*, Kap. 17, S. 591 f.
[240] ER Ziff. 46
[241] Kugelmann DuD 2001, 215 (217); ders. TMR 2002, 14 (16); Magnin, S. 56 f.
[242] Lackner/Kühl – *Kühl* Vor § 201 Rn 2
[243] Lackner/Kühl – *Kühl* Vor § 201 Rn 2; Sch/Sch – *Lenckner* § 203 Rn 21

als eigener Gliederungspunkt diskutiert.

Den Erläuterungen zufolge will die Konvention anhand dieses Merkmals vor allem Verhaltensweisen ausschließen, die mit Wissen und Wollen des Berechtigten erfolgen, beispielsweise einen System- oder Sicherheitstest. Nach der deutschen Strafrechtsdogmatik handelt es sich hier um einen Fall des tatbestandsausschließenden Einverständnisses, wenn dadurch bereits die Tatbestandsmäßigkeit entfällt, anderenfalls um eine Einwilligung, die die Rechtswidrigkeit tatbestandsmäßigen Verhaltens beseitigt.[244] Ebenso wenig sollen sozialadäquate Verhaltensweisen[245] durch Art. 2 pönalisiert werden. Dafür nennen die Materialien folgende Beispiele: Nicht tatbestandsmäßig sei der Zugriff auf solche Systeme, die der Öffentlichkeit frei zugänglich sind. Darunter fallen beispielsweise WWW-Seiten. In diesem Fall beabsichtigt der Webautor den Besuch seiner Seite durch eine breite Öffentlichkeit. Anders zu beurteilen ist der Sachverhalt freilich, falls Teilbereiche der Homepage nicht frei zugänglich sind oder der Täter sich den geschützten HTML-Quellcode einer Seite anzeigen lässt.

Eine weitere sozialadäquate Verhaltensweise stellt der Einsatz technischer Hilfsmittel dar, um Informationen im Netz zu lokalisieren, sog. „bots". Ebenso werden Cookies als rechtmäßig betrachtet, trotz der Beeinträchtigungen der Privatsphäre, die von ihnen ausgehen können.[246] In diesem Beispiel willige der Benutzer – ausdrücklich oder mutmaßlich – ein, wenn er nicht von Anfang an die Installierung dieser Datenpakete ablehnt bzw. sie nachträglich entfernt. Die Erläuterungen übersehen dabei, dass Cookies in der Regel ohne Wissen des Nutzers auf der Festplatte deponiert werden. Zusammenfassend sollen alle Standardhilfsmittel, die in den üblichen Kommunikationsprotokollen und Programmen enthalten sind, aus dem Anwendungsbereich von Art. 2 herausgenommen werden.

3.1.5 Art. 2 Satz 2 – Einschränkungen im Anwendungsbereich

Artikel 2 Satz 1 eröffnet einen sehr umfangreichen Anwendungsbereich, der eine Vielzahl von Verhaltensweisen mit Strafe bedroht. Mit dem „fragmentarischen Charakter des Strafrechts"[247] als „Vorzug des freiheitlichen Rechtsstaats"[248] ist dies nur schwer zu vereinen und hat deshalb, nicht zuletzt auf Grund der Meinungsverschiedenheiten bei den Beratungen[249], die Verfasser der Konvention dazu bewogen, den nationalen Gesetzgebern die in Satz 2 dargestellten Gestaltungsmöglichkeiten einzuräumen. Die Erläuterungen führen aus, dass die Kritik an einer Kriminalisierung des „Hacking" vor allem aus den Situationen resultiere, wo keine Gefährdung durch das bloße Eindringen entstand oder wo Systemeinbrüche Fehler und Lücken in den Sicherheitsvorkehrungen aufdeckten.[250] Dies habe dazu geführt, dass einige Länder die Strafbarkeitsschwelle für „Hacking"-Delikte höher angesetzt haben und weitere qualifizierende Umstände fordern. Den Unterzeichnerstaaten wird daher durch Art. 2 Satz 2 die Möglichkeit eingeräumt, das Hinzutreten weiterer qualifizierender Umstände zu erfordern. Namentlich kommen in Betracht:

Im objektiven Tatbestand die Verletzung von Sicherheitsmaßnahmen oder die Beschränkung

[244] Jescheck, Strafrecht AT, § 34 I, S. 373
[245] Nach wohl hM kein eigenständiger Rechtfertigungsgrund, sondern nur Auslegungsgrundsatz. Dazu: Jescheck, Strafrecht AT, § 25 IV, S. 251 ff. und § 36, S. 400 ff.; Lackner/Kühl – *Kühl* § 201 Rn 14 sowie Vor § 32 Rn 29 mwN
[246] Siehe dazu Kapitel 1.7.1.2.
[247] Binding, Lehrbuch Bes. Teil, S. 20 ff.
[248] Jescheck/Weigend, Strafrecht AT, § 7 II, S. 53
[249] ER Ziff. 49 f.
[250] ER Ziff. 49

des Delikts auf Computersysteme, die über ein Netzwerk (öffentliche und private, lokale und flächendeckende, usw.) miteinander verbunden sind. Bemerkenswert ist vor allem die letztgenannte Einschränkungsmöglichkeit, denn bei Delikten in Bezug auf ein nicht vernetztes Computersystem handelt es sich gerade nicht mehr um solche im Cyberspace, wie dies in der Überschrift zum Ausdruck kommt. In subjektiver Hinsicht kann die Absicht, Computerdaten erlangen zu wollen, oder eine andere unredliche Absicht als weiteres Merkmal erfordert werden.

3.1.6 Vergleichbare Tatbestände im deutschen Strafrecht

Das deutsche Strafrecht weist mit Ausnahme der Delikte, die im Jahr 1986 durch das 2. WiKG eingefügt worden sind, keine Grundlage zur strafrechtlichen Erfassung von Computerkriminalität auf. Vor allem die flächendeckende Verbreitung der Datennetze in den 1990er Jahren konnte der Gesetzgeber damals noch nicht antizipieren. Die folgenden Untersuchungen beleuchten daher vergleichbare Vorschriften im deutschen Strafrecht und zeigen Defizite gegenüber der Konvention auf.

3.1.6.1 § 202a StGB – Ausspähen von Daten

§ 202a StGB scheint auf den ersten Blick nicht mit Art. 2 vergleichbar zu sein, da er auf ein „Verschaffen“ von Daten abstellt, das vom natürlichen Wortsinn her chronologisch erst nach dem Eindringen in ein System erfolgen kann. An dieser Stelle äußert sich allerdings abermals die Unbestimmtheit des Zugriffsmerkmals in Art. 2. Wer in ein Computersystem eindringt, kann sich über den Erfolg seines Tuns nur dadurch vergewissern, indem er sich die bzw. einige Inhalte des kompromittierten Systems auf seinem Bildschirm anzeigen lässt. Fälle, in denen ein potentieller Eindringling darauf verzichtet, können wohl nicht mehr als „vorsätzliches“ Eindringen qualifiziert werden. In dem Moment, in dem die ersten Verzeichnisse des Zielsystems auf dem Monitor des Hackers erscheinen, werden auch die ersten Daten auf seinen Computer übertragen. Anders ist eine Visualisierung technisch nicht möglich. Lässt sich dieser Vorgang als Verschaffen von Daten qualifizieren, stellt § 202a StGB (unter weiteren Voraussetzungen) einen dem Art. 2 vergleichbaren Tatbestand dar, obwohl der Gesetzgeber bei seiner Einführung „das bloße Eindringen in ein Computersystem“ von Strafe verschonen wollte.[251]

3.1.6.1.1 Rechtsgut

§ 202a StGB wurde durch das 2. WiKG eingefügt, um eine Lücke im Recht des Datenschutzes zu schließen, die sich im Rahmen der Entstehung und Verbreitung der neuen Informations- und Kommunikationstechnologien auftat. Das BDSG schützt allein vor der unbefugten Verwendung personenbezogener Daten im Sinne von § 3 Abs. 1 BDSG. § 201 StGB bezieht sich auf die Aufnahme bzw. das Abhören des nichtöffentlich gesprochenen Wortes und § 202 Abs. 3 StGB a.F. erfasste lediglich (auch auf elektronischen Datenträgern) fixierte menschliche Gedankenerklärungen, so dass Daten während ihrer Übermittlung schutzlos waren.[252] Durch die Einführung von § 202a StGB sollten als Daten dargestellte Informationen in umfassender Weise vor Spionageakten geschützt werden. Dieser Schutz wurde deshalb als notwendig erachtet, weil digital übertragene Daten mit Hilfe von Computern technisch sehr viel

[251] Beschlussempfehlung und Bericht des Rechtsausschusses: BT-Drs. 10/5058 S. 28
[252] BT-Drs. 10/5058, S. 28

leichter als Telefongespräche abgehört und analysiert werden können.[253] Aus diesem umfassenden Ansatz folgt, dass das von der Vorschrift geschützte Rechtsgut das formelle Geheimhaltungsinteresse des über die Speicherung und Übermittlung von Daten Verfügungsberechtigten ist.[254] Geschützt wird das Verfügungsrecht desjenigen, der unabhängig von den Eigentumsverhältnissen am Datenträger kraft seiner Berechtigung am gedanklichen Inhalt der Daten – nicht nur der verkörperten Informationen – darüber bestimmen kann, wem sie zugänglich gemacht werden sollen.[255] Formell bedeutet dies, dass auch nicht in materiellem Sinne „geheime" Daten erfasst werden. Dies folgt aus der Parallelität zu § 202 StGB, der das formal begrenzte Briefgeheimnis schützt, und aus dem Fehlen des Tatbestandsmerkmals „Geheimnis", das sich in § 203 StGB findet.[256] Die von Teilen der Literatur[257] geforderte einschränkende Auslegung, dass die Daten einen Vermögenswert aufweisen müssen und es sich daher um ein Vermögensdelikt handele, lässt sich auf Grund des insofern neutralen Wortlauts nicht aufrechterhalten. Die Daten werden zwar auf Grund der Verfügungsbefugnis oft einen wirtschaftlichen Wert besitzen. Dabei handelt es sich aber um einen bloßen Schutzreflex.[258] Träger des Rechtsguts ist der an den Daten Verfügungsberechtigte.[259] Darüber hinaus soll auch noch der vom Inhalt der Daten Betroffene, wenn er in seinem Recht auf Wahrung der Vertraulichkeit gegenüber dem Berechtigten berührt ist, mitgeschützt sein.[260] Diese Ansicht lässt sich aber mit dem Wortlaut der Vorschrift und der Intention des Gesetzgebers nur schwer vereinbaren.[261]

3.1.6.1.2 Tathandlung

Die Tathandlung besteht darin, dass der Täter sich selbst oder einem anderen Daten verschafft. In der Literatur wird zu Recht kritisiert, dass der Gesetzgeber die Tathandlung näher hätte umschreiben müssen, da wegen der einzigartigen Beschaffenheit von Daten nicht ohne weiteres auf die andernorts im StGB (z.B. §§ 96, 259 StGB) entwickelten Auslegungsregeln zurückgegriffen werden kann.[262] Schon nach dem bloßen Wortsinn geht das „Verschaffen" gemäß § 202a StGB über das „Zugriffnehmen" im Sinne der Konvention hinaus. Erforderlich ist, dass der Täter die Herrschaftsgewalt über die Daten erlangt, so dass er über sie verfügen kann.[263] Dies wird auf Grund der in der Praxis zumeist großen Datenmengen in erster Linie der Fall sein, wenn der Täter die Daten auf einem Datenträger fixiert, d.h. abspeichert, ohne Rücksicht darauf, welches Medium (Diskette, CD, Netzwerklaufwerk beim Versand per E-mail usw.) er als Datenträger für die Kopie wählt, oder ob er gar den originalen Datenträger mitnimmt. Unter „Verschaffen" sollte darüber hinaus jedoch auch das nicht „computerbezogene" Festhalten von Daten erfasst werden, denn auf Grund der methodisch neutral formulierten Tathandlung ist eine derartige Einschränkung nicht nachvollziehbar.[264] Der Täter verschafft sich also auch dann Daten, wenn er sie notiert oder in sonstiger Form festhält. Bis zu

[253] BT-Drs. 10/5058, S. 28
[254] Lackner/Kühl – *Kühl* § 202a Rn 1
[255] LK (11. Aufl.) – *Schünemann* § 202a Rn 2; Möhrenschlager wistra 1986, 128 (140); Sch/Sch – *Lenckner* § 202a Rn 1; SK – *Hoyer* § 202a Rn 1; einschränkend: Tröndle/Fischer § 202a Rn 2
[256] Preuße, S. 35
[257] Bühler MDR 1987, 448 (452); Haft NStZ 1987, 6 (9)
[258] Haß, S. 467, (480); LK – *Schünemann* § 202a Rn 1; Sch/Sch – *Lenckner* § 202a Rn 1
[259] Sch/Sch – *Lenckner* § 202a Rn 1; LK – *Schünemann* § 202a Rn 1, SK – *Hoyer* § 202a Rn 1
[260] Lackner/Kühl – *Kühl* § 202a Rn 1
[261] Ablehnend daher Schmitz JA 1995, 478; Lenckner/Winkelbauer CR 1986, 483 (485)
[262] Bühler MDR 1987, 448 (453)
[263] LK – *Schünemann* § 202a Rn 6; Sch/Sch – *Lenckner* § 202a Rn 10;
[264] Hilgendorf JuS 1996, 702 (704 f.); Lackner/Kühl – *Kühl* § 202a Rn 5; LK – *Schünemann* § 202a Rn 6; Sch/Sch – *Lenckner* § 202a Rn 10; Tröndle/Fischer § 202a Rn 10; aA: Hauptmann JurPC 1989, 215 (217); aA wohl auch Haft NStZ 1987, 6 (10), der den Begriff des Datenträgers jedoch nicht näher definiert.

diesem Punkt ergeben sich keine Abgrenzungsschwierigkeiten zu Art. 2.

Umstritten ist allerdings, wie eine nur sinnliche Wahrnehmung der Daten, ohne weitere Fixierung, zu beurteilen ist. Damit wird die Situation des „bloßen Eindringens“ beschrieben, nachdem ein Hacker Passwortabfragen oder sonstige Sicherheitsmechanismen überwunden oder umgangen hat und sich nunmehr vom Erfolg seines Tuns vergewissert, indem er sich die auf dem kompromittierten System gespeicherten Daten auf dem Bildschirm anzeigen lässt. Greift man auf den Verschaffensbegriff des § 96 StGB zurück, so genügt jede sinnliche Wahrnehmung, durch die sich der Täter Kenntnis von den Daten verschafft.[265] Daher würde auch das Betrachten am Bildschirm genügen. Weite Teile der Literatur beurteilen dieses Ergebnis, das der von der Bundesregierung gewollten Straffreiheit des „Hackens“[266] zuwider läuft, als unakzeptabel und reduzieren den Verschaffensbegriff teleologisch.[267] Teilweise wird vertreten, dass nur eine gesicherte Kenntnisnahme tatbestandsmäßig sein soll, wozu der Täter in der Lage sein muss, die wahrgenommenen Daten zu reproduzieren und zu verwerten.[268] Andere Autoren gehen weiter und verlangen die Abspeicherung auf einem Datenträger.[269] Problematisch an der ersten Auffassung erscheint, dass sie in der Praxis zu einem erheblichen Maß an Rechtsunsicherheit beitragen wird. Den Ermittlungsbehörden wird es nicht erspart bleiben, sich mit dem individuellen Erinnerungsvermögen diverser Hacker auseinander zu setzen. Praktikabler ist dagegen der zweite Ansatz. Sobald Daten gespeichert werden, existieren „handfeste“ Beweismittel. Einer technischen Betrachtung hält jedoch keine der beiden Meinungen stand. Wie bereits eingangs angedeutet, werden die ersten Daten auf den Computer des potentiellen Eindringlings in dem Moment übertragen, in dem er sich die Inhalte des „geknackten“ Systems auf seinem Monitor anzeigen lässt.[270] Anders ist eine Visualisierung technisch nicht möglich. Die empfangenen Bilddaten werden dazu zunächst im Arbeitsspeicher abgelegt und teilweise darüber hinaus auch auf der Festplatte zwischengespeichert. Um dennoch den Willen der Bundesregierung umzusetzen, differenzieren manche Autoren zwischen Daten, die mit einem Zugriff auf das System verbunden sind, und solchen, die sich im System befinden. Der „Verschaffensbegriff“ soll abermals teleologisch reduziert werden, indem ein Erlangen der Zugangsdaten aus dem Tatbestand ausgeschieden wird.[271] Diese Ansicht lässt jedoch offen, anhand welcher Kriterien eine Unterscheidung zwischen beiden Arten von Daten erfolgen soll. Außerdem wird der einheitliche Datenbegriff des § 202a StGB unnötig aufgespalten. Im Ergebnis lässt sich daher eine „Hacking“-Strafbarkeit bereits *de lege lata* gut vertreten.[272] Für die folgenden Ausführungen soll dennoch der wohl hM in der Literatur gefolgt werden, da sie den Willen des Gesetzgebers am besten zum Ausdruck bringt.

3.1.6.1.3 Ergebnis zu § 202a StGB

§ 202a StGB unterscheidet sich in zweierlei Hinsicht von Art. 2: Zum einen erfasst er keine Manipulationen an der Hardware eines Computersystems. Zum anderen wir die Tathandlung des „sich Verschaffens“ von der hM im Softwarebereich teleologisch auf die Fälle der „Datenspionage“ reduziert. Dadurch sollen „Hacking“-Sachverhalte aus dem Anwendungsbereich der Vorschrift herausgenommen werden. Mit dieser einschränkenden Auslegung will die in

[265] Lackner/Kühl – *Kühl* § 202a Rn 5; Sch/Sch – *Lenckner* § 202a Rn 10; Tröndle/Fischer § 202a Rn 10; kritisch: Bühler MDR 1987, 448 (453)
[266] BT-Drs. 10/5058, S. 28
[267] Dogmatische Herleitung bei Preuße, S. 89 ff.
[268] Hilgendorf JuS 1996, 702 (705), LK – *Schünemann* § 202a Rn 6
[269] Haft NStZ 1987, 6 (10); Hauptmann JurPC, 215 (218)
[270] Hauptmann JurPC, 215 (217); Schmitz JA 1995, 478 (483)
[271] Lackner/Kühl – *Kühl* § 202a Rn 5; Tröndle/Fischer § 202a Rn 11
[272] Jessen, S. 179

der wissenschaftlichen Diskussion vorherrschende Meinung den Willen des deutschen Gesetzgebers umsetzen, nach dem das „bloßen Eindringen“ in ein Computersystem nicht nach § 202a StGB kriminalisiert werden soll.

Art. 2 der Konvention geht einen anderen Weg, indem er bereits Gefährdungen[273] der Geheimsphäre pönalisiert, ohne dass es zu einem Spionageerfolg und damit einer Verletzung dieses geschützten Bereichs kommen muss. Diese Vorschrift steht damit im Widerspruch zur Intention des deutschen Gesetzgebers bei Erlass des 2. WiKG.

3.1.6.2 § 17 Abs. 2 Nr. 1 UWG (Betriebsspionage)

Geschäfts- und Betriebsgeheimnisse besitzen im modernen Wirtschaftsleben erheblichen Vermögenswert, der oft über dem gewerblicher Schutzrechte liegen kann.[274] Sie werden daher strafrechtlich durch die §§ 17-20a UWG geschützt. § 17 UWG definiert drei Tatbestände betreffend den Geheimnisverrat (Abs. 1), die Betriebsspionage (Abs. 2 Nr. 1) sowie die unbefugte Geheimnisverwertung (Abs. 2 Nr. 2); § 18 stellt auf die sog. „Vorlagenfreibeuterei“ ab, d.h. die unbefugte Nutzung anvertrauter Geheimnisse durch Selbstständige; §§ 20 und 20a UWG stellen bestimmte Vorbereitungshandlungen unter Strafe und regeln die Anwendung der §§ 17 und 18 UWG für Auslandstaten. § 19 UWG sieht für Verstöße gegen §§ 17 und 18 UWG eine zivilrechtliche Schadensersatzpflicht vor. Vergleichbar mit Art. 2 erscheint in erster Linie § 17 Abs. 2 Nr. 1 UWG, der in Bezug auf die Tathandlung eine starke Ähnlichkeit zu § 202a StGB aufweist.

3.1.6.2.1 Rechtsgut und Tatbestand

§ 17 UWG schützt das Geschäfts- und Betriebsgeheimnis zu Gunsten des Betriebsinhabers und zu Gunsten eines unverfälschten Wettbewerbs. Die derzeit geltende Fassung wurde durch das 2. WiKG eingefügt.[275] Die Tathandlung unterscheidet sich im Wortlaut von § 202a StGB nur dadurch, dass der Täter sich ein Geschäfts- oder Betriebsgeheimnis „verschaffen oder sichern“ muss, wobei lit. a)-c) abschließend[276] drei Tatmittel aufzählt. Für einen Vergleich mit Art. 2 ist allein die in Art. 17 Abs. 2 Nr. 1 lit. a) UWG beschriebene „[…] Anwendung technischer Mittel […]“ von Bedeutung. Lit. b) und c) beschreiben keine computerspezifischen Sachverhalte.

„Sich Verschaffen“ wird wegen des identischen Wortlauts, der gleichen Entstehungsgeschichte wie § 202a StGB (2. WiKG) und dem Fehlen anders lautender Hinweise im Normkontext wie im Rahmen von § 202a StGB ausgelegt.[277] Der bloß flüchtige Blick auf ein Geschäfts- oder Betriebsgeheimnis beim Eindringen in ein Computersystem (lit. a)), stellt daher kein Verschaffen dar. „Sichern“ geht bereits vom natürlichen Wortsinn über „sich verschaffen“ hinaus und meint die Festigung und Vertiefung der Kenntnis(möglichkeit).[278] Auch diese Variante erfasst daher nicht das Hacken eines Computersystems.

[273] Hoeren/Sieber – *Sieber* 19 Rn 30, Kugelmann DuD 2001, 215 (218), auch wenn Art. 2 ff. im technischen Sinne keine Gefährdungsdelikte sind, sondern einen Erfolg voraussetzen.
[274] BGHZ 16, 172 (175 f.)
[275] Köhler/Piper – *Köhler* § 17 UWG Rn 1
[276] Köhler/Piper – *Köhler* § 17 UWG Rn 27
[277] Köhler/Piper – *Köhler* § 17 UWG Rn 26; Preuße, S. 95
[278] Köhler/Piper – *Köhler* § 17 UWG Rn 26

3.1.6.2.2 Ergebnis zu § 17 Abs. 2 Nr. 1 UWG

§ 17 Abs. 2 Nr. 1 UWG besitzt bzgl. der Tathandlung eine starke Ähnlichkeit zu § 202a StGB. Das Verbum „verschaffen“ wird in beiden Tatbeständen synonym verwendet und ist nicht schon mit dem Zugriff auf ein System erfüllt. Insofern kann auf die Ausführungen zu § 202a StGB verwiesen werden. Ebenso wenig erfasst die Tathandlungsvariante „sichern“ den flüchtigen Blick auf Daten, da bereits vom natürlichen Wortsinn die Festigung von Kenntnissen gemeint ist.

3.1.7 Bewertung Art. 2

Die Transformation von Art. 2 in das deutsche Strafrecht würde einen kriminalpolitischen Richtungswechsel im Vergleich zum 2. WiKG bedeuten. Dort äußerte der Gesetzgeber den Willen, das „bloße Eindringen“ in ein Computersystem nicht mit Strafe bedrohen zu wollen.[279] Statt einer bloßen Gefährdung von Daten und Systemen, die durch Hacker entstehen kann, stellt § 202a StGB nur auf den Verletzungserfolg der „Computerspionage“ ab. Dazu ist, wie die Darstellungen oben gezeigt haben, eine teleologische Reduktion des „Verschaffensbegriffs“ erforderlich, die sich in der Strafrechtslehre mittlerweile etabliert hat. Ohne eine Einschränkung dieses Merkmals ist eine „Hacking“-Strafbarkeit bereits *de lege lata* durch § 202a StGB angelegt, wodurch im Softwarebereich eine Übereinstimmung zu Art. 2 entstünde.

Für eine darüber hinausgehende Umsetzung von Art. 2 in deutsches Strafrecht ergeben sich vor allem Bedenken aus der Unbestimmtheit diese Tatbestandes. Die Erläuterungen zum Konventionstext beschränken sich ähnlich wie der Schriftliche Bericht des Rechtsausschusses zu § 202a StGB mit der Formulierung des „Eindringens“ in ein Computersystem. Dieser Terminologie liegt offensichtlich die Annahme zu Grunde, dass ein modernes Computersystem nach Überwindung einer Sicherheitshürde alle Daten und Funktionen preisgibt. Dies entspricht jedoch nicht der technischen Realität. „Echte“ Mehrbenutzersysteme wie „Unix“ oder „Linux“ vergeben Rechte in Abhängigkeit der auszuführenden Operation, des Benutzers oder einer Gruppe von Benutzern. Erlangt ein Hacker eine Gastberechtigung in einem solchen System, kann er weder die Daten der anderen Benutzer betrachten noch irgendwelche Beschädigungen am System (auf Softwareebene) vornehmen. Der Strafgrund des „Hacking“, den die Konvention in der Gefahr der Begehung weiterer Computerdelikte sieht, ist in diesem Fall nicht gegeben. Er liegt nur dann vor, wenn es dem Eindringling gelingt, die Administratoren- (engl. *root*) Rechte im Computersystem zu erlangen. Auf derartige Erwägungen geht Art. 2 nicht ein. Ein nach Art. 59 GG erforderliches Zustimmungsgesetz wird diese Frage näher beleuchten müssen, um nicht Gefahr zu laufen, wegen mangelnder Bestimmtheit[280] rechtswidrig zu sein.

Im Ergebnis ist eine generalisierende Betrachtungsweise des „Eindringens in ein Computersystem“ daher abzulehnen, da sie an der technischen Realität vorbeigeht und in rechtsdogmatischer Hinsicht bedenklich ist.

[279] Beschlussempfehlung und Bericht des Rechtsausschusses: BT-Drs. 10/5058, S. 28

[280] Allgemein zur Bestimmtheit von Strafvorschriften: Jescheck/Weigend, Strafrecht AT, § 15 III S. 136, § 58 IV S. 609

3.2 Artikel 3 – Rechtswidriges Abfangen[281]

Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um das mit technischen Hilfsmitteln bewirkte unbefugte Abfangen nichtöffentlicher Computerdatenübertragungen an ein Computersystem, aus einem Computersystem oder innerhalb eines Computersystems einschließlich elektromagnetischer Abstrahlungen aus einem Computersystem, das Träger solcher Computerdaten ist, nach ihrem innerstaatlichen Recht als Straftat festzulegen, wenn die Handlung vorsätzlich begangen wird. Eine Vertragspartei kann als Voraussetzung vorsehen, dass die Straftat in unredlicher Absicht oder in Zusammenhang mit einem Computersystem, das mit einem anderen Computersystem verbunden ist, begangen worden sein muss.

3.2.1 Anwendungsbereich

Art. 3 ergänzt den Schutz der Privatsphäre, indem er das Abfangen von Datenübertragungen im Zusammenhang mit Computern kriminalisiert. Dabei handelt es sich um eine Rechtsposition, die im deutschen Recht einfachgesetzlich durch Art. 8 EMRK[282] und verfassungsrechtlich durch Art. 10 GG[283] sowie Art. 1 Abs. 2 iVm 2 Abs. 2 GG[284] garantiert wird[285]. Nach dem Wortlaut bezieht sich Art. 8 Abs. 1 EMRK nur auf den Briefverkehr (engl. *correspondence*; franz. *correspondance*). Die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (EGMR) hat den Anwendungsbereich darüber hinaus auf Telefongespräche erweitert.[286] In der Kommentarliteratur wird vertreten, dass jede Kommunikationsform, die innerstaatlich vergleichbaren Schutz wie die traditionelle „Briefpost" erfährt, als „*correspondence/correspondance*" zu qualifizieren sei.[287] Art. 3 erstreckt sich den Erläuterungen zufolge auf alle Formen elektronischen Datentransfers, gleichgültig ob über Telefon, als Fax, Email oder als „*file transfer*". Die Gefährdungslage wird als vergleichbar zum Abhören herkömmlicher Sprachtelefonie bewertet. Aus dem Verweis auf Art. 8 EMRK wird deutlich, dass nur ein Austausch, an dem Privatpersonen beteiligt sind, von Art. 3 erfasst wird.[288] Datenübertragungen im Behördenverkehr werden nicht geschützt.[289] Der Tatbestand des Art. 3 wurde im Wesentlichen von dem Delikt „*Unauthorised Interception"* aus der Empfehlung Nr. R (89) 9[290] übernommen. Gängige Methoden werden in Kapitel 1.7.1 dargestellt.

3.2.2 Tatbestand

Die Tat bezieht sich auf Computerdatenübertragungen sowie auf elektromagnetische Abstrahlungen, aus denen Daten rekonstruiert werden können. Die emittierte Strahlung selbst besitzt keine Datenqualität im Sinne von Art. 1 lit. b) (siehe dazu Kapitel 2.2). An Übertragungsvor-

---

[281] ER Ziff. 51-59

[282] Zustimmungsgesetz vom 07.08.1952, BGBl. 1952 II, S. 685; BVerfGE 10, 271 (274) = NJW 1960, 1243 ff.; BayVerfGH NJW 1961, 1619; aM Echterhölter JZ 1955, 689 (691), für einen „übergesetzlichen Charakter" der EMRK.

[283] Zur mittelbaren Drittwirkung von Art. 10 GG nach der Privatisierung der Deutschen Bundespost: Groß JZ 1999, 326 (328)

[284] BVerfGE 90, 255 (260); Jarass/Pieroth – *Jarass* Art. 2 Rn 28; Meyer-Goßner MRK Art. 8 Rn 1

[285] Siehe dazu auch Kapitel 4.2.3.1.

[286] Klass./.D, GH 28, 21 ff. = EuGRZ 1979, 278 (284); Lüdi./.CH, GH 238, 19 = EuGRZ 1992, 300 ff.; Malone./.GB, GH 82, 30 ff. = EuGRZ 1985, 17 ff.

[287] Frowein/Peukert – *Frowein* Art. 8 Rn 34; zu den daraus resultierenden aktiven Schutzpflichten: Frowein/Peukert – *Frowein* Art. 8 Rn 9 ff., 35

[288] Frowein/Peukert – *Frowein* Art. 8 Rn 1 ff., 35

[289] Anders etwa § 202 StGB, vgl. Sch/Sch – *Lenckner* § 202 Rn 2

[290] *Recommendation on Computer-Related Crime*; Europarat, Computer-Related Crime, S. 53; Online: http://cm.coe.int/ta/rec/1989/89r9.htm (01.03.2004), allerdings ohne den „Report on Crime Problems", auf den die Empfehlung Bezug nimmt.

gängen werden nicht nur diejenigen zwischen verschiedenen, sondern auch solche innerhalb eines Computersystems erfasst, beispielsweise zwischen CPU und Peripheriegeräten. Es ist daher nicht nötig, dass zwei Personen miteinander kommunizieren. In diesem Zusammenhang ist auch Satz 2 zu sehen, der im Umkehrschluss verdeutlicht, dass Art. 3 ebenso wenig wie Art. 2 ein spezifisches „Netzwerkdelikt" ist, sondern grundsätzlich auch auf nicht vernetzte Rechner Anwendung findet. Nicht das Fernmeldegeheimnis, sondern die Privatsphäre eines jeden einzelnen Nutzers von EDV-Technik steht im Vordergrund.

Allerdings werden nicht alle Übertragungsvorgänge geschützt, sondern nur „nicht-öffentliche". Den Erläuterungen zufolge ist damit nicht der Inhalt der Daten, sondern der Ablauf des Kommunikationsvorgangs gemeint. Es kann sich daher um öffentlich zugängliche Daten handeln, solange die Beteiligten trotzdem in vertraulicher Weise miteinander kommunizieren wollen.[291] Auch wirtschaftliche Erwägungen kommen für einen Ausschluss der Öffentlichkeit in Betracht, beispielsweise bei kostenpflichtigen Pay-TV-Angeboten.[292] Das Merkmal bezweckt nicht den Ausschluss öffentlicher Übertragungswege. Auch die Kommunikation zwischen Arbeitnehmern wird unabhängig davon, ob sie geschäftlich oder privat erfolgt, in den Anwendungsbereich von Art. 3 miteinbezogen.[293]

Die Tathandlung besteht im „Abfangen" von Datenübertragungen. Damit werden alle Formen des Abhörens, Beobachtens sowie Überwachens eines Kommunikationsvorgangs verstanden, die zu einer Kenntnisnahme des Inhalts eines Kommunikationsvorgangs führen.[294] Dies kann durch einen direkten Zugriff auf das Computersystem erfolgen oder indirekt durch den Einsatz elektronischer Abhörtechnik.[295] „Abfangen" schließt auch die Anfertigung von Aufzeichnungen und Kopien mit ein. Die Tathandlung setzt den Einsatz technischer Hilfsmittel voraus. Darunter sind alle Arten von Hard- und Software zu verstehen, die Eingriffe in fremde Kommunikationen erlauben oder erleichtern.[296] Das Merkmal soll den Tatbestand begrenzen, indem es beispielsweise „den Blick über die Schulter" oder „die Benutzung eines Fernglases zum Ablesen der Daten auf dem Bildschirm" ausschließt.

Das Erfordernis einer besonderen Sicherung der übertragenen Daten wurde in den Tatbestand nicht aufgenommen. Zwar sahen auch die Verfasser der Konvention eine Gefahr der Überkriminalisierung und führten aus, dass nicht jedes „Mithören" unter Amateurfunkern strafbar sein soll.[297] Aus den Erläuterungen geht jedoch keine Möglichkeit hervor, wie der Anwendungsbereich der Vorschrift begrenzt werden kann. Dieses Problem dürfte sich in der Praxis vor allem dort stellen, wo WLAN-Technik zum Einsatz kommt. Die überwiegende Zahl der Nutzer dieser Technologie ahnt nicht, dass ihre Daten im Umkreis mehrerer Hundert Meter unverschlüsselt an eine Öffentlichkeit „ausgestrahlt" werden. Auch ohne besondere technische Kenntnisse können diese Datenübertragungen von jedermann mitgelesen und „abgefangen" werden.

3.2.3 Unbefugt

Wie im Rahmen von Art. 2 zählen auch die Erläuterungen zu Art. 3 eine Reihe von Sachverhalten auf, in denen sich eine Befugnis zum Abfangen von Datenübertragungen ergibt. An

[291] ER Ziff. 54
[292] ER Ziff. 54
[293] ER Ziff. 54
[294] ER Ziff. 53
[295] ER Ziff. 53
[296] ER Ziff. 53
[297] ER Ziff. 56

dieser Stelle werden beispielsweise Sicherheitstests und Schutzmaßnahmen genannt, die mit Wissen und Wollen des (der) Berechtigten erfolgen. Nach deutschrechtlichem Verständnis wäre hier nicht nur an eine Rechtfertigung, sondern bereits an einen Tatbestandsausschluss zu denken. Abhörmaßnahmen sind auch dann nicht unbefugt, wenn auf Grund einer gesetzlichen Grundlage in die Privatsphäre eingegriffen wird. Zu denken wäre in diesem Fall vor allem an die Tätigkeit der Sicherheits- und Ermittlungsbehörden. Ein weiterer Fall, der die Rechtswidrigkeit den Erläuterungen zufolge entfallen ließe, wäre die Ausübung sozialüblicher Verhaltensweisen. Darunter verstehen die Verfasser der Konvention beispielsweise den Einsatz von Cookies.[298] Diese Auffassung muss als zu undifferenziert kritisiert werden. Cookies werden bei Verwendung der Standardeinstellungen der meisten Browser[299] immer noch ohne Wissen und Wollen der Nutzer platziert. Gerade persistente Cookies von Drittanbietern, die der Erstellung persönlicher Verhaltens- und Konsumprofile in industriellem Umfang dienen, genießen in Bezug auf den Schutz der Privatsphäre einen zweifelhaften Ruf und sind von einer Sozialüblichkeit weit entfernt.[300]

3.2.4 Art. 3 Satz 2 – Einschränkungen

Die Verfasser der Konvention sahen einen engen Zusammenhang zwischen Art. 2 und 3. Zur Wahrung der Einheitlichkeit der Rechtsordnung sieht Satz 2 daher vor, dass die Vertragsstaaten wie bei Art. 2 Satz 2 weitere einschränkende Merkmale in den Tatbestand aufnehmen können. In objektiver Hinsicht kann die Vernetzung der betroffenen Computer verlangt werden; subjektiv das Vorliegen einer unredlichen Absicht. Anders als in Art. 2 Satz 2 kann die Verletzung von Sicherheitsmaßnahmen jedoch nicht einschränkend verlangt werden.

3.2.5 Vergleichbare Tatbestände im deutschen Strafrecht

Vom Wortlaut her scheinen vor allem die §§ 202a und 206 StGB vergleichbar zu sein.

3.2.5.1 § 202a StGB – Ausspähen von Daten

§ 202a StGB weist einen ähnlichen Anwendungsbereich wie Art. 3 auf. Es kommt nicht darauf an, ob die geschützten Daten ein materielles Geheimnis darstellen, d.h. nur einem begrenzten Personenkreis bekannt sind, sondern lediglich, ob sie sich in einer formellen Geheimhaltungssphäre (bzw. Geheimhaltungszustand bei der Übertragung) befinden. Hinsichtlich des Rechtsguts kann auf die Ausführungen in Kapitel 3.1.6.1.1 verwiesen werden. In Hinblick auf die Tathandlung spricht § 202a StGB von einem „Verschaffen“, das vom natürlichen Wortsinn über ein „Abfangen“ hinausgeht, welches sinngemäß nur im Übertragungsstadium von Daten ansetzen kann. Dies wird allerdings dadurch relativiert, dass Übertragungsvorgänge im Sinne von Art. 3 auch solche sind, die innerhalb eines Computersystems stattfinden. Letztlich spricht auch die Schutzintention des Art. 3, Beeinträchtigungen der Privatsphäre abzuwehren, für eine Vergleichbarkeit beider Tatbestände.

Für einen Vergleich sind an dieser Stelle, nachdem die Tathandlung des § 202a StGB bereits in Kapitel 3.1.6.1.2 dargestellt wurde, nur noch die Merkmale, „nicht für ihn bestimmt“ sowie „gegen unberechtigten Zugang besonders gesichert“ von Bedeutung. Ersteres weist Ähnlichkeiten mit den „nichtöffentlichen“ Datenübertragungen im Sinne der Konvention auf. „Unbe-

[298] ER Ziff. 58; im Anwendungsbereich von Art. 2: ER Ziff. 48
[299] Beispielsweise „Microsoft Internet Explorer“, „Netscape Navigator“, “Mozilla“ usw.
[300] Ausführlich dazu: Kapitel 1.7.1.2

fugt“ ist nach hM als Verweis auf das allgemeine Deliktsmerkmal der Rechtswidrigkeit gemeint[301] und braucht daher nicht näher erläutert zu werden.

3.2.5.1.1 Datenbestimmung

Die Bestimmung der Daten richtet sich danach, wer zum Zeitpunkt der Tathandlung nach dem Willen des Verfügungsberechtigten Zugang zu den Daten haben sollte.[302] Nach der neueren Rechtsprechung ist innerhalb eines Arbeits- bzw. Dienstverhältnisses entscheidend, ob jemand die generelle Nutzungsbefugnis hatte. Auf die Zulässigkeit des Datenabrufs im konkreten Einzelfall kommt es nicht an.[303] Auf diese Weise lässt sich auch der Fall des angestellten Programmierers lösen, der heimlich eine Kopie des von ihm für den Arbeitgeber angefertigten Programms erstellt und diese dann für eigene Zwecke nutzt.[304] Die Daten sind wegen der generellen Nutzungsbefugnis für ihn bestimmt, so dass eine Strafbarkeit wegen Ausspähens derselben ausscheidet. § 202a StGB zielt ebenso wenig wie § 202 StGB auf den „Insider“ ab, der sich lediglich treuwidrig verhält. Daher handelt es sich auch nicht um eine allgemeine Regelung zur (Insider-) Computerspionage.[305] Unberührt davon bleibt die urheber- und insbesondere arbeitsrechtliche Bewertung des Falles.[306] Folgt man dieser Auffassung, die an die allgemeine Befugnis anknüpft, so lässt sich eine Beschränkung der straffreien Zugriffe im Arbeitsverhältnis auf solche während der regelmäßigen Arbeitszeiten nicht aufrechterhalten. In Zeiten flexibler Arbeitszeiten und mobiler Arbeitsplätze erscheint diese Ansicht übertrieben bürokratisch.[307]

Für die Berechtigung des Verfügungsberechtigten kommt es auf die rechtliche Macht über die Daten an. Nicht entscheidend sind das Eigentum am Datenträger oder der Inhalt der Daten.[308] Die originäre Berechtigung an gespeicherten Daten richtet sich nach dem Akt der Erschaffung, d.h. nach dem Skripturakt der erstmaligen Datenabspeicherung.[309] Sie kann danach weiter übertragen werden, wenn die Vereinbarungen zwischen dem Nutzer und dem Primärberechtigten dies zulassen.[310] Befinden sich die Daten im Übertragungsstadium, ist auch der Empfänger Berechtigter.[311] Da die Bestimmung vom Willen des Berechtigten abhängt, ähnlich wie beim Diebstahl bzgl. der Frage des Gewahrsamsbruchs, kommt die dogmatische Figur des Einverständnisses, die von der Einwilligung strikt zu unterscheiden ist[312], zur Anwendung. Strafbar im Sinne von § 202a StGB kann sich nur machen, für wen die Daten noch nicht, nicht mehr, nicht unter diesen Umständen oder nicht zu dieser Zeit bestimmt sind („Datendiebstahl“).[313]

Für Programmdaten (z.B. WWW-Seiten, Java, ActiveX-Applets, usw.), die nach dem Willen

[301] Lackner/Kühl – *Kühl* § 202a Rn 7; Sch/Sch – *Lenckner* § 202a Rn 11
[302] BT-Drs. 10/5058, S. 29; Hilgendorf JuS 1996, 509 (512); LK – *Schünemann* (11. Aufl.) § 202a Rn 9; Sch/Sch – *Lenckner* § 202a Rn 6
[303] BayObLG NJW 1999, 1727 (1728); kritisch: Pätzel NJW 1999, 3246
[304] Siehe Schlüchter, S. 59 (63)
[305] Lenckner/Winkelbauer CR 1986, 483 (486)
[306] LK – *Schünemann* § 202a Rn 10
[307] aA: LK – *Schünemann* § 202a Rn 10, Lenckner/Winkelbauer CR 1986, 483 (486) und Schmitz JA 1995, 478 (482)
[308] Lackner/Kühl – *Kühl* § 202a Rn 3; LK – *Schünemann* § 202a Rn 12; Sch/Sch – *Lenckner* § 202a Rn 6; SK – *Hoyer* § 202a Rn 5; aA: Gössel BT 1 § 37 Rn 92
[309] LK – *Schünemann* § 202a Rn 12
[310] Hilgendorf JuS 1996, 509 (512), Schmitz JA 1995, 478 (481)
[311] Lackner/Kühl – *Kühl* § 202a Rn 3; Möhrenschlager wistra 1986, 127 (140)
[312] Jescheck/Weigend, Strafrecht AT, § 34 I, S. 373
[313] Haß, S. 467 (482)

des Gesetzgebers erfasst werden sollen, wird die Norm durch dieses Merkmal de facto zur Urheberschutzvorschrift. Mit Ausnahme von sog. „Open Source"-Produkten ist der Quellcode im Unterschied zu den beim bestimmungsgemäßen Gebrauch des Programms anfallenden Daten regelmäßig nicht für den Nutzer bestimmt. Die Vorschrift überschneidet sich daher an dieser Stelle mit Regelungen aus dem Urheberstrafrecht[314]. Eine Begrenzung des Anwendungsbereiches könnte – um die Wertungen des UrhG nicht zu unterminieren und in Hinblick auf das durch § 202a StGB geschützte Rechtsgut[315] – wie folgt vorgenommen werden[316]: Beschränkt sich der Täter auf das bloße Kopieren von Software, an der er zwar das Recht zur Nutzung – etwa durch den Kauf einer Programmkopie –, jedoch nicht zur Vervielfältigung hat, so kommt Urheberrecht zur Anwendung. § 202a StGB scheidet aus, weil der Täter sich die Originale, die er für das Anfertigen der Kopien benötigt, nicht mehr verschaffen muss.[317] Überschreitet er dagegen sein ihm eingeräumtes Nutzungsrecht durch den Versuch, an die nicht für ihn bestimmten Programmquelldaten heranzukommen, um deren gedanklichen Inhalt für einen anderen als die urheberrechtlich gestatteten Zwecke (beispielsweise durch §§ 69d, 69e UrhG) zu verwenden, liegt, wenn die weiteren Merkmale erfüllt sind, der Tatbestand des § 202a StGB vor.[318] Durch diese Auslegung können die Wertungen des Urheberrechts im Rahmen von § 202a StGB berücksichtigt werden.[319] Diese Abgrenzung basiert auf der Überlegung, dass bei der Nutzung von Computerprogrammen zwischen zwei Arten von Daten zu unterscheiden ist: zunächst der „Quellcode", der in kompilierter Form die Idee des Programms verkörpert, und im Unterschied dazu die „Ausgabedaten", mit denen der Nutzer bestimmungsgemäß in Kontakt kommt. Unberührt von dieser Abgrenzung bleiben Programme aus dem „Open Source"-Bereich, bei der die Nutzer nach dem Willen der Programmierer Einblick in die Quelldaten nehmen können, um die Software weiterzuentwickeln.

3.2.5.1.2 Die Datensicherung

Wann Daten gegen unberechtigten Zugang besonders gesichert sind, ist im Einzelnen umstritten. Einigkeit besteht insoweit, als der Berechtigte dem Täter in objektiver Hinsicht eine Schranke setzen muss, der ein subjektives Geheimhaltungsinteresse zu Grunde liegt.[320]

Das Merkmal „Zugang" wird im StGB nicht legal definiert. Unklar ist deshalb, ob damit lediglich die unmittelbare (logische) Zugriffsmöglichkeit auf die Daten beschrieben wird oder bereits der physische Zugang zum Computersystem oder zu einzelnen räumlichen Sicherheitsbereichen. Einen Anhaltspunkt könnte insofern die Anlage zu § 9 Satz 1 BDSG liefern, die in Nr. 2 von Maßnahmen zur „Zugangskontrolle" in Bezug auf die Nutzung von Datenverarbeitungssystemen spricht. Damit ist allerdings, wie ein Umkehrschluss zu § 9a BDSG zeigt, nur die Hardware gemeint, während § 202a StGB auf Daten im Sinne von § 202a Abs. 2 StGB abstellt. Auf Grund dieser unterschiedlichen Anknüpfungspunkte und der abweichenden Anwendungsgebiete beider Gesetze ist die datenschutzrechtliche Beschreibung des Zugangsmerkmals auf das Ausspähen von Daten im Sinne des StGB nicht übertragbar. Im Interesse größtmöglicher Sicherheit ist der Literatur deshalb darin zuzustimmen, den Zugangs-

[314] von Gravenreuth NStZ 1989, 201 (205); Lackner/Kühl – *Kühl* § 202a Rn 3; Sch/Sch – *Lenckner* § 202a Rn 6
[315] LK – *Schünemann* § 202a Rn 10; Tröndle/Fischer § 202a Rn 7; aA: Lenckner/Winkelbauer CuR 1986, 483 (486) und Schlüchter, S. 65
[316] Ähnlich: Leicht IuR 1987, 45 (50); Lenckner/Winkelbauer CR 1986, 483 (486)
[317] Tröndle/Fischer § 202a Rn 7
[318] LK – *Schünemann* § 202a Rn 10; Sch/Sch – *Lenckner* § 202a Rn 6
[319] Köhler/Piper – *Köhler* § 17 UWG Rn 10
[320] BT-Drs. 10/5058, S. 29; Leicht IuR 1987, 45 (45); Lenckner/Winkelbauer CR 1986, 483 (486); LK – *Schünemann* § 202a Rn 14; Sch/Sch – *Lenckner* § 202a Rn 7; Tröndle/Fischer § 202a Rn 8

begriff ohne Bezugnahme auf das BDSG möglichst weit auszulegen.[321] Ein Zugang liegt daher vor, wenn der Täter auf der physikalischen Ebene in der Lage ist, Manipulationen an der Hardware vorzunehmen und/oder auf der logischen Ebene mit dem System arbeiten kann.[322]

Umstritten ist weiterhin, ob das Merkmal „unberechtigt" neben dem Kriterium „nicht für ihn bestimmt" eine eigenständige Bedeutung hat. Ein Teil der Literatur verneint dies ohne nähere Begründung.[323] Nach anderer Ansicht korrespondiert das Tatbestandsmerkmal „unberechtigt" mit dem der „Bestimmtheit" der Daten. Nur diejenigen, für die die Daten bestimmt sind, können berechtigten Zugang haben; *allen* anderen muss die Zugangssicherung die fehlende Berechtigung verdeutlichen. Das Merkmal setzt nach dieser zweiten Ansicht einen Qualitätsstandard für Sicherheitsmechanismen. Es dürfen nicht irgendwelche sein, sondern nur solche, die gegenüber allen Unberechtigten, also den Personen, für die die Daten nicht bestimmt sind, bestehen. Sind die Daten auch nur einer Person gegenüber, für die sie nicht bestimmt sind, nicht geschützt (z.B. Systemadministrator, Reinigungs- und Wachpersonal, usw.), soll überhaupt keine tatbestandsmäßige Sicherung im Sinne von § 202a StGB vorliegen.[324] Diese Ansicht wird zu Recht kritisiert[325], denn der Gesetzeswortlaut spricht nicht davon, dass die Daten gegen jeden Zugang besonders gesichert sein müssen. Sie ist somit abzulehnen, da sie den Tatbestand über Gebühr einschränkt.

Zur Auslegung des Merkmals „besondere Sicherung" soll nach Ansicht des Gesetzgebers auf die Regelungen in §§ 202 Abs. 2 und 243 Abs. 1 Nr. 2 StGB zurückgegriffen werden.[326] Da beide Tatbestände sich jedoch auf den Schutz körperlicher Gegenstände beziehen, sind die dort entwickelten Grundsätze nicht unmittelbar auf die Sicherung unkörperlicher Daten übertragbar.[327] Anhaltspunkte können jedoch den Erkenntnisse zu § 243 Abs. 1 Nr. 2 StGB entnommen werden, der im Gegensatz zu § 202 Abs. 2 StGB nicht nur von „verschlossenen Behältnissen", sondern auch von „anderen Schutzvorrichtungen" spricht, die jedenfalls nach dem Gesetzeswortlaut keine Gegenständlichkeit voraussetzen. Danach müssen Sicherheitsvorrichtungen geeignet und bestimmt sein, den tatbestandlichen Erfolg zu erschweren. Maßgebliche Kriterien sind in objektiver Hinsicht der Sicherungsgrad und in subjektiver Hinsicht der vom Berechtigte verfolgte Schutzzweck.[328] Die Anforderungen, die an den Sicherungsgrad gestellt werden, dürfen nicht überspannt werden. Sicherlich geht es zu weit, eine besondere Sicherung erst dann anzunehmen, wenn sie dem Täter ein unüberwindbares Hindernis bereitet.[329] Wie in der Praxis bereits mehrfach bewiesen, gibt es einerseits keine derartigen Schutzmechanismen, wodurch das Merkmal ad absurdum geführt würde. Andererseits kann vor allem im Hinblick auf viktimodogmatische Überlegungen[330] nicht jede Vorkehrung genügen, die bereits von einem Laien überwunden werden kann, da es dann an der Manifestierung strafwürdiger krimineller Energie durch den Täter fehlt.[331] Praxisgerecht erscheint daher der Ansatz, eine besondere Sicherung dann anzunehmen, wenn der Berechtigte nach objektiven und für alle gleichermaßen geltenden Maßstäbe die Sicherung sorgfältig ausgesucht, instal-

[321] Leicht IuR 1987, 45 (46); Lenckner/Winkelbauer CR 1986, 483 (487)
[322] Jessen, S. 33, Weck, S. 36;
[323] Tröndle/Fischer § 202a Rn 8
[324] Lenckner/Winkelbauer CR 1986, 483 (487); Sch/Sch – *Lenckner* § 202a Rn 9; Meurer, FS-Kitagawa, S. 976
[325] Hilgendorf JuS 1996, 702 (704); Jessen, S. 136 f.; Leicht IuR 1987, 45 (46); LK – *Schünemann* § 202a Rn 15; Tröndle/Fischer § 202a Rn 8
[326] BT-Drs. 10/5058, S.29
[327] Leicht IuR 1987, 45 (46)
[328] Hilgendorf JuS 1996, 702 (702); Leicht IuR 1987, 45 (46); Sch/Sch – *Lenckner* § 202a Rn 7
[329] So noch: LK – Jähnke (10. Aufl.) § 202a Rn 15, 10; aA mittlerweile: LK – *Schünemann* (11. Aufl.) § 202a Rn 15
[330] Siehe: Sch/Sch – *Lenckner* Vorbem §§ 13 ff. Rn 70b
[331] Leicht IuR 1987, 45 (45); LK – *Schünemann* § 202a Rn 7; Lenckner/Winkelbauer CR 1986, 483 (486)

liert und betrieben hat.[332] Auf einen nicht unerheblichen Aufwand des Täters für die Überwindung der Sicherheit abzustellen[333], ist in zweifacher Hinsicht nicht befriedigend: Zum einen „knackt" ein versierter Eindringling Schutzvorrichtungen erheblich schneller als ein Amateur. Zum anderen ist daran zu denken, dass auf Grund der technischen Komplexität heutiger Anlagen, hochsichere Systeme binnen weniger Augenblicke durch die Veröffentlichung einschlägiger „*exploits*"[334] im Internet jedem gegenüber schutzlos werden können. In einem solchen Fall hat der Systemadministrator aber bis zur Aufdeckung des Fehlers objektiv sorgfältig gearbeitet, weshalb ihm strafrechtlicher Schutz erst versagt werden sollte, wenn er nach Bekanntwerden des Sicherheitsmangels nicht umgehend Abhilfe schafft. Der Grad der erforderlichen Sorgfalt kann anhand der Bedeutung der Daten bestimmt werden.

In subjektiver Hinsicht besteht Streit darüber, ob der Schutzzweck der Sicherung exklusiv in der Abwehr von Risiken für die bedrohten Daten bestehen muss[335] oder sich darüber hinaus auch auf andere gefährdete Interessen und Rechtsgüter erstrecken darf, jedenfalls solange die Funktion der Zugangssicherung nicht nur völlig untergeordnete Bedeutung hat.[336] Richtig ist auch hier eine vermittelnde Position einzunehmen. Konsequenzen hat dies vor allem für die Frage, ob nicht unmittelbar an den Daten angreifende Sicherungsvorrichtungen solche im Sinne des § 202a StGB sind, z.B. verschlossene Türen, der Pförtner am Tor des Betriebsgeländes, usw. Zwar fordert der Gesetzgeber keine strenge Unmittelbarkeit – anderenfalls hätte er dieses Kriterium in den Tatbestand aufgenommen –, jedoch fehlt es an der erforderlichen Dokumentation des Geheimhaltungsinteresses, wenn die Zugangssicherung nur ein völlig nachrangiger Zweck ist. Nach der hier vertretenen Ansicht wird eine tatbestandliche Datensicherung dann bejaht, wenn der Schutz von Informationen zumindest gleichrangig neben anderen Zielen steht. Dies bedeutet, dass das geschlossenen Firmentor nicht mehr als Sicherungsmaßnahme betrachtet wird, wohingegen der gesicherte Zugang zum Rechenzentrum sehr wohl eine Datensicherung darstellt. Der Schutz muss nicht unmittelbar am einzelnen Datum ansetzen, was wohl nur kryptographische Verfahren leisten, darf andererseits jedoch nicht nur reflexartig darauf ausstrahlen.[337]

Gängige Zugangssicherungen lassen sich danach unterscheiden, ob sie Daten im Übermittlungsstadium betreffen oder gespeicherte Daten. Da Daten während der Übertragung nicht stofflich fixiert sind, kommen auch keine körperlichen Sicherheitsvorkehrungen in Betracht. Die Isolierung von Kabeln und sonstige Abschirmungen, die das Austreten elektromagnetischer Strahlung verhindert, aus der Daten rekonstruiert werden können, dient regelmäßig allein dem störungsfreien Betrieb und nicht der Sicherung von Daten.[338] Etwas anderes muss freilich bei besonderen Abschirmungen etwa in Funknetzbereich (z.B. WLAN, Blue Tooth, usw.) gelten. Übrig bleiben daher allein kryptographische Verfahren (Verschlüsselung), obwohl hierdurch im eigentlichen Sinne nicht der Zugang zu den Daten, sondern nur zu ihrem Bedeutungsgehalt verhindert wird. Wenn aber nach dem Willen des Gesetzgebers auch Daten im Übermittlungsstadium durch § 202a StGB geschützt werden sollen, kommt man mangels Alternativen nicht umhin, Verschlüsselungsverfahren als besondere Zugangssicherungen an-

[332] Jessen, S. 120
[333] LK – *Schünemann* § 202a Rn 15
[334] Dt. ausbeuten, ausnutzen; hier: Sicherheitsloch in einem Computersystem, das durch sog. „*bug fixes*" (Software, die der Fehlerbeseitigung dient) der Hersteller behoben werden kann.
[335] Leicht IuR 1987, 45 (47)
[336] Jessen, S. 120; LK – *Schünemann* § 202a Rn 15; Sch/Sch – *Lenckner* § 202a Rn 7
[337] Vertreter dieser Ansicht siehe Fn 336.
[338] Leicht IuR 1987, 45 (47 f.), jedoch mit der Begründung, dass derartige Vorrichtungen für den Täter nicht erkennbar sind und daher das Geheimhaltungsinteresse nicht ausreichend dokumentieren; dagegen zu Recht: LK – *Schünemann* § 202a Rn 14

zuerkennen.[339] Gleichzeitig handelt es sich hierbei auch um sehr effektive Verfahren. Es bestehen auch keine Bedenken gegen steganographische Methoden[340], wenn das erforderliche Maß an Sorgfalt aufgewendet wird. Erkennt der Täter diese Art der Verschlüsselung nicht, kann dies auf Grund der Intention des Gesetzgebers an der Tauglichkeit der Sicherung nichts ändern. In Betracht kommt allenfalls ein Tatbestandsirrtum nach § 16 StGB. Gespeicherte Daten können darüber hinaus durch betriebsorganisatorische[341] (sog. „*Closed Shop*" Betrieb[342]) und physische Maßnahmen (z.B. Wegsperren von Rechner, Datenträger, usw.) sowie durch hard- (Magnetkarten, Biometrische Verfahren, usw.) und softwaretechnische Mechanismen (z.B. Passwörter, Kryptographie, usw.) geschützt werden. Umstritten ist, ob bloße Kopiersperren zum Schutz vor Softwarepiraterie darunter fallen sollen. Nach der hier vertretenen Auffassung muss dies verneint werden, da in solchen Fällen die Wertungen des Urheberrechts zu berücksichtigen sind, so dass sich eine Strafbarkeit allenfalls nach §§ 106 iVm 69a ff. UrhG ergeben kann.[343]

Das Merkmal der besonderen Sicherung beeinflusst darüber hinaus die Auslegung der Tathandlung. Ein „Verschaffen" von Daten im Sinne von § 202a StGB setzt nach verbreiteter Ansicht[344] voraus, dass dies gerade unter Überwindung der Zugangssicherung erfolgte. Anders als bei § 243 Abs. 1 Nr. 2 StGB wirke das Merkmal nicht nur straferhöhend, sondern bereits strafbegründend. Weiterhin kann durch diese Auslegung viktimodogmatischen Überlegungen Rechnung getragen werden, die besagen, dass der strafrechtliche Schutz dort zurücktreten soll, wo das Opfer sich selbst durch zumutbare und mögliche Maßnahmen vor Schaden schützen könne. Beispielsweise verneint die Literatur[345] strafrechtlichen Schutz durch § 202a StGB, wenn der Täter einem Arbeitskollegen über die Schulter blickt und Daten auf seinem Bildschirm abliest oder ein Fernglas dazu benutzt. Diese Ansicht überzeugt vor allem in systematischer Hinsicht und ist geeignet, eine Überkriminalisierung zu vermeiden.

3.2.5.1.3 Ergebnis zu § 202a StGB

§ 202a StGB unterscheidet sich von Art. 3 in mehreren Punkten. In Bezug auf die Tathandlung weicht der Wortlaut beider Vorschriften deutlich voneinander ab. Inhaltlich besteht jedoch starke Ähnlichkeit. Ein „Abfangen" im Sinne von Art. 3 scheint den Tatbestand zwar auf Übertragungsvorgänge in Netzwerke zu beschränken, während § 202a StGB auch gespeicherte Daten erfasst. Diese Unterscheidung wird jedoch dadurch nivelliert, dass Datenübertragungen im Sinne der Konvention auch solche innerhalb eines Computersystems sind.[346] Sowohl „verschaffen" als auch „abfangen" bezeichnen letztlich übereinstimmend eine Kenntnisnahme des Dateninhalts. Einschränkend kommt bei der Konvention hinzu, dass dieser Er-

[339] Jessen, S. 161; LK – *Schünemann* § 202a Rn 16;Lenckner/Winkelbauer CR 1986, 483 (487); Leicht IuR 1987, 45 (51 f.); Möhrenschlager wistra 1986, 128 (140); Sch/Sch – *Lenckner* § 202a Rn 8; Tröndle/Fischer § 202a Rn 8

[340] Damit werden kryptographische Verfahren bezeichnet, die darauf beruhen, dass Daten äußerlich nicht erkennbar in anderen Daten versteckt werden, beispielsweise soll in einem geschlossenen Text nur jedes x-te Wort oder jedes x-te Zeichen eine Bedeutung haben, wenn es in einer vorher vereinbarten Reihenfolge neu kombiniert wird; MK – Graf § 202a Rn 41

[341] LK – *Schünemann* § 202a Rn 16; Sch/Sch – *Lenckner* § 202a Rn 8; Tröndle/Fischer § 202a Rn 8

[342] Räumliche Einteilung in hierarchisch abgestufte Sicherheitszonen; ausführlich dazu: Leicht IuR 1987, 45 (48) und Lenckner/Winkelbauer CR 1986, 483 (487)

[343] Haß, S. 481 f.; LK – *Schünemann* § 202a Rn 15; aA: Sch/Sch – *Lenckner* § 202a Rn 8

[344] Hilgendorf JuS 1996, 702 (705); LK – *Schünemann* § 202a Rn 7; OLG Celle CR 1990, 276 (277) mit Anmerkung von Etter; Sch/Sch – *Lenckner* § 202a Rn 7, 10; Sch/Sch – *Lenckner* Vorbem §§ 13 ff. Rn 70b mwN;

[345] Hilgendorf JuS 1996, 702 (705); LK – *Schünemann* § 202a Rn 7

[346] Siehe Kapitel 3.2.2

folg unter Zuhilfenahme „technischer Hilfsmittel“ bewirkt werden muss. Im Gegensatz zum deutschen Recht genügt dazu der „Blick über die Schulter“ oder eine andere „untechnische“ Verhaltenweise nicht.
Das Merkmal „nicht-öffentlich“ ähnelt inhaltlich der „Datenbestimmung“ in § 202a StGB. In beiden Fällen wird damit der Wille des Verfügungsberechtigten bezeichnet, die Daten, die kein Geheimnis im materiellen Sinne darstellen müssen, nicht einem beliebigen Personenkreis zugänglich zu machen. Während das StGB zur Bestimmung der Berechtigung vor allem auf den sog. „Skripturakt“, d.h. die Datenerzeugung abstellt, kommt es im Sinne der Konvention auf die Modalitäten der Übertragung an.

Der entscheidende Unterschied besteht in der Zugangssicherung, die von Art. 3 überhaupt nicht verlangt wird. Zwar deutet das Merkmal „technische Hilfsmittel“ im Tatbestand von Art. 3 zunächst auf Schutzvorrichtungen hinsichtlich der Daten hin, denn anderenfalls müsste der Täter nicht mit den genannten Werkzeugen vorgehen. Bei genauerer Betrachtung wird dadurch allerdings nur der Vorgang des „Abfangens“ näher charakterisiert und untechnische Tathandlungen werden ausgeschieden.

3.2.5.2 § 17 Abs. 2 Nr. 1 lit. a) UWG (Betriebsspionage)

Wie bereits in Kapitel 3.1.6.2.1 dargestellt, wird das Merkmal des „Verschaffens“ im Rahmen von § 17 Abs. 2 Nr. 1 UWG und § 202a StGB ähnlich ausgelegt. Insofern ergibt sich eine Vergleichbarkeit zu Art. 3.

3.2.5.2.1 Tatbestand

Für einen Vergleich sind an dieser Stelle die objektiven Merkmale „Geschäfts- oder Betriebsgeheimnis“ sowie „Anwendung technischer Hilfsmittel“ und die subjektiven Beweggründe „zu Zwecken des Wettbewerbs“, „aus Eigennutz“, „zu Gunsten eines Dritten“ sowie „in der Absicht, dem Inhaber des Geschäftsbetriebs Schaden zuzufügen“ von Bedeutung.

Im Wettbewerbsrecht werden nicht beliebige Daten geschützt, sondern nur solche, die ein Geschäfts- oder Betriebsgeheimnis verkörpern. Erstgenanntes umfasst grundsätzlich geheime Angaben in Bezug auf Zustand oder Marktverhalten eines Unternehmens; zweitgenanntes vorwiegend technische Daten, wie insbesondere auch Computerprogramme.[347] Die „Anwendung technischer Mittel“ beinhaltet das „Anzapfen“ von EDV-Anlagen und Datenleitungen sowie den Einsatz von Computern.[348] Neben dem allgemeinen Vorsatz verlangt der subjektive Tatbestand das Vorliegen eines der vier in § 17 Abs. 2 Nr. 1 UWG aufgezählten Beweggründe.

3.2.5.2.2 Ergebnis zu § 17 Abs. 2 Nr. 1 UWG

§ 17 Abs. 2 Nr. 1 lit. a) UWG schützt nicht beliebige Daten, sondern nur materiell geheime mit besonderem Unternehmensbezug. Anders als § 202a StGB müssen diese jedoch nicht besonders gesichert sein. Annähernd wortgleich zu Art. 3 stellt das Wettbewerbsrecht auf den Einsatz technischer Hilfsmittel ab und verlangt wie Art. 3 Satz 2 besondere subjektive Beweggründe.

[347] Köhler/Piper – *Köhler* § 17 UWG Rn 10 mwN
[348] Köhler/Piper – *Köhler* § 17 UWG Rn 27

3.2.5.3 § 206 StGB – Verletzung des Post- oder Fernmeldegeheimnisses

§ 206 StGB erscheint vergleichbar mit Art. 3, weil dieser auf das Abfangen von Computerdaten während der Übertragung abstellt. Übertragungsvorgänge gehören nach der Legaldefinition des § 3 Nr. 16 TKG, die auch Anhaltspunkte für das Strafrecht liefert, zur Telekommunikation und werden durch das Fernmeldegeheimnis geschützt. § 206 StGB trat im Zuge der Postreform an die Stelle des § 354 StGB[349], da das Delikt durch die Privatisierung von Briefpost und Telekommunikation kein Amtsdelikt mehr darstellte.

Der Tatbestand des § 206 StGB beschreibt kein typisches Computerdelikt. Tatobjekte sind nicht Daten, sondern „Tatsachen" (Abs. 1) usw., die dem Post- und Fernmeldegeheimnis unterliegen. Dementsprechend kommt es auch nicht auf ein „Abfangen" oder „Verschaffen" an, sondern beispielsweise auf die Weitergabe dieser Kenntnisse (Abs. 1). Abs. 2 bezieht sich nur auf körperliche Gegenstände[350] und kommt daher für einen Vergleich zu Art. 3 von vornherein nicht in Betracht. Ebenso wenig weisen die Abs. 3-5 Ähnlichkeit zu Art. 3 auf.

3.2.6 Bewertung Art. 3

Art. 3 zielt auf den Schutz der Privatsphäre ab, ohne dem Betroffenen – wie etwa § 202a – StGB Anstrengungen zum Selbstschutz abzuverlangen. Ebenso wenig erfolgt eine Beschränkung auf besonders schutzwürdige Daten, wie etwa im Wettbewerbsrecht (Geschäfts- bzw. Betriebsgeheimnisse). Gerade im Internet, das auf Grund seiner Entstehung als Wissenschaftsnetz nahezu keine proprietären Sicherheitsmechanismen kennt, droht die Gefahr der Überkriminalisierung. Die einzige Abhilfe bestünde – wie die Ausführungen in Kapitel 3.2.5.1.2 gezeigt haben – im Erfordernis der Verschlüsselung der übermittelten Daten. Zwar heben die Erläuterungen in diesem Zusammenhang auf die Pay-TV-Technik ab, die ohne Kryptographie nicht zu vermarkten wäre, allerdings ohne die Zugangssicherung in den Rang eines Tatbestandsmerkmals zu erheben. Eine Begrenzung des Tatbestands wäre möglich, indem das Merkmal „technische Hilfsmittel" restriktiv ausgelegt würde. Durch die Bezugnahme auf das Tatobjekt „elektromagnetische Abstrahlungen" wird dies im Wortlaut von Art. 3 bereits angedeutet, denn auf derartige Strahlung kann nur mit einem hohen technischen Aufwand zugegriffen werden. Jedoch scheint es problematisch, die Begrenzung der Strafbarkeit nach Art. 3 von der Güte der eingesetzten Technik abhängig zu machen, da dieses Kriterium inhaltlich zu unbestimmt ist und von Fall zu Fall anders zu beurteilen sein wird. In Betracht käme ebenso, nicht alle, sondern nur besonders schutzwürdige Daten (beispielsweise materiell geheime) strafrechtlich zu schützen. Zusammenfassend bleibt daher zwar zu begrüßen, dass Art. 3 einen verstärkten Schutz der Privatsphäre intendiert. An der gesetzestechnischen Umsetzung muss hingegen kritisiert werden, dass der Tatbestand, ähnlich wie bereits Art. 2, kaum begrenzbar ist.

[349] BegleitG zum TKG, Art. 2 Abs. 13 Nr. 6, BGBl. 1997 I, S. 3108 ff.
[350] Tröndle/Fischer § 206 Rn 11

3.3 Artikel 4 – Eingriffe in Daten[351]

(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um das unbefugte Beschädigen, Löschen, Beeinträchtigen, Verändern oder Unterdrücken von Computerdaten als Straftat nach ihrem innerstaatlichen Recht festzulegen, wenn die Handlung vorsätzlich begangen wird.

(2) Eine Vertragspartei kann sich das Recht vorbehalten, als Voraussetzung vorzusehen, dass das in Absatz 1 beschriebene Verhalten zu einem schweren Schaden geführt haben muss.

3.3.1 Anwendungsbereich

Art. 4 zielt darauf ab, Computerdaten und Computerprogrammen einen vergleichbaren Schutz vor der vorsätzlichen Zufügung von Schaden zu bieten, wie ihn körperliche Gegenstände bereits genießen. Der Tatbestand erinnert an § 303 StGB, mit dem Unterschied, dass es sich um unkörperliche Tatobjekte handelt. Die Erläuterungen führen aus, dass die Norm den Schutz der Integrität und der fehlerfreien Funktion der gespeicherten Daten oder Programme beabsichtigt. In Computernetzen wird dieses Schutzgut vor allem durch Schadprogramme wie Viren, Würmer usw. beeinträchtigt (siehe dazu Kapitel 1.7.2).

3.3.2 Tatbestand

In Bezug auf den Begriff der „Computerdaten“ kann auf die Ausführungen zu Art. 1 lit. b). (Kapitel 2.2) verwiesen werden. Als Tathandlungen kommen das „Beschädigen, Löschen, Beeinträchtigen, Verändern und Unterdrücken“ von Computerdaten in Betracht. Die Varianten „Beschädigen“ und „Beeinträchtigen“ überschneiden sich weitgehend und erfassen negative Veränderungen der Integrität oder des Informationsgehalts von Daten und Programmen. Das „Löschen“ von Daten stellt das Äquivalent zur Zerstörung von körperlichen Gegenständen dar. Die Daten werden dadurch vernichtet und unerkennbar gemacht. Das „Unterdrücken“ von Computerdaten beinhaltet jede Handlung, die die Verfügbarkeit von Daten für diejenige Person, die Zugang zu dem Computer oder dem Datenträger hat, auf dem sie gespeichert sind, verhindert oder beendet. Unter „Veränderung“ ist jede Modifikation bestehender Daten zu verstehen. Art. 4 erfasst daher den Erläuterungen zufolge sowohl das Einbringen von Schadprogrammen, wie Viren und Trojanern, als auch die daraus resultierenden Veränderungen von Daten.[352]

3.3.3 Unbefugt

In Bezug auf das Merkmal „unbefugt“ kann grundsätzlich auf die Ausführungen zu Art. 2 verwiesen werden (Kapitel 3.1.4). Wie bereits dort beschrieben, legen die Erläuterungen großen Wert darauf, dass Handlungen mit Wissen und Wollen des Berechtigten – etwa Sicherheitstests – nicht kriminalisiert werden sollen.

Besondere Erwähnung in den Erläuterungen finden darüber hinaus die sog. „Anonymisierungsdienste“.[353] Diese bieten als Dienstleistung – untechnisch gesprochen – die Verschleierung der Identität des Benutzers an, indem beispielsweise (eindeutige) IP- oder Email-

[351] ER Ziff. 60-64
[352] ER Ziff. 61
[353] ER Ziff. 62

Adressen des Benutzers unterdrückt oder in sonstiger Weise unkenntlich gemacht werden.[354] Dies geschieht in der Regel durch eine Modifikation der Verbindungsdaten (siehe Kapitel 2.4). Die Erläuterungen betrachten derartige Aktivitäten grundsätzlich als legitimen Schutz der Privatsphäre und damit nicht als unbefugt. Die Vertragsparteien können jedoch Ausnahmen von diesem Prinzip vorsehen, soweit diese Dienste zu kriminellen Zwecken missbraucht werden.

3.3.4 Art. 4 Abs. 2 – Vorbehalt

Im Unterschied zu Art. 2 und 3 erlaubt Art. 4 Abs. 2 den Vertragsparteien einen Vorbehalt bezüglich der Umsetzung eines Merkmals im Tatbestand zu erklären. Dabei handelt es sich um das Erfordernis eines „schweren Schadens", das in Abs. 1 nicht vorgesehen ist. Anders als bei den Art. 2 und 3, die zwar Anpassungen im Tatbestand erlauben, jedoch keinen Vorbehalt vorsehen, sind die Vertragsparteien, soweit sie von der Möglichkeit in Art. 4 Abs. 2 Gebrauch machen, gehalten, die in den Art. 42 f. vorgeschrieben Voraussetzungen zu beachten. Dort wird zum einen auf den *numerus clausus* der Vorbehalte in Bezug auf die Konvention hingewiesen. Zum anderen heißt es hinsichtlich des Verfahrens, dass der Generalsekretär durch eine schriftliche Notifikation zu benachrichtigen sei, soweit von einem Vorbehalt Gebrauch gemacht, Art. 42, bzw. soweit dieser zurückgenommen oder geändert werde, Art. 43.

Vorbehalte kommen im Unterschied zu flexiblen Voraussetzungen im Tatbestand[355] immer dann zur Anwendung, wenn der Europarat besonderes Augenmerk auf eine einheitliche Umsetzung legt. In diesem Zusammenhang sieht Art. 43 Abs. 3 daher vor, dass der Generalsekretär sich in regelmäßigen Abständen bei den Vertragsparteien nach den Aussichten für die Rücknahme eines Vorbehalts erkundigen kann.

3.3.5 Vergleichbare Tatbestände im deutschen Strafrecht

Das StGB enthält im 27. Abschnitt (Sachbeschädigung) mit § 303a StGB einen annähernd wortgleichen Tatbestand.

3.3.5.1 § 303a StGB – Datenveränderung

In der Literatur findet sich die formelhafte Formulierung, dass das geschützte Rechtsgut das „Interesse"[356] des Verfügungsberechtigten an der unversehrten Verwendbarkeit der „in den gespeicherten Daten verkörperten Informationen"[357] sei. Richtigerweise sollte auf die Integrität der Daten[358] abgestellt werden, da anderenfalls die Codierung der Informationen[359], d.h. die Darstellung der vermittelten Inhalte,[360] entgegen dem Wortlaut der Vorschrift keinen Schutz erfährt. Auf einen Vermögenswert der Daten kommt es – wie bei § 202a StGB – man-

[354] Bekanntestes Beispiel; http://www.anonymizer.com (01.03.2004)
[355] Siehe Art. 2 Satz 2 sowie Art. 3 Satz 2.
[356] So wörtlich: LK – *Tolksdorf* § 303a Rn 2; Möhrenschlager wistra 1986, 128 (141); NK – *Zaczyk* § 303a Rn 2; Sch/Sch – *Stree* § 303a Rn 1, wenngleich zweifelhaft erscheint, inwieweit ein „Interesse" ein schutzfähiges Rechtsgut darstellen kann; aA: SK – *Hoyer* (6. Aufl.) § 303a Rn 1
[357] Sch/Sch – *Stree* § 303a Rn 1; Tröndle/Fischer § 303a Rn 2
[358] Hilgendorf JuS 1996, 890 (890); Lackner/Kühl – *Kühl* § 303a Rn 1; LK – *Tolksdorf* § 303a Rn 2; Möhrenschlager wistra 1986, 128 (141); Schlüchter, S. 70 f.; Sondermann, S. 25; SK – *Hoyer* § 303a Rn 1; wohl auch: BayObLG wistra 1993, 304 (305)
[359] Hilgendorf JuS1996, 890 (891)
[360] Siehe zum Datenbegriff des StGB: Kapitel 2.2.1

gels besonderer Anhaltspunkte im Gesetz nicht an.[361]

3.3.5.1.1 Tatbestand

Tatobjekte sind wegen des Verweises auf § 202a StGB Daten in der dort bestimmten Form (siehe Kapitel 2.2.1). Als Tathandlungen kommen das „Löschen", „Unterdrücken", „Unbrauchbarmachen" und „Verändern" in Betracht. Mit Ausnahme der dritten Variante sind sie wortgleich zur deutschen Übersetzung von Art. 4, so dass an dieser Stelle nur ein kurzer Überblick gegeben wird.

Wie auch im Rahmen von Art. 4 überschneiden sich die einzelnen Tathandlungen, um Strafbarkeitslücken zu vermeiden.[362] Das „Löschen" entspricht dem Zerstören von Sachen im Sinne von § 303 StGB. Erforderlich ist, dass die Daten dauerhaft und unwiederbringlich vom Datenträger entfernt bzw. unkenntlich gemacht werden.[363] Eine „Datenunterdrückung" liegt vor, wenn die Daten zwar nicht gelöscht, dem Zugriff des Berechtigten jedoch wenigstens vorübergehend entzogen und deshalb nicht mehr von ihm verwendet werden können.[364] Die Fälle der „Datenveränderung" erfassen die inhaltliche Modifikation eines einzelnen Datums (des Codes und der Information), die Abänderung der Reihenfolge mehrerer Daten sowie die Veränderung des Datenkontextes, ohne dass dies in allen Varianten eine Funktionsbeeinträchtigung zur Folge haben müsste.[365]

Klärungsbedarf besteht vor allem in Hinblick auf das Kriterium des „Unbrauchbarmachens", das die deutsche Strafnorm an Stelle des „Beschädigens" bzw. „Beeinträchtigens" im Sinne der Konvention verwendet. Daten werden „unbrauchbar gemacht", wenn sie zwar nicht gelöscht oder unterdrückt, in ihrer Gebrauchsfähigkeit jedoch derart beeinträchtigt werden, dass sie nicht mehr zu ihrem bestimmungemäßem Zweck verwendet werden können.[366] Dies dürfte, um die einzelnen Varianten klar voneinander abgrenzen zu können, in erster Linie bei sinnentstellenden Hinzufügungen[367], nicht jedoch bei (Teil-) Löschungen[368] der Fall sein, da diese Handlung bereits von der 1. Variante erfasst wird. Ebenso wie Art. 4 will auch § 303a StGB den Problemen im Zusammenhang mit Computerviren entgegentreten. Dabei kommt es in erster Linie auf die technische Wirkungsweise des Virus an. Wird der Benutzer im Rahmen seiner Reproduktion oder durch eine „Zusatzfunktionen" lediglich belästigt, liegt nach verbreiteter Ansicht keine der in § 303a StGB aufgezählten Tatvarianten vor.[369]

[361] Lackner/Kühl – *Kühl* § 303a Rn 1; Schlüchter, S. 71; SK – *Hoyer* § 303a Rn 3 und § 202a Rn 1; vermittelnde Ansicht: Hilgendorf JuS 1996, 890 (890), LK – *Tolksdorf* § 303a Rn 2 sowie Welp IuR 1986, 443 (448 f.)

[362] Lackner/Kühl – *Kühl* § 303a Rn 3; LK – *Tolksdorf* § 303a Rn 19; Sch/Sch – *Stree* § 303a Rn 4; Tröndle/Fischer § 303a Rn 8

[363] BT-Drs. 10/5058, S. 34; Lackner/Kühl – *Kühl* § 303a Rn 3; Sch/Sch – *Stree* § 303a Rn 4; Tröndle/Fischer § 303a Rn 9; differenzierend: Hilgendorf JuS 1996, 890 (891); LK – *Tolksdorf* § 303a Rn 23, 24

[364] BT-Drs. 10/5058 S. 35; Hilgendorf JuS 1996, 890 (891); Lackner/Kühl – *Kühl* § 303a Rn 4; Sch/Sch – *Stree* § 303a Rn 4

[365] Hilgendorf JuS 1996, 890 (891); Lackner/Kühl – *Kühl* § 303a Rn 3; T/K § 303a Rn 8; Welp IuR 1988 Sonderheft, 434 (435); eine Funktionsbeeinträchtigung erfordernd: BT-Drs. 10/5058, S.35; eine Bedeutungsverschiebung erfordernd: SK – *Hoyer* § 303a Rn 11; zu eng: Sch/Sch – *Stree* § 303a Rn 4

[366] BT-Drs. 10/5058, S. 35; Hilgendorf JuS 1996, 890 (891)

[367] SK – *Hoyer* § 303a Rn 10; Tröndle/Fischer § 303a Rn 11

[368] So jedoch: Sch/Sch – *Stree* § 303a Rn 4

[369] Eingehend: Mühle, S. 160; ungenau: LK – *Tolksdorf* § 303a Rn 32

3.3.5.1.2 Rechtswidrigkeit

Das Merkmal „rechtswidrig“ hat nach heute weit verbreiteter Auffassung[370] eine Doppelfunktion: Es soll zum einen den Tatbestand eingrenzen und zum anderen Ausdruck des allgemeinen Verbrechensmerkmals der Rechtswidrigkeit sein. Eine Einschränkung ist nötig, da § 303a StGB – würde man in dem Wort „rechtswidrig“ nur einen Hinweis auf das allgemeine Verbrechensmerkmal sehen – keine per se sozialinadäquaten Vorgänge beschreibt. So würde beispielsweise die Veränderung selbst zusammengestellter Daten strafrechtlich sanktioniert werden, obwohl es sich hierbei ganz offensichtlich um einen alltäglichen und unbedenklichen Vorgang handelt, der keinen Unrechtsgehalt aufweist.[371] Nach der ganz herrschenden Meinung besteht eine wesentliche Aufgabe des gesetzlichen Tatbestandes jedoch gerade darin – vor allem im Hinblick auf das Bestimmtheitsgebot nach Art. 103 Abs. 2 GG und § 1 StGB – den Unrechtsgehalt einer Deliktsart positiv zu vertypen.[372] Diese Anforderungen erfüllt § 303a StGB nur, wenn der Tatbestand um ein ungeschriebenes Tatbestandsmerkmal ergänzt[373] oder dem Wort „rechtswidrig“ eine weitere, den Tatbestand beschränkende Bedeutung zugewiesen wird. Den Vorzug verdient die letztgenannte Auffassung, da sie einerseits einen Anhaltspunkt im Wortlaut der Norm findet und andererseits mit der Auslegung des Merkmals „unbefugt“ in Tatbeständen korrespondiert, die ohne eine „rechtswidrig“ begangene Tathandlung ebenfalls keinen typischen Unwertgehalt aufweisen. Vergleiche etwa § 107a StGB, Wahlfälschung). Der Vorgang des Wählens an sich ist neutral und wird erst durch die „rechtswidrige“ – etwa infolge von §§ 45, 92a, 101, 108c StGB – Stimmabgabe strafwürdig.

Ohne eine Beschränkung des Tatbestandes würde § 303a StGB eine Vielzahl sozialadäquater Handlungen pönalisieren, wenn auf der zweiten Prüfungsebene gerade kein Rechtfertigungsgrund zur Hand wäre. Zwar ist an eine rechtfertigende Einwilligung des Täters in eine eigene Rechtsgutsverletzung zu denken, allerdings ist *Hilgendorf*[374] darin zuzustimmen, dass dies „hochgradig konstruiert“ erscheint. Die Ansicht in der Literatur, der hier gefolgt wird, leitet daher aus dem Merkmal der Rechtswidrigkeit auf der Tatbestandsebene ein Kriterium für die Datenzuordnung ab und verengt damit den Kreis der tauglichen Tatobjekte. Entscheidend ist das Verfügungs- bzw. Nutzungsrecht des Täters bzw. eines Dritten an den Daten. Dabei soll es sich um eine „eigentümerähnliche“ Rechtsposition[375] handeln, die mit dem Kriterium der „Fremdheit“ in § 303 StGB korrespondiert. Ein Teil der Literatur[376] stellt auf die Perspektive des Täters ab und hinterfragt sein positives Recht an den Daten. Eine andere Ansicht beleuchtet die Berechtigung aus dem Blickwinkel, ob Nutzungsrechte Dritter bestehen, die ein Löschen, Unterdrücken, usw. rechtswidrig erscheinen lassen, da dem Täter in negativer Hinsicht das Recht fehlt, über die Daten zu verfügen.[377] Im Ergebnis weichen beide Meinungen nur unwesentlich voneinander ab. Bei dem Verfügungs-/Nutzungsrecht (des Berechtigten oder Dritten) an den Daten kann es sich nur um eine obligatorische Rechtsposition handeln, da mit Ausnahme von §§ 1068, 1273 BGB sowie den grundstücksgleichen Rechten dingliche Rechte nur (körperliche) Sachen zum Gegenstand haben können.[378] Teilweise wird in der Literatur[379]

[370] Granderath DB 1986, Beil. 18, 1 (3); Hilgendorf JuS 1996, 890 (892); Lackner/Kühl – *Kühl* § 303a Rn 4; Schlüchter, S. 74; Sondermann, S. 154 f.; SK – *Hoyer* § 303a Rn 2; Tröndle/Fischer § 303a Rn 13

[371] Welp IuR 1988, 443 (446) sieht daher in der gesetzlichen Deliktsbeschreibung eine angemessene Bezeichnung für Berufsgruppen (z.B. Programmierer und Datentypisten), nicht aber für kriminelles Unrecht.

[372] Jescheck/Weigend, Strafrecht AT, § 25 I, S. 244 ff. mwN; Schlüchter, S. 68

[373] LK – *Tolksdorf* § 303a Rn 7, unter Hinweis auf eine mangels hinreichender Bestimmtheit drohende Verfassungswidrigkeit der Norm; Sch/Sch – *Stree* § 303a Rn 6

[374] Hilgendorf JuS1996, 890 (892); LK – *Tolksdorf* § 303a Rn 8 ff.

[375] Lenckner/Winkelbauer CR 1986, 824 (829)

[376] Hilgendorf JuS1996, 890 (892 f.)

[377] SK – *Hoyer* § 303a Rn 5

[378] Palandt – *Bassenge* Einf v 854 Rn 4

[379] Gerhards, S. 49 ff.; Preuße, S. 80

auf eine Parallele zu § 274 Abs. 1 Nr. 2 StGB abgestellt – eine Vorschrift, die ebenfalls durch das 2. WiKG eingefügt wurde – , die jedoch keine neuen Erkenntnisse für taugliche Zuordnungskriterien im Rahmen des § 303a StGB liefert, da § 274 Abs.1 Nr. 2 StGB im Zusammenhang mit Nr. 1 zu interpretieren ist[380], der letztlich wieder auf das zivilrechtliche, aus § 903 BGB entspringende Beweisführungsrecht verweist.

Grundsätzlich muss zwischen dem originären und dem derivativen Erwerb der Berechtigung unterschieden werden. Während der abgeleitete Rechtserwerb ohne weiteres durch übereinstimmende Willenserklärung vollzogen wird, bereitet die Bestimmung der ursprünglichen Befugnis erhebliche Probleme. In Ermangelung gesetzgeberischer Vorgaben stellt *Welp*[381] aus Gründen der „Plausibilität" auf den Vorgang der erstmaligen Abspeicherung ab, den er – wie andere Autoren[382] – als „Skripturakt" bezeichnet. *Samson* hingegen hält grundsätzlich das Eigentum am Datenträger für vorrangig.[383] Diese Ansicht vermag jedoch keine Antwort auf die Frage zu geben, wann eine strafbare Veränderung von Daten im Übertragungsstadium vorliegt. Mangels Speicherung existiert zu diesem Zeitpunkt kein Datenträger, von dem eine Berechtigung an den Daten abgeleitet werden könnte.[384] Ebenso wenig kann es darauf ankommen, wer vom Inhalt der Daten betroffen ist.[385] Anderenfalls könnte ein ursprüngliches Verfügungsrecht nur an solchen Daten begründet werden, die einen selbst betreffen. Dieser Ansatz entspricht nicht mehr dem heutigem Meinungsstand.[386] Darüber hinaus schützt § 303a StGB nicht wie § 43 BDSG die Persönlichkeitssphäre, sondern das Interesse des Verfügungsberechtigten an der ungestörten Verwendbarkeit seiner gespeicherten Daten (siehe Kapitel 3.3.5.1). Auch die geistige Urheberschaft kann nicht entscheidend sein, da § 303a StGB keine Strafnorm des Urheberrechts ist, wie auch in Bezug auf das Rechtsgut deutlich wird. Anderenfalls bestünde die Gefahr, die Wertungen des Urheberrecht zu unterlaufen. Dieser Bereich ist zudem bereits durch die §§ 69a ff., 106 ff. UrhG abgedeckt.

Grundsätzlich vorzugswürdig ist daher die erstgenannte Ansicht, die auf den erstmaligen „Skripturakt" abstellt. Auch diese Meinung versagt jedoch im Mehrpersonenverhältnis, beispielsweise wenn ein Arbeitnehmer auf Weisung des Arbeitgebers Daten verändert. Obwohl der physische Akt des Speicherns unmittelbar durch den Angestellten wahrgenommen wird, soll vom Ergebnis her die Berechtigung an den Daten doch dem Vorgesetzten zufallen. *Hilgendorf*[387] schlägt daher vor, den Skripturakt demjenigen zuzurechen, auf dessen Weisung er erfolgt und verweist zur Begründung auf die vergleichbar argumentierende „Geistigkeitstheorie"[388] im Urkundenstrafrecht bzw. bei § 69b UrhG. Im Ergebnis erscheint diese Ansicht aus Gründen der „Plausibilität"[389] als vorzugswürdig, wenngleich *Tolksdorf*[390] darin zuzustimmen ist, dass sich keine Anhaltspunkte dafür im Gesetz finden.

[380] SK – *Hoyer* § 274 (6. Aufl.)Rn 19
[381] Welp IuR 1988, 443 (447)
[382] Hilgendorf JuS1996, 890 (893); Sondermann, S. 35
[383] SK – *Samson* (5. Aufl.) § 303a Rn 14
[384] LK – *Tolksdorf* § 303a Rn 9; Sondermann, S. 35; Tröndle/Fischer § 303a Rn 6
[385] So jedoch: Lackner/Kühl – *Kühl* § 303a Rn 4, allerdings mit der Einschränkung, dass dem Betroffenen ein Recht auf Unversehrtheit der Daten zustehe.
[386] Bühler MDR 1987, 448 (455); Hilgendorf JuS1996, 890 (892); LK – *Tolksdorf* § 303a Rn 10; Lenckner/Winkelbauer CR 1986, 824 (829)
[387] Hilgendorf JuS1996, 890 (893)
[388] Wessels/Hettinger, Strafrecht BT 1, Rn 801
[389] Siehe Fn 381
[390] LK – *Tolksdorf* § 303a Rn 11

3.3.5.1.3 Ergebnis zu § 303a StGB

§ 303a StGB und Art. 4 sind annähernd wortgleich, mit Ausnahme der Tathandlung „unbrauchbar machen“, die die deutsche Strafnorm an Stelle des „Beschädigens“ und „Beeinträchtigens“ im Sinne der Konvention verwendet. Diesbezüglich ergeben sich allerdings keine nennenswerten Abweichungen. § 303a StGB ist überdies nicht an den Eintritt eines schweren Schadens geknüpft, den die Unterzeichnerstaaten auf Grund eines Vorbehalts nach Art. 4 Abs. 2 bei der Transformation in nationales Recht in den Tatbestand aufnehmen können.

3.3.5.2 § 303 StGB – Sachbeschädigung am Datenträger bzw. Löschen eines Programms

Nach einer älteren Auffassung wurde das Löschen bzw. Verändern von Daten bereits unter § 303 StGB subsumiert.[391] Die Vertreter dieser Ansicht argumentierten, dass beim Löschen eines Magnetbandes die Magnetisierung des Datenträgers verändert werde. Darin solle ein substanzrelevanter Eingriff liegen. Die Gegner dieser Auffassung entgegneten schon früh, dass ein Magnetfeld keine Sachqualität aufweise, so dass § 303 StGB mangels eines tauglichen Tatobjekts ausscheide.[392] Dieser Kritik ist zuzustimmen. Selbst wenn man das Magnetfeld eine Datenträgers systemwidrig als Sache im strafrechtlichen Sinne qualifiziert, fehlt es beim Löschen von Daten immer noch an einer Substanzverletzung im Sinne einer Verringerung oder Verschlechterung der Substanz. Das Feld weist vielleicht an vielen Stellen eine andere Polarität und Intensität auf. Dies vermag die physische Qualität des Datenträgers jedoch nicht zu verschlechtern. Ebenso wenig wird die Brauchbarkeit des Datenträgers zu seinem bestimmungsgemäßen Zweck geschmälert, denn es können weiterhin Daten gespeichert werden. Die dargestellte Ansicht strapaziert den Wortlaut des Sachbeschädigungstatbestandes daher über Gebühr und ist aus den genannten Gründen abzulehnen.[393] § 303 StGB ist folglich auch nicht mit Art. 4 vergleichbar.

3.3.6 Bewertung Art. 4

Im Rahmen der Transformation von Art. 4 in nationales Strafrecht besteht kein Änderungsbedarf, da mit § 303a StGB bereits ein vergleichbarer Tatbestand vorhanden ist. Das wesentliche Defizit beider Tatbestände besteht darin, dass sie kein brauchbares Zuordnungskriterium für unkörperliche Daten enthalten, so dass Zweifel an ihrer Bestimmtheit bestehen. Im deutschen Strafrecht kann insbesondere nicht auf das Kriterium der „Fremdheit“ (vgl. etwa §§ 242, 303 StGB) abgestellt werden, das sich nach den zivilrechtlichen Eigentumsverhältnissen bestimmt, weil Daten auf Grund ihrer Unkörperlichkeit nicht eigentumsfähig sind. Aus diesem Grund vermag auch der Tatbestand der Sachbeschädigung – wie dargestellt – keinen geeigneten Schutz vor Datenveränderungen zu bieten. Art. 4 bringt in Bezug auf die Berechtigung an Daten keine neuen Vorgaben und Erkenntnisse. Es wird daher bei den in Kapitel 3.3.5.1.2 gemachten Ausführungen bleiben. Schwer nachvollziehbar ist, warum der deutsche Gesetzgeber nicht wie im Rahmen von § 202a StGB auf die Bestimmung der Daten abstellt.

[391] Haft NStZ 1987, 6 (10); Tiedemann WM 1983, 1326 (1329); Winkelbauer CuR 1985, 40 (44)
[392] Lampe GA 1975, 1 (16, 22); Gerstenberg NJW 1956, 540 „Tonband- Fall“; Naucke, Strafrecht, § 1 Rn 107 ff., „Tonband“-Fall
[393] Ausführlich: Gerhards, S. 13 ff.

3.4 Artikel 5 – Eingriffe in das System[394]

Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um die unbefugte und schwere Behinderung der Funktionsweise eines Computersystems durch Eingeben, Übertragen, Beschädigen, Löschen, Beeinträchtigen, Verändern oder Unterdrücken von Computerdaten als Straftat nach ihrem innerstaatlichen Recht festzulegen, wenn die Handlung vorsätzlich begangen wird.

3.4.1 Anwendungsbereich

Den Erläuterungen zufolge schützt Art. 5 das Interesse der Betreiber und Nutzer von Computer- und Telekommunikationssystemen an deren fehlerfreier Funktion. An dieser Umschreibung fällt vor allem auf, dass auch die Funktionsfähigkeit von Vorrichtungen aus dem Telekommunikationsbereich genannt wird.[395] Wie bei Art. 3 griffen die Verfasser der Konvention auf einen bereits in der Empfehlung Nr. R (89) 9[396] enthaltenen Entwurf zurück, der dort nicht wie jetzt mit „*System Interference*“, sondern mit „*Computer Sabotage*“ überschrieben war. Der Tatbestand ist nicht auf bestimmte Funktionen eines Computersystems beschränkt worden, um einen möglichst umfangreichen Anwendungsbereich zu eröffnen.

3.4.2 Tatbestand

Der Tatbestand unterscheidet sich von Art. 4 an zwei Stellen: Zum einen erfordern Eingriffe in Systeme über eine Manipulation an Computerdaten (siehe Kapitel 2.2) hinaus, dass diese Handlungen „zu schweren Behinderungen der Funktionsweise eines Computersystems“ führen. Zum anderen wurde der Kreis der Tathandlungen um die Varianten „Eingeben“ und „Übertragen“ von Daten erweitert. Da als Tatobjekte nur Daten in Betracht kommen, scheiden Hardwaremanipulationen aus dem Tatbestand aus. Eingriffe in Systeme beziehen sich nur auf Manipulationshandlungen an der Software.

In Bezug auf den Taterfolg stellt Art. 5 nicht auf bestimmte Funktionen eines Computersystems ab, so dass unter einer „Behinderung der Funktionsweise“ jede Beeinträchtigung des ordnungsgemäßen Betriebs zu verstehen ist. Wann diese Manipulation als „schwer“ zu betrachten ist, wird im Tatbestand nicht näher definiert. Die Erläuterungen schlagen beispielsweise vor, eine bestimmte Schadenshöhe zu verlangen. Die Tathandlung „übertragen“ wurde eingefügt, um DoS/DDoS-Attacken (siehe Kapitel 1.7.3), Viren (siehe Kapitel 1.7.2.1) und Spam[397]- Emails begegnen zu können.[398]

Die ersten beiden Beispiele betreffen die Übermittlung zu vieler, schadhafter oder modifizierter Computerdaten, mit dem Ziel, technische Probleme auf den Empfängersystemen auszulösen. Demgegenüber nimmt die Spam-Problematik eine Sonderstellung ein, denn unerwünschte Werbeemails verfolgen keine zielgerichtete Schädigungsabsicht. Zwar können sie Beein-

---

[394] ER Ziff. 65-70
[395] ER Ziff. 65
[396] *Recommendation on Computer-Related Crime*; Europarat, Computer-Related Crime, S. 46; Online: http://cm.coe.int/ta/rec/1989/89r9.htm (01.03.2004), allerdings ohne den „Report on Crime Problems“, auf den die Empfehlung Bezug nimmt.
[397] Der Begriff wird in erster Linie von der amerikanischen Büchsenfleischmarke SPAM (engl. *spiced pork and ham*) abgeleitet und hat seine Internet-typische Bedeutung durch einen Sketch der englischen Comedy Truppe „Monty Python“ erlangt. Daneben wird auch die Ansicht vertreten, dass es sich um eine Kombination der englischen Vokabeln *spill* und *cram* handele.
[398] ER Ziff. 67 und 69

trächtigungen sowohl beim Benutzer als auch bei den Maildienstleistern hervorrufen. Allerdings scheint zweifelhaft, ob diese strafwürdigen Charakter – jedenfalls im Sinne von Art. 5 – aufweisen. Bei den Empfängern unerwünschter Nachrichten handelt es sich in erster Linie um zusätzlichen Zeitaufwand zum Aussortieren der Junk-Mails bzw. um Extrakosten für das Herunterladen der Nachrichten vom Mailserver. Zu einer Funktionsbeeinträchtigung des Computersystems des Benutzers kommt es jedenfalls nicht. Anders vermag sich die Spam-Problematik auf Seiten der Mailanbieter auswirken. In Spitzenzeiten kann es zu Engpässen in Bezug auf die verfügbare Bandbreite kommen, wodurch die Nachrichtenbeförderung insgesamt verlangsamt wird. Jedoch fehlt den Junk-Mail-Versendern Vorsatz in Bezug auf eine Behinderung der Provider. Ganz im Gegenteil wollen sie gerade die Zustellung der Emails, um potentielle Kunden zu werben. Art. 5 erfasst daher weder die Beeinträchtigung auf Seiten der Nutzer noch der Mailanbieter. Dennoch gehen die Erläuterungen von einem verbleibenden Anwendungsbereich der Vorschrift aus, wo durch die Zusendung unerwünschter Werbeemails Kommunikationsvorgänge vorsätzlich und ernsthaft behindert werden.[399]

3.4.3 Unbefugt

Wie schon im Rahmen der vorhergehenden Tatbestände stellen auch die Erläuterungen zu Art. 5 klar, dass Handlungen mit Wissen und Wollen des Berechtigten sowie sozialadäquate Verhaltensweisen (z.B. Sicherheitstests) nicht unbefugt erfolgen.

3.4.4 Vergleichbare Tatbestände im deutschen Strafrecht

Im Anschluss an die Datenveränderung, § 303a StGB, definiert das StGB im 27. Abschnitt den Tatbestand der Computersabotage, § 303b StGB.

3.4.4.1 § 303b StGB – Computersabotage

§ 303b StGB enthält in Abs. 1 Nr. 1 eine Qualifikation zu § 303a StGB; Abs. 1 Nr. 2 beschreibt hingegen einen selbstständigen Tatbestand. Nach der herrschenden Meinung wird das „Interesse“[400] von Wirtschaft und Verwaltung an der störungsfreien Funktion ihrer Datenverarbeitung geschützt.[401]

3.4.4.2 Tatbestand

Durch die Tathandlung muss der Täter eine Datenverarbeitung stören, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist. Der Begriff der „Datenverarbeitung“ ist weit auszulegen. Nach dem Willen des Gesetzgebers wird „[...] jedweder Umgang mit Daten und ihre Verwertung“[402] erfasst, d.h. der gesamte Vorgang von der Dateneingabe, inklusive der internen Rechenvorgänge, bis zur Ausgabe. Entgegen dem Wortlaut vertritt eine Mindermeinung die Ansicht, dass unter Berücksichtigung von Sinn

[399] ER Ziff. 69

[400] So wörtlich: LK – *Tolksdorf* § 303b Rn 2; Möhrenschlager wistra 1986, 128 (142); Sch/Sch – *Stree* § 303b Rn 1, wobei gegen ein „Interesse“ als Rechtsgut die gleichen Bedenken wie bei § 303a StGB stehen (siehe Kapitel 3.3.5.1).

[401] Siehe Fn 400; ebenso: Bühler MDR 1987, 448 (456); Hilgendorf JuS 1996, 1082 (1082) sowie Lackner/Kühl – *Kühl* § 303b Rn 1, ohne den Begriff des „Interesses“; aA: NK – *Zaczyk* § 303b Rn 1; aA: SK – *Hoyer* § 303b Rn 1 f.; differenzierend: Tröndle/Fischer § 303b Rn 2

[402] BT-Drs. 10/5058, S. 35

und Zweck der Vorschrift der einzelne Datenverarbeitungsvorgang nicht in den Tatbestand einbezogen werde.[403] Diese Auffassung steht im Widerspruch zur ausdrücklichen Intention des Gesetzgebers[404] und findet keine Anhaltspunkte im Tatbestand. Sie ist daher abzulehnen.

Das Merkmal der „Fremdheit" bemisst sich unabhängig von der Organisationsform nach den bürgerlich-rechtlichen Eigentumsverhältnissen.[405] Die wirtschaftliche Zuordnung des Betriebs usw. zum Vermögen des Täters – etwa bei einer Ein-Mann-GmbH – ändert nichts an den Eigentumsverhältnissen und bleibt daher außer Betracht. Für eine derartige Sichtweise spricht die einheitliche Verwendung des Merkmals „fremd" im StGB (z.B. §§ 242 StGB), insbesondere im 27. Abschnitt in den §§ 303, 305 und 305a StGB. Eine Ausnahme muss für die Organe einer juristischen Person gemacht werden, da diese selbst nicht handlungsfähig ist. In diesem Fall ist die Datenverarbeitungsanlage für die gesetzlichen Vertreter nicht fremd, es sei denn, sie gehen deliktisch gegen die Interessen des Verbandes vor.[406]

Es werden nicht alle Datenverarbeitungen geschützt, sondern nur solche, die einem „Betrieb", einem „Unternehmen" oder einer „Behörde" zugeordnet werden können. Eine verallgemeinerungsfähige Definition hierfür fehlt[407], so dass in jedem Rechtsgebiet eigenständige Begriffsbestimmungen verwendet werden. Allen drei Ausdrücken ist jedoch gemein, dass sie jeweils eine Organisationseinheit bezeichnen, die Personen und Sachmittel bündelt, um nicht nur vorübergehend einen bestimmten Zweck zu verfolgen. Nicht erfasst werden damit jedenfalls private Anwender außerhalb der genannten Strukturen.[408]

Die Datenverarbeitung muss darüber hinaus von „wesentlicher Bedeutung" für den betroffenen Betrieb usw. sein. Wann dies der Fall ist, lässt sich nicht immer zweifelsfrei bestimmen.[409] Für den Gesetzgeber stand jedoch außer Frage, dass der Ausfall einer elektrischen Schreibmaschine oder eines Taschenrechners nicht genügen sollte.[410] Vielmehr muss ein EDV-Prozess beeinträchtigt werden, der für den Betrieb von zentraler Bedeutung ist, ohne dass eine Betriebsstörung – d.h. eine Beeinträchtigung der ordnungsgemäßen Funktionsweise des Betriebs[411] – wie etwa bei § 316b StGB erforderlich wäre[412]. Wesentliche Bedeutung wird eine Datenverarbeitung allerdings nur dann haben, wenn bei ihrer Störung das Ausbleiben einer Funktionsbeeinträchtigung des Betriebes usw. nur mehr vom Zufall abhängt, d.h. die Störung der Datenverarbeitung die Funktionsfähigkeit des Betriebs usw. wenigstens konkret gefährdet.[413] Kann bereits *ex ante* ausgeschlossen werden, dass die Folgen einer Manipulation nennenswerten Aufwand an Kosten, Arbeitszeit oder anderen Ressourcen verursachen werden, kann sie nicht als wesentlich eingestuft werden.

Eine „Störung" liegt vor, wenn es zu einer nicht nur unerheblichen Beeinträchtigung des reibungslosen Ablaufs auch nur eines Datenverarbeitungsvorgangs kommt. Eine bloße Gefähr-

[403] LK – *Tolksdorf* § 303b Rn 3, 15; zweifelnd: Lackner/Kühl – *Kühl* § 303b Rn 2; differenzierend: Hilgendorf JuS 1996, 1082 (1082 f.)
[404] BT-Drs. 10/5058, S. 35
[405] Schulze-Heimig, S. 203 unter Hinweis auf die eigene Rechtspersönlichkeit juristischer Personen; SK – *Hoyer* § 303b Rn 9; aA: LK – *Tolksdorf* § 303b Rn 10; ebenso: Lenckner/Winkelbauer CR 1986, 824 (830); Sch/Sch – *Stree* § 303b Rn 6 sowie Sondermann, S. 95
[406] Hilgendorf JuS 1996, 1082 (1083); Schulze-Heimig, S. 205
[407] § 14 StGB setzt die Begriffe voraus; § 11 Abs. 1 Nr. 7 StGB stellt klar, dass auch Gerichte Behörden sind.
[408] LK – *Schünemann* § 14 Rn 54; Sch/Sch – *Lenckner*/*Perron* § 14 Rn 28 und 29; Schulze-Heimig, S. 201; SK – *Samson* (5. Aufl.) § 14 Rn 4
[409] Achenbach NJW 1986, 1835 (1838), spricht daher von einem „Zuwachs an ungenauem Strafrecht".
[410] BT-Drs. 10/5058, S. 35
[411] Sch/Sch – *Cramer*/*Sternberg-Lieben* § 316b Rn 6
[412] Gerhards, S. 86 ff.; Sch/Sch – *Stree* § 303b Rn 7; Sondermann, S. 90 ff.
[413] SK – *Hoyer* § 303b Rn 2, 10

dung ist nicht ausreichend. Da die Begrenzung des Tatbestandes allein durch das Kriterium der „wesentlichen Bedeutung“ erfolgt, kann von einem umfassenden Störungsbegriff ausgegangen werden.

Die Tathandlungen können anhand der Tatobjekte, auf die sie sich beziehen, unterschieden werden: Abs. 1 Nr. 1 erfasst Manipulationen an der Software, Abs. 1 Nr. 2 nachteilige Veränderungen an der Hardware. Abs. 1 Nr. 1 verweist bzgl. der Einzelheiten der Tathandlung vollständig auf § 303a Abs. 1 StGB, so dass es sich in dieser Variante um einen Qualifikationstatbestand der Datenveränderung handelt. Zur Vermeidung von Wiederholungen wird auf die Ausführungen im Rahmen von Art. 4 verwiesen (siehe Kapitel 3.3.5.1).

Hinsichtlich der Hardwaremanipulationen unterscheidet § 303b Abs. 1 Nr. 2 StGB zwischen dem „Zerstören“, „Beschädigen“, „Unbrauchbarmachen“, „Beseitigen“ und „Verändern“ von „Datenverarbeitungsanlagen“ und „Datenträgern“. Zur Erläuterung des Begriffs der „Datenverarbeitungsanlage“ kann auf die Ausführungen in Kapitel 2.1.1 verwiesen werden. Ein Datenträger ist ein körperlicher Gegenstand, auf dem Daten wenigstens vorübergehend abgelegt und wieder aufgerufen werden können (Speicherchip, Festplatte, Diskette, DVD, CD usw.). Die ersten beiden Handlungsvarianten sollen sich nach dem Willen des Gesetzgebers an § 303 StGB orientieren.[414] Dies ist auch nicht weiter problematisch, da sowohl Datenverarbeitungsanlagen als auch Datenträger im Gegensatz zu Daten körperliche Objekte darstellen. Wie bei einer Sachbeschädigung sind demnach Eingriffe in die Sachsubstanz gemeint. Ein „Unbrauchbarmachen“ erfordert in Anlehnung an die zu §§ 109e und 316b StGB gewonnenen Erkenntnisse grundsätzlich eine nicht unerhebliche Einschränkung der Gebrauchsfähigkeit.[415] Damit die Variante eine eigenständige Bedeutung behält, sind einschränkend nur die Fälle ohne Einwirkungen auf die Substanz gemeint. Das „Beseitigen“ setzt nach dem allgemeinen Sprachgebrauch voraus, dass die zu entfernende Sache räumlich aus dem Herrschaftsbereich des Nutzungsberechtigten entzogen wird. Ein Aussperren des Berechtigten genügt nur nach einer vereinzelt vertretenen Auffassung.[416] Eine „Veränderung“ der Hardware liegt vor, wenn ihr Zustand in irgendeiner Weise – also auch zum Vorteil des Berechtigten – verändert wird.[417]

3.4.4.3 Ergebnis zu § 303b StGB

§ 303b StGB weicht an verschiedenen Stellen von Art. 5 ab. Der wohl gravierendste Unterschied besteht darin, dass eine Computersabotage im Sinne des StGB nicht nur Manipulationen an der Software – so Art. 5 –, sondern auch an der Hardware sanktioniert. Dadurch, dass das deutsche Strafrecht nicht beliebige Datenverarbeitungsvorgänge in den Tatbestand aufgenommen hat, sondern nur solche, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine fremde Behörde von Bedeutung sind, bleibt es hinter der Konvention zurück. Privatanwender werden damit ausdrücklich ausgeschlossen. Beide Normen erfordern ein gewisses Ausmaß der Beeinträchtigung. Bei § 303b StGB genügt, dass ein Datenverarbeitungsvorgang von „wesentlicher Bedeutung“ manipuliert wird, ohne dass es auf das Ausmaß der Störung im Einzelfall ankommt. Art. 5 hingegen differenziert nicht nach einzelnen Funktionsweisen eines Computersystems, sondern stellt allein auf die konkrete Funktionsbeeinträchtigung ab. In Bezug auf DoS/DDoS-Attacken, Viren und Spam-Emails, die die Konvention durch die Handlungsvariante „übertragen“ erfassen will, fehlt eine Entsprechung in § 303b

[414] BT-Drs. 10/5058, S. 36
[415] Sch/Sch – *Stree* § 303b Rn 15
[416] Schulze-Heimig, S. 220 f.
[417] Hilgendorf JuS 1996, 1082 (1082); SK – *Hoyer* § 303b Rn 7

StGB. Viren dürften in den meisten Fällen bereits eine Datenveränderung bewirken und unter § 303b Abs. 1 Nr. 1 StGB fallen. Eine pauschale Aussage zu DoS/DDoS-Attacken kann auf Grund der Abweichungen in der technischen Ausführung (siehe Kapitel 1.7.3) nicht getroffen werden. Solange sich derartige Angriffe auf das „Überfluten“ eines Zielrechners mit Anfragen beschränken, liegt jedenfalls keine der in § 303a StGB beschriebenen Tathandlungen vor, so dass auch eine Strafbarkeit nach § 303b Abs. 1 Nr. 1 StGB ausscheidet. Für Spam-Emails gilt das gleiche.

3.4.5 Bewertung Art. 5

Art. 5 steht in § 303b StGB ein vergleichbarer Tatbestand gegenüber, der jedoch vor allem in Hinblick auf die Computersysteme von Privatanwendern hinter den Vorgaben der Konvention zurück bleibt. Im Übrigen begegnet der Tatbestand des „Eingriffs in Systeme“ den gleichen Bedenken wie Art. 4. Dadurch, dass der Kreis der tauglichen Tatobjekte nicht zumindest auf „fremde“ Computersysteme eingegrenzt wird, sind selbst Manipulationen am eigenen Computer zunächst tatbestandsmäßig. Maßgebliche Bedeutung erlangt in diesem Fall wie auch in den anderen Tatbeständen der Konvention das Merkmal „unbefugt“, ohne dass sich weitere Anhaltspunkte zur Bestimmung der Berechtigung an den Daten aus dem Wortlaut ergeben. Es bestehen daher Bedenken in Bezug auf die hinreichende Bestimmtheit von Art. 5, da es dem Tatbestand nicht gelingt, eine Verbotsmaterie erschöpfend zu beschreiben.

3.5 Artikel 6 – Missbrauch von Vorrichtungen[418]

(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um folgende Handlungen, wenn sie vorsätzlich und unbefugt begangen werden, als Straftaten nach ihrem innerstaatlichen Recht festzulegen:

> *a) das Herstellen, Verkaufen, Beschaffen zwecks Gebrauch, Einführen, Verbreiten oder anderweitige Zugänglichmachen*
>
> *i) einer Vorrichtung einschließlich eines Computerprogramms, die in erster Linie zu dem Zweck konstruiert oder bearbeitet worden ist, eine der nach den Artikeln 2 bis 5 fest gelegten Straftaten zu begehen,*
>
> *ii) eines Computerpassworts, eines Zugriffscodes oder ähnlicher Daten, die den Zugriff auf ein Computersystem als Ganzes oder auf einen Teil davon ermöglichen,*
>
> *mit dem Vorsatz, sie zu verwenden, um eine der nach den Artikeln 2 bis 5 festgelegten Straftaten zu begehen und*
>
> *b) den Besitz eines unter Buchstabe a) Ziffer 1 oder 2 bezeichneten Mittels mit dem Vorsatz, es zu verwenden, um eine der nach den Artikeln 2 bis 5 festgelegten Straftaten zu begehen. Eine Vertragspartei kann als gesetzliche Voraussetzung vorsehen, dass erst der Besitz einer bestimmten Anzahl dieser Mittel die Strafbarkeit begründet.*

(2) Dieser Artikel darf nicht so ausgelegt werden, als schreibe er die Strafbarkeit in Fällen vor, in denen das Herstellen, Verkaufen, Beschaffen zwecks Gebrauch, Einführen, Verbreiten oder anderweitige Zugänglichmachen oder der Besitz nach Absatz 1 nicht zum Zweck der Begehung einer nach den Artikeln 2 bis 5 festgelegten Straftat, sondern beispielsweise zum genehmigten Testen oder zum Schutz eines Computersystems erfolgt.

(3) Jede Vertragspartei kann sich das Recht vorbehalten, Absatz 1 nicht anzuwenden, soweit der Vorbehalt nicht das Verkaufen, Verbreiten oder anderweitige Zugänglichmachen der in Absatz 1 Buchstabe a Ziffer 2 bezeichneten Mittel betrifft.

3.5.1 Anwendungsbereich

Art. 6 bezweckt die Begründung einer eigenständigen und unabhängigen Strafbarkeit für Vorbereitungshandlungen im Bereich der Art. 2 bis 5. Die Begehung dieser Delikte setzt oftmals den Besitz bestimmter Hilfsmittel (sog. „Hacker-Tools“) voraus, wodurch ein starker Anreiz für die Anfertigung und Verbreitung derartiger Tatwerkzeuge entstehen kann. Nach Ansicht der Verfasser besteht daher bereits im Präventivbereich ein Strafbedürfnis. In diesem Zusammenhang ist von Bedeutung, dass die Unterzeichnerstaaten zwar grundsätzlich durch Art. 11 Abs. 2 zur Begründung einer Versuchsstrafbarkeit im Bereich der Art. 3-5 verpflichtet sind, sich nach Art. 11 Abs. 3 jedoch das Recht vorbehalten können, diese in nationales Recht umzusetzen. In diesem Fall wäre die Sanktionierung von Vorbereitungshandlungen nach Art. 6 die einzige Möglichkeit, präventiven Strafrechtsschutz zu gewähren. Diese Ausweitung der Strafbarkeit kann auf aktuelle Entwicklungen innerhalb des Europarats und der EU sowie einiger Mitgliedsländer in Bezug auf den Schutz von Zugangskontrollierten Diensten und Zugangskontrolldiensten aufbauen.[419] Ein ähnlicher Weg wurde bereits in der „Genfer Konvention über Geldfälschung“ aus dem Jahre 1929 eingeschlagen.

---

[418] ER Ziff. 71-78

[419] *European Convention on the legal protection of services based on, or consisting of, conditional access* – ETS No 178; Richtlinie 98/84/EG des Europäischen Parlaments und des Rats vom 20.11.1998 über den Schutz von Zugangskontrollierten Diensten und Zugangskontrolldiensten.

3.5.2 Tatbestand

Bei den Tatobjekten handelt es sich nach Abs. 1 lit. a) Ziffer 1 um „Vorrichtungen einschließlich eines Computerprogramms, die in erster Linie zu dem Zweck konstruiert oder bearbeitet wurden, eine der nach den Artikeln 2 bis 5 festgelegten Straftaten zu begehen“, und gemäß Ziffer 2 um „Computerpasswörter, Zugriffscodes oder ähnlicher Daten, die den Zugriff auf ein Computersystem als Ganzes oder auf einen Teil davon ermöglichen.“ Ziffer 1 bezieht sich im Unterschied zu Ziffer 2 sowohl auf hard- als auch auf softwaremäßige Tatwerkzeuge. In objektiver Hinsicht ist nicht erforderlich, dass diese Vorrichtungen ausschließlich der Begehung von Straftaten nach Art. 2-5 dienen. Von universell einsetzbaren Werkzeugen müssen sie sich jedoch dadurch unterscheiden, dass sie vorrangig für kriminelle Zwecke erstellt oder aus bestehenden Vorrichtungen weiterentwickelt wurden. Ausweislich der Erläuterungen sollte der Tatbestand nicht auf ausschließlich für strafbare Zwecke konstruierte oder angepasste Hilfsmittel beschränkt werden, da man in diesem Fall Beweisprobleme erwartete. Jedoch scheint sich diese Befürchtung durch die jetzige Formulierung nur verschlimmert zu haben, denn der Begriff „vorrangig“ bringt keinen Zuwachs an Bestimmtheit. Jedenfalls könnte eine Begrenzung des Tatbestandes ohne objektiven Anhaltspunkt nur anhand des Vorsatzes des Täters vorgenommen werden. Dies würde dazu führen, dass Hilfsmittel, die in rechtmäßiger Weise produziert und vertrieben wurden, nicht von vornherein aus dem Anwendungsbereich der Norm ausgeschieden werden können. Gerade dies wurde ausweislich der Erläuterungen nicht bezweckt. Ebenso wenig wurde dieser Weg in der „Genfer Konvention über Geldfälschung“ gewählt. Mit „Computerprogrammen“ in Abs. 1 lit. a) Ziffer 1 sind vor allem Schadprogramme wie Viren und Trojaner (siehe Kapitel 1.7.2.1) gemeint, die eigens dazu entworfen wurden, Datenverarbeitungsvorgänge zu beeinträchtigen oder Zugriff auf ein fremdes System zu ermöglichen. Abs. 1 lit. a) Ziff. 2 wurde nicht eigens erläutert.

Als Tathandlungen kommen nach Abs. 1 lit. a) das „Herstellen“, „Verkaufen“, „Beschaffen zwecks Gebrauch“, „Einführen“, „Verbreiten“ oder „anderweitige Zugänglichmachen“ sowie nach Abs. 1 lit. b) der Besitz der unter Abs. 1 lit. a) Ziffern 1 und 2 aufgezählten Mittel in Betracht. Erläuterungsbedarf besteht allein in Bezug auf die letzten beiden Varianten. Unter „Verbreiten“ ist eine aktive Weitergabe an andere Personen gemeint. Der Begriff wird auch von Art. 9 verwendet, wo er vom „Übertragen“ von Inhalten über ein Computersystem abzugrenzen ist. Beide Varianten erhalten einen eigenständigen Bedeutungsgehalt, wenn das „Verbreiten“ auf die Übertragung von Sachsubstanz und das „Übertragen“ auf körperlose Datenübertragungen beschränkt werden.[420] Das „Zugänglichmachen“ besteht hingegen darin, dass der Dateninhaber bestimmte Informationen zum Abruf über ein Netzwerk bereit hält. Gemeint sind damit vor allem sog. „On-demand-Dienste“, aber auch Hyperlinks, die zu einem entsprechenden Angebot im Internet führen. Der Begriff hat auch Eingang gefunden in das „Gesetz zur Regelung des Urheberechts in der Informationsgesellschaft“[421], das das nationale Urheberrecht in Bezug auf die „neuen Medien“ (z.B. Internet) an geändertes, europäisches[422] und internationales[423] Recht anpasst (dazu mehr in Kapitel 3.9). Abs. 1 lit. b) Satz 2 ermöglicht den Vertragsparteien, eine quantitative Schranke für die Besitzstrafbarkeit zu ziehen. Erst die Herrschaftsmacht über eine bestimmte Zahl an Vorrichtungen kann als strafwürdig erachtet werden.

[420] Ähnlich wird der Begriff des „Verbreitens“ im StGB definiert, beispielsweise in § 74d Abs. 1 StGB, Lackner/Kühl – *Lackner* § 74d Rn 5 mwN

[421] BGBl. 2003 I, 1774 ff.

[422] Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22. Mai 2001 (Richtlinie zur Harmonisierung bestimmter Aspekte ders Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft)

[423] WIPO-Urheberrechtsvertrag und WIPO-Vertrag über Darbietungen und Tonträger; http://www.wipo.int/treaties/en/index.html (01.03.2004)

In subjektiver Hinsicht erfordert Abs. 1 lit. a) und b) Vorsatz sowohl in Bezug auf die objektiven Tatbestandsmerkmale als auch auf die (untechnische) Absicht, die beschriebenen Tatwerkzeuge für Straftaten nach den Art. 2-5 zu verwenden. Dieses besondere subjektive Element wurde ergänzt, um einer Kriminalisierung von Vorrichtungen vorzubeugen, die in rechtmäßiger Weise hergestellt und vertrieben werden.

3.5.3 Art. 6 Abs. 2, Abs.3 – Einschränkung und Vorbehalt

Mit Abs. 2 reagieren die Verfasser der Konvention auf Kritik aus den Reihen von IT-Sicherheitsexperten. An den ersten Entwürfen war bemängelt worden, dass neutrale Sicherheitswerkzeuge nur durch eine Täterabsicht zu „Hacker-Tools" werden könnten. Es soll noch einmal verdeutlicht werden, dass solche Vorrichtungen von Art. 6 nicht erfasst würden, die zum berechtigten Test oder Schutz eines Computersystems entworfen oder angepasst wurden. Solche Handlungen würden im Übrigen auch nicht „unbefugt" begangen. Demzufolge ist Abs. 2 überflüssig. Abs. 3 enthält einen Vorbehalt im Sinne von Art. 42. Den Vertragsparteien bleibt es überlassen, Abs. 1 in nationales Recht umzusetzen, solange wenigstens der Verkauf, die Verbreitung und das anderweitige Zugänglichmachen eines Computerpassworts, eines Zugriffscodes oder ähnlicher Daten nach Abs. 1 lit. a) Ziffer 2 sanktioniert würde.

3.5.4 Vergleichbare Tatbestände im deutschen Strafrecht

Art. 6 zielt auf eine Kriminalisierung von Vorbereitungshandlungen ab, die im deutschen Kernstrafrecht bislang keine unmittelbare Entsprechung findet. Im Vorbereitungsstadium kann unter weiteren Voraussetzungen allenfalls § 30 StGB zur Anwendung kommen, der sich jedoch nicht auf den Verkehr mit rechtswidrigen Vorrichtungen bezieht und nur die Vorbereitung von Verbrechen erfasst. Im Nebenstrafrecht findet sich eine Strafnorm in Bezug auf „Umgehungsvorrichtungen" in § 4 Zugangskontrolldiensteschutz-Gesetz (ZKDSG).

3.5.4.1 § 4 ZKDSG

Das ZKDSG[424] vom 19. März 2002 dient der Umsetzung der Richtlinie 1998/84/EG des Europäischen Parlaments und des Rats über den rechtlichen Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten vom 20. November 1998[425]. Der Anwendungsbereich des Gesetzes besteht darin, die Umgehung von Schutzvorrichtungen entgeltpflichtiger Inhaltdienste im Fernseh-, Rundfunk- und Internetbereich („Dienste der Informationsgesellschaft") zu unterbinden.[426]

3.5.4.2 Tatbestand

§ 4 ZKDSG stellt eine Strafnorm dar, die Verstöße gegen das Verbot des § 3 Nr. 1 ZKDGS, „gewerbsmäßig" Umgehungsvorrichtungen „herzustellen", „einzuführen" oder zu „verbreiten", mit Geldstrafe oder bis zu einem Jahr Freiheitsstrafe sanktioniert. Die Begriffe „Umgehungsvorrichtungen", „zugangskontrollierte Dienste" und „Zugangskontrolldienste" sind in § 2 ZKGSD legal definiert. Für den Bereich der Computernetze ist vor allem § 2 Nr. 1 lit. b) ZKDSG von Bedeutung, der Dienste nach § 2 des TDG zu den zugangskontrollierten Diens-

[424] BGBl. 2002 I, S. 1090 ff.
[425] Abl. L 320 vom 28. November 1998, S. 54
[426] Regierungsentwurf mit amtlicher Begründung und Stellungnahme des Bundesrats (Anlage 2): BT-Drs. 14/7229, S. 6

ten zählt, sofern sie gegen Entgelt erbracht und durch einen Zugangskontrolldienst geschützt werden. Teledienste sind vereinfachend gesprochen alle Dienstleistungen und Inhalte, die auf die Übermittlung von Daten aufbauen, d.h. „mittels Telekommunikation (§ 3 Nr. 16 TKG)“ übertragen werden, § 2 Abs. 1 TDG. Wegen der Einzelheiten kann auf die Ausführungen in Kapitel 2.3.1.2 verwiesen werden. „Umgehungsvorrichtungen“ sind nach § 2 Nr. 3 ZKDSG technische Verfahren oder Vorrichtungen, die dazu bestimmt oder entsprechend angepasst sind, die unerlaubte Nutzung eines zugangskontrollierten Dienstes zu ermöglichen. In der amtlichen Begründung werden sie auch als „Hackerwerkzeuge“ bezeichnet.[427] Vor allem Entschlüsselungsprogrammen im Pay-TV-Bereich komme eine große wirtschaftliche Bedeutung zu, der vor allem bei gewerbsmäßigen Eingriffen nur eine geringe Hemmschwelle gegenüberstehe. § 4 ZKDSG solle daher bereits im Präventivbereich abschreckende Wirkung entfalten.[428]

3.5.4.3 Ergebnis § 4 ZKDSG

§ 4 ZKDSG sanktioniert ähnlich wie Art. 6 Handlungen im Vorbereitungsstadium zu anderen Delikten. Abgesehen davon unterscheiden sich beide Tatbestände beträchtlich. Art. 2-6 der Konvention bezwecken als Informationsdelikte im engeren Sinne den Schutz des ungestörten Kommunikationsflusses. Demgegenüber bezieht sich das ZKDSG nicht auf den Austausch von Nachrichten, sondern auf den unberechtigten Zugang zu entgeltpflichtigen Diensten. Die wirtschaftliche Grundlage der Anbieter derartiger Dienste soll durch die Verbote des § 3 ZKDSG gesichert werden. In diesem Zusammenhang ist auch der Gewinnherausgabeanspruch des Anbieters zu sehen, der zwar im Regierungsentwurf noch enthalten war, jedoch nicht verabschiedet wurde, da er wohl mit der Systematik des deutschen Bereicherungsrechts unvereinbar war.[429] Das ZKDSG erfasst im Computerbereich demnach nur Inhaltsdienste im Sinne von §§ 2 Nr. 1 ZKDSG, 2 TDG und 2 MDStV, wohingegen Art. 6 auch den Übertragungsvorgang betrifft (vor allem Art. 3 „Rechtswidriges Abfangen“). Auch sind „Umgehungsvorrichtungen“ mit den „Hacker-Tools“ nach Art. 6 nicht vergleichbar, da eine Umgehung bereits vom natürlichen Wortsinn her stets eine Zugangssicherung erfordert, auf die die Konvention in den Art. 2-5 gerade verzichtet. Ein weiterer entscheidender Unterschied besteht darin, dass das ZKDSG nur auf gewerbliche Aktivitäten Anwendung findet. § 4 ZKDSG deckt daher nur einen kleinen Ausschnitt aus dem möglichen Anwendungsbereich des Art. 6 ab.

3.5.5 Bewertung Art. 6

Art. 6 ist neben den Tatbeständen zur „Echtzeit-Erhebung von Computerdaten“, Art. 20 und 21, die wohl umstrittenste Norm des Übereinkommens. Kritisiert wird vor allem, dass der Anwendungsbereich von Art. 6 nicht anhand objektiver Kriterien, sondern allein in subjektiver Hinsicht beschränkt werden könne.[430] Zu diesem Defizit haben die Verfasser der Konvention selbst beigetragen, indem sie darauf verzichteten, lediglich speziell für strafwürdige Verhaltensweisen konstruierte oder angepasste Vorrichtungen in Art. 6 Abs. 1 lit. a) Ziffer 1 aufzunehmen. Die Begründung hierfür in den Erläuterungen lautet, dass man einerseits keine Einschränkung des Anwendungsbereichs der Norm intendierte und andererseits mit Beweisproblemen rechnete.[431] Im Ergebnis kam ein Tatbestand heraus, der objektiv – ähnlich wie die

[427] Anlage 1 zu BT-Drs. 14/7229, S. 8
[428] Anlage 1 zu BT-Drs- 14/7229, S. 8
[429] Anlage 2 zu BT-Drs. 14/7229, S. 10
[430] Bäumler DuD 2001, 348 (350); Emmert KES 2002, 6ff.; Kugelmann DuD 2001, 215 (218); ders. TMR 2002, 14 (16)
[431] ER Ziff. 73

Art. 2-5 – kaum begrenzbar ist und durch seine Unbestimmtheit allenfalls Beweisschwierigkeiten geschaffen als solche vermieden hat. Ebenso beurteilte der Bundesrat Art. 6 und sah eine vergleichbare Problematik im Rahmen von § 4 ZKDSG.[432] An Stelle den Tatbestand des Art. 6 Abs. 1 zu korrigieren, wurde ein Abs. 2 aufgenommen, der die Unterzeichnerstaaten dazu auffordert, Abs. 1 nicht so auszulegen, dass er Sicherheitstests erfasse. Befriedigende Ergebnisse lassen sich lediglich dann erzielen, wenn Abs. 1 dahingehend eingeschränkt wird, dass nur ausschließlich für kriminelle Zwecke konstruierte Vorrichtungen und Programme (beispielsweise Viren, Trojaner, usw.) taugliche Tatobjekte darstellen.

[432] Anlage 2 zu BT-Drs. 14/7229, S. 10

3.6 Artikel 7 – Computerurkundenfälschung[433]

Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um das vorsätzliche und unbefugte Eingeben, Verändern, Löschen oder Unterdrücken von Computerdaten als Straftat nach ihrem innerstaatlichen Recht vorzusehen, wenn dies zu unechten Daten führt und beabsichtigt ist, dass diese Daten für rechtliche Zwecke angesehen oder einer Handlung zugrunde gelegt werden, als wären sie echt, gleichviel, ob die Daten unmittelbar lesbar und verständlich sind. Eine Vertragspartei kann als Voraussetzung vorsehen, dass erst eine betrügerische oder ähnliche unredliche Absicht die Strafbarkeit begründet.

3.6.1 Anwendungsbereich

Art. 7 unterscheidet sich von den vorhergehenden Normen dahingehend, dass er nicht den Schutz des Informationsaustauschens bezweckt, sondern als Bestandteil einer zweiten Gruppe von Tatbeständen in der Konvention – zusammen mit den Art. 8-10 – eine Harmonisierung und Anpassung herkömmlicher Tatbestände an die durch die modernen Medien veränderten gesellschaftlichen Rahmenbedingungen intendiert.[434] Art. 7 soll dazu eine Parallele zum Tatbestand der Urkundenfälschung an körperlichen Dokumenten im Bereich des elektronischen Datenverkehrs schaffen. Körperliche Dokumente werden im alltäglichen Rechtsverkehr zusehends durch maschinenlesbare Daten zurückgedrängt. Diesen fehlt in vielen Rechtsordnungen die Urkundenqualität, die für einen strafrechtlichen Schutz erforderlich wäre. Art. 7 beabsichtigt daher im Ergebnis eine Gleichstellung rechtlich erheblicher Computerdaten mit körperlichen Urkunden. Das geschützte Rechtsgut ist demnach die Sicherheit und Zuverlässigkeit des Beweisverkehrs mit elektronischen Daten.

3.6.2 Tatbestand

Als Tatobjekte kommen Computerdaten (siehe Kapitel 2.2) in Betracht, die sowohl für den privaten als auch den hoheitlichen Rechtsverkehr Bedeutung haben. Rechtliche Bedeutung kommt ihnen dann zu, wenn sie sich im weitesten Sinne auf Rechtsgeschäfte beziehen oder Urkunden mit rechtlicher Bedeutung gleichstehen. Die unbefugte „Eingabe" richtiger oder falscher Daten ist der Herstellung einer unechten Urkunde vergleichbar. Nachträgliches „Verändern" (Modifizieren, Verändern, teilweises Ändern), „Löschen" (Entfernen von Daten von einem Datenträger) und „Unterdrücken" (Zurückhalten, Verstecken von Daten) entspricht generell der Verfälschung einer echten Urkunde. Die Auslegung dieser drei Handlungsvarianten orientiert sich an der im Rahmen von Art. 4 (siehe Kapitel 3.3.2). Der Gebrauch „unechter Daten" wurde neben dem Herstellen nicht eigens im Tatbestand erwähnt.

In den Rechtsordnungen der Unterzeichnerstaaten bezeichnet die „Unechtheit" einer Urkunde entweder ihre inhaltliche Richtigkeit, die Identität von dem aus der Urkunde ersichtlichen und tatsächlichen Aussteller oder beides.[435] Den Erläuterungen zufolge bezieht Art. 7 die „Echtheit" zumindest auf die Urheberschaft an einem Datensatz. Darüber hinaus steht es den Unterzeichnerstaaten frei, auch die Wahrhaftigkeit des Inhalts unter das Merkmal „unecht" zu subsumieren.[436]

---

[433] ER Ziff. 81-85

[434] Beispielsweise erfassen die Strafnormen einiger US-Bundesstaaten in Hinblick auf Pornografie keine elektronischen Bilder, ER Ziff. 79

[435] ER Ziff. 82

[436] ER Ziff. 82

In subjektiver Hinsicht erfordert Art. 7 neben dem allgemeinen Vorsatz die Absicht, die unechten als echte Daten im Rechtsverkehr zu verwenden. Obwohl im Wortlaut nicht angesprochen, erinnert dies an die Täuschungsabsicht der Urkundendelikte im deutschen Strafrecht.

3.6.3 Unbefugt

Anders als im Rahmen der vorhergehenden Artikel nimmt das Merkmal „unbefugt" keine zentrale Stellung mehr ein, da der Tatbestand mit hinreichender Bestimmtheit eine Verbotsmaterie umschreibt.

3.6.4 Einschränkung nach Satz 2

Satz 2 ermöglicht den Vertragsparteien bei der Umsetzung in nationales Recht, das Hinzutreten einer betrügerischen oder ähnlich unredlichen Absicht zu verlangen.

3.6.5 Vergleichbare Tatbestände im deutschen Strafrecht

Das deutsche StGB beschreibt die Urkundendelikte im 23. Abschnitt. Für einen Vergleich werden im Folgenden die §§ 267, 268, 269 und 270 StGB näher untersucht. Von Bedeutung ist vor allem der durch das 2. WiKG eingefügte Tatbestand der Fälschung beweiserheblicher Daten, § 269 StGB, der Lücken im Recht der Urkundenfälschung im Zusammenhang mit der EDV-Technik schließen sollte. § 274 Abs. 1 Nr. 2 StGB, dessen Tatbestand von beweiserheblichen Daten spricht, wurde nicht näher beleuchtet, da er nach der ganz herrschenden Meinung nicht wie Art. 7 die Echtheit von Daten, sondern das berechtigte Interesse an ihrer beweismäßigen Verfügbarkeit[437] schützt.

3.6.5.1 § 267 StGB – Urkundenfälschung

In der Kommentarliteratur findet sich die formelhafte Definition, dass § 267 StGB die Sicherheit und Zuverlässigkeit des Beweisverkehrs mit Urkunden schütze.[438] Die Norm stellt nicht auf die inhaltliche Richtigkeit des Gewährsobjekts (sog. schriftliche Lüge) ab, sondern darauf, ob der wirkliche Aussteller und der, der aus der Urkunde hervorgeht, identisch sind.[439] In Bezug auf das geschützte Rechtsgut und den Urkundenbegriff sind zahlreiche Einzelheiten noch umstritten, auf die es hier jedoch nicht ankommt.

3.6.5.1.1 Tatbestand

Tatobjekt des § 267 StGB sind Urkunden. Nach der ganz herrschenden Meinung handelt es sich dabei um verkörperte Gedankenerklärungen (Perpetuierungsfunktion), die den Aussteller erkennen lassen (Garantiefunktion) und geeignet und bestimmt sind, für ein Rechtsverhältnis

[437] Freund JuS 1994, 207 (210); Lackner/Kühl – *Kühl* § 274 Rn 1; Sch/Sch – *Cramer* § 274 Rn 1; SK – *Hoyer* (6. Aufl.) § 274 Rn 1

[438] Lackner/Kühl – *Kühl* § 267 Rn 1; Sch/Sch – *Cramer* § 267 Rn 1; Sieber, Computerkriminalität und Strafrecht, S. 270; Tröndle/Fischer § 267 Rn 1; aA: NK – *Puppe* § 267 Rn 1 ff.; aA: SK – *Hoyer* (6. Aufl.) Vor § 267 Rn. 12 ff., der die individuelle Dispositionsfreiheit als geschütztes Rechtsgut bezeichnet.

[439] Lackner/Kühl – *Kühl* § 267 Rn 1; LK – *Gribbohm* § 267 Rn 160 ff.; Sch/Sch – *Cramer* § 267 Rn 48; aA: NK – *Puppe* § 267 Rn 75 ff.; aA: SK – *Hoyer* § 267 Rn 55 ff., wonach eine Urkunde unecht sei, wenn eines der für den Urkundenbegriff konstitutiven Charakteristika nicht erfüllt ist.

Beweis zu erbringen (Beweisfunktion).[440] EDV-Daten genügen lediglich in begrenztem Umfang den Anforderungen des strafrechtlichen Urkundenbegriffs.

Nach der bereits auf das Reichsgericht zurückgehenden Erklärungstheorie[441] verkörpern Urkunden im Sinne von § 267 StGB menschliche Gedankenerklärungen. Dadurch unterscheiden sie sich von den sog. Augenscheinsobjekten (z.B. Fußspuren, Fingerabdrücke, usw.), die keinen eigenständigen gedanklichen Inhalt aufweisen. Für den Bereich der EDV hat dies zur Folge, dass Daten, die ganz oder zum Teil das Ergebnis automatisierter Rechenvorgänge sind, streng genommen keinen oder nur einen reduzierten „menschlichen" Gedankeninhalt fixieren und deshalb keine Urkundenqualität besitzen. Wegen den fließenden Übergängen zwischen menschlichen Erklärungen und „selbstständig" durch ein Gerät bewirkten Operationen führt diese Ansicht in der Praxis zu erheblichen Abgrenzungsschwierigkeiten. Es wird deshalb in der Literatur vorgeschlagen, Daten dann unter den Urkundenbegriff zu subsumieren, wenn sie das Ergebnis einer vom Menschen programmierten Software sind.[442] Diese Meinung führt zwar zu praxisgerechten Ergebnissen, droht allerdings die Abgrenzung zu § 268 StGB zu verwischen, der auf die „selbsttätige" Darstellung durch ein technisches Gerät abstellt. Dabei handelt es sich jedoch nach zutreffender Ansicht in der Literatur nicht um eine Unzulänglichkeit bei der Auslegung der Urkundenfälschung, sondern um eine mangelhafte Konzeption des § 268 StGB, die zu zufällig-willkürlichen Differenzierungen führt.[443]

Der Großteil der EDV-Daten wird allerdings durch das Erfordernis der Verkörperung ohnehin aus dem Tatbestand von § 267 StGB ausgeschieden.[444] Die Daten müssten dazu dauerhaft und visuell erfassbar fixiert sein.[445] Durch das erste Kriterium werden alle Daten in elektronischen und elektromagnetischen Speicher- und Leitungsbauteilen ausgeschlossen; durch das zweite – selbst wenn man die optische Wahrnehmbarkeit mit der wohl hM bei Geheim- und Kurzschriften[446] bejaht – solche auf gängigen Speichermedien (Festplatte, Diskette, CD, usw.). Geringere Anforderungen in diesem Bereich stellt § 268 StGB. Eine „Darstellung" von Daten, usw. erfordert lediglich eine stoffliche Fixierung, ohne dass diese visuell wahrnehmbar sein müsste.

Hinsichtlich der Beweiseignung und -bestimmung ergeben sich auf Grund der Zustandsform der EDV-Daten keine wesentlichen Besonderheiten. Ähnlich verhält es sich mit der Erkennbarkeit des Ausstellers.[447]

3.6.5.1.2 Ergebnis zu § 267 StGB

§ 267 StGB vermag nur dauerhaft und visuell wahrnehmbar verkörperte Daten gegen Fälschungen zu schützen. Daten im Sinn von Art. 1 lit. b) erfahren dadurch, mangels Urkundenqualität, keinen Schutz. § 267 StGB bietet im elektronischen Rechtsverkehr daher keinen zu Art. 7 vergleichbaren Schutz.

---

[440] So bereits RGSt 6, 290; BGHSt 3, S. 84; 4, S. 285; 13, S. 235, 16, S. 96; Lackner/Kühl – *Kühl* § 267 Rn 2; LK – *Gribbohm* § 267 Rn 4 ff.; NK – *Puppe* § 267 Rn 16 ff.; Sch/Sch – *Cramer* § 267 Rn 2; SK – *Hoyer* § 267 Rn 4 ff.

[441] RGSt 17, 103 (106f.)

[442] Sch/Sch – *Cramer* § 267 Rn 4; Sieber, Computerkriminalität und Strafrecht, S. 281 ff.

[443] Freund JuS 1994, 207 (208)

[444] Sieber, Computerkriminalität und Strafrecht, S. 283

[445] Lackner/Kühl – *Kühl* § 267 Rn 6; LK – *Gribbohm* § 267 Rn 10; NK – *Puppe* § 267 Rn 48; SK – *Hoyer* § 267 Rn 28 ff.

[446] Freund JuS 1993, 1016 (1019); Sch/Sch – *Cramer* § 267 Rn 7; SK – *Hoyer* § 267 Rn 31

[447] Teilweise aA: Sieber, Computerkriminalität und Strafrecht, S. 284 ff.

3.6.5.2 § 268 StGB – Fälschung technischer Aufzeichnungen

Der Tatbestand der Fälschung technischer Aufzeichnungen, § 268 StGB, ist strukturgleich mit dem der Urkundenfälschung hinsichtlich der Tathandlungen, des Strafmaßes, der Anordnung der Versuchsstrafbarkeit sowie der Technik der Regelbeispiele. Der entscheidende Unterschied besteht darin, dass § 268 StGB sich auf technische Aufzeichnungen im Sinne von § 268 Abs. 2 StGB und nicht auf Urkunden bezieht. Aus dieser Ähnlichkeit folgt, dass die Vorschrift eine vergleichbare Schutzrichtung wie die Urkundenfälschung aufweist und nach der Intention des Gesetzgebers eine Lücke im Schutz der „Sicherheit und Zuverlässigkeit des Beweisverkehrs“ schließen sollte, die sich dadurch aufgetan hatte, dass immer mehr technische Aufzeichnungen an die Stelle von Urkunden getreten waren.[448] § 268 StGB schützt nicht wie § 267 StGB das Vertrauen des Rechtsverkehrs, dass hinter einer verkörperten Erklärung ein bestimmter Aussteller steht (Garantiefunktion der Urkunde), sondern dass eine technische Aufzeichnung das Ergebnis eines normalen, automatischen Herstellungsvorgangs ist.[449]

3.6.5.2.1 Tatbestand

Tatobjekte sind technische Aufzeichnungen im Sinne von § 268 Abs. 2 StGB, wozu die Darstellung von Mess- und Rechenwertern, Zuständen und Geschehensabläufen und auch Daten (siehe dazu Kapitel 2.2.1) gezählt werden. Dabei handelt es sich um Augenscheinsobjekte, die keine menschliche Erklärung verkörpern. Stattdessen erfüllen technische Aufzeichnungen eine sog. „Translations- bzw. Klassifikationsfunktion“, indem sie Gewähr für die Unbestechlichkeit eines automatisierten Aufzeichnungsvorgangs erbringen.[450]

Um von einer „Darstellung“ sprechen zu können, dürfen die Daten nicht nur vorübergehend stofflich fixiert sein, wenngleich auch nicht – wie bei § 267 StGB – notwendigerweise in sichtbarer Form. Keine ausreichende Perpetuierung soll danach vorliegen, wenn sich die Daten als elektrische Spannungszustände im Arbeitsspeicher einer Datenverarbeitungsanlage befinden; anders hingegen, wenn sie auf einem Festspeicher abgelegt werden.[451] Während dies für die optischen Datenträger (CD, DVD, Blue Ray, usw.) noch nachvollziehbar ist, da die Daten in Form von Vertiefungen und Erhöhungen (sog. „*lands*“ und „*pits*“) in die Oberfläche des Mediums „eingebrannt“ werden und dadurch physische Realität gewinnen, kommt es bei den magnetischen Medien – außer zu einer Änderung des Magnetfelds – zu keiner stofflichen Veränderung des magnetischen Substrats.[452] In diesem Fall werden die Daten in einer flüchtigen Zustandsform abgelegt, die vergleichbar mit der temporären Fixierung im Arbeitsspeicher ist (sog. „RAM“). Trotzdem werden sie – anders als Daten im RAM-Speicher – als körperlich fixiert betrachtet. Ähnliche Unsicherheiten bei der Anwendung des § 268 StGB ergeben sich für neuere Datenträger wie beispielsweise Speicherkarten[453], die vor allem im Bereich der Digitalfotografie Verwendung finden. Ohne eine genaue Analyse der technischen Einzelheiten dürfte in diesen Fällen nicht klar sein, wann von einer stofflichen Fixie-

[448] BT-Drs. V/4094 S. 37; Lackner/Kühl – *Kühl* § 268 Rn 1

[449] Freund JuS 1994, 207 (207); Sch/Sch – *Cramer* § 268 Rn 2; aA: SK – *Hoyer* § (6. Aufl.) 268 Rn 1, Schutzgut sei die Dispositionsfreiheit der potentiellen Empfänger; missverständlich: Lackner/Kühl – *Kühl* § 268 Rn 2, wonach mittelbar das Interesse an inhaltlicher Richtigkeit geschützt sei.

[450] SK – *Hoyer* § 268 Rn 3 mwN

[451] Lackner/Kühl – *Kühl* § 268 Rn 3; SK – *Hoyer* §268 Rn 10; Welp CR 1992, 291 (293);
aA: LK – *Gribbohm* § 268 Rn 6 sowie Sch/Sch – *Cramer* § 268 Rn 8, die auch einer lediglich elektronischen Fixierung die erforderliche Dauerhaftigkeit zusprechen.

[452] Dies wurde bereits im „Tonband“- Fall der 1960er Jahre erkannt. Siehe dazu Kapitel 3.3.5.2.

[453] Gebräuchliche Standards sind etwa: Compact Flash Card, IBM MicroDrive, Smart Media Card, Multi Media Card, Secure Digital Card, Memory Stick, u.a.

rung gesprochen werden kann. Ein Ausweg aus diesen Abgrenzungsschwierigkeiten bestünde darin, auf das Kriterium der „Körperlichkeit“ zu verzichten und stattdessen die Dauerhaftigkeit der Datenspeicherung, insbesondere im Sinne der Unabhängigkeit von der Stromversorgung, genügen zu lassen. Diese Differenzierung liegt offensichtlich auch der bisher herrschenden Meinung zu Grunde, die eine ausreichende Fixierung von Daten im Arbeitsspeicher verneint, auf magnetischen Festspeichern jedoch bejaht. Beide Speichertechnologien unterscheiden sich nur durch ihre Abhängigkeit bzw. Unabhängigkeit von der Stromversorgung, lassen die Substanz des Datenträgers im Übrigen jedoch unberührt.

Darüber hinaus fordert die Rechtsprechung unter überwiegender Zustimmung der Literatur, dass die Darstellung der Daten in einem vom Gerät selbst abtrennbaren Gegenstand enthalten sein müssen.[454] Durch diesen Ansatz sollen Anzeigegeräte ausgeschlossen werden, die in einem fortlaufenden Messvorgang jeweils nachfolgende Messwerte mit einfließen lassen (z.B. Stromzähler, Gas- und Wasseruhren, usw.). Für den Bereich der Computerdaten bedeutet dies, dass Daten auf der fest montierten Festplatte ausscheiden, wohingegen auswechselbare Speichermedien wohl genügen – auch elektromagnetische – sofern man die Zweifel bzgl. der körperlichen Fixierung ignoriert. Am eindeutigsten dürften – wie oben gezeigt – die optischen Wechseldatenträger (CD, DVD, Blue-Ray, usw.) diese Anforderungen erfüllen.

Das Erfordernis der selbsttätigen Bewirkung der Aufzeichnung wird dann bejaht, wenn das Gerät durch einen in Programmierung oder Konstruktion festgelegten automatischen Vorgang einen Aufzeichnungsinhalt mit neuem Informationsgehalt hervorbringt.[455] An dieser Stelle werden üblicherweise Tonbandaufzeichnungen, Filme, Fotografien, Fotokopien und Maschinen geschriebene Briefe aus dem Tatbestand ausgeschlossen.[456] In diesen Fällen tritt keine eigenständige Leistung des Gerätes hinzu, sondern es liegt lediglich eine Perpetuierung eines unmittelbar durch menschliches Verhalten bestimmten Vorgangs vor. Daher können auch Computerausdrucke nur dann technische Aufzeichnungen sein, wenn sie eigenständige Rechenvorgänge dokumentieren und nicht nur wie elektrische Schreibmaschinen eingesetzt werden, um zuvor am Bildschirm editierte Texte, ohne weitere Rechenleistung, als Ausdrucke zu verkörpern.[457] Unabhängig vom Ausdruck werden EDV-Daten nur dann den Anforderungen von § 268 StGB genügen, wenn die Ausgabedaten (engl. *output data*) gegenüber den Eingabedaten (engl. *input data*) einen eigenständigen Informationsgehalt aufweisen, der durch die Datenverarbeitungsanlage als Ergebnis kombinatorischer oder rechnerischer Operationen hinzugefügt wurde.[458] Zwar wird dies für einen Großteil der EDV-Daten zutreffen (z.B. im automatischen Verfahren erstellte Steuerbescheide[459], usw.), daneben kennt die moderne Informationsgesellschaft jedoch auch eine Vielzahl von Daten, bei denen nicht klar ist, ob diese Voraussetzungen im Einzelfall vorliegen werden. Zu denken ist vor allem an elektronischen Zahlungsverkehr, Datenbanken und Archive, Emails, elektronischen Handel (engl. *e-commerce*), elektronische Bankgeschäfte (engl. *e-banking*), usw. Gerade wenn Passwortabfragen einen Benutzer gegenüber einem Computer identifizieren, erscheint es höchst zweifelhaft, von einer eigenständigen Translationsleistung der Maschine zu sprechen. Ohne eine Untersuchung der technischen Abläufe im Einzelnen ist die Beantwortung dieser Frage nicht möglich. Die Vorschrift trägt durch dieses Kriterium daher in erheblichem Umfang zur

[454] BGHSt 29, 204 (208) = JR 1980, 427 mit zustimmender Anm. von Kienapfel; ders., Urkunden und Gewährschaftsträger, S. 178 f.; LK – *Gribbohm* § 268 Rn 6; NK – *Puppe* § 268 Rn 24; Wessels/Hettinger, Strafrecht BT/1, Rn 862; aA: SK – *Hoyer* § 268 Rn 9

[455] Lackner/Kühl – *Kühl* § 268 Rn 4; Sch/Sch – *Cramer* § 268 Rn 15 ff.

[456] Freund JuS 1994, 207, 208; Sch/Sch – *Cramer* § 268 Rn 17

[457] Lackner/Kühl – *Kühl* § 268 Rn 4; SK – *Hoyer* § 268 Rn 18; differenzierend: LK – *Gribbohm* § 268 Rn 16; aA: NK – *Puppe* § 268 Rn 20

[458] So im Ergebnis: Sieber, Computerkriminalität und Strafrecht, S. 312 f.

[459] Sieber, Computerkriminalität und Strafrecht, S. 313

Rechtsunsicherheit bei.[460]

Für den Bereich der Computerdaten im Sinne der Konvention bedeutet dies, dass alle vom Benutzer selbst, ohne Hinzutreten einer automatisierten Rechnerleistung, erstellten Datensätze (Emails, Datenbanken, usw.) von § 268 StGB mangels selbsttätiger Bewirkung nicht geschützt werden. Zur Anwendung kann dann § 267 StGB kommen, allerdings nur für solche Daten, die Urkundsqualität besitzen (siehe Kapitel 3.6.5.1.1), also im Wesentlichen bei Ausdrucken. Hinzu kommt, dass, jedenfalls wenn man der Ansicht des BGH und eines Teils der Literatur folgt, nur solche Daten erfasst werden, die auf einem Speichermedium von der Datenverarbeitungsanlage abgetrennt werden können.

Darüber hinaus muss die technische Aufzeichnung ihren „Gegenstand allgemein oder für Eingeweihte" erkennen lassen. Viele Aufzeichnungen werden körperlich fest mit ihrem Bezugsobjekt verbunden sein (z.B. aufgedruckte Wiegeergebnisse, usw.), so dass sich diese Frage eigentlich nicht stellt; daneben sind aber auch Fälle denkbar, in denen ein solcher „Beweisbezug" fehlt (z.B. Röntgenbild ohne Vermerk, zu welchem Patienten es gehört). Dann liegt auch keine technische Aufzeichnung vor.[461] Als Mindestvoraussetzung wird in der Literatur eine körperlich feste Verbindung zwischen technischer Aufzeichnung und Bezugsobjekt oder ein entsprechender Beziehungsvermerk gefordert, wie er vor allem in Bezug auf Daten in Betracht kommt.[462] Daneben hat das Merkmal der Beweisbestimmung in Hinblick auf den beabsichtigten Rechtsgüterschutz keine besondere Bedeutung.[463]

Strafbar sind das Herstellen einer unechten, Verfälschen einer echten und/oder Gebrauchen einer unechten oder verfälschten technischen Aufzeichnung. Formal entsprechen diese Tathandlungsalternativen denen der Urkundenfälschung. Der entscheidende Unterschied liegt jedoch im Echtheitsbegriff des § 268 StGB, der sich auf eine technische Aufzeichnung und nicht auf eine Urkunde bezieht, so dass – mangels eines Ausstellers und einer Erklärung – die Auslegungsgrundsätze des § 267 StGB nicht ohne weiteres herangezogen werden können. Nach der wohl hM liegt eine unechte technische Aufzeichnung dann vor, wenn sie nicht das Ergebnis eines selbsttätigen und unbeeinflussten Herstellungsvorgangs ist.[464] Im Einzelnen ist allerdings noch vieles umstritten.

3.6.5.2.2 Ergebnis zu § 268 StGB

Als technische Aufzeichnungen nach § 268 Abs. 2 StGB wird nur eine Teil der Computerdaten nach Art. 7 und Art. 1 lit. b) geschützt. Weitgehend ungeklärt ist bislang, welche Speichertechnologien die Anforderungen einer dauerhaften stofflichen Fixierung als Voraussetzung für eine „Darstellung von Daten" erfüllen. Darüber hinaus kommen nur Daten auf Wechseldatenträgern in Betracht, denn nur diese können – wie von der hM gefordert – vom „technischen Gerät" abgetrennt werden. Eine wesentliche Einschränkung besteht schließlich im Erfordernis der „selbsttätigen" Bewirkung der Aufzeichnung, die im EDV-Bereich auf Grund fließender Übergänge im Rahmen der Verarbeitungsvorgänge zu erheblichen Abgrenzungsschwierigkeiten führt. Auch in Bezug auf die „Echtheit" einer technischen Aufzeichnung ergeben sich Unterschiede. Auf eine Täuschung über die Identität des Ausstellers wie bei Art. 7 kommt es nicht an. Vielmehr ist entscheidend, ob eine Aufzeichnung nach § 268

[460] Kritisch daher: Freund JuS 1994, 207 (208)
[461] Sch/Sch – *Cramer* § 268 Rn 19
[462] LK – *Gribbohm* § 268 Rn 22 f.; NK – *Puppe* § 268 Rn 12; SK – *Hoyer* § 268 Rn 12 f.
[463] Freund JuS 1994, 207 (209)
[464] Lackner/Kühl – *Kühl* § 268 Rn 7; Sch/Sch – *Cramer* § 268 Rn 33; Tröndle/Fischer § 268 Rn 11a; aA: Sieber, Computerkriminalität und Strafrecht, S. 322 und SK – *Hoyer* § 268 Rn 4 ff., 24

Abs. 2 StGB das Ergebnis eines ungestörten technischen Aufzeichnungsprozesses ist.

3.6.5.3 § 269 StGB – Fälschung beweiserheblicher Daten

§ 269 StGB schützt in sachlicher Übereinstimmung zu den §§ 267 und 268 StGB die Sicherheit und Zuverlässigkeit des Beweisverkehrs mit beweiserheblichen Daten[465], dort wo diese weder Urkunden noch technische Aufzeichnungen darstellen. Zwar wurde der Tatbestand bei seiner Einführung durch das 2. WiKG von der Literatur skeptisch aufgenommen.[466] Dies dürfte jedoch vor allem daran gelegen haben, dass der elektronische Geschäftsverkehr in den 1980er Jahren noch am Anfang seiner Entwicklung stand und nur wenige einschlägige Fälle bekannt waren. Die aktuelle technische Entwicklung zeigt, dass Computerdaten in Zukunft eine wachsende Bedeutung im Rechtsverkehr haben werden (vor allem bei Transaktionen im Internet). In diesem Zusammenhang ist auch das Gesetz zur Anpassung von Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr vom 13.07.2001[467] zu sehen, das in bestimmten Fällen die Schriftform mit der elektronischen Form nach dem Signaturgesetz gleichsetzt. Auf diese Weise wurde der Weg für die elektronische Urkunde geebnet, die auch strafrechtlichen Schutz verdient.

3.6.5.3.1 Tatbestand

Tatobjekte sind „[…] Daten, die bei ihrer Wahrnehmung einer Urkunde gleichstehen würden […]". Aus diesem Erfordernis des „hypothetischen Vergleichs"[468] wird deutlich, dass die tatbestandlichen Daten ähnlich wie bei § 202a Abs. 2 StGB mit bloßem Auge nicht erkennbar sein dürfen. Die Gesetzesbegründung führt dazu aus, dass wie bei § 263a StGB ein Verweis auf § 202a Abs. 2 StGB unterblieb, da der Tatbestand der Datenveränderung von Manipulationen an bereits gespeicherten Daten ausgeht, wohingegen eine Fälschung beweiserheblicher Daten bzw. ein Computerbetrug auch Dateneingaben erfasst.[469] Im Übrigen kann wegen der Einzelheiten des Datenbegriffs auf die Ausführungen in Kapitel 2.2.1 verwiesen werden. Einschränkend stellt § 269 StGB nicht auf Daten schlechthin, sondern nur auf „beweiserhebliche" ab. Dieser Zusatz ist überflüssig, da er sich bereits aus dem hypothetischen Vergleich zu Urkunden ergibt.[470] In der Entwurfsfassung hieß es dazu noch, dass nur solche Daten erfasst würden, „[…] die dazu bestimmt sind, bei einer Verarbeitung im Rechtsverkehr als Beweisdaten für rechtlich erhebliche Zwecke benutzt zu werden […]." Die Literatur weist in diesem Zusammenhang zu Recht darauf hin, dass das einzelne Datum nicht einer Urkunde gleichstehe, sondern sich diese aus Daten im weiteren Sinne (in der Regel alphanumerische Zeichen) zusammensetzte.[471] Es ginge daher zu weit, in Bezug auf einzelne Daten den hypothetischen Urkundenmaßstab anzulegen. Vielmehr muss genügen, dass einzelne Daten geeignet sind, zusammen mit anderen Beweis zu erbringen.[472]

Von zentraler Bedeutung ist das Erfordernis des hypothetischen Vergleichs zu Urkunden, das,

[465] Freund JuS 1994, 207 (209); Lackner/Kühl – *Kühl* § 269 Rn 1; LK – *Gribbohm* § 269 Rn 1; Sch/Sch – *Cramer* § 269 Rn 4; aA: SK – *Hoyer* (6. Aufl.) § 269 Rn 1, „Dispositionsfreiheit der Teilnehmer am Rechtsverkehr".
[466] Kritisch vor allem: NK – *Puppe* § 269 Rn 7
[467] BGBl. 2001 I, S. 1542
[468] BT-Drs. 10/5058, S. 34
[469] BT-Drs. 10/5058, S. 34
[470] BT-Drs. 10/5058, S. 34; Sch/Sch – *Cramer* § 269 Rn 9
[471] Sch/Sch – *Cramer* § 269 Rn 10; SK – *Hoyer* § 269 Rn 6
[472] Sch/Sch – *Cramer* § 269 Rn 10; SK – *Hoyer* § 269 Rn 6

obwohl die visuelle Wahrnehmbarkeit von Daten vom Tatbestand für überflüssig erklärt wird, im Übrigen am strafrechtlichen Urkundenbegriff festhält. Wie eine körperliche muss auch eine „virtuelle“ Urkunde eine menschliche Gedankenerklärung verkörpern. Es ist daher in jedem Einzelfall zu hinterfragen, welchen Erklärungsinhalt ein bestimmter Datensatz beinhaltet. Danach scheiden alle Daten aus, die Ergebnis eines selbsttätigen Herstellungsvorgangs sind, wie beispielsweise Protokolldaten[473], jedoch gerade keine abschichtbare Gedankenerklärung enthalten. In Betracht kommt in diesem Fall eine technische Aufzeichnung nach § 268 Abs. 2 StGB. Auch Daten, die als Entwürfe für spätere Ausdrucke dienen, sind in der Regel, wenn sie nicht unabhängig von dem körperlichen Beweisstück für den Rechtsverkehr bestimmt sind, keine Computerurkunden. Die Ausdrucke können jedoch als sog. „EDV-Urkunden“ Schutz durch § 267 StGB erfahren.[474] Computerprogramme beinhalten nach zutreffender Ansicht keinen eigenständigen Erklärungsgehalt, da die Programmierer damit keinen rechtlich erheblichen Willen äußern, sondern vielmehr einen gestalterischen Erfolg begründen wollen. Ihr Schutz richtet sich daher in erster Linie nach den Regeln des Urheberrechts.[475] Anders verhält es sich dagegen mit der Beschriftung von Scheckkartenblanketten mit den Daten fremder Benutzer. Auf dem Magnetstreifen einer solchen Karte befindet sich eine Garantieerklärung der ausstellenden Bank hinsichtlich der Berechtigung ihres Kunden.[476] Unklar ist darüber hinaus, welche Anforderungen an die Verbindung einer Mehrheit von Dateien ohne eigenständigen Erklärungsgehalt zu stellen sind, um nach einem hypothetischen Vergleich von einer zusammengesetzten Urkunde sprechen zu können bzw. inwieweit den sog. „Indexdateien“[477], die den Beweisbezug herstellen, selbst Urkundenqualität zukommt. Richtigerweise wird wohl eine inhaltliche logische Verbindung genügen müssen, die auch die Verweisdateien selbst mit einbezieht, denn einen physische Verbindung von Dateien entspricht nicht der technischen Realität.[478]

Weiterhin ist umstritten, unter welchen Voraussetzungen die „Computerurkunde“ ihre Perpetuierungsfunktion wahrnimmt. Eine Urkunde im herkömmlichen Sinne muss dazu eine stoffliche und – untrennbar damit verbunden – sichtbare Fixierung einer Gedankenerklärung vornehmen. Während der Tatbestand des § 269 StGB ausdrücklich auf die visuelle Wahrnehmbarkeit verzichtet, bleibt unklar, welche Anforderungen an die Stofflichkeit und Dauerhaftigkeit zu stellen sind. Wie bei § 268 StGB dargestellt wurde, erfüllen derzeit nur die optischen Wechseldatenträger die Anforderungen einer körperlichen Fixierung. Elektromagnetische Medien speichern Daten in Form flüchtiger Spannungszustände und Änderungen eines Magnetfelds, ohne Auswirkungen auf die Substanz. Insofern kann schwerlich von einer physischen Manifestierung gesprochen werden, so dass Teile der Literatur im Erfordernis des hypothetischen Vergleichs auch zu Recht einen Verzicht auf die Körperlichkeit der Datenspeicherung erblicken.[479] Stattdessen sollte allein auf die Dauerhaftigkeit im Sinne einer Unabhängigkeit von der Stromversorgung abgestellt werden, um Abgrenzungsschwierigkeiten im Zusammenhang mit unterschiedlichen Speichertechnologien zu vermeiden (siehe auch die Ausführungen zu § 268 StGB, Kapitel 3.6.5.3.1).

Darüber hinaus müssen die Daten „beweiserheblich“, d.h. zum Beweis rechtserheblicher Tatsachen in objektiver Hinsicht geeignet und subjektiv dazu bestimmt sein. Beide Kriterien sind

[473] NK – *Puppe* § 269 Rn 13
[474] Lackner/Kühl – *Kühl* § 269 Rn 4
[475] NK – *Puppe* § 269 Rn 14; SK – *Hoyer* § 269 Rn 16
[476] AG Böblingen Az.: 9 Ls (Cs) 1449/87 = WM 1990, 64 (65); BGH 38, 120 (121) = NJW 1992, 445 (445)
[477] Beispielsweise diejenigen Daten, die innerhalb einer relationalen Datenbank den Bezug zwischen miteinander in Verbindung stehenden Tabellen herstellen.
[478] Lackner/Kühl – *Kühl* § 269 Rn 5; NK – *Puppe* § 269 Rn 22 ff.; Welp CR 1992, 354 (357 f.); ablehnend: SK – *Hoyer* § 269 Rn 18 mwN
[479] Lackner/Kühl – *Kühl* § 269 Rn 6; LK – *Gribbohm* § 269 Rn 13; Sch/Sch – *Cramer* § 269 Rn 14

wie im Rahmen der Urkundenfälschung in einem weiten Sinne zu verstehen und bringen keine wesentliche Einschränkung für die „Datenurkunde“.[480] Die „Echtheit“ beurteilt sich danach, ob der tatsächliche Aussteller der Daten mit demjenigen identisch ist, der aus ihnen hervorgeht. Nach der im Zusammenhang mit der Urkundenfälschung entwickelten Geistigkeitstheorie handelt es sich dabei um diejenige Person, der die Daten rechtlich zugerechnet werden können. In Anlehnung an die zu § 267 StGB entwickelten Auslegungsgrundsätze sollte wegen der Strukturgleichheit beider Tatbestände genügen, dass der Aussteller nicht unmittelbar aus der Datenurkunde hervorgehen muss, solange er unter Zuhilfenahme weiterer Umstände bestimmt werden kann.[481] In Bezug auf den Echtheitsschutz kommt elektronischen Signaturen eine besondere Bedeutung zu.

3.6.5.3.2 Tathandlung

In Bezug auf die Tathandlung unterscheidet § 269 StGB zwischen dem „Speichern“ oder „Verändern“ von Daten, so dass bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde vorliegen würde, sowie dem „Gebrauch“ derart verfälschter Daten. Zur Bestimmung der ersten beiden Handlungsalternativen orientiert sich die Literatur an den Legaldefinitionen in § 3 Abs. 4 Nr. 1 und Nr. 2 BDSG.[482] Wegen der unterschiedlichen Anwendungsbereiche beider Gesetze erscheinen die Begriffsbestimmungen aber nicht unmittelbar übertragbar zu sein. Da auf Grund des Erfordernisses des hypothetischen Vergleichs nach dem Speicher oder Verändern eine „Datenurkunde“ entstehen muss, die bis auf die visuelle Wahrnehmbarkeit den Urkundenbegriff des § 267 StGB erfüllt, dürfen sich die Tathandlungen nicht im vorübergehenden Ablegen oder Modifizieren von Daten im Arbeitsspeicher eines Computers erschöpfen.[483] Vielmehr kommt parallel zum „Herstellen“ einer unechten Urkunde im Sinne von § 267 StGB nur das erstmalige Abspeichern einer „Datenurkunde“ auf einem dauerhaften Datenträger bzw. das Verändern dauerhaft gespeicherter Daten in Betracht[484], so dass diese erstmals Urkundenqualität erlangen. Vergleichbar zum Verfälschen einer unechten Urkunde wäre, dass eine bereits gespeicherte Datenurkunde durch das dauerhafte Hinzufügen weiterer Daten (Speichern von Daten) oder das nicht nur vorübergehende Ersetzen oder Weglassen vorhandener Daten (Verändern) geändert wird.[485] Ein „Gebrauchen“ liegt ähnlich wie bei § 267 StGB dann vor, wenn die Daten einem potentiellen Beweisadressaten unmittelbar zugänglich gemacht werden. Diese Tatbestandsvariante wurde neben dem Speichern in einem Fall bejaht, in dem der Täter eine präparierte Scheckkarte an einem Geldautomaten einsetzte.[486] In subjektiver Hinsicht ist neben dem allgemeinen Vorsatz in Bezug auf alle objektiven Tatbestandsmerkmale eine besondere Täuschungsabsicht erforderlich.

3.6.5.3.3 Ergebnis zu § 269 StGB

§ 269 StGB schützt nach seinem Wortlaut Daten, die bis auf das Erfordernis der visuellen Wahrnehmbarkeit Urkundenqualität nach § 267 StGB besitzen. Dieses Erfordernis des hypo-

[480] Lackner/Kühl – *Kühl* § 269 Rn 4; LK – *Gribbohm* § 269 Rn 9
[481] Lackner/Kühl – *Kühl* § 269 Rn 6; Möhrenschlager wistra1986, 128 (135); aA: SK – *Hoyer* § 269 Rn 22
[482] Bühler MDR 1987, 448 (454); LK – *Gribbohm* § 269 Rn 11
[483] aA: Sch/Sch – *Cramer* § 269 Rn 16; ohne Bezugnahme auf die Dauerhaftigkeit der Speicherung: SK – *Hoyer* § 269 Rn 8 ff.
[484] Zur Abgrenzung „Herstellen einer unechten“ und „Verfälschen einer echten Datenurkunde“: NK – *Puppe* § 269 Rn 31; aA: Lackner/Kühl – *Kühl* § 269 Rn 8 ff. und Tröndle/Fischer § 269 Rn 4 ff., die im „Speichern“ die Parallele zum Herstellen und im „Verändern“ zum Verfälschen einer Urkunde sehen.
[485] aA: SK – *Hoyer* § 269 Rn 9, der beim Löschen von Daten eine Datenunterdrückung nach § 274 Abs. 1 Nr. 2 StGB annimmt.
[486] Freund JuS 1994, 207 (209) mwN

thetischen Vergleichs erweist sich vor allem in Bezug auf die Perpetuierungsfunktion von Urkunden als problematisch. Wie bereits im Rahmen von § 268 StGB dargestellt, werden Daten nur in Ausnahmefällen bei ihrer Speicherung körperlich fixiert. Um durch unterschiedliche Speichertechnologien drohende Abgrenzungsschwierigkeiten zu vermeiden, sollte stattdessen auf die Dauerhaftigkeit der Speicherung im Sinne einer Unabhängigkeit von der Stromversorgung abgestellt werden. Art. 7 stellt demgegenüber keine vergleichbar hohen Anforderungen an die Datenurkunde. Dies gilt auch in Bezug auf die durch die Daten dargestellte Erklärung, die das Ergebnis eines wenigstens teilweise „selbsttätigen" Verarbeitungsvorgangs sein kann. Im nationalen Strafrecht wäre dann allenfalls § 268 StGB einschlägig, wobei sich dieser Tatbestand nicht auf die Identität des aus den Daten ersichtlichen und des tatsächlichen Ausstellers, sondern auf einen fehlerfreien Aufzeichnungsprozess bezieht. In subjektiver Hinsicht verlangt § 269 StGB eine besondere Täuschungsabsicht, während nach Art. 7 Abs. 2 eine „betrügerische oder ähnlich unredliche Absicht" eine lediglich fakultative Voraussetzung der Strafbarkeit darstellt.

3.6.5.4 § 270 StGB – Täuschung im Rechtsverkehr bei Datenverarbeitung

§ 270 StGB beinhaltet keinen eigenständigen Straftatbestand, sondern stellt die „fälschliche Beeinflussung einer Datenverarbeitung" einer „Täuschung im Rechtsverkehr" gleich. Dies ist etwa relevant für die Tatbestände der §§ 267, 268, 269 StGB. Die Gleichstellung ist nach neuerer Ansicht[487] unverzichtbar, um Strafbarkeitslücken zu schließen, während ihr auf der Grundlage der bislang herrschenden Meinung[488] lediglich deklaratorischer Charakter zukam. Diese unterschiedliche Bewertung lässt sich wie folgt erklären: Beide Meinungen stimmen darin überein, dass nach dem Wortsinn nur ein Mensch, niemals jedoch eine Maschine getäuscht werden könne. Dadurch erklärt sich auch die Existenz von § 263a StGB. Während die Täuschungshandlung beim Betrugstatbestand jedoch einen unmittelbaren Personenbezug aufweise, sei dies, jedenfalls nach der bislang hM, zur „Täuschung im Rechtsverkehr" bei den Urkundendelikten nicht erforderlich. Dort genüge es, wenn unechte Beweisstücke zunächst von einem Automaten verarbeitet würden, wenn nicht auszuschließen ist, dass sie zu einem späteren Zeitpunkt menschliches Verhalten beeinflussen werden. Eine strenge Unmittelbarkeit wird nach dieser Auffassung nicht verlangt. Der Meinungsstreit muss nicht entschieden werden, da er für einen Vergleich zu Art. 7, der nicht zwischen der Täuschung eines Menschen und der Beeinflussung eines Datenverarbeitungsvorgangs unterscheidet, bedeutungslos ist. § 270 StGB beinhaltet keine weiteren vergleichbaren Tatbestandsmerkmale.

3.6.6 Bewertung Art. 7

Art. 7 findet in § 269 StGB eine vergleichbare Bestimmung im deutschen Strafrecht. Dieser Tatbestand wurde aus vergleichbaren Erwägungen in das StGB eingefügt, nämlich um den im Wesentlichen auf Schriftstücke beschränkten Urkundenschutz durch den Einsatz moderner EDV-Technologien nicht zu verkürzen.[489] Anders als bei den Art. 2-6 bestehen keine Bedenken an der Bestimmtheit des Tatbestandes. Die Verbotsmaterie „Herstellen unechter Daten", egal ob aus einer Datenvorlage oder ohne eine solche, wird hinreichend beschrieben. Art. 7 geht geringfügig über § 269 StGB hinaus, da er sich nicht an einem engen Urkundenbegriff orientiert, sondern schlechthin alle rechtserheblichen Daten vor Verfälschung schützt.

[487] SK – *Hoyer* (6. Aufl.) § 270 Rn 1ff.
[488] Lackner/Kühl – *Kühl* § 270 Rn 1; Lenckner/Winkelbauer CR 1986, 824 (828); LK – Tröndle (10. Aufl.) § 267 Rn 189; Sch/Sch – *Cramer* § 270 Rn 1
[489] BT-Drs. 10/5058, S. 33

3.7 Artikel 8 – Computerbetrug[490]

Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um die vorsätzliche und unbefugte Beschädigung des Vermögens eines anderen durch

a) Eingeben, Verändern, Löschen oder Unterdrücken von Computerdaten,

b) Eingreifen in die Funktionsweise eines Computers oder Systems

in der betrügerischen oder unredlichen Absicht, sich oder einem anderen unbefugt einen wirtschaftlichen Vorteil zu verschaffen, als Straftat nach ihrem innerstaatlichen Recht festzulegen.

3.7.1 Anwendungsbereich

Art. 8 geht wie die Art. 3 und 5 im Wesentlichen auf einen Entwurf in der Empfehlung Nr. R (89) 9[491] des Europarates zurück. Den Verfassern der Konvention kam es darauf an, den strafrechtlichen Vermögensschutz im Bereich der neuen Medien zu ergänzen. Dort, wo automatisierte Systeme Vermögensgegenstände verwalten, kann es durch strafwürdige Manipulationen an Hard- und Software zu rechtswidrigen Vermögensverschiebungen kommen, die von den bestehenden Betrugsvorschriften oftmals nicht erfasst werden.

3.7.2 Tatbestand

Der Taterfolg besteht in einem unmittelbaren Vermögensschaden (engl. *„[...] the causing of a loss of property to another [...]"*) eines anderen. Der Begriff ist weit auszulegen und umfasst den Verlust von Geld sowie materiellen und immateriellen Vermögensgegenständen, sofern ihnen ein wirtschaftlicher Wert zukommt.

Als Tathandlungen werden von lit. a) das „Eingeben", „Verändern", „Löschen" oder „Unterdrücken" von Computerdaten nach Art. 1 lit. b) (siehe Kapitel 2.2) genannt. Zu ihrer Auslegung kann auf die Artikel 4, 5 und 7 zurückgegriffen werden. Lit. b) pönalisiert als Auffangtatbestand das sonstige „Eingreifen in die Funktionsweise eines Computers oder Systems" (engl. „*computer system"*), womit alle Arten von Hard- und Softwaremanipulationen gemeint sind, die nicht bereits von den ersten vier Handlungsvarianten erfasst werden.

In subjektiver Hinsicht verlangt der Tatbestand neben dem allgemeinen Vorsatz eine „betrügerische oder unredliche Absicht", die sich auf die Erlangung eines wirtschaftlichen Vorteils für den Täter oder einen anderen beziehen muss. Der in der Empfehlung Nr. R (89) 9 enthaltene Entwurf stellte noch auf die Absicht ab, einem anderen Vermögen zu entziehen, wobei die Aufnahme dieses subjektiven Merkmals nur optional vorgesehen war. Nach Ansicht der Verfasser soll der Tatbestand dadurch begrenzt werden. Eine derartige Absicht liege beispielsweise nicht vor, wenn ein Nutzer automatisierte Programme zum Preisvergleich von Konsumgütern im Internet benutze (engl. *bots*).

Ähnlich unbestimmt wie in den vorangegangenen Artikeln führen die Erläuterungen aus, dass nur solches Verhalten „unbefugt" sei, dass nicht mit gängigen Verhaltensweisen im Rechts-

[490] ER Ziff. 86-90

[491] *Recommendation on Computer-Related Crime*; Europarat, Computer-Related Crime, S. 36; Online: http://cm.coe.int/ta/rec/1989/89r9.htm (01.03.2004), allerdings ohne den „Report on Crime Problems", auf den die Empfehlung Bezug nimmt.

verkehr korrespondiere, sich beispielsweise nicht auf einen wirksamen Vertrag stützen könne.

3.7.3 Vergleichbare Tatbestände im deutschen Strafrecht

Betrugstatbestände definiert das deutsche StGB im 22. Abschnitt. Für einen Vergleich zu Art. 8 kommt lediglich die durch das 2. WiKG eingeführte Norm des Computerbetrugs nach § 263a StGB in Betracht. Der Grundtatbestand des § 263 StGB weist nach der vorherrschenden Meinung[492] wenigstens hinsichtlich der Täuschungshandlung einen individuellen Personenbezug auf, d.h. dass die Tathandlung auf die unmittelbare Einwirkung auf das intellektuelle Vorstellungsbild eines Menschen gerichtet ist. Wenn dagegen ein Datenverarbeitungsvorgang manipuliert wird, wird kein Mensch getäuscht, sondern eine Maschine manipuliert, so dass alleine eine Strafbarkeit wegen Computerbetrugs in Betracht kommt.

3.7.3.1 § 263a StGB – Computerbetrug

Geschütztes Rechtsgut ist ebenso wie bei § 263 StGB ausschließlich das Vermögen. Ein darüber hinausgehendes allgemeines Interesse an der Funktionstüchtigkeit der in Wirtschaft und Verwaltung verwendeten EDV-Anlagen ist ein bloßer Schutzreflex und als eigenständiges Rechtsgut abzulehnen.[493] Der Norm wurde bei ihrer Einführung neben § 269 StGB eine Schlüsselrolle bei der Bekämpfung der Computerkriminalität beigemessen. Bislang kam ihr allerdings nur in den Fallgruppen des Leerspielens von Geldspielautomaten und des Codekartenmissbrauchs größere Bedeutung zu. In der Literatur wurden vor allem gegen die dritte Handlungsvariante verfassungsrechtliche Bedenken erhoben.[494] Nach dem Willen des Gesetzgebers soll sich die Auslegung des § 263a StGB wegen der strukturellen Parallelität am Betrugstatbestand orientieren.[495]

3.7.3.2 Taterfolg

Zwischenerfolg aller Tathandlungen ist die „Beeinflussung des Ergebnisses eines Datenverarbeitungsvorgangs“. Dieses Merkmal korrespondiert mit der Irrtumserregung und Vermögensverfügung im Betrugstatbestand.[496] Zum Datenbegriff siehe die Darstellungen in Kapitel 2.2.1. Von einem Verweis auf die Einschränkungen des § 202a StGB wurde wie bei § 269 StGB abgesehen, da neben Manipulationen an gespeicherten Daten auch die Eingabe „neuer“ Daten erfasst werden sollte.[497] Der Begriff der Datenverarbeitung wurde in Kapitel 2.1.1 dargestellt. Umstritten ist, ob die Beeinflussung eines Datenverarbeitungsvorgangs eine „programmwidrige“ Einflussnahme erfordert, d.h. eine Änderung des Programmablaufs.[498] Nach

[492] Bühler MDR 1987, 448 (449); Lackner/Kühl – *Kühl* § 263 Rn 6; Lenckner/Winkelbauer CR 1986, 824 (828); Möhrenschlager wistra 1986, 128 (131); Sch/Sch – *Cramer* § 263 Rn 6; Tiedemann JZ 1986, 865 (867); Tröndle/Fischer § 263 Rn 10; für einen Personenbezug auch der anderen Tatbestandsmerkmale: BT-Drs. 10/5058, S. 30

[493] Lackner/Kühl – *Kühl* § 263a Rn 1; LK – *Tiedemann* (11. Aufl.) § 263a Rn 13; NK – *Kindhäuser* § 263a Rn 2 BGHSt 40, 331 (334)

[494] U.a. Kleb-Braun JA 1986, 249 (259); Spahn Jura 1989, 513 (519); aA: BGHSt 38, 120 (121 f.); LK – *Tiedemann* § 263a Rn 4

[495] BT-Drs. 10/5058, S. 30

[496] RegE BT-Drs. 10/318, S. 19; LK – *Tiedemann* § 263a Rn 26, 65; Möhrenschlager wistra 1986, 128 (133); NK – *Kindhäuser* § 263a Rn 5

[497] BT-Drs. 10/5058, S. 30 und 34

[498] BayObLG JR 1994, 289 (294) mit Anm. Achenbach; Tröndle/Fischer § 263a Rn 20; aA bzgl. 3. und 4. Variante: Lackner/Kühl – *Kühl* § 263a Rn 22; LK – *Tiedemann* § 263a Rn 26; Möhrenschlager wistra 1986, 128 (133)

dem natürlichen Wortsinn ergibt sich eine derartige Einschränkung nicht. Verlangt man einen programmwidrigen Eingriff, würden die meisten Fälle des Scheckkartenmissbrauchs und des Leerspielens von Automaten nicht mehr vom Tatbestand erfasst. Zu denken wäre dann nur noch an technische Manipulationen (z.B. Beschreiben von Blanketten mit entsprechender Hardware, usw.), nicht jedoch an den – jedenfalls äußerlich – ordnungsgemäßen Einsatz einer gestohlenen Karte an einem Automaten bzw. die Betätigung der Risikotaste im „richtigen" Zeitpunkt. Als Folge der Beeinflussung muss es zu einer Vermögensdisposition der Datenverarbeitungsanlage kommen[499] – entspricht der Vermögensverfügung bei § 263 StGB –, die unmittelbar in einen Vermögensschaden beim Opfer mündet. Hinsichtlich des Vermögensschadens beim Geschädigten ergeben sich keine Abweichungen zu § 263 StGB, d.h. er ist dann zu bejahen, wenn der durch die Vermögensdisposition verursachten Vermögensminderung keine äquivalente Vermögensmehrung gegenübertritt. Die Einzelheiten sind für einen Vergleich zu Art. 8 nicht von Bedeutung.

3.7.3.3 Tathandlung

§ 263a StGB unterscheidet zwischen vier Tathandlungen. Wie bei Art. 8 stellt die vierte Variante („oder sonst durch unbefugte Einwirkung auf den Ablauf beeinflusst") einen Auffangtatbestand dar.

Bei der „unrichtigen Gestaltung eines Programms" handelt es sich, da alle Programme aus Daten bestehen, um einen Unterfall (lex specialis) der 2. Variante.[500] Wann ein Programm unrichtig ist, ist umstritten. Eine Ansicht stellt auf den Willen des Berechtigten ab[501], während die wohl herrschende Meinung[502] in Anlehnung an das sonstige Betrugsstrafrecht an die objektive Wirklichkeit anknüpft. Vorzugswürdig ist die vorherrschende Meinung, da anderenfalls eine unrichtige Programmgestaltung durch einen Programmierer selbst nicht möglich wäre.[503] Die 2. Variante betrifft die „Verwendung unrichtiger oder unvollständiger Daten", d.h. im Wesentlichen Manipulationen bei der Dateneingabe (sog. „Inputmanipulationen[504]). Bei der Bestimmung der Unrichtigkeit und Unvollständigkeit ist, wie in Bezug auf die „unrichtige Gestaltung eines Programms" (1. Variante), eine objektive Betrachtungsweise in Anlehnung an den tatsachenbezogenen Täuschungsbegriff des § 263 StGB anzulegen. Daten sind unrichtig, wenn die durch sie dargestellten Informationen nicht der Realität entsprechen, indem Lebenssachverhalte falsch wiedergeben werden. Unvollständig sind sie beim teilweisen Weglassen bestimmter Angaben, die zusammen einen Lebenssachverhalt ausmachen.[505] Daten werden verwendet, wenn sie Eingang in einen beginnenden oder bereits angelaufenen Datenverarbeitungsprozess finden.[506]

Die „unbefugte Verwendung von Daten" wurde als 3. Variante eingefügt, um der Verwendung von Magnetkarten an Automaten durch Nichtberechtigte sowie der Nutzung fremder Btx-Anschlüsse strafrechtlich begegnen zu können. Im Unterschied zur 2. Variante sind die

[499] LK – *Tiedemann* § 263a Rn 68; Lenckner/Winkelbauer CR 1986, 654 (659); Möhrenschlager wistra 1986, 128 (133)
[500] BT-Drs. 10/318, S. 20; Granderath DB 1986, Beilage Nr. 18, 1 (4); Lackner/Kühl – *Kühl* § 263a Rn 6; LK – *Tiedemann* § 263a Rn 27
[501] BT-Drs. 10/318, S. 20; Lenckner/Winkelbauer CR 1986, 654 (656); Sch/Sch – *Cramer* § 263a Rn 6
[502] Hilgendorf JuS 1997, 130 (131); Lackner/Kühl – *Kühl* § 263a Rn 7; LK – *Tiedemann* § 263a Rn 31; Tröndle/Fischer § 263a Rn 6
[503] LK – *Tiedemann* § 263a Rn 31
[504] Sieber, Computerkriminalität und Strafrecht, S. 42
[505] Hilgendorf JuS 1997, 130 (131); LK – *Tiedemann* § 263a Rn 33, 34; NK – *Kindhäuser* § 263a Rn 25; Sch/Sch – *Cramer* § 263a Rn 25
[506] Lackner/Kühl – *Kühl* § 263a Rn 9; Tröndle/Fischer § 263a Rn 8

Daten in diesem Fall richtig, werden aber ohne Befugnis verwendet.[507] Der Begriff der „Verwendung“ ist weitgehend identisch mit dem der 2. Variante.[508] Erheblich umstritten ist allerdings das Merkmal „unbefugt“, dem entscheidende Bedeutung bei der Begrenzung des Tatbestandes zukommt. Im Wesentlichen existieren drei Auffassungen:

Nach der subjektivierenden Ansicht[509] entscheide sich die Frage der Unbefugtheit nach dem ausdrücklichen oder mutmaßlichen Willen des über die Daten Verfügungsberechtigten. Da § 263a StGB wie der Betrugstatbestand das Individualvermögen schütze, sei die Verwendung von Daten dann „unbefugt“, wenn sie dem Willen des Rechtsgutsträgers widerspreche.[510] Diese Auffassung ist in der Praxis zwar leicht zu handhaben[511], jedoch erweitert sie den Anwendungsbereich der Norm im Vergleich zu den anderen beiden Ansichten am stärksten. Die Grenze zur „Computeruntreue“[512] wird verwischt, so dass auch nicht betrugsspezifische Sachverhalte erfasst werden[513]. Da diese Ansicht nicht die rechtsstaatlich gebotene Begrenzung des Tatbestandes erlaubt, ist sie abzulehnen.

Nach einer zweiten Ansicht, die auf das OLG Celle zurückgeht, ergebe sich die Unbefugtheit aus dem Willen des Berechtigten in Bezug auf „computerspezifische“ Vorgänge.[514] Bei einer äußerlich ordnungsgemäßen Bedienung eines DV-Vorgangs sei kein Raum für einen der Datenverwendung entgegenstehenden Willen. Gegen diese Meinung wird zu Recht eingewendet, dass sie zu unbestimmt sei, da nicht klar werde, welche Vorgänge im Einzelnen „computerspezifischen“ Charakter trügen.[515] Gleichzeitig ist sie zu eng, da, anders als vom historischen Gesetzgeber intendiert[516], bestimmte Sachverhalte des Geldautomatenmissbrauchs (Bankomat) nicht erfasst werden. So könnte der Scheckkartendieb, der mit einer gestohlenen Karte von einem fremden Konto Geld am Automaten abhebt, trotz eindeutig fehlender Berechtigung in Bezug auf die Kartendaten, nicht wegen Computerbetrugs bestraft werden.[517] Die Ansicht des OLG Celle ist daher abzulehnen.

Eine dritte Meinung[518] fordert, sich wegen der Strukturgleichheit zu § 263 StGB stärker am Betrugstatbestand zu orientieren. Eine „unbefugte“ Verwendung von Daten solle demnach nur in Fällen einer „täuschungsgleichen Handlung“ vorliegen, d.h. wenn bei Einsatz der Daten gegenüber einer natürlichen Person eine Täuschung anzunehmen wäre. Diese Auffassung kann sich hinsichtlich der Anlehnung an den Betrugstatbestand auf den Willen des historischen Gesetzgebers stützen.[519] Methodisch findet sich für die Heranziehung eines Vergleichs eine Parallele in § 269 StGB.[520] Gegen diese Auffassung wird vor allem eingewendet, dass sie

[507] LK – *Tiedemann* § 263a Rn 40; NK – *Kindhäuser* § 263a Rn 28
[508] Zu Abweichungen im Einzelnen siehe: LK – *Tiedemann* § 263a Rn 41
[509] BayObLG NJW 1991, 438 (440); BGH 40, 331 (334 f.); Granderath DB 1986, Beilage Nr. 18, 1 (4); auf eine „vertragswidrige“ Verwendung der Daten abstellend: Maurach/Schroeder/Maiwald BT/1 § 41 VI Rn 233; Überblick bei: LK – *Tiedemann* § 263a Rn 42 f.
[510] BayObLG NJW 1991, 438 (440) in Anlehnung an § 17 Abs. 2 UWG, der ebenfalls auf das 2. WiKG zurückgeht; BGH 40, 331 (334 f.)
[511] Hilgendorf JuS 1997, 130 (132); daran zweifelnd: LK – *Tiedemann* § 263a Rn 43 mwN
[512] so: SK – *Günther* (5. Aufl.) § 263a Rn 18
[513] Beispiele bei Hilgendorf JuS 1997, 130 (132 f.)
[514] OLG Celle NStZ 1989, 367 f.; mit Besprechung Neumann JuS 1990, 535 ff.; Haurand/Vahle RDV 1990, 128 (132 f.)
[515] BayObLG NJW 1991, 438 (440)
[516] BT-Drs. 10/5058, S. 30
[517] LK – *Tiedemann* § 263a Rn 45
[518] OLG Köln NJW 1992, 125 (126 f.); Lackner/Kühl – *Kühl* § 263a Rn 13; NK – *Kindhäuser* § 263a Rn 29; Sch/Sch – *Cramer* § 263a Rn 13; Tröndle/Fischer § 263a Rn 11
[519] BT-Drs. 10/318, S. 19
[520] LK – *Tiedemann* § 263a Rn 44

zu unbestimmt sei[521] bzw. zu einer übermäßigen Normativierung der Tathandlungen des § 263a StGB führe.[522] Dafür ermöglicht sie, im Unterschied zur erstgenannten Meinung, eine restriktive Auslegung der „unbefugten" Verwendung von Daten und damit eine Begrenzung des Tatbestandes. Gegenüber der zweiten Auffassung zeichnet sie sich dadurch aus, dass kein Rückgriff auf schwer abgrenzbare „computerspezifische" Vorgänge erforderlich ist und vom Gesetzgeber gezielt inkriminierte Fälle des Bankomatenmissbrauchs erfasst werden. Im Ergebnis verdient diese Meinung daher den Vorzug.

Die 4. Variante stellt einen Auffangtatbestand dar, indem sie „sonstige unbefugte Einwirkungen auf den Ablauf" eines Datenverarbeitungsvorgangs pönalisiert. Darunter sollen alle Hard- und Softwaremanipulationen fallen, die nicht bereits von den ersten drei Varianten erfasst werden[523], wie beispielsweise Manipulationen an der Hardware oder in Bezug auf die Datenausgabe.[524] Nach einer Ansicht[525] ist hier das Merkmal „unbefugt" nicht identisch mit dem in der 3. Variante, sondern bedarf einer Interpretation in Anlehnung an die 1. und 2. Variante. Die Unbefugtheit bedeutet dann, dass als Ergebnis des Datenverarbeitungsvorgangs trotz Eingabe richtiger Daten unrichtige, d.h. nicht der objektiven Realität entsprechende, produziert werden. Aus dem Wortlaut ergibt sich diese Auslegung nicht, allenfalls aus dem Erfordernis der Strukturgleichheit zum Betrugstatbestand.

3.7.3.4 Subjektiver Tatbestand

In subjektiver Hinsicht folgt § 263a StGB dem Aufbau des Betrugstatbestandes. Danach ist neben Eventualvorsatzes in Bezug auf alle Elemente des Tatbestandes die Absicht des Täters erforderlich, sich oder einem anderen einen rechtswidrigen Vermögensvorteil zu verschaffen.

3.7.3.5 Ergebnis zu § 263a StGB

§ 263a StGB strebt anders als Art. 8 die Strukturgleichheit zum Betrugstatbestand an, wodurch Schwierigkeiten bei der Bestimmung einer „intellektersetzenden" Täuschungshandlung entstehen. Vor allem in Bezug auf die ersten beiden Handlungsvarianten weist er starke Ähnlichkeit zur Konvention auf, mit dem Unterschied, dass ein Computerbetrug nach nationalem Recht die Verwendung objektiv unrichtiger Daten voraussetzt, wohingegen Art. 8 das „Eingeben, Löschen, usw." beliebiger Daten genügen lässt. Übereinstimmung besteht darüber hinaus in der Schaffung eines Auffangtatbestandes in beiden Tatbeständen, der neben Manipulationen an der Software auch solche an der Hardware erfasst. In subjektiver Hinsicht verlangen beide Normen neben dem allgemeinen Vorsatz das Vorliegen einer besonderen Absicht der Bereicherung.

3.7.4 Bewertung Art. 8

Art. 8 ist wie auch § 263a StGB im Kontext internationaler Bemühungen zur Bekämpfung betrügerischer Handlungen im Zusammenhang mit modernen Technologien zu sehen. So wurden bereits im OECD-Bericht[526] aus dem Jahr 1986, in der Empfehlung Nr. R (89) 9[527]

[521] Achenbach Jura 1991, 225 (228); Hilgendorf JuS 1997, 130 (132)
[522] LK – *Tiedemann* § 263a Rn 44
[523] BT-Drs. 10/5058, S. 30
[524] LK – *Tiedemann* § 263a Rn 62
[525] Lackner/Kühl – *Kühl* § 263a Rn 15; LK – *Tiedemann* § 263a Rn 63; aA: NK – *Kindhäuser* § 263 a Rn 64
[526] OECD, Computer-Related Crime, S. 39
[527] Siehe Fn 491

des Europarats, 1989, sowie durch die „International Association of Penal Law“ (IAPL)[528] Entwürfe einer entsprechenden Norm vorgestellt. Zur legislatorischen Erfassung des „Computerbetrugs“ zeigen die Ansätze in den einzelnen Ländern, dass entweder ein Betrugs- oder ein Diebstahlsmodell in Betracht kommt. Während die Betrugslösungen bei der Definition einer Täuschungshandlung auf Schwierigkeiten treffen, stehen die Diebstahlslösungen vor dem Problem, den Kreis der Tatobjekte auf nichtkörperliche Daten auszudehnen. Im kontinentaleuropäischen Raum hat sich die Orientierung am Betrugstatbestand durchgesetzt, der auch Art. 8 folgt.

[528] Überblick bei: LK – *Tiedemann* § 263a Rn 8 ff.

3.8 Artikel 9 – Straftaten in Bezug auf Kinderpornografie[529]

(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um die folgenden Handlungen, wenn sie vorsätzlich und unbefugt begangen werden, als Straftaten nach ihrem innerstaatlichen Recht festzulegen:

a) das Herstellen von Kinderpornografie zum Zweck ihrer Verbreitung über ein Computersystem;
b) das Anbieten oder Zugänglichmachen von Kinderpornografie über ein Computersystem;
c) das Verbreiten oder Übertragen von Kinderpornografie über ein Computersystem;
d) das Beschaffen von Kinderpornografie über ein Computersystem für sich selbst oder einen anderen;
e) den Besitz von Kinderpornografie in einem Computersystem oder auf einem Computerdatenträger.

(2) Im Sinne von Absatz 1 umfasst „Kinderpornografie" pornografisches Material mit der visuellen Darstellung

a) einer minderjährigen Person bei sexuell eindeutigen Handlungen;
b) einer Person, die als eine minderjährige Person bei sexuell eindeutigen Handlungen erscheint;
c) realistischer Bilder, die eine minderjährige Person bei sexuell eindeutigen Handlungen zeigen.

(3) Im Sinne von Absatz 2 umfasst der Ausdruck „minderjährige Person" alle Personen unter 18 Jahren. Eine Vertragspartei kann jedoch eine niedrigere Altersgrenze vorsehen, wobei 16 Jahre nicht unterschritten werden dürfen.

(4) Jede Vertragspartei kann sich das Recht vorbehalten, die Absätze 1 Buchstaben d und e sowie 2 Buchstaben b und c ganz oder teilweise nicht anzuwenden.

3.8.1 Anwendungsbereich

Art. 9 stellt die einzige inhaltsbezogene Strafnorm der Konvention dar. Die Sanktionierung anderer rechtswidriger Inhalte, etwa rassistischer Propaganda, war vom Sachverständigenausschuss PC-CY (siehe Kapitel 1.3) erörtert worden, scheiterte zunächst jedoch an den Bedenken einiger Delegationen in Bezug auf das Recht der freien Meinungsäußerung. Es dauerte nach der Verabschiedung der Konvention durch das Ministerkomitee noch etwa ein Jahr bis das erste Zusatzprotokoll zur Bekämpfung fremdenfeindlicher Inhalte im Zusammenhang mit Computersystemen, vor allem dem Internet, beschlossen wurde (siehe dazu Kapitel 1.3).

Art. 9 dient ausweislich der Erläuterungen nicht dem Schutz potentieller Konsumenten vor kinderpornografischem Material, sondern dem der kindlichen Darsteller vor sexueller Ausbeutung. Abs. 2 lit. a) stellt dabei unmittelbar auf die Bewahrung Minderjähriger vor sexuellen Handlungen an ihnen ab; Lit. b) und c), die keine Minderjährigkeit oder reale Darstellungen verlangen, dienen mittelbar demselben Zweck, indem sie sich gegen die einschlägige „Szene" wenden bzw. die Ermutigung oder Verführung von Kindern zu entsprechenden Handlungen unterbinden. Der Tatbestand ist dabei auf Handlungen im Zusammenhang mit einem Computersystem beschränkt. Das Hauptaugenmerk gilt freilich nicht dem Einzelplatzrechner ohne Netzwerkanschluss, sondern dem Medium Internet, dass sich als einer der Hauptvertriebswege in den letzten Jahren etabliert hat.[530] Art. 9 ist Teil einer internationalen Initiative zur Bekämpfung von Kinderpornografie, die bereits in einem Aktionsplan des Europarats[531], in dem kürzlich verabschiedeten Fakultativprotokoll zur UN-Kinderrechtskonven-

[529] ER Ziff. 91-106
[530] ER Ziff. 93
[531] 2. Gipfel der Staats- und Regierungschefs des Europarats zum Thema Kinderpornografie, Straßburg, 10.-11. Oktober 1997, http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Fight_against_sexual_exploitation_of_children/Introduction.asp (01.03.2004)

tion[532] sowie im EU-Kommissionsvorschlag für einen Rahmenbeschluss zur Bekämpfung der sexuellen Ausbeutung von Kindern und Kinderpornografie[533] Ausdruck gefunden hat.

3.8.2 Tatbestand

Der Tatbestand beschreibt in Abs. 1 lit. a) bis e) zunächst sieben verschiedene Tathandlungen in Bezug auf kinderpornografische Materialien und Computersysteme. Im Anschluss daran geben die Abs. 2 und 3 Legaldefinitionen für die Begriffe „Kinderpornografie" und „minderjährige Person".

„Kinderpornografie" umfasst nach Abs. 2 sichtbare Darstellungen einer minderjährigen Person bei sexuell eindeutigen Handlungen, lit. a), einer Person, die lediglich als minderjährig erscheint bei sexuell eindeutigen Handlungen, lit. b), sowie von Bildern, die, obwohl sie als „real" erscheinen, in Wirklichkeit kein Kind bei sexuell eindeutigen Handlungen zeigen, lit. c). Dieses letztgenannte Szenario schließt Darstellungen realer Personen, die – etwa durch Morphen[534] – verändert wurden, sowie vollständig vom Computer generierte Bilder ein. Sichtbare Darstellung sind auch Daten auf einer Computerdiskette oder einem sonstigen Datenträger, wenn aus ihnen ein visuell wahrnehmbares Bild erstellt werden kann. Eine Schlüsselrolle kommt dem Begriff der „sexuell eindeutigen Handlung" zu, der im Tatbestand nicht definiert wurde. Den Erläuterungen zufolge sollen sie zumindest vorliegen bei Geschlechtsverkehr, einschließlich genital-genital-, oral-genital-, anal-genital- oder oral-anal-Verkehr, zwischen Minderjährigen oder zwischen einem Erwachsenem und einem Minderjährigen desgleichen oder anderen Geschlechts, Brutalitäten, Masturbation, sadistischem oder masochistischem Missbrauch in einem sexuellen Zusammenhang oder lüsterner Zurschaustellung der Genitalien oder des Schambereichs eines Minderjährigen. Es spielt keine Rolle, ob das dargestellte Verhalten real oder nur vorgetäuscht ist. Dabei obliegt es den Unterzeichnerstaaten, derartige Darstellungen entsprechend ihrem Rechtsempfinden als obszön, unvereinbar mit öffentlichen Moralvorstellungen oder sonst nicht akzeptabel zu klassifizieren. Künstlerische, medizinische, wissenschaftliche oder ähnliche Aspekte verdienen in diesem Zusammenhang eine besondere Berücksichtigung.

„Minderjährig" ist nach Abs. 3, wer das 18. Lebensjahr noch nicht vollendet hat. Diese Altersgrenze wurde in Übereinstimmung mit Art. 1 der UN-Kinderrechtskonvention zum Zwecke internationaler Harmonisierung festgelegt. Es handelt sich nicht um das Mindestalter, ab dem Kinder von ihrem Recht auf sexuelle Selbstbestimmung Gebrauch machen können, sondern um eine Altersgrenze, unter der sie vor sexueller Ausbeutung geschützt werden sollen. Abs. 3 Satz 2 erlaubt die Festsetzung einer niedrigeren Altersgrenze, sofern diese 16 Jahre nicht unterschreitet.

3.8.3 Tathandlungen

Abs. 1 differenziert zwischen sieben Handlungsvarianten, die sich teilweise überschneiden, um einen lückenlosen Schutz zu gewährleisten.

[532] „Optional Protocol to the UN Convention on the rights of the child, on the sale of children, child prostitution and child pornography"; Online: http://www.unicef.org/crc/crc.htm (01.04.2004)

[533] KOM 2000/854, Abl. EG 2001/C 62 E/25, S. 327 ff.

[534] Ausdruck aus der digitalen Bildbearbeitung, der auf den griechischen Begriff „Metamorphose" zurückgeht. Dabei erzeugt der Computer zwischen einem Start- und einem Endbild eine Sequenz sich allmählich verändernder Bilder, die dann in einer Animation eine „Veränderung" des einen in das andere Bild zeigen.

Abs. 1 lit. a) pönalisiert das „Herstellen“ von Kinderpornografie im Sinne einer Vorbereitungshandlung zum Zweck ihrer Verbreitung über ein Computersystem. Nach Abs. 1 lit. b) ist das „Anbieten“ oder „Zugänglichmachen“ von Kinderpornografie über ein Computersystem strafbar. Dadurch sollen Dritte zum einen davon abgehalten werden, derartige Materialien von Personen zu erlangen, die sie auch tatsächlich beschaffen können. Zum anderen soll das Plazieren im Internet unterbunden werden – einschließlich des Setzens und Sammelns von Hyperlinks –, damit derartige Darstellungen nicht zur Erstellung von Kinderpornografie-Seiten im WWW benutzt werden können. Abs. 1 lit. c) stellt das „Verbreiten“ oder „Übertragen“ von Kinderpornografie über ein Computersystem unter Strafe. Unter „Verbreiten“ ist eine aktive Weitergabe zu verstehen. „Übertragen“ erfasst das Versenden von einem Computer zum nächsten. „Beschaffen für sich selbst oder einen anderen“ in Abs. 1 lit. d) bedeutet das aktive Erwerben von Kinderpornografie, beispielsweise durch Herunterladen. Der „Besitz“ von Kinderpornografie in einem Computersystem oder auf einem Datenträger, wie einer Diskette oder einer CD-Rom, wird von Abs. 1 lit. e) pönalisiert.

3.8.4 Unbefugt

Nach Auffassung der Verfasser der Konvention soll das Merkmal „unbefugt“ auf die besondere Bedeutung der Freiheitsrechte, wie dem Recht auf freie Meinungsäußerung und dem Recht auf Schutz der Privatsphäre, im Zusammenhang mit Pornografie hinweisen.[535] Darstellungen, die künstlerischen, medizinischen, wissenschaftlichen oder ähnlichen Zwecken dienen, können an dieser Stelle aus dem Tatbestand ausgeschieden werden. Ebenso können sich aus diesen Erwägungen Rechtfertigungs- bzw. Entschuldigungsgründe ergeben.[536] Den Vertragsparteien steht es auch frei, als objektive Bedingung der Strafbarkeit die tatsächliche Minderjährigkeit der abgebildeten Person vorzusehen.[537]

3.8.5 Subjektiver Tatbestand

In subjektiver Hinsicht ist Vorsatz erforderlich. An dieser Stelle schlägt der Erläuternde Bericht die Schaffung einer abgestuften Providerverantwortlichkeit durch die Aufnahme besonderer subjektiver Elemente vor.[538] Die bloße Vermittlung des Zugangs zu internationalen Computernetzen oder das Bereithalten fremder Inhalte stellt nach dieser Ansicht kein vorsätzliches „anbieten“, „zugänglich machen“, usw. kinderpornografischen Materials dar. Es soll insofern keine Rechtspflicht konstituiert werden, das Verhalten Dritter zu überwachen.[539]

3.8.6 Abs. 4 – Vorbehalt

Abs. 4 erlaubt den Vertragsparteien Vorbehalte hinsichtlich der Abs. 1 lit. d) und lit. e) sowie Abs. 2 lit. b) und lit. c). Das Recht, diese Absätze nicht anzuwenden, kann in Bezug auf alle oder einzelne in Anspruch genommen werden. Jeder dieser Vorbehalte muss gegenüber dem Generalsekretär des Europarats zum Zeitpunkt der Unterzeichnung oder der Hinterlegung der Ratifikations-, Annahme-, Genehmigungs- oder Beitrittsurkunde durch die Vertragsparteien gemäß Art. 42 erklärt werden.

[535] ER Ziff. 103
[536] ER Ziff. 103
[537] ER Ziff. 103
[538] ER Ziff. 105
[539] ER Ziff. 105

3.8.7 Vergleichbare Tatbestände im deutschen Strafrecht

Das Sexualstrafrecht im Dreizehnten Abschnitt des StGB ist durch das „Gesetz zur Änderung der Vorschriften über die Straftaten gegen die sexuelle Selbstbestimmung und zur Änderung anderer Vorschriften“[540] vom 27.12.2003 mit Wirkung zum 01.04.2004 grundlegend geändert worden. In Bezug auf die Verbreitung einschlägiger Schriften ist von der Novellierung vor allem die sog. „harte“ Pornografie betroffen. § 184 Abs. 2 StGB a.F. wurde zu diesem Zweck geändert und die Abs. 3-7 a.F. sind weggefallen. Neu geschaffen wurden dafür die §§ 184a und 184b StGB. Die erstgenannte Vorschrift bezieht sich auf Gewalt- und Tierpornografie; die zweitgenannte auf Kinderpornografie. Im Bereich der sog. „einfachen/weichen“ Pornografie – existiert seit der Änderung des § 184 StGB durch das 4. StRG kein absolutes Verbreitungsverbot mehr, woran sich auch in der Neufassung des § 184 Abs. 1 und 2 StGB nichts geändert hat. Mit § 184c StGB n.F. wurde eine dem § 184 Abs. 2 StGB a.F. entsprechende Norm geschaffen, die zusätzlich zum Rundfunk die Verbreitungswege „Medien- und Teledienste“ erfasst. Für einen Vergleich zu Art. 9 sind allein die §§ 184b und 184c StGB von Bedeutung und sollen daher im Folgenden näher betrachtet werden.

Darüber hinaus enthält das kürzlich novellierte Jugendschutzrecht[541] mit § 23 JMStV eine Strafnorm im Bereich des Jugendmedienschutzes, deren Einschlägigkeit für die Umsetzung von Art. 9 untersucht werden soll.

3.8.7.1 § 184b StGB n.F. – Verbreitung, Erwerb und Besitz kinderpornografischer Schriften

Bis 31.03.2004 stellte § 184 StGB a.F. den Grundtatbestand in Bezug auf „pornographische Schriften“ jeglicher Art dar. Aufgrund mannigfaltiger Änderungen war der Schutzzweck der Vorschrift uneinheitlich. Ursprünglich diente sie nur der Bewahrung der Öffentlichkeit vor „unzüchtigen Veröffentlichungen“, um ungewollte Konfrontationen mit pornografischem Material zu vermeiden.[542] Wenig später wurde der Jugendschutz im Sinne eines Konsumentenschutzes tatbestandlich verankert. Weitere 70 Jahre danach brachte das 4. StRG vom 23.11.1973[543] durch Einfügung eines Abs. 3 eine Differenzierung in die sog. „harte“ und „einfache“ Pornografie. Als zusätzliche Rechtsgüter wurden der Schutz vor Gewalttätern, Pädophilen und Sodomiten sowie der Schutz Heranwachsender und junger Erwachsener in ihrer Entwicklung in die Norm aufgenommen.[544] Das 27. StÄG[545] vom 23.07.1993 änderte u.a. Abs. 4 und 5 und integrierte als weiteres Rechtsgut den Schutz der kindlichen Darsteller pornografischer Darstellungen.[546] Aus diesem Grund wurde die für Pornografiedelikte an sich fremde Voraussetzung des „tatsächlichen“ Geschehens in den Tatbestand aufgenommen und später durch das IuKDG[547] um das Merkmal „wirklichkeitsnah“ ergänzt. Um der Verbreitung von kinderpornographischen Materialien nachhaltiger als bisher mit den Mitteln des Strafrechts begegnen zu können[548], löste § 184b StGB mit Wirkung zum 01.04.2004[549] § 184 Abs.

[540] BGBl. 2003 I, S. 3007
[541] Nachweise im folgenden Kapitel 3.8.7.3
[542] Schroeder NJW 1993, 2581 (2581)
[543] BGBl. 1973 I, S. 1725
[544] LK – *Laufhütte* § 184 Rn 2; Schroeder NJW 1993, 2581 (2581)
[545] BGBl. 1993 I, S. 1346
[546] Eingehend zum Ganzen: Schroeder NJW 1993, 2581 ff.; ders. JZ 1999, 827 ff.; ders., Pornographie, Jugendschutz und Kunstfreiheit, S. 1 ff.
[547] Informations- und Kommunikationsdienste Gesetz; BGBl. 1997 I, S. 1870 ff.; siehe dazu Kapitel 2.3.1.2
[548] BMJ, Pressemitteilung Nr. 106/3, S. 4
[549] „Gesetz zur Änderung der Vorschriften über die Straftaten der sexuellen Selbstbestimmung und zur Änderung anderer Vorschriften“, siehe Fn 540

3-5, 6 Satz 3 sowie Abs. 7 a.F. in Bezug auf Kinderpornografie ab.[550] Da sich die Änderung darüber hinaus im Wesentlichen in der Anhebung des Strafrahmens für einzelne Tatvarianten erschöpfen, blieb der Schutzzweck unverändert, so dass § 184b StGB n.F., wie vorher § 184 Abs. 3-5 StGB a.F., Kinder sowohl als Darsteller als auch als Konsumenten kinderpornographischer Darstellungen schützt.

3.8.7.1.1 Tatbestand

§ 184b StGB n.F. sanktioniert – wie zuvor § 184 Abs. 3-5 StGB a.F. – das „Verbreiten", „öffentliche Ausstellen", usw. einschlägiger „Schriften". Wegen des Verweises auf § 11 Abs. 3 StGB stehen den Schriften „Ton- und Bildträger, Datenspeicher, Abbildungen und andere Darstellungen" gleich. Der eigentliche Oberbegriff ist nicht Schriften, sondern „Darstellungen".[551] Dabei handelt es sich um körperliche Gebilde von gewisser Dauer, die, sinnlich wahrnehmbar, eine Vorstellung oder einen Gedanken ausdrücken.[552] „Datenspeicher" wurden durch Art. 4 Nr. 1 IuKDG[553] vom 22.07.1997 eingefügt. Den Gesetzesmaterialien[554] zufolge handelt es ich dabei um Vorrichtungen, die durch elektronische, elektromagnetische, optische, chemische oder sonstige Verfahren gedankliche Inhalte verkörpern. Die Dauerhaftigkeit der Speicherung soll nicht entscheidend sein, so dass sowohl der flüchtige Arbeitsspeicher (RAM) als auch stromunabhängige Datenträger (z.B. Festplatte, Diskette, CD usw.) erfasst werden.[555] Andererseits lehnt die Gesetzesbegründung die Erfassung von Echtzeit-(Live) Übertragungen ab, selbst wenn diese eine kurzfristige Zwischenspeicherung erfordern.[556]

Für Datenübertragungen in Computernetzen hatte dies zur Folge, dass die Handlungsvariante „Verbreiten"[557] mangels eines körperlichen Substanztransfers, den die höchstgerichtliche Rechtsprechung[558] bislang verlangte, abgelehnt wurde. Sowohl beim Hoch- als auch beim Herunterladen einer Datei werden lediglich unkörperliche Informationen, keine stofflichen Datenspeicher im Sinne der oben dargestellten Definition ausgetauscht. Der BGH hat diese Rechtsprechung in einer Entscheidung vom 27.06.2001[559] unter zweifelhafter Auslegung des „Datenspeicher"-Begriffs aufgegeben. In den Urteilsgründen führt das Gericht dazu aus: „Digitalisierte Bilder, die ins Internet gestellt werden, sind Datenspeicher in diesem Sinne [im Sinne von § 11 Abs. 3 StGB, *Anm. des Verf.*]; genauer: auf einem Speichermedium – in der Regel der Festplatte des Servers – gespeicherte Daten."[560] Dabei übersieht der BGH, dass digitalisierte Bilder eben keine körperlichen Gebilde im Sinne der oben genannten Definition sind, sondern allein die Festplatte des Servers dieses Kriterium erfüllt. Freilich kann dieser physikalische Datenträger nicht mittels elektrischer Signale an einen anderen Computer übertragen werden, so dass eine Bestrafung wegen Verbreitung pornografischer Darstellungen nach § 184 StGB a.F. an dem engen strafrechtlichen Schriftenbegriff gescheitert wäre.[561]

---

[550] Regierungsentwurf BT-Drs. 15/350, S. 50
[551] RegE IuKDG BT-Drs. 13/7385, S. 36; Lackner/Kühl – *Lackner* § 11 Rn 28; Sch/Sch – *Eser* § 11 Rn 78; Tröndle/Fischer § 11 Rn 33
[552] BT-Drs. 13/7385, S. 36; Sieber JZ 1996, 494, (495); Sch/Sch – *Eser* § 11 Rn. 78; Tröndle/Fischer § 11 Rn 33; Walter NStZ 1990, 523 (523) mwN
[553] Siehe Kapitel 2.3.1.2, Fn 211
[554] BT-Drs. 13/7385, S. 36
[555] BT-Drs. 13/7385, S. 36
[556] BT-Drs. 13/7385, S. 36
[557] Dazu im Folgenden, Kapitel 3.8.7.1.2
[558] BGHSt 18, 63 (64) = NJW 1963, 60; BGH NJW 1999, 1979 (1980)
[559] BGHSt 47, 55 = MMR 2001, 676 = ZUM 2002, 283 mit krit. Anm. von Gercke
[560] BGHSt 47, 55 (58)
[561] Ebenso: Bornemann NJW 2003, 787 (788) sowie Liesching NJW 2002, 3281 (3283)

Diese Erweiterung des „Datenspeicher"-Begriffs durch den BGH ist abzulehnen, da sie dazu führt, dass entweder die flüchtige Bildschirmanzeige als körperlicher Gegenstand[562] betrachtet oder dass das Körperlichkeitskriterium des „Datenspeicher"-Begriffs[563] aufgegeben werden muss.[564] Die erstgenannte Schlussfolgerung widerspricht der technischen Realität und die zweitgenannte den Gesetzesmaterialien zu § 11 Abs. 3 StGB.[565] Darüber hinaus droht die Unterscheidung der Handlungsvarianten „Verbreiten" und „Zugänglichmachen", die bislang in einem Substanztransfer bestand[566], ohne ersichtlichen Grund nivelliert zu werden.[567] Die Gleichstellung digitalisierter Bilder mit Datenspeichern im Sinne von § 11 Abs. 3 StGB ist daher abzulehnen.

Ebenso fragwürdig erscheint die Ansicht des OLG Hamburg[568], das Bilddateien zwar nicht als Datenspeicher, sondern als „Darstellungen", die auf „Datenspeichern" festgehalten seien, betrachtet. Umgangsprachlich handelt es sich bei digitalisierten Bildern sicherlich um Darstellungen. Allerdings erfordert der „Darstellungs"-Begriff im Sinne von § 11 Abs. 3 StGB das Vorliegen eines körperlichen Gebildes. Dies trifft sicherlich für Printerzeugnisse zu, bei denen die Darstellung fest mit dem Substrat verbunden ist. Eine flüchtige Bildschirmanzeige erfüllt dieses Kriterium jedoch nicht.[569] Auch die Ansicht des OLG Hamburg ist daher aus vergleichbaren Gründen abzulehnen. Das Gleiche gilt für die Auffassung des OLG Stuttgart, das „Datenträger im Btx-Verfahren", ohne diesen Sachverhalt näher zu erläutern, „Bildträgern" im Sinne von § 11 Abs. 3 StGB a.F. gleichstellt und ein „Verbreiten" dann bejaht, wenn zwar die nicht beschriebenen Datenträger, jedoch die darauf gespeicherten Texte im „Btx-Verfahren" „zur Verbreitung bestimmt sind".[570]

Eine Definition von „Pornografie" bereitet Literatur und Rechtsprechung, ähnlich wie zuvor die Umschreibung des Merkmals „unzüchtig", erhebliche Schwierigkeiten. Da es sich um einen Begriff handelt, der von den jeweiligen gesellschaftlichen und kulturellen Wertvorstellungen einer Epoche abhängt, unterliegt er einem beständigen Wandel. Im Einzelfall entscheidet sich im Rahmen einer nur begrenzt überprüfbaren tatrichterlichen Würdigung, ob die Grenze zur Strafbarkeit überschritten wurde. Dabei ist umstritten, ob den einzelnen Tatbestandsvarianten eine einheitliche Begriffsverwendung zu Grunde liegt.[571] Wegen der dargestellten Schwierigkeiten überhaupt eine Definition zu finden, fällt dieser Streit jedoch nicht weiter ins Gewicht. Bei aller Uneinigkeit über den Pornografiebegriff besteht doch eine Übereinstimmung in Bezug auf zwei Kriterien: Einschlägigen Schriften kommt es überwiegend oder ausschließlich auf die Hervorrufung eines sexuellen Reizes beim Betrachter an (Stimulierungstendenz), wobei die durch die jeweiligen Wertvorstellungen gezogenen Grenzen des sexuellen Anstandes überschritten werden (Anstandsverletzung).[572] Aus dieser subjektivierten Definition wird deutlich, dass die Einordnung letztlich vom jeweiligen Betrachter abhängen wird. Darüber hinaus werden von den einzelnen Autoren zahlreiche weitere Charakteristika diskutiert, wobei vor allem die Abgrenzung zum Kunstbegriff zunehmend Schwierigkeiten

[562] Dagegen: Sieber JZ 1996, 494 (495); Tröndle/Fischer § 11 Rn 36 a sowie Walther NStZ 1990, 523 (523) jeweils mwN
[563] So noch: Sch/Sch – *Eser* § 11 Rn 78
[564] Kritisch daher: Tröndle/Fischer § 11 Rn 36 und 36a
[565] BT-Drs. 13/7385, S. 36
[566] Siehe dazu Kapitel 3.8.7.1.2
[567] Ebenso: Gercke ZUM 2002, 283 (288)
[568] OLG Hamburg NStZ-RR 1999, 329 (329)
[569] Siehe Fn 564
[570] OLG Stuttgart NStZ 1992, 38
[571] Lackner/Kühl – *Kühl* § 184 Rn 8; LK – *Laufhütte* § 184 Rn 13; Sch/Sch – *Lenckner*/*Perron* § 184 Rn 52; SK – *Horn*/*Wolters* (7. Aufl.) § 184 Rn 64; § 184 Rn 34; aA: Mahrenholz ZUM 1998, 525 (526 f.)
[572] BT-Drs. VI/3521, S. 60; Lackner/Kühl – *Kühl* § 184 Rn 2; LK – *Laufhütte* § 184 Rn 4 ff.; Sch/Sch – *Lenckner*/*Perron* § 184 Rn 4; SK – *Horn*/*Wolters* § 184 Rn 4; Tröndle/Fischer § 184 Rn 7 f.

verursacht.[573]

§ 184b StGB n.F. definiert ebenso wenig wie seine Vorgängerregelung, wann ein „sexueller Missbrauch von Kindern" vorliegt. Dazu ist vielmehr ein Rückgriff auf die §§ 176 bis 176b StGB erforderlich, auf die § 184b StGB n.F. mittlerweile verweist. Kinder sind danach Personen, die das 14. Lebensjahr noch nicht vollendet haben, § 176 Abs. 1 StGB n.F. Problematisch an der Bezugnahme ist vor allem der Fall, bei dem der Täter von einem Kind, das an sich selbst sexuelle Handlungen vornimmt, Bilder anfertigt, § 176 Abs. 4 Nr. 2 StGB n.F. (§ 176 Abs. 3 Nr. 2 StGB a.F.). Nach dem insoweit eindeutigen Wortlaut der Vorschrift ist dies nur strafbar, wenn er das Kind zuvor dazu bestimmt hat. Als Konsequenz für § 184b StGB n.F. bedeutet dies, dass pornografische Schriften nur vorliegen, wenn der Vorgang des „Bestimmens" aus dem Bild visuell wahrnehmbar hervorgeht. Es steht außer Frage, dass dies nur in Ausnahmen der Fall sein wird.[574] Nach Auffassung der Rechtsprechung soll es daher genügen, wenn die Darstellung bei einem „verständigen" Betrachter den Schluss zulässt, dass das Opfer zu den Handlungen bestimmt worden sei.[575]

Das im Rahmen von § 176 StGB zentrale Merkmal der „sexuellen Handlung" wird auch nach der Novellierung der Vorschrift nicht legal definiert. § 184f Nr. 1 StGB n.F. (§ 184c StGB a.F.) bringt nur eine Einschränkung, indem er ausgehend von einem vorgegebenen Begriff der sexuellen Handlung, der im Rahmen des 4. StRG an die Stelle der „unzüchtigen Handlung" getreten ist, die strafrechtliche Erheblichkeit am jeweils betroffenen Rechtsgut festmacht. Damit wiederholt die Norm lediglich allgemeine dogmatische und systematische Grundsätze ohne auf die eigentlichen Sachfragen einzugehen.[576] Nach allgemeiner Ansicht in Literatur und Rechtsprechung liegt eine sexuelle Handlung dann vor, wenn in objektiver Hinsicht nach dem äußeren Erscheinungsbild für den verständigen Betrachter ein Sexualbezug erkennbar ist. Ob darüber hinaus noch eine subjektive Absicht des Handelnden erforderlich sein muss, ist umstritten, wird jedoch mehrheitlich verneint.[577]

Abs. 3 n.F. (Abs. 4 a.F.) ist ein Qualifikationstatbestand der Abs. 1 und 2 n.F., wenn die pornografischen Schriften in Bezug auf den sexuellen Missbrauch von Kindern ein „tatsächliches oder wirklichkeitsnahes" Geschehen wiedergeben und der Täter „gewerbsmäßig" oder als „Mitglied einer Bande" handelt. Mit „tatsächlich" ist gemeint, dass die Darstellungen Handlungen wiedergeben müssen, die wie Kinderpornografie aussehen (sog. Realpornografie). Dabei wird es sich vor allem um Foto- und Filmaufnahmen handeln, wohingegen wörtliche Darstellungen und Zeichnungen ausscheiden.[578] Das Merkmal „wirklichkeitsnah", das durch das IuKDG[579] eingefügt wurde, will Geschehensabläufe in computergenerierten Scheinrealitäten erfassen, die nach dem Willen des Herstellers für den Betrachter als solche nicht mehr erkennbar sind.[580] Insofern wird der Strafgrund des „Darstellerschutzes" in Frage gestellt. Mit steigender Rechnerleistung wird der Übergang zwischen „Real- und Fiktivpornografie" zusehends fließender, so dass sich kinderpornografisches Material nicht mehr lediglich auf Foto- und Filmaufnahmen beschränken dürfte. Abs. 4 n.F. (Abs. 5 a.F.) betrifft ebenfalls kinderpor-

[573] BVerfG JZ 1991, 465 ff. mit Anm. Gusy; Lackner/Kühl – *Kühl* § 184 Rn 3; Sch/Sch – *Lenckner*/*Perron* § 184 Rn 5a; SK – *Horn*/*Wolters* § 184 Rn 6 ff.
[574] Sch/Sch – *Lenckner*/*Perron* § 184 Rn 55; SK – *Horn*/*Wolters* § 184 Rn 66
[575] BGH 43, 366 (368); 45, 41 (42), 47, 55 (61 f.); OLG Koblenz NJW 1979, 1467 (1468); differenzierend: SK – *Horn*/*Wolters* § 184 Rn 66
[576] Sch/Sch – *Lenckner/Perron* § 184c Rn 1, 4; Tröndle/Fischer § 184c Rn 5
[577] BGH NJW 1992, 325; BGH NStZ 1985, 24; Lackner/Kühl – *Kühl* § 184c Rn 2 ff.; Sch/Sch – *Lenckner*/*Perron* § 184c Rn 5 ff.; Tröndle/Fischer § 184c Rn 4
[578] Lackner/Kühl – *Kühl* § 184 Rn 8a; Sch/Sch – *Lenckner/Perron* § 184 Rn 61
[579] Siehe Fn 211
[580] Sch/Sch – *Lenckner/Perron* § 184 Rn 61; SK – *Horn*/*Wolters* § 184 Rn 76; Tröndle/Fischer § 184 Rn 48

nografisches Material, das ein „tatsächliches oder wirklichkeitsnahes“ Geschehen wiedergibt.

3.8.7.1.2 Tathandlungen

Die Tathandlungen des § 184b StGB n.F. entsprechen denen der Vorgängerregelung (§ 184 Abs. 3-5 StGB a.F.). „Verbreiten“ erforderte nach der früher herrschenden Meinung eine körperliche Weitergabe.[581] Nach geänderter höchstrichterlicher Rechtsprechung genügt für die Verbreitung von Schriften im Internet nunmehr ein Bereitstellen zum Abruf oder ein Versenden beispielsweise per Email. Auf eine Substanzweitergabe kommt es nicht mehr an.[582]

„Öffentlich Ausstellen“, „Anschlagen“ und „Vorführen“ sind, wie sich aus dem Wort „oder“ ergibt, eine beispielhafte Aufzählung unter dem Oberbegriff des „Zugänglichmachens“, Abs. 1 Nr. 2 n.F. (Abs. 3 Nr. 2 a.F.). Hierbei genügt es, dass sich ein anderer vom Inhalt der Schriften durch sinnliche Wahrnehmung Kenntnis verschaffen kann. Auf einen Substanztransfer kommt es nicht an. Es genügt daher auch ein Bereitstellen von digitalen Bildern und Filmen auf einem Server zum Herunterladen durch Benutzer.[583] Abs. 1 Nr. 3 n.F. (Abs. 3 Nr. 3 a.F.) zählt bestimmte Vorbereitungshandlungen zu Taten nach Abs. 1 Nr. 1, 2 n.F. (Abs. 3 Nr. 1, 2 a.F.) auf, die in Bezug auf die Absicht im Sinne von zielgerichtetem Handeln vorliegen müssen. „Herstellen“ betrifft alle menschlichen Handlungen bei der Anfertigung pornografischer Schriften, usw. Zeitlich im Anschluss knüpft das „Vorrätighalten“ im Sinne eines Bereithaltens zur Abgabe an. „Anbieten“, „Ankündigen“ und „Anpreisen“ betreffen alle Vorgänge zur Bewerbung pornografischen Materials. „Liefern“ bedeutet, dass die Sache zur eigenen Verfügungsgewalt des Bestellers übergeben wird. Spiegelbildlich steht das „Beziehen“ durch den Konsumenten gegenüber. „Einführen“ und „Ausführen“ betrifft die Vorgänge des Verbringens über eine Grenze. Wie bei § 184 Abs. 1 Nr. 9 StGB a.F. wurde diese Variante wegen außenpolitischer Gründe für erforderlich gehalten.[584] Insgesamt ist eine möglichst lückenlose Sanktionierung vom Produzenten bis zum Konsumenten bezweckt.[585]

Abs. 2 und Abs. 4 S. 1 n.F. (Abs. 5 S. 1 a.F.) sanktionieren das „Unternehmen“ (§ 11 Abs. 1 Nr. 6 StGB) des „Verschaffens des Besitzes“ (Abs. 4 S. 1 n.F.) sowie den „Besitz“ (Abs. 4 S. 2 n.F.) kinderpornografischer Schriften. Umstritten ist, ob das Merkmal des „Besitzverschaffens“ wie bei § 29 Abs. 1 Nr. 3 BtMG[586] oder in Anlehnung an den Hehlereitatbestand[587], § 259 StGB, auszulegen ist. Die praktische Auswirkung dieses Meinungsstreits besteht darin, dass das „sich oder einem Dritten“ verschaffen im Hehlereitatbestand ein einverständliches Zusammenwirken („[…] ankauft oder sonst sich oder einem Dritten verschafft […]“, § 259 StGB) von Vor- und Hehlereitäter voraussetzt. Eine derartige Einschränkung aus dogmatischen Gründen ist bei § 184b Abs. 2 und 4 StGB n.F. nicht geboten. Den Besitz verschafft sich, wer ein tatsächliches Herrschaftsverhältnis durch ein Erwerbs- oder Gebrauchsüberlassungsgeschäft im zivilrechtlichen Sinne begründet. Daneben hat das Dauerdelikt des Besit-

[581] BGHSt 18, 63 (64); BGH NJW 1963, 60; BGH NJW 1977, 1695 (1695); Lackner/Kühl – *Kühl* § 184 Rn 5; Sch/Sch – *Lenckner/Perron* § 184 Rn 57

[582] BGHSt 47, 55 (59) = MMR 2001, 676 ff., mit ablehnender Anm. Gercke; ders. ZUM 2002, 283 (285 f.); Siehe bereits Kapitel 3.8.7.1.1, im Zusammenhang mit dem strafrechtlichen Begriff der Schriften in § 11 Abs. 3 StGB

[583] Gercke ZUM 2002, 283 (288); Lackner/Kühl – *Kühl* § 184 Rn 5; Sch/Sch – *Lenckner/Perron* § 184 Rn 58, 15; SK – *Horn/Wolters* § 184 Rn 71, 16, 6d ff

[584] LK – *Laufhütte* § 184 Rn 1

[585] Lackner/Kühl – *Kühl* § 184 Rn 5; Sch/Sch – *Lenckner/Perron* § 184 Rn 57 ff.; Tröndle/Fischer Rn § 184 Rn 31 ff.

[586] BT-Drs. 12/3001, S. 6; Lackner/Kühl – *Kühl* § 184 Rn 8b

[587] Schroeder NJW 1993, 2581 (2583)

zens nur noch in Ausnahmefällen eigenständige Bedeutung.[588]

3.8.7.1.3 Vorsatz

Es genügt grundsätzlich bedingter Vorsatz, vor allem in Bezug auf den pornografischen Charakter der Schriften sowie auf die Darstellung eines „wirklichkeitsnahen" Geschehens. Hierzu ist eine Parallelwertung in der Laiensphäre ausreichend.[589] Abs. 1 Nr. 3 n.F. (Abs. 3 Nr. 3 a.F.) erfordert darüber hinaus die Absicht, das pornografische Material zu verwenden.[590]

3.8.7.1.4 Ergebnis zu § 184b n.F. StGB

In Bezug auf die geschützten Rechtsgüter erscheinen vor allem § 184b Abs. 3 und 4 (§ 184 Abs. 4 und 5 StGB a.F.) StGB n.F. mit Art. 9 vergleichbar, die auf ein „tatsächliches oder wirklichkeitsnahes Geschehen" abstellen und dadurch verdeutlichen, dass es vorrangig nicht auf die Bewahrung der Konsumenten vor der Konfrontation mit einschlägigem Material, sondern auf den Schutz der kindlichen Darsteller ankommt.

Erhebliche Unterschiede bestehen in Bezug auf die Tatobjekte in Art. 9 und § 184b StGB n.F. Während die Konvention „visuelle Darstellungen" einschlägigen Materials genügen lässt, ist die Strafnorm des StGB auf „Schriften" im Sinne von § 11 Abs. 3 StGB beschränkt. Vor allem die deutsche Rechtsprechung hat erhebliche Probleme damit, unter welchen Voraussetzungen die Übertragung von digitalisierten Bildern und Filmen im Internet ein „Verbreiten" von „Schriften" darstellen kann. Die Änderung der Rechtsprechung in BGH 47, 55 stößt daher zu Recht auf erhebliche Kritik.

Inhaltlich besteht ein wesentlicher Unterschied beider Tatbestände jedoch in der Altersgrenze in Bezug auf Kindesmissbrauch. Während § 184b StGB n.F., der auf die §§ 176 bis 176b StGB n.F. Bezug nimmt, von 14 Jahren ausgeht, bejaht Art. 9 Abs. 2 die Schutzwürdigkeit „minderjähriger Personen" grundsätzlich bis zu einem Alter von 18 Jahren, dass die Unterzeichnerstaaten nach Art. 9 Abs. 2 Satz 2 optional bis auf 16 Jahre absenken können.

3.8.7.2 § 184c StGB n.F. – Verbreitung pornografischer Darbietungen durch Rundfunk, Medien- oder Teledienste

§ 184c StGB n.F. knüpft an den bisherigen § 184 Abs. 2 StGB a.F. an. Die neue Regelung unterscheidet sich von der alten im Wesentlichen dadurch, dass neben dem Rundfunk nunmehr auch Medien- und Teledienste als Verbreitungskanäle pornografischer „Darbietungen" – nicht „Darstellungen" – erfasst werden sowie durch eine Anhebung des Strafmasses. Zu Klarstellungszwecken wurde Satz 2 eingefügt, der eine Verbreitung „einfacher" Pornografie aus dem Anwendungsbereich von § 184 Abs. 1 Satz StGB n.F. herausnimmt, sofern sichergestellt ist, dass sie Kindern und Jugendlichen nicht zugänglich ist. Dieses Ergebnis wurde bislang von einigen Autoren durch eine teleologische Reduktion des § 184 Abs. 2 StGB a.F. erzielt.[591]

---

[588] Schroeder NJW 1993, 2581 (2583); Sch/Sch – *Lenckner/Perron* § 184 Rn 65
[589] Sch/Sch – *Lenckner/Perron* § 184 Rn 66
[590] Lackner/Kühl – *Kühl* § 184 Rn 9; Sch/Sch – *Lenckner/Perron* § 184 Rn 66; SK – *Horn*/*Wolters* § 184 Rn 73; Tröndle/Fischer § 184 Rn 56
[591] Etwa Sch/Sch – *Lenckner/Perron* § 184 Rn 51

Bei der Übertragung vom Daten im Internet soll sich aufgrund der Gesetzesmaterialien folgender Anwendungsbereich für § 184c StGB n.F. ergeben:

Wie zuvor § 184 Abs. 2 StGB a.F.[592] sei auch § 184c StGB n.F. auf „Live"-Angebote beschränkt.[593] Darbietungen, bei denen eine Speicherung erfolgt, fielen unter den „Schriften"-Begriff des § 11 Abs. 3 StGB Sie würden daher – bei entsprechendem Inhalt – von § 184b StGB n.F. erfasst werden.[594] § 184c StGB n.F. dürfte daher in erster Linie zur Anwendung kommen, wenn Darbietungen per Kamera, die an einen Computer angeschlossen ist (engl. *web cam*), übertragen werden. Die dazu technisch erforderliche Zwischenspeicherung (sog. *Caching*) stelle nach der Begründung zu Art. 4 Nr. 1 IuKDG[595], durch den § 11 Abs. 3 StGB erweitert wurde, gerade keine ausreichend lange Manifestierung dar, um von einer Schrift im strafrechtlichen Sinne ausgehen zu können.[596] Jedoch heißt es an der gleichen Stelle in den Gesetzesmaterialien auch, dass selbst der flüchtige Arbeitsspeicher eines Computers als „Datenspeicher" im Sinne von § 11 Abs. 3 StGB gelte, weil es auf die Dauerhaftigkeit der Speicherung nicht ankomme.[597] An dieser Stelle zeigt sich die bereits dargestellte Widersprüchlichkeit des strafrechtlichen „Schriften"-Begriffs.[598]

Strafbarkeitslücken drohen dort, wo sog. „Streaming Media"[599] Angebote zeitverzögert, d.h. nicht „live" im Sinne von § 184c StGB n.F., übertragen werden. Solange derartige Materialien auf dem Computer des Konsumenten nur „*gecached*" (zwischengespeichert) werden, was der technischen Realität entspricht[600], liegen weder „Schriften" im Sinne von §§ 184b StGB n.F. iVm § 11 Abs. 3 StGB[601] noch „Darbietungen" im Sinne von § 184c StGB n.F. vor.[602] Allenfalls beim Anbieter derartiger Angebote kann ein „Zugänglichmachen" bejaht werden. Befindet sich dieser – wie im Regelfall – im Ausland, stellt sich die Frage, ob inländisches Strafrecht zur Anwendung kommt.

3.8.7.3 Strafnormen im Jugendschutzrecht

Das Jugendschutzrecht ist mit Wirkung zum 01.04.2003 grundlegend reformiert worden. An die Stelle des Gesetzes zum Schutze der Jugend in der Öffentlichkeit (JÖSchG)[603] und des Gesetzes über die Verbreitung jugendgefährdender Schriften und Medieninhalte (GjSM)[604] treten nun das Jugendschutzgesetz (JuSchG)[605]des Bundes und der Jugendmedienschutz-

[592] Lackner/Kühl – *Kühl* § 184 Rn 7; Sch/Sch – *Lenckner/Perron* § 184 Rn 51; Tröndle/Fischer § 184 Rn 22
[593] RegE BT-Drs. 15/350, S. 52
[594] RegE BT-Drs. 15/350, S. 52
[595] Siehe Fn 211
[596] BT-Drs. 13/7385, S. 36
[597] BT-Drs. 13/7385, S. 36
[598] Siehe Kapitel 3.8.7.1.1
[599] Engl *Streaming* = Dt. Strömen; In Bezug auf Computer wird damit eine Technologie beschrieben, die es erlaubt, Video- und Audiodaten so aufzubereiten, dass Echtzeit-Audio- und Videoempfang in Computernetzen möglich wird. Ein Teil der Daten wird zunächst zwischengespeicherte und kann dann bereits während des Herunterladens abgespielt werden (Langenscheidts Internet-Wörterbuch, http://www.networds.de/ (01.04.2004)
[600] Siehe beispielsweise die Dokumentation des T-Online Breitband Portals „T-Online Vision", http://www.t-online-vision.de/c/11/14/87/1114876.html (01.04.2004)
[601] Siehe Fn 596
[602] Siehe Fn 593
[603] BGBl. 1985 I, S. 425 ff.
[604] BGBl. 1985 I, S. 1502 ff.
[605] BGBl. 2002 I, S. 2730 ff.

Staatsvertrag der (JMStV)[606] der Länder. Die Reform sollte wie die vorherigen Neuerungen den „[…] gewandelten Anforderungen eines modernen Kinder- und Jugendschutzes Rechnung tragen […]“.[607] Im Wesentlichen beschränken sich die Änderungen auf den Jugendmedienschutz, so dass große Teile des GjSM und des JÖSchG weitgehend inhaltsgleich übernommen wurden.

Die wesentliche Zielsetzung bei der Neuregelung bestand darin, den Jugendschutz für alle elektronischen Online-Medien im JMStV der Länder zu konzentrieren.[608] Dazu verzichtete der Bund auf Jugendschutzregelungen in Bezug auf Teledienste nach dem TDG, für die er bekanntlich die Gesetzgebungskompetenz beansprucht.[609] Stattdessen wurden die Tele- und die Mediendienste unter dem Begriff der „Telemedien“ nach § 1 Abs. 3 JuSchG zusammengefasst und einheitlich dem Jugendmedienschutz-Staatsvertrag unterworfen.[610] Diese Zusammenfassung ist ebenso wenig gelungen, wie die zuvor erfolgte Aufspaltung in „Teledienste“ nach dem TDG und „Mediendienste“ nach dem MDStV.[611] Dies wird an § 1 Abs. 2 Satz 2 JuSchG deutlich, der dem gegenständlichen Verbreiten gegenständlicher Trägermedien das elektronische Verbreiten gegenständlicher Trägermedien gleichstellt. In der Begründung zum Regierungsentwurf wird hierzu ausgeführt, „[…] dass die unkörperliche elektronische Verbreitung zum Beispiel einer Musik- oder Videokassette oder einer Zeitschrift als Attachement zu einer E-Mail der körperlichen Verbreitung gleichsteht.“[612] Es ist evident, dass weder eine Musik- noch eine Videokassette sich als Anhang einer Email versenden lassen.[613] Übermittelt wird vielmehr der digitalisierte Inhalt, wobei dann kein Träger-, sondern ein Telemedium nach § 1 Abs. 3 JuSchG vorliegt.[614] Aufgrund dieser misslungenen Abgrenzung der Täger- von den Telemedien kann daher – jedenfalls *de lege lata* – keine Rede sein von einer Vereinheitlichung des Jugendmedienschutzes. Vielmehr handelt es sich – anders als *Bornemann*[615] und *Langenfeld*[616] dies sehen – um eine Zielsetzung *de lege ferenda*. Da jedoch der erklärte Wille des Gesetzgebers[617] auf eine derartige Zusammenfassung abzielt, sollte – wie bereits bei § 2 Abs. 2 Nr. 3 TDG – von einem „Redaktionsversehen“[618] ausgegangen werden.

Einschlägig für einen Vergleich zu Art. 9, dessen Hauptaugenmerk dem Verbreitungsweg „Internet“ gilt[619], sind daher die Strafbestimmungen des JMStV in § 23 JMStV. Ergänzend käme § 27 JuSchG für kinderpornografisches Material auf Wechseldatenträgern (= Trägermedien nach § 1 Abs. 2 JuSchG) in Betracht, der wegen des Schwerpunkts der Konvention im Online-Bereich an dieser Stelle nicht näher beleuchtet werden soll.

3.8.7.3.1 § 23 Jugendmedienschutz-Staatsvertrag

Strafbar nach § 23 JMStV ist das „Verbreiten“ und „Zugänglichmachen“ offensichtlich

[606] Staatsvertrag über den Schutz der Menschenwürde und den Jugendschutz in Rundfunk und Telemedien vom 20.11.2002, Nds. GVBl. 2002, S. 706; online: http://www.schure.de/22620/jmstv.htm (01.04.2004)
[607] BT-Drs. 14/9013, S. 13
[608] Bornemann NJW 2003, 787 (787); Langenfeld MMR 2003, 303 (303)
[609] Siehe Kapitel 2.3.1.2
[610] Bornemann NJW 2003, 787 (787); Langenfeld MMR 2003, 303 (303)
[611] Siehe Kapitel 2.3.1.2
[612] BT-Drs. 14/9013, S. 18
[613] So auch: Liesching NJW 2002, 3281 (3283)
[614] Siehe Fn 613
[615] Bornemann NJW 2003, 787
[616] Langenfeld MMR 2003, 303
[617] BT-Drs. 14/9013, S. 13
[618] Siehe Kapitel 2.3.1.2
[619] Siehe Kapitel 3.8.1

schwer jugendgefährdender Angebote (§ 4 Abs. 2 Satz 1 Nr. 3 JMStV) im Rundfunk oder ohne die erforderlichen Sicherheitsmechanismen in Telemedien, § 4 Abs. 2 Satz 2 JMStV. Dabei entspricht der Wortlaut von § 4 Abs. 2 Satz 1 Nr. 3 JMStV weitgehend dem von § 15 Abs. 2 Nr. 5 JuSchG. In der amtlichen Begründung zum JuSchG heißt es dort, dass die Vorschrift dem bisher geltenden § 6 Nr. 3 GjSM entsprechen soll, wobei „[…] die Nummern 1 bis 5 eine für die Praxis hilfreiche exemplarische Erläuterung sind, was als schwer jugendgefährdend zu verstehen ist.“[620] Die Auslegung der offensichtlich schwer jugendgefährdenden Angebote im Sinne des JMStV kann sich daher an den in § 15 Abs. 2 JuSchG aufgezählten Beispielen orientieren. Da § 15 Abs. 2 Nr. 1 JuSchG Bezug nimmt auf § 184 StGB, wird deutlich, dass sich das Jugendschutzrecht in Bezug auf Kinderpornografie am Strafrecht orientiert.

3.8.7.3.2 Ergebnis zu § 23 JMStV

In Übereinstimmung zu Art. 9 erfasst § 23 JMStV als Teilmenge der offensichtlich schwer jugendgefährdenden Angebote kinderpornografische Materialien. Im Gegensatz zur Konvention wird jedoch nur das „Verbreiten“ und „Zugänglichmachen“ pönalisiert. Ein weiterer Unterschied besteht darin, dass § 23 JMStV einschlägige Angebote straflos lässt, solange sie nur einer geschlossenen Benutzergruppe von Erwachsenen zugänglich gemacht werden, § 4 Abs. 2 Satz 2 JMStV. Hinsichtlich des geschützten Rechtsguts unterscheiden sich beide Normen dadurch, dass Art. 9 Kinder sowohl vor der Rolle des Konsumenten als auch der des Darstellers schützen will, während das deutsche Jugendschutzrecht vorrangig auf die Bewahrung vor einer ungewollten Konfrontation mit einschlägigem Material abstellt.

3.8.8 Bewertung Art. 9

Art. 9 sanktioniert nicht die Verbreitung von Pornografie im Allgemeinen, sondern ist auf Darstellungen von Fällen des Kindermissbrauchs, die denen der §§ 176 bis 176b StGB n.F. entsprechen, beschränkt. Vorrangiges Schutzgut ist die Bewahrung der kindlichen Darsteller vor sexueller Ausbeutung. Daneben zielen vor allem Art. 9 Abs. 2 und 3, die nicht auf reale, sondern auf fiktive Kinderpornografie abstellen, auf die Bekämpfung einer einschlägigen Szene der Konsumenten ab. Umsetzungsbedarf besteht einerseits in Bezug auf eine Anhebung der Altersgrenze auf wenigstens 16 Jahre. Anderseits drohen im deutschen Recht Strafbarkeitslücken durch die Beschränkung der einschlägigen Tatbestände auf „Darstellungen“ und „Darbietungen“. Vorzugswürdig ist es hingegen, auf Tatobjekte in Form „visuelle Darstellungen“ abzustellen, um auf diese Weise auch unkörperliche Computerdaten erfassen zu können.

[620] BT-Drs. 14/9013, S. 24

3.9 Artikel 10 – Straftaten in Zusammenhang mit Verletzungen des Urheberrechts und verwandter Schutzrechte[621]

(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um Urheberrechtsverletzungen, wie sie nach dem Recht dieser Vertragspartei aufgrund ihrer Verpflichtungen nach der Pariser Fassung vom 24. Juli 1971 der Berner Übereinkunft zum Schutz von Werken der Literatur und Kunst, dem Übereinkommen über handelsbezogene Aspekte der Rechte des geistigen Eigentums und dem WIPO-Urheberrechtsübereinkommen umschrieben sind, mit Ausnahme der nach diesen Übereinkünften verliehenen Urheberpersönlichkeitsrechte als Straftaten nach ihrem innerstaatlichem Recht festzulegen, wenn diese Handlungen vorsätzlich, in gewerbsmäßigem Umfang und mittels eines Computersystems begangen werden.

(2) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um Verletzungen verwandter Schutzrechte, wie sie nach dem Recht dieser Vertragspartei aufgrund ihrer Verpflichtungen nach dem in Rom unterzeichneten Internationalen Abkommen über den Schutz der ausübenden Künstler, der Hersteller von Tonträgern und der Sendeunternehmen (Abkommen von Rom), dem Übereinkommen über handelsbezogene Aspekte der Rechte des geistigen Eigentums und dem WIPO-Vertrag betreffend Darbietungen und Tonträger umschrieben sind, mit Ausnahme der nach diesen Übereinkünften verliehenen Urheberpersönlichkeitsrechte als Straftaten nach ihrem innerstaatlichem Recht festzulegen, wenn diese Handlungen vorsätzlich, in gewerbsmäßigem Umfang und mittels eines Computersystems begangen werden.

(3) Eine Vertragspartei kann sich das Recht vorbehalten, eine strafrechtliche Verantwortlichkeit nach den Absätzen 1 und 2 unter begrenzten Umständen nicht vorzusehen, soweit andere wirksame Abhilfen zur Verfügung stehen und dieser Vorbehalt die internationalen Verpflichtungen dieser Vertragspartei aus den in den Absätzen 1 und 2 genannten völkerrechtlichen Übereinkünften nicht beeinträchtigt.

3.9.1 Anwendungsbereich

Neben den computerspezifischen Delikten in den Art. 2-6, der Anpassung bestehender Tatbestände in den Art. 7 und 8 sowie der Bekämpfung von Kinderpornografie stellt der strafrechtliche Schutz von Urheberrechten und verwandten Schutzrechten durch Art. 10 einen vierten Schwerpunkt im materiellrechtlichen Teil der Konvention dar. Dieser Tatbestand trägt der zunehmenden wirtschaftlichen und rechtlichen Bedeutung von Immaterialgütern in der modernen Informationsgesellschaft Rechnung. Die Computertechnologie und die internationalen Datennetze (Internet) haben in den letzten Jahren die rechtswidrige Herstellung und Verbreitung geschützter Werke dramatisch erleichtert. Zu denken ist beispielsweise an die Konvertierung geschützter Musiktitel in Platz sparende MP3-Dateien[622] und die anschließende Verbreitung über P2P-Netzwerke[623]. Dank Breitbandverkabelung sind diese Tauschbörsen nicht mehr alleine auf die Weitergabe von Audiodateien beschränkt, sondern in den letzten Jahren gerieten zusehends auch geschützte Software und komplette Hollywood-Filme in das Visier der Raubkopierer (siehe dazu Kapitel 1.7.4.1). Da Daten in Computernetzen nicht an Landesgrenzen Halt machen, die räumliche Wirkung nationalen Urheberrechts jedoch territorial beschränkt ist (Territorialitätsprinzip)[624], ist an dieser Stelle das internationale Urheberrecht gefordert. Art. 10 verfolgt in diesem Zusammenhang, wie beispielsweise auch Art. 61 TRIPs, das Ziel, international garantierte Urheber- und Schutzrechte strafrechtlich zu schützen. Dabei steht es den Unterzeichnerstaaten frei, in ihren Rechtsordnungen weitergehende Strafbestimmungen zu erlassen.

Art. 10 schützt nur Immaterialrechtsgüter auf kulturellem Gebiet. Patente, Marken und sonsti-

[621] ER Ziff. 107-117
[622] Siehe Fn 124
[623] Siehe Kapitel 1.7.4.1.
[624] Schack, Rn 768 ff.

ge gewerbliche Erzeugnisse geistigen Schaffens werden nicht erfasst. Abs. 1 pönalisiert Verstöße gegen das Urheberrecht im engeren Sinne; Abs. 2 gegen verwandte Schutzrechte (engl. *neighbouring rights*). Der jeweilige Schutzgegenstand beurteilt sich nach dem nationalen Recht und entsprechend der Verpflichtungen, die eine Vertragspartei im Hinblick auf die zitierten internationalen Übereinkünfte übernommen hat. Auf Grund der Akzessorietät des Urheberstrafrechts zum Urheberrecht, können sich erhebliche Abweichungen in den jeweiligen nationalen Rechtsordnungen ergeben.

3.9.2 Tatbestand

Der Tatbestand wird im Wesentlichen durch die Bezugnahme auf internationale Verträge zum Urheberrecht und verwandten Schutzrechten ausgefüllt. Die Formulierung „aufgrund ihrer Verpflichtung" (engl. „*pursuant to the obligations it has undertaken*") in beiden Absätzen stellt klar, dass die Vertragsparteien des Cybercrime-Übereinkommens nur zur Sanktionierung von Missachtungen derjenigen urheberrechtlichen Übereinkommen verpflichtet sind, denen sie selbst beigetreten sind. Vorbehalte oder Erklärungen, die nach einem dieser Übereinkommen gestattet waren, setzen sich im Anwendungsbereich des Art. 10 fort. An dieser Stelle äußert sich die Akzessorietät des Urheberstrafrechts zum Urheberrecht. Einschränkend stellt Art. 10 nur auf „gewerbsmäßige" Handlungen, die „mittels eines Computersystems" begangen wurden ab und schließt die Verletzung von „Urheberpersönlichkeitsrechten" von der Gewährung strafrechtlichen Schutzes völlig aus. Diese Merkmale werden in den Erläuterungen nicht näher definiert.

3.9.2.1 Art. 10 Abs. 1 – Urheberrecht

Bei den Übereinkommen, auf die in Art. 10 Abs. 1 Bezug genommen wird, handelt es sich um die „Berner Übereinkunft zum Schutz von Werken der Literatur und Kunst in der Pariser Fassung vom 24. Juli 1971" (RBÜ)[625], das „Übereinkommen über handelsbezogene Aspekte der Rechte des geistigen Eigentums" (TRIPs)[626] sowie den WIPO[627]-Urheberrechtsvertrag (WCT)[628].

3.9.2.1.1 RBÜ[629]

Bei der „Berner Übereinkunft zum Schutz von Werken der Literatur und Kunst" handelt es sich um einen der ältesten der heute noch geltenden Staatsverträge. Die ursprüngliche Fassung ist auf den 09.09.1886 datiert und wurde bislang sieben Mal – zuletzt 1971 in Paris – revidiert[630]. In der BRD ist das Abkommen seit dem 10.10.1974 in Kraft.[631] Der sachliche Anwendungsbereich der RBÜ umfasst „alle Erzeugnisse auf dem Gebiet der Literatur, der

[625] Paris Act of 24 July 1971 of the Bern Convention for the Protection of Literary and Artistic Works
[626] Agreement On Trade Related Aspects of Intellectual Property Rights.
[627] World Intellectual Property Organization; gegründet am 26.04.1970 auf der Grundlage des Übereinkommens zur Errichtung der Weltorganisation für geistiges Eigentum (WIPO-Konvention vom 14.07.1967, BGBl. 1970 II, S. 295 ff.). Seit Dezember 1974 hat sie den Rang einer UN-Sonderorganisation; *Sitz* in Genf. Im Jahr 2000 waren 171 Länder Mitglieder, http://www.wipo.org.
[628] WIPO Copyright Treaty
[629] Ausführlich dazu: Handbuch des Urheberrechts – *v. Lewinski* § 57 S. Rn 18-34; Rehbinder, Rn 479, 480; Schack, Rn 833-851, jeweils mwN.
[630] BGBl. 1973 II, S. 1069 ff.
[631] BGBl. 1974 II, S. 1079

Wissenschaft und der Kunst“, Art. 2 Abs. 1 RBÜ[632]. Der Werkbegriff wurde offen gestaltet und kann auch ohne Vertragsänderung neuen Entwicklungen (beispielsweise Computerprogrammen) angepasst werden. In persönlicher Hinsicht schließt die RBÜ alle Urheber ein, die die Staatsangehörigkeit eines Verbandslandes besitzen oder sich dort gewöhnlich aufhalten oder deren Werk zuerst in einem Verbandsland veröffentlicht wird.[633] Der Konventionsschutz entfaltet sich durch den Grundsatz der Inländerbehandlung und die konventionseigenen Mindestrechte.[634] Der Inländerbehandlungsgrundsatz nach Art. 5 Abs. 1 ordnet an, dass jeder Angehörige eines Verbandsstaates in den anderen Verbandsstaaten in Bezug auf die durch die RBÜ geschützten Werke wie ein Inländer zu behandeln sei. Es handelt sich um ein fremdenrechtliches Prinzip, dessen großer Vorzug es ist, ohne materielle Eingriffe in fremde Rechtsordnungen auszukommen und trotzdem im Vertrauen auf das Prinzip der Gegenseitigkeit ein weitgehend einheitliches Schutzniveau zu schaffen.[635] Der wesentliche Nachteil besteht darin, dass ausländische Urheber im Inland besser geschützt sein können als Inländer im anderen Verbandsstaat.[636] Zur Kompensation dieses Defizits enthält die RBÜ einen seit 1886 ständig wachsenden Katalog von Mindestrechten, wie beispielsweise das Urheberpersönlichkeitsrecht (Art. 6bis), das Übersetzungsrecht (Art. 8), das Vervielfältigungsrecht (Art. 9), das Aufführungs-, Sende- und Vortragsrecht (Art. 11, 11bis, 11ter) und das Bearbeitungsrecht (Art. 12 und 14). Auf diese Mindestrechte können sich die Urheber unmittelbar berufen, wenn auch nicht im Ursprungsland des Werks, Art. 5 Abs. 3 S. 1. Dadurch, dass die EGen zum 01.01.1995 Vertragspartei der WTO wurden, innerhalb der das TRIPs (dazu im Folgenden) gilt, welches in Art. 9 Abs. 1 wiederum auf Art. 1-21 RBÜ, mit Ausnahme des Urheberpersönlichkeitsrechts in Art. 6bis, verweist, wurden diese Teile der RBÜ Bestandteil des europäischen Gemeinschaftsrechts.[637]

3.9.2.1.2 TRIPs[638]

Die Uruguay-Runde des GATT[639] endete mit dem WTO-Übereinkommen[640], durch das die WTO als Nachfolgeorganisation des GATT ins Leben gerufen wurde. Anhang C dieses Übereinkommens ist das TRIPs, das umfassende Regelungen zum Immaterialgüterschutz beinhaltet. Das Urheberrecht einschließlich der verwandten Schutzrechte in den Art. 9-13 TRIPs[641] bildet neben Normen zum gewerblichen Rechtschutz (z.B. Marken, Patente, Gebrauchsmuster) nur einen Teilbereich des Übereinkommens. In der BRD ist es am 01.01.1995 in Kraft getreten.[642] Kernstücke des TRIPs auf dem Gebiet des Urheberrechts sind der in Art. 3 niedergelegte (differenzierte) Grundsatz der Inländergleichbehandlung, die Meistbegünstigungsklausel in Art. 4 (Grundsatz, dass Vergünstigungen zwischen zwei Vertragspartnern allen Vertragspartnern gewährt werden müssen; sog. „Ausländerparität“) sowie die Bezugnahme auf die RBÜ hinsichtlich der dort gewährten Mindestrechte mit Ausnahme des Urheberpersönlichkeitsrechts, Art. 9, 1 Abs. 1.[643] Das TRIPs konkurriert damit nicht mit der RBÜ, sondern gewährt zusätzlichen Schutz, indem es beispielsweise Computerprogramme und Sam-

[632] Alle Artikel des Abschnitts 3.9.2.1.1 beziehen sich auf die RBÜ.
[633] Handbuch des Urheberrechts – *v. Lewinski* § 57 S. Rn 23; Schack, Rn 841
[634] Handbuch des Urheberrechts – *v. Lewinski* § 57 S. Rn 25; Rehbinder, Rn 479, 480; Schack, Rn 845-849
[635] Schack, Rn 847
[636] Rehbinder, Rn 481; Schack, Rn 845
[637] Schack, Rn 883
[638] Handbuch des Urheberrechts – *v. Lewinski* § 57 S. Rn 66-76; Rehbinder, Rn 483; Schack, Rn 880-884
[639] General Agreement on Tarifs and Trade; am 30.10.1947 in Genf von 23 Ländern unterzeichnet. Das Ziel war der Abbau von Zoll- und Handelsschranken.
[640] BGBl. 1994 II, S. 1438, in Kraft seit dem 01.01.1995 (BGBl. 1995 II, S. 456)
[641] Alle Artikel des Abschnitts 3.9.2.1.2 beziehen sich auf das TRIPs.
[642] BGBl. 1994 II, S. 1730 ff.
[643] Handbuch des Urheberrechts – *v. Lewinski* § 57 S. Rn 69, 70, 71-74; Rehbinder, Rn 483

melwerke (Art. 10) in den Kreis der geschützten Werke mit einbezieht („Bern plus“).[644] In verfahrensrechtlicher Hinsicht ist das Streitschlichtungsverfahren des GATT beachtlich, das auf die im TRIPs Abkommen geregelten Rechte anwendbar ist.

3.9.2.1.3 WCT[645]

Der WIPO-Urheberrechtsvertrag ist keine Revision der RBÜ, sondern ein Sonderabkommen[646] im Sinne von Art. 20 RBÜ, Art. 1 Abs.1 WCT[647]. Als solches darf er nicht hinter den Garantien der RBÜ zurückbleiben bzw. im Widerspruch dazu stehen, Art. 1 Abs. 2, 4. Er ist am 06.12.2001 in Kraft getreten.[648] Die BRD hat den WCT am 20.12.1996 unterzeichnet und am 10.08.2003 ratifiziert.[649] Durch das „Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft“[650] vom 10.09.2003 wurde das deutsche UrhG an die Vorgaben des WIPO-Vertrags angepasst.[651] Nach Art. 17 Abs. 3 steht es im Gegensatz zur RBÜ nicht nur Staaten, sondern auch der EG offen, Vertragspartner des WCT zu werden. Die EG hat zu diesem Zweck die Richtlinie 2001/29/EG „[…] zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft […]“ verabschiedet, die am 22. Juni 2001 in Kraft getreten ist[652] und die Richtlinien 92/100/EWG sowie 93/98/EWG abändert.

Die Bedeutung des WCT besteht in einer Ergänzung und Anpassung der RBÜ in Bezug auf die neuen Techniken, insbesondere internationale Computernetzwerke.[653] Nach Art. 4 und 5 WCT wird der Schutz des Berner Verbandes auf Computerprogramme und Datensammlungen (Datenbanken) ausgedehnt. Art. 6-8 WCT gewähren Mindestrechte hinsichtlich der Verbreitung, der gewerblichen Vermietung und der öffentlichen Wiedergabe – einschließlich Online-Übermittlungen[654] – bestimmter Werkstücke.[655] Art. 11 WCT verbietet die Umgehung „wirksamer technischer Vorkehrungen“; Art. 12 WCT regelt den Schutz bestimmter für die Ausübung des Urheberrechts notwendiger Informationen.

WIPO-Verträge in anderen Bereichen – beispielsweise Rundfunk und Folklore – befinden sich im Vorbereitungsstadium.[656]

3.9.2.2 Art. 10 Abs. 2 – Verwandte Leistungsschutzrechte

Art. 10 Abs. 2 nimmt Bezug auf das Rom-Abkommen (RA), das TRIPs sowie den WIPO-

[644] Rehbinder, Rn 483
[645] Handbuch des Urheberrechts – *v. Lewinski* § 57 S. Rn 79-92; Schack, Rn 885 mwN; Online: http://www.wipo.int/treaties/en/ip/wct/index.html (01.04.2004)
[646] Handbuch des Urheberrechts – *v. Lewinski* § 57 S. Rn 79
[647] Alle Artikel des Abschnitts 3.9.2.1.3 beziehen sich auf das WCT.
[648] Online: http://www.wipo.int/treaties/en/ShowResults.jsp?search_what=N&treaty_id=16 (01.04.2004)
[649] BGBl. 2003 II, S. 754
[650] BGBl. 2003 I, S. 1774
[651] Beschlussempfehlung des Rechtsausschusses, BT-Drs. 15/837, S. 1 f.
[652] Abl. EG L 167, S. 10 ff.
[653] Handbuch des Urheberrechts – *v. Lewinski* § 57 S. Rn 78; v. Lewinski CR 1997, 438 (438); Schack, Rn 885b
[654] Handbuch des Urheberrechts – *v. Lewinski* § 57 S. Rn 83; Online: Laga, „Die WIPO Abkommen zum Urheberrecht und zu verwandten Schutzrechten vom Dezember 1996 (WCT und WPPT)“
[655] v. Lewinski CR 1997, 438 (440 f.); Schack, Rn 885b
[656] Handbuch des Urheberrechts – *v. Lewinski* § 57 S. Rn 11 ff.; v. Lewinski CR 1997, 438 (443); Schack, Rn 885 ff; Vorschlag der EU-Kommission hinsichtlich eines neuen WIPO-Vertrags in Bezug auf Sendeunternehmen, http://europa.eu.int/comm/internal_market/en/intprop/news/01-wipo.htm (01.04.2004)

Vertrag betreffend Darbietungen und Tonträger (WPPT)[657].

3.9.2.2.1 RA[658]

Bei dem Rom-Abkommen (RA) vom 26.10.1961, in der BRD am 21.10.1966 in Kraft getreten[659], handelt es sich um den ersten und wichtigsten völkerrechtlichen Vertrag auf dem Gebiet des internationalen Leistungsschutzrechts.[660] Neben den ausübenden Künstlern (Art. 3 lit. a) RA[661]) schützt es die Hersteller von Tonträgern (Art. 3 lit. a), b)) sowie Sendeunternehmen (Art. 6). Art. 1 stellt klar, dass das RA die urheberrechtlichen Garantien unberührt lässt. Der Schutz des RA ruht auf zwei Säulen: zum einen gilt der Grundsatz der Inländerbehandlung, der in Art. 2 näher umschrieben wird. Zum anderen gewährt das Abkommen einen Katalog von Mindestrechten, der in seiner Schutzintensität in Abhängigkeit der jeweiligen Leistung stark variiert.[662] Während hinsichtlich der Interpreten in Art. 7 nur ein vages Rechtsschutzziel definiert wurde, können sich die Hersteller von Tonträgern und die Sendeunternehmen auf die in Art. 10 und 13 definierten Mindestrechte unmittelbar berufen.[663]

3.9.2.2.2 WPPT[664]

Der WPPT, der zusammen mit dem WCT am 20.12.1996 in Genf angenommen wurde und am 20.02.2002 in Kraft getreten ist[665], unterscheidet sich vom WCT dadurch, dass er nicht das Urheberrecht, sondern verwandte Leistungsschutzrechte zum Gegenstand hat. Strukturell weicht er vom WCT darüber hinaus dadurch ab, dass er nur eine auf „[…] die in diesem Vertrag gewährten Rechte […]“ beschränkte Inländerbehandlung vorsieht. Im Unterschied zum RA gewährt er nur den ausübenden Künstlern, Art. 2 lit. a) WPPT[666], und den Tonträgerherstellern, Art. 2 lit. b), d), besonderen Schutz. Aus diesem Grund befindet sich ein gesonderter WIPO-Vertrag in Bezug auf Sendeunternehmen in Vorbereitung.[667] Inhaltlich bemerkenswert sind vor allem das in Art. 5 niedergelegte Künstlerpersönlichkeitsrecht sowie die selbstständigen Verwertungsrechte der Vervielfältigung, Art. 7, 11, Verbreitung, Art. 8, 12, Vermietung, Art. 9, 13 und Online-Übermittlung, 10, 14, auf die sich die Künstler unmittelbar berufen können. In diesem Zusammenhang ist auch das Verbot von Förmlichkeiten in Art. 20 von besonderer Bedeutung. Deutschland hat den WPPT zusammen mit dem WCT ratifiziert.[668] Das deutsche Urheberrecht wurde durch das „Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft“[669] vom 10.09.2003 angepasst.[670]

---

[657] WIPO Performances and Phonograms Treaty
[658] Handbuch des Urheberrechts – *v. Lewinski* § 57 S. Rn 44-55; Rehbinder, Rn 484; Schack, Rn 857-863; Straus GRUR Int. 1985, 19 ff.
[659] BGBl. 1965 II, S. 1245 ff.
[660] Handbuch des Urheberrechts – *v. Lewinski* § 57 S. Rn 44; Schack, Rn 858
[661] Alle Artikel des Abschnitts 3.9.2.2.1 beziehen sich auf das RA.
[662] Handbuch des Urheberrechts – *v. Lewinski* § 57 S. Rn 50-54; Rehbinder, Rn 484; Schack, Rn 863
[663] Rehbinder, Rn 484; Schack, Rn 861-863
[664] Handbuch des Urheberrechts – *v. Lewinski* § 57 S. Rn 93, 94; Rehbinder, Rn 484; Schack, Rn 857 ff., jeweils mwN; Online, http://www.wipo.int/treaties/en/ip/wppt/index.html (01.04.2004)
[665] Online, http://www.wipo.int/treaties/notifications/wppt/index2.html (01.04.2004)
[666] Alle Artikel des Abschnitts 3.9.2.2.2 beziehen sich auf den WPPT.
[667] Siehe Fn 656
[668] Siehe Fn 649.
[669] Siehe Fn 650
[670] Siehe Fn 651

3.9.3 Subjektiver Tatbestand

Die Verletzungen des Urheberrechts und verwandter Schutzrechte müssen „absichtlich" erfolgen, um die strafrechtliche Verantwortlichkeit auszulösen. Im Gegensatz zu allen anderen materiellrechtlichen Vorschriften in der Konvention wird der Ausdruck „absichtlich" (engl. „*wilfully*") an Stelle des Begriffs „vorsätzlich" (engl. „*intentionally*") sowohl in Abs. 1 als auch in Abs. 2 verwendet. Mit dieser Wortwahl wollten sich die Verfasser lediglich an die Terminologie der Strafnorm des Art. 61 TRIPs anlehnen, im Übrigen jedoch keine besonderen subjektiven Voraussetzungen begründen.[671]

3.9.4 Rechtswidrigkeit

Das Merkmal „unbefugt" wurde nicht in den Tatbestand dieses Artikels aufgenommen, da es wegen des Begriffs der „Verletzung", der bereits die Verwendung urheberrechtlich geschützten Materials ohne Berechtigung andeutet, als überflüssig erachtet wurde.[672] Die Verfasser weisen darauf hin, dass aus seinem Fehlen nicht der Umkehrschluss gezogen werden soll, dass die andernorts in der Konvention damit in Zusammenhang stehenden strafrechtlichen Verteidigungsmöglichkeiten ausgeschlossen seien.[673]

3.9.5 Art. 10 Abs. 3 – Vorbehalt

Absatz 3 gestattet den Vertragsparteien, unter besonderen Umständen keine Strafbarkeit nach den Abs. 1 und 2 zu begründen (z.B. bei Parallelimporten, Mietrechten, usw.), solange andere wirksame Abhilfen, einschließlich zivil- oder verwaltungsrechtlicher Mittel, verfügbar sind. Die untere Schwelle der Strafbarkeit wird durch Art. 61 TRIPs gesetzt.[674]

3.9.6 Vergleichbare Tatbestände im deutschen Strafrecht

Das deutsche Urheberrecht weist Straftatbestände in den §§ 106-108b UrhG auf. Für einen Vergleich kommen die §§ 106 und 108 UrhG in Betracht, jeweils in Verbindung mit § 108a UrhG, da auch Art. 10 gewerbsmäßiges Handeln erfordert sowie § 108b UrhG. § 107 UrhG pönalisiert Verletzungen eines Teilbereichs des Urheberpersönlichkeitsrechts (§ 13 S. 2 UrhG), das von Art. 10 ausdrücklich ausgeschlossen wird. §§ 106 und 108 UrhG erfordern isoliert betrachtet kein gewerbsmäßiges Vorgehen des Täters. Jedoch greift § 108a UrhG die Gewerbsmäßigkeit als strafschärfendes, persönliches Merkmal im Sinne von § 28 Abs. 2 StGB auf und verweist bzgl. der Tathandlungen auf die §§ 106 und 108 UrhG. Wegen der Akzessorietät des Urheberstrafrechts zum Zivilrecht ist bzgl. Tatobjekten und Tathandlung auf die urheberrechtlichen Regelungen zurückzugreifen.

3.9.6.1 §§ 106, 108a UrhG – Unerlaubte Verwertung urheberrechtlich geschützter Werke

Die Überschrift der Strafnorm ist missverständlich, da nur einzelne unerlaubte Verwertungshandlungen mit Strafe bedroht werden. Schutzgut ist nach allgemeiner Ansicht sowohl das geistige Eigentum im Allgemeinen und als auch das Verwertungsrecht des Berechtigten im

[671] ER Ziff. 113
[672] ER Ziff. 115
[673] ER Ziff. 115
[674] ER Ziff. 116

Besonderen.[675]

3.9.6.1.1 Tatbestand

Tatobjekte nach § 106 UrhG sind ein „Werk“ oder eine „Bearbeitung oder Umgestaltung eines Werkes“. Der zivilrechtliche Werkbegriff ist in § 2 Abs. 2 UrhG als „persönliche geistige Schöpfung“ definiert. Beispiele hierfür finden sich in § 2 Abs. 1 UrhG. Der urheberstrafrechtliche Werkbegriff stimmt mit dem dargestellten zivilrechtlichen überein.[676] Ausnahmen, die vor allem für sittenwidrige, verbotene oder mit einem Verbreitungsverbot belegte Werke, Werkteile, Sammelwerke, Computerprogramme und Datenbankwerke diskutiert wurden[677], werden zu Recht aufgrund des eindeutigen Wortlauts des § 106 UrhG abgelehnt.[678]

Grundsätzlich gilt nach der Rechtsprechung, dass ein Werk eine gewisse Gestaltungshöhe bzw. einen Eigentümlichkeitsgrad aufweisen muss, indem es subjektiv neu ist und individuelle Züge seines Schöpfers erkennen lässt.[679] Da der BGH an die schöpferische Leistung der einzelnen Werkarten unterschiedliche Anforderungen stellt[680], ist umstritten, ob auch die sog. „kleine Münze“ – ein Werk, das sich durch eine geringe Gestaltungshöhe auszeichnet – geschützt sein kann. Vor allem in Bezug auf Computerprogramme und wissenschaftliche Arbeiten ist der BGH in letzter Zeit auf Grund entsprechender EG-Richtlinien[681] von seinen hohen Anforderungen abgerückt.[682]

Die Begriffe „Bearbeitung“ und „Umgestaltung“ ergeben sich aus §§ 3 und 23 UrhG. Ungeklärt ist ihr Verhältnis zueinander. Der Wortlaut des § 23 UrhG legt nahe, dass die Umgestaltung als Oberbegriff jede Bearbeitung umfasst. *Plassmann*[683] betrachten diesen Schluss nicht als zwingend und geht von einer weitgehend zufälligen Verwendung der Begriffe in § 106 UrhG aus. *Ilzhöfer*[684] vertritt hingegen die Meinung, dass eine Bearbeitung das ursprüngliche Werk erkennen lasse, während es eine Umgestaltung zu verschleiern versuche. Aus dem Gesetzeswortlaut lassen sich diese Ansichten nicht begründen. Eine Bearbeitung ist daher – wie bereits eingangs dargestellt – ein Unterfall der Umgestaltung, die dann vorliegt, wenn das Originalwerk unter Aufbringung einer eigenständigen schöpferischen Leistung geändert wurde.[685]

[675] Hildebrandt, S. 32 mwN; Schricker – *Haß* § 106 Rn 1
[676] Handbuch des Urheberrechts – *Flechsig* § 90 Rn 10; Schricker – *Haß* § 106 Rn 2
[677] Überblick bei: Hildebrandt, S. 36 ff.
[678] Fromm/Nordemann – *Nordemann/Vinck* § 106 Rn 2; Handbuch des Urheberrechts – *Flechsig* § 90 Rn 10; Schricker – *Haß* § 106 Rn 2
[679] Fromm/Nordemann – *Nordemann/Vinck* § 2 Rn 3 ff.; Ilzhöfer, Rn 562; Schricker – *Loewenheim* § 2 Rn 8 ff.
[680] Beispiele bei: Fromm/Nordemann – *Nordemann/Vinck* § 2 Rn 29 ff.
[681] Richtlinie 91/250/EWG des Rates über den Schutz von Computerprogrammen vom 14. Mai 1991; Richtlinie 93/98/EWG des Rates zur Harmonisierung der Schutzdauer des Urherbrechts und bestimmter verwandter Schutzrechte vom 29. Oktober 1993; EGRL des Rates über den rechtlichen Schutz von Datenbanken vom 11. März 1996
[682] Ursprünglich: BGHZ 1994, 276 (284) „Inkasso-Programm“; Änderung der Rechtsprechung:, BGHZ 123, 208 (211) „Buchhaltungsprogramm“
[683] Plassmann, S. 209 mwN
[684] Ilzhöfer, Rn 641mwN
[685] Fromm/Nordemann – *Nordemann/Vinck* § 3 Rn 3; Handbuch des Urheberrechts – *G. Schulze/Hoeren* § 9 Rn 207, 209; Schricker – *Loewenheim* § 3 Rn 5 f., der zusätzlich auf das Kriterium der „Abhängigkeit vom Originalwerk“ abstellt.

3.9.6.1.2 Tathandlungen

Als Tathandlungen nennt § 106 UrhG die „Vervielfältigung", „Verbreitung" und „öffentliche Wiedergabe" der geschützten Werke. Die ersten beiden Varianten stellen eine Verwertung in körperlicher, § 15 Abs. 1 UrhG, die dritte eine in unkörperlicher Form dar, § 15 Abs. 2 UrhG.

Eine „Vervielfältigung" nach § 16 UrhG setzt voraus, dass ein körperlicher Gegenstand hergestellt wird, der das Werk in sinnlich unmittelbar (z.B. Gemälde, usw.) oder mittelbar (z.B. Audio/Videokassette, Diskette, usw.) wahrnehmbarer Weise wiedergibt.[686] Auf die Anzahl der Vervielfältigungsstücke sowie das Verfahren, in dem diese hergestellt werden, kommt es nicht an. Im EDV-Bereich ist die Frage umstritten, ob das vorübergehende Laden von Daten in den Arbeitsspeicher eine Vervielfältigung im Rechtssinne darstellt.[687] Ein Ausgangspunkt für die Erörterung dieses Problems kann zunächst der Wortlaut des § 15 Abs. 1 UrhG sein. Danach ist nur die Herstellung einer körperlichen Kopie eine Vervielfältigung im Rechtssinne. Während dies für permanente Datenträger wie Disketten[688], Festplatten und CD-Rom ganz überwiegend mit der Begründung bejaht wird, dass in diesen Fällen eine gewisse Dauerhaftigkeit der Datenmanifestierung vorliege, sei dies bei einer Speicherung im RAM gerade anders, da bei einem Stromausfall die Daten sofort verloren gingen.[689] Darauf kann entgegnet werden, dass das Urheberrecht auch vergängliche Werke aus Backwerk oder Eis schützt, so dass es auf eine Dauerhaftigkeit nicht ankommen kann.[690] Auch der Wortlaut des § 69c Nr. 1 Satz 2 UrhG vermag diese Frage nicht zu beantworten.[691] Es heißt dort lediglich „[…] soweit das Laden, usw. eine Vervielfältigung erfordert […]." Daraus kann nicht abgeleitet werden, dass das Laden zwangsläufig einen entsprechenden Eingriff in das körperliche Verwertungsrecht des Urhebers bedeutet. Es gilt darüber hinaus zu beachten, dass §§ 69a UrhG nur Regelungen in Bezug auf Programme enthalten, d.h. unselbstständige Routinen nicht erfassen, und damit nur einen kleinen Ausschnitt des Ladens in den Arbeitspeicher behandeln. Eine Lösung des Problems kann in allgemeinen urheberrechtlichen Grundsätzen liegen. *Loewenheim*[692] führt insofern zutreffend aus, dass die reine Benutzung – anders als bei technischen Schutzrechten – urheberrechtlich nicht relevant ist, außer es werden dadurch zusätzliche Nutzungen des Werks ermöglicht. Dies ist in der Regel beim bloßen Laden in den Arbeitsspeicher nicht der Fall.[693] Wenig Sinn macht es dagegen, zwischen gewöhnlichen (Einzelplatzcomputer) und außergewöhnlichen (Netzwerk) Nutzungen zu differenzieren[694], da eine Abgrenzung als unsicher erscheint und letztendlich von technischen Zufälligkeiten abhängt. Das Laden in den Arbeitsspeicher stellt nach der vorzugswürdigen Ansicht[695] keine Vervielfältigung im Sinne von § 16 UrhG dar.

Ähnlich verhält es sich mit der sog. sukzessiven Teilvervielfältigung. Damit ist das technische Übertragungskonzept moderner Computernetzwerke gemeint. Daten werden in Paketen über zum Teil unterschiedliche Zwischenstationen vom Sender zum Empfänger geroutet. Auf dem Weg dorthin werden sie von speziellen Servern zwischengespeichert (sog. *caching*), um die Netzwerkgeschwindigkeit zu steigern. Beim Empfänger trifft nach einiger Zeit das komplette

[686] Fromm/Nordemann – *Nordemann* § 16 UrhG Rn 1; Schricker – *Loewenheim* § 16 UrhG Rn 6
[687] Fromm/Nordemann – *Vinck* § 16 Rn 2; Schricker – *Loewenheim* § 16 Rn 16 ff.
[688] LG Nürnberg-Fürth CR 1991, 108; Schack, Rn 378
[689] Schricker – *Loewenheim* § 69c Rn 9
[690] BGHZ 37, 1 (7); Bortloff ZUM 1993, 476 (481); Mehrings GRUR 1983, 275 (278); Schricker – *Loewenheim* § 16 Rn 19 ff.
[691] BGH NJW 1994, 1216 (1217) „Holzhandelsprogramm"; BHGZ 112, 264 (287) „Betriebssystem"
[692] Schricker – *Loewenheim* § 69c Rn 6 mwN
[693] Schricker – *Loewenheim* § 69c Rn 6; aA: Fromm/Nordemann – *Nordemann/Vinck* § 69c Rn 3
[694] So aber: Hildebrandt, S. 82
[695] Siehe Fn 692

Werk ein. Solange es sich lediglich zur Benutzung im Arbeitsspeicher befindet, liegt nach den oben dargestellten Grundsätzen keine Vervielfältigung vor. Anders hingegen, soweit zusätzliche Nutzungen ermöglicht werden, was beim bloßen „Cachen“ in der Regel nicht der Fall sein dürfte. Ungeklärt ist die Frage, wie die Cache-Server selbst zu behandeln sind. Datenpakete werden dort zum Teil als vollständige Programme zwischengespeichert. Die Kopien werden normalerweise nach kurzer Zeit gelöscht, um je nach Nachfrage Platz für neue Daten zu schaffen. Wie oben gezeigt, kommt es auf die Dauerhaftigkeit der Kopie nicht an. Jedoch lassen sich mit der Figur der Einwilligung brauchbare Ergebnisse erzielen. Jeder Urheber, der Daten über Computernetzwerke versendet, muss sich darüber klar sein, dass seine Daten aus Gründen der Netzwerktechnologie „gecached“ werden.[696]

Das Recht zur „Verbreitung“ ist in § 17 UrhG definiert. Es umfasst das öffentliche Anbieten sowie das Inverkehrbringen des körperlichen Originals oder eines körperlichen Vervielfältigungsstücks des Werks. Bloße Online-Datenübertragungen in Computernetzen scheiden mangels eines körperlichen Verbreitungsstückes aus.[697] Das Angebot an die Öffentlichkeit (§ 15 Abs. 3 UrhG entsprechend) ist eine Vorbereitungshandlung zum Inverkehrbringen. Für die zweite Handlungsvariante ist entscheidend, dass die tatsächliche Herrschaft über das Werk übergeht. Dahinstehen kann, ob dies im Rahmen einer Veräußerung, Vermietung oder eines sonstigen Grundgeschäfts erfolgt[698]. Der sog. Erschöpfungsgrundsatz in § 17 Abs. 2 UrhG sieht Schranken für das Verbreitungsrecht des Urhebers vor.

Die „öffentliche Wiedergabe“ nach § 15 Abs. 2 UrhG regelt die unkörperliche Verwertung des Werks. § 19 UrhG gewährt dem Urheber das Vortrags-, Aufführungs- sowie ein Vorführungsrecht. Das Vortrags- und das Aufführungsrecht beziehen sich auf die Darbietung von Sprach- bzw. Musikwerken vor einem anwesenden Publikum, § 19 Abs. 1-3 UrhG. Das Vorführungsrecht erfasst die Wiedergabe von Werken der bildenden Künste, Lichtbildwerke, Filmwerke, usw. mittels technischer Hilfsmittel. Neu hinzugekommen durch das „Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft“[699] vom 10.09.2003 ist das „Recht der öffentlichen Zugänglichmachung“ in § 19a UrhG. Damit wurden EU-Recht sowie Art. 8 des WCT[700] und Art. 10 und 14 des WPPT[701] umgesetzt. „Zugänglichmachen“ setzt voraus, dass Dritten der Zugriff auf das betreffende geschützte Werk eröffnet wird.[702] Der Begriff der „Öffentlichkeit“ ist in § 15 Abs. 3 UrhG definiert. Vorausgesetzt wird keine Weltöffentlichkeit, sondern es genügt durchaus ein kleinerer Kreis, der nicht durch persönliche Beziehungen verbunden ist.[703] Die Vorschrift ist technologieneutral formuliert und erfasst auch „Filesharing“-Systeme[704] wie Gnutella, KaZaA usw.[705] Das Senderecht in § 20 UrhG bezieht sich auf Rundfunksendungen (TV, Radio), unabhängig davon, mittels welcher Technik sie übertragen werden. §§ 21 und 22 UrhG werden hingegen als sog. Zweitverwertungsrechte bezeichnet. Sie knüpfen jeweils an § 19 bzw. 20 UrhG an. Die Zweitverwertungsrechte basieren auf der Überlegung, dass eine Erweiterung des Nutzerkreises (Öffentlichkeit nach § 15 Abs. 3 UrhG) durch den Verkauf eines Vervielfältigungsstücks nicht abgegolten ist.[706]

[696] Bechthold ZUM 1997, 427 (436 f.); Schwarz GRUR 1996, 836 (840 f.)
[697] Fromm/Nordemann – *Nordemann* § 17 Rn 7; Schricker – *Loewenheim* § 17 Rn 4 ff.
[698] Ilzhöfer, Rn 622; Schack, Rn 386
[699] Siehe Fn 650
[700] Siehe Kapitel 3.9.2.1.3
[701] Siehe Kapitel 3.9.2.2.2
[702] Dreier/Schulze – *Dreier* § 19a Rn 6; Handbuch des Urheberrechts – *Hoeren* § 21 Rn 60 ff.
[703] Dreier/Schulze – *Dreier* § 19a Rn 7; Handbuch des Urheberrechts – *Hoeren* § 21 Rn 60 ff.
[704] Siehe dazu Kapitel 1.7.4.1
[705] Dreier/Schulze – *Dreier* § 19a Rn 6
[706] Schack, Rn 399 ff.

3.9.6.1.3 Schranken

§ 106 UrhG pönalisiert eine Verletzung der bezeichneten Verwertungsrechte nur dann, wenn sie „[...] in anderen als den gesetzlich zugelassenen Fällen erfolgt [...]". Nach der heute allgemein vertretenen Auffassung[707] handelt es sich dabei um einen Verweis auf die Schrankenbestimmungen des Urheberrechts in §§ 45 ff. UrhG. An dieser Stelle kommt die Akzessorietät des Urheberstrafrechts zum Urheberzivilrecht zum Ausdruck. *Lampe*[708] ist darin zuzustimmen, dass sie in dogmatischer Sicht eine Sonderstellung einnehmen, da sie einen strafrechtlichen Tatbestand wie an keiner Stelle sonst im Strafrecht durch subjektive (z.B. „Zitierwille" bei § 51 UrhG) und objektive (z.B. „einzelne Vervielfältigungsstücke" bei § 53) Kriterien einschränken. Eine Erläuterung der Schrankenbestimmungen würde an dieser Stelle zu weit führen.

3.9.6.1.4 Ohne Einwilligung des Berechtigten

Darüber hinaus muss der Täter „ohne die Einwilligung des Berechtigten" handeln. Umstritten ist, ob dieses Merkmal auf der Tatbestands- oder der Rechtswidrigkeitsebene anzusiedeln ist. Die Ansicht, die dem Merkmal eine tatbestandsausschließende Wirkung zuspricht, stützt sich auf eine Parallele zu § 248b StGB.[709] Dort wird dem Merkmal „gegen den Willen des Berechtigten" eben diese Wirkung zugesprochen.[710] Die Gegenmeinung argumentiert mit dem Schutzgut des § 106 UrhG. Dabei handele es sich nicht um den freien Willen des Berechtigten, sondern um die von §§ 106 ff. UrhG aufgezählten Verwertungs- und Schutzrechte.[711] Überzeugender noch ist dem Merkmal mit *Hildebrandt*[712] eine Doppelfunktion zuzusprechen: Auf der Tatbestandsebene müsse geprüft werden, ob der Beschuldigte zur Nutzung des Werkes berechtigt sei, etwa nach §§ 31 ff. UrhG. Darüber hinaus wird auf die Möglichkeit einer Einwilligung nach den allgemeinen strafrechtlichen Vorschriften verwiesen. *Hildebrandt* zieht zur Begründung eine Parallele zwischen § 242 StGB und § 106 UrhG. Eine Sache könne nur derjenige stehlen, für den sie „fremd" sei. Das Merkmal „fremd" bezieht sich auf die zivilrechtlich zu beurteilenden Eigentumsverhältnisse. Da Immaterialgüter keine Sachen sind, können sie auch nicht über das Merkmal der „Fremdheit" dem jeweils Berechtigten zugeordnet werden. Im Rahmen des Urheberrechts treten an die Stelle der Eigentumsverhältnisse die urheberrechtlichen Verwertungs- und Nutzungsrechte. Daraus werde deutlich, dass die „Fremdheit" im Diebstahlstatbestand mit dem Merkmal der fehlenden Einwilligung bei § 106 UrhG korrespondiere. Dort wie hier sei das entsprechende Zuordnungskriterium auf der Tatbestandsebene zu behandeln. Dies bedeute jedoch ebenso wenig wie bei § 242 StGB, dass die strafrechtlichen Grundsätzen folgende Einwilligung ausgeschlossen wäre.[713] Beim Diebstahl entfällt die Rechtswidrigkeit der Zueignung beispielsweise, wenn der Verfügungsberechtigte in die Zueignung einwilligt.[714]

3.9.6.1.5 § 108a UrhG – Gewerbsmäßigkeit

§ 108a UrhG stellt einen Qualifikationstatbestand zu §§ 106-108 UrhG dar. Die Gewerbsmä-

[707] Fromm/Nordemann – *Vinck* § 106 UrhG Rn 3; Schricker – *Haß* § 106 UrhG Rn 7 jeweils mwN
[708] Lampe GA 1978, 7 (10 ff.)
[709] Weber, Der strafrechtliche Schutz des Urheberrechts, S. 268
[710] Lackner/Kühl – *Kühl* § 248b Rn 4; Sch/Sch – *Eser* § 248b Rn 7; Tröndle/Fischer § 248b Rn 6
[711] Schack, Rn 745
[712] Hildebrandt, S. 150 ff.
[713] Etwa in Fällen, in denen die zivilrechtliche zu beurteilende Übertragung der Nutzungsrechte unwirksam war.
[714] Sch/Sch – *Eser* § 242 Rn 58

ßigkeit ist ein strafschärfendes persönliches Merkmal im Sinne von § 28 Abs. 2 StGB.[715] Gewerbsmäßiges Handeln wird von der Rechtsprechung bejaht, wenn der Täter sich durch die wiederholte Begehung von Straftaten eine fortlaufende Einnahmequelle von einiger Dauer und einigem Umfang verschaffen will.[716]

3.9.6.1.6 Ergebnis zu §§ 106, 108a UrhG

Auf Grund der Akzessorietät von Art. 10 zum internationalen Urheberrecht und der schwer überschaubaren Reichweite dieses Gebiets beschränkt sich ein Vergleich zu §§ 106, 108a UrhG auf grundsätzliche Fragen.

Maßgebliche Bedeutung für die inhaltliche Reichweite der von Art. 10 Abs. 1 geschützten Urheberrechte in Bezug auf die Informationstechnologie kommt nach seiner Ratifikation[717] dem WCT zu. Eine wesentliche Auswirkung der Umsetzung dieses internationalen Vertrags findet sich in dem neu in das deutsche Urheberrecht eingefügten § 19a UrhG. Dadurch, dass diese Norm das „Recht der öffentlichen Zugänglichmachung" als unkörperliche Form der Verwertung ausschließlich dem Urheber zuweist, hat sich dessen Rechtsstellung in Bezug auf urheberrechtswidrige Verwertungshandlungen im Internet – vor allem im Rahmen sog. „Filesharing"-Systemen – signifikant verbessert. Im Unterschied zu §§ 106, 108a UrhG ist Art. 10 Abs. 1 nicht auf bestimmte unerlaubte Verwertungsakte beschränkt. Er erinnert damit an die zivilrechtliche Schadensersatznorm des § 97 UrhG und geht über das deutsche Urheberstrafrecht hinaus. In Bezug auf die Gewerbsmäßigkeit bleibt er hinter § 106 UrhG zurück, der dieses Merkmal nicht verlangt. In diesem Fall kann jedoch der Qualifikationstatbestand des § 108a UrhG eingreifen. Anders als Art. 10 Abs. 1 erfordert das nationale Urheberstrafrecht nicht, dass die Verletzungshandlungen „mittels eines Computersystems" begangen werden. Computerbezogene Tathandlungen werden mit den oben dargestellten Schwierigkeiten vor allem im Bereich der „Vervielfältigung" grundsätzlich erfasst. In Bezug auf die Werkqualität von Computerprogrammen ist der BGH von seinen hohen Anforderung mittlerweile abgerückt.

3.9.6.2 §§ 108, 108a UrhG – Unerlaubte Eingriffe in verwandte Schutzrechte

Nach überwiegender Ansicht ist Schutzgut des § 108 UrhG die unternehmerische Leistung des Berechtigten.[718] Dies wird daraus abgeleitet, dass die Norm mit Ausnahme von § 108 Abs. 1 Nr. 7 UrhG, der auf urheberpersönlichkeitsrechtliche Aspekte Bezug nimmt, nur verwertungsrechtliche Interessen schützt.

3.9.6.2.1 Tatbestand

§ 108 Abs. 1 UrhG pönalisiert bestimmte Eingriffe in die Leistungsschutzrechte nach §§ 70 ff. UrhG. Strukturell ist der Tatbestand § 106 UrhG nachempfunden. Nr. 1 schützt „wissenschaftliche Ausgaben" nach § 70 UrhG, deren „Bearbeitungen", § 3 UrhG, oder „Umgestaltungen", § 23 UrhG, gegen unerlaubte „Vervielfältigung", „Verbreitung" oder „öffentliche Wiedergabe", § 15 Abs. 1 Nr. 1, Nr. 2, Abs. 2 UrhG. Tatobjekt nach Nr. 2 sind „nachgelasse-

[715] Schricker – *Haß* § 108a Rn 1
[716] Grundsätzlich zur „Gewerbsmäßigkeit" im Hehlereitatbestand: BGHSt. 1, 383 ff.; AG Mainz CR 1989, 626 (627)
[717] Siehe Fn 649
[718] Handbuch des Urheberrechts – *Flechsig* § 90 Rn 92; Hildebrandt, S. 204; Weber, S. 255

ne Werke“ im Sinne von § 71 UrhG. Hinsichtlich der Tathandlung verweist § 108 Abs. 1 Nr. 2 UrhG auf § 71 UrhG und dieser wiederum auf die §§ 15-24 UrhG. Dies hat zur Folge, dass anders als bei Nr. 1 auch eine Verletzung des Ausstellungsrechts (§§ 15 Abs. 1 Nr. 3, 18 UrhG) sanktioniert wird. Nr. 3 nimmt Bezug auf „Lichtbilder“ nach § 72 UrhG, jedoch mit der Einschränkung, dass keine „[...] Erzeugnisse, die ähnlich wie Lichtbilder hergestellt werden [...]“, erfasst werden, da sie von Nr. 3 unerwähnt bleiben.

Nr. 4 dient dem Schutz der „ausübenden Künstler“, § 73 UrhG, „[...] die ein Werk vortragen oder aufführen oder bei dem Vortrag oder der Aufführung eines Werks künstlerisch mitwirken“. Ob der Vortrags- oder Aufführungsbegriff des § 108 UrhG mit dem des § 19 UrhG übereinstimmt ist umstritten. Während der BGH[719] die Frage bislang offen gelassen hat, ist die überwiegende Literatur[720] der Auffassung, dass die Begriffe nicht übereinstimmen, insbesondere auch Studiomusiker erfasst würden. Diese Auslegung sichert den praktischen Anwendungsbereich der Norm und entspricht der Intention des Gesetzgebers.[721] Hinsichtlich der Tathandlungen nimmt § 108 Abs. 1 Nr. 4 UrhG Bezug auf die §§ 74, 75 Abs. 1, Abs. 2 UrhG sowie § 76 Abs. 1 UrhG. Im Ergebnis entsprechen diese den in Bezug auf das Urheberrecht in §§ 15-17 sowie 19-22 UrhG geregelten Verwertungsrechten.[722] Ausgenommen sind wiederum die persönlichkeitsrechtlichen Befugnisse aus § 83 UrhG.

Nr. 5-7 pönalisiert unberechtigte Eingriffe in technische Leistungsschutzrechte. Tatobjekte sind „Tonträger“ (§ 16 Abs. 2 UrhG), „Funksendungen“ sowie „Bildträger“ oder „Bild- und Tonträger“. Die Tathandlungen werden in den §§ 85, 87, 94 und 95 UrhG beschrieben. Die Strafwürdigkeit der Verletzung technischer Leistungsschutzrechte wird bisweilen in Frage gestellt.[723]

Nr. 8 wurde eingefügt durch das IuKDG, um die Richtlinie 96/9/EG des Europäischen Parlamentes und Rates vom 11. März 1996 über den rechtlichen Schutz von Datenbanken umzusetzen.[724] Eine Legaldefinition des Datenbankbegriffs nimmt § 87a UrhG vor. Die Tathandlungen „vervielfältigen“, „verbreiten“ und „öffentlich wiedergeben“ sind in § 87b UrhG genannt und decken sich im Wesentlichen mit denen in § 15 Abs. 1 Nr. 1, 2, Abs. 2 UrhG in Bezug auf das Urheberrecht.

3.9.6.2.2 Schranken

Ebenso wie § 106 UrhG für das Urheberrecht verweist § 108 UrhG für die verwandten Leistungsschutzrechte auf die Schrankenbestimmungen des UrhG. Anders als dort gelten allerdings keine einheitlichen Schranken. § 108 Abs. 1 Nr. 1-3 UrhG unterliegen den Vorschriften des 1. Teils und damit auch den §§ 45 ff. UrhG. Das gleiche gilt grundsätzlich für Nr. 4, 5 und 7, jedoch mit zahlreichen Ausnahmen. Nr. 6 und 8 folgen speziellen Schrankenbestimmungen.

3.9.6.2.3 Ohne Einwilligung des Berechtigten

„Ohne Einwilligung des Berechtigten“ weisen wie bei § 106 UrhG auf ein tatbestand-

[719] BGH GRUR 1983, 22 (24) „Tonmeister I“
[720] Fromm/Nordemann – Hertin § 73 UrhG Rn 3; Schricker – Krüger, Urheberrecht, § 73 UrhG Rn 16
[721] Hildebrandt, S. 209
[722] Hildebrandt, S. 211
[723] Schack, Rn 741
[724] BT-Drs. 13/7934, S. 42 f.

sausschließendes Einverständnis oder eine rechtfertigende Einwilligung hin. Es ergeben sich keine Unterschiede zu § 106 UrhG[725], so dass auf die Darstellung oben verwiesen werden kann (siehe Kapitel 3.9.6.1.3).

3.9.6.2.4 § 108a UrhG – Gewerbsmäßigkeit

Es ergeben sich keine Unterschiede zu § 106 UrhG, so dass auf die Darstellungen dort (3.9.6.1.5) verwiesen werden kann.

3.9.6.2.5 Ergebnis zu §§ 108, 108a UrhG

Art. 10 Abs. 2 nimmt zum Schutzumfang verwandter Leistungsschutzrechte Bezug auf das RA und den WPPT. Letzterer wurde von der BRD zusammen mit dem WPPT ratifiziert.[726]Aus dem Tatbestand von § 108 UrhG ist ersichtlich, dass der deutsche Gesetzgeber einen umfassenden strafrechtlichen Schutz der Leistungsschutzrechte intendierte. Die Bestimmung wird von der Literatur daher auch als „perfektionische" Strafvorschrift ohne größere praktische Bedeutung kritisiert.[727] Dennoch sanktioniert § 108 UrhG nicht jegliche Beeinträchtigung von Leistungsschutzrechten. Dafür ist er jedoch nicht wie Art. 10 Abs. 2 an die einschränkenden Kriterien der „Gewerbsmäßigkeit" und der „Begehung mittels eines Computersystems" gebunden. Im Übrigen kann auf die Ausführungen zu § 106 UrhG verwiesen werden.

3.9.6.3 § 108b – Unerlaubte Eingriffe in technische Schutzmaßnahmen und zur Rechtewahrnehmung erforderliche Informationen

§ 108b UrhG sanktioniert bestimmte Eingriffe in technische Schutzvorrichtungen nach § 95a UrhG und zur Rechtewahrnehmung erforderliche Informationen nach § 95c UrhG. Alle Vorschriften wurden durch das „Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft"[728] eingefügt und dienen der Umsetzung von EU-Recht und der Art. 11 und 12 WCT sowie der Art. 18 und 19 WPPT.[729] Im Bereich digitalisierter Werke – etwa Audio-CDs, Computerspiele, DVD-Filme – liegt es auf der Hand, dass Kopierschutzmechanismen eine zentrale Funktion beim Schutz des geistigen Eigentums zukommt. Aufgrund der zum Teil nahezu wörtlichen Umsetzung[730] der einschlägigen Bestimmungen in den WIPO-Verträgen kann davon ausgegangen werden, dass das deutsche Urheberstrafrecht bzgl. technischer Schutzmaßnahmen jedenfalls nicht nennenswert hinter dem von Art. 10 geforderten Niveau zurückbleibt. Inhaltlich besteht eine starke Ähnlichkeit zum ZKDSG[731].

3.9.7 Bewertung Art. 10

Art. 10 intendiert im Gegensatz zum deutschen Urheberstrafrecht einen lückenlosen straf-

[725] Schricker – *Haß* § 108 UrhG Rn 11
[726] Siehe Kapitel 3.9.2.2.2.
[727] Fromm/Nordemann – *Vinck* § 108; Schricker – *Loewenheim* § 108 Rn 1; Weber, S. 382 ff.
[728] Siehe Fn 650.
[729] Dreier/Schulze – *Dreier* § 108b Rn 1, § 95a Rn 1, § 95c Rn 1; Handbuch des Urheberrechts – *Flechsig* § 90 Rn 118, *Peukert* § 34 Rn 3; § 35 Rn 1
[730] So auch: Dreier/Schulze – *Dreier* § 95a Rn 1
[731] Siehe Kapitel 3.5.4; Abgrenzung siehe: Dreier/Schulze – *Dreier* § 108b Rn 3; Handbuch des Urheberrechts – *Flechsig* § 90 Rn 119

rechtlichen Schutz des Urheberrechts und der verwandten Schutzrechte, schränkt diesen Anwendungsbereich jedoch durch die Merkmale der „Gewerbsmäßigkeit“ und der „Begehung mittels eines Computersystems“ ein. Insoweit liegt eine starke Ähnlichkeit zur zivilrechtlichen Schadensersatznorm des § 97 UrhG vor. In diesem Zusammenhang kommt Art. 10 Abs. 3 besondere Bedeutung dahingehend zu, als er den Unterzeichnerstaaten in beschränktem Umfang von Pflicht zur Begründung strafrechtlicher Verantwortlichkeit befreit, soweit „andere wirksame Abhilfen“ zur Verfügung stehen. Ausweislich der Erläuterungen kann es sich dabei auch um zivil- oder verwaltungsrechtliche Instrumentarien (engl. *„civil and/or administrative measures”*), wie § 97 UrhG, handeln. Die letzte Urheberrechtsnovelle, durch die eine Ratifikation der WIPO-Verträge vorbereitet wurde, ermöglicht eine weitere Annäherung des deutschen Urheberstrafrechts an Art. 10.

3.10 Artikel 11 – Versuch und Beteiligung[732]

(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um die vorsätzliche Beteiligung an der Begehung einer der nach den Artikeln 2 bis 10 festgelegten Straftaten mit dem Vorsatz, eine solche Straftat zu begehen, als Straftat nach ihrem innerstaatlichen Recht festzulegen.

(2) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um den Versuch der Begehung einer der nach den Artikeln 3 bis 5 sowie 7, 8, 9 Absatz 1 Buchstabe a und 9 Absatz 1 Buchstabe c festgelegten Straftaten als Straftat nach ihrem innerstaatlichen Recht festzulegen, wenn dieser Versuch vorsätzlich begangen wird.

(3) Jeder Staat kann sich das Recht vorbehalten, Absatz 2 ganz oder teilweise nicht anzuwenden.

3.10.1 Anwendungsbereich

Der Zweck dieser Vorschrift besteht darin, eine Versuchs- und Teilnahmestrafbarkeit in Bezug auf die in der Konvention definierten Tatbestände zu begründen. Abs. 1 regelt die vorsätzliche Teilnahme an einer vorsätzlichen Straftat. Abs. 2, der nach Abs. 3 im Rahmen eines Vorbehalts abbedungen werden kann, pönalisiert den vorsätzlichen Versuch einer Straftat nach Art. 3 bis 5 sowie 7, 8, 9 Abs. 1 lit. a) und 9 Abs. 1 lit. c).

3.10.2 Abs.1 – Beteiligung

Anders als das deutsche Strafrecht §§ 26 und 27 StGB differenziert Art. 11 Abs. 1 nicht zwischen „Anstiftung“ und „Beihilfe“. In objektiver Hinsicht wurden keine Beteiligungsvoraussetzungen geregelt. Subjektiv ist – wie im deutschen Recht – Doppelvorsatz bzgl. Beteiligung und Haupttat erforderlich. An dieser Stelle soll den Erläuterungen zufolge[733] die Verantwortlichkeit von Leitungs- und Zugangsprovidern[734], die keine Kenntnis von den übermittelten Inhalten haben, begrenzt werden. An eine abgestufte Verantwortlichkeit nach objektiven Kriterien wie beispielsweise in § 9 TDG wurde hier nicht gedacht.[735]

3.10.3 Abs. 2, 3 – Versuch

Ebenso wenig wurden objektive Kriterien für die von Abs. 2 vorgesehene Versuchsstrafbarkeit vorgesehen. Subjektiv ist nicht näher bestimmter Vorsatz erforderlich. Von einer allgemeinen Versuchstrafbarkeit wurde im Wesentlichen Abstand genommen, da der Versuch bestimmter Handlungen, beispielsweise des Anbietens oder Zugänglichmachens, vom Wortsinn als nahezu unmöglich erschien. Darüber hinaus wollten die Verfasser dem Umstand Rechnung tragen, dass viele Rechtssysteme keine generelle, sondern nur eine abgestufte Versuchsstrafbarkeit kennen. Abs. 3 ermöglicht, entweder überhaupt keine Versuchsstrafbarkeit anzuordnen oder diese auf einzelne Tatbestände oder Teile hiervon zu beschränken. Der Sinn und Zweck dieses Absatzes besteht darin, den Vertragsparteien einen Umsetzungsspielraum einzuräumen, um möglichst vielen Staaten die Ratifikation ohne grundlegende Veränderungen ihrer Rechtsordnungen zu ermöglichen.

---

[732] ER Ziff. 118-122
[733] ER Ziff. 119
[734] Zu den Begriffen: Hoeren/Sieber – *Sieber* 1 Rn 17
[735] ER Ziff. 119

3.10.4 Teilnahme und Versuch im deutschen Strafrecht

Die „Teilnahme“ untergliedert sich in Anstiftung und Beihilfe nach §§ 26 und 27 StGB. Der Grundsatz der limitierten Akzessorietät erfordert, dass der Haupttäter vorsätzlich und rechtswidrig gehandelt hat.[736] Seine Schuld kann dahinstehen. Die §§ 26 und 27 StGB erfüllen zweifellos die Anforderungen des Art. 11 Abs. 1, so dass bezüglich der Teilnahme kein Umsetzungsbedarf besteht.

Der Verbrechensversuch ist stets strafbar, §§ 22, 23 Abs. 1, 12 Abs. 1 StGB. In anderen Fällen kommt es darauf an, ob das Gesetz die Strafbarkeit des Versuchs ausdrücklich anordnet. Im Bereich der Computerkriminalität ist dies beispielsweise bei §§ 263a Abs. 2 iVm § 263, 269 Abs. 2 sowie 303a und 303b StGB der Fall. Aufgrund der von Art. 11 Abs. 3 vorgesehenen Möglichkeit, eine Versuchsstrafbarkeit gänzlich auszuschließen, können die Anforderung an eine Umsetzung erst bestimmt werden, nachdem sich der deutsche Gesetzgeber zum Vorbehalt des § 11 Abs. 3 erklärt hat.

[736] Lackner/Kühl – *Kühl* Vor § 25 Rn 9 ff.; Sch/Sch – *Cramer*/*Heine* Vorbem §§ 25 ff. Rn 23 ff.

3.11 Artikel 12 – Verantwortlichkeit juristischer Personen[737]

(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um sicherzustellen, dass eine juristische Personen für eine nach diesem Übereinkommen festgelegte Straftat verantwortlich gemacht werden kann, die zu ihrem Vorteil von einer natürlichen Person begangen wird, die allein oder als Teil eines Organs der juristischen Person handelt und innerhalb der juristischen Person eine Führungsposition auf folgender Grundlage innehat:

a) Befugnis zur Vertretung der juristischen Person,

b) Befugnis, Entscheidungen im Namen der juristischen Person zu treffen,

c) Kontrollbefugnis innerhalb der juristischen Person.

(2) Abgesehen von den in Absatz 1 bereits genannten Fällen trifft jede Vertragspartei die erforderlichen Maßnahmen, um sicherzustellen, dass eine juristische Person verantwortlich gemacht werden kann, wenn mangelnde Überwachung oder Kontrolle durch eine natürliche Person nach Absatz 1 es ermöglicht hat, dass eine in ihrem Auftrag handelnde natürliche Person eine nach diesem Übereinkommen festgelegte Straftat zum Vorteil der juristischen Person begeht.

(3) Vorbehaltlich der Rechtsgrundsätze der Vertragspartei kann die Verantwortlichkeit einer juristischen Person straf-, zivil- oder verwaltungsrechtlicher Art sein.

(4) Diese Verantwortlichkeit berührt nicht die strafrechtliche Verantwortlichkeit der natürlichen Personen, welche die Straftat begangen haben.

3.11.1 Anwendungsbereich

Art. 12 behandelt die Verantwortlichkeit juristischer Personen für Zuwiderhandlungen ihrer Repräsentanten und sonstigen Mitarbeiter gegen die Strafvorschriften der Konvention. Gemäß Abs. 3 kann die Verantwortlichkeit straf-, zivil- oder verwaltungsrechtlicher Natur sein. Jedenfalls muss sie die Verhängung „[...] wirksamer, angemessener und abschreckender [...] Sanktionen oder Maßnahmen [...]“ zulassen, Art. 13 Abs. 2. Um die nationalen Rechtsgrundsätze der Unterzeichnerstaaten soweit wie möglich berücksichtigen zu können, wurde Art. 12 Abs. 3 aufgenommen. Nach deutschrechtlichem Verständnis kommt jedenfalls keine zivilrechtliche Regelung in Betracht. Dies liegt daran, dass die Strafgewalt (*ius puniendi*) hier zu Lande als Teil der allgemeinen Staatsgewalt verstanden und die Regelung der Beziehung zwischen Staat und Privaten traditionell dem öffentlichen Recht (*ius publicum*) zugeordnet wird, zu dem auch das Strafrecht zählt.[738] Wie sich aus Abs. 3 ergibt, erfordert Art. 12 jedoch nicht die Schaffung einer Strafnorm im engeren Sinne (Justizstrafrecht).

Die Anerkennung der strafrechtlichen Verantwortung von Verbänden folgt einem internationalen, vor allem europäischen Trend. *De lege ferenda* wird versucht, Verbänden das Verhalten ihrer Mitarbeiter in Führungspositionen zuzurechnen, wenn diese Straftatbestände verwirklichen oder andere Mitarbeiter nicht ausreichend beaufsichtigen, so dass jene Straftaten verüben können. Eine Verantwortlichkeit von Verbänden ist in zahlreichen europäischen Ländern vorgesehen[739], dem Bußgeldrecht der EU[740] nicht fremd und in verschiedenen internationalen Abkommen der jüngeren Vergangenheit zu finden.[741] Hervorzuheben ist vor allem

[737] ER Ziff. 123-127
[738] Jescheck/Weigend § 2 I, S. 11
[739] Überblick bei KK/OWiG – *Rogall* § 30 Rn 233 ff.
[740] Art. 83 Abs. 2 EGV lit. a) iVm Art 81 Abs. 1, 82 EGV
[741] Übersicht bei: Lütolf, S. 96 ff.; Sch/Sch – *Cramer*/*Heine* Vorbem §§ 25 ff. Rn 121 ff.

das Übereinkommen zum strafrechtlichen Schutz der Umwelt des Europarats vom 04.11.1998 (ETS. Nr. 172), das in Art. 9 eine dem Art. 12 weitgehend entsprechende Vorschrift aufweist.

3.11.2 Tatbestand

Der objektive Tatbestand differenziert zwischen zwei Möglichkeiten, die Verantwortlichkeit eines Verbandes zu begründen: Nach Abs. 1 kann eine strafbare Handlung von einer der in Abs. 1 lit. a) bis c) aufgezählten Personen selbst begangen werden. Abs. 2 erfasst hingegen Verletzungen der Aufsichtspflicht, die Straftaten im Sinne der Konvention durch nachgeordnete Mitarbeiter zulassen.
Abs. 1 enthält vier Tatbestandsmerkmale. Es muss eine Straftat im Sinne der Konvention (1) zum Vorteil des Verbandes (2) durch eine Person in einer Führungsposition (3) begangen werden, die in Ausübung der ihr zustehenden Befugnisse (4) handelt. Straftaten im Sinne der Konvention erfassen auch die Beteiligung an einer fremden Tat. Eine Person in einer Führungsposition ist eine natürliche Person, die – wie ein Direktor – Leitungsmacht innehat.

Darüber hinaus verpflichtet Abs. 2 die Möglichkeit zu schaffen, Verbände zur Verantwortung zu ziehen, wenn die in Abs. 1 lit. a) bis c) genannten Personen ihre Aufsichtspflicht über nachgeordnete Mitarbeiter verletzen (1), die dann Straftaten im Sinne der Konvention (2) zum Vorteil des Verbandes begehen (3). Die unzureichende Überwachung muss kausal für die Begehung der Straftaten werden. Die Art und Intensität der Aufsichtspflicht bestimmt sich nach Faktoren wie der Art des Unternehmens, seiner Größe, Sicherheitsstandards sowie den üblichen Geschäftsgewohnheiten.[742] Eine generelle Pflicht zur Überwachung der Kommunikation der Mitarbeiter soll nicht begründet werden.[743] Die Norm ist nicht auf ISP anwendbar, auf deren Systemen Straftaten durch Kunden, Nutzer oder dritte Personen begangen werden, jedenfalls solange es nicht gleichzeitig Mitarbeiter des ISP sind, die innerhalb ihrer Befugnisse handeln.

Abs. 4 stellt klar, dass die Verantwortlichkeit juristischer Personen die der natürlichen Personen nicht berührt.

3.11.3 Vergleichbare Normen im deutschen Strafrecht

Das geltende deutsche Recht kennt keine Strafbarkeit von Verbänden mit eigener Rechtspersönlichkeit im engeren Sinne. Dies wurde bislang vor allem mit der Begründung abgelehnt, dass juristischen Personen die Schuldfähigkeit fehle.[744] Gemäß § 46 Abs. 1 S. 1 StGB ist nach dem Schuldprinzip (*nulla poena sine culpa*) die persönliche Vorwerfbarkeit das zentrale strafbegründende und strafbegrenzende Kriterium.[745] Die in der Strafe liegende sozialethische Missbilligung mache gegenüber einer leblosen Vermögensmasse oder gegenüber unbeteiligten Mitgliedern keinen Sinn.[746] Auch könne der Zugriff auf die aus Straftaten der Mitarbeiter erlangten Gewinne durch andere Mittel als durch Strafe realisiert werden (z.B. Einziehung nach §§ 74, 75; Verfall § 73 Abs. 3 StGB, § 29a Abs. 2 OWiG; Abführung des Mehrerlöses §§ 8, 10 Abs. 2 WiStG, usw.).[747] Zweifel bestünden darüber hinaus an ihrer Handlungs- und Straffähigkeit.[748]

[742] ER Ziff. 125
[743] ER Ziff. 125, 54
[744] Jescheck/Weigend, § 23 VII, S. 226
[745] Jescheck/Weigend, § 4 I, S. 23 f.; Lackner/Kühl – *Lackner* § 46 Rn 1; Sch/Sch – *Stree* § 46 Rn 8
[746] Jescheck/Weigend, § 23 VII, S. 227 f.
[747] Jescheck/Weigend, § 23 VII, S. 227 f.
[748] Jescheck/Weigend; § 23 VII, S. 227 S. 227; aA: KK/OWiG – *Rogall* § 30 Rn 10, 12

3.11.3.1 Geldbuße gegen juristische Personen und Personenvereinigungen – § 30 OWiG

Das Ordnungswidrigkeitenrecht gilt nach heutigem Verständnis als Strafrecht im weiteren Sinne. Bereits im Allgemeinen Preußischen Landrecht war eine Unterscheidung zwischen Kriminal-(Justiz-)strafrecht und Polizei- und Verwaltungsstrafrecht bekannt, die jedoch in das StGB von 1871 keinen Eingang fand. Stattdessen wurde eine Gruppe von Tatbeständen geschaffen, denen lediglich Bagatellcharakter zugesprochen wurde (§§ 360-370 StGB a.F.). Obwohl dieser Bereich mittlerweile formal aus dem Kernstrafrecht in das OWiG ausgelagert wurde, wird die Abgrenzung immer noch nach quantitativen Aspekten der Strafwürdigkeit vorgenommen. Ordnungswidrigkeiten fehle „[…] der Grad der Verwerflichkeit der Tätergesinnung, welche das schwere sozialethische Unwerturteil des Kriminalstrafrechts rechtfertige.“[749] Der EGMR hat im Fall „Öztürk“ die Einordnung des Ordnungswidrigkeitenrechts unter das Strafrecht im weiteren Sinne bestätigt, indem er Art. 6 EMRK, der das Verfahren in Strafsachen betrifft, auf das Verfahren wegen Ordnungswidrigkeiten anwendete.[750]

In diesem Kontext ermöglicht § 30 OWiG die Verhängung von Bußgeldern, wenn eine der in Abs. 1 Nr. 1-4 genannten Personen eine Straftat oder Ordnungswidrigkeit im Pflichtenkreis des Verbandes oder zum seinem finanziellen Vorteil begeht. Damit wird keine „einzelne Ordnungswidrigkeit“ bezeichnet, sondern vielmehr eine Verbandstäterschaft als Bestandteil eines allgemeinen Teils des Ordnungswidrigkeitenrechts begründet.[751]

3.11.3.1.1 Tatbestand

Gegen eine „juristische Person (jP)“ oder eine dieser gleichgestellten „Personenvereinigungen (PV)“ ist die Festsetzung einer Geldbuße zulässig. Juristische Personen sind alle Verbände, denen die Rechtsordnung eine eigene Rechtspersönlichkeit zuerkennt. Durch Abs. 1 Nr. 2 und Nr. 3 werden nicht rechtsfähige Vereine und Personenhandelsgesellschaften gleichgestellt.

Abs. 1 bestimmt einen abschließenden Personenkreis möglicher „Täter“.[752] Gemeinsam ist allen Personen, dass sie gesetzliche oder rechtsgeschäftliche Vertretungsmacht[753] für den Verband haben müssen. Es kommen also nicht nur Organe oder Organteile in Betracht. Bemerkenswert ist, dass die Norm hierdurch Einzelunternehmen begünstigt, weil aufgrund der Tat eines Prokuristen im Pflichtenkreis einer natürlichen Person keine Geldbuße festgesetzt werden könne.[754]

Die Vertreter müssen eine tatbestandliche, rechtswidrige und schuldhafte[755] Straftat oder OWi begehen (sog. Anknüpfungs- bzw. Bezugstat).[756] Kausal bedingt durch die Straftat oder OWi müssen „Pflichten“, welche die jP oder PV treffen, „verletzt“, oder die jP oder die PV „bereichert“ worden sein, wobei eine zukünftige Bereicherung genügt. Bei den genannten Pflichten handelt es sich vor allem um die auch in § 130 OWiG genannten Aufsichtspflich-

[749] Jescheck/Weigend, § 7 V, S. 56 ff.; zur Entstehung des Ordnungswidrigkeitenrechts: KK/OWiG – *Bohnert* Einleitung Rn 50 ff.
[750] EGMR NJW 1985, 1273 ff.
[751] KK/OWiG – *Rogall* § 30 Rn 2 mwN
[752] Göhler § 30 Rn 9
[753] Bohnert § 30 Rn 19; Göhler § 30 Rn 10 f.; KK/OWiG – *Rogall* § 30 Rn 51
[754] Göhler § 30 Rn 11
[755] BGH NStZ 1994, 346 (346);OLG Hamm wistra 2000, 393 (394)
[756] Bohnert § 30 Rn 7; Göhler § 30 Rn 15; KK/OWiG – *Rogall* § 30 Rn 71

ten.[757] Weitere betriebsbezogene Pflichten ergeben sich insbesondere aus verwaltungsrechtlichen Gesetzen, die die jP oder die PV beispielsweise als Arbeitgeber, als Gewerbetreibende, als Unternehmer, usw. betreffen. Letztendlich schränkt dieses Kriterium den Tatbestand nicht wirklich ein, denn auch sog. Allgemeinpflichten – z.B. Verkehrssicherung, Produkthaftung, usw. – treffen die jP bzw. die PV, wenn sie sich in ihrem Wirkungskreis entfalten.[758] Bei einer Bereicherung kommt es auf einen Vermögensvorteil der jP oder PV an. Da der Täter „als" Vertreter des Verbandes handeln muss, kommt es auf einen inneren Zusammenhang zwischen seiner Tat und dem Wirkungskreis der jP/PV an, der jedoch bei Bereicherungshandlungen nicht besonders eng sein braucht.[759]

Nur Handlungen des Täters in der Funktion eines „Organs, usw." werden erfasst. Dies liegt regelmäßig dann vor, wenn der Vertreter im Interesse des Verbandes und in Wahrnehmung dessen Angelegenheiten tätig wird. Dahinstehen kann jedoch, ob er seinen unternehmensinternen Zuständigkeitsbereich überschreitet, solange er sich noch im Geschäfts- bzw. Wirkungskreis der jP/PV bewegt.[760]

Das „Bußgeld", das nach pflichtgemäßem Ermessen verhängt werden „kann", beträgt abweichend von § 17 Abs. 1 OWiG bis zu 500.000 €, § 30 Abs. 2 Nr. 1 OWiG. Nach Abs. 2 S. 2 kann auch auf den Bußgeldrahmen der subsidiären Ordnungswidrigkeit zurückgegriffen werden, wenn dieser das Höchstmaß nach S. 1 übersteigt. Sofern es sich bei der Tat des Vertreters um eine Straftat nach § 298 StGB oder § 263 StGB handelt, kommt darüber hinaus der erhöhte Bußgeldrahmen der §§ 81 Abs. 2 S. 1, 81 Abs. 1 Nr. 1 GWB in Betracht, der Geldbußen bis zur dreifachen Höhe des erlangten Mehrerlöses erlaubt. Ein ähnliches Ergebnis ergibt sich durch den Verweis von § 30 Abs. 3 OWiG auf § 17 Abs. 4 OWiG.

3.11.3.1.2 Ergebnis zu § 30 OWiG

Der Anwendungsbereich von Art. 12 Abs. 1 ist auf Straftaten im Sinne der Konvention zum Vorteil einer juristischen Person begrenzt. § 30 OWiG lässt eine beliebige OWi oder Straftat genügen, wobei neben juristischen Personen auch nicht rechtrechtsfähige PV in Betracht kommen. Ebenso wenig muss die Zuwiderhandlung zum Vorteil der jP/PV gereichen, solange sie ihrem Pflichtenkreis zugeordnet werden kann. § 30 OWiG geht daher grundsätzlich über Art. 12 Abs. 1 hinaus. Inwieweit er im Übrigen die Vorgaben von Art. 12 Abs. 1 erfüllt, beurteilt sich nach dem eingangs dargestellten Maßstab der Art. 12 Abs. 3 und Art. 13 Abs. 2. Danach muss die Konventionsbestimmung nicht im Rahmen einer justizstrafrechtlichen Norm umgesetzt werden, solange die Verhängung „[...] wirksamer, angemessener und abschreckender [...] Sanktionen oder Maßnahmen [...]" ermöglicht wird. In Hinblick auf den oben dargestellten Bußgeldkatalog bestehen diesbezüglich keine ernsthaften Bedenken.

3.11.3.2 Verletzung der Aufsichtspflicht in Betrieben und Unternehmen – § 130 OWiG

§ 130 OWiG stellt einen Auffangtatbestand dar für den Fall, dass die Verletzung der Aufsichtspflicht nicht selbst bereits als bedingt vorsätzliche Täterschaft, Beteiligung an einer

[757] BGH wistra 1986, 111 (112) mit Anm. Göhler; Rspr. Übersicht bei Leube wistra 1987, 41 (44) zum Kartell-OWiG
[758] Göhler § 30 Rn 20; KK/OWiG – *Rogall* § 30 Rn 76 f.
[759] Bohnert § 30 Rn 38; Göhler § 30 Rn 27; KK/OWiG – *Rogall* § 30 Rn 84 ff.
[760] Göhler § 30 Rn 26; differenzierend: KK/OWiG – *Rogall* § 30 Rn 91

fremden Tat oder fahrlässige Nebentäterschaft zu qualifizieren ist.[761] Die Norm schützt nicht etwa ein abstraktes staatliches Ordnungsinteresse, sondern vielmehr die durch die einzelnen Straf- und Bußgeldvorschriften geschützten Rechtsgüter.[762]

3.11.3.2.1 Tatbestand

Der Täterkreis ist auf den Inhaber des Betriebs oder Unternehmens begrenzt. Es kann sich sowohl um eine natürliche als auch eine juristische Person handeln. Über § 9 OWiG erstreckt sich (entsprechend § 14 StGB) der Anwendungsbereich auf die für den Betriebsinhaber handelnden Personen.[763]

Die Tathandlung besteht im „Unterlassen der erforderlichen Aufsichtsmaßnahmen". § 130 OWiG stellt demnach ein echtes Unterlassungsdelikt dar.[764] Das erforderliche Maß wird vor allem durch die Beachtung der bestehenden Gebote und Verbote an den Inhaber des Betriebs bestimmt und ist daher vom jeweiligen Einzelfall abhängig. Maßgebliche Faktoren sind Unternehmensgröße, Überwachungsmöglichkeiten, Zuverlässigkeit des Personals, usw.[765] § 130 OWiG erfasst nur die Verletzung zumutbarer Aufsichtsmaßnahmen, denn nach richtiger Ansicht darf die Vorschrift nicht dazu führen, dass die Organisation eines Betriebs von staatlicher Seite gestaltet wird.[766]

Neben der Aufsichtspflichtverletzung durch den Betriebsinhaber ist als zweite Pflichtverletzung die Zuwiderhandlung gegen betriebsbezogene Pflichten erforderlich.[767] Beide Pflichten müssen durch verschiedene Personen verletzt werden.[768] Dadurch, dass der Gesetzgeber weder eine „rechtswidrige Tat" (§ 10 Abs. 1 Nr. 5 StGB) noch eine „mit Geldbuße bedrohte Handlung" voraussetzt, wird deutlich, dass in der Person des Handelnden weder eine ahndbare OWi noch eine strafbare Handlung vorliegen muss.[769] Durch diese Formulierung wird sichergestellt, dass auch Rechtsverstöße durch Betriebsangehörige erfasst werden, die nicht Normadressaten sind und daher keine tauglichen Täter darstellen.[770] Inwieweit objektive und subjektive Merkmale sowie Rechtswidrigkeit vorliegen müssen, ist im Einzelnen umstritten.[771] Die Betriebsbezogenheit der Pflichtverletzung beurteilt sich ähnlich wie im Rahmen von § 30 OWiG.[772]

Der Zusammenhang zwischen Aufsichtspflichtverletzung und Zuwiderhandlung besteht darin, dass bei „gehöriger Aufsicht" eine Verletzung betriebsbezogener Pflichten verhindert oder wesentlich erschwert worden wäre. *Göhler*[773] und *Rogall*[774] erblicken in dieser Formel eine Abschwächung des Kausalitätserfordernisse durch eine Rezeption der Risikoerhöhungslehre. Danach wäre eine Zuwiderhandlung bei gehöriger Aufsicht „verhindert" worden, wenn eine an Sicherheit grenzende Wahrscheinlichkeit dafür spreche, dass es bei Beachtung der Auf-

[761] Bohnert § 130 Rn 1; Göhler § 130 Rn 25 f.; zur Entstehungsgeschichte: KK/OWiG – *Rogall* § 130 Rn 7 ff.
[762] Göhler § 130 Rn 3a; KK/OWiG – *Rogall* § 130 Rn 14
[763] Göhler § 130 Rn 4 ff.
[764] Bohnert § 130 Rn 2; Göhler § 130 Rn 9; KK/OWiG – *Rogall* § 130 Rn 15
[765] Göhler § 130 Rn 10 ff.
[766] Göhler § 130 Rn 10; KK/OWiG – *Rogall* § 130 Rn 49
[767] Bohnert § 130 Rn 16; Göhler § 130 Rn 17; KK/OWiG – *Rogall* § 130 Rn 72 ff.
[768] Bohnert § 130 Rn 16
[769] Bohnert § 130 Rn 24; Göhler § 130 Rn 21; KK/OWiG – *Rogall* § 130 Rn 75
[770] Göhler § 130 Rn 21; KK/OWiG – *Rogall* § 130 Rn 76
[771] Bohnert § 130 Rn 25 f,; Göhler § 130 Rn 21; KK/OWiG – *Rogall* § 130 Rn 75 f.
[772] Göhler § 130 Rn 18; aA: KK/OWiG – Rogall § 30 Rn 73
[773] Göhler § 130 Rn 22
[774] KK/OWiG – *Rogall* § 130 Rn 97

sichtspflichten nicht zu der Zuwiderhandlung gekommen wäre.[775] Wenig geklärt ist dagegen, wann die Pflichtverletzung „wesentlich erschwert" wurde.[776] *Rogall*[777] legt eine Risikoverringerung um mehr als 25 % zu Grunde, ohne jedoch anzugeben, wie dieser Wert bestimmt werden solle.

Das Bußgeld beträgt bei vorsätzlichem Handeln im Höchstmaß 500.000 €, bei fahrlässigem gemäß § 17 Abs. 2 OWiG 250.000 €. Sowohl die vorsätzliche als auch die fahrlässige Aufsichtspflichtverletzung ist ahndbar. Der Vorsatz muss sich nicht auf die Zuwiderhandlung gegen Pflichten des Inhabers beziehen, da es sich hierbei um eine Bedingung der Ahndung handelt.[778]

3.11.3.2.2 Ergebnis zu § 130 OWiG

§ 130 OWiG korrespondiert mit Art. 12 Abs. 2. Im Unterschied zur Konvention verlangt das deutsche Ordnungswidrigkeitenrecht die schuldhafte (vorsätzliche oder fahrlässige) Verletzung einer Aufsichtspflicht, ohne jedoch auf eine bestimmte Zuwiderhandlungen beschränkt zu sein. Im Übrigen kann auf die Darstellungen in Kapitel 3.11.3.1.2 verwiesen werden.

3.11.4 Bewertung Art. 12

Art. 12 begründet eine vom Individualunrecht gesonderte Verbandsverantwortlichkeit für Zuwiderhandlungen der Repräsentanten und sonstigen Mitarbeiter einer juristischen Person gegen die Strafnormen der Konvention. Im deutschen Justizstrafrecht hat dies bislang wegen dogmatischer Bedenken vor allem in Bezug auf die Schuld-, Handlungs- und Straffähigkeit von Verbänden (noch) keinen Niederschlag gefunden.[779] *De lege ferenda* ist seit einigen Jahren jedoch im europäischen und internationalen Kontext eine Trendwende zu verzeichnen, die auch von Art. 12 aufgegriffen wird. Wie sich aus Art. 12 Abs. 3 ergibt, verlangt die Strafnorm der Konvention keine Transformation in nationales Kriminalstrafrecht, solange die Anforderungen aus Art. 13 Abs. 2 erfüllt werden können. Im Bereich der Wirtschaftskriminalität kommt dem erhöhten Bußgeldrahmen des GWB und des § 17 Abs. 4 OWiG bei Erzielung wirtschaftlicher Vorteile besondere Bedeutung zu. Im Ergebnis findet Art. 12 daher in §§ 30 und 130 OWiG eine weitgehende Entsprechung. Ein weiterer Ansatz, um dogmatische Schwierigkeiten im Rahmen der Verantwortlichkeit von Verbänden zu überwinden, wird in der Literatur im Maßregelrecht gesehen, das keine individuelle Schuld voraussetzt.[780] Im Einzelnen ist jedoch noch vieles umstritten, so dass eine Erörterung an dieser Stelle zu weit führen würde.

[775] KK/OWiG – *Rogall* § 130 Rn 99
[776] Göhler § 130 Rn 22a; KK/OWiG – *Rogall* § 130 Rn 100 f.
[777] KK/OWiG – *Rogall* § 130 Rn 99; aA: Göhler § 130 Rn 22a
[778] Göhler § 130 Rn 16a; KK/OWiG – *Rogall* § 130 Rn 103
[779] Jescheck/Weigend, § 23 VII, S. 228 f.; Schmitt, S. 28; kritisch: Tiedemann, Wirtschaftsstrafrecht AT, S. 146 f.
[780] Sch/Sch – *Cramer*/*Heine* Vorbem §§ 25 ff. Rn 128 mwN

3.12 Artikel 13 – Sanktionen und Maßnahmen[781]

(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um sicherzustellen, dass die nach den Artikeln 2 bis 11 festgelegten Straftaten mit wirksamen, angemessenen und abschreckenden Sanktionen bedroht werden, die Freiheitsentziehung einschließen.

(2) Jede Vertragspartei stellt sicher, dass juristische Personen, die nach Artikel 12 verantwortlich gemacht werden, mit wirksamen, angemessenen und abschreckenden strafrechtlichen oder nichtstrafrechtlichen Sanktionen oder Maßnahmen bedroht werden, die Geldsanktionen umfassen.

3.12.1 Anwendungsbereich

Art. 13 verpflichtet die Vertragsparteien „[...] wirksame, angemessene und abschreckende [...]“ Sanktionen und Maßnahmen für Verstöße gegen die Konvention vorzusehen. Insgesamt werden nur recht vage Aussagen getroffen, die den Parteien große Spielräume bieten. Abs. 1 erwähnt ausdrücklich, dass auch Freiheitsstrafe in Betracht kommt. Die Norm stellt es den Vertragsparteien frei, andere Sanktionen und Maßnahmen wie z.B. einstweilige Verfügungen, die Anordnung der Einziehung und des Verfalls usw. in Abhängigkeit der Schwere der jeweiligen Straftat vorzusehen.

3.12.2 Rechtsfolgen der Tat im deutschen Strafrecht

Die Rechtsfolgen einer Straftat werden im dritten Abschnitt des Allgemeinen Teils des StGB geregelt, §§ 38-76a StGB. Es bestehen keine Zweifel, dass sie den Anforderungen nach Art. 13 genügen, so dass kein weiterer Umsetzungsbedarf besteht.

[781] ER Ziff. 128-130

4 Verfahrensrecht

Kapitel II, Abschnitt 2 trägt die Überschrift „Verfahrensrecht“. Art. 14 definiert den Anwendungsbereich der Normen im 2. Abschnitt. Dieser umfasst nicht nur die in Abschnitt 1 beschriebenen Computerdelikte, sondern nach Art. 14 Abs. 2 lit. b) und c) alle Sachverhalte, in denen Computer als Tatmittel Verwendung finden sowie auf die Erhebung von Beweismitteln in elektronischer Form. Art. 15 enthält sehr allgemein gehaltene rechtsstaatliche Anforderungen in Bezug auf polizeiliche Eingriffsgrundlagen. Im Anschluss daran normieren die Art. 16-21 spezifische Befugnisnormen. Art. 22 betrifft die Gerichtsbarkeit im Sinne des internationalen Strafanwendungsrechts.

Die einzelnen Ermächtigungsgrundlagen sollen den besonderen Anforderungen im Bereich der Computerkriminalität Rechnung tragen. Wegen der Flüchtigkeit von Daten liegt ein Schwerpunkt in der Schaffung von Eilmaßnahmen, die die Sicherung von Beweisen in elektronischer Form erleichtern sollen, bevor beweiserhebliche Daten gelöscht oder verändert werden können. Wegen der eingeschränkten richterlichen Kontrolle in derartigen Fällen droht die Gefahr schwerer Grundrechtseingriffe. Diesbezüglich enthält Art. 15 (Bedingungen und Garantien) nur vage Bestimmungen zum Schutz der Betroffenen.

Im Einzelnen versucht Abschnitt 2 gemäß den Erläuterungen folgende Anforderungen zu erfüllen: Standardbefugnisse wie Durchsuchung und Beschlagnahme werden an die technischen Gegebenheiten angepasst. Neue Ermächtigungen wie die beschleunigte Sicherung von Daten, Art. 16, 17, wurden ergänzend geschaffen. Befugnisse in Bezug auf Telekommunikation wurden ausgeweitet, um auf ihrer Grundlage Daten im Übertragungsstadium abfangen zu können. Einige dieser Änderungen wurden bereits in der Empfehlung Nr. R (95) 13[782] diskutiert. Inhaltlich wird zwischen Inhalts-, Verbindungs- und Kundendaten, formal zwischen gespeicherten und im Übertragungsstadium befindlichen Daten unterschieden. Legaldefinitionen befinden sich zum Teil in Art. 1 sowie in Art. 18. Begrifflich orientierten sich die Verfasser am herkömmlichen Sprachgebrauch (z.B. Beschlagnahme und Durchsuchung) sowie an der in anderen internationalen Foren (z.B. *G8 High Tech Crime Subgroup*) verwendeten Terminologie.

4.1 Artikel 14 – Geltungsbereich verfahrensrechtlicher Bestimmungen[783]

(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um die Befugnisse und Verfahren festzulegen, die in diesem Abschnitt für die Zwecke besonderer strafrechtlicher Ermittlungen oder Verfahren vorgesehen sind.

(2) Soweit in Artikel 21 nicht eigens etwas anderes vorgesehen ist, wendet jede Vertragspartei die in Absatz 1 bezeichneten Befugnisse und Verfahren an in Bezug auf

a) die nach den Artikeln 2 bis 11 festgelegten Straftaten,
b) andere mittels eines Computersystems begangene Straftaten und
c) die Erhebung in elektronischer Form vorhandener Beweise für eine Straftat.

---

[782] *Recommendation of the Committee of Ministers to Member States Concerning Problems of Criminal Procedural Law Connected with Information Technology*; Online: http://cm.coe.int/ta/rec/1995/95r13.htm (01.03.2004)

[783] ER Ziff. 140-144

(3) a) Jede Vertragspartei kann sich das Recht vorbehalten, die in Artikel 20 bezeichneten Maßnahmen nur auf Straftaten oder Arten von Straftaten anzuwenden, die in dem Vorbehalt bezeichnet sind; die Reihe dieser Straftaten oder Arten von Straftaten darf nicht enger gefasst sein als die Reihe der Straftaten, auf die sie die in Artikel 21 bezeichneten Maßnahmen anwendet. Jede Vertragspartei prüft die Möglichkeit, einen solchen Vorbehalt so zu beschränken, dass die in Artikel 20 bezeichnete Maßnahme im weitesten Umfang angewendet werden kann.

b)[784] Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system

i) is being operated for the benefit of a closed group of users, and
ii) does not employ public communications networks and is not connected with another computer system, whether public or private,

that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.

b)[785] Soweit eine Vertragspartei aufgrund ihrer zum Zeitpunkt der Annahme dieses Übereinkommens geltenden Rechtslage nicht in der Lage ist, die in den Artikeln 20 und 21beschriebenen Maßnahmen in Bezug auf Kommunikationen innerhalb des Computersystems eines Dienstanbieters zu ergreifen, wenn dieses System

i) zu Gunsten einer geschlossenen Benutzergruppe betrieben wird und
ii) keinen Zugang zu einem öffentlichen Kommunikationsnetze besitzt und nicht mit einem anderen Computersystem, sei es einem öffentlichen oder privaten, verbunden ist,

kann die Vertragspartei sich das Recht vorbehalten, diese Maßnahmen auf derartige Kommunikationen nicht anzuwenden. Jede Vertragspartei prüft die Möglichkeit, einen solchen Vorbehalt so zu beschränken, dass die in den Artikeln 20 und 21 bezeichneten Maßnahmen in weitestem Umfang angewendet werden können.

4.1.1 Anwendungsbereich

Art. 14 Abs. 1 verpflichtet die Vertragsparteien, die im 2. Abschnitt folgenden Verfahrensbestimmungen und Befugnisnormen durch gesetzgeberische und andere Maßnahmen in nationales Recht umzusetzen.

Abs. 2 erweitert den möglichen Anwendungsbereich der prozessualen Bestimmungen in Abschnitt 2 erheblich. Nach lit. b) und c) sollen die Verfahrensbestimmungen und Befugnisse auf Delikte im Zusammenhang mit Computern im Allgemeinen bzw. auf jegliche Form elektronischer Beweismittel angewendet werden. Damit bezweckt Art. 14 einerseits einen Gleichlauf und eine Vereinheitlichung des formellen Rechts in Bezug auf die Beschaffung und das Sammeln von Computerdaten und sonstigen Daten. Andererseits wird als erklärtes Ziel der Konvention die generelle Zulassung von Beweisen in elektronischer Form in Strafverfahren deutlich.

4.1.2 Einschränkungen

Dieser umfassende Anwendungsbereich wird in dreifacher Hinsicht eingeschränkt:

[784] Ergänzung in „letzter Sekunde“, die von der Arbeitsübersetzung des BMJ nicht berücksichtigt werden konnte und daher an dieser Stelle im englischen Original wiedergegeben wird.
[785] Übersetzung durch den Verfasser.

Zum einen verweist Abs. 2 auf eine Einschränkung in Art. 21 Abs. 1. Dort ist vorgesehen, dass das Abfangen von Inhaltsdaten nur in Bezug auf eine Reihe schwerer Straftaten möglich ist, deren Bestimmung dem nationalen Gesetzgeber obliegt. Damit folgt Art. 21 dem Beispiel vieler Länder in Bezug auf das Abhören des gesprochenen Wortes. Dies darf nur in Fällen geschehen, in denen ein nicht völlig unbedeutender Verdacht in Bezug auf schwere Straftaten vorliegt. Diese einschränkende Voraussetzung will einen Ausgleich zwischen Datenschutz und staatlichem Eingriff in die Privatsphäre gewährleisten. Eben aus diesen Gründen ermöglicht Art. 21 Abs. 1, parallel zum Abhören des gesprochenen Wortes, das Abfangen von Inhaltsdaten auf bestimmte Katalogtaten zu beschränken.

Die zweite Einschränkung findet sich in Abs. 3 lit. a), der – an einer nicht zu erwartenden Stelle in der Konvention – einen Vorbehalt bzgl. der Umsetzung von Art. 20 und 21 ermöglicht. Dabei ist allerdings zu berücksichtigen, dass der Anwendungsbereich von Art. 20 nicht kleiner sein darf als der von Art. 21. Der Vorbehalt in Abs. 3 wurde aufgenommen, weil in vielen Rechtsordnungen Verbindungs- und Inhaltsdaten in Bezug auf Belange des Datenschutzes und der Verletzung der Privatsphäre gleich behandelt werden. Mit Hilfe des Vorbehalts kann der Eingriff in Verbindungsdaten auf die Fälle des Art. 21 beschränkt werden. Abs. 3 lit. a) Satz 2 ermutigt die Vertragsparteien, einen etwaigen Vorbehalt so restriktiv wie möglich zu gestalten. Dahinter steckt die Überlegung, dass Verbindungsdaten einerseits nicht dieselbe Sensibilität in Bezug auf Belange des Datenschutzes und den Schutz der Privatsphäre wie Inhaltsdaten aufweisen. Aus ihnen können die Inhalte der Kommunikation nicht entnommen werden. Andererseits haben die Ermittlungsbehörden ein erhebliches Interesse an den Verbindungsdaten, da diese oftmals die einzige Möglichkeit darstellen, in Netzwerken einen möglichen Täter zurückzuverfolgen.

In letzter Sekunde wurde auf den Wunsch zweier Delegationen[786] in Abs. 3 lit. b) eine dritte Einschränkung hinsichtlich der Art. 20 und 21 aufgenommen. Danach können sich Vertragsparteien in Bezug auf örtlich begrenzte Netzwerke, ohne Zugang zur Außenwelt über öffentliche Telekommunikationseinrichtungen, vorbehalten, die Art. 20 und 21 anzuwenden, wenn dies ihre zur Zeit der Annahme der Konvention geltende Rechtslage nicht zulässt. Gemeint sind damit vor allem betriebliche LANs (engl. *corporate networks*). Wenn der Benutzer fälschlicherweise annimmt, dass es sich um ein geschlossenes Netzwerk handele, soll er nach Ansicht der Verfasser der Konvention nicht von der Anwendung von Art. 20 und 21 verschont bleiben.

4.1.3 Vergleichbare Befugnisnormen im deutschen Strafverfahrensrecht

Die im Folgenden zu vergleichenden Befugnisse können sich aus Landes- und aus Bundesrecht ergeben. Dies hängt davon ab, welchem Bereich polizeilichen Tätigwerdens die in der Konvention dargestellten Bestimmungen zuzuordnen sind. Handelt es sich um Rechtsgrundlagen auf dem Gebiet der präventiven Gefahrenabwehr, läge die Gesetzgebungskompetenz nach Art. 70 GG bei den Ländern[787], so dass vor allem das Polizei- und Sicherheitsrecht der Länder für einen Vergleich in Betracht käme. Bei repressivem Tätigwerden der Ermittlungsbehörden, einschließlich der Aufgaben und Befugnisse im Ermittlungsverfahren[788], läge die Kompetenz nach Art. 74 Abs. 1 Nr. 1 GG beim Bund. Auf Grund der unterschiedlichen Gesetzgebungskompetenzen sind beide Aufgabenbereiche strikt zu trennen.

[786] Siehe Arbeitsübersetzung des BMJ, S. 18 Fußnote 6, ohne Angaben, welche Delegationen dies waren.
[787] BVerfGE 3, 407 (433); 8, 143 (150); 40, 261 (266); Jarass/Pieroth – *Pieroth* Art. 70 Rn 12
[788] Jarass/Pieroth – *Pieroth* Art. 74 Rn 8 f.; von Münch/Kunig – *Kunig* Art. 74 Rn 12, 19

In Abs. 2 lit. a) – c) ist bestimmt, dass die in Abschnitt 2 der Konvention dargestellten Befugnisse in Bezug auf die nach Art. 2-11 festgelegten Straftaten, andere mittels eines Computers begangene Straftaten sowie die Erhebung von Beweisen in elektronischer Form für eine Straftat angewendet werden sollen. Damit sind Tätigkeiten gemeint, deren Schwerpunkt im Bereich der Ermittlung und Verfolgung von Straftaten liegt. Überschneidungen zum Aufgabenbereich der Gefahrenabwehr, etwa wenn aus Ermittlungen bzgl. bereits verübter Straftaten Erkenntnisse gewonnen werden, die auch der Verhütung zukünftiger Straftaten dienen können, ändern an dieser grundsätzlichen Einordnung in den repressiven Bereich nichts.[789] Für den weiteren Gang der Untersuchung bedeutet dies eine Weichenstellung insofern, als die polizeilichen Befugnisse aus dem durch die Länder geregelten Gefahrenabwehr- und Sicherheitsrecht nicht weiter untersucht werden sollen.[790] Zur Verfolgung von Straftaten können sich die Ermittlungsbehörden vor allem auf die §§ 94 StPO stützen, die im Folgenden mit den Befugnissen der Konvention kontrastiert werden.

4.1.4 Bewertung Art. 14

Anders als die meisten materiellrechtlichen Bestimmungen der Konvention, vor allem im Bereich des Sanktionsrechts, Art. 12, oder des Strafanwendungsrechts, Art. 22, zielen die verfahrensrechtlichen Normen auf eine grundlegende Änderung der Rechtsordnungen der Vertragsstaaten ab, indem sie Geltung nicht nur für die Tatbestände der Konvention, sondern auch für die Computerkriminalität im Allgemeinen, Art. 14 Abs. 2 lit. b), und noch darüber hinaus für alle Beweismittel in elektronischer Form, Art. 14 Abs. 2 lit. c), beanspruchen. Die Möglichkeit eines Vorbehalts ist nur für die „Echtzeiterhebung“ von Inhalts- und Verbindungsdaten nach Art. 20 und 21 vorgesehen. Weitere Einschränkungen können sich allerdings aus Art. 15 ergeben, der eine vage Absichtserklärung hinsichtlich Schutzmechanismen („Bedingungen und Garantien“) für die von den Maßnahmen Betroffenen enthält. In diesem Zusammenhang ist von Bedeutung, dass die Cybercrime-Konvention von Deutschland noch nicht ratifiziert wurde. Zur Geltung im Hoheitsgebiet der BRD bedarf es eines Zustimmungsgesetzes nach Art. 59 Abs. 2 GG (siehe Kapitel 1.4), das selbst den Anforderungen des Grundgesetzes genügen muss. Insofern stellt sich die Frage, inwieweit die nachfolgend zu erörternden Befugnisse mit bestehenden Rechtsprinzipien vereinbar sind.

[789] Eingehend zur Abgrenzung: Germann, S. 239 ff.
[790] Zu präventivpolizeilichem Tätigwerden: German, S. 239 ff.; Greiner, Die Verhinderung verbotener Internetinhalte im Wege polizeilicher Gefahrenabwehr

4.2 Artikel 15 – Bedingungen und Garantien[791]

(1) Jede Vertragspartei stellt sicher, dass für die Schaffung, Umsetzung und Anwendung der in diesem Abschnitt vorgesehenen Befugnisse und Verfahren Bedingungen und Garantie ihres innerstaatlichen Rechts gelten, die einen angemessenen Schutz der Menschenrechte und Freiheiten einschließlich der Rechte vorsehen, die sich aus ihren Verpflichtungen nach dem Übereinkommen des Europarats zum Schutz der Menschenrechte und Grundfreiheiten (1950), dem Internationalen Pakt der Vereinten Nationen über bürgerliche und politische Rechte (1966) und anderen anwendbaren völkerrechtlichen Übereinkünften über Menschenrechte ergeben und zu denen der Grundsatz der Verhältnismäßigkeit gehören muss.

(2) Diese Bedingungen und Garantien umfassen, soweit dies in Anbetracht der Art der betreffenden Befugnis oder des betreffenden Verfahrens angebracht ist, unter anderem die Kontrolle dieser Befugnis oder dieses Verfahrens durch ein Gericht oder eine andere unabhängige Stelle, die Begründung der Anwendung und eine Begrenzung im Hinblick auf den Umfang und die Dauer dieser Befugnis oder dieses Verfahrens.

(3) Soweit dies mit dem öffentlichen Interesse, insbesondere mit der ordnungsgemäßen Rechtspflege, vereinbar ist, berücksichtigt eine Vertragspartei die Auswirkungen der in diesem Abschnitt vorgesehenen Befugnisse und Verfahren auf die Rechte, Verantwortlichkeiten und berechtigten Interessen Dritter.

4.2.1 Anwendungsbereich

Art. 15 trägt dem Umstand Rechnung, dass das Völkerrecht bezüglich Eingriffen in die Rechte Privater nur Vorgaben machen kann, die dann, innerhalb der Grenzen der jeweiligen innerstaatlichen Rechtsordnung, von den nationalen Gesetzgebern umgesetzt werden.[792] Neben dem allgemeinen Aufruf an die Vertragsstaaten, ihre nationalen Menschen- und Freiheitsrechte sowie sonstigen Rechtsprinzipien zu berücksichtigen, besteht die wesentliche Bedeutung von Art. 15 darin, ein Mindestschutzniveau für die von Ermittlungsmaßnahmen[793] Betroffenen durch die Bezugnahme auf internationale Übereinkünfte und den Grundsatz der Verhältnismäßigkeit zu begründen. Im Spannungsverhältnis zwischen dem staatlichem Strafverfolgungsinteresse einerseits und den Menschen- und Freiheitsrechten andererseits, insbesondere der Informationsfreiheit und dem Recht auf Schutz der Privatsphäre, erschien es den Verfassern auf Grund der unterschiedlichen Rechtsordnungen der Unterzeichnerstaaten unmöglich, Detailregelungen zu finden, die in allen Vertragsstaaten gleichermaßen zur Anwendung kommen könnten.

4.2.2 Schutzmechanismen

Der durch Art. 15 intendierte Schutz der Menschen- und Freiheitsrechte ruht im Wesentlichen auf zwei Säulen:

Zum einen wird er dadurch gewährleistet, dass Abs. 1 auf die Verpflichtungen der Vertragsstaaten zum Schutz der Menschenrechte und Grundfreiheiten aus internationalen Abkommen verweist. Dabei handelt es sich um das Übereinkommen des Europarats zum Schutz der Menschenrechte und seine Zusatzprotokolle[794], das vor allem für die europäischen Vertragsstaaten von Bedeutung ist, und andere völkerrechtliche Übereinkommen zum Schutz der Menschen-

[791] ER Ziff. 145-148
[792] Kugelmann DuD 2001, 215 (218)
[793] Art. 15 bezieht sich nach seinem Abs. 1 lediglich auf die Befugnisse des 2. Abschnitts, d.h. Art. 16-21.
[794] ETS Nr. 004, 009, 046, 114, 117 und 177; EuR: http://conventions.coe.int/ (01.03.2004)

rechte, wie beispielsweise das Amerikanische Menschrechtsübereinkommen[795] aus dem Jahr 1969 oder die Afrikanische Menschen- und Bürgerrechtscharta[796] von 1981, sowie der häufiger ratifizierte Internationale Pakt der Vereinten Nationen über bürgerliche und politische Rechte[797] aus dem Jahr 1966. Der Verweis gilt jeweils nur in Bezug auf Vertragsstaaten dieser Übereinkommen und im Rahmen ihrer dort übernommenen Verpflichtungen.

Zum anderen soll ein Mindestschutz durch die Bezugnahme auf den allgemeinen „Verhältnismäßigkeitsgrundsatz" (engl. *principle of proportionality*) gewährleistet werden. Für die europäischen Vertragsstaaten ergibt sich dieser bereits aus der EMRK und der damit in Zusammenhang stehenden Rechtsprechung.[798] Vereinfacht gesprochen bedeutet „Verhältnismäßigkeit" im Sinne der Konvention, dass Befugnisse und Verfahrensbestimmungen und ihre Umsetzung im Einzelfall proportional zur Natur und den Umständen der Zuwiderhandlung sein sollen. Zum Teil ist dieser Grundsatz bereits in die Konvention integriert, wie sich etwa am Straftatenkatalog des Art. 21 zeigt.

Abs. 2 nennt exemplarisch („unter anderem") die Kontrolle durch ein Gericht oder eine andere unabhängige Stelle, die Begründung der Maßnahme sowie ihre Begrenzung im Hinblick auf Umfang und Dauer dieser Befugnis, ohne damit e contrario die von Art. 15 vorgesehenen Schutzmechanismen auf diese Fälle zu beschränken.[799] Es bleibt dem nationalen Gesetzgeber überlassen, zu entscheiden, bei welchen Maßnahmen die Eingriffintensität ein Maß erreicht, das die Einbindung bestimmter Bedingungen und Garantien erfordert.[800]

Abs. 3 sieht in der deutschen Übersetzung vor, dass die Interessen Dritter berücksichtigt werden müssen, soweit vorrangige öffentliche Interessen, vor allem an einer ordnungsgemäßen Rechtspflege, der öffentlichen Sicherheit und Gesundheit usw. nicht entgegenstehen. Für ein Ermessen in Bezug auf die Einbeziehung privater Belange in die Interessenabwägung finden sich keine Anhaltspunkte. Im englischen Original heißt es dagegen: „*[…] a Party shall consider […]*", was einen Spielraum für den nationalen Gesetzgeber andeutet, denn anderenfalls müsste es lauten: „*[…] a Party considers […]*". Eine von den Verfassern nur als fakultativ intendierte Einbeziehung privater Interessen in die Abwägung mit öffentlichen Strafverfolgungsinteressen wird weiter untermauert durch die Materialien zu Art. 15, die ausführen, dass eine Vertragspartei andere Interessen berücksichtigen sollte (engl. „*[…] Parties should consider other interests […]*"). Im Ergebnis kann daher mit hoher Wahrscheinlichkeit von einer Ungenauigkeit in der deutschen Übersetzung ausgegangen werden. Als relevante private Belange nennt der Erläuternde Bericht das Interesse an der Minimierung der Beeinträchtigung privater Verbraucherdienste, den Schutz vor Haftung der Anbieter wegen der Weitergabe von Kundendaten an die Ermittlungsbehörden oder Belange von Eigentümern.[801]

4.2.3 „Bedingungen und Garantien" im Grundgesetz

Da die Cybercrime-Konvention als völkerrechtlicher Vertrag der Inkorporation in nationales

[795] *Organization of American States* (OAS): http://www.oas.org/juridico/english/Treaties/b-32.htm (01.03.2004)
[796] Online: http://www.africa-union.org/Official_documents/Treaties_%20Conventions_%20Protocols/Banjul%20Charter.pdf (01.04.2004)
[797] Online: http://www.auswaertiges-amt.de/www/de/infoservice/download/pdf/mr/zivilpakt.pdf (01.04.2004); In der BRD am 23.03.1976 in Kraft getreten, BGB. 1973 II, S. 1533 ff.; BGBl. 1976 II, S. 1068
[798] Beispielsweise im Verbot unangemessen langer Untersuchungshaft, Art. 5 Abs. 3 EMRK, dazu Krey JA 1983, 638 (639); Urteil des EGMR vom 15.07.1982 im Fall „Eckle", EuGRZ 1983, 371 ff.
[799] ER Ziff. 147
[800] ER Ziff. 147, 148
[801] ER Ziff. 148

Recht bedarf, bevor sie unmittelbare Wirkung entfalten kann, und der Gesetzgeber gemäß Art. 20 Abs. 3 GG an die verfassungsmäßige Ordnung gebunden ist, kommen den „Garantien“ im Grundgesetz bei einem Vergleich zentrale Bedeutung zu. Wie sich aus Art. 15 Abs. 1 und Abs. 2 ergibt, versteht die Konvention unter „Garantien und Bedingungen“ nicht nur Mechanismen, die nach deutschem Verständnis den Grundrechten in den Art. 1 bis 19 GG sowie den Art. 101 und 103 GG entsprechen, sondern auch sonstige verfassungsrechtliche Anforderungen an das Strafrecht, wie den im Rechtsstaatsprinzip verankerten Verhältnismäßigkeitsgrundsatz. Die folgenden Ausführungen geben nur einen Überblick über die für besonders relevant erachteten „Garantien und Bedingungen“ im deutschen GG. Im Übrigen wird auf die angegebene Literatur verwiesen.

4.2.3.1 Schutz der Privatsphäre

Der Schutz der Privatsphäre wird im Grundgesetz im Wesentlichen durch das Zusammenspiel der Art. 13, 10 und 2 Abs. 1 iVm 1 Abs. 1 GG (in der Ausprägung des Allgemeinen Persönlichkeitsrechts und des Rechts auf informationelle Selbstbestimmung) gewährleistet. Beim Abhören von Datenübertragungen, die mit Hilfe öffentlicher Fernmeldeanlagen übertragen werden („Internet“), ist vorrangig das Fernmeldegeheimnis betroffen.[802] Art. 13 GG bleibt daneben nur anwendbar bei Zugriffen der Ermittlungsbehörden in den räumlich gegenständlichen Wohnungsbereich, etwa im Rahmen einer Durchsuchung und/oder Beschlagnahme von Hardware. Das allgemeine Persönlichkeitsrecht wird in der Rechtsprechung des BVerfG als Generalklausel verwendet, um beispielsweise die Weitergabe von Akten[803] und ärztlichen Aufzeichnungen[804] zu beschränken oder die Privatsphäre gegen die Berichterstattung in den Medien zu schützen.[805] Im Bereich der Datennetze kann es bei der Weitergabe von Daten zwischen den Ermittlungsbehörden oder an sonstige Stellen eine eigenständige Rolle spielen. Ähnliche Bedeutung kommt dem Recht auf informationelle Selbstbestimmung zu, das in Kapitel 4.2.3.1.2 näher dargestellt wird.

4.2.3.1.1 Art. 10 Abs. 1 GG – Fernmeldegeheimnis

Art. 10 Abs.1 GG gewährleistet das Brief-, Post- und Fernmeldegeheimnis. Im Bereich der Datennetze ist insbesondere das Fernmeldegeheimnis bedroht. Der Schutzbereich der Norm umfasst den gesamten Bereich der Individualkommunikation durch unkörperliche Signale.[806] Neben der klassischen Telefon- und Telefaxkommunikation werden auch Datenübertragungen erfasst.[807] Insofern ist der Schutzbereich technologieoffen, so dass das Fernmeldegeheimnis auch als Grundrecht auf „unbeachtete Kommunikation“ bezeichnet werden kann.[808]

Nach zutreffender Ansicht bezieht sich der grundrechtliche Schutz nicht nur auf die Inhalte (Inhaltsdaten), sondern auch auf die äußeren Umstände (Verbindungsdaten), wie die beteiligten Personen, den Ort, den Zeitpunkt und die Dauer der Verbindung, usw. einer Nachrichten-

[802] BGH NStZ 1997, 247 (248); von Mangoldt/Klein/Starck – *Gusy* Art. 10 Rn 101
[803] BVerfGE 27, 344 ff. („Scheidungsakten“)
[804] BVerfGE 32, 373 ff. („Arztkartei“); 44, 353 („Suchtkranke“)
[805] BVerfGE 35, 202 ff. („Lebach“); 63, 131 („Gegendarstellung“)
[806] Ipsen, Rn 287; Jarass/Pieroth – *Jarass* Art. 10 Rn 6
[807] BGH NStZ 1997, 247 (247); BVerfGE 46, 120 (142); von Münch/Kunig – *Löwer* Art. 10 Rn 18
[808] 12. Tätigkeitsbericht des Bundesbeauftragten für Datenschutz, BT-Drs. 11/6458, S. 39

übermittlung.[809] Die Verbindungsdaten haben mit der Umstellung von analoger auf digitale Vermittlungstechnik durch die Deutsche Telekom an Bedeutung gewonnen, da sie nunmehr nach der Beendigung einer Verbindung ohne größeren Aufwand gespeichert werden können. Der erzeugte Datensatz enthält neben den Nummern der verbundenen Anschlüsse auch das Datum, die Uhrzeit und die Dauer der Verbindung(en) sowie die Art des in Anspruch genommenen Telekommunikationsdienstes.[810] Im Mobilfunkbereich erlauben Verbindungsdaten – auch sog. „stand-by"-Daten ohne eine bestehende Verbindung – überdies die Positionsbestimmung eines Teilnehmers. Die Speicherung von Verbindungsdaten stellt einen Eingriff in Art. 10 Abs. 1 GG dar.[811]

Umstritten ist, ob vom Fernmeldegeheimnis nur Daten während der Übermittlung erfasst werden, oder auch solche, die in einer Mailbox[812] „ruhen". Zum Teil wird die Übertragung von Daten unter Zwischenschaltung eines elektronischen Nachrichtenfachs als einheitlicher Vorgang bewertet, mit der Konsequenz, dass der grundrechtliche Schutz durch Art. 10 Abs. 1 GG bestünde.[813] Eine andere Ansicht differenziert zwischen drei voneinander unabhängig zu beurteilenden Übertragungsstadien.[814] In der verfassungsrechtlichen Literatur und Rechtsprechung wurde dieses Problem bislang nicht diskutiert. Aufgrund der Vielzahl unterschiedlicher Sachverhalte, die unter den Oberbegriff „Mailbox" subsumiert werden[815], erscheint eine generelle Aussage als unmöglich.

Darüber hinaus kommt es nicht darauf an, ob öffentliche oder private Anbieter die Infrastruktur für die Übertragung der Signale zur Verfügung stellen (Kabel-, Funknetze, usw.). Uneinigkeit besteht allerdings darüber, ob auch Übertragungen in geschlossenen Netzen (etwa LANs) geschützt sein sollen.[816] Dies würde ausgehend vom traditionellen Wortsinn des Begriffs „Fernmeldetechnik" eine erhebliche Ausweitung des Schutzbereichs von Art. 10 Abs. 1 GG bedeuten, denn bedingt durch technologische Neuerungen sind in den letzten Jahren eine erhebliche Anzahl privater Netze entstanden.[817] Letztendlich ist auch das, was landläufig als „Internet" bezeichnet wird, nichts anderes als ein „Zwischennetz" zwischen zahlreichen privaten, örtlich begrenzten Netzen.[818] Es wäre daher nur konsequent, das Fernmeldegeheimnis über den Leitungsweg „Internet", der sich zumeist der öffentlich zugänglichen Telekommunikationsinfrastruktur bedient, auch auf private Übermittlungswege auszudehnen.[819] Anderenfalls würde der Grundrechtsschutz, vor allen in heterogenen Netzwerken, dem Zufall überlassen bleiben.

Nach gefestigter Ansicht in Literatur und Rechtsprechung begründet Art. 10 Abs. 1 über die abwehrrechtliche Dimension hinaus eine objektive Schutzpflicht des Staates, die ihren Ausdruck beispielsweise in der Schaffung des § 202a StGB gefunden hat.[820] Nach der Privatisie-

[809] BHGSt 35, 32 = NStZ 1988, 142; BVerfGE 67, 157 (172); 85, 386 (396); KK – *Nack* § 100a Rn 2; OLG Köln NJW 1970, 1856 (1856); OLG Saarbrücken NStZ 1991, 386 mit Anm. Krehl; OVG Münster NJW 1975, 1335 (1335); Schmidt-Bleibtreu/Klein – *Schmidt-Bleibtreu* Art. 10 Rn 6; Welp NStZ 1994, 209 (209)
[810] Bericht des Bundesbeauftragten für den Datenschutz vom 27.01.1989: BT-Drs. 11/3932, S. 32 f.
[811] BVerfGE 100, 313 (366); Jarass/Pieroth – *Jarass* Art. 10 Rn 11; von Münch/Kunig – *Löwer* Art. 10 Rn 7
[812] Zum Begriff: Palm/Roy NJW 1996, 1791 (1791 f.)
[813] Überblick über den Streitstand und Nachweise in Kapitel 4.8.4.2
[814] KK – *Nack* § 100a Rn 7; Palm/Roy NJW 1996, 1791 (1793)
[815] Siehe Fn 814
[816] Bejahend: BAG NJW 1987, 674 (676); Dreier – *Hermes* Art. 10 Rn. 33; von Mangoldt/Klein/Starck – *Gusy* Art. 10 Rn 41
[817] Dreier – *Hermes* Art. 10 Rn 33
[818] Sachs – *Krüger/Pagenkopf* Art. 10 Rn 14a
[819] So: Dreier – *Hermes* Art. 10 Rn 33; aA: Sachs – *Krüger/Pagenkopf* Art. 10 Rn 14a; differenzierend: von Mangoldt/Klein/Starck – *Gusy* Art. 10 Rn 43; von Münch/Kunig – *Löwer* Art. 10 Rn 18
[820] BVerfGE 67, 157 (185); Ipsen, Rn 289

rung des Telekommunikationssektors bedurfte es der einfachgesetzlichen Vorschrift des § 85 Abs. 2 TKG, um nicht-staatliche Stellen zur Wahrung des zwischen Privaten und öffentlicher Gewalt bestehenden Fernmeldegeheimnisses zu verpflichten.[821]

Art. 10 wird nicht schrankenlos gewährt. Abs. 2 Satz 1 normiert einen einfachen Gesetzesvorbehalt.[822] Darauf basieren beispielsweise die §§ 99 ff. StPO, mit den für Datennetze wichtigen §§ 100a f. und 100g f. StPO.[823] Art. 10 Abs. 2 Satz GG enthält darüber hinaus eine sog. „Staatsschutzklausel", von der der Gesetzgeber durch das G 10 Gesetz vom 13. August 1968 Gebrauch[824] gemacht hat. Art. 10 Abs. 1 GG ist der entscheidungserhebliche Prüfungsmaßstab für das Abfangen nichtöffentlicher Datenübertragungen, solange dies nicht mit einem Betreten des durch Art. 13 GG geschützten räumlichen Bereichs verbunden ist.[825]

4.2.3.1.2 Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG – Recht auf informationelle Selbstbestimmung

Dem Wortlaut nach wird man ein „Recht auf informationelle Selbstbestimmung" im GG vergeblich suchen. Dies ist auch nicht weiter verwunderlich, da die Problematik der großflächigen Datenerhebung, -speicherung und -verarbeitung technologiebedingt erst vor etwa 20 Jahren aufkam. Das BVerfG leitete dieses Recht in der insoweit grundlegenden „Volkszählungsentscheidung"[826] aus dem allgemeinen Persönlichkeitsrecht ab und sprach ihm ohne Rücksicht auf seine fehlende Gesetzgebungszuständigkeit Grundrechtsrang zu.[827]

Der Schutzbereich dieses Grundrechts umfasst die Befugnis jedes Einzelnen, „[…] selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu entscheiden."[828] Dabei sind insbesondere solche Informationen gemeint, die geeignet sind, „die engere Persönlichkeitssphäre zu beeinträchtigen."[829] Abgewehrt werden kann damit zum einen die staatliche Erhebung personenbezogener Daten. Zum anderen begründet das Recht auf informationelle Selbstbestimmung zwar kein subjektives Recht, jedoch die objektive Rechtspflicht des Staates, durch gesetzgeberische Maßnahmen die beliebige Erhebung von Daten durch Private zu verhindern.[830] Im Bereich der Datennetze ist dieses Grundrecht vor allem bei der Erhebung, Verarbeitung und Speicherung von Verbindungs- und Inhaltsdaten von Bedeutung.[831] Dieses Grundrecht ist auf gesetzlicher Grundlage auf Grund überwiegender Allgemeininteressen einschränkbar.[832]

4.2.3.2 Art. 5 Abs. 1 Satz 1 GG – Meinungs- und Informationsfreiheit

Art. 5 Abs. 1 S. 1 GG schützt die Meinungs- und Informationsfreiheit. In der Rechtswissen-

[821] Sachs – *Krüger/Pagenkopf* Art. 10 Rn 26
[822] Jarass/Pieroth – *Jarass* Art. 10 Rn 17; von Mangoldt/Klein/Starck – *Gusy* Art. 10 Rn 64; von Münch/Kunig – Löwer Art. 10 Rn 27 ff.
[823] Dreier – *Hermes* Art. 10 Rn 62 f.; von Münch/Kunig – *Löwer* Art. 10 Rn 40; Sachs – *Krüger/Pagenkopf* Art. 10 Rn 32 ff.
[824] BGBl. 1968 I, S. 949 ff.
[825] BGH NStZ 1997, 247 (248); von Mangoldt/Klein/Starck – *Gusy* Art. 10 Rn 101
[826] BVerfGE 65, 1 ff.
[827] Kritisch daher: Ipsen, Rn 298; Jarass/Pieroth – *Jarass* Art. 2 Rn 32; Krause JuS 1984, 268 (268)
[828] BVerfGE 65, 1 (43)
[829] BVerfGE 54, 148 (153); 72, 155 (170)
[830] Ipsen, Rn 301; von Mangoldt/Klein/Starck – *Gusy* Art. 10 Rn 57; von Münch/Kunig – *Löwer* Art. 10 Rn 4
[831] Dreier – *Dreier* Art. 10 Rn 52; Ipsen, Rn 300; von Münch/Kunig – *Kunig* Art. 10 Rn 38
[832] BVerfGE 65, 1 (44) „Volkszählungsentscheidung"

schaft hat sich bislang noch kein einheitlicher Begriff der „Meinung“ herausgebildet.[833] Nach der Rechtsprechung des BVerfG ist grundsätzlich ein weiter Maßstab anzulegen.[834] Der Meinungsbegriff umfasst jedenfalls die Kundgabe von Werturteilen und Tatsachen. Ohne näher auf die Einzelheiten einzugehen, wird deutlich, dass Ermittlungs- und Verfolgungsmaßnahmen in Computernetzen die Freiheit, Meinungen zu äußern und zu verbreiten, beeinträchtigen können, wenn Nutzer diese wegen befürchteter Überwachungsmaßnahmen nicht mehr frei kundtun.[835]

Ähnlich verhält es sich mit der Informationsfreiheit, deren Schutzbereich die ungehinderte Unterrichtung aus allgemein zugänglichen Quellen umfasst. „Allgemein zugänglich“ sind Informationsquellen dann, wenn „sie technisch geeignet und bestimmt sind, der Allgemeinheit, d.h. einem individuell nicht bestimmbaren Personenkreis, Informationen zu verschaffen“.[836] „Allgemein zugänglich“ sind daher auch weite Bereiche des Internets, soweit sie nicht durch Passwörter oder ähnliche Mechanismen für eine bestimmte Benutzergruppe (z.B. örtlich begrenzte Teilnetze oder einzelne WWW-Seiten) abgegrenzt sind.[837] Durch Rechtsvorschriften und andere staatliche Maßnahmen kann der Charakter der allgemeinen Zugänglichkeit nicht verändert werden, da anderenfalls der Staat, gegen den sich die Grundrechte als Abwehrrechte richten, den Schutzbereich einschränkend definieren könnte.[838] Ein Eingriff liegt dann vor, wenn die Informationsaufnahme verboten oder einem Erlaubnisvorbehalt unterworfen wird; im Bereich der Computernetze, wenn Ermittlungs- oder Verfolgungsmaßnahmen den Zugriff auf bestimmte Quellen im Netz beeinträchtigen.

Die Meinungs- und die Informationsfreiheit sind nach Art. 5 Abs. 2 GG durch die Vorschriften der allgemeinen Gesetze, die gesetzlichen Bestimmungen zum Schutze der Jugend sowie durch das Recht der persönlichen Ehre beschränkbar. Da die Cybercrime-Konvention überwiegend dem Bereich des Strafrechts zuzuordnen ist, ist entscheidend, inwieweit Normen des Strafrechts allgemeine Gesetze darstellen. In der Rechtsprechung des BVerfG hat sich die Formel etabliert, dass ein Gesetz dann allgemein sei, „wenn es sich nicht gegen die Äußerung einer Meinung als solche richtet, sondern vielmehr dem Schutz eines schlechthin, ohne Rücksicht auf eine bestimmte Meinung zu schützenden Rechtsgut, dient“.[839] In diese Richtung weist auch die wohl herrschende Sonderrechtslehre, die die Allgemeinheit von Gesetzen dann bejaht, wenn sie sich nur reflexiv auf die Kommunikationsfreiheiten auswirken.[840] Für strafrechtliche Normen bedeutet dies, dass sie überwiegend allgemeine Gesetze darstellen.[841] Wie im bereits geltenden deutschen Strafrecht ist eine Einzelfallbetrachtung[842] geboten, so dass an dieser Stelle keine pauschale Aussage für die Konvention getroffen werden kann.

[833] von Mangoldt/Klein/Starck – *Starck* Art. 5 Rn 23; von Münch/Kunig – *Wendt* Art. 5 Rn 8
[834] BVerfGE 61, 1 (9)
[835] Kugelmann TMR 2002, 14 (22)
[836] BVerfGE 27, 71 (83); 33, 52 (65); von Mangoldt/Klein/Starck – *Starck* Art. 5 Rn 45; von Münch/Kunig – *Wendt* Art. 5 Rn 23
[837] Ipsen, Rn 403, von Mangoldt/Klein/Starck – *Starck* Art. 5 Rn 45, die allerdings innerhalb des Internets nicht nach frei zugänglichen und abgetrennten Bereichen differenzieren.
[838] Ipsen, Rn 402; Jarass/Pieroth – *Jarass* Art. 5 Rn 16
[839] BVerfGE 7, 198 (209); 62, 230 (244); 71, 162 (175)
[840] Ipsen, Rn 443 mwN
[841] Ipsen, Rn 449; von Mangoldt/Klein/Starck – Starck Art. 5 Rn 186, 232 ff.; von Münch/Kunig – Wendt Art. 5 Rn 74
[842] Ipsen, Rn 449; von Mangoldt/Klein/Starck – Starck Art. 5 Rn 186, 232 ff.; von Münch/Kunig – Wendt Art. 5 Rn 74

4.2.3.3 Verhältnismäßigkeitsgrundsatz (Übermaßverbot)

Der Verhältnismäßigkeitsgrundsatz wird aus dem Rechtsstaatsprinzip hergeleitet. Dieses wiederum findet sich zwar nicht in den verfassungsrechtlichen Grundentscheidungen des Art. 20 GG, wird vom BVerfG jedoch aus einer „Zusammenschau der Bestimmungen des Art. 20 Abs. 3 GG über die Bindung der Einzelgewalten und der Art. 1 Abs. 3, 19 Abs. 4, 28 Abs. 1 Satz 1 GG sowie aus der Gesamtkonzeption des Grundgesetzes“[843] hergeleitet. Die genaue dogmatische Grundlage ist noch nicht geklärt.[844]

Inhaltlich bildet der Grundsatz der Verhältnismäßigkeit eine Schranke (Schranke-Schranke) für staatliche Eingriffe in Grundrechte und einfachgesetzliche subjektive Rechte. Er bindet alle staatliche Gewalt[845], sofern sie subjektive (bzw. subjektiv-öffentliche) Rechte des Bürgers zu schmälern droht. Vereinfachend gesprochen verlangt der Verhältnismäßigkeitsgrundsatz ein angemessenes Verhältnis zwischen Mittel und Zweck des staatlichen Eingriffs. Nach der heute herrschenden Meinung setzt sich das Übermaßverbot aus der Prüfung der Geeignetheit einer Maßnahme auf der ersten, der Erforderlichkeit auf der zweiten und der Angemessenheit (Verhältnismäßigkeit im engeren Sinne) auf der dritten Stufe zusammen.[846] Wegen der drohenden Eingriffsintensität kommt dem Übermaßverbot im Bereich des Strafrechts besondere Bedeutung zu.[847]

4.2.3.4 Justizgrundrechte – Art. 19 Abs. 4, 101 und 103 GG

Die Art. 19 Abs. 4, 101 und 103 GG können unter dem Oberbegriff „Justiz- bzw. Verfahrensgrundrechte“ zusammengefasst werden. Dies ist etwas missverständlich, da die genannten Artikel sich nicht nur an die Justiz, sondern – vor allem Art. 103 Abs. 2 GG – auch an den Gesetzgeber wenden. Im Einzelnen entfalten die Verfahrensgrundrechte folgende Schutzbereiche:

Art. 19 Abs. 4 GG garantiert den Rechtsweg, wenn jemand durch die öffentliche Gewalt in seinen Rechten verletzt wird. Der Begriff der „öffentlichen Gewalt“ wird zur Vermeidung eines unendlichen Instanzenzuges auf die vollziehende Gewalt im Sinne von Art. 20 Abs. 3 GG eingeschränkt.[848] Es genügt darüber hinaus, wenn der Kläger eine Verletzung subjektiver Rechte behauptet und diese zumindest als möglich[849] erscheint, denn über das tatsächliche Vorliegen der Rechtsverletzung sollen die Gerichte gerade erst entscheiden.[850] Die Rechtsweggarantie ermöglicht die Überprüfung staatlicher Verfahren oder Befugnisse, wie es auch Art. 15 Abs. 2 der Konvention vorsieht.

Art. 101 Abs. 1 GG nimmt die Forderung nach Kontrolle durch ein unabhängiges Gericht oder eine andere Stelle aus Art. 15 Abs. 2 auf. Gesetzlicher Richter im Sinne der Norm ist nur derjenige Richter, der in jeder Hinsicht – also vor allem in Hinblick auf Art. 97 Abs. 1 GG – den Anforderungen des Grundgesetzes entspricht.[851] Damit wird auch die Unabhängig-

[843] BVerfGE 2, 280 (403)
[844] Maurer, Staatsrecht I, § 8 Rn 4
[845] Jarass/Pieroth – *Jarass* Art. 20 Rn 81; Maurer, Staatsrecht I, § 8 Rn 55
[846] Jarass/Pieroth – *Jarass* Art. 20 Rn 83 ff.; bisweilen wird auch eine zwei- bzw. vierstufige Prüfung angenommen; für zwei Stufen: Maurer, Staatsrecht I, § 8 Rn 56; vier Stufen: Ipsen, Rn 171 ff.
[847] BVerfGE 90, 145 (172); Schroeder, Strafprozessrecht, Rn 106
[848] BVerfGE 10, 264 (267); Ipsen, Rn 832
[849] Dreier – *Schulze-Fielitz* Art. 19 Rn 56; Jarass/Pieroth – *Jarass* Art. 19 Rn 28
[850] Dreier – *Schulze-Fielitz* Art. 19 Rn 56; Ipsen, Rn 834; Jarass/Pieroth – *Jarass* Art. 19 Rn 28
[851] BVerfGE 3, 377 (381); 60, 175 (214); 82, 286 (298)

keit des Richters, der gemäß Art. 19 Abs. 4 GG gegen belastende Exekutivakte angerufen wird, verfassungsrechtlich verbürgt.

Art. 103 GG enthält grundsätzliche, rechtsstaatliche Gewährleistungen. Abs. 1 gibt einen Anspruch auf rechtliches Gehör. Abs. 2, der wörtlich durch § 1 StGB übernommen wurde, enthält das an den Gesetzgeber gerichtete Bestimmtheitsgebot[852] in Bezug auf den Tatbestand (*nullum crimen sine lege)* und die Strafandrohung (*nulla poena sine lege)* sowie das Verbot des rückwirkenden Erlasses von Strafgesetzen. An die Rechtsprechung adressiert beinhaltet dieser Absatz die Verbote, eine Verurteilung auf Gewohnheitsrecht oder eine Analogie zu Lasten des Täters zu stützen. Art. 103 Abs. 3 GG enthält schließlich das strafrechtliche Doppelbestrafungsverbot (*ne bis in idem*).

Soweit Art. 15 Abs. 2 nach einer Begründung und zeitlichen Begrenzung der Maßnahme verlangt, dürfte dies bereits Teil des Verhältnismäßigkeitsprinzips sein.

4.2.4 Bewertung Art. 15

Art. 15 enthält die vage Absichtserklärung, die Rechte der betroffenen Bürger zu schützen. Darüber hinaus dürfte die Norm keine weitergehende Bedeutung erlangen, da im zweistufigen völkerrechtlichen Rechtssetzungsverfahren die Transformation der Konvention in nationales Recht durch ein Zustimmungsgesetz des Bundestages erfolgen muss, das sich seinerseits an den grundgesetzlichen Vorgaben und damit unter anderem an den dargestellten Grundrechten messen lassen muss. Wünschenswert wäre statt dessen gewesen, Detailregelungen zum Datenschutz in die Konvention aufzunehmen.

[852] BVerfGE 75, 329 (342)

4.3 Artikel 16 – Beschleunigte Sicherung gespeicherter Computerdaten[853]

(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, damit ihre zuständigen Behörden die beschleunigte Sicherung bestimmter Computerdaten einschließlich Verbindungsdaten, die mittels eines Computersystems gespeichert wurden, anordnen oder in ähnlicher Weise bewirken können, insbesondere wenn Gründe zu der Annahme bestehen, dass bei diesen Computerdaten eine besondere Gefahr des Verlustes oder der Veränderung besteht.

(2) Führt eine Vertragspartei Absatz 1 so durch, dass eine Person im Wege der Anordnung aufgefordert wird, bestimmte gespeicherte Computerdaten, die sich in ihrem Besitz oder ihrer Verfügungsgewalt befinden, sicherzustellen, so trifft diese Vertragspartei die erforderlichen gesetzgeberischen und anderen Maßnahmen, um diese Person zu verpflichten, die Integrität dieser Computerdaten so lange wie notwendig für die Dauer von bis zu 90 Tagen zu sichern und zu erhalten, um den zuständigen Behörden zu ermöglichen, um deren Weitergabe zu ersuchen. Eine Vertragspartei kann vorsehen, dass diese Anordnung anschließend verlängert werden kann.

(3) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen oder anderen Maßnahmen, um den Verwahrer oder eine andere Person, welche die Computerdaten zu sichern hat, zu verpflichten, die Durchführung dieser Verfahren für den nach ihrem innerstaatlichen Recht vorgesehenen Zeitraum vertraulich zu behandeln.

(4) Die Befugnisse und Verfahren nach diesem Artikel unterliegen den Artikeln 14 und 15.

4.3.1 Anwendungsbereich

Art. 16 und 17 beinhalten strafprozessuale Befugnisnormen, die die Sicherung von Daten unabhängig vom zu Grunde liegenden Speichermedium ermöglichen. Damit erweitern sie vor allem die nationalen Durchsuchungs-, Beschlagnahme- und Herausgabebefugnisse, die üblicherweise nicht an den unkörperlichen Daten, sondern am stofflichen Datenträger ansetzen. In Bezug auf die Durchführung der Sicherung bleibt offen, ob eine passive Duldungspflicht der Betroffenen gegenüber Maßnahmen der Ermittlungsbehörden oder eine aktive Mitwirkungspflicht vor allem von Dienstanbietern begründet werden soll. Art. 16 und 17 beziehen sich auf bereits gespeicherte Daten, wie etwa bei einem Serviceprovider. Nicht gemeint ist der in die Zukunft gerichtete Vorgang der Erhebung und des Sammelns von Informationen (engl. *data retention*). In diesem Fall sind allein die Art. 20 und 21 einschlägig. Ein weiteres Charakteristikum der Art. 16 und 17 besteht darin, dass sie eine „beschleunigte" Sicherung von Daten erlauben. Dadurch wird der Flüchtigkeit von Daten Rechnung getragen, die eine Beweissicherung zur Durchführung eines Strafverfahrens erheblich erschwert. Darüber hinaus stoßen Sicherstellung und Beschlagnahme dort an ihre Grenzen, wo – etwa bei Datenübertragungen – kein körperlicher Datenträger präsent ist, der in Verwahrung genommen werden könnte. Schließlich soll die Effektivität der polizeilichen Ermittlungsarbeit dadurch gesteigert werden, dass Daten an den Schnittstellen der Übertragung in Netzwerken, bei den Dienstanbietern, erfasst werden können.

4.3.2 Beschleunigte Sicherung von Daten

Unter Sicherung von Daten versteht der Erläuternde Bericht, dass bereits existierende, gespeicherte Daten vor allen Einflüssen bewahrt werden, die ihren zum Zeitpunkt der Sicherung bestehenden Zustand verändern oder verschlechtern könnten. In Hinblick auf die Sicherungsmethoden ergeben sich weder aus dem Wortlaut des Art. 16 noch aus den Erläuterungen Beschränkungen auf bestimmte Verfahren. In der Praxis dürfte es sich vor allem um eine Si-

[853] ER Ziff. 158-164

cherung der Originaldaten handeln, indem Dritte von einem Zugriff ausgeschlossen werden, bzw. um die Anfertigung von Kopien mit identischem Inhalt.[854] Die Sicherung kann entweder gegen eine Person angeordnet werden und begründet damit eine aktive Mitwirkungspflicht oder „in ähnlicher Weise bewirkt werden". Die zweite Alternative soll den Unterzeichnerstaaten Flexibilität bei der Umsetzung von Art. 16 ermöglichen, indem sie die Sicherung beispielsweise durch eine Beschlagnahme oder eine Herausgabeanordnung des körperlichen Datenträgers bewirken können, ohne eine „neue" Spezialbefugnis in Bezug auf Computerdaten schaffen zu müssen.[855] Art. 16 erlaubt den Ermittlungsbehörden ausweislich der Erläuterungen keinen Zugriff auf den Inhalt der Daten, solange keine besondere Befugnisnorm, etwa im Zusammenhang mit einer Durchsuchung, sie dazu ermächtigt. Dadurch kann auch der Eilcharakter der Maßnahme gerechtfertigt werden, der durch den Begriff „beschleunigt" zum Ausdruck kommt. Zwar droht dann die Gefahr, dass keine ausreichende richterliche Überprüfung der Anordnungsvoraussetzungen vorgenommen werden kann. Solange die Ermittlungsbehörden nicht auf die Inhalte einer Kommunikation zugreifen können, ist die Eingriffsintensität jedoch begrenzt.

Die Befugnis zur Sicherung von Daten bezieht sich auf alle Arten von gespeicherten Daten, personenbezogene wie betriebliche, Inhalts-, Verbindungs- und sonstige Daten. Daten unterliegen insbesondere dann dem Zugriff der Ermittlungsbehörden, wenn eine „besondere Gefahr ihres Verlustes oder ihrer Beschädigung" besteht, etwa wenn sie – vor allem Verbindungsdaten – üblicherweise nur für kurze Zeit aufbewahrt werden oder wenn Zweifel an der Verlässlichkeit des Inhabers der Daten bestehen.

4.3.3 Sicherungszweck

Durch den Verweis in Abs. 4 auf Art. 14 wird deutlich, dass die Sicherung nur „[…] für die Zwecke besonderer strafrechtlicher Ermittlungen oder Verfahren vorgesehen ist." Damit soll die Maßnahme auf konkrete Ermittlungen im Einzelfall in Bezug auf Daten mit Beweiswert eingeschränkt werden. Eine weitere Beschränkung liegt darin, dass sich die Sicherungsanordnung immer auf bestimmte Daten „[…] im Besitz oder unter der Verfügungsgewalt einer Person […]" beziehen muss.

4.3.4 Dauer der Sicherung

Für die Dauer der Sicherung sieht Art. 16 Abs. 2 einen Zeitraum von bis zu 90 Tagen vor. Sie soll grundsätzlich lange genug sein, um den Ermittlungsbehörden durch die Anordnung weiterer Maßnahmen – wie Durchsuchung und Beschlagnahme – die Kenntnisnahme vom Inhalt der Daten zu ermöglichen.

Auf Belange des Datenschutzes geht die Konvention an dieser Stelle mit Ausnahme eines Verweises auf Art. 15 nicht weiter ein. Diesbezüglich sind für die europäischen Vertragsstaaten grundsätzlich die Richtlinien EG 46/95 und als „Detaillierung und Ergänzung"[856] im Bereich der Telekommunikation EG 66/97 von Bedeutung. Beide gelten jedoch nicht für „Tätigkeiten eines Staates im strafrechtlichen Bereich", Art. 3 Abs. 2 Spiegelstrich 1 EG 46/95, Art. 1 Abs. 2 EG 66/97, so dass es bei den jeweiligen nationalen Datenschutzbestimmungen bleibt.

[854] ER Ziff. 155
[855] ER Ziff. 160
[856] Art. 1 Abs. 2 Richtlinie 97/66/EG

4.3.5 Adressat der Sicherungsanordnung

Die Sicherungsanordnung kann gegen diejenigen Personen gerichtet werden, die „im Besitz der Daten sind oder Verfügungsgewalt an ihnen haben“. Grundsätzlich können daher sowohl beim Verdächtigen als auch bei Dritten, die vor allem im Übertragungsstadium eine Zugriffsmöglichkeit erlangen, Daten gesichert werden. Die Begriffe „Besitz“ und „Verfügungsgewalt“ stellen allein auf das natürliche Herrschaftsverhältnis über die Daten ab. Vor allem bei der Benutzung öffentlicher Telekommunikationsinfrastrukturen werden Daten der Nutzer bei den Telekommunikationsunternehmen gespeichert und können dort gesichert werden. Wenn eine Anordnung gegen Dritte ergeht, so werden diese durch Abs. 3 zum vertraulichen Umgang mit den Daten verpflichtet. Dies dient sowohl dazu, die Wirksamkeit der Ermittlungsmaßnahmen zu unterstützen als auch die Datenschutzbelange der Betroffenen zu wahren.

4.3.6 Grenzüberschreitende Sachverhalte

Bei grenzüberschreitenden Sachverhalten spielt Art. 29 eine besondere Rolle. Diese Vorschrift betrifft die zwischenstaatliche Rechtshilfe bei der beschleunigten Sicherung von Computerdaten. Art. 29 Abs. 7 sieht vor, dass eine Sicherung im Falle eines Ersuchens um Rechtshilfen für mindestens 60 Tage angeordnet werden soll, um der ersuchenden Vertragspartei ein Ersuchen um Durchsuchung oder ähnlichen Zugriff bzw. Beschlagnahme oder ähnliche Sicherstellung oder Weitergabe der Daten zu ermöglichen.

4.3.7 Vergleichbare Befugnisnormen im deutschen Strafprozessrecht

Die Zugriff auf beweiserhebliche Daten ist in der StPO mit Ausnahme von §§ 100g f. StPO nicht ausdrücklich geregelt. Stattdessen beziehen sich die Befugnisse der Strafverfolgungsbehörden – mit der genannten Ausnahme – auf gegenständlich verkörperte Beweisobjekte („Gegenstände“, „Papiere“). Dies ist auch nicht weiter verwunderlich, da die meisten Befugnisse, bis auf punktuelle Reformen, auf das vorletzte Jahrhundert zurückdatieren. Erst mit dem Übergang vom Industrie- ins Informationszeitalter gewann die unverkörperte Information in allen Lebensbereichen an Bedeutung. Diesem Wandel hat die StPO in Bezug auf die dadurch zur Verfügung stehenden Beweismittel bislang nur sehr zurückhaltend Rechnung getragen.

Die folgenden Darstellungen untersuchen die Frage, inwieweit die Sicherung von Daten durch die §§ 94 ff. StPO ermöglicht wird. In Betracht kommt vor allem das Erstellen von Sicherheitskopien, worin oft ein milderer Eingriff zur Beschlagnahme des ganzen Datenträgers gesehen wird. Die Frage, ob eine EDV-Anlage in Betrieb genommen werden darf, um darauf befindliche Dateien zu beschlagnahmen, stellt sich primär bei Durchsuchung und soll auch dort weiter behandelt werden. Auf §§ 100g f. StPO soll im Zusammenhang mit Art. 17 eingegangen werden, der die Verbindungsdaten aus dem Anwendungsbereich des Art. 16 herausgreift.

Die §§ 111b ff. StPO betreffen den Sonderfall der Sicherstellung bei Vorliegen der Verfalls- und Einziehungsvoraussetzungen nach §§ 73 ff. StGB und werden im Folgenden mangels Relevanz für Datennetzdelikte nicht näher erörtert werden.

4.3.7.1 § 94 StPO – [Sicherstellung von Beweisgegenständen]

§ 94 StPO ermöglicht die Sicherstellung von Beweisgegenständen und des Führerscheins zur

Einziehung. „Sicherstellung“ ist der Oberbegriff für die formlose Sicherstellung, Abs. 1, und die formell und inhaltlich den Anforderungen des § 98 StPO unterworfene Beschlagnahme.[857] Insofern ist die amtliche Überschrift des achten Abschnitts zu eng gehalten. Eine Beschlagnahme ist nur dann nötig, wenn der Gewahrsamsinhaber die Beweisgegenstände nicht freiwillig herausgibt. Im Übrigen setzt die Beschlagnahme keinen entgegenstehenden Willen des Sachinhabers voraus.[858]

4.3.7.2 Gegenstände als Beweismittel

§ 94 Abs. 1 StPO ermöglicht die Sicherstellung von Gegenständen, die als Beweismittel für die Untersuchung von Bedeutung sein können. Auf die Möglichkeit der Sicherstellung eines Führerscheins nach Abs. 3 wird im Folgenden nicht weiter eingegangen, da er für die Sicherung von Daten keine weitere Rolle spielt.

Da die StPO nur vier Beweismittel kennt – Zeugen, §§ 48-71 StPO, Sachverständige, §§ 72-85 StPO, Augenschein bzw. Augenscheinsobjekte, §§ 86-93 StPO, und Urkunden §§ 249-256 StPO –, von denen nur zwei dem sachlichen Bereich zugeordnet werden können, kommen auch nur Augenscheinsobjekte und Urkunden als Gegenstände einer Sicherstellung in Betracht. Daten stellen jedenfalls keine Urkunden dar, da sie, bevor sie nicht ausgedruckt werden, keine verlesbaren Schriftstücke im Sinne von § 249 StPO sind.[859] Auf den materiellrechtlichen Urkundenbegriff aus § 267 StPO kommt es nicht an, da dieser sich nicht mit dem verfahrensrechtlichen deckt.[860] Daten könnten jedoch Augenscheinsobjekte sein. Dazu müssten sie einer sinnlichen Wahrnehmung durch den Richter zugänglich sein.[861] Zweifellos trifft dies nicht für die Binärzeichen auf einer Magnetschicht einer Festplatte oder die Abfolge mikroskopisch kleiner Vertiefungen und Erhebungen (*„lands“* und *„pit“*) auf einem optischen Datenträger zu. Jedoch können diese Binärzeichen unter Zuhilfenahme entsprechender Soft- und Hardware sinnlich wahrnehmbar gemacht werden. Eben dies geschieht bei Schallplatten und Tonbändern, die in der höchstrichterlichen Rechtsprechung vereinzelt nicht nur als Augenscheinsobjekte über ihre äußere Beschaffenheit, sondern unter Einschränkungen[862] auch über ihren geistigen Inhalt betrachtet werden.[863] Konsequenterweise müsste dann auch der geistige Inhalt der Audioaufzeichnungen gesondert vom körperlichen Träger der Sicherstellung unterliegen, etwa durch Kopieren von Bändern oder dem Erstellen von Abschriften. Denn unter Verhältnismäßigkeitsgesichtspunkten wären die Ermittlungsbehörden gehalten, den Eingriff in die Rechte des Betroffenen so gering wie möglich zu halten.[864] Dies wäre ganz offensichtlich der Fall, wenn die Originale der Schallplatten und Tonbänder bei Adressaten der Maßnahme verbleiben könnten. Diese Frage wurde in den zitierten Urteilen jedoch nicht entschieden. Eine derartige Auslegung widerspricht auch dem natürlichen Wortsinn des „Gegenstands“-Begriffs. Aus einem Vergleich zu Audiobändern und Schallplatten lässt sich daraus keine Schlussfolgerung für die Sicherstellung von Computerdaten ziehen.

Jedoch ist es seit Bestehen der Reichsstrafprozessordnung üblich, Abschriften bzw. Fotokopien von Urkunden herzustellen. In diesem Fall ist noch nicht geklärt, ob es sich dabei um

[857] Löwe/Rosenberg – *Schäfer* § 94 Rn 3; Meyer-Goßner § 94 Rn 11
[858] Löwe/Rosenberg – *Schäfer* § 94 Rn 26
[859] Bär, S. 211; Eisenberg, Rn 2003, 2320, 2323; KK – *Nack* § 94 Rn 3; Löwe/Rosenberg – *Gollwitzer* § 249 Rn 7; aA: KK – *Diemer* § 249 Rn 27
[860] KK – *Diemer* § 249 Rn 9; Meyer-Goßner § 249 Rn 3; SK/StPO – *Schlüchter* § 249 Rn 9 ff.
[861] BGHSt 18, 51 (53) = NJW 1962, 2361; KK – *Senge* § 86 Rn 1; Meyer-Goßner § 86 Rn 2
[862] Siehe dazu Kapitel 4.6.6.1.1.
[863] BGHSt 14, 339 (341); 27, 135 (136)
[864] Siehe Kapitel 4.2.3.3; KK – *Nack* § 94 Rn 13; Löwe/Rosenberg – *Schäfer* § 94 Rn 35

eine Sicherstellung des „geistigen Inhalts“ der Urkunde[865], des körperlichen Originals[866], der körperlichen Abschrift/Fotokopie[867] oder aber um einen Sicherstellungsersatz[868] handele. Jedenfalls wird § 94 StPO unter Hinweis auf den Verhältnismäßigkeitsgrundsatz und ein „a maiore ad minus“-Argument als ausreichende Rechtsgrundlage betrachtet. Die bloße Kopie sei oft der mildere Eingriff, vor allem wenn es um die Sicherstellung von geschäftlichen Papieren gehe, deren Verbleib im Betrieb für die Weiterführung der Geschäfte erforderlich ist. Eine Ablichtung stelle ein Minus gegenüber der Wegnahme des körperlichen Originals dar, und sei daher von Sicherstellungsnormen gedeckt.[869] Aus dieser Parallele zu körperlichen Urkunden folgern große Teile der Lehre, dass das Kopieren von Daten zum Zweck ihrer Sicherstellung durch die §§ 94 ff. StPO gedeckt sei, da dies stets der mildere Eingriff sei und überdies ein Minus gegenüber der Wegnahme des Datenträgers darstelle.[870]

In der wissenschaftlichen Diskussion wurde bislang keine Kritik an dem Vergleich der Computerdatenträger mit den schriftlichen Urkunden geäußert. Bei genauerer Betrachtung ergibt sich folgende Bewertung:

Richtig ist, dass es bei der Sicherstellung von Datenträgern ähnlich wie bei der von Urkunden in der Regel um den gedanklichen Inhalt des Beweisgegenstandes geht.[871] Ausnahmsweise kommt es auf die äußere Beschaffenheit an, etwa im Zusammenhang mit Fingerabdrücken auf dem Beweisobjekt usw. Falsch ist jedoch, dass Computerdaten mit dem Substrat Datenträger ähnlich fest verbunden wären wie die Beschriftung einer Urkunde mit dem Trägermedium Papier.[872] Es besteht gerade kein untrennbarer Zusammenhang zwischen beweisrelevanter Information und Beweisgegenstand, so dass sich die Beweisbedeutung auch nicht auf den körperlichen Datenträger erstreckt.[873] Ganz im Gegenteil hat die moderne Computertechnik eine Loslösung des Beweisbezuges zwischen gedanklichem Inhalt und stofflichem Medium bewirkt, indem digitalisierte Information beliebig oft vervielfältigt und auf beliebigen, genormten Datenträgern manifestiert (gespeichert) werden können. Auf die Einheit „Speichermedium-Inhalt“ kann es umgekehrt nur dann ankommen, wenn im Strafverfahren Tatsachen in Bezug auf diese Verbindung in Frage stehen, etwa ob ein bestimmter Datenträger mit einer bestimmten Hardware beschriftet wurde.

Da es demnach keinen untrennbaren Beweisbezug zwischen Speichermedium und Daten gibt, sind die Sicherstellungsvoraussetzungen in Bezug auf die Daten – den gedanklichen Inhalt – und nicht in Bezug auf den Datenträger zu beurteilen.[874] Am Beispiel von Servern, die eine Vielzahl von Daten unterschiedlicher Nutzer „beinhalten“, zeigt sich besonders deutlich, dass die Gleichstellung von Urkunden mit Datenträgern nicht überzeugen kann. Wollen die Ermittlungsbehörden beispielsweise die Email eines Verdächtigen auf dem Server des Emailanbieters sicherstellen[875], dann besteht nur bzgl. dieser einen Nachricht der erforderliche[876] Anfangsverdacht. Eine Sicherstellung des Servers würde jedoch nicht nur die „verdächtige“

[865] Schäfer wistra 1989, 8 (12)
[866] Sieg wistra 1984, 172 (173); Koch wistra 1983, 63 (65)
[867] Löwe/Rosenberg – *Schäfer* § 94 Rn 48; OLG Hamburg NJW 1967, 166; OLG München NJW 1978, 601
[868] Meyer-Goßner § 94 Rn 16
[869] Bär, S. 270 ff.; Möhrenschlager wistra 1991, 321 (329); Schäfer wistra 1989, 8 (12)
[870] Bär, S. 271; Möhrenschlager wistra 1991, 321 (329); Schäfer wistra 1989, 8 (12)
[871] Siehe Fn 866.
[872] So aber: Bär, S. 247 f.; Roßnagel – *Bär* 7 Rn 106
[873] So aber: Bär, S. 247 f., Roßnagel – *Bär* 7 Rn 106 sowie Schäfer wistra 1989, 8 (11 f.)
[874] aA: Siehe Fn 873
[875] Zur Frage, ob in diesem Fall eine Sicherstellung oder eine Überwachung der Telekommunikation vorliegt: Kapitel 4.8.4.2
[876] Eisenberg, Rn 2324 mwN.

Nachricht erfassen, sondern eine Vielzahl anderer Emails unterschiedlicher Nutzer. Bei einer durchschnittlichen Mailboxgröße von 12 Megabyte[877] und einer theoretischen Serverkapazität von 500 GB[878], genau genommen über 42.500[879] anderer Nutzer. Dabei besteht Einigkeit in der wissenschaftlichen Diskussion, dass „Ausforschungs"-Sicherstellungen unzulässig sind[880], so dass sich die Maßnahme nur auf die beweisrelevante Nachricht beziehen darf. Dies ist offensichtlich bei dem Zugriff auf einen Email-Server und allgemein bei allen anderen Netzwerklaufwerken, die von einer Vielzahl von Nutzern gemeinsam genutzt werden, nicht gewährleistet. Bei Email-Servern kommt noch erschwerend hinzu, dass bislang nicht geklärt ist, ob auf sie nur unter den Voraussetzungen der §§ 100a f. StPO zugegriffen werden kann.[881]

Darüber hinaus kommt es beim staatlichen Zugriff auf einen vernetzten Server zu einer anderen Art des Rechtseingriffs als bei der Sicherstellung einer Urkunde. Wegen der großen Speicherkapazität moderner Computerdatenträger sind die Daten einer Vielzahl von Nutzern gefährdet. Schriftstücke beinhalten dagegen einen begrenzten gedanklichen Inhalt, der einem überschaubaren Personenkreis zugeordnet werden kann. Im diesem Zusammenhang drohen anders als im Zusammenhang mit Schriftstücken nicht gerechtfertige Eingriffe in das Recht auf informationelle Selbstbestimmung[882], und wegen der Nähe zur Telekommunikation, in das Fernmeldegeheimnis[883].

Aus diesen Gründen ist der Vergleich von Urkunden mit Computerdatenträgern nach der hier vertretenen Auffassung nicht tragfähig und abzulehnen. In Bezug auf Schriftstücke mag die Anfertigung von Kopien der mildere Eingriff sein, der daher von § 94 StPO gedeckt ist. Auf Computerdatenträger sind diese Erkenntnisse jedenfalls nicht übertragbar. Deshalb kommt es für Sicherstellung von Daten durch Anfertigen von Kopien auf die Tatbestandsvoraussetzungen des § 94 StPO in Bezug auf die gedanklichen Inhalte an. Daten sind danach keine Gegenstände und unterliegen nicht der Sicherstellung.[884] Diese Argumentation wird auch durch den Sinn und Zweck des Verhältnismäßigkeitsgrundsatzes getragen. Als Bestandteil des Rechtsstaatsprinzips dient er in erster Linie dazu, staatliche Eingriffe auf das im Einzelfall erforderliche Maß zu reduzieren, soweit die sonstigen Eingriffsvoraussetzungen vorliegen, und nicht den Anwendungsbereich einer Befugnisnorm über ihren Wortlaut auszudehnen.[885] An dieser Stelle zeigt sich die Reformbedürftigkeit der auf körperliche Gegenstände fixierten StPO, die dem Gesetzgeber und nicht dem Richter überlassen werden sollte.

4.3.7.3 Ablauf

Die Sicherstellung wird durch die Begründung eines amtlichen Verwahrungsverhältnisses oder in sonstiger Weise bewirkt. Bei der Beschlagnahme muss zuvor eine förmliche Anordnung nach § 98 StPO ergangen sein. Beide Fälle der Sicherstellung erfordern, dass über die Sache durch Inbesitznahme oder durch sonstige Maßnahmen ein amtliches Herrschaftsverhältnis begründet wird, durch das dem ursprünglichen Inhaber die (rechtliche) Verfügungs-

[877] Das Beispiel entspricht dem „Freemail"-Angebot des Anbieters „web.de", http://freemail.web.de/ (01.04.2004)
[878] Gängige PC Festplatten erreichen bereits über 100 GB und Server besitzen mehrere davon.
[879] 500 GB = 512.000 MB : 12 MB = 42.666,6
[880] Eisenberg, Rn 2324 mwN; Löwe/Rosenberg – *Schäfer* § 94 Rn 12; Meyer-Goßner § 94 Rn 6
[881] Siehe dazu Kapitel 4.8.4.2
[882] Siehe Kapitel 4.2.3.1.2
[883] Siehe Kapitel 4.2.3.1.1
[884] Ebenso: Möhrenschlager wistra 1991, 321 (329); Schnabl JURA 2004, 379 (382)
[885] Maurer, Staatsrecht I, § 8 Rn 55

gewalt über die Sache entzogen wird.[886] Der BGH hat in zwei Entscheidungen, die jeweils körperliche Gegenstände betrafen (Akten des Verteidigers), klar gestellt, dass diese Grundsätze sowohl für die Inverwahrnahme als auch für die Sicherstellung „in anderer Weise" gelten.[887]

Fraglich ist, ob die Sicherstellung bereits dann bewirkt ist, wenn die Ermittlungsbehörden eine Kopie der Daten anfertigen, und der ursprüngliche Datensatz und der Datenträger bei dem Maßnahmeadressaten verbleiben. Zweifel an einer Bewirkung der Sicherstellung bestehen insofern, als der Dateninhaber in seiner tatsächlichen Verfügungsmöglichkeit nicht beschränkt wird. Nach der Literatur soll es jedoch genügen, wenn der Sachinhaber durch Gebote und Verbote in seiner rechtlichen Verfügungsmacht beschränkt wird.[888] Zweifelhaft erscheint dies insbesondere dann, wenn der Beschuldigte der Gewahrsamsinhaber ist oder wenn Bedenken an der Vertrauenswürdigkeit eines Dritten bestehen, der sich im Besitz der Daten befindet[889], wie einen Serviceprovider.

Bär vertritt die Ansicht, dass das Kopieren von Daten kein Problem der Gegenstandsqualität der Daten sei, sondern lediglich die Art der Sicherstellung betreffe.[890] Dabei legt er seiner Argumentation die Vergleichbarkeit von Computerdatenträgern mit Schriftstücken zu Grunde, die in Kapitel 4.3.7.2 widerlegt wurde. Die Sicherstellung „in anderer Weise" ersetzt lediglich die Inverwahrnahme bestimmter Gegenstände, bei denen dies in der Regel nicht möglich oder geboten ist[891], erweitert aber nicht den Kreis der beschlagnahmefähigen Objekte. Die Gegenstandsqualität von Daten ist daher nach unabhängig vom Ablauf der Sicherstellung zu beurteilen und mit den in Kapitel 4.3.7.2 dargestellten Gründen zu verneinen.

4.3.7.4 Beschlagnahmezweck

Der Zweck der Sicherstellung besteht darin, Gegenstände zu sichern, denen für die Untersuchung eine potentielle Beweisbedeutung zukommt. Dadurch wird eine Begrenzung der Eingriffsermächtigung in zweifacher Hinsicht erreicht: Eine Sicherstellung ist nur im Rahmen eines bereits stattfindenden Ermittlungsverfahrens zulässig und nur hinsichtlich der für das Strafverfahren potentiell relevanten Gegenstände.[892] Mit „Untersuchung" ist das gesamte Strafverfahren gemeint, ab dem Zeitpunkt, zu dem ein Ermittlungsverfahren anhängig ist bis zu seinem rechtskräftigen Abschluss. Eine förmliche Einleitung ist nicht erforderlich. Es muss jedoch ein entsprechender Anfangsverdacht – d.h. tatsächliche Anhaltspunkte im Sinne von § 152 Abs. 2 StPO – bestehen. Auf diese Weise soll eine unzulässige Ausforschung von Straftaten „ins Blaue hinein" verhindert werden.[893] Die Sicherstellung kann dann nach allgemeiner Ansicht auch die erste Ermittlungshandlung sein.[894] Bedeutung für das Strafverfahren kommt allen Gegenständen zu, die verfahrensrechtliche oder materiellrechtliche Fragen betreffen. Nicht notwendig ist, dass der Gegenstand später zum Beweismittel wird, solange zum Zeitpunkt der Sicherstellung die Möglichkeit bestand, dass er für Untersuchungszwecke verwen-

[886] Löwe/Rosenberg – *Schäfer* § 94 Rn 30; Meyer-Goßner § 94 Rn 14
[887] BGHSt 3, 395 (400); 15, 149 (150)
[888] Löwe/Rosenberg – *Schäfer* § 94 Rn 33; KK – *Nack* § 94 Rn 16; Meyer-Goßner § 94 Rn 15
[889] Löwe/Rosenberg – *Schäfer* § 94 Rn 33
[890] Bär, S. 270
[891] Löwe/Rosenberg – *Schäfer* § 94 Rn 33; Meyer-Goßner § 94 Rn 16
[892] Löwe/Rosenberg – *Schäfer* § 94 Rn 11 ff.; Meyer-Goßner § 94 Rn 6 ff.
[893] LG Köln StV 1983, 56 (56); Lüttger/Kaul GA 1961, 74 (76); Meyer-Goßner § 94 Rn 8; SK/StPO – *Rudolphi* § 94 Rn 7; Wilhelm NJW 1959, 1716 (1717)
[894] Löwe/Rosenberg – *Schäfer* § 94 Rn 13 mwN

det werden kann.[895]

4.3.7.5 Dauer

Die §§ 94 ff. StPO sehen keine zeitliche Beschränkung für die Sicherstellung von Daten vor. Belange des Datenschutzes finden daher keine angemessene Berücksichtigung. Nachdem der ursprüngliche Anwendungsbereich der Norm auf körperliche Gegenstände beschränkt war, stellte sich dieses Erfordernis bislang nicht. Ein Mindestschutz persönlicher Daten ist nur bei der richterlichen Anordnung der förmlichen Beschlagnahme nach § 98 Abs. 1 StPO gewährleistet. Bei der formlosen Sicherstellung müssen die Daten erst nach der rechtskräftigen Beendigung des Verfahrens herausgegeben werden.[896] Dies kann erheblich Zeit in Anspruch nehmen, während der die Daten dem Zugriff der Ermittlungsbehörden ausgesetzt sind.

4.3.7.6 Verhältnismäßigkeit

Dem Verhältnismäßigkeitsgrundsatz kommt im Bereich der Sicherstellung besondere Bedeutung zu. Dies liegt zum einen daran, dass die Eingriffsvoraussetzungen in den §§ 94 ff. StPO außerordentlich weit gefasst sind und zum anderen, dass die Sicherstellung mit erheblichen Eingriffen in die Grundrechte der allgemeinen Handlungsfreiheit aus Art. 2 Abs. 1 GG, der Achtung der Privatsphäre aus Art. 2 Abs. 1, Art. 1 Abs. 1 GG und – im Bereich der Sicherstellung von Daten – der informationellen Selbstbestimmung aus Art. 2 Abs. 1 GG, Art. 1 Abs. 1 GG verbunden ist.

Das Übermaßverbot erfordert eine Prüfung der oben genannten Grundrechte im Rahmen einer Abwägung, inwieweit sie in einem angemessenen Verhältnis zum staatlichen Interesse an einer effektiven Strafverfolgung, das als Bestandteil des Rechtsstaatsprinzips ebenfalls Verfassungsrang genießt[897], stehen. Wenn mildere Maßnahmen möglich sind, die den gleichen Erfolg bewirken, so ist die Sicherstellung rechtswidrig. Im weiteren Strafverfahren führt dies zu einem Verwertungsverbot.[898] Der Verhältnismäßigkeitsgrundsatz beschränkt insofern das in § 152 Abs. 2 StPO festgeschriebene Legalitätsprinzip.

Ein Eingriff in die Privatsphäre wirkt stets besonders schwer.[899] Daten kann ohne nähere Prüfung in der Regel nicht angesehen werden, ob sie dem privaten oder einem anderen Lebensbereich zuzuordnen sind. Anerkannt ist darüber hinaus, dass die Interessen Unbeteiligter bei der Interessenabwägung im Einzelfall zu prüfen sind.[900] Wie bereits in Bezug auf die Beweismitteleigenschaft (Kapitel 4.3.7.2) und den Ablauf einer Sicherstellung (Kapitel 4.3.7.3) gezeigt, kann der Verhältnismäßigkeitsgrundsatz nicht herangezogen werden, um die Grenzen einer strafprozessualen Eingriffsnorm zu erweitern. Dies würde der dogmatischen Funktion des Übermaßverbotes gerade widersprechen. Strukturelle Schwächen des Strafprozessrechts, die sich aus der historischen Beschränkung auf körperliche Gegenstände ergeben, können nicht im Wege der Auslegung behoben werden. Verhältnismäßig ist eine Kopie von Daten nur dann, wenn die Sicherstellung des gesamten Datenträgers auf §§ 94 ff. StPO hätte gestützt werden können, weil ein Anfangsverdacht in Bezug auf alle darauf gespeicherten Daten vorlag, und die Anfertigung von Duplikaten daher ein „echtes“ Minus zur Sicherstellung des

[895] Löwe/Rosenberg – *Schäfer* § 94 Rn 11 ff.; Meyer-Goßner § 94 Rn 5 ff.
[896] Löwe/Rosenberg – *Schäfer* § 94 Rn 58; KK – *Nack* § 94 Rn 24 f.
[897] Siehe dazu Kapitel 4.2.3.3
[898] Löwe/Rosenberg – *Schäfer* § 94 Rn 35
[899] BVerfGE 44, 353 (372 f., 380 ff.); Löwe/Rosenberg – *Schäfer* § 94 Rn 37
[900] Meyer-Goßner § 94 Rn 18

körperlichen Speichermediums darstellt. In anderen Fällen ist das Kopieren von Daten nicht der „verhältnismäßigere“ Eingriff.

4.3.7.7 Beschlagnahmeverbote

Der Kreis der sicherstellungsfähigen Gegenstände wird durch die §§ 96 und 97 StPO begrenzt. Danach ist die Beschlagnahme von Behördenakten grundsätzlich unzulässig, es sei denn, die Behörde handelt offensichtlich willkürlich oder rechtsmissbräuchlich.[901] Darüber unterliegen Gegenstände bei Personen, denen ein Zeugnisverweigerungsrecht zusteht, nicht der Beschlagnahme. § 97 StPO ergänzt insofern die §§ 52 ff. StPO.

4.3.7.8 Ergebnis zu § 94 StPO

Im Unterschied zu Art. 16 erlaubt § 94 StPO nur die Beschlagnahme von körperlichen Datenträgern. Zwar wird in der wissenschaftlichen Diskussion die Ansicht vertreten, dass das Kopieren von Daten stets den milderen Eingriff gegenüber der Beschlagnahme des gesamten Speichermediums darstelle. Nach der hier vertretenen Ansicht wird dieses Ergebnis abgelehnt, da es aus einem fehlerhaften Vergleich von Computerdatenträgern mit Urkunden im Sinne der StPO resultiert. Daten können nur dann durch Kopieren sichergestellt werden, wenn die Ermittlungsbehörden auf den ganzen Datenträger zugreifen könnten, da ein Anfangsverdacht in Bezug auf alle darauf gespeicherten Daten besteht. Vor allem bei Speichermedien in Computernetzen (Server, Netzwerklaufwerke), auf denen sich große Datenmengen unterschiedlicher Benutzer befinden, führt dies zu Einschränkungen bei der Sicherstellung von Daten. Ein weiterer Unterschied beider Regelungen besteht darin, dass § 94 StPO anders als Art. 16 keine Höchstdauer für die Sicherung von Daten vorsieht, jedoch in Verbindung mit § 97 StPO bestimmte beschlagnahmefreie Gegenstände vom Zugriff der Ermittlungsbehörden ausnimmt.

4.3.8 Bewertung Art. 16

Anders als § 94 StPO erfordert Art. 16 keine Körperlichkeit der zu sichernden/sicherzustellenden Beweismittel. Dadurch wird der unmittelbare Zugriff auf die Computerdaten eröffnet und es ist kein „Umweg“ über die Datenträger – wie im Rahmen von § 94 StPO – erforderlich. Dieser Ansatz entspricht den Bedürfnissen der Praxis, denn im Zusammenhang mit Daten ergibt sich die Beweisbedeutung in aller Regel aus ihrem „gedanklichen Inhalt“ und nicht aus der Beschaffenheit des Datenträgers, auf dem sie gespeichert sind. Durch die Begrenzung der Datenaufbewahrung auf höchstens 90 Tage, Art. 16 Abs. 3, trägt die Konvention in geringem Umfang der im Vergleich zur Sicherstellung körperlicher Objekte veränderte Eingriffsqualität Rechnung. Bei der „Sicherstellung“ von Daten ist aufgrund der großen Kapazitäten moderner Datenträger neben dem Eigentumsrecht am Speichermedium vor allem das Recht auf informationelle Selbstbestimmung in Bezug auf die gespeicherten Informationen bedroht. Um die Eingriffsintensität in rechtstaatlicher Weise zu begrenzen, sind neben zeitlichen Höchstgrenzen für Aufbewahrung von Informationen differenzierte Datenschutzregelungen erforderlich. Abgesehen von einem pauschalen Hinweis in Abs. 3 geht Art. 16 darauf überhaupt nicht ein. An einen Gleichlauf von beschlagnahmefreien Daten und Zeugnisverweigerungsrechten haben die Verfasser der Konvention ebenfalls nicht gedacht. Zusammenfassend bleibt daher zu kritisieren, dass der Anwendungsbereich von Art. 16 zu unscharf formuliert wurde und somit in Zusammenhang mit den fehlenden Datenschutzbe-

[901] Kühne, Rn 511; Löwe/Rosenberg – *Schäfer* § 96 Rn 4 ff.; Meyer-Goßner § 96 Rn 1 f.

stimmungen eine unverhältnismäßige Beeinträchtigung der Rechte der Betroffenen droht.

4.4 Artikel 17 – Beschleunigte Sicherung und Teilweitergabe von Verbindungsdaten[902]

(1) Jede Vertragspartei trifft in Bezug auf Verbindungsdaten, die nach Artikel 16 zu sichern sind, alle erforderlichen gesetzgeberischen und anderen Maßnahmen, um sicherzustellen,

> *a) dass diese beschleunigte Sicherung von Verbindungsdaten unabhängig davon möglich ist, ob ein oder mehrere Dienstanbieter an der Übertragung dieser Kommunikation mitgewirkt haben;*
>
> *b) dass Verbindungsdaten in so ausreichender Menge beschleunigt an die zuständige Behörde der Vertragspartei oder an eine von dieser Behörde bezeichnete Person weitergegeben werden, dass die Vertragspartei die Dienstanbieter und den Weg feststellen kann, auf dem die Kommunikation übertragen wurde.*

(2) Die Befugnisse und Verfahren nach diesem Artikel unterliegen den Artikeln 14 und 15.

4.4.1 Anwendungsbereich

Art. 17 steht in engem Zusammenhang zu Art. 16. Aus dessen sachlich nicht auf bestimmte Datenarten beschränktem Anwendungsbereich greift er nur die Verbindungsdaten (siehe dazu Kapitel 2.4) heraus. Eine eigenständige Bedeutung kommt ihm insoweit zu, als er die lückenlose Sicherung von Metadaten ermöglichen will, die bei mehraktigen Übertragungsakten unter Umständen bei verschiedenen Dienstanbietern anfallen. Diese Zielsetzung wird bei einer näheren Betrachtung der technischen Umsetzung einer Datenübertragung in modernen Computernetzen nachvollziehbar. Im Unterschied zur herkömmlichen Sprachtelefonie werden Daten in Computernetzen nicht über eine „stehende" Verbindung zwischen zwei Endpunkten übertragen, sondern es können beliebig viele Zwischenstationen durchlaufen werden. Insofern spricht man von einer paketvermittelten, virtuellen (engl. *packet switched*) Verbindung.[903] An Knotenpunkten im Netz unternehmen die Server von Dienstanbietern das Leiten von Daten von einer Station zur nächsten, bis die Datenpakete ihr Ziel erreichen (engl. *routing*).[904] Innerhalb einer Datenübertragung können die einzelnen Datenpakete je nach Last im Netz unterschiedliche Wege einschlagen. Verbindungsdaten können daher bei einer Vielzahl verschiedener Anbieter und an unterschiedlichen Orten anfallen. Art. 17 soll in diesem Zusammenhang den Ermittlungsbehörden die Möglichkeit verschaffen, die Sicherung von Verbindungsdaten gegen alle Dienstanbieter anordnen zu können.

4.4.2 Verbindungsdaten

Der Begriff der „Verbindungsdaten" im Sinne der Konvention ist in Art. 1 lit. d) definiert. Zusammenfassend handelt es sich dabei um alle Daten, die von einem Computer im Rahmen einer Datenübertragung erzeugt werden, um die Inhaltsdaten vom Ausgangs- an den Zielort leiten zu können. Im Übrigen kann auf die Ausführungen in Kapitel 2.4 verwiesen werden. Besondere Bedeutung kommt in den heutigen Computernetzen der IP-Adresse zu. Ohne die technischen Grundlagen näher zu beleuchten, liegt ihre wesentliche Bedeutung darin, dass sie

---

[902] ER Ziff. 165-169

[903] Taschenbuch der Informatik – *Löffler* Kap. 6, S. 167 f., 184 ff.; Diese Leitungswege können beispielsweise über die Windows-Programme *„tracert"* und *„traceroute"* visualisiert werden, siehe dazu die „Windows" Hilfefunktion.

[904] Taschenbuch der Informatik – *Löffler*, Kap. 6, S. 167; Diese Leitungswege können beispielsweise mit Hilfe der Windows-Programme *„tracert"* und *„traceroute"* visualisiert werden; siehe auch Kapitel 1.7.1.1.4.

eine weltweit eindeutige Identifizierung eines Rechners – nicht unbedingt einer Person – in einem TCP/IP-basierten Netzwerk erlaubt. Bei TCP/IP handelt es sich um Netzwerkprotokolle – Regeln für die Datenübertragung zwischen vernetzten Computern –, deren Verwendung konstitutiv für die Netze ist, die nach heutigem Verständnis das sog. Internet[905] bilden.[906] Jeder angeschlossene Computer muss über eine derartige Adresse verfügen, damit ihn Datenübertragungen erreichen können.[907] Das IP-Protokoll übernimmt die netzübergreifende, globale Adressierung im Internet. Dazu werden die zu übertragenden Daten in Pakete von vordefinierter Größe aufgeteilt und wie in einem Briefumschlag, der außen die weltweit eindeutige IP-Nummer[908] als Adresse trägt, an den jeweiligen Empfänger geleitet.[909] Bei diesem werden sie in einer während der Übertragung festgelegten Reihenfolge wieder zur vollständigen Datei zusammengesetzt.[910] Ohne die Feststellung der IP-Adressen kann der Leitungsweg einer Datenübertragung nicht zurückverfolgt werden.[911] Der Inhalt der Daten wird durch die IP-Adresse nicht offen gelegt.[912]

Am Beispiel dieser IP-Adresse lässt sich verdeutlichen, warum nur das gleichzeitige Vorgehen gegen mehrere Dienstanbieter – wie von Art. 17 Abs. 1 lit. a) vorgesehen – eine erfolgreiche Zurückverfolgung einer Datenübertragung im Internet ermöglicht. IP-Adressen werden mittlerweile fast ausschließlich dynamisch vergeben, d.h. ein Computer (engl. *host*) erhält bei jeder Verbindung mit einem Zugangsanbieter (z.B. T-Online, Rechenzentren der Universitäten usw.) eine neue Kennung.[913] Dies dient vor allem der Wahrung der Datenschutzbelange des Betroffenen. Bei einer statischen Kennung könnten durch Überwachung derselben detaillierte Profile erstellt werden. Gleichzeitig erschwert die dynamische Vergabe von Adressen jedoch auch die Tätigkeit der Ermittlungsbehörden, weil keine eindeutige Zuordnung zu einem Computer möglich ist. Allerdings protokollieren die Zugangsanbieter in der Regel, welche Adressen wann vergeben wurden. Da jeder Zugangsanbieter über ein bestimmtes, begrenztes Kontingent an IP-Adressen verfügt, kann die Datenübertragung an einen bestimmten Ausgangsort zurückverfolgt werden und, sofern eine entsprechende Protokolldatei bei der Adressvergabe erstellt wurde, sogar eine bestimmter Computer identifiziert werden. Bei Einwahlverbindungen erfolgt dies über den Telefonanschluss, in Netzwerken über die Hardwareadresse des Netzwerkadapters[914] (sog. MAC). Teilen sich mehrer Benutzer einen PC, so kann nur bei Systemen, die eine Identifikation des jeweiligen Nutzers verlangen (z.B. Unix/Linux, WinXP usw.) über lokale Protokolldateien eine weitere Individualisierung vorgenommen

[905] Siehe dazu die Darstellungen der Internet Society (ISOC), einer Dachorganisation der untergeordneten netzbezogenen Organisationen, zur Entwicklung des Netzes, das heute als „Internet" bezeichnet wird: http://www.isoc.org/internet/history/ (01.04.2004)

[906] Allerdings gerät auch diese Beschreibung mittlerweile ins Wanken, da die Verwendung von Gateways (dt. Übergängen zwischen Netzen unterschiedlicher Protokolle) den Übergang zwischen TCP/IP-Netzen und sonstigen Netzen vollkommen problemlos und für den Nutzer nicht mehr bemerkbar ermöglicht; Plate, Internet – Möglichkeiten und Dienste, 1.2

[907] Plate, Internet – Möglichkeiten und Dienste, 1.4.1; Taschenbuch der Informatik – *Löffler*, Kap. 6, S. 217

[908] Die IP-Adresse wird durch eine 32-Bit lange Zahl dargestellt, unterteilt in vier Zahlenfolgen (sog. IPv4) zu je 1 Byte (8 Bit). Diese Bytes werden dezimal notiert und durch Punkte getrennt. Für jedes der vier Zahlenfelder ergeben sich daher 2^8 (= 256) Möglichkeiten; Taschenbuch der Informatik – *Löffler*, Kap. 6, S. 217, 219 f.; Die IP-Adresse des WWW-Servers der Universität Regensburg lautet beispielsweise: 132.199.1.205

[909] Plate, Internet – Möglichkeiten und Dienste, 1.4.1; Taschenbuch der Informatik – *Löffler*, Kap. 6, S. 219 f.

[910] Plate, Internet – Möglichkeiten und Dienste, 1.4.1; Taschenbuch der Informatik – *Löffler*, Kap. 6, S. 184

[911] Plate, Internet – Möglichkeiten und Dienste, 1.4; Taschenbuch der Informatik – *Löffler*, Kap. 6, S. 184, 217 ff.

[912] Plate, Internet – Möglichkeiten und Dienste, 1.4.1; Taschenbuch der Informatik – *Löffler*, Kap. 6, S. 184, 217 ff.

[913] Bei Windows-Betriebssystemen lässt sich dies beispielsweise im Register „Netzwerkverbindungen" überprüfen.

[914] Sog. Physikalische Adresse. Unter WinXP kann diese beispielsweise mit dem Befehl „ipconfig/all" ermittelt werden.

werden.

4.4.3 Beschleunigte Sicherung und Teilweitergabe

Das Merkmal „beschleunigt“ trägt wie bei Art. 16 der Flüchtigkeit von Computerdaten Rechnung. Für Verbindungsdaten gilt dies in gesteigertem Maße, da sie für die Dienstanbieter außer zu Test- und Wartungszwecken und bisweilen für die Erstellung von Abrechnungen keine besondere Funktion erfüllen und daher in der Regel rasch gelöscht werden.[915] In Bezug auf den Sicherungsbegriff kann ebenfalls auf Art. 16 zurückgegriffen werden, d.h. es bleibt den Vertragsparteien unbenommen, ob sie eine „neue“ Befugnis in Bezug auf unkörperliche Daten schaffen oder aber den Sicherungserfolg mit den herkömmlichen Befugnissen, also vor allem der Durchsuchung und Beschlagnahme von Datenträgern, bewirken wollen.

Die besondere Bedeutung von Art. 17 besteht darüber hinaus darin, dass er den Ermittlungsbehörden die Möglichkeit verschaffen will, an Stelle von Einzelanordnungen gegen bestimmte Diensteanbieter, Sammelanordnungen gegen eine unbestimmte Vielzahl von Providern erlassen zu können. Dahinter steckt die Überlegung, dass Datenübertragungen in Computernetzen in der Regel über beliebige Zwischenstationen[916] (engl. *server*) geleitet (engl. *routing*) werden. An jedem beteiligten Server können Verbindungsdaten anfallen. Will man den exakten Leitungsweg nachvollziehen, kann dies nur durch die sukzessive Identifikation der einzelnen Zwischenstationen erfolgen. In diesem Zusammenhang schlagen die Erläuterungen vor, dass eine Sammelanordnung in Bezug auf die Sicherstellung von Verbindungsdaten schrittweise in Abhängigkeit vom Bekanntwerden der „Zwischenstationen“ zugestellt werden könnte, ohne dass die Anordnungsvoraussetzungen in Bezug auf die jeweiligen Maßnahmeadressaten – die Betreiber der Server – jeweils neu überprüft werden müssten, solange sie sich auf den selben Kommunikationsvorgang beziehen.[917] Weiterhin sollen einzelne Dienstanbieter zum „verlängerten Arm“ der Ermittlungsbehörden werden, indem Sicherungsanordnungen, die gegen sie erlassen wurden, die Verpflichtung enthalten, weitere an der Datenübertragung beteiligte Anbieter zu identifizieren und diesen die entsprechende Anordnung zu übermitteln.[918] Begründet werden diese Vorschläge vor allem mit der Zeitersparnis gegenüber einem individualisierten Vorgehen der Ermittlungsbehörden.[919]

Über die bloße Sicherung hinaus zielt Art. 17 Abs. 1 lit. b) auf eine „Teilweitergabe“ der gesicherten Daten ab. Diese Variante gewinnt nur dann eine eigenständige Bedeutung, wenn die Unterzeichnerstaaten wie im Rahmen von Art. 16[920], die Sicherung nicht durch die zuständigen Behörden, sondern durch die Dienstanbieter vornehmen lassen. Um dann in den „Besitz“ der Daten zu gelangen, ist eine Mitwirkung der Provider – die Teilweitergabe der Daten – erforderlich. Teilweitergabe bedeutet in diesem Zusammenhang, dass zunächst nur derjenige Teil der Daten an die zuständigen Stellen weitergegeben wird, der diesen erlaubt festzustellen, ob und welche anderen Provider an der Übertragung beteiligt waren, um auch gegen diese vorgehen zu können.[921] Nach dem Grundkonzept[922] der Art. 16 und 17 wird der andere Teil der Daten, der nicht weitergegeben wird, im Übrigen nur gesichert, d.h. sein *status quo* wird „eingefroren“, ohne dass die Ermittler Kenntnis vom Inhalt nehmen. Dazu ist vielmehr eine

[915] ER Ziff. 166
[916] Siehe Kapitel 4.4.1
[917] ER Ziff. 168
[918] ER Ziff. 168
[919] ER Ziff. 168
[920] Siehe Kapitel 4.3.2; ER Ziff. 151 f., 155, 160 f.
[921] ER Ziff. 169
[922] Siehe dazu ausführlich Kapitel 4.3.2.

gesonderte Rechtsgrundlage erforderlich. Lit. b) trägt damit den technischen Voraussetzungen der Datenübermittlung in Computernetzen, die in der Regel mehrere Zwischenstationen involviert, Rechnung.[923]

4.4.4 Sicherungszweck und Sicherungsdauer

In Bezug auf den Sicherungszweck ergeben sich keine Abweichungen zu Art. 16. Anders hingegen für die Sicherungsdauer, für die Art. 17, wenigstens ausdrücklich, keine zeitliche Obergrenzen vorsieht. Belange des Datenschutzes oder Beschlagnahmeverbote werden neben einem allgemeinen Hinweis in Art. 17 Abs. 2 auf Art. 14 und 15 nicht weiter erwähnt.

4.4.5 Adressaten der Sicherungsanordnung

Da Verbindungsdaten üblicherweise nicht beim Nutzer, sondern beim Anbieter anfallen, ist dieser potentieller Adressat der Maßnahme.

4.4.6 Vergleichbare Befugnisnormen im deutschen Strafprozessrecht

Soweit Verbindungsdaten auf Datenträgern gesichert werden, kommt grundsätzlich eine Sicherstellung der zu Grunde liegenden Datenträger nach § 94 StPO in Betracht. Dabei sind jedoch die in Kapitel 4.3.7.1 dargestellten Besonderheiten zu beachten. Daneben ermöglicht § 100g Abs. 1 Satz 1 StPO die Einholung von Auskünften über vergangene Telekommunikationsverbindungen. § 100g Abs. 1 Satz 3 StPO wird an dieser Stelle nicht in den Vergleich miteinbezogen, da eine Auskunft über *zukünftige* Telekommunikationsverbindungen begrifflich und inhaltlich eine Überwachung darstellt[924] und daher den Anwendungsbereich von Art. 17, der auf bereits gespeicherte Daten beschränkt ist, überschreitet. Ebenso wenig scheint § 100g Abs. 2 StPO (sog. Zielwahlsuche) mit Art. 17 vergleichbar, da diese Variante eher Elemente einer Rasterfahndung aufweist.[925]

4.4.6.1 § 94 StPO – [Sicherstellung von Beweisgegenständen]

§ 94 StPO ermöglicht den Strafverfolgungsbehörden keinen Zugriff auf die Verbindungsdaten einer Datenübertragung, da diese nach der ganz herrschenden Auffassung dem Fernmeldegeheimnis (siehe Kapitel 4.2.3.1.1) unterliegen, in das nicht auf Grund einer Beschlagnahmeanordnung eingegriffen werden kann. § 94 StPO gibt den Ermittlungsbehörden lediglich die Befugnis, das Grundrecht auf Eigentum zu beschränken. Eingriffe der Strafverfolgungsbehörden in das Fernmeldegeheimnis sind abschließend durch die §§ 100a f. und 100g f. StPO geregelt.[926]

4.4.6.2 § 100g Abs. 1 Satz 1 StPO – [Auskunft über Telekommunikationsverbindungsdaten]

§ 100g StPO ersetzt § 12 FAG, der zum 31.12.2001 außer Kraft getreten ist. Zusammen mit §

[923] Siehe Kapitel 4.4.1
[924] Ebenso: SK/StPO – *Wolter* § 100g Rn 1, 12; ausführlich dazu: Kapitel 4.7.9
[925] Meyer-Goßner § 100g Rn 11; SK/StPO – *Wolter* § 100g Rn 12
[926] LG Hanau, Beschluss vom 23.09.1999 – 3 Qs 149/99 = NJW 1999, 3647; KK – *Nack* § 100a Rn 1; SK/StPO – *Rudolphi* Vorbemerkung vor § 94 Rn 13

100h StPO ist er seinerseits zum 31.12.2004 befristet[927], um dann – wie es in der Begründung zum Gesetzentwurf der Bundesregierung heißt – einem „harmonischen Gesamtsystem der strafprozessualen heimlichen Ermittlungsmaßnahmen“ zu weichen, das eine einheitliche Berücksichtigung der Zeugnisverweigerungsrechte ermöglicht.[928] Durch die Neuregelung sollte Bedenken an der Verfassungsmäßigkeit von § 12 FAG begegnet werden[929], indem vor allem die Anordnungsvoraussetzungen angehoben wurden. Gleichzeitig wurde der bestehende Auskunftsanspruch durch § 100g Abs. 1 Satz 3 StPO auf zukünftige Verbindungsdaten erweitert. Damit ermöglicht die Befugnis nicht nur Auskünfte über vergangene Telekommunikationsvorgänge, sondern auch die Überwachung[930] zukünftiger Verbindungen. Abs. 1 Satz 3 StPO wird wegen des Überwachungscharakters im Zusammenhang mit Art. 20 näher erläutert werden. In der Praxis dürften die §§ 100g, 100h StPO vor allem als Vorstufe zu einer (großen) Überwachung nach §§ 100a, 100b StPO relevant werden, da sie an keinen enumerativen Straftatenkatalog gebunden sind sowie Taten in Verbindung mit einer Endeinrichtung nach § 3 Nr. 3 TKG erfassen.[931] Darüber hinaus dienen sie der Standortbestimmung von Mobiltelefonen, jedoch nur soweit eine Verbindung zu Stande kommt, § 100g Abs. 3 Nr. 1 StPO. Durch diese Einschränkung soll die Abfrage sog. *„stand-by“*-Daten zur Positionsbestimmung ausgeschlossen werden, die nicht dem Fernmeldegeheimnis unterliegen.[932] Insgesamt stellt § 100g StPO eine heterogene Norm mit stark voneinander abweichenden Befugnissen im Einzelnen dar. Abs. 1 Satz 1 und 2 werden zu Recht in die Nähe der Übermittlungsnorm des § 161 Abs. 1 StPO gerückt, wohingegen Abs. 1 Satz 3 Ähnlichkeit zur Überwachungsvorschrift des § 100a StPO und die durch Abs. 2 geregelte „Zielwahlsuche“ zur Raster- und Schleppnetzfahndung aufweist.[933] Für einen Vergleich mit Art. 17 soll im Folgenden allein § 100g Abs. 1 Satz 1 StPO untersucht werden.

4.4.6.2.1 Telekommunikationsverbindungsdaten

Der Kreis der Daten, über die Auskünfte eingeholt werden können, wird durch Abs. 3 abschließend definiert.[934] Insoweit kann auf die Ausführungen in Kapitel 2.4.1 verwiesen werden. Zusammenfassend gesprochen handelt es sich bei Verbindungsdaten (bzw. Metadaten) um Daten, die bei einer Datenübertragung anfallen, ohne Informationen über die ausgetauschten Inhalte zu enthalten. In der Regel wird es sich dabei um Auskünfte über die Beteiligten, Ort, Zeit und Dauer der Kommunikation, die verwendete Infrastruktur und Dienste und dergleichen handeln. Ihre zunehmende Bedeutung kann im Wesentlichen auf die Einführung der Digitaltechnik im Telekommunikationssektor zurückgeführt werden, durch die ihre Erfassung in größerem Umfang erst ermöglicht wurde.[935]

4.4.6.2.2 Umfang der Auskunftserteilung

§ 100g Abs. 1 Satz 1 StPO bestimmt nicht näher, in welcher Art und Weise die Dienstanbieter Auskunft zu erteilen haben. Fraglich ist insbesondere, ob die Herausgabe der Protokolldateien

[927] BGBl. 2001 I, S. 3879 ff.
[928] RegE mit Stellungnahme des BR: BR-Drs. 702/01, S. 10 f.
[929] BVerfG Urteil vom 12. März 2003 – Az. 1 BvR 330/96 und 1 BvR 348/99
[930] Ebenso: SK/StPO – Wolter § 100g Rn 1, 12, der zutreffend von einer „kleinen Telefonüberwachung“ spricht
[931] SK/StPO – *Wolter* § 100g Rn 5
[932] SK/StPO – *Wolter* § 100g Rn 6
[933] SK/StPO – *Wolter* § 100g Rn 12
[934] Meyer-Goßner § 100g Rn 4; SK/StPO – *Wolter* § 100g Rn 17
[935] Bär, S. 353 unter Bezugnahme auf den 11. Tätigkeitsbericht des Bundesdatenschutzbeauftragten, BT-Drs. 11/3932, S. 32

genügt oder ob eine inhaltliche Aufbereitung der Verbindungsdaten erforderlich ist. Aus dem Gesetz ergeben sich dafür keine Anhaltspunkte. Ein Vergleich zur Editionspflicht des § 95 StPO erscheint wenig hilfreich, da Eingriffe in das Fernmeldegeheimnis auf der Grundlage der StPO abschließend durch die §§ 100a, 100g StPO geregelt sind.[936]

Für den Umfang der Auskunftspflicht ist von zentraler Bedeutung, dass die TK-Anbieter nur Auskünfte über solche Daten geben müssen, die von ihnen in rechtmäßiger Weise erhoben aufbewahrt werden durften, d.h. legal zur Verfügung stehen.[937] Um welche Daten es sich dabei handelt, wird für den Bereich der Telekommunikation durch die Telekommunikationsdatenschutzverordnung (TDSV) und ergänzend – wegen § 1 Abs. 2 TDSV – durch das BDSG beschrieben.[938] Für die Verarbeitung und Nutzung personenbezogener Daten sehen beide Gesetze grundsätzlich ein allgemeines Verbot mit Erlaubnisvorbehalt vor, §§ 3 Abs. 1 TDSV, 4 Abs. 1 BDSG. § 6 Abs. 1 TDSV erlaubt als lex specialis zum BDSG für den TK-Bereich die Erhebung von Verbindungsdaten (§ 2 Nr. 4 TDSV) für die in der Verordnung genannten Zwecke (sog. Zweckbindungsgebote).[939] Dabei handelt es sich im Wesentlichen um die Entgeltermittlung und Entgeltabrechnung nach § 7 TDSV, den Einzelverbindungsnachweis nach § 8 TDSV, Störungen und Missbrauch nach § 9 TDSV sowie die Mitteilung ankommender Verbindungen nach § 10 TDSV. Im Übrigen sind die Verbindungsdaten nach § 6 Abs. 2 TDSV spätestens am Tag nach Beendigung der Verbindung unverzüglich zu löschen.

Trotz aller Akribie des deutschen Gesetzgebers in Bezug auf die Belange des Datenschutzes im Telekommunikationsbereich bleibt die eigentliche Sachfrage, nämlich welche Daten im Einzelnen für die oben genannten Zwecke erforderlich sind, offen. Dies gilt insbesondere für IP-Adressen. Erhebliche Kritik in diesem Zusammenhang hat eine Entscheidung des Regierungspräsidiums Darmstadt in der Funktion als zuständige Datenschutz-Aufsichtsbehörde hervorgerufen.[940] Es ging um Frage, ob der Provider T-Online die IP-Adressen von Kunden speichern darf, die einen umsatz- und zeitunabhängigen Pauschaltarif (engl. *flat rate*) für den Zugang zum Internet nutzen. T-Online machte geltend, dass trotz Pauschaltarifs eine Protokollierung der IP-Adressen zu Abrechungszwecken erforderlich sei. Das Regierungspräsidium bestätigte diese Ansicht, trotz der Kritik durch das „Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein“[941] und durch die einschlägige Fachpresse.[942] Unabhängig davon, ob in technischer Hinsicht eine Speicherung erforderlich ist, muss aus der rechtlichen Perspektive gefordert werden, dass die aufgezeichneten Kennungen anonymisiert werden, nachdem sie für Abrechnungszwecke benutzt wurden. Denn selbst dann kann nachgewiesen werden, wie von T-Online gefordert, dass IP-Adressen vergeben wurden und somit die ordnungsgemäße Möglichkeit des Zugangs bestand. Um welche Kennungen es sich im Einzelnen handelt ist für den Nachweis der Tatsache, ob überhaupt IP-Adressen erteilt wurden, hingegen unerheblich.[943] Die Aufzeichnung der Kennungen erfolgte damit nicht zu Abrechnungszwecken, § 7 TDSV, und war damit rechtswidrig.

---

[936] KK – *Nack* § 100a Rn 1 mwN

[937] Eisenberg, Rn 2450d, 2450g; KK – *Nack* § 100g Rn 6; Meyer-Goßner § 100g Rn 4, 10; SK/StPO – *Wolter* § 100g Rn 17

[938] Soweit einzelne Datenübertragungen als Teledienste qualifiziert werden können, kommt darüber hinaus das Teledienstedatenschutzgesetz (TDDSG) in Betracht, so Roßnagel – *Schulz* 3 § 1 TDDSG Rn 32ff

[939] Handbuch Datenschutzrecht – *Groß* 7.8 Rn 25 f.

[940] Heise Meldung vom 14.01.2003 mit einem Kommentar von Stefan Jaeger: http://www.heise.de/ct/aktuell/meldung/33674

[941] Pressemitteilung vom 16.01.2003, http://www.datenschutzzentrum.de/material/themen/presse/ipspeich.htm (01.04.2004)

[942] Siehe Fn 940; Rötzer, telepolis, 16.01.2003

[943] Ebenso „Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein“ Fn 941, Jäger Fn 940 sowie Rötzer Fn 942

Weitere Fälle einer gerichtlichen oder behördlichen Überprüfung der Erhebung von Verbindungsdaten durch Internetprovider liegen bislang nicht vor. Ein Grund dafür ist sicherlich, dass es sich bei der Aufzeichnung von Daten durch die Internetprovider um einen heimlichen Vorgang handelt, der kaum kontrolliert werden kann. Im Ergebnis bleibt daher unklar, inwieweit der Auskunftsanspruch des § 100g Abs. 1 Satz 1 StPO durch das datenschutzrechtliche Verbot mit Erlaubnisvorbehalt in Bezug auf die Erhebung und Verarbeitung von Verbindungsdaten im Datennetzbereich eingeschränkt wird.[944] Eine Erhebung von Verbindungszusammen mit Inhaltsdaten ist weiterhin unter den Voraussetzungen der §§ 100a und 100b StPO möglich.[945]

4.4.6.2.3 Verdacht einer Straftat

Die Erteilung der Auskunft kann angeordnet werden, wenn der Verdacht einer Straftat besteht. Diese Tat muss entweder von „erheblicher Bedeutung“[946] sein oder mittels einer Endeinrichtung nach § 3 Nr. 3 des TKG begangen werden. Der Ausdruck „insbesondere“ in Abs. 1 Satz 1 verdeutlicht, dass kein abschließender Straftatenkatalog wie bei §§ 100a f. StPO geschaffen werden sollte, dieser jedoch zur Konkretisierung der wenig bestimmten Formulierung „Straftat von erheblicher Bedeutung“ herangezogen werden kann.[947] Bagatelldelikte werden damit ausgeschlossen, es sei denn, sie weisen den beschriebenen Telekommunikationsbezug auf. Darin liegt eine wesentliche Einschränkung gegenüber der Vorgängerregelung des § 12 FAG, um verfassungsrechtlichen Bedenken insbesondere in Bezug auf den Verhältnismäßigkeitsgrundsatz und das Fernmeldegeheimnis zu begegnen.[948] Im Übrigen genügt wie bei § 100a StPO einfacher Tatverdacht auf der Grundlage objektivierbarer Tatsachen.

4.4.6.2.4 Zeitlicher Rahmen

Eine zeitliche Höchstgrenze ist weder für den Auskunftszeitraum noch für die Aufbewahrung von Verbindungsdaten durch die §§ 100g f. StPO vorgesehen. Die Daten dürfen gespeichert werden, solange sie zu Strafverfolgungszwecken erforderlich erscheinen. Danach verlangen die §§ 100h Abs. 1 Satz 3 iVm 100b Abs. 6 StPO ihre unverzügliche Vernichtung, über die eine Niederschrift zu erstellen ist. Die zeitliche Befristung der §§ 100h Abs. 1 Satz 3 Hs. 2 iVm 100b Abs. 2 Satz 4 StPO gilt nur für Auskünfte über zukünftige Verbindungen, d.h. für Überwachungsmaßnahmen.

4.4.6.2.5 Adressaten der Auskunftsanordnung

Verbindungsdaten fallen üblicherweise bei den Anbietern von Telekommunikationsdiensten an. Diesem Umstand trägt § 100g Abs. 1 Satz 1 StPO dadurch Rechnung, dass nur dieser Personenkreis, die Anbieter geschäftsmäßiger Telekommunikationsdienste nach § 3 Nr. 5 TKG, auskunftspflichtig ist. Im Umkehrschluss bedeutet dies, dass Verbindungsdaten beim Benutzer, etwa die „Verlaufsanzeige“ im Browser, nicht nach § 100g Abs. 1 Satz 1 StPO ermittelt werden können. Die Auskunftsanordnung muss den Auskunftspflichtigen nicht individualisie-

[944] Eisenberg, Rn 2450d, 2450g; Meyer-Goßner § 100g Rn 4, 10; SK/StPO – *Wolter* § 100g Rn 17
[945] BT-Drs. 14/7258, S. 4
[946] Diese Formulierung wird auch von den §§ 163e, 163f sowie 100c Abs. 1 Nr. 1 lit. b) StPO verwendet.
[947] KK – *Nack* § 100g Rn 4; Meyer-Goßner § 100g Rn 6; SK/StPO – *Wolter* § 100g Rn 12
[948] Zur einengenden Auslegung der § 12 FAG in Hinblick auf Art. 10 Abs. 1 GG: Pressemitteilung des BVerfG 20/2003 vom 12. März 2003, S. 1; Urteil des BVerfG vom 12.03.2003, Az. 1 BvR 330/96; BT-Drs. 14/7008, S. 6

ren, da nach § 100g Abs. 1 Satz 1 StPO alle geschäftsmäßigen Anbieter von Telekommunikationsdiensten auskunftspflichtig sind.[949] § 88 Abs. 1 TKG verpflichtet sie in diesem Zusammenhang, die erforderlichen technischen Einrichtungen auf eigene Kosten vorzuhalten. Einer Individualisierung bedarf hingegen der von der Auskunftsanordnung Betroffene. Die näheren Einzelheiten bestimmt § 100h Abs. 1 StPO. Dies wird vor dem Hintergrund verständlich, dass nur der betroffene Kunde, nicht jedoch der Anbieter einer Telekommunikationsdienstleistung, vom Fernmeldegeheimnis geschützt wird in das § 100g StPO einzugreifen gestattet.

4.4.6.2.6 Datenschutzbelange und Zeugnisverweigerungsrechte

Das Auskunftsbegehren ist in seinem Umfang auf diejenigen Daten beschränkt, die von den Telekommunikationsanbietern in zulässiger Weise erhoben werden dürfen.[950] § 100h Abs. 2 StPO synchronisiert den Eingriff in Verbindungsdaten darüber hinaus mit den Zeugnisverweigerungsrechten der Geistlichen, Verteidiger und Abgeordneten nach §§ 53 Abs. 1 Satz 1 Nr. 1, 2 und 4 StPO. Bemerkenswert an dieser Einschränkung ist vor allem, dass sie nur einen Ausschnitt aus dem Kreis der Personen aufgreift, die nach § 53 StPO zur Verweigerung des Zeugnisses berechtigt sind, sowie dass eine entsprechende Beschränkung bei §§ 100a f. StPO fehlt[951], obwohl die Überwachung der Inhalte einer Telekommunikation den intensiveren Eingriff darstellt. Eine Auskunft über Telekommunikationen der ausgenommenen Personen zieht ein Beweisverwertungsverbot gemäß § 100h Abs. 2 Satz 1 Hs. 2 StPO nach sich, unter der Einschränkung, dass die zur Verweigerung des Zeugnisses Berechtigten nicht der Teilnahme oder einer Begünstigung, Strafvereitelung oder Hehlerei verdächtig sind.[952]

4.4.6.2.7 Ergebnis zu § 100g Abs. 1 Satz 1 StPO

Vom Wortlaut her unterscheiden sich die Auskunftsanordnung nach § 100g Abs. 1 Satz 1 StPO und die „Beschleunigte Sicherung und Teilweitergabe von Verbindungsdaten“ nach Art. 17 erheblich. Im Ergebnis erlauben beide Normen jedoch den Zugriff der Strafverfolgungsbehörden auf Verbindungsdaten im Zusammenhang mit Datenübertragungen, wobei die StPO über die Konvention hinausgeht, indem sie im Rahmen einer Auskunftsanordnung die Offenlegung der Inhalte der Verbindungsdaten erlaubt. Auch der Eilbedürftigkeit der Befugnis des Art. 17 wird durch den Verweis auf die Anordnungskompetenz der Staatsanwaltschaft bei Gefahr im Verzug Rechnung getragen, §§ 100h Abs. 1 Satz 3, 100b Abs. 1 Satz 2 StPO. Strukturell unterscheiden sich beide Normen dadurch, dass § 100g Abs. 1 Satz 1 StPO – wie auch § 100b Abs. 3 StPO – von einer grundsätzlichen Kooperationspflicht aller Telekommunikationsanbieter bei Überwachungsmaßnahmen ausgeht. In der Praxis bedeutet dies, dass bei einer Auskunfts- bzw. Überwachungsanordnung nicht der Anbieter zu individualisieren ist, sondern der Betroffene, in dessen Fernmeldegeheimnis eingegriffen wird. Bedenken der Verfasser der Konvention, dass separate Anordnungen gegen eine Vielzahl von Anbietern bei einer Datenübertragung im Internet erforderlich seien und zu erheblichen zeitlichen Verzögerungen der Ermittlungsmaßnahmen führen würden, treffen daher im deutschen Recht nicht zu. Eine einmalig erwirkte Anordnung, die in Bezug auf die Bestimmtheit des Betroffenen und die übrigen Anordnungsvoraussetzungen den Anforderungen des § 100h Abs. 1 StPO genügt, kann notfalls gleichzeitig gegen beliebig viele Anbieter eingesetzt werden. Problematisch erscheint allenfalls die Erfassung von IP-Adressen, Routing-Informationen und sonstigen

[949] Noch deutlicher wird dies im Wortlaut von § 100b Abs. 3 Satz 1 StPO.
[950] Siehe Kapitel 4.4.6.2.2.
[951] KK – *Nack* § 100h Rn 7; Meyer-Goßner § 100h Rn 9
[952] KK – *Nack* § 100h Rn 7; Meyer-Goßner § 100h Rn 9

computerbezogenen Verbindungsdaten. In dieser Hinsicht unterscheiden sich beide Normen allerdings nicht. Es können immer nur diejenigen Daten gesichert bzw. im Rahmen einer Auskunft weitergegeben werden, die zuvor von den Anbietern in rechtmäßiger Weise erhoben werden durften. Diese Frage beantworten die jeweiligen Datenschutzbestimmungen und nicht strafrechtliche Befugnisnormen, die an bereits gespeicherten Daten ansetzen.

4.4.7 Bewertung Art. 17

Art. 17 enthält keine über § 100g Abs. 1 Satz 1 StPO hinausgehenden Befugnisse. Der Regelungszweck der Vorschrift besteht darin, Sammelanordnungen in Bezug auf die Sicherung von Verbindungsdaten gegen eine Vielzahl von Anbietern erlassen zu können, um eine zeitliche Verzögerung der Ermittlungen zu vermeiden. Eine derartige Gefahrenlage besteht im deutschen Recht nicht. Als wesentliches Defizit bleibt dagegen festzuhalten, dass den Rechten des Betroffenen – vor allem dem Fernmeldegeheimnis – nicht in angemessener Weise Rechnung getragen wird. Wegen der Ähnlichkeit zu Art. 16 kann im Übrigen auf die Ausführungen dort verwiesen werden.

4.5 Artikel 18 – Herausgabeanordnung[953]

(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um ihren zuständigen Behörden die Befugnis zu erteilen, anzuordnen,

> *a) dass eine Person in ihrem Hoheitsgebiet bestimmte Computerdaten, die sich in ihrem Besitz oder ihrer Verfügungsgewalt befinden und die in einem Computersystem oder auf einem Computerdatenträger gespeichert sind, vorzulegen hat und*
>
> *b) dass ein Dienstanbieter, der seine Dienste im Hoheitsgebiet der Vertragspartei anbietet, Kundendaten in Zusammenhang mit diesen Diensten, die sich in seinem Besitz oder seiner Verfügungsgewalt befinden, vorzulegen hat.*

(2) Die Befugnisse und Verfahren nach diesem Artikel unterliegen den Artikeln 14 und 15.

(3) Im Sinne dieses Artikels bedeuten „Kundendaten" alle in Form von Computerdaten oder in anderer Form enthaltenen Informationen, die bei einem Dienstanbieter über Kunden seiner Dienste vorliegen, mit Ausnahme von Verbindungsdaten oder inhaltsbezogenen Daten, durch die folgendes festgestellt werden kann:

> *a) die Art des genutzten Kommunikationsdienstes, die dafür getroffenen technischen Maßnahmen und die Dienstdauer;*
>
> *b) die Identität des Kunden, seine Post- oder Hausanschrift, Telefon- und sonstige Zugangsnummer sowie Angaben über Rechnungsstellung und Zahlung, die auf der Grundlage des Vertrags oder der Vereinbarung in Bezug auf den Dienst zur Verfügung stehen.*
>
> *c) gegebenenfalls andere Informationen über den Ort der Installation der Kommunikationsanlage, die auf der Grundlage des Vertrags oder der Vereinbarung in Bezug auf den Dienst vorliegen.*

4.5.1 Anwendungsbereich

Art. 18 will den Strafverfolgungsbehörden zum einen die Möglichkeit einräumen, gegen beliebige Personen die Herausgabe von Daten, mit Ausnahme zukünftiger Inhalts- und Verbindungsdaten, anordnen zu können. Zum anderen sollen die zuständigen Behörden in die Lage versetzt werden, von den Dienstanbietern die Herausgabe von Kundendaten nach Abs. 3 zu verlangen. Dadurch werden bereits bestehende Editionsbefugnisse auf unkörperliche Daten unabhängig vom zu Grunde liegenden Speichermedium erweitert sowie der Zugriff auf Kundendaten, als dritte Kategorie neben den Inhalts-[954] und Verbindungsdaten[955], explizit normiert. Die Verfasser der Konvention ließen sich von der Überlegung leiten, dass die Anordnung der Herausgabe oftmals den milderen Eingriff zu Durchsuchung und Beschlagnahme darstellt.[956]

4.5.2 Computerdaten und Kundendaten

Die Herausgabeanordnung kann sich nach Art. 1 lit. a) auf „Computerdaten" und nach lit. b) auf „Kundendaten" bei den Dienstanbietern beziehen. Die erste Alternative beinhaltet alle Arten von Daten mit Ausnahme von Inhalts- und Verbindungsdaten zukünftiger Telekommunikationen. Diese Einschränkung ergibt sich zwar nicht aus dem Wortlaut von Art. 18, jedoch aus einem Umkehrschluss zur Existenz der Art. 20 und 21 sowie den Erläuterungen zu Art.

[953] ER Ziff. 170-183
[954] Siehe dazu Art. 21
[955] Siehe dazu Art. 20
[956] ER Ziff. 170

18.[957] In Bezug auf „Verbindungsdaten“ bereits vollendeter Datenübertragungen kann es zu Überschneidungen mit Art. 17 Abs. 1 lit. b) kommen.

Kundendaten im Sinne von Art. 18 Abs. 1 lit. b) werden in Abs. 3 legal definiert. Es handelt sich um alle Daten eines Dienstanbieters über seine Kunden mit Ausnahme der Verbindungs- und Inhaltsdaten. In Betracht kommen daher in erster Linie Informationen, die im Rahmen der Vertragsbeziehung zwischen Dienstanbieter und Kunde gespeichert werden. Dahinstehen kann, ob diese Angaben in Form von Computerdaten nach Art. 1 lit. b) (siehe Kapitel 2.2) oder in schriftlicher Form vorliegen. Kunden im Sinne der Vorschrift sind alle Personen, die Dienste eines TK-Anbieters in Anspruch nehmen, egal ob auf langfristiger oder Call-by-Call (Einzelverbindung), entgeltlicher oder unentgeltlicher Basis. Auch die Daten Dritter werden erfasst, soweit sie den Zugang eines registrierten Kunden benutzen. Die Bedeutung der Kundendaten besteht vor allem darin, Verdächtige zu identifizieren, indem Telefonnummern oder sonstige Kennungen mit persönlichen Daten zusammengeführt werden.

Nach Abs. 3 lit. a) sind Kundendaten alle Informationen über den Nutzer und die Nutzung eines Dienstes: Daten über die Art des Dienstes, die vom Kunden hierfür genutzten technischen Maßnahmen und die Dienstdauer. Technische Maßnahmen sind alle Vorkehrungen, die ein Kunde für die Nutzung eines Dienstes getroffen hat. Hierzu zählt die Reservierung von Nummern und Adressen (z.B. Telefonnummern, URLs, Emailadressen, usw.) ebenso wie die Registrierung von Telefonanlagen und Netzwerkgeräten. An dieser Stelle verschwimmt die Definition der Kunden- mit der der Verbindungsdaten. Lit. b) und c) beziehen darüber hinaus Informationen über die Identität des Nutzers, wie seine Post- und Hausanschrift, Telefon- und Zugangsnummern, Angaben über Rechnungsstellung und Zahlung, usw., sowie gegebenenfalls weitere Informationen über den Ort der Installation der Kommunikationsanlage in den Kreis der Kundendaten mit ein, soweit diese auf Grund des Vertragsverhältnisses erhoben werden dürfen. Der Erläuternde Bericht weist an dieser Stelle darauf hin, dass Art. 18 keine an die Dienstanbieter gerichtete Verpflichtung enthält, die bezeichneten Angaben zu erheben und zu überprüfen.[958] Dies gilt insbesondere für Prepaid-Mobiltelefon-Kunden und die Verwendung von Pseudonymen. In welcher Art und Weise die Daten herauszugeben sind, wird von Art. 18 nicht näher geregelt.

4.5.3 Besitz oder Kontrolle

Die herauszugebenden Daten müssen sich im „Besitz oder in der Verfügungsgewalt“ der Person befinden (engl. *„in that person's possession or control”*), gegen die die Anordnung ergeht. Unter „Besitz“ versteht die Konvention die physische Herrschaft über Daten, soweit dies auf Grund ihrer Unkörperlichkeit möglich ist.[959] Die Formulierung „Verfügungsgewalt“ bezieht sich vor allem auf Netzwerke, d.h. Konstellationen, in denen Daten nicht lokal gespeichert sind, jedoch über Netzwerkverbindungen von Servern auf dem Hoheitsgebiet der anordnenden Vertragspartei abgerufen werden können.[960] Damit ist jedoch nur der legale Zugriff auf Daten in einem Netzwerk gemeint. Die lediglich theoretisch bestehende Möglichkeit, die Verfügungsgewalt unter Verletzung der Rechte Dritter oder sonstiger Vorschriften auszuüben, ist nicht gemeint.[961] Abs. 1 lit. a) erlaubt die Anordnung der Herausgabe von Computerdaten gegen beliebige Personen; Lit. b) richtet sich gegen Dienstanbieter und die in ihrem Besitz oder ihrer Verfügungsgewalt befindlichen Kundendaten. Einschränkend ist zu beachten, dass

[957] ER Ziff. 180
[958] ER Ziff. 181
[959] ER Ziff. 173
[960] ER Ziff. 173
[961] ER Ziff. 173

nur solche Kundendaten von den Anbietern herauszugeben sind, die in Zusammenhang zu solchen Diensten stehen, die auf dem Hoheitsgebiet der anordnenden Partei erbracht werden.

4.5.4 Bedingungen und Garantien

Art. 18 Abs. 2 verweist auf die Bedingungen und Garantien der Art. 14 und 15. Ein Mindestschutzniveau der Rechte der Anordnungsadressaten ist weder in Bezug auf die Anordnungszuständigkeit noch auf die Art der Daten vorgesehen. Insbesondere bestimmt die Norm keine datenschutzrechtliche Anforderung. Als Einschränkung der Befugnisse aus Art. 18 ist nur die Formulierung in Art. 14 Abs. 1 zu sehen, dass sich Maßnahmen des 2. Abschnitts – und damit auch die Herausgabeanordnung – auf „[…] besondere strafrechtliche Ermittlungen oder Verfahren […]“ beziehen müssen. Die Herausgabeanordnung muss daher in personeller und sachlicher Hinsicht auf bestimmte Personen, Telefonnummern, Emailadressen, usw. beschränkt werden. Eine unbegrenzte Datensammlung soll auf diese Weise vermieden werden.

4.5.5 Vergleichbare Befugnisnormen im deutschen Strafprozessrecht

Die Herausgabe bestimmter Gegenstände an die Strafverfolgungsbehörden wird im deutschen Strafprozessrecht durch § 95 StPO geregelt. In Bezug auf „Bestandsdaten“ gibt § 89 Abs. 6 TKG die Möglichkeit, für das Vertragsverhältnis zwischen Anbieter und Nutzer von Telekommunikationsdiensten relevante Informationen abzufragen.

4.5.5.1 § 95 StPO – [Herausgabepflicht]

§ 95 StPO sieht eine Pflicht zur Herausgabe (Edition) von Gegenständen im Sinne von § 94 StPO vor. Die Vorschrift statuiert damit eine aktive Mitwirkungspflicht des Herausgabepflichtigen, die nach § 95 Abs. 2 StPO durch die Ordnungsmittel des § 70 StPO erzwungen werden kann. Ihr Hauptanwendungsbereich besteht darin, dass ein Beweisgegenstand im Rahmen einer Durchsuchung nicht gefunden und deshalb auch nicht beschlagnahmt werden kann.[962] Durch die Formulierung „Gegenstände der vorbezeichneten Art“ nimmt § 95 StPO unmittelbar Bezug auf § 94 StPO. Objekte des Herausgabeverlangens können ebenso wie dort nur Gegenstände sein. Diese müssen „vorgelegt“ oder „ausgeliefert“ werden, was auf das Erfordernis ihrer Körperlichkeit hindeutet. Welche Konsequenzen sich hieraus für unkörperliche Daten ergeben, ist Gegenstand der folgenden Darstellungen.

4.5.5.1.1 Gegenstände der vorbezeichneten Art

„Gegenstände der vorbezeichneten Art“ sind grundsätzlich solche, die der Sicherstellung nach § 94 StPO unterliegen. Aus den Verben „vorlegen“ und „ausliefern“ ergibt sich darüber hinaus, dass nur bewegliche Gegenstände in Betracht kommen.[963] Da sich in Bezug auf den Gegenstandsbegriff im Übrigen keine Abweichungen zu § 94 StPO ergeben, wird insoweit auf die Ausführungen in Kapitel 4.3.7.2 verwiesen. Unkörperliche Daten unterliegen danach mangels Gegenständlichkeit nicht der Herausgabepflicht. Es kann jedoch die Herausgabe der Datenträger angeordnet werden.

Es stellt sich jedoch ebenso wie im Rahmen des § 94 StPO die Frage, inwieweit die Heraus-

[962] Löwe/Rosenberg – *Schäfer* § 95 Rn 1; SK/StPO – *Rudolphi* § 95 Rn 1
[963] KK – *Nack* § 95 Rn 1; Löwe/Rosenberg – *Schäfer* § 95Rn 1

gabe von Fotokopien (Urkunden) bzw. sonstigen Kopien (Daten) als milderes Mittel zur Herausgabe des gesamten Speichermediums angeordnet werden kann. Ein Teil der Literatur argumentiert vor allem in Hinblick auf die „elektronischen" Buchführungsunterlagen eines Kaufmanns nach §§ 239 Abs. 4, 257 Abs. 3 HGB, dass sich das Editionsverlangen in Verbindung mit § 261 HGB auf die Herausgabe lesbarer Reproduktionen beziehe, während § 94 StPO den Datenträger selbst betreffe.[964] Andere Autoren beschränken sich nicht auf die handelsrechtlichen Unterlagen, sondern bejahen allgemein die Pflicht zur Herausgabe von Kopien als milderen Eingriff zur Herausgabe der Originals.[965] Gestützt auf eine solche Argumentation ließe sich auch die Herausgabe von Daten begründen, die zuvor auf einen Datenträger kopiert wurden. Diese Meinung, die sich wie bei der Beschlagnahme von Daten im Wesentlichen auf eine „a maiore ad minus"-Argumentation stützt, ist – wie schon dort[966] – abzulehnen.

Zum einen ist die Gegenstandsqualität von Daten unabhängig von der Verhältnismäßigkeit eines Eingriffs in die Rechte des Betroffenen zu beurteilen. Das Übermaßverbot erfüllt dogmatisch die Funktion, den Anwendungsbereich einer Eingriffsnorm zu begrenzen[967], nicht ihn noch auszuweiten, indem das Tatbestandsmerkmal „Gegenstände" extensiv interpretiert wird.[968] Zum anderen statuiert § 95 StPO nicht wie die Sicherstellungsnormen lediglich eine Duldungspflicht des Betroffenen, sondern verlangt ihm eine aktive Mitwirkung ab. Dies kann mit den Ordnungs- und Zwangsmitteln des § 70 StPO durchgesetzt werden, so dass die Herausgabeanordnung eine größere Eingriffsintensität als die Sicherstellung gewinnen kann. Daraus folgt, dass die Eingriffsvoraussetzungen restriktiv zu behandeln sind. Weiterhin stellen die handelsrechtlichen Unterlagen wohl einen Sonderfall dar, der nicht verallgemeinerungsfähig ist. Die Möglichkeit der elektronischen Buchführung soll den Kaufleuten einen rationellen Geschäftsbetrieb erlauben.[969] Elektronische Unterlagen müssen im Gegenzug für dieses Zugeständnis nach § 239 Abs. 4 Satz 2 HGB „[…] jederzeit innerhalb angemessener Frist […]" lesbar gemacht werden können. Werden die Unterlagen angefordert, regelt § 261 HGB neben der Herausgabe- auch die Kostentragungspflicht des betroffenen Kaufmanns. Derartige Sonderregelungen fehlen bzgl. anderer Kopien und Daten und verdeutlichen den Ausnahmecharakter der handelsrechtlichen Vorschriften. Aber auch eine Interpretation des Gegenstandsbegriffs in § 95 StPO nach grammatischen, historischen, systematischen und teleologischen Gesichtspunkten ergibt, dass das Editionsverlangen nur die Pflicht zur Herausgabe bereits existierender körperlicher Gegenstände und nicht die Anfertigung neuer Gegenstände umfassen kann.[970] Als Ergebnis bleibt daher festzuhalten, dass eine Herausgabe von Daten mangels Gegenstandsqualität nicht in Betracht kommt. Eine Pflicht zur Anfertigung von Kopien auf Datenträgern, die herausgabefähige Gegenstände nach § 95 StPO sein könnten, besteht darüber hinaus nicht. Die weiteren Ausführungen beziehen sich daher auf die Herausgabe der stofflichen Datenträger.

4.5.5.1.2 Gewahrsam des Herausgabepflichtigen

Die Editionspflicht trifft nur den jeweiligen Gewahrsamsinhaber. Anders als im Rahmen der Sicherstellung ist eine Gewahrsamsbeziehung zwischen dem Normadressaten und der herauszugebenden Sache konstitutive Bedingung für das Herausgabeverlangen. Damit soll sicherge-

[964] Löwe/Rosenberg – *Schäfer* § 95 Rn 1; Meyer-Goßner § 95 Rn 8; aA: Bär, S. 418 ff., der sowohl die direkte als auch die analoge Anwendung von § 261 HGB im Strafprozessrecht mit überzeugenden Gründen ablehnt.
[965] KK – *Nack* § 95 Rn 1; SK/StPO – *Rudolphi* § 95 Rn 8
[966] Siehe Kapitel 4.3.7.2
[967] Maurer, Staatsrecht I, § 8 Rn 55 mwN
[968] Siehe zum Ganzen Kapitel 4.3.7.2.
[969] Löwe/Rosenberg – *Schäfer* § 95 Rn 3
[970] Ausführlich hierzu: Bär, S. 397-403

stellt werden, dass das Gebot zur aktiven Mitwirkung auch erfüllt werden kann. Anderenfalls bestünden rechtsstaatliche Bedenken gegen die Norm. Zur Ausfüllung des Gewahrsamsbegriffs orientiert sich die Literatur im Wesentlichen am materiell-rechtlichen Gewahrsam, wie etwa im Rahmen von § 242 StGB.[971] Das materielle Recht versteht unter „Gewahrsam" ein tatsächliches Herrschaftsverhältnis zwischen einer Person und einer Sache.[972] In Bezug auf körperliche Speichermedien bereitet der Gewahrsamsbegriff keine größeren Schwierigkeiten. Da der Herausgabepflichtige den Gegenstand „vorzulegen" bzw. „auszuliefern" hat, erfüllt er seine Mitwirkungspflicht bereits, indem er den Datenträger übergibt. Sind die Daten verschlüsselt oder nur mit einer besonderen Benutzerberechtigung zugänglich, ist der Anordnungsadressat nicht verpflichtet, den Zugriff auf diese Daten zu ermöglichen. Anderenfalls würde die Herausgabepflicht zur Beweisbeschaffungspflicht modifiziert werden.[973] Da Gegenstand des Herausgabeverlangens nur der körperliche[974] Datenträger ist, kommt es für die Beurteilung der Gewahrsamsverhältnisse allein auf die Herrschaft über das Speichermedium und nicht auf logische Zugriffsrechte auf einzelne Dateien an. Das *tatsächliche*[975] Herrschaftsverhältnis kann immer nur am Datenträger ansetzen und sich auf die gespeicherten Daten erstrecken. Bei Netzwerklaufwerken bedeutet dies, dass es nicht auf die logischen Zugriffsrechte der Nutzer, sondern auf die physische Einwirkungsmöglichkeit durch den Betreiber des Servers ankommt. Die gegenteilige Ansicht[976], die auf die Zugriffsrechte an den Daten abstellt, verkennt, dass Daten keinen „Gegenstand der vorbezeichneten Art" darstellen, sondern allein das Speichermedium, d.h. in der Regel die Festplatte, diese Anforderung erfüllt. Der Nutzer, der mittels eines Netzwerkes auf die Daten zugreifen kann, übt kein Herrschaftsverhältnis über die Speichermedien des Betreibers aus. Er kontrolliert allein die unkörperlichen Daten, wobei auch hier eine Eingriffsmöglichkeit durch den Betreiber des Servers besteht, und nicht die Sachsubstanz des Datenträgers.

4.5.5.1.3 Beschränkungen im Anwendungsbereich von § 95 StPO

§ 95 StPO enthält dem Wortlaut nach keine Beschränkungen. Insbesondere erlaubt er vom Wortlaut her eine Herausgabeanordnung auch gegen Beschuldigte und gegen Personen, die nach den §§ 52 ff. StPO zur Verweigerung des Zeugnisses berechtigt sind. Nach allgemeiner Ansicht[977] im Schrifttum steht der Editionspflicht des Beschuldigten jedoch der *„nemo tenetur se ispsum accusare"*-Grundsatz entgegen. Danach muss niemand sich an seiner eigenen Überführung aktiv beteiligen. Zwar wurde dieser Grundsatz in der StPO nicht kodifiziert. Nach der Rechtsprechung des BVerfG ergibt er sich jedoch aus dem allgemeinen Persönlichkeitsrecht und der Menschenwürdegarantie der Art. 2 Abs. 1, 1 Abs. 1 GG.[978] Der Beschuldigte kann daher nicht zur Vorlage oder Auslieferung von Beweisgegenständen herangezogen werden. Gegenüber Zeugnisverweigerungsberechtigten kann die Herausgabe zwar zunächst angeordnet werden. Auf Grund von § 95 Abs. 2 Satz 2 StPO, der die Festsetzung der in § 70 StPO genannten Ordnungs- und Zwangsmittel verbietet, bleibt die Weigerung der Herausgabe allerdings folgenlos. Im Übrigen wird durch die Bezugnahme auf „Gegenstände der vorbezeichneten Art" verdeutlicht, dass die Beschlagnahmeverbote des § 97 StPO zu beachten

[971] Bär, S. 410; Löwe/Rosenberg – *Schäfer* § 95 Rn 4
[972] Sch/Sch – *Eser* § 242 Rn 23; Tröndle/Fischer § 242 Rn 11
[973] Bär, S. 413, für den „Online-Zugriff" auf beweisrelevante Daten; Löwe/Rosenberg – *Schäfer* § 95 Rn 3; ebenso: Leicht IuR 1986, 346 (352); Nelles JuS 1987, 51 (53) sowie Sieber, The International Emergence of Criminal Information Law, S. 54
[974] KK – *Nack* § 95 Rn 1; Löwe/Rosenberg – *Schäfer* § 95 Rn 2, 4; Meyer-Goßner § 95 Rn 3
[975] Löwe/Rosenberg – *Schäfer* § 95 Rn 4; Sch/Sch – *Eser* § 242 Rn 23; Tröndle/Fischer § 242 Rn 11
[976] Bär, S. 413
[977] KK – *Nack* § 95 Rn 2; Löwe/Rosenberg – *Schäfer* § 95 Rn 5; Meyer-Goßner § 95 Rn 5
[978] BVerfGE 38, 105 (113); 55, 144 (150); 56, 37 (45)

sind.[979]

4.5.5.1.4 Verhältnismäßigkeit

Wie bei allen Eingriffen in die Rechte Privater durch die öffentliche Gewalt ist der Verhältnismäßigkeitsgrundsatz zu beachten. Zweck und Mittel der Zwangsmaßnahme müssen in einem angemessenen Verhältnis stehen. Die Eingriffsintensität staatlicher Maßnahmen soll dadurch auf ein im Einzelfall angemessenes Niveau angepasst werden. Das Übermaßverbot kann nicht dazu herangezogen werden, den Anwendungsbereich einer Eingriffsnorm auszuweiten. Anderenfalls würde die dogmatische Funktion dieses Rechtsgrundsatzes umgekehrt werden. Die insoweit von Teilen der Literatur vertretene Ansicht, dass der Beschuldigte zur Herausgabe von Kopien oder lesbaren Reproduktionen als milderer Eingriff zur Edition der Originale herangezogen werden könne, ist mit Ausnahme handelsrechtlicher Unterlagen abzulehnen.[980] Der Gegenstandsbegriff der StPO ist ein körperlicher, der nicht unter Zuhilfenahme missverstandener Verhältnismäßigkeitserwägungen auf unkörperliche Daten ausgedehnt werden kann.

4.5.5.1.5 Ergebnis zu § 95 StPO

Im Gegensatz zu Art. 18 bezieht sich § 95 StPO nur auf körperliche Objekte. Daten sind weder „Gegenstände der vorbezeichneten Art“, d.h. solche im Sinne von § 94 StPO, noch können sie „vorgelegt“ oder „ausgeliefert“ werden. Auch der Umweg über eine extensive Auslegung des Verhältnismäßigkeitsgrundsatzes kann, da er seine dogmatische Funktion ins Gegenteil verkehren würde, nicht zu dem Ergebnis führen, dass Daten auf Grund einer Anordnung nach § 95 StPO herauszugeben wären.

4.5.5.2 § 89 Abs. 6 TKG – Abfrage von Bestandsdaten

§ 89 Abs. 6 TKG erlaubt die Abfrage so genannter „Bestandsdaten“. Dabei handelt es sich um Informationen der Anbieter von Telekommunikationsdiensten über die Verträge mit den Benutzern dieser Dienstleistungen. Im Gegensatz zu Art. 18 Abs. 1 lit. b) ist ein Zugriff der Strafverfolgungsbehörden nur möglich „im Einzelfall“ und „soweit“ dies für bestimmte hoheitliche Aufgaben erforderlich ist. In Betracht kommen in erster Linie die Verfolgung von Straftaten und Ordnungswidrigkeiten sowie nachrichtendienstliche Tätigkeiten. Weder den Kunden noch Dritten darf die Auskunftserteilung mitgeteilt werden.

4.5.6 Bewertung Art. 18

Art. 18 Abs. 1 lit. a) geht in Bezug auf die Herausgabe beliebiger Daten, mit Ausnahme von Inhalts- und Verbindungsdaten, über das Herausgabegebot des § 95 StPO hinaus, da er nicht auf körperliche Gegenstände beschränkt ist. Etwas anderes gilt jedoch für „Kundendaten“ nach Art. 18 Abs. 1 lit. b), die weitgehend mit den „Bestandsdaten“ im Sinne des TKG korrespondieren dürften. Diesbezüglich ergeben sich keine gravierenden Unterschiede. Kritisch bleibt anzumerken, dass Abs. 1 lit. a) die Rechte von Beschuldigten und Personen mit Zeugnisverweigerungsrechten, etwa Geistliche und Strafverteidiger, nicht in angemessener Weise berücksichtigt. Insoweit sind keine Ausnahmen von der Herausgabepflicht vorgesehen. In

[979] KK – *Nack* § 95 Rn 2; Löwe/Rosenberg – *Schäfer* § 95 Rn 2
[980] Siehe dazu Kapitel 4.5.5.1.1. Im Ergebnis ebenso: Bär, S. 416

Bezug auf Kundendaten, Abs. 1 lit. b), besteht ein wesentliches Defizit darin, dass der behördliche Zugriff nicht auf Einzelfälle im Zusammenhang mit der Erfüllung hoheitlicher Aufgaben beschränkt wurde. Statt in beiden Fällen detaillierte Regelungen zum Schutz der Rechte der Betroffenen vorzusehen, enthält Abs. 2 lediglich einen allgemeinen Hinweis auf die Art. 14 und 15, die den Anwendungsbereich sowie Bedingungen und Garantien für alle Befugnisse der Konvention definieren.

4.6 Artikel 19 – Durchsuchung und Beschlagnahme gespeicherter Computerdaten[981]

(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um ihren zuständigen Behörden die Befugnis zu erteilen,

a) ein Computersystem oder einen Teil davon sowie die darin gespeicherten Computerdaten und

b) einen Computerdatenträger, auf dem Computerdaten gespeichert sein können,

in ihrem Hoheitsgebiet zu durchsuchen oder in ähnlicher Weise darauf Zugriff zu nehmen.

(2) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um sicherzustellen, dass ihre Behörden, wenn sie ein bestimmtes Computersystem oder einen Teil davon nach Absatz 1 Buchstabe a) durchsuchen oder in ähnlicher Weise darauf Zugriff nehmen und Grund zu der Annahme haben, dass die gesuchten Daten in einem anderen Computersystem oder einem Teil davon in ihrem Hoheitsgebiet gespeichert sind, und diese Daten von dem ersten System aus rechtmäßig zugänglich oder verfügbar sind, die Durchsuchung oder den ähnlichen Zugriff rasch auf das andere System ausdehnen können.

(3) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um ihren zuständigen Behörden die Befugnis zu erteilen, Computerdaten, auf die nach Absatz 1 oder 2 Zugriff genommen wurde, zu beschlagnahmen oder in ähnlicher Weise sicherzustellen. Diese Maßnahmen umfassen die Befugnis,

a) ein Computersystem oder einen Teil davon oder einen Computerdatenträger zu beschlagnahmen oder in ähnlicher Weise sicherzustellen,

b) eine Kopie dieser Computerdaten anzufertigen und zurückzubehalten,

c) die Integrität der einschlägigen gespeicherten Computerdaten zu erhalten und

d) diese Computerdaten in dem Computersystem, auf das Zugriff genommen wurde, unzugänglich zu machen oder sie daraus zu entfernen.

(4) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um ihren zuständigen Behörden die Befugnis zu erteilen, anzuordnen, dass jede Person, die Kenntnisse über die Funktionsweise des Computersystems oder Maßnahmen zum Schutz der darin enthaltenen Daten hat, in vernünftigem Maß die notwendigen Auskünfte zu erteilen hat, um die Durchführung der in den Absätzen 1 und 2 genannten Maßnahmen zu ermöglichen.

(5) Die Befugnisse und Verfahren nach diesem Artikel unterliegen den Artikeln 14 und 15.

4.6.1 Anwendungsbereich

Art. 19 enthält in den Absätzen 1 und 2 Bestimmungen zur Durchsuchung von Computersystemen, Datenträgern, Daten sowie Netzwerken. Abs. 3 bezieht sich auf die Beschlagnahme dieser Objekte und Absatz 4 regelt – an einer nach deutschem Verständnis unerwarteten Stelle – die Auskunftspflichten derjenigen Personen, die mit dem betroffenen Computersystem usw. vertraut sind. Dem Erläuternden Bericht zufolge besteht der vorrangige Zweck der Vorschrift darin, bestehende Befugnisse zu modernisieren und zu harmonisieren.[982] Unkörperliche Computerdaten sollen im Ergebnis wie stoffliche Datenträger der Durchsuchung und Beschlagnahme durch die zuständigen Behörden unterliegen. Absatz 4 trägt in diesem Zusammenhang dem Umstand Rechnung, dass Computerdaten vielfach gegen den Zugriff Dritter, also auch

[981] ER Ziff. 184-204
[982] ER Ziff. 184

der Ermittlungsbehörden, gesichert sind, so dass ein Zugang zu den Informationen oftmals nur unter Heranziehung der Systemkundigen möglich ist. Einschränkungen im Anwendungsbereich von Art. 19 ergeben sich aus dem Verweis in Abs. 5 auf die Art. 14 und 15 in Bezug auf den Geltungsbereich und die Bedingungen und Garantien nach nationalem Recht.

4.6.2 Abs. 1 und 2 – Durchsuchung

Abs. 1 und 2 erlauben die Durchsuchung bestimmter Objekte und gehen von der Prämisse aus, dass die Grundsätze, die für die Durchsuchung körperlicher Gegenstände entwickelt wurden, auch auf die Durchsuchung unkörperlicher Gegenstände übertragen werden können. Dementsprechend soll durch die Abs. 1 und 2 lediglich der Kreis der durchsuchungsfähigen Objekte erweitert werden. Dies ist erforderlich, da die Durchsuchungsbefugnisse in den Rechtsordnungen vieler Unterzeichnerstaaten noch auf körperliche Gegenstände beschränkt sind. In diesen Fällen ist umstritten, inwieweit die herkömmlichen Rechtsgrundlagen für ein EDV-Umfeld zur Geltung kommen können. Insbesondere die Durchsuchung von Netzwerken, die die Daten einer Vielzahl von Nutzern beherbergen sowie große räumliche Distanzen überbrücken können, erscheint besonders problematisch. Bestimmte Durchsuchungszwecke, wie etwa das Auffinden von Beweismitteln oder die Ergreifung des Beschuldigten, werden von Art. 19 Abs. 1 und 2 nicht ausdrücklich benannt. Eine Ergreifungsdurchsuchung kann wegen der Beschaffenheit der Durchsuchungsobjekte allerdings ausgeschlossen werden, so dass es allein auf das Auffinden beweisrelevanter Informationen ankommen kann.

4.6.2.1 Durchsuchungsobjekte

Durchsuchungsobjekte sind nach Abs. 1 lit. a) „Computersysteme oder Teile davon“ sowie die „darin gespeicherten Daten“; nach lit. b) „Computerdatenträger, auf denen Computerdaten gespeichert sein können“. Dadurch wird die Durchsuchung körperlicher Gegenstände nach Daten und die Durchsuchung unkörperlicher Daten nach bestimmten Inhalten ermöglicht.[983] Wegen der Reichweite des Begriffs „Computersysteme“ kann auf die Darstellungen in Kapitel 2.1 verwiesen werden. „Computerdatenträger“ dürften bereits von dieser umfassenden Definition erfasst sein und wurden daher wohl lediglich zu Klarstellungszwecken in lit. b) eigens erwähnt.

Abs. 2 erlaubt die Durchsuchung eines „anderen Computersystems“ nach darin gespeicherten Daten, solange diese Daten von dem ursprünglich durchsuchten System aus in rechtmäßiger Weise zugänglich oder verfügbar sind. Probleme können sich bei der Abgrenzung von Abs. 1 und Abs. 2 aus dem weiten Verständnis der „Computersysteme“ nach Art. 1 lit. a) ergeben, nach dem auch vernetzte Rechner zum Teil als ein Computersystem betrachtet werden.[984] Der Erläuternde Bericht bezeichnet LANs, die private Übertragungswege benutzen, als ein Computersystem, wohingegen mehrere Systeme sich dadurch auszeichnen, dass sie öffentliche Telekommunikationsnetze zur Übertragung benutzen.[985] Abs. 1 dürfte im Unterschied zu Abs. 2 daher vorwiegend auf kleinflächige Netze Anwendung finden. Differenzierte Abgrenzungskriterien sind weder dem Wortlaut des Art. 19 Abs. 1 und 2 noch Art. 1 lit. a) zu entnehmen.

[983] ER Ziff. 191
[984] Eingehend zum Begriff des Computersystems im Sinne von Art. 1 lit. a): Kapitel 2.1
[985] ER Ziff. 188

4.6.2.2 Durchsuchungshandlung

Abs. 1 und Abs. 2 ermöglichen die „Durchsuchung und den Zugriff in ähnlicher Weise". Unter „Durchsuchen" ist das Suchen, Lesen, Überprüfen und Durchsehen von Daten zu verstehen.[986] Begrifflich werden das Suchen *nach* Daten und das Suchen *in* Daten – im Sinne eines Untersuchens von Daten – erfasst.[987] Die einheitliche Terminologie will auf die Nähe zur traditionellen Durchsuchung hinweisen. Der Begriff „Zugriff" hat eine weitgehend neutrale Bedeutung. Er wurde verwendet, weil er besser in ein technologisches Umfeld zu passen schien. Beide Begriffe zusammen sollen eine Verbindung traditioneller Durchsuchungskonzepte mit neuen Durchsuchungsobjekten zum Ausdruck bringen.[988] In Hinblick auf die technische Umsetzung äußert sich der Erläuternde Bericht nicht weiter. Wenn jedoch unkörperliche Daten, die ohne entsprechende Ausrüstung nicht visualisiert werden können, in den Kreis durchsuchungsfähiger Objekte miteinbezogen werden, bedeutet dies, dass auch Vorgänge wie die Inbetriebnahme fremder EDV-Anlagen, die Benutzung von Programmen, usw. erfasst sein müssen.

4.6.3 Abs. 3 – Beschlagnahme und Sicherstellung in ähnlicher Weise

Abs. 3 erlaubt die „Beschlagnahme oder Sicherstellung in ähnlicher Weise" von Computerdaten. Darunter ist einerseits die körperliche Wegnahme[989] des Datenträgers, auf dem die Daten gespeichert sind, zu verstehen, lit. a), sowie andererseits weitere Maßnahmen in Bezug auf unkörperliche Daten, um einen ähnlichen Erfolg wie durch die physische Wegnahme des Speichermediums zu bewirken. Die Konvention verwendet für diese zweite Alternative die Formulierung „Sicherstellung in ähnlicher Weise".[990] Abs. 3 bezieht sich nur auf diejenigen Daten, die im Rahmen einer Durchsuchung nach den Abs. 1 und 2 gefunden wurden. Andere Daten, werden nicht eigens erwähnt. Daraus folgt zum einen, dass die Verfasser der Konvention von einem engen Verhältnis zwischen Durchsuchung und Beschlagnahme ausgingen, sowie zum anderen, dass andere Daten als solche, die durch Maßnahmen nach den Abs. 1 und 2 lokalisiert wurden, offenbar nicht nach Abs. 3 beschlagnahmt werden können.

4.6.4 Objekte der Beschlagnahme

Objekte der Beschlagnahme im Sinne von Abs. 3 Satz 1 sind „Computerdaten".[991] Auf Grund ihrer Unkörperlichkeit kommt eine Wegnahme bereits begrifflich nicht in Betracht. Abs. 3 Satz 2 präzisiert daher Satz 1, indem er bestimmte Beschlagnahmemodalitäten konkret benennt. Zunächst kommt die Wegnahme des körperlichen Speichermediums, auch des ganzen Computersystems, in Betracht, lit. a). Da es sich um stoffliche Gegenstände handelt, ergeben sich keine Besonderheiten zur herkömmlichen Beschlagnahme. Lit. b) löst sich vom körperlichen Speichermedium, indem er die Anfertigung von Kopien der zu beschlagnahmenden Daten erlaubt. Um den Inhaber der Daten daran zu hindern, an der bei ihm verbleibenden Kopie Änderungen vorzunehmen, sieht lit. d) weiterhin die Möglichkeit vor, die Daten dort, wo sie beschlagnahmt wurden, unzugänglich zu machen oder gänzlich zu entfernen, ohne sie jedoch permanent zu löschen, um sie gegebenenfalls nach dem Ende der Untersuchung wiederherzustellen.[992] Maßnahmen nach lit. d) ergänzen daher solche nach lit. b) hinsichtlich des Ziels,

[986] ER Ziff. 189, 190
[987] Siehe Fn 983
[988] ER Ziff. 191
[989] ER Ziff. 197
[990] ER Ziff. 197
[991] Siehe dazu Kapitel 2.2.
[992] ER Ziff. 198

ein behördliches Herrschaftsverhältnis über Daten zu begründen, das demjenigen entspricht, das durch die Wegnahme physischer Gegenstände entsteht.[993] Ein Unzugänglichmachen im Sinne von lit. c) bezieht sich vor allem auf den Einsatz von Verschlüsselungsverfahren, um Dritten den Zugang zu den Daten zu vereiteln. Diese Variante ist vor allem für Fälle des Zugriffs auf Schadprogramme wie Viren oder Würmer vorgesehen.[994]

Als Sonderfall im Bereich der Beschlagnahmeobjekte betrachtet der Erläuternde Bericht E-mails.[995] In technischer Hinsicht lassen sich vom Erstellen der elektronischen Nachricht bis zum Lesen durch den Empfänger unterschiedliche Übertragungsstadien differenzieren, während derer die Emails unter anderem auf Servern der Maildienstleister „ruhen". Weder der Wortlaut der Konvention noch der Erläuternde Bericht[996] nehmen Stellung zu der Frage, ob Emails beschlagnahmt werden können oder ob auf sie nur im Wege einer Überwachung der Telekommunikation zugegriffen werden kann.[997]

4.6.5 Abs. 4 – Erteilung von Auskünften

Abs. 4 sieht vor, dass systemkundige Personen zur Erteilung von Auskünften über die Funktionsweise einer Computeranlage herangezogen werden können, um Durchsuchungen nach den Abs. 1 und 2 zu ermöglichen. Diese Vorschrift basiert auf der Überlegung, dass Computersysteme und Daten oft verschlüsselt oder durch Passwörter gesichert sind bzw. die technische Komplexität einer EDV-Anlage eine Durchsuchung für Außenstehende, wozu auch die Strafverfolgungsbehörden zählen, nahezu unmöglich machen.[998]

Innerhalb des genannten Personenkreises wird nicht zwischen verdächtigen und dritten Personen unterschieden. In Bezug auf den Verdächtigen kann Abs. 4 wegen des „*nemo tenetur, se ipsum accusare*"-Grundsatzes nicht zur Anwendung kommen. Dabei handelt es sich um ein Prinzip, das auch dem internationalen Recht nicht unbekannt ist, auf das Art. 19 Abs. 5 iVm Art. 15 Abs. 1 verweisen. Namentlich spricht Art. 14 Abs. 3 lit. g) des „Internationalen Paktes der Vereinten Nationen über bürgerliche und politische Rechte"[999] von dem Grundrecht eines Beschuldigten, „[…] *not to be compelled to testify against himself or to confess guilt*." Im Ergebnis kann Abs. 4 sich daher nicht auf den Beschuldigten beziehen.

Die Auskunftserteilung ist auf die „notwendigen Auskünfte, um die in Abs. 1 und 2 genannten Maßnahme zu ermöglichen" „in einem vernünftigen Maß" beschränkt. Unter einem „vernünftigen Maß" versteht der Erläuternde Bericht[1000] vor allem die Weitergabe von Passwörtern und Informationen über weitere Sicherheitsmaßnahmen, soweit der Geheimnisbereich anderer Nutzer und die Vertraulichkeit von Daten nicht übermäßig verletzt werden. Die Bestimmung, wann dies der Fall ist, ist im Einzelnen dem nationalen Gesetzgeber überlassen. Die Pflicht zur Auskunftserteilung soll auch die Weitergabe der angeforderten Daten in verständlicher und lesbarer Form an die zuständigen Behörden umfassen.

[993] ER Ziff. 197, 199
[994] ER Ziff. 198
[995] ER Ziff. 190
[996] ER Ziff. 190
[997] Auch im deutschen Recht umstritten. Siehe dazu Kapitel 4.8.4.2.
[998] ER Ziff. 200 f.
[999] Siehe dazu Kapitel 4.2.2.
[1000] ER Ziff. 202

4.6.6 Vergleichbare Befugnisse im deutschen Strafprozessrecht

Art. 19 stellt eine „Sammelvorschrift“ dar, die nach deutschem Verständnis separate Befugnisse in einem Artikel bündelt. Die folgenden Ausführungen werden daher die Durchsuchungs-, Beschlagnahme- und Zeugen- bzw. Sachverständigenvorschriften der StPO in den für einen Vergleich relevanten Punkten beleuchten.

4.6.6.1 §§ 102 ff. StPO – [Durchsuchung]

Die §§ 102 ff. erlauben die Durchsuchung von Personen, Sachen und Wohnungen von Verdächtigen und anderen Personen. Sie beschränken die Grundrechte aus Art. 2 und 13 GG.[1001] Systematisch unterscheidet die StPO zwischen Durchsuchungen beim Verdächtigen, § 102 StPO, und bei Dritten, § 103 StPO. Die Anordnungskompetenz wird durch § 105 Abs. 1 StPO geregelt, während die §§ 104, 105 Abs. 2 und 3, 106, 107 und 110 StPO die Modalitäten des Durchsuchungsverfahrens regeln. Da Art. 19 nicht zwischen Durchsuchungen beim Verdächtigen oder bei Dritten unterscheidet, werden im Folgenden beide Eingriffsermächtigungen nach deutschem Recht, die sich in struktureller Hinsicht stark ähneln, untersucht. Während § 102 StPO die Ergreifung des Verdächtigen (sog. Ergreifungsdurchsuchung) sowie das Auffinden von Beweismitteln (sog. Ermittlungsdurchsuchung) als Durchsuchungszwecke bezeichnet, spricht § 103 StPO von der Ergreifung des Beschuldigten sowie der Verfolgung von Spuren oder der Beschlagnahme bestimmter Gegenstände. Trotz dieser Abweichungen im Wortlaut unterscheiden sich die Durchsuchungszwecke beider Normen nach allgemeiner Ansicht in sachlicher Hinsicht nicht.[1002] Da die Durchsuchung von Datenträgern aus offensichtlichen Gründen nicht der Ergreifung des Beschuldigten dient, soll die Ergreifungsdurchsuchung im Weiteren nicht näher untersucht werden. Von den Vorschriften in Bezug auf das Durchsuchungsverfahren weist nur § 110 StPO computerspezifische Besonderheiten auf.

4.6.6.1.1 Durchsuchungsobjekte

Die Durchsuchungsobjekte unterscheiden sich bei den §§ 102 und 103 nicht. Die insoweit einhellige Ansicht in der Kommentarliteratur[1003] folgert dies daraus, dass beide Normen grundsätzlich den gleichen Durchsuchungsbegriff verwenden, der durch § 103 Abs. 1 Satz 2 StPO lediglich auf Gebäude erweitert wird. Die folgenden Ausführungen gelten daher sowohl für Durchsuchungen beim Verdächtigen als auch bei anderen Personen.

Die §§ 102 f. StPO erlauben die Durchsuchung der Wohnung, der Person und der Sachen des Betroffenen sowie im Ausnahmefall des Verdachts einer Straftat nach § 129a StGB ganzer Gebäude. Damit wird eine räumlich gegenständliche Sphäre abgegrenzt, in der der grundrechtliche Schutz des Betroffenen auf Grund der strafprozessualen Eingriffsermächtigungen eingeschränkt ist. Dieser örtlichen Beschränkung der Durchsuchung kommt im Bereich der Durchsuchung von Netzwerken eine besondere Bedeutung zu, die später noch zu erörtert sein wird. Zunächst soll jedoch die Frage beantwortet werden, inwieweit die StPO die Durchsuchung von Sachen nach unkörperlichen Daten ermöglicht.[1004] Bei der Durchsuchung einer EDV-Anlage kommt es nicht vorrangig darauf an, Bestandteile eines Computers als Augen-

[1001] Meyer-Goßner § 102 Rn 1; SK/ StPO – *Rudolphi* Vorbemerkung vor § 94 Rn 13
[1002] KK – *Nack* § 102 Rn 4; Löwe/Rosenberg – *Schäfer* § 102 Rn 23; Meyer-Goßner § 102 Rn 12 f., § 103 Rn 5 f.
[1003] KK – *Nack* § 103 Rn 3; Löwe/Rosenberg – *Schäfer* § 103 Rn 13; Meyer-Goßner § 103 Rn 3; SK/StPO – *Rudolphi* § 103 Rn 5
[1004] Schnabl JURA 2004, 379 (381)

scheinsobjekte über ihre äußere Beschaffenheit zu suchen, sondern von entscheidender Bedeutung sind die Informationen, die sich in einem Computersystem befinden. Die Fragestellung lässt sich also insofern präzisieren, inwieweit die §§ 102 f. StPO die Durchsuchung von Sachen (Datenträgern) nach unkörperlichen Daten erlauben oder bei einer Durchsuchung von Sachen auf das Auffinden anderer Sachen beschränkt sind (z.B. Durchsuchung der Bekleidung des Verdächtigen nach darin befindlichen Wechseldatenträgern).

In der Literatur wird dieses Problem dahingehend diskutiert, inwieweit den Ermittlungsbehörden die Inbetriebnahme der EDV-Anlage des Betroffenen gestattet ist.[1005] Diese Einordnung ist nicht gänzlich überzeugend, da für eine Suche nach Daten lediglich die Datenträger einer EDV-Anlage von Bedeutung sind. Während des Betriebs eines Computers handelt es sich dabei um den Arbeitsspeicher auf der Hauptplatine und in der Peripherie. Im Übrigen um stromunabhängige interne oder wechselbare Datenträger. Die weitere Peripherie – z.B. Monitor, Maus, usw. – ist für eine Suche nach Daten nicht von Bedeutung. Die zunehmende Standardisierung im Hard- und Software-Bereich erfordert es in der Regel nicht mehr, für eine Durchsuchung der Datenträger des Betroffenen dessen EDV-Anlage zu benutzen. Selbst interne Festplatten können mittels weniger Handgriffe gewechselt werden und an andere Anlagen zum Zwecke der Durchsuchung angeschlossen werden. Die Datensicherheit ist bei sachgerechtem Ausbau nicht mehr gefährdet als bei dem Transport der Anlage in die Räumlichkeiten der zuständigen Behörden. Entscheidend ist allein, welche Zugriffsmöglichkeiten den Ermittlungsbehörden auf Datenträger des Betroffenen auf Grund der §§ 102 f. StPO eingeräumt werden[1006], mit anderen Worten, inwieweit die Dateistruktur auf den Datenträgern nach bestimmten unkörperlichen Datensätzen durchsucht werden kann und nicht, ob die EDV-Anlage an sich in Betrieb genommen werden darf.

In der Rechtsprechung des BGH wird die Durchsuchbarkeit von Datenträgern – bzw. der gesamten EDV-Anlage – ohne eine nähere Auseinandersetzung mit der Problematik vorausgesetzt.[1007] Es wird lediglich erörtert, inwieweit Daten unter den Begriff der „Papiere“ des § 110 StPO subsumiert werden können und welche Einschränkungen hinsichtlich der personellen Zuständigkeit für die Sichtung der Daten aus der Norm folgen. In der Literatur wurde die Frage bislang nur von *Bär*[1008] erörtert und bejaht. Andere Autoren setzen die Durchsuchbarkeit von Datenträgern nach Daten ebenfalls voraus oder schließen sich der Ansicht *Bärs* an.[1009]

Ausgehend vom Wortlaut der §§ 102 und 103 StPO kommt es für die Lösung dieser Problematik darauf an, inwieweit EDV-Daten auf einem Datenträger Beweismittel im Sinne der StPO darstellen bzw. ob sich die Beweismittelqualität der Datenträger auf die unkörperlichen geistigen Inhalte erstreckt. Insoweit kann weitgehend auf die Ausführungen in Kapitel 4.3.7.2 verwiesen werden. Dort wurde die Subsumtion von Daten unter den strafprozessualen Urkundenbegriff bereits mit der Begründung abgelehnt, dass Daten, bevor sie ausgedruckt werden, nicht verlesbar sind. Die wohl herrschende Meinung lässt eine Darstellung am Bildschirm, mangels eines stofflichen Substrats, nicht genügen.[1010] Daten könnten jedoch auch Gegenstand eines Augenscheins sein. Dabei handelt es sich um ein sachliches Beweismittel, das auf den sinnlichen Wahrnehmungen eines Richters beruht und nicht als Zeugen-, Sachverständigen- oder Urkundenbeweis bzw. Beschuldigtenvernehmung gesetzlich geregelt ist. Grund-

[1005] Bär, S. 183 ff. mwN; Schnabl JURA 2004, 379 (381)
[1006] Ebenso: Radtke JurPC 1999, Web-Dok. 173/1999, Abs. 6
[1007] BGH StV 1988, 90 (91); BGH 3. Strafsenat, Beschluss vom 5. August 2003, Az: StB 7/03, 2 BJs 11/03 - 5 - StB 7/03, Ziff. 3 lit. b) = wistra 2003, 432 f.; Der Ermittlungsrichter des Bundesgerichtshofes, Beschluss vom 14.12.1998, Az.: 2 BJs 82/98-3
[1008] Bär, S. 183 ff.
[1009] Radtke JurPC 1999, Abs. 6; Rogall ZStW 110, 745 (751); Schroth/Schneider CR 1992, 173
[1010] Nachweise siehe Kapitel 4.3.7.2.

sätzlich beziehen sich sinnliche Wahrnehmungen lediglich auf die Feststellung der gegenständlichen Existenz einer stofflichen Sache oder Sachgesamtheit, auf Örtlichkeiten sowie auf Vorgänge und Verhaltsweisen von Personen.[1011] Computerdaten lassen sich keiner dieser Kategorien zuordnen. Jedoch hat der BGH in zwei Entscheidungen zu der Frage Stellung genommen, inwieweit die gedanklichen Inhalte von Tonträgern in das Verfahren eingeführt werden können.[1012] In BGHSt 14, 339 ff. ging es um das Geständnis eines Angeklagten in Gegenwart eines Polizeibeamten, das auf ein Tonband aufgezeichnet wurde und in der Hauptverhandlung im Zusammenhang mit der Vernehmung des Polizeibeamten abgespielt wurde. BGHSt 27, 135 ff. betraf den Fall, dass ein Telefongespräch zwischen dem Angeklagten und einem Zeugen durch die Ermittlungsbehörden aufgezeichnet wurde und anschließend von einem Polizeibeamten in eine Niederschrift übertragen und diese vom übertragenden Beamten unterzeichnet wurde. Anschließend wurde die Niederschrift ohne Abspielen der Bänder in der Hauptverhandlung verlesen. Die erstgenannte Entscheidung führt nun in missverständlicher Weise aus, dass „*[...] das Tonband als getreue Verkörperung der damaligen Erklärung des Angeklagten [...] selbstständige Beweiskraft als Gegenstand eines Augenscheinsbeweises gewinne*". Zwar lässt sich zunächst die Schlussfolgerung ziehen, dass dem gedanklichen Inhalt des Tonbandes losgelöst vom stofflichen Substrat Beweiswert zugemessen und es in den Rang eines Beweismittels erhoben wird. Darauf gestützt ließe sich – wie von *Bär*[1013] unternommen – eine Parallele zu EDV-Daten ziehen. Diese Schlussfolgerung berücksichtigt allerdings den Ausnahmecharakter der zitierten BGH-Entscheidungen nicht. Die Fundstelle BGH 14, 339 ff. ließ den Inhalt des Tonträgers nur ergänzend zur Aussage der Beweisperson in der Hauptverhandlung zu. Die Entscheidung BGHSt 27, 135 ff. stellte entscheidend darauf ab, dass die Aufzeichnung des Telefongesprächs in Gegenwart eines Polizeibeamten erfolgte und dieser die inhaltliche Übereinstimmung des Tonbandes mit der Niederschrift durch seine Unterschrift auf dem Protokoll garantierte. Entscheidend in beiden Fällen war damit die Unverfälschtheit des Tonbandes.[1014] Wenn nun bereits an die Authentizität eines Tonbandes derart hohe Anforderungen gestellt werden, so verbietet sich die Ausdehnung der Beweismittelqualität auf EDV-Daten erst Recht, da diese in besonders hohem Maß der Verfälschung zugänglich sind. Abgesehen von der bewussten Modifikation von Daten führt bereits deren Visualisierung auf verschiedenen Hard- und Softwareplattformen zu unterschiedlichen Ergebnissen, was die Unverlässlichkeit von Computerdaten noch weiter untermauert. Im Ergebnis muss daher die Beweismittelqualität von EDV-Daten verneint werden. Auf Grund ihrer fehlenden Stofflichkeit stellen sie keine Augenscheinsobjekte dar. Ebenso wenig kann die Beweisqualität der Datenträger auf ihre geistigen Inhalte erstreckt werden.

Bei der Durchsuchung von Datenträgern muss darüber hinaus grundsätzlich zwischen lokalen und Netzwerkdatenträgern unterschieden werden. Erstgenannte meinen alle Speichermedien in unmittelbar räumlicher Beziehung zur durchsuchten EDV-Anlage (typischerweise interne Festplatten), zweitgenannte Netzwerklaufwerke an räumlich entfernten Punkten. Art. 19 Abs. 1 erlaubt diesbezüglich die Durchsuchung von LANs, Abs. 2 die Suche in großflächigen Netzen. *Bär* weist in diesem Zusammenhang zutreffend darauf hin, dass die §§ 102 f. aus rechtsstaatlichen Gründen in persönlicher Hinsicht auf bestimmte Betroffene und räumlich auf bestimmte Objekte (Wohnung und andere Räume, Personen, Sachen im Gewahrsam) beschränkt sind.[1015] Soll die Durchsuchung daher auf geografisch entfernte Server ausgeweitet werden,

[1011] Eisenberg, Rn 2220; KK – *Senge* § 86 Rn 1
[1012] BGHSt 14, 339 ff.; 27, 135 ff.
[1013] Bär, S. 212
[1014] Eisenberg, Rn 2291
[1015] Bär, S. 217 ff.; ebenso: Löwe/Rosenberg – *Schäfer* § 105 Rn 15; Meyer-Goßner § 105 Rn 5 sowie SK/StPO – *Rudolphi* § 105 Rn 14; grundlegend zum Ganzen: BVerfGE 42, 212 (220 f.)

muss die Durchsuchungsanordnung ebenfalls auf diese Örtlichkeiten erstreckt werden.[1016] Darüber hinaus gilt es zu bedenken, dass es sich bei einem Netzwerkserver nur selten um eine dem Verdächtigen „gehörende Sache“ handeln wird. Es ist daher eine Anordnung nach § 103 StPO erforderlich, die nur unter den einschränkenden Voraussetzungen ergehen kann, dass bestimmte bewiesene Tatsachen – nicht nur Vermutungen wie im Fall des § 102 StPO – die Annahme rechtfertigen, dass die „gesuchte […] Spur oder Sache“ sich in den zu durchsuchenden Räumen befindet“. Terminologisch ist die Einordnung der gesuchten Daten unter die Begriffe der „gesuchten […] Spur oder Sache“ nur schwer nachvollziehbar.

4.6.6.1.2 Einschränkungen

Eine Beschränkung der Durchsuchung von Datenträgern ergibt sich in Bezug auf die zur Untersuchung berechtigten Personen aus § 110 StPO. Die Vorschrift wurde 1974 in die StPO aufgenommen und ermöglicht die Aussonderung beweiserheblicher Papiere, die ursprünglich allein dem Ermittlungsrichter vorbehalten war, aus Gründen der Verfahrensbeschleunigung nunmehr auch der Staatsanwaltschaft. Die Norm bezweckt den Schutz der Geheimsphäre, soweit dies bei dem mit einer Durchsuchung verbundenen Eingriff noch möglich ist.[1017] Trotz des scheinbar entgegenstehenden Wortlauts werden von der Rechtsprechung und Literatur auch Computerdaten unter den Begriff der „Papiere“ subsumiert.[1018] Auf den Werkstoff „Papier“ kommt es nicht an, soweit es um die Aufzeichnung und Speicherung von menschlichen Äußerungen geht.[1019] Da es sich um eine Schutzvorschrift zu Gunsten des Betroffenen handelt, ist eine Ausweitung des Anwendungsbereiches aus rechtsstaatlichen Gründen unbedenklich.

Darüber hinaus kommt dem Übermaßverbot im Bereich der Durchsuchung von EDV-Daten zentrale Bedeutung zu. Diese resultiert vor allem daraus, dass durch die Technik der Digitalisierung große Mengen an Informationen auf kleinstem Raum gespeichert werden können. Diese Informationen können eine Vielzahl von Personen und Sachverhalten betreffen und mit Hilfe der Suchfunktionen eines Computers mit wenig Aufwand aufbereitet und gesichtet werden. Es drohen daher Eingriffe in die Grundrechte einer Vielzahl von Personen (etwa bei der Durchsuchung von Kundenkarteien, usw.). Von besonderer Bedeutung ist im Rahmen von Informationseingriffen durch die Ermittlungsbehörden das im Volkszählungsurteil des BVerfG entwickelte Recht auf informationelle Selbstbestimmung[1020]. Nur durch ein maßvolles Handeln der Ermittlungsbehörden kann sichergestellt werden, dass Belange des Datenschutzes in ausreichender Weise berücksichtigt werden. Wegen der größeren Eingriffsintensität, die Durchsuchungen bei nicht Verdächtigen haben können, kommt dem Verhältnismäßigkeitsgrundsatz im Rahmen von § 103 StPO eine gegenüber § 102 StPO größere Bedeutung zu.[1021]

4.6.6.1.3 Ergebnis zu §§ 102 ff. StPO

Die Durchsuchungsbefugnisse der §§ 102 ff. StPO sind mit Art. 19 Abs. 1 und 2 vergleichbar.

[1016] Schnabl JURA 2004, 379 (381)
[1017] Löwe/Rosenberg – *Schäfer* § 110 Rn 1
[1018] Der Ermittlungsrichter des Bundesgerichtshofes, Beschluss vom 14.12.1998, Az.: 2 BJs 82/98-3, JurPC Web-Dok. 146/1999; BGH NJW 1995, 3397; BGH StV 1988, 90 (91); KK – *Nack* § 110 Rn 2; Löwe/Rosenberg – *Schäfer* § 110 Rn 4; Meyer-Goßner § 110 Rn 1
[1019] KK – *Nack* § 110 Rn 2
[1020] Siehe dazu Kapitel 4.2.3.1.2
[1021] Bär, S. 223 ff.

Eine wesentliche Funktion von Art. 19 Abs. 1 und 2 besteht in der Erweiterung der herkömmlichen Rechtsgrundlagen auf unkörperliche Durchsuchungsobjekte. In diesem Bereich geht die Konvention über die §§ 102 ff. StPO hinaus, da nach der hier vertretenen Auffassung EDV-Daten keine Beweismittel im Sinne der StPO darstellen und daher nicht durchsucht werden können. Im Ergebnis wurde mit dieser Begründung auch die Beschlagnahme von Daten durch Anfertigung von Kopien verneint.[1022] Im Bereich der Durchsuchung von Netzwerken geht Art. 19 Abs. 2 deutlich über die Vorgaben der StPO hinaus. Den §§ 102 und 103 StPO ist gemeinsam, dass sie einen sowohl in persönlicher als auch in sachlicher Hinsicht klar umgrenzten Bereich definieren, in dem Durchsuchungen beim Verdächtigen oder bei Dritten zulässig sind. Auf diese Weise wird die Mess- und Kontrollierbarkeit von Eingriffen in die Rechte der Betroffenen gewährleistet. Eben diesen Grundsatz des deutschen Verfahrensrechts übergeht Art. 19 Abs. 2, indem er die Ausdehnung von Durchsuchungen in Netzwerkumgebungen ohne separate Anordnung erlaubt.

4.6.6.2 § 94 StPO – [Sicherstellung von Beweisgegenständen]

Hinsichtlich der Sicherstellung von Beweisgegenständen kann grundsätzlich auf die Ausführungen in Kapitel 4.3.7.1 verwiesen werden. Auf das Sonderproblem der Beschlagnahme von Emails wird im Zusammenhang mit Art. 21 eingegangen werden. Im Vergleich zu Art. 19 Abs. 3 ergibt sich folgendes Ergebnis:

Eine Beschlagnahme von EDV-Daten ist von der StPO zumindest nicht unmittelbar vorgesehen. Die Vorschrift spricht von „Gegenständen“ der Beschlagnahme, was allgemein als Hinweis auf deren Körperlichkeit verstanden wird. Allerdings vertritt die wohl herrschende Meinung die Auffassung, dass eine Anfertigung von Kopien als milderer Eingriff zur Beschlagnahme des Datenträgers in Betracht komme. Dieser Ansicht ist abzulehnen. Vor allem in Bezug auf Netzwerklaufwerke scheint diese „a maiore ad minus“-Argumentation mehr als fragwürdig.[1023] Daher bleibt § 94 StPO nach der hier vertretenen Meinung in Bezug auf die Erstellung von Kopien teilweise hinter Art. 19 Abs. 3 zurück. Völlig fremd sind dem deutschen Beschlagnahmerecht die beispielhaft von Art. 19 Abs. 3 lit. c) und d) erwähnten Möglichkeiten, ein staatliches Herrschaftsverhältnis durch Sicherungsmaßnahmen an den Daten zu begründen. Der Regelfall im deutschen Verfahrensrecht bleibt die Beschlagnahme des körperlichen Datenträgers.

4.6.6.3 §§ 48 ff StPO – [Zeugenpflichten]

Im deutschen Strafprozessrecht besteht die Möglichkeit, Auskünfte von bestimmten Personen zu erlangen, soweit sie als Zeugen, §§ 48 ff. StPO, oder Sachverständige, §§ 72 StPO, am Verfahren beteiligt werden. Für beide persönlichen Beweismittel gelten grundsätzlich die gleichen Vorschriften, § 72 StPO. Wegen zahlreicher Ausnahmen von dieser Regel – vor allem hinsichtlich der Vereidigung, Ablehnung von Sachverständigen, der Ungehorsamsfolgen und der Entschädigung für die Teilnahme am Verfahren[1024] – ist jedoch eine Abgrenzung erforderlich.

Die Unterscheidung ist im Einzelnen umstritten und es wird eine Vielzahl von Abgrenzungs-

[1022] Siehe Kapitel 4.3.7.2.
[1023] Nachweise in Kapitel 4.3.7.2.
[1024] Einzelheiten bei Löwe/Rosenberg – *Dahs* § 85 Rn 1 mwN

kriterien diskutiert.[1025] Zusammenfassend kann an dieser Stelle festgehalten werden, dass sich Sachverständige vor allem durch ihre besondere Sachkunde und den Anlass ihrer Wahrnehmungen – behördliche Bestellung – von Zeugen unterscheiden.[1026] Aus dem Erläuternden Bericht[1027] ergibt sich, dass nach Art. 19 Abs. 4 vor allem Netzwerkadministratoren auskunftspflichtig sein sollen. Dabei handelt es sich um Personen, die Computernetze verwalten, indem sie beispielsweise Benutzer registrieren oder löschen, Rechte zuweisen, oder in sonstiger Weise die Funktionalität eines Netzwerkes gewährleisten. Administratoren verfügen in der Regel über „Superrechte" (sog. *root access*) und umfassende Kenntnisse des Netzwerks. Diese besondere Sachkunde macht sie jedoch noch nicht zu Sachverständigen, es sei denn, sie werden zur Begutachtung einer Anlage von den Behörden eigens beauftragt. Ohne Gutachtenauftrag erworbene Kenntnisse aus der Tätigkeit als Systemverwalter verleihen ihnen dagegen eine potentielle Zeugenstellung im Sinne der §§ 48 ff. StPO. Da der Erläuternde Bericht schwerpunktmäßig auf Administratoren in ihrer Tätigkeit als Systembetreuer abstellt, sollen im Folgenden auch nur die Vorschriften hinsichtlich der Zeugen näher beleuchtet werden.

Die generelle Pflicht zur Zeugenaussage wird, ohne von der StPO näher geregelt zu sein, vom BVerfG[1028] und den anderen Gerichten[1029] aus den allgemeinen Staatsbürgerpflichten des Art. 33 GG hergeleitet. Zeugen im Sinne der StPO sind Personen, die Angaben über eigene Wahrnehmungen in einem nicht gegen sie gerichteten Strafverfahren machen.[1030] Die Zeugenstellung ist, wie § 161a StPO zeigt, nicht auf das Hauptverfahren beschränkt. Gegen Zeugen, die ihren staatsbürgerlichen Pflichten nicht nachkommen, können – vor allem nach §§ 51, 70 StPO – Sanktionen verhängt werden. Die inhaltliche Richtigkeit der Aussagen wird durch die Ermahnung zur Wahrheit, § 57 StPO, die Vereidigung, §§ 59 ff. StPO, sowie durch die Strafnormen der §§ 153 ff. StGB gewährleistet. Im Gegenzug gewährleistet die StPO den Zeugen durch die §§ 52 ff. StPO Schutz.

Art. 19 Abs. 4 formuliert, dass die „notwendigen Auskünfte" „in vernünftigem Maß" zu erteilen sind. Damit ist die Reichweite der Zeugenpflichten angesprochen, die auch im deutschen Recht umstritten ist. Der Disput entzündet sich im Einzelnen an der Frage, ob Zeugen dazu verpflichtet sind, sich auf ihre Aussage vorzubereiten oder gar weitere Beweise zu beschaffen oder Erkundigungen einzuholen. Nach herrschender Ansicht erschöpfen sich die Pflichten des Zeugen jedoch im Erscheinen vor Gericht, der wahrheitsgemäßen Aussage sowie deren Beeidigung.[1031] Die Weitergabe von Passwörtern und sonstigen Zugangsinformationen zu geschützten EDV-Daten ist davon umfasst. [1032] Als Nebenpflichten sieht die StPO die Gegenüberstellung, § 58 Abs. 2 StPO, sowie unter bestimmten weiteren Voraussetzungen die Duldung einzelner Untersuchungshandlungen, § 81c StPO, vor. Nach der Rechtsprechung ist auch die Teilnahme und Mitwirkung bei einer Augenscheinseinnahme mit umfasst.[1033] Weitere Nebenpflichten bestehen nicht und bedürften nach der Lehre vom Gesetzesvorbehalt[1034] einer ausdrücklichen rechtlichen Grundlage. Eine vorbereitende Informationspflicht scheitert in der Praxis auch daran, dass Zeugen in einem Strafverfahren grundsätzlich ohne Angabe des Beweisthemas geladen werden. Im Zivilverfahren gilt hingegen § 377 Abs. 2 Nr. 2 ZPO. Aus

[1025] Löwe/Rosenberg – *Dahs* § 85 Rn 4 ff. mwN
[1026] KK – *Pelchen* § 85 Rn 1; Löwe/Rosenberg – *Dahs* § 85 Rn 11; Meyer-Goßner § 85 Rn 3
[1027] ER Ziff. 200
[1028] BVerfGE 33, 23 (31); 38, 105 (118); 38, 312 (320); 49, 280 (284); 76, 363 (383)
[1029] OLG Köln NJW 1981, 2480 (2481); OLG Stuttgart NJW 1956, 840
[1030] KK – *Pelchen* Vor § 48 Rn 1; Löwe/Rosenberg – *Dahs* Vor § 48 Rn 1; Meyer-Goßner Vor § 48 Rn 1
[1031] KK – *Pelchen* Vor § 48 Rn 3; Löwe/Rosenberg – *Dahs* Vor § 48 Rn 6; Meyer-Goßner Vor § 48 Rn 5
[1032] KK – *Nack* § 94 Rn 4; einschränkend: LG Oldenburg CR 1988, 679 sowie Möhrenschlager wistra 1991, 321 (329)
[1033] BGH GA 1965, 108
[1034] Nachweise siehe Fn 1037

dem Fehlen einer entsprechenden Vorschrift in der StPO kann man schließen, dass die StPO von keiner Vorbereitungspflicht der Zeugen ausgeht. Eine darüber hinausgehende Beweisbeschaffungs- oder Erkundigungspflicht kann erst Recht nicht bestehen. Zur Auffrischung des Gedächtnisses sind jedoch Vorhalte an den Zeugen zulässig.[1035]

4.6.6.4 Ergebnis zu §§ 48 ff. StPO

Art. 19 Abs. 4 normiert an unerwarteter Stelle Auskunftspflichten systemkundiger Personen und ist daher mit den §§ 48 ff. StPO vergleichbar. Aus dem Wortlaut der Konvention geht nicht hervor, ob die betroffenen Personen als Zeugen oder Sachverständige am Verfahren beteiligt werden sollen. Der Verdächtige selbst kann von der Auskunftspflicht wegen des „*nemo tenetur se ispsum accusare*"-Grundsatzes nicht betroffen sein. Solange Personen mit besonderer Sachkunde nicht behördlich zu Sachverständigen bestellt wurden, handelt es sich um sachverständige Zeugen im Sinne von Art. 48 StPO. Diese unterliegen den Zwangs-, aber auch den Schutzmaßnahmen der StPO. Von besonderer Bedeutung ist das Auskunftsverweigerungsrecht des § 55 StPO.

4.6.6.5 Auskunftserteilung durch andere Personen

In Kapitel 4.6.6.3 wurde dargestellt, unter welchen Voraussetzungen die deutschen Ermittlungsbehörden Personen als Zeugen vernehmen können, um beweisrelevante Informationen zu gewinnen. Daneben besteht nach allgemeiner Ansicht[1036] die Möglichkeit, im Rahmen des sog. „allgemeinen Ermittlungsgrundsatzes" gemäß § 161 Abs. 1 Satz 1 2. Alternative StPO formlose Auskunfts- und Vorlageersuchen an beliebige Individuen zu richten. Entscheidend ist in diesem Fall, welche inhaltliche Reichweite einem derartigen Auskunftsbegehren zukommt. Die Grenze muss bei grundrechtsrelevanten Maßnahmen anhand der Lehre vom Gesetzesvorbehalt gezogen werden.[1037] Danach bedarf ein staatlicher Eingriff in einen durch ein Grundrecht geschützten Bereich einer gesetzlichen Grundlage.[1038] § 161 Abs. 1 Satz 1 2. Alternative StPO genügt diesen Anforderungen nach überwiegender Auffassung[1039] nicht bzw. nur in begrenztem Maße.[1040] Seine Bedeutung erschöpft sich darin, den staatsanwaltschaftlichen Aufgabenbereich zu umreißen, nicht jedoch die Befugnis zum Eingriff in Grundrechte zu verleihen.[1041] Hinzu kommt, dass bei Auskunfts- und Vorlageersuchen in Bezug auf EDV-Daten ein Eingriff in das Recht auf informationelle Selbstbestimmung[1042] droht. Im insoweit grundlegenden „Volksurteil"[1043] hat das BVerfG klargestellt, dass eine Beschränkung dieses Rechts „[…] eine verfassungsmäßige gesetzliche Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muss […]"[1044], erfordert. § 161 Abs. 1 Satz 1 2. Alternative erfüllt diese Anforderungen als bloße Aufgabenzuweisungsnorm sicherlich nicht.[1045] Der allgemeine Ermittlungsgrundsatz stellt

[1035] Meyer-Goßner § 69 Rn 7
[1036] Bär, S. 446 (449); LG Frankfurt NJW 1954, 688 (689); Löwe/Rosenberg – *Rieß* § 161 Rn 13; Meyer-Goßner § 161 Rn 2; Müller NJW 1963, 833 (886 f.)
[1037] Zum Vorbehalt des Gesetzes im öffentlichen Recht: Maurer, Allgemeines Verwaltungsrecht, § 6, Rn 3 sowie Erichsen/Ehler – *Ossenbühl* § 9 Rn 9 ff., jeweils mwN
[1038] Siehe Fn 1037
[1039] Kleinknecht/Meyer-Goßner (44. Aufl.) § 161 Rn 7; Löwe/Rosenberg – *Rieß* § 161 Rn 31, § 163 Rn 3 ff.; SK/StPO – *Rudolphi* Vor § 94 Rn 45; SK/StPO – *Wolter* Vor § 151 Rn 92
[1040] KK – *Wache* § 161 Rn 1; Meyer-Goßner (ab 45. Aufl.) § 161 Rn 1 f.
[1041] Nachweise siehe Fn 1039, 1040
[1042] Siehe dazu Kapitel 4.2.3.1.2
[1043] BVerfGE 65, 1 ff.
[1044] BVerfGE 65, 1 (Leitsatz 2)
[1045] Nachweise siehe Fn 1039

gemeine Ermittlungsgrundsatz stellt daher für die Staatsanwaltschaft keine ausreichende gesetzliche Ermächtigung dar, um zwangsweise Auskünfte einholen zu können.[1046]

4.6.7 Bewertung Art. 19

Art. 19 entzieht sich einer einheitlichen Beurteilung, da er in seinen Absätzen drei voneinander zu unterscheidende Befugnisse in sich regelt. Auch innerhalb der ersten Gruppe, Abs. 1 und 2, ergeben sich unterschiedliche Zielrichtungen.

Der wesentliche Regelungsgehalt von Abs. 1 bezieht sich – wie der des Abs. 3 und des Art. 16 – auf die Beschlagnahme von Daten in der Erweiterung des strafprozessualen Beweismittelbegriffs auf unkörperliche Objekte. Dies ist weder in Bezug auf die Durchsuchungs- noch die Beschlagnahmebefugnisse unmittelbar von der deutschen StPO vorgesehen. Hier zu Lande behalf man sich bislang mit einer bedenklich weiten Ausdehnung der Beweisbedeutung körperlicher Datenträger, die als Augenscheinsobjekte durchsucht oder sichergestellt worden waren, auf ihre unkörperlichen Inhalte. Vor allem in Bezug auf Netzwerklaufwerke stößt diese Argumentation an ihre Grenzen. Eine Umsetzung von Art. 19 Abs. 1, Abs. 3 sowie Art. 16 dürfte daher zunächst eine Anpassung des Beweismittelrechts dahingehend erfordern, dass die Beweismittelqualität unkörperlicher Daten unabhängig vom zu Grunde liegenden Speichermedium geklärt wird.

Die Umsetzung von Art. 19 Abs. 2 begegnet grundlegenderen Bedenken. Die wesentliche Bedeutung dieses Absatzes besteht darin, individualisierte und an bestimmte Objekte anknüpfende Durchsuchungsanordnungen im Bereich von Computernetzen ausweiten zu können. Im Gegensatz dazu knüpfen die deutschen Durchsuchungsbefugnisse an den räumlich begrenzten Bereich der Wohn- und Geschäftsräume der Betroffenen an. Dadurch soll die Eingriffsintensität behördlicher Ermittlungsmaßnahmen gesteuert und begrenzt werden. Eben dieser rechtsstaatlich gebotene Schutz der Betroffenen wäre bei einer Umsetzung von Art. 19 Abs. 2 nicht mehr gewährleistet.

Art. 19 Abs. 4 findet eine Entsprechung im deutschen Strafrecht, soweit er sich auf die in der StPO geregelten Zeugenpflichten bezieht. Auch hierzu Lande wurde bereits entschieden, dass Zeugen unter bestimmten Voraussetzungen zur Weitergabe von Passwörtern und sonstigen Zugangsinformationen in Bezug auf geschützte EDV-Daten verpflichtet sind.[1047] Eine darüber hinausgehende Beweisbeschaffungspflicht in Bezug auf die genannte Personengruppe findet sich in der StPO nicht. Der Wortlaut von Art. 19 Abs. 4 ist in diesem Zusammenhang missverständlich. Einerseits sollen „notwendige Auskünfte" „in vernünftigem Maß" erteilt werden, um Maßnahmen nach den Abs. 1 und 2 durchführen zu können. Dies deutet darauf hin, dass systemkundige Personen nicht nur über eigene Wahrnehmungen berichten, sondern darüber hinaus weitere Informationen ermitteln sollen. Andererseits heißt es, dass nur eine Person, die bereits „[…] Kenntnisse hat […]", zur Auskunft verpflichtet werden soll. Damit wären wiederum nur eigene, bereits vorhandene Wahrnehmungen gemeint. Aufgrund der letztgenannten Formulierung lässt Abs. 4 sich einschränkend in dem Sinne auslegen, dass er keine an Zeugen gerichtete Beweisbeschaffungspflicht beinhaltet. Die Erläuterungen zu Art. 19 bringen in diesem Fall keine weitergehende Klärung.

In Bezug auf den Verdächtigen kann Absatz 4 wegen des „*nemo tenetur se ipsum accusare*"-Grundsatzes[1048] keine Anwendung finden. Ein entsprechender Hinweis wäre zu Klarstel-

[1046] Im Ergebnis ebenso: Bär, S. 449 f.
[1047] Nachweise in Kapitel 4.6.6.3
[1048] Siehe bereits Kapitel 4.6.5

lungszwecken wünschenswert gewesen.

Soweit Art. 19 Abs. 4 auf eine „allgemeine Auskunftspflicht“ anderer Personen abzielt, findet sich keine Entsprechung in der StPO. Eine Umsetzung erscheint aus rechtsstaatlicher Sicht problematisch, da im Ergebnis eine Zwangsmaßnahme entstünde, deren Reichweite der Aussagepflicht eines Zeugen entspräche, ohne jedoch die Rechte des Betroffenen, beispielsweise durch Auskunftsverweigerungsrechte, Hinweispflichten seitens der Behörden usw., zu berücksichtigen.

4.7 Artikel 20 – Echtzeit-Erhebung von Verbindungsdaten[1049]

(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um ihren zuständigen Behörden die Befugnis zu erteilen,

a) Verbindungsdaten, die mit bestimmten in ihrem Hoheitsgebiet mittels eines Computersystems übertragenen Kommunikationen in Zusammenhang stehen, durch Anwendung technischer Mittel im Hoheitsgebiet dieser Vertragspartei in Echtzeit zu erheben oder aufzuzeichnen, und

b) einen Dienstanbieter im Rahmen seiner bestehenden technischen Möglichkeiten zu zwingen,

i) solche Verbindungsdaten durch Anwendung technischer Mittel im Hoheitsgebiet dieser Vertragspartei in Echtzeit zu erheben oder aufzuzeichnen oder

ii) bei der Erhebung oder Aufzeichnung solcher Verbindungsdaten in Echtzeit mit den zuständigen Behörden zusammenzuarbeiten und diese zu unterstützen.

(2) Kann eine Vertragspartei die in Absatz 1 Buchstabe a bezeichneten Maßnahmen aufgrund der in ihrer innerstaatlichen Rechtsordnung festgelegten Grundsätze nicht ergreifen, so kann sie stattdessen die erforderlichen gesetzgeberischen und anderen Maßnahmen treffen, um sicherzustellen, dass Verbindungsdaten, die mit bestimmten Kommunikationen in ihrem Hoheitsgebiet in Zusammenhang stehen, durch Anwendung technischer Mittel in diesem Hoheitsgebiet in Echtzeit erhoben oder aufgezeichnet werden.

(3) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um einen Dienstanbieter zu verpflichten, die Tatsache, dass eine nach diesem Artikel vorgesehene Befugnis ausgeübt wird, sowie alle Informationen darüber vertraulich zu behandeln.

(4) Die Befugnisse und Verfahren nach diesem Artikel unterliegen den Artikeln 14 und 15.

4.7.1 Anwendungsbereich

Art. 20 und 21 betreffen die Überwachung von Computerdatenübertragungen. Art. 20 bezieht sich auf Verbindungs-, Art. 21 auf Inhaltsdaten. Da die Verfasser der Konvention den behördlichen Eingriff in die Inhalte als gravierender als den in die äußeren Umstände einer Kommunikation einstufen[1050], ist Art. 21 auf Katalogtaten beschränkt, deren Bestimmung dem nationalen Gesetzgeber vorbehalten bleibt. Im Übrigen unterscheiden sich beide Vorschriften nur hinsichtlich der verwendeten Terminologie, woraus sich in inhaltlicher Hinsicht keine weiteren Abweichungen ergeben sollen[1051], so dass die folgenden Darstellungen gleichermaßen für Art. 20 und 21 gelten.

„Echtzeit-Erhebung“ bedeutet, dass Daten zum Zeitpunkt der Übertragung überwacht und gespeichert werden. Art. 20 und 21 beziehen sich auf zukünftige Datenübertragungen und unterscheiden sich dadurch von den Befugnissen der Art. 16 bis 19, die auf bereits existierende Daten beschränkt sind. Ohne die Befugnisse des Art. 20 wären die zuständigen Behörden auf bereits gespeicherte Verbindungsdaten vergangener Kommunikationen angewiesen, die auf Grund nationaler Datenschutzbestimmungen oftmals nur in begrenztem Umfang zur Verfügung stehen. Die wesentliche Bedeutung von Art. 20 und 21 besteht somit darin, den Ermittlungsbehörden die Überwachung zukünftiger Datenübertragungen zu ermöglichen.

Inhaltlich können die Überwachungsmaßnahmen sowohl an herkömmlichen Telekommunika-

[1049] ER Ziff. 216-227
[1050] ER Ziff. 210
[1051] ER Ziff. 210

tionsnetzen als auch an eigens für die Übertragung von Computerdaten geschaffenen Netzwerken ansetzen. Damit will die Konvention dem Umstand Rechnung tragen, dass die Unterscheidung zwischen Telekommunikation und computervermittelter Kommunikation durch das Zusammenwachsen von Telekommunikations- und Informationstechnologien zusehends an Kontur verliert. Datenübertragungen zwischen Computern finden in heterogenen Netzwerken statt (virtuelle Netze), die als Übertragungswege sowohl öffentliche Telefonleitungen und Funkstrecken nutzen, als auch spezielle Computernetze. Ebenso wenig kommt es nach dem Wortlaut der Konvention darauf an, ob private oder öffentliche Netze zur Übertragung genutzt werden.

Die Überwachung von Datenübertragungen zwischen Computern ist nach Ansicht der Verfasser der Konvention für die Aufklärung von Straftaten wenigstens ebenso bedeutsam wie das Abhören von Telefongesprächen.[1052] Dies resultiert zum einen daraus, dass Computernetzwerke bedeutende Kommunikationswege für Straftäter darstellen (z.B. Emails, Instant Messaging, usw.), die dem herkömmlichen Telefon mittlerweile nicht mehr nachstehen. Zum anderen ist in dem Bereich der Computerkriminalität, in der ein EDV-System nicht Tatwerkzeug, sondern Tatobjekt ist – etwa in den Fällen der Computermanipulation und Computersabotage – die Erhebung von Inhalts- und Verbindungsdaten oftmals die einzige Möglichkeit, Beweise für die Tatbegehung zu gewinnen.[1053]

4.7.2 Verbindungsdaten

Der Begriff der „Verbindungsdaten“ wird in Art. 1 lit. d) definiert. Insoweit kann auf die Ausführungen in Kapitel 2.4 verwiesen werden. „Verbindungsdaten“ nach Art. 20 sind demnach alle Daten, die die äußeren Umstände einer Datenübertragung zwischen Computersystemen betreffen. Im Gegensatz dazu repräsentieren „Inhaltsdaten“ die Inhalte einer Kommunikation und bedürfen daher eines stärkeren Schutzes.[1054] Um diese Unterscheidung terminologisch zu unterstreichen, spricht die Konvention von der „Echtzeit-Erhebung von Verbindungsdaten“ und dem „Echtzeit-Abfangen“ von Inhaltsdaten. Inhaltlich ist in beiden Fällen ein „Erheben und Aufzeichnen“ von Daten gemeint.[1055]

4.7.3 Erheben oder Aufzeichnen

Art. 20 und 21 sollen die zuständigen Behörden in die Lage versetzen, bestimmte Verbindungs- und Inhaltsdaten „zu erheben oder aufzuzeichnen“. Trotz der unterschiedlichen Überschriften „Erhebung von Verbindungsdaten“ und „Abfangen von Inhaltsdaten“ wird durch diese Verben zum Ausdruck gebracht, dass sich die Überwachung von Datenübertragungen in beiden Fällen zumindest in technischer Hinsicht kaum unterscheiden wird. Die Regelung der Einzelheiten – wie beispielsweise die Einrichtung bestimmter Übergabepunkte – bleibt den nationalen Gesetzgebern vorbehalten. Insoweit wird alleine auf die „Anwendung technischer Mittel“ Bezug genommen, ohne dass diese näher definiert würden.

4.7.4 Bestimmte Kommunikationen

Diejenigen Verbindungsdaten, die auf Grund von Art. 20 erhoben werden dürfen, müssen mit „bestimmten Kommunikationen“ auf dem Hoheitsgebiet einer Vertragspartei in Zusammen-

[1052] ER Ziff. 218
[1053] ER Ziff. 218
[1054] Siehe dazu Kapitel 4.8.2.
[1055] ER Ziff. 210

hang stehen.[1056] Die zu überwachenden Datenübertragungen müssen demnach genau bezeichnet werden. Eine generelle und undifferenzierte Erhebung und Aufzeichnung von Verbindungsdaten in großen Mengen wird von Art. 20 nicht autorisiert. Anknüpfungspunkt dafür kann sowohl eine zu überwachende Person als auch ein bestimmter Anschluss sein.[1057] Der Begriff der „Kommunikation" wird in diesem Zusammenhang im Plural verwendet, um Situationen begegnen zu können, in denen die Verbindungsdaten mehrerer Datenübertragungen erhoben werden müssen, um den Zielpunkt oder den bzw. die Verantwortlichen bestimmen zu können.[1058] Der Erläuternde Bericht führt als Beispiel einen Mehrpersonenhaushalt an, in dem verschiedene Personen einen Anschluss benutzen.[1059] In Bezug auf die Individuen handelt es sich um verschiedene Kommunikationen; hinsichtlich des Anschlusses, um eine zu überwachende Stelle.

4.7.5 Einschränkungen im räumlichen Anwendungsbereich

Die Echtzeit-Erhebung von Verbindungsdaten ist auf Kommunikationen beschränkt, die mittels eines Computersystems „in dem Hoheitsgebiet" einer Vertragspartei stattfinden. Dies soll dann der Fall sein, wenn sich eine der teilnehmenden Parteien (Mensch oder Computer) oder die Übertragungswege in dem Staatsgebiet der Vertragspartei befinden.[1060] In der Praxis wird die Vorschrift daher vor allem dort Anwendung finden, wo ein Dienstanbieter physische Infrastruktur oder sonstige Ausrüstung in dem Hoheitsgebiet eines Vertragsstaates unterhält, ohne dass es auf den Schwerpunkt seiner Geschäftstätigkeit oder den Sitz des Unternehmens ankommt. Außerhalb seines Hoheitsgebiets hätte ein Unterzeichnerstaat nicht die erforderliche Hoheitsgewalt, um in die Rechte Privater einzugreifen.

4.7.6 Verhältnis von Abs. 1 zu Abs. 2

Art. 20 Abs. 1 sieht grundsätzlich die Erhebung von Verbindungsdaten sowohl durch die zuständigen staatlichen Behörden unmittelbar vor, lit. a), als auch durch die beteiligten Dienstanbieter, lit. b). Beide Varianten treten kumulativ nebeneinander, um eine möglichst lückenlose Überwachung von Verbindungsdaten zu gewährleisten.[1061] Soweit die Dienstanbieter nach Abs. 1 lit. b) zur Kooperation gezwungen werden, kann dies nur im Rahmen „ihrer bestehenden technischen Möglichkeiten" geschehen. Dies bedeutet, dass sie nicht dazu verpflichtet werden, zusätzliche sachliche oder personelle Ressourcen bereitzustellen oder zu entwickeln, um eine Überwachung vorzunehmen oder dabei behilflich zu sein. Wenn es jedoch der organisatorische und technische *status quo* der Anbieter erlaubt, Daten zu erheben oder aufzuzeichnen oder dabei behilflich zu sein, werden sie im Rahmen dieser bestehenden Möglichkeiten zur Zusammenarbeit verpflichtet.[1062] Darunter wird auch die Neukonfiguration eines Computersystems zur Durchführung der Überwachung verstanden, wenn dies ohne größeren Aufwand ist, sowie der Einsatz von Software im Besitz der Dienstanbieter, die bislang für den ordnungsgemäßen Geschäftsbetrieb keine Verwendung fand.[1063]

Soweit die zuständigen Behörden in manchen Unterzeichnerstaaten nicht in der Lage sind, die

[1056] ER Ziff. 219
[1057] ER Ziff. 219
[1058] ER Ziff. 219
[1059] ER Ziff. 219
[1060] ER Ziff. 222
[1061] ER Ziff. 221
[1062] ER Ziff. 221
[1063] ER Ziff. 221

Echtzeit-Erhebung selbst vorzunehmen, soll Abs. 2 Abhilfe schaffen.[1064] Darin ist vorgesehen, in einem solchen Fall die Verbindungsdaten bestimmter Kommunikationen „durch die Anwendung technischer Mittel zu erheben oder aufzuzeichnen". Der einzige Unterschied zu Abs. 1 lit. b) besteht darin, dass nicht die „Dienstanbieter" zur Überwachung verpflichtet werden. Stattdessen soll sich ihre Mitwirkung beispielsweise in der Bereitstellung der erforderlichen Ausrüstung erschöpfen.[1065] Die Abweichung gegenüber Abs. 1 lit. b) erscheint insofern marginal.

4.7.7 Abs. 3 – Vertraulichkeit

Abs. 3 verpflichtet die betroffenen Dienstanbieter zur Wahrung der Vertraulichkeit. Dies dient in erster Linie dazu, den Erfolg der Überwachung zu gewährleisten, der von der Heimlichkeit der Maßnahme abhängt. Darüber hinaus werden die Dienstanbieter von jeder vertraglichen oder sonstigen rechtlichen Verpflichtung befreit, ihre Kunden über die Erhebung von Daten zu informieren. Dort, wo Normen zur Wahrung der Vertraulichkeit geschaffen werden, unterliegen diese den Bedingungen und Garantien der Art. 14 und 15. Der Erläuternde Bericht spricht in dieser Hinsicht vor allem den zeitlichen Umfang der Geheimhaltung an, ohne jedoch eine Höchstdauer zu definieren.[1066]

4.7.8 Vorbehalt nach Art. 14 Abs. 3

Die Konvention enthält an einer „ungewöhnlichen" Stelle einen fakultativen Vorbehalt bzgl. der Anwendung von Art. 20 in zweifacher Hinsicht. Art. 14 Abs. 3 lit. a) ermöglicht die Überwachung von Verbindungsdaten auf das Vorliegen bestimmter Katalogtaten zu beschränken, wobei dieser Straftatenkatalog nicht enger sein darf als der obligatorische des Art. 21. Darüber hinaus sieht lit. b) eine weitere Ausnahme in Bezug auf abgegrenzte LANs vor, die keine öffentlichen Übertragungswege involvieren. Wegen der Einzelheiten kann auf die Ausführungen in Kapitel 4.1.2 verwiesen werden.

4.7.9 Vergleichbare Befugnisse im deutschen Strafprozessrecht

Das deutsche Strafprozessrecht sah bis 1968 keine Befugnis zur Überwachung des Fernmeldeverkehrs vor. Das Fernmeldegeheimnis konnte bis dato nur auf Grund von § 12 FAG[1067] beschränkt werden. § 12 FAG lautete in der seit dem 1. Juli 1998 geltenden Fassung, die zum 31.12.2001 außer Kraft getreten ist:

> *„In strafgerichtlichen Untersuchungen kann der Richter und bei Gefahr im Verzug auch die Staatsanwaltschaft Auskunft über den Fernmeldeverkehr verlangen, wenn die Mitteilungen an den Beschuldigten gerichtet waren oder wenn Tatsachen vorliegen, aus denen zu schließen ist, dass die Mitteilungen von dem Beschuldigten herrührten oder für ihn bestimmt waren und dass die Auskunft für die Untersuchung Bedeutung hat."*

Aus der Präposition „über" ergab sich, dass Gegenstand der Auskünfte nur die äußeren Umstände des Fernmeldeverkehrs sein konnten (sog. Verbindungsdaten.). Das Vergangenheitstem-

[1064] ER Ziff. 223 f.
[1065] ER Ziff. 224
[1066] ER Ziff. 226
[1067] Ursprünglich § 8c des Telegraphengesetzes aus dem Jahr 1927, RGBl. 1927, Teil 1, S. 331, 332; Nach der Neubekanntmachung des Telegraphengesetzes als „Gesetz über Fernmeldeanlagen" vom 14.01.1928 (RGBl. 1928, Teil 1, S. 8 ff.) wurde § 8c in § 12 FAG umbenannt.

pus verdeutlichte, dass lediglich der vor dem Wirksamwerden der Auskunftsanordnung bereits beendete Fernmeldeverkehr betroffen war. Wegen der bis in die 1990er Jahre vorherrschenden analogen Vermittlungstechnik, die aus technischen Gründen nur eine beschränkte Speicherung von Verbindungsdaten ermöglichte, fristete die Norm anfangs nur ein Schattendasein.[1068] Behördliche Eingriffe in das Fernmeldegeheimnis waren damit zunächst in zweifacher Hinsicht begrenzt.

Dies änderte sich erst durch das „Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses" (Artikel 10-Gesetz) vom 13.08.1968.[1069] Art. 1 autorisierte die Nachrichtendienste und Verfassungsschutzbehörden zur Überwachung des Fernmeldeverkehrs; Art. 2 fügte die Urfassung der §§ 100a und 100b in die StPO ein. Die Erweiterung zum Auskunftsbegehren nach § 12 FAG bestand darin, dass die zuständigen Behörden nun nicht mehr auf Angaben über die äußeren Umstände beschränkt waren, sondern kumulativ auf die Inhalte einer fernmündlichen Kommunikation zugreifen konnten.[1070] Darüber hinaus bezogen sich die Ermächtigungen auf den zukünftigen, nach Wirksamwerden der Überwachungsanordnung, stattfindenden Fernmeldeverkehr, der während der Übertragung abgehört und „auf Tonträger aufgezeichnet" werden durfte. Die damit verbundene erhöhte Eingriffsintensität in das Fernmeldegeheimnis wurde im strafrechtlichen Bereich zum einen mit dem sicherheitspolitischen Bedürfnis einer effektiven Strafverfolgung bei besonders schweren Straftaten gerechtfertigt; zum anderen wurde in kriminalistischer Hinsicht argumentiert, dass moderne Fernmeldeanlagen in verstärkter Weise zur Planung und Begehung von Straftaten Einsatz fänden, ohne dass dieser Entwicklung durch entsprechende Rechtsgrundlagen seitens der zuständigen staatlichen Behörden begegnet wurde.[1071] Trotz heftiger Kontroversen bei der Verabschiedung hielt das Artikel 10-Gesetz einer verfassungsrechtlichen Überprüfung im sog. „Abhörurteil"[1072] stand. Ebenso wenig sah der EGMR einen Widerspruch zur EMRK.[1073] Im Rahmen das 7. Gesetzes zur Änderung des Außenwirtschaftsgesetzes[1074] wurden am 28.02.1992 neben den Nachrichtendiensten und Verfassungsschutz- sowie Strafverfolgungsbehörden auch die Zollkriminalämter zur Überwachung des Fernmeldeverkehrs ermächtigt.

Bis zum 31.12.2001 konnte in das Fernmeldegeheimnis daher wie folgt eingegriffen werden:

Die Strafverfolgungsbehörden durften gestützt auf § 12 FAG Auskünfte über in der Vergangenheit liegende Telekommunikationsvorgänge verlangen. Inhalts- und Verbindungsdaten zukünftiger Kommunikationen konnten nach §§ 100a und 100b StPO überwacht werden. Die Verfassungsschutzbehörden von Bund und Ländern, der Bundesnachrichtendienst sowie der Militärische Abschirmdienst (ehemals Amt für Sicherheit der Bundeswehr) durften gestützt auf § 1 Abs. 1 Artikel 10-Gesetz, die Zollkriminalämter gestützt auf §§ 39 ff. AWG, zukünftige Telekommunikationsvorgänge überwachen. Auskünfte über vergangene Kommunikationen waren ihnen grundsätzlich verwehrt. Begrifflich bezogen sich Auskünfte auf Verbindungsdaten des vergangenen Fernmeldeverkehrs; Überwachungen betrafen Inhalts- und Verbindungsdaten zukünftiger Kommunikationen.

[1068] KK – *Nack* § 100a Rn 17; Klesczewski JZ 1997, 719 (719 f.); Palm/Roy NJW 1996, 1791 (1796)
[1069] BGBl. 1968 I, S. 949 ff.
[1070] Spätestens seit der Neufassung durch das Poststrukturgesetz (BGBl. 1989 I, S. 1026 ff.) hatte die Post die „Überwachung und Aufzeichnung des Fernmeldeverkehrs" schlechthin zu ermöglichen; dazu KK – *Nack* § 100a Rn 2; Stenger CR 1990, 786 (793); Welp NStZ 1994, 209 (213)
[1071] BT-Drs V/1880, 7 ff.
[1072] BVerfGE 30, 1 ff.
[1073] „Klass" Urteil des EGMR, EUGRZ 1979, 278 ff.
[1074] BGBl. 1992 I, S. 372ff.

Durch das Gesetz zur Änderung der Strafprozessordnung vom 20.12.2001[1075] sowie das Terrorismusbekämpfungsgesetz vom 09.01.2002[1076] wurde die begriffliche Unterscheidung zwischen „Auskünften" und „Überwachung" weitgehend aufgegeben sowie die Befugnisse der Nachrichtendienste, zeitlich befristet bis zum 11.01.2007, Art. 22 Abs. 2 Terrorismusbekämpfungsgesetz, erweitert. Auskünfte dürfen nunmehr auch über zukünftige Telekommunikationsdaten – zum Teil auch Teledienstenutzungsdaten – eingeholt werden, und zwar auch durch die Nachrichtendienste.[1077] Der Auskunftsbegriff wurde in zeitlicher Hinsicht vom bereits abgewickelten Fernmeldeverkehr gelöst und bezieht sich im geltenden Recht allein auf Verbindungsdaten. Die Literatur spricht insofern von einer „kleinen Telefonüberwachung".[1078]

In jüngster Zeit hat sich die Zahl der Telefonanschlüsse, die überwacht werden, maßgeblich erhöht. Die amtliche Statistik der „Regulierungsbehörde für Post und Telekommunikation" (RegTP) weist einen Anstieg von 7.776 Anordnungen 1997 auf 21.874 im Jahr 2002 auf.[1079] Dabei handelt es sich ausschließlich um Überwachungen nach §§ 100a und 100b StPO. Die folgenden Ausführungen beschränken sich – wie sich bereits aus der Kapitelüberschrift ergibt – auf die in der StPO normierten Befugnisse, da diese allein für einen Vergleich zu Art. 20 und 21 relevant erscheinen. Diese Einschränkung ergibt sich aus Art. 14 Abs. 2, der die Anwendung der Konvention im Wesentlichen auf den Bereich „strafrechtlicher" Befugnisse und Verfahren vorsieht.

4.7.9.1 §§ 100g f. StPO – [Auskunft über Telekommunikationsverbindungsdaten]

Zur Entstehung, Geltung und zu grundsätzlichen Unterschieden zur Vorgängerregelung des § 12 FAG kann auf die Darstellungen in Kapitel 4.4.6.2 verwiesen werden. Für einen Vergleich mit Art. 20 soll an dieser Stelle lediglich untersucht werden, unter welchen Voraussetzungen die §§ 100g f. StPO die Erteilung von Auskünften über zukünftiger TK Verbindungen erlauben.

4.7.9.1.1 § 100g Abs. 1 Satz 3 StPO – Auskünfte über zukünftige Verbindungsdaten

Innerhalb von § 100g StPO erlaubt Abs. 1 Satz 3 die Einholung von Auskünften über zukünftige Verbindungsdaten. Diejenigen Daten, die vom Auskunftsbegehren erfasst werden, sind in Abs. 3 abschließend aufgezählt. Für die im Zusammenhang mit Datenübertragungen im Internet besonders bedeutsamen IP-Adressen kann auf die Ausführungen in den Kapiteln 4.4.6.2.1 und 2.4.1 verwiesen werden.

Vom natürlichen Wortsinn her ist eine Erteilung von Auskünften über zukünftige TK-Verbindungsdaten kaum nachvollziehbar. Auskünfte setzen grundsätzlich voraus, dass der interessierende Nachrichtenverkehr bereits stattgefunden hat.[1080] Wird er sich erst in der Zu-

[1075] BGBl. 2001 I, S. 3879 ff.
[1076] BGBl. 2002 I, S. 361 ff.
[1077] § 100g Abs. 1 Satz 3 StPO, § 8 Abs. 3a Satz 2 BNDG, § 8 Abs. 8 BVerfSchG, § 10 Abs. 3 MADG
[1078] SK/StPO – *Wolter* § 100g Rn 1, 12
[1079] Nach § 88 Abs. 5 TKG haben die Betreiber von Telekommunikationsanlagen eine Jahresstatistik über die nach §§ 100a und 100b StPO angeordneten Überwachungsmaßnahmen zu erstellen und der Regulierungsbehörde (RegTP) unentgeltlich zur Verfügung zu stellen. Die aktuellen Zahlen wurden vom BMI veröffentlicht, Pressemitteilung des BMI, 35/03; http://www.bundesregierung.de/Anlage486211/PM_35-2003.pdf (01.04.2004)
[1080] Welp NStZ 1994, 209 (214)

kunft ereignen, kommen nur Überwachungsmaßnahmen zur Ermittlung der gewünschten Informationen in Betracht. Diese dürften sich mit Ausnahme der geringeren Anordnungsvoraussetzungen inhaltlich nicht von denen des § 100a StPO unterscheiden. § 100g StPO regelt daher im Unterschied zur Vorgängerregelung des § 12 FAG nicht mehr nur die Weitergabe von Verbindungsdaten, sondern auch ihre Erhebung durch eine Überwachung des Telekommunikationsverkehrs.

Vor dem 01.01.2002 erlaubte § 12 FAG nur die Einholung von Auskünften „[…] über den Fernmeldeverkehr, wenn die Mitteilungen an den Beschuldigten gerichtet *waren* oder wenn Tatsachen vorliegen, aus denen zu schließen ist, dass die Mitteilungen von dem Beschuldigten *herrührten* oder für ihn bestimmt *waren* und dass die Auskunft für die Untersuchung Bedeutung hat." Die Verwendung des Vergangenheitstempus schloss – wenigstens begrifflich – den behördlichen Zugriff auf den zukünftigen Fernmeldeverkehr aus. In der Praxis konnte die Beschränkung auf vergangene Verbindungen allerdings durch das Zusammenspiel mit § 6 Abs. 3 TDSV a.F., der eine Speicherung der Verbindungsdaten von bis zu 80 Tagen erlaubte, umgangen werden, indem die Anordnung der Auskunftserteilung iterativ im Abstand von jeweils 80 Tagen wiederholt wurde. Auf diese Weise konnte der betroffene Anschluss „etappenweise" und vor allem ohne Bindung an die einschränkenden Voraussetzungen des § 100a StPO überwacht werden. Die Literatur sah darin zu Recht einen Wertungswiderspruch[1081], der durch die Neufassung des § 100g StPO weitgehend aufgelöst wurde.

4.7.9.1.2 Zeitlicher Rahmen

Im Unterschied zur Einholung von Auskünften über vergangene Telekommunikationen (§ 100g Abs. 1 Satz 1 StPO) sieht § 100h Abs. 1 Satz 3 Hs. 2 iVm § 100b Abs. 2 Satz 4 StPO eine Befristung[1082] der Überwachung zukünftiger Verbindungsdaten (§ 100g Abs. 1 Satz 3 StPO) auf höchstens drei Monate vor, wobei eine Verlängerung[1083] um jeweils drei Monate zulässig ist, soweit die Anordnungsvoraussetzungen fortbestehen. Diese Befristung wird vor dem Hintergrund verständlich, dass § 100g Abs. 1 Satz 3 StPO eine Vorschrift im Sinne von § 3 Abs. 1 TDSV darstellt, für die die Beschränkungen der §§ 6 ff. TDSV keine Anwendung finden (siehe dazu Kapitel 4.7.9.1.3).[1084]

4.7.9.1.3 Datenschutzbelange

Der Überwachungscharakter des § 100g StPO wird grundsätzlich durch den in § 3 Abs. 1 TDSV niedergelegten Vorbehalt gegenüber anderen Vorschriften verstärkt. Bislang konnte eine Auskunft nur über solche Daten erteilt werden, die vom Anbieter in rechtmäßiger Weise erhoben worden waren. Dies beurteilte sich in erster Linie nach der TDSV, die die Arten der zu erhebenden Verbindungsdaten und die Verwendungszwecke abschließend regelte. Datenschutzbelange der Betroffenen gingen auf Grund der chronologischen Nachrangigkeit des Auskunftsverlangens zur Erhebung der Daten durch die Anbieter dem behördlichen Strafverfolgungsinteresse vor. Da § 100g Abs. 1 Satz 3 StPO nunmehr die Erteilung einer Anordnung vor dem Anfallen der Daten beim Anbieter ermöglicht, stellt die strafprozessuale Norm eine der TDSV vorrangige Regelung dar.[1085] Die privaten Datenschutzbelange treten dadurch, soweit von der Befugnis des § 100g Abs. 1 Satz 3 StPO Gebrauch gemacht wird, hinter die be-

[1081] SK/StPO – *Wolter* § 100g Rn 4; Welp NStZ 1994, 209 (214 f.)
[1082] Eisenberg, Rn 2450g; KK – *Nack* § 100h Rn 6; Meyer-Goßner § 100h Rn 5
[1083] Eisenberg, Rn 2450g; KK – *Nack* § 100h Rn 6; Meyer-Goßner § 100h Rn 5
[1084] Eisenberg, Rn 2450g; Meyer-Goßner § 100g Rn 10; SK/StPO – *Wolter* § 100g Rn 15
[1085] KK – *Nack* § 100g Rn 6; Meyer-Goßner § 100g Rn 10

hördlichen Strafverfolgungsinteressen zurück.

4.7.9.1.4 Überwachung eines abgegrenzten Netzwerks (LAN)

Die §§ 100g f. StPO enthalten keinen ausdrücklichen Vorbehalt bezüglich der Überwachung begrenzter Netzwerke (LANs) wie dies etwa Art. 14 Abs. 3 lit. b) vorsieht. Allerdings kennt § 100g Abs. 1 StPO nur eine Auskunftspflicht von Anbietern, die „geschäftsmäßige Telekommunikationsdienste" erbringen. Nach § 3 Nr. 5 TKG ist das „geschäftsmäßige Erbringen von Telekommunikationsdienstleistungen das nachhaltige Angebot von Telekommunikation einschließlich des Angebots von Übertragungswegen für Dritte mit oder ohne Gewinnerzielungsabsicht". Soweit diese telekommunikationsrechtliche Begriffsbestimmung auf die StPO übertragen werden kann[1086], kommt es danach auf den Begriff der „Nachhaltigkeit" an. In zeitlicher wie qualitativer Hinsicht dürfte damit eine gewisse Dauerhaftigkeit und Professionalität der Bereitstellung von Telekommunikationsressourcen gemeint sein, wie sie in rein privaten Netzwerken nur im Ausnahmefall angetroffen werden dürfte.

Eine ausdrückliche Ausnahme für private Netzwerke ergibt sich aus § 3 Abs. 1 Satz 1 TKÜV. Die Überwachung der Telekommunikation haben danach nur diejenigen Anbieter zu ermöglichen, deren Dienstleistungen der „Öffentlichkeit" angeboten werden.[1087] Darunter fallen weder Haustelefonanlagen noch abgegrenzte LANs.

4.7.9.1.5 Vertraulichkeit der Überwachung

Wie bereits Art. 20 geht auch § 100g Abs. 1 Satz 3 StPO davon aus, dass Überwachungsmaßnahmen grundsätzlich ohne das Wissen der Beteiligten erfolgen. Die Pflicht zur Geheimhaltung ergibt sich für die Dienstanbieter aus § 5 TKÜV. Unter den Voraussetzungen des § 101 StPO sind die Beteiligten in der Regel erst nach der Beendigung der Überwachung von der Staatsanwaltschaft oder dem Richter in Kenntnis zu setzen.

4.7.9.1.6 Ergebnis zu § 100g Abs. 1 Satz 3 StPO

Im deutschen Strafverfahrensrecht wurde mit § 100g Abs. 1 Satz 3 StPO eine Befugnis geschaffen, um Verbindungsdaten in Bezug auf zukünftige Telekommunikationen zu überwachen. Die Vorschrift erlaubt dem Richter und bei Gefahr im Verzug der Staatsanwaltschaft, §§ 100h Abs. 1 Satz 3 iVm § 100b Abs. 1 StPO, die Erteilung von Auskünften gegen diejenigen anzuordnen, die „geschäftsmäßige Telekommunikationsdienste" erbringen. Für den Fall der Weigerung können die in § 70 StPO bestimmten Ordnungs- und Zwangsmittel gegen die Dienstanbieter festgesetzt werden, §§ 100h Abs. 1 Satz 3 iVm 95 Abs. 2 StPO. Daher ist § 100g Abs. 1 Satz 3 StPO mit Art. 20 Abs. 1 lit. b) sowie Abs. 2 vergleichbar, da er zwar die zuständigen Behörden nicht selbst zur Überwachung von Verbindungsdaten ermächtigt, jedoch – im Zusammenspiel mit § 88 TKG – den Dienstanbietern die Verpflichtung zur Zusammenarbeit mit den Strafverfolgungsbehörden auferlegt. Die Befugnis ist nicht auf bestimmte Katalogtaten beschränkt, sondern kommt generell bei „Straftaten von erheblicher Bedeutung" sowie „mittels einer Endeinrichtung nach § 3 Nr. 3 TKG begangenen Straftaten" zur Anwendung. Wegen der spärlichen Angaben, die Art. 20 in Bezug auf die genauen Anordnungsvoraussetzungen macht, lassen sich weitere Gemeinsamkeiten und Unterschiede nur

[1086] Siehe dazu bereits Kapitel 2.3.1.1.
[1087] Eisenberg, Rn 2403, unter Hinweis auf den Begriff der „Öffentlichkeit" in TDG und MDStV.

schwer feststellen.

4.7.9.2 §§ 100a, 100b StPO – [Überwachung der Telekommunikation]

Die §§ 100a f. StPO erlauben die Überwachung und Aufzeichnung der TK schlechthin. Da der Zugriff nicht auf Verbindungsdaten beschränkt wird, sondern auch die Inhalte einer Telekommunikation erfasst werden, wird auf die Vorschrift im Zusammenhang mit Art. 21 eingegangen.

4.7.10 Bewertung Art. 20

Art. 20 ermächtigt zu weit reichenden staatlichen Eingriffen in die Rechte Privater. Betroffen sind sowohl die Anbieter von Telekommunikationsdiensten, die zur Zusammenarbeit bei Überwachungsmaßnahmen mit den Behörden gezwungen werden können, als auch die Nutzer dieser Dienste. Trotzdem lässt es die Konvention in Bezug auf den Schutz dieser Rechtspositionen mit einem bloßen Hinweis auf die Art. 14 und 15 genügen. Allein Art. 14 Abs. 3 wird konkreter, indem er einen Vorbehalt hinsichtlich bestimmter Katalogtaten vorsieht. Wünschenswert wäre vor allem eine detaillierte Regelung der Anordnungsvoraussetzung, etwa hinsichtlich eines Richtervorbehalts, die Berücksichtigung von Zeugnisverweigerungsrechten sowie von Datenschutzbelangen der Betroffenen gewesen. Anderenfalls scheint der angemessene Schutz der Rechte der Betroffenen nicht gewährleistet.

4.8 Artikel 21 – Abfangen von Inhaltsdaten[1088]

(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um ihren zuständigen Behörden in Bezug auf eine Reihe schwerer Straftaten, die nach ihrem innerstaatlichen Recht zu bestimmen sind, die Befugnis zu erteilen,

a) inhaltsbezogene Daten bestimmter Kommunikationen in ihrem Hoheitsgebiet, die mit einem Computersystem übertragen wurden, durch Anwendung technischer Mittel im Hoheitsgebiet dieser Vertragspartei in Echtzeit zu erheben oder aufzuzeichnen, und

b) einen Dienstanbieter im Rahmen seiner bestehenden technischen Möglichkeiten zu zwingen,

i) solche inhaltsbezogenen Daten durch Anwendung technischer Mittel im Hoheitsgebiet dieser Vertragspartei in Echtzeit zu erheben oder aufzuzeichnen oder

ii) bei der Erhebung oder Aufzeichnung solcher inhaltsbezogener Daten in Echtzeit mit den zuständigen Behörden zusammenzuarbeiten und diese zu unterstützen.

(2) Kann eine Vertragspartei die in Absatz 1 Buchstabe a bezeichneten Maßnahmen aufgrund der in ihrer innerstaatlichen Rechtsordnung festgelegten Grundsätze nicht ergreifen, so kann sie stattdessen die erforderlichen gesetzgeberischen und anderen Maßnahmen treffen, um sicherzustellen, dass inhaltsbezogene Daten bestimmter Kommunikationen in ihrem Hoheitsgebiet durch Anwendung technischer Mittel in diesem Hoheitsgebiet in Echtzeit erhoben oder aufgezeichnet werden.

(3) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um einen Dienstanbieter zu verpflichten, die Tatsache, dass eine nach diesem Artikel vorgesehene Befugnis ausgeübt wird, sowie alle Informationen darüber vertraulich zu behandeln.

(4) Die Befugnisse und Verfahren nach diesem Artikel unterliegen den Artikeln 14 und 15.

4.8.1 Anwendungsbereich

Art. 21 ist weitgehend wortgleich mit Art. 20, mit dem Unterschied, dass er sich nicht auf Verbindungs-, sondern auf Inhaltsdaten bezieht. Die besondere Bedeutung dieser Befugnis im Bereich der Computerkriminalität wird vor allem dort deutlich, wo der Straftatbestand im Übertragen rechtswidriger Inhalte – beispielsweise kinderpornografische Materialien[1089], Schadprogramme[1090] usw. – besteht. Den Erläuterungen zufolge kann in diesem Fall bereits die Übertragung bzw. Zugänglichmachung der Daten strafbar sein.[1091] Anders bei der Überwachung der herkömmlichen Sprachtelefonie. Dort erfüllt das gesprochenen Wort in der Regel keinen Straftatbestand, sondern dient als Beweismittel für andere, nicht inhaltsbezogene Delikte.[1092] Dennoch wiegen auch in diesen Fällen Eingriffe in die Inhalte einer Kommunikation schwerer als solche in deren äußere Umstände, so dass das Abfangen von Inhaltsdaten zu Recht zwingend auf einen Katalog „schwerer Straftaten“ beschränkt ist, deren Bestimmung dem nationalen Gesetzgeber obliegt. Im Übrigen kann auf die Ausführungen zu Art. 20 verwiesen werden.

[1088] ER Ziff. 228-231
[1089] Siehe Kapitel 3.9
[1090] Ausführlich zu Schadprogrammen Kapitel 1.7.2
[1091] ER Ziff. 228
[1092] ER Ziff. 228

4.8.2 Inhaltsdaten

Der Begriff der „Inhaltsdaten“ wurde in der Konvention nicht eigens definiert. Der Erläuternde Bericht definiert sie als „Summe aller Informationen, die bei einer Übertragung von Computerdaten übermittelt werden, mit Ausnahme der Verbindungsdaten nach Art. 1 lit. d)“.[1093]

4.8.3 Vorbehalt nach Art. 14 Abs. 3

Neben dem obligatorischen Vorbehalt in Art. 21 in Bezug auf bestimmte Katalogtaten, die nicht näher bestimmt wurden, sieht Art. 14 Abs. 3 lit. b) die fakultative Möglichkeit vor, abgegrenzte Netzwerke, die keine öffentlich zugänglichen Übertragungswege involvieren, aus dem Anwendungsbereich von Art. 21 auszunehmen.

4.8.4 Vergleichbare Befugnisse im deutschen Strafprozessrecht

Hinsichtlich der Entstehung und Systematik der relevanten Überwachungsnormen kann auf die Darstellungen in Kapitel 4.7.9 verwiesen werden. Für einen Vergleich zu Art. 21 sind allein die §§ 100a und 100b StPO relevant.

4.8.4.1 §§ 100a und 100b StPO – [Überwachung der Telekommunikation]

In strafrechtlichen Ermittlungen erlauben die §§ 100a und 100b StPO eine Überwachung der Telekommunikation. Während § 100a StPO die materiellen Eingriffsvoraussetzungen regelt, betrifft § 100b StPO das dabei zu beachtende Verfahren. Beide Vorschriften wurden 1968 durch das Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (G 10 Gesetz[1094]) zusammen mit Befugnissen zu Staatssicherheitszwecken[1095] in die StPO eingefügt. Praktische Bedeutung erlangten sie bislang fast ausschließlich bei der Überwachung herkömmlicher Sprachtelefonie. Bedingt durch Fortschritte in der Telefon- und Computertechnologie, sowie vor allem durch den konsequenten Ausbau von Breitbandnetzwerken, erschöpft sich die Bedeutung klassischer „Fernsprechanlagen“ mittlerweile jedoch nicht mehr in der Übertragung des gesprochenen Wortes über räumliche Entfernungen, sondern moderne „Telekommunikationsanlagen“ übernehmen den globalen und kostengünstigen Transport großer Mengen digitalisierter Daten, die Sprach-, Text-, Bild-, Ton- und andere unkörperliche Mitteilungen enthalten können. Die §§ 100a und 100b StPO wurden diesen geänderten technischen Rahmenbedingungen durch zahllose Änderungen im Wortlaut angepasst und erfuhren dadurch einen grundlegenden Bedeutungswandel. Die folgenden Ausführungen untersuchen daher, inwieweit die §§ 100a und 100b StPO die Überwachung moderner Telekommunikation, losgelöst von der herkömmlichen Sprachtelefonie, ermöglichen.

4.8.4.2 Begriff der Telekommunikation

Seit der Änderung der §§ 100a und 100b StPO durch das „Begleitgesetz zum Telekommunikationsgesetz (BegleitG)“[1096] erlauben die genannten Befugnisse nicht mehr die Überwachung und Aufzeichnung des „Fernmeldeverkehrs“, sondern der „Telekommunikation“. Wie bereits in Kapitel 2.3.1.1 dargestellt, handelt es sich dabei nicht nur um eine terminologische

[1093] ER Ziff. 229; siehe dazu auch Kapitel 2.4.
[1094] BGBl. 1968 I, S. 949 ff.
[1095] Siehe dazu Kapitel 4.7.9.
[1096] BGBl. 1997 I, S. 3108 ff.

Anpassung an den Sprachgebrauch des TKG, sondern auch um eine inhaltliche Erweiterung in Bezug auf die geänderten Inhalte, die über moderne Telekommunikationsnetze übertragen werden.[1097] Aus dem gleichen Grund war bereits im „Gesetz zur Neustrukturierung des Post- und Fernmeldewesens und der Deutschen Bundespost (Poststrukturgesetz)“ vom 08.06.1989[1098] die Formulierung „Überwachung und *Aufnahme* des Fernmeldeverkehrs auf Tonträger“ durch den Wortlaut „Überwachung und *Aufzeichnung* des Fernmeldeverkehrs“ ersetzt worden. Diese Auffassung wird durch die sog. „Direktruf“-Entscheidung des BVerfG[1099] untermauert, die klarstellt, dass vom Begriff „Fernmeldewesen“ auch digitale Nachrichtenübertragungen“ erfasst werden. Mit „Überwachung und Aufzeichnung der Telekommunikation“ in der gegenwärtigen Gesetzesfassung werden damit in Anlehnung an die telekommunikationsrechtliche Begriffsbestimmung des § 3 Nr. 16 TKG jegliche Datenübertragungen erfasst.

Einen Sonderfall im Rahmen der Telekommunikationsüberwachung stellt die Überwachung von „Mailboxen“ dar. Im Rahmen der Konvention wurde dieses Problem bereits im Zusammenhang mit der Beschlagnahme (Art. 19) von Emails in Kapitel 4.6.4 angesprochen. Der Begriff der „Mailbox“ wird in der Literatur uneinheitlich verwendet.[1100] Nach dem natürlichen Wortsinn handelt es sich um einen „elektronischen Briefkasten“ in unterschiedlichsten technischen Gestaltungen. Funktional nimmt er bei Gesprächsnotizen (engl. *voicemail*) die Aufgaben eines Anrufbeantworters wahr[1101], bei schriftlichen Nachrichten (engl. *email*[1102]) die eines Ablagefachs oder Briefkastens. Ausschlaggebend für den hier verwendeten Begriff der „Mailbox“ ist, dass schriftliche oder gesprochene Nachrichten in einer Mailbox abgelegt werden können, um zu einem anderen Zeitpunkt vom Empfänger abgerufen zu werden. Bei technischer Betrachtungsweise handelt es sich um einen oder mehrere Übermittlungsvorgänge zur Mailbox hin, der Speicherung der Nachricht auf einem Datenträger des Dienstanbieters sowie einem weiteren Übermittlungsvorgang beim Abruf der Nachricht durch den Empfänger.[1103] In rechtlicher Hinsicht stellt sich die Frage, ob es sich dabei um einen einheitlichen Sachverhalt oder um drei gesondert voneinander zu beurteilende Phasen handelt.

Dies hat erhebliche praktische Konsequenzen dafür, ob der Zugriff der Ermittlungsbehörden auf die „ruhenden“ Daten im Wege der Beschlagnahme oder nur unter den einschränkenden Voraussetzungen einer Überwachung der Telekommunikation möglich ist.[1104] Sofern auch die gespeicherten Nachrichten unter den Telekommunikationsbegriff subsumiert werden, ist fraglich, inwieweit sie einer Überwachung zugänglich sind, obwohl sie sich nicht im Übermittlungsstadium befinden.[1105] Für die Beschlagnahme von Emails vertritt das LG Hanau[1106] die Ansicht, dass es sich vom Absenden der elektronischen Nachricht bis zum Lesen durch den Empfänger um einen einheitlichen Vorgang handele. Emails werden in einem System der Nachrichtenübermittlung mit Zwischenspeicherung nach § 14 TDSV (§ 16 TDSV n.F.) übertragen und seien daher insgesamt dem Bereich der Telekommunikation zuzuordnen. Auf die

[1097] Eingehend zum Ganzen mit Nachweisen, Kapitel 2.3.1.1
[1098] BGBl. 1989 I, S. 1026 ff. (S. 1050); Bär, S. 301, 305 ff.
[1099] BVerfGE 46, 120 (Leitsatz 2); Bär, S. 305 f.
[1100] Stenger CR 1990, 786 (787); Palm/Roy NJW 1996, 1791 (1792)
[1101] Palm/Roy NJW 1996, 1791 (1792): „[…] Zugang zur Mailbox mittels eines Endgeräts über das Telefon oder Datex-Netz […]“
[1102] Zu Entstehung und technischen Grundlagen der „elektronische Post“: Plate, Internet – Möglichkeiten und Dienste, 2.1
[1103] KK – *Nack* § 100a Rn 7; Palm/Roy NJW 1996, 1791 (1793); Plate, Internet – Möglichkeiten und Dienste, 2.1; Taschenbuch der Informatik – *Plate/Henning*, Kap. 21, S. 689 f.
[1104] KK – *Nack* § 100a Rn 8; Palm/Roy NJW 1996, 1791 (1792 f.)
[1105] KK – *Nack* § 100a Rn 8; Palm/Roy NJW 1996, 1791 (1793)
[1106] LG Hanau vom 23.09.1999 – Az.: 3 Qs 149/99

einzelnen Übertragungsvorgänge im Sinne von § 3 Nr. 16 TKG komme es daher nicht an. Die Einordnung von Emails unter § 14 TDSV a.F. wird durch die amtliche Begründung zu § 16 TDSV n.F. gestützt[1107], der inhaltlich der Vorgängerregelung entspricht. Als Konsequenz verneint das LG Hanau die Beschlagnahmefähigkeit von Emails zu Recht, da § 94 StPO keine Eingriffe in das Fernmeldegeheimnis erlaube. Inwieweit §§ 100a f. StPO den Zugriff auf „ruhende" Emails gestatten, war in der zitierten Entscheidung nicht von Bedeutung.

Einen anderen Weg ging der Ermittlungsrichter des BGH bei der Überwachung einer Voicemailbox.[1108] Zunächst wurde die Beschlagnahmefähigkeit der auf der Mailbox gespeicherten Gesprächsdaten mangels Körperlichkeit verneint. Im Anschluss daran führte das Gericht aus, dass es als „sachgerecht" erscheine, unter die Überwachung des Fernmeldeverkehrs auch den Zugriff auf gespeicherte Daten zu subsumieren. Dies vor allem in Hinblick auf die betroffenen Grundrechte aus Art. 10 und 13 GG, in die unter Verhältnismäßigkeitsgesichtspunkten nur unter den Einschränkungen der §§ 100a f. StPO eingegriffen werden dürfe. Damit verdeutlichte der BGH, dass er gespeicherte Gesprächsdaten grundsätzlich dem Fernmeldeverkehr zuordnet und der Zugriff im Wege der Überwachung erfolgt, obwohl sich die Daten nicht im Übertragungsstadium befinden. In der Literatur stieß diese Entscheidung auf erhebliche Kritik. *Palm/Roy* führen aus, dass sich die Einzelrichterentscheidung im Wesentlichen von Praktikabilitätserwägungen leiten ließ.[1109] *Bizer* beanstandete, dass der eindeutige Wortlaut des § 3 Nr. 16 TKG eine Einordnung gespeicherter Daten unter den Telekommunikationsbegriff nicht erlaube[1110] und *Bär* sah die Wortlautgrenze des Überwachungsbegriffs überschritten.[1111] Ganz entscheidend gegen diese Ansicht des BGH spricht auch der Wortlaut des § 39 Abs. 1 Satz 1 AWG, der den Zollkriminalämtern eine Überwachung und Aufzeichnung „[…] der Telekommunikation *einschließlich der dazu nach Wirksamwerden der Anordnung (§ 40 AWG) innerhalb des Telekommunikationsnetzes in Datenspeichern abgelegten Inhalte* […]" erlaubt. *Ricke*[1112] führt zu Recht aus, dass es sich bei den *„abgelegten Inhalten"* um Nachrichten in Mailboxen handele, woraus im Umkehrschluss gefolgert werden könne, dass die §§ 100a f. StPO, die gerade keinen vergleichbaren Passus enthielten, sich nicht auf ruhende Daten bezögen.

In der Literatur wird daher ein anderer Ansatz vertreten. Da von Telekommunikation – jedenfalls begrifflich – nur während der Übertragung, jedoch nicht während des Ruhens von Nachrichten in einer Mailbox, die Rede sein könne, komme eine Überwachung auch nur während der Übermittlung in und des Abrufs aus der Mailbox in Betracht.[1113] Während die Daten auf dem Datenträger des Anbieters ruhen, könne der Zugriff nur im Wege der Beschlagnahme erfolgen.[1114] *De lege lata* sei dies die einzige Möglichkeit des Zugriffs, so dass Wertungswidersprüche zwischen den beiden Maßnahmen bis auf Weiteres hinzunehmen seien.[1115]

Bei einem Vergleich der drei Ansichten ist der Ansatz des LG Hanau und des Ermittlungsrichters des BGH begrüßenswert, Nachrichten, die in Mailboxen abgelegt wurden, dem Telekommunikations- bzw. Fernmeldebereich zuzuordnen. Auf diese Weise wird dem Fernmel-

[1107] BMWA, Begründung zur Telekommunikations-Datenschutzverordnung, S. 6, http://www.bmwi.de/Redaktion/Inhalte/Downloads/Homepage_2Fdownload_2Ftelekommunikation__post_2Ftdsv-Begruendung.pdf,property=pdf.pdf (01.04.2004)
[1108] Ermittlungsrichter des BGH NJW 1997, 1934 ff. = CR 1996, 488 = DuD 1996, 625 = NStZ 1997, 247 ff
[1109] Palm/Roy NJW 1997, 1904 (1905)
[1110] Anmerkung Bizer zu BGH 31.07.1995, Az.: 1 BGs 625/95, DuD 1996, 627 (627)
[1111] Anmerkung Bär zu BGH 31.07.1996 1, Az.: BGs 625/95, CR 1996, 490 (491); ebenso: Bizer, siehe Fn 1110
[1112] AWR-Kommentar – *Ricke* § 39 AWG Rn 15
[1113] KK – *Nack* § 100a Rn 5, 6; Schnabl JURA 2004, 379 (384)
[1114] KK – *Nack* § 100a Rn 7 ff.; Palm/Roy NJW 1996, 1791 (1794); Palm/Roy NJW 1997, 1904 (1905)
[1115] Palm/Roy NJW 1996, 1791 (1796)

degeheimnis der größtmögliche Schutzbereich zu Gunsten der Betroffenen eingeräumt. Diese Sichtweise wird sich jedoch in Hinblick auf den Wortlaut des § 3 Nr. 16 TKG und der begrifflichen Anpassung der §§ 100a ff. StPO in Zukunft nur schwer aufrechterhalten lassen. Telekommunikation betrifft schon dem natürlichen Wortsinn nach nur Nachrichten im Übermittlungsstadium, nicht jedoch gespeicherte Daten. Soweit der BGH trotz dieser weiten Auslegung des Fernmelde- bzw. Telekommunikationsbegriffs den Zugriff im Wege der Überwachung erlaubt, ist diese Ansicht abzulehnen, da sie die Wortlautgrenzen der Eingriffsgrundlage überspannt. Die Entscheidung bringt jedoch deutlich das Dilemma der geltenden Rechtslage zum Vorschein. Wenn abrufbereit gespeicherte Nachrichten aus dem Schutzbereich des Art. 10 Abs. 1 GG genommen werden – das Postgeheimnis schützt nach ganz herrschender Meinung nur körperliche Nachrichtenübermittlungen[1116] – hängt die Intensität des Schutzes von Nachrichten, die mittels moderner Technologien übertragen wurden, von Zufällen ab (Zeitpunkt des Nachrichtenabrufs). Gerade im Bereich von Emails ergibt sich ein nur schwer überschaubares Gefährdungspotential für die Privatsphäre der Betroffenen. Anders als Voicemail-Nachrichten wird elektronische Post im Internet über eine Vielzahl von Zwischenstationen geleitet und abgespeichert.[1117] Auf jedem der beteiligten Server könnte sie, sofern man der Literaturansicht folgt, *de lege lata* zusammen mit dem Datenträger beschlagnahmt werden. Vorzugswürdig erscheint daher die Ansicht des LG Hanau, die zeitlich verzögerte Übermittlung von Nachrichten auf elektronischem Wege insgesamt dem Telekommunikationsbereich zuzuordnen und eine Beschlagnahme abzulehnen.

4.8.4.3 Überwachung und Aufzeichnung

§§ 100a und 100b StPO erlauben die „Überwachung und Aufzeichnung" der Telekommunikation, ohne beide Begriffe näher zu definieren. Im Bereich der Sprachtelefonie verstand man darunter das Mithören der Gespräche, deren Aufnahme auf Tonträger sowie die Anfertigung von Abschriften und Fotokopien; in Bezug auf den Fernschreibverkehr handelte es sich um das Mitlesen der übermittelten Inhalte.[1118] Wie bereits dargestellt, werden in modernen Telekommunikationsnetzen neben dem gesprochenen und geschriebenen Wort auch Bilder und sonstige Daten übertragen, die aus offensichtlichen Gründen weder abgehört noch mitgelesen werden können. Die auf der Grundlage von § 88 Abs. 2 TKG erlassene Rechtsverordnung (TKÜV) sieht daher vor, dass vollständige Kopien der übertragenen Daten von den Dienstanbietern zu erstellen sind, § 9 TKÜV. Die dazu technisch erforderlichen Einrichtungen sind von den Betreibern von Telekommunikationsanlagen auf eigene Kosten zu gestalten und vorzuhalten, § 88 Abs. 1 TKG.

4.8.4.4 Verdacht der Begehung einer Katalogstraftat

Eine Telekommunikationsüberwachung darf angeordnet werden, wenn „bestimmte Tatsachen" den Verdacht begründen, dass jemand als „Täter oder Teilnehmer" eine der in § 100a Satz 1 Nr. 1-5 StPO bezeichneten Katalogtaten „begangen oder in Fällen, in denen der Versuch strafbar ist, zu begehen versucht oder durch eine Straftat vorbereitet hat." Das Gesetz verlangt weder dringenden (z.B. §§ 81 Abs. 2, 112 Abs. 1 StPO) noch hinreichenden Verdacht (z.B. § 203 StPO), sondern einen durch „bestimmte Tatsachen" begründeten Tatverdacht. Wie bei den §§ 100c Abs. 1, 111, 100g Abs. 1, 138 Abs. 2 sowie 163d StPO genügen

[1116] Jarass/Pieroth – *Jarass* Art. 10 Rn 4 mwN

[1117] Begrifflich ungenau insofern KK – *Nack* § 100a Rn 7 und LG Hanau, Urteil vom 23.09.1999 – Az.: 3 Qs 149/99, die von einer „[…] Speicherung der Homepage im Internet auf dem Speichermedium des Mailboxbetreibers […]" sprechen.

[1118] Meyer-Goßner § 100a Rn 3; SK/StPO – *Rudolphi* § 100a Rn 7

„bloßes Gerede, nicht überprüfte Gerüchte und Vermutungen alleine nicht."[1119] Erforderlich ist vielmehr, dass auf Grund kriminalistischer Erfahrung und der Auswertung von Indizien und Beweismitteln mit einiger Wahrscheinlichkeit auf eine Katalogtat geschlossen werden kann. Der Kreis der Katalogtaten ist durch § 100a Satz 1 StPO abschließend bestimmt.[1120] Darin ist die Entscheidung des Gesetzgebers zu erblicken, in welchen Fällen der Eingriff mit dem Verhältnismäßigkeitsprinzip als vereinbar erscheint.

4.8.4.5 Adressaten der Überwachungsanordnung

Adressaten der Überwachungsanordnung sind wie bei einer Überwachung nach § 100g StPO zunächst diejenigen, die „[…] geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken […]", § 100b Abs. 3 Satz 1 StPO. Insoweit kann auf die Ausführungen in Kapitel 4.4.6.2.5 verwiesen werden.

Davon zu unterscheiden ist der von der Maßnahme „Betroffene". Dabei handelt es sich in erster Linie um den Beschuldigten, unter bestimmten Voraussetzungen jedoch auch um weitere Personen. § 100a Satz 2 StPO schränkt dies auf die beiden Fälle ein, dass entweder „[…] auf Grund bestimmter Tatsachen anzunehmen ist, dass diese Personen Nachrichten von oder für den Beschuldigten entgegennehmen […]" (sog. Nachrichtenmittler), oder dass „[…] der Beschuldigte ihren Anschluss benutzt […]". In der zweiten Alternative kommt es nach dem Gesetzeswortlaut nicht auf die Kenntnis des Betroffenen hiervon an. Nach verbreiteter Ansicht in der Literatur kann daher beispielsweise der Anschluss eines Haushaltsvorstandes, von Freunden, Nachbarn, Bekannten und Gastwirten überwacht werden, sowie öffentliche Telefonzellen.[1121] Der weite Anwendungsbereich der Norm ist in der Literatur zu Recht auf Kritik gestoßen.[1122]

In Computernetzen ist die Reichweite von § 100a Satz 2 StPO nur schwer überschaubar. Daten können – vor allem im Internet – über beliebig viele Zwischenstationen geleitet werden, die ihrerseits über „Anschlüsse" an das Datennetz verfügen. *Bär*[1123] versucht den Anwendungsbereich der Norm daher durch eine restriktive Auslegung des Benutzungsbegriffs zu begrenzen. Seiner Ansicht nach kann von einer Benutzung nur dann gesprochen werden, wenn „eine Sache zu einem bestimmten Zweck verwendet wird." Dieser bestimmte Zweck liege nur dann vor, wenn die Zugangsberechtigungen eines Rechners, der an der Datenübertragung im Netzwerk beteiligt ist, zur Herstellung einer weiteren Verbindung benutzt würden. Diese Auslegung führt zwar zu einer Begrenzung des Anwendungsbereiches der Norm. Jedoch enthält der Gesetzeswortlaut keinen Anhaltspunkt dafür, dass die von besonderen Berechtigungen unabhängige Weiterleitung von Server zu Server keine „Benutzung" darstellen solle. Die paketvermittelte Datenübertragung auf der Grundlage der TCP/IP-Protokolle führt zwangsläufig zu einer Benutzung beliebig vieler zwischengeschalteter Anschlüsse, da sie gerade nicht an eine „stehende" Leitung gebunden ist. § 100a Satz 2 StPO erlaubt daher grundsätzlich die Überwachung aller beteiligten Server. Wegen der zufälligen Leitungswege im Internet dürfte in der Praxis vor allem die Überwachung der zentralen Netzknotenpunkte in Betracht kommen.

[1119] KK – *Nack* § 100a Rn 24; Löwe/Rosenberg – *Schäfer* § 100a Rn 12; Meyer-Goßner § 100a Rn 6
[1120] KK – *Nack* § 100a Rn 1; Meyer-Goßner § 100a Rn 4; SK/StPO – *Rudolphi* § 100a Rn 10
[1121] Löwe/Rosenberg – *Schäfer* § 100a Rn 21; SK/StPO – *Rudolphi* § 100a Rn 15
[1122] Welp, Die strafprozessuale Überwachung des Post- und Fernmeldeverkehrs, S. 76 f.
[1123] Bär, S. 332 f.

4.8.4.6 Subsidiaritätsprinzip

Der Gesetzgeber trägt der hohen Eingriffsintensität der Telekommunikationsüberwachung dadurch Rechnung, dass er neben der Beschränkung auf bestimmte Katalogtaten und dem allgemeinen Verhältnismäßigkeitsprinzip verlangt, dass „[…] die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsorts des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wäre." Durch diese Formulierung kommt das Subsidiaritäts- bzw. *ultima ratio*-Prinzip zum Ausdruck.[1124] Aussichtslosigkeit liegt nach dem natürlichen Wortsinn nur dann vor, wenn keine anderen Aufklärungsmittel vorhanden sind. Eine wesentlichen Erschwerung wird dann bejaht, wenn das Ausweichen auf andere Ermittlungsmaßnahmen mit einem erheblich größeren Zeitaufwand verbunden und zu einer erheblichen Verfahrensverzögerung führen würde.[1125] Eine vergleichbare Einschränkung ist im Anwendungsbereich des § 100g StPO nicht vorgesehen, woraus zu schließen ist, dass auch der deutsche Gesetzgeber Eingriffe in die Inhalte einer Kommunikation als schwerwiegender beurteilt als solche in die äußeren Umstände.

4.8.4.7 Überwachung eines abgegrenzten Netzwerks (LAN)

Ebenso wenig wie die §§ 100g f. StPO sehen die §§ 100a f. StPO einen Anwendungsvorbehalt hinsichtlich abgegrenzter Netzwerke vor, die keine öffentlich zugänglichen Übertragungsstrecken involvieren. Jedoch kommt es wiederum auf die Erbringung „geschäftsmäßiger Telekommunikationsdienstleistungen" an, so dass auf die Darstellungen in Kapitel 4.7.9.1.4 verwiesen werden kann.[1126]

4.8.4.8 Ergebnis zu § 100a StPO

Der deutsche Gesetzgeber überlässt die unmittelbare technische Ausführung der Überwachung der Inhalte einer Kommunikation ebenso wie die der äußeren Umstände (Verbindungsdaten) den geschäftsmäßigen Anbietern von Telekommunikationsdiensten. Die §§ 100a und 100b StPO sind daher – im Zusammenhang mit § 88 TKG und der TKÜV – strukturell mit Art. 21 Abs. 1 lit. b) und Abs. 2 vergleichbar. Wegen der Parallelität von Art. 21 und 20 sowie §§ 100g f. und 100a f. StPO kann grundsätzlich auf die Ausführungen in Kapitel 4.7.9.1.6 verwiesen werden. In Bezug auf die inhaltliche Reichweite stehen die deutschen Überwachungsbefugnisse der Konvention in nichts nach. Die Darstellungen zum „Telekommunikationsbegriff" haben gezeigt, dass die StPO sich vom historischen Verständnis des Fernmeldeverkehrs gelöst hat und in Anlehnung an die modernen Definitionen des TKG nunmehr die Übertragung jeglicher Arten von Nachrichten erfasst. Problematisch bleibt allein der Zugriff auf Emails. Die höchstrichterliche Rechtsprechung kann in Bezug auf die Ausdehnung der Überwachungsnormen auf ruhende Nachrichten nicht überzeugen. Hinsichtlich der von der Überwachung Betroffenen gehen die §§ 100a f. StPO durch die Möglichkeit der Erstreckung der Maßnahmen auf andere Personen als den Beschuldigten nach § 100a Satz 2 StPO über die Vorgaben des Art. 21 hinaus. Diesbezüglich wurden in der Literatur zu Recht Bedenken erhoben, insbesondere in Bezug auf die zweite Alternative, die in Datennetzen ausgehend vom Wortlaut kaum begrenzbar erscheint.[1127] Eine wesentliche Einschränkung gegenüber den Vorgaben der Konvention enthält der in der deutschen Befugnisnorm verankerte Subsidiaritätsgrundsatz. Dadurch wird klargestellt, dass die Eingriffsintensität einer Überwachung der

[1124] KK – *Nack* § 100a Rn 23; Löwe/Rosenberg – *Schäfer* § 100a Rn 13; Meyer-Goßner § 100a Rn 7
[1125] KK – *Nack* § 100a Rn 23; Löwe/Rosenberg – *Schäfer* § 100a Rn 13; Meyer-Goßner § 100a Rn 7 f.
[1126] Ebenso: KK – *Nack* § 100a Rn 18 mwN
[1127] Nachweise siehe Kapitel 4.8.4.5

Inhalte einer Telekommunikation als derart gravierend beurteilt wird, dass sie nur als *ultima ratio* in Betracht kommt. Im Übrigen enthält Art. 21 ebenso wie Art. 20 zu wenig Angaben, um einen weitergehenden Vergleich vornehmen zu können.

4.8.5 Bewertung Art. 21

Art. 21 unterscheidet sich strukturell kaum von Art. 20. Die dort festgestellten Defizite lassen sich daher gleichermaßen im Zusammenhang mit Art. 21 kritisieren. Wegen der höheren Eingriffsintensität wiegen sie hier sogar noch schwerer. Da das deutsche Verfahrensrecht jedoch *de lege lata* der Konvention in nichts nachsteht, sondern vor allem in Bezug auf den Schutz der Rechte der Betroffenen über Art. 21 hinausgeht, ist keine Transformation in nationales Recht erforderlich, so dass sich auch die Defizite dieser Vorschrift zumindest im nationalen Recht nicht negativ auswirken werden.

4.9 Artikel 22 – Gerichtsbarkeit[1128]

(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um die Gerichtsbarkeit für eine Straftat, die in Übereinstimmung mit den Artikeln 2 bis 11 dieses Übereinkommens festgelegt worden ist, zu begründen, wenn die Straftat wie folgt begangen wird:

a) in ihrem Hoheitsgebiet,
b) an Bord eines Schiffs, das ihre Flagge führt,
c) an Bord eines Flugzeugs, das nach den Rechtsvorschriften dieser Vertragspartei eingetragen ist, oder
d) von einem ihrer Staatsangehörigen, wenn die Tat nach dem am Tatort geltenden Recht strafbar ist oder die Straftat außerhalb der territorialen Gerichtsbarkeit irgendeines Staates begangen wird.

(2) Jeder Staat kann sich das Recht vorbehalten, die in Absatz 1 Buchstaben b bis d oder in Teilen davon enthaltenen Vorschriften in Bezug auf die Gerichtsbarkeit nicht oder nur in bestimmten Fällen oder unter bestimmten Bedingungen anzuwenden.

(3) Jede Vertragspartei trifft die erforderlichen Maßnahmen, um ihre Gerichtsbarkeit für die in Artikel 24 Absatz 1 bezeichneten Straftaten in den Fällen zu begründen, in denen sich ein mutmaßlicher Täter in ihrem Hoheitsgebiet aufhält und sie ihn allein wegen seiner Staatsangehörigkeit nicht an eine andere Vertragspartei ausliefert, nachdem ein Auslieferungsersuchen gestellt worden ist.

(4) Dieses Übereinkommen schließt die Ausübung einer Strafgerichtsbarkeit nach innerstaatlichem Recht nicht aus.

(5) Wird die Gerichtsbarkeit für eine angebliche Straftat, die in Übereinstimmung mit diesem Übereinkommen festgelegt worden ist, von mehr als einer Vertragspartei in Anspruch genommen, so konsultieren die beteiligten Vertragsparteien einander gegebenenfalls, um die für die Strafverfolgung am ehesten geeignete Gerichtsbarkeit zu bestimmen.

4.9.1 Anwendungsbereich

Art. 22 normiert unter der Überschrift „Gerichtsbarkeit" unter welchen Voraussetzungen ein Vertragsstaat die Anwendbarkeit seines nationalen Strafrechts begründen muss. Darüber hinaus wird keine Aussage getroffen, wann ausländisches Strafrecht zur Anwendung kommt. Es handelt sich daher ebenso wie bei §§ 3-7 StGB um „einseitige Kollisionsnormen" bzw. um „Strafanwendungsrecht".[1129] Art. 22 stellt kein strafrechtliches Pendant zum IPR dar, da er keine Aussage zum Verhältnis zwischen ausländischem und inländischem Strafrecht trifft. Vielmehr wird allein ein Mindestanwendungsbereich nationalen Rechts festgelegt, um eine effektive Strafverfolgung zu gewährleisten.

4.9.2 Abs. 1 lit. a) – Territorialitätsprinzip

Abs. 1 lit. a) basiert auf dem Territorialitätsprinzip. Jede Vertragspartei ist verpflichtet, Straftaten zu sanktionieren, die in ihrem Hoheitsgebiet begangen werden. Inländisches Recht findet auf alle im Inland begangene Taten ohne Rücksicht auf die Staatsanghörigkeit des Täters Anwendung. Lit. a) erlaubt einer Vertragspartei ihre Zuständigkeit dann zu bejahen, wenn sowohl der Täter als auch das angegriffene Computersystem oder nur das Computersystem

[1128] ER Ziff. 232-239
[1129] Für §§ 3-7 StGB: Lackner/Kühl Vor §§ 3- 7 Rn 1; MK – *Ambos* Vor §§ 3-7 Rn 1; Sch/Sch – *Eser* Vorbem §§ 3-7 Rn 1; auch „transnationales Strafrecht": MK – *Ambos* Vor §§ 3-7 Rn 1; Sch/Sch – *Eser* Vorbem §§ 3-7 Rn 2

sich in ihrem Hoheitsgebiet befinden.[1130] Darüber hinaus wurde der Tatort, d.h. der Ort an dem die Tat im rechtlichen Sinne „begangen“ wurde, nicht näher definiert.

Die im Rahmen der Entwurfsarbeiten diskutierte Schaffung eines Gerichtsstandes für Straftaten im Zusammenhang mit Satelliten setzte sich nicht durch.[1131]

4.9.3 Abs. 1 lit. b) und c) – Flaggenprinzip

Abs. 1 lit. b) und c) erweitern den in lit. a) niedergelegten Gebietsgrundsatz. Diese Buchstaben verlangen von jeder Vertragspartei, ihr nationales Recht auf Straftaten anzuwenden, die auf Schiffen unter ihrer Flagge oder auf Flugzeugen, die nach ihren Rechtsvorschriften registriert sind, begangen wurden. Beide Transportmittel werden als erweitertes Hoheitsgebiet eines Staates betrachtet. Der praktische Anwendungsbereich dieser Normen besteht darin, Straftaten ahnden zu können, die auf Fahrzeugen unter der Flagge eines Vertragsstaates begangen werden, die sich nicht in dessen Hoheitsgebiet befinden, so dass bereits lit. a) eingreifen könnte.

4.9.4 Abs. 1 lit. d) – Personalprinzip sowie Grundsatz der stellvertretenden Strafrechtspflege

Abs. 1 lit. d) weist zunächst Elemente des aktiven Personal- (bzw. Personalitäts- oder Staatsangehörigkeits-) prinzips auf, indem er auf die Staatsangehörigkeit des Täters abstellt. Dieser Grundsatz ist am Weitesten in Ländern verbreitet, deren Rechtsordnungen an die römische Rechtstradition anknüpfen (engl. *civil law*). Er beruht auf der Bejahung einer besonderen Treuepflicht des Täters gegenüber seiner Heimat und ihren Gesetzen.[1132]

Darüber hinaus nimmt lit. d) jedoch auch Charakteristika des Grundsatzes der stellvertretenden Rechtspflege auf, indem er eine Strafbarkeit am Ort der Tat voraussetzt. Darin kommt der Susidiaritätsgedanke zum Ausdruck, der aus Gründen internationaler Solidarität bei der Verbrechensbekämpfung die Anwendung der inländischen Rechtsordnung dort zulässt, wo die territorial zuständige Strafgewalt aus tatsächlichen oder rechtlichen Gründen an der Ausübung ihrer Strafgewalt gehindert ist.[1133] Dieses Prinzip wird auch in Abs. 3 wieder aufgegriffen.

4.9.5 Abs. 2 – Vorbehalt; Abs. 3 – „*aut dedere aut judicare*“

Abs. 2 erlaubt den Vertragsparteien einen Vorbehalt bzgl. der Buchstaben b) bis d). Dieser darf sich jedoch nicht auf lit. a) erstrecken.

Abs. 3 sieht vor, dass mutmaßliche Täter, um deren Auslieferung auf der Grundlage von Art. 24 Abs. 1 ersucht wurde, die jedoch allein auf Grund ihrer Staatsangehörigkeit nicht ausgeliefert werden, von der ersuchten Partei verfolgt werden müssen. Insofern gilt das Prinzip „*aut dedere aut judicare/punire* (Grotius)“. Abs. 3 weist Ähnlichkeiten zu Abs. 1 lit. d) auf.

[1130] ER Ziff. 233
[1131] ER Ziff. 234
[1132] ER Ziff. 236
[1133] ER Ziff. 236 f.

4.9.6 Abs. 4 und Abs. 5

Abs. 4 stellt klar, dass eine weitergehende Anwendung nationalen Strafrechts von Art. 22 im Übrigen unberührt bleibt. Die Konvention sieht nur einen Mindestanwendungsbereich vor, ohne weitergehende Bestimmungen auszuschließen.

Abs. 5 betrifft den Fall, dass mehrere Rechtsordnungen Anwendung finden. In einem solchen „Kollisionsfall", sollen sich die Vertragsparteien „gegebenenfalls konsultieren". Eine dem IPR vergleichbare Kollisionsregelung wird damit nicht getroffen.[1134] Bestenfalls handelt es sich um eine vage Absichtserklärung.[1135]

4.9.7 Deutsches Strafanwendungsrecht

Die Anwendung deutschen Strafrechts wird in den §§ 3-7 StGB geregelt. Von entscheidender Bedeutung ist darüber hinaus § 9 StGB, der den Ort der Tat festlegt, an den die zuvor genannten Vorschriften anknüpfen.

4.9.7.1 §§ 3 und 4 StGB – Territorialitäts- und Flaggenprinzip

§ 3 StGB verankert seit dem 2. StRG[1136], in Kraft getreten am 01.01.1975, wieder das Territorialitätsprinzip als Grundsatz des Internationalen Strafrechts im StGB.[1137] Bis dahin galt das 1940[1138] vom nationalsozialistischen Gesetzgeber eingeführte allgemeine Personalitätsprinzip, das den zuvor primär geltenden Gebietsgrundsatz abgelöst hatte. § 4 StGB legt das Flaggenprinzip nieder. Insoweit ergeben sich keine Unterschiede zu Art. 22 Abs. 1 lit. a) bis c).

4.9.7.2 §§ 5 und 7 StGB

Das aktive Personalitätsprinzip, das an die Staatsangehörigkeit des Täters anknüpft, findet sich nur mehr an vereinzelten Stellen im StGB und dort meist in Verbindung mit weiteren Voraussetzungen.[1139] Ausprägungen weisen die §§ 5 Nr. 3a, 5b, 8, 9, 11a, 12, 13, 14a, 15 sowie § 7 Abs. 2 Nr. 1 StGB auf. § 5 Nr. 3 lit. a), 5 lit. b), 8 lit. a) sowie 9 StGB verlangt darüber hinaus, dass der Täter, der Deutscher ist, „[…] seine Lebensgrundlage im räumlichen Geltungsbereich dieses Gesetzes (StGB) haben muss". Diese Einschränkung ist vor dem Hintergrund verständlich, dass das aktive Personalitätsprinzip an besondere staatsbürgerliche Loyalitäts- und Treuepflichten anknüpft, die der Gesetzgeber nur denjenigen Deutschen zumutet, die einen besonderen – hier räumlichen – Bezug zum Geltungsbereich des deutschen Rechts haben.[1140]

Vom Wortlaut her weitgehend identisch zu Art. 22 Abs. 1 lit. d) der Konvention ist § 7 Abs. 2 Nr. 1 1. Alt. StGB. Nach verbreiteter Ansicht kombiniert diese Norm Elemente des aktiven Personalprinzips sowie des Grundsatzes der stellvertretenden Strafrechtspflege.[1141] § 7 Abs. 2

[1134] ER Ziff. 239
[1135] ER Ziff. 239
[1136] BGBl. 1969 I, S. 717 ff.
[1137] Lackner/Kühl – *Lackner* Rn 1; MK – *Ambos* § 3 Rn 1; NK – *Lemke* § 3 Rn 1; Sch/Sch – *Eser* § 3 Rn 1; SK – *Hoyer* § 3 Rn 1
[1138] GeltungsbereichsVO vom 06.05.1940; RGBl. 1940 I, S. 754 f.
[1139] MK – *Ambos* § 5 Rn 2; Sch/Sch – *Eser* §§ 3-7 Rn 6
[1140] Lackner/Kühl – *Lackner* Vor §§ 3-7 Rn 2; Sch/Sch – *Eser* § 5 Rn. 9; Tröndle/Fischer § 5 Rn 3
[1141] Lackner/Kühl – *Lackner* § 7 Rn 1; Sch/Sch – *Eser* § 7 Rn 1; SK – *Hoyer* § 7 Rn 9; aA: LK – *Tröndle* § 7 Rn 1 sowie Tröndle JR 1977, 1 (2), der in Abs. 2 Nr. 1 insgesamt eine Ausprägung des Personalprinzips sieht.

Nr. 2 StGB verfolgt eine ähnliche Zielsetzung wie Art. 22 Abs. 3.

4.9.7.3 § 9 StGB – Ort der Tat

Mit der Rückkehr des StGB zum Territorialitätsprinzip kommt § 9 StGB, der regelt, an welchem Ort eine Tat begangen wird, zentrale Bedeutung zu. Die inhaltlichen Grenzen des in § 3 StGB niedergelegten Gebietsgrundsatzes können nur mit Blick auf den Ort der Tatbegehung bestimmt werden.[1142] Abs. 1 stellt auf die täterschaftliche Begehung, Abs. 2 auf die Teilnahme ab. § 9 StGB liegt das sog. Ubiquitätsprinzip zu Grunde, wonach als Tatort sowohl der Ort der Begehung der Tathandlung als auch der Ort des tatbestandsmäßigen Erfolgs gilt. Damit wurde ein Jahrzehnte langer Streit zwischen den Anhängern der Tätigkeits- und denjenigen der Erfolgstheorie beendet.[1143] Praktische Bedeutung erlangt dieser Grundsatz vor allem bei Distanzdelikten, bei denen der Handlungs- und der Erfolgsort auseinander fallen.

Dazu wird es bei Delikten in Datennetzen regelmäßig kommen, da ein wesentlicher Anwendungsbereich von Netzwerken in der Übertragung von Informationen über große räumliche Entfernungen besteht. Solange der Täter im Inland handelt oder sich der Erfolg von Auslandstaten im Inland verwirklicht, ergeben sich keine Besonderheiten. Größere Schwierigkeiten bereitet allerdings der Fall, dass Handlungen im Ausland vorgenommen werden, deren Wirkungen sich im Inland zeigen, ohne dass es sich nach deutschrechtlichem Verständnis um Erfolgsdelikte im Sinne der allgemeinen Verbrechenslehre handelt. Angesprochen sind die sog. abstrakten Gefährdungsdelikte, die lediglich eine gefährliche Handlung voraussetzen.[1144] Ein Erfolg im Sinne einer zeitlich-räumlich von der Handlung abgrenzbaren Wirkung am Tatobjekt wird darüber hinaus im Tatbestand dieser Delikte nicht beschrieben, so dass der Anwendungsbereich von § 9 Abs. 1 Var. 3 und 4 StGB an sich nicht eröffnet wäre.

In einer neueren Entscheidung hat sich der BGH[1145] über derartige dogmatische Bedenken hinweggesetzt und einen australischen Staatsbürger (nach seiner Einreise in die BRD), der auf einem australischen Webserver rechtsextremistisches Inhalte veröffentlicht hat, wegen Volksverhetzung nach § 130 StGB verurteilt. In der Entscheidung wurde zwar eine Tathandlung in Deutschland verneint, dadurch dass die Informationen in Deutschland über das Internet abgerufen werden konnten, jedoch eine „Eignung zur Friedensstörung“ im Inland bejaht und im Sinne eines Erfolgseinstritts unter § 9 Abs. 1 3. Var. StGB subsumiert. Wenn man mit der zitierten Entscheidung[1146] und der wohl hM[1147] in der Literatur § 130 StGB als abstraktes (bzw. abstrakt-konkretes oder auch potentielles) Gefährdungsdelikt einordnet, lässt sich diese Ansicht nur durch eine extensive Interpretation des Erfolgsbegriffs in § 9 Abs. 1 StGB nachvollziehen.[1148]

In der Praxis führt diese Auffassung dazu, dass Teile des deutschen Strafrechts auf das gesamte WWW-Angebot Anwendung fänden. Deutschland würde – ähnlich wie die USA im militärischen Bereich – zum „Weltpolizisten“ in Sachen strafbarer Internetinhalte avancieren. Auf Grund des in § 152 StPO niedergelegten Legalitätsprinzips wäre die deutsche Staatsan-

[1142] LK – *Gribbohm* § 9 Rn 1 f.; MK – *Ambos/Ruegenberg* § 9 Rn 1
[1143] Jescheck/Weigend, Strafrecht AT, § 18 IV, S. 177 ff.; LK – *Tröndle* § 9 Rn 1; NK – *Lemke* § 9 Rn 3 ff.
[1144] Lackner/Kühl – *Kühl* Vor § 13 Rn 32; Sch/Sch – *Lenckner* Vorbem §§ 13 ff. Rn 129; Tröndle/Fischer Vor § 13 Rn 13a
[1145] BGH Urteil vom 12.12.2000, ZUM-RD 2001, 103 = BGHSt 46, 212 ff.; kritisch: Gercke ZUM 2002, 283 ff.
[1146] BGHSt 46, 212 (218)
[1147] Kienle, 76 ff.; Sieber NJW 1999, 2065 (2067); Tröndle/Fischer Vor § 13 Rn 13a
[1148] Eingehend dazu und im Ergebnis ablehnend: Kienle, 41ff.; MK – *Ambos*/*Ruegenberg* § 9 Rn 32 ff. sowie Sieber NJW 1999, 2065 (2065 f), der den Begriff des „Tathandlungserfolgs“ prägt.

waltschaft zu weltweiten Ermittlungen veranlasst. Eine Beschränkung dieses evident sinnlosen Unterfangens wäre nur über § 153c StPO möglich.[1149] Aber auch in rechtlicher Hinsicht kann die Ansicht des BGH nicht überzeugen. Zum einen widerspricht sie der gefestigten Dogmatik der abstrakten Gefährdungsdelikte.[1150] Zum anderen ist *Gercke*[1151] darin zuzustimmen, dass das Völkerrecht dem nationalen Strafanspruch Grenzen setzt. Das völkerrechtliche Souveränitätsprinzip verlangt für die Erfassung strafrechtlicher relevanter Vorgänge außerhalb des eigenen Staatsgebiets „sinnvolle Anknüpfungspunkte", die einen Bezug zum eigenen Staat begründen.[1152] Inwieweit diese Voraussetzungen vorliegen, ist im Rahmen einer umfassenden Interessenabwägung festzustellen. Ob die Bereithaltung rechtswidriger Inhalte an einem beliebigen Ort der Welt mit der bloßen Möglichkeit des Abrufs im Inland zur Begründung dieses Inlandsbezugs genügt, erscheint höchst zweifelhaft.[1153]

Um eine deutsche Allzuständigkeit bei der Bekämpfung von Äußerungs- und Verbreitungsdelikten im Internet zu vermeiden, schlägt die Literatur[1154] eine Differenzierung anhand der verwendeten Technologie vor. Danach soll ein ausländischer Anbieter rechtswidriger Inhalte im Internet nur dann nach deutschem Strafrecht verantwortlich sein, wenn er diese Inhalte nach Deutschland versendet, etwa per Email, nicht jedoch, wenn er sie lediglich zum Abruf auf einem ausländischen Server mit der bloßen Möglichkeit der Kenntnisnahme im Inland bereithält. Diese Ansicht trägt zwar den technischen Gegebenheiten Rechnung, vermag jedoch nicht die dogmatischen Bedenken auszuräumen, dass abstrakte Gefährdungsdelikte keinen Erfolgseintritt voraussetzen. Folgt man jedoch der Ansicht *Siebers*[1155] und legt den Erfolgsbegriff des § 9 StGB in Anlehnung an die §§ 13 und 78a StGB abweichend von der allgemeinen strafrechtlichen Tatbestandslehre aus, so erscheint einzig die dargestellte technologieorientierte Differenzierung dogmatisch und praktisch konsequent. Anderenfalls bleibt es bei den allgemeinen Grundsätzen, wonach der Tatort abstrakter Gefährdungsdelikte mangels eines tatbestandlichen Erfolgs nach der Tathandlung zu bestimmen ist.[1156]

4.9.7.4 Ergebnis zum internationalen Strafanwendungsrecht

Sowohl Art. 22 als auch das deutsche Strafanwendungsrecht gehen ursprünglich vom Territorialitätsprinzip aus. Abweichungen ergeben sich im Wesentlichen aus dem umfassenden Verständnis des Tatortes nach der Ubiquitätstheorie des § 9 StGB. Diese Unterschiede bestehen allerdings nur dann, wenn man die „Möglichkeit einer abstrakten Gefahr im Inland" mit dem BGH als Erfolg eines abstrakten Gefährdungsdelikts qualifiziert und sich über die gefestigte Dogmatik in der deutschen Verbrechenslehre hinwegsetzt.

4.9.8 Bewertung Art. 22

Art. 22 Abs. 1 sieht durch die Buchstaben a) bis d) die Begründung ganz unterschiedlicher Strafanwendungsprinzipien vor. Die Grundentscheidung geht jedoch in Richtung des Territorialitätsprinzips. Dies lässt sich im Umkehrschluss aus Abs. 2 entnehmen, der einen Vorbehalt lediglich in Bezug auf die Buchstaben b) bis d) enthält und somit von der zwingenden Umset-

[1149] Sieber NJW 1999, 2065 (2067 f.)
[1150] Siehe Fn 1144
[1151] Gercke ZUM 2002, 283 (286)
[1152] „Lotus-Entscheidung" des StIGH vom 07.09.1927, abgedruckt in: StIGHE 5, 71 ff.
[1153] MK – *Ambos*/*Ruegenberg* § 9 Rn 34
[1154] Gercke ZUM 2002, 283 (286); Sieber NJW 1999, 2065 (2070 ff.)
[1155] Sieber NJW 1999, 2065 (2068 ff.)
[1156] Im Ergebnis ebenso: Kienle, S. 52

zung von lit. a) ausgeht. Die eigentliche Sachfrage, nämlich der Ort an dem eine Tat begangen wurde, bleibt von Art. 22 unbeantwortet.

5 Zusammenfassung der Ergebnisse

1. „Convention on Cybercrime“ ist ein in die Irre führender Titel für den vorliegenden völkerrechtlichen Vertrag, der durch den Europarat vorbereitet und ausgearbeitet wurde. Das Augenmerk des europäischen Gremiums galt nicht etwa dem Teilbereich der Netzwerkdelikte, wie es der Wortbestandteil „Cyber“ vermuten ließe, sondern vielmehr jeder strafrechtlich relevanten Konstellation, an der ein EDV-System als Tatmittel oder -werkzeug beteiligt sein kann. Richtigerweise wäre das Übereinkommen daher mit „Convention on Computercrime“ zu überschreiben. Auf Grund dieses sehr allgemein gehaltenen Ansatzes lässt der vorliegende Entwurf an vielen Stellen die – im strafrechtlichen Bereich – wünschenswerte Regelungsdichte vermissen.

2. Generell begrüßenswert hingegen ist der „Allgemeine Teil“ in Art. 1, der Grundbegriffe der Computerkriminalität auf einheitliche und zeitgemäße Weise definiert. Das deutsche Recht lässt entsprechende Legaldefinitionen sowie eine Abstimmung zwischen materiellem Recht und Verfahrensrecht, sowie Kern- und Nebenstrafrecht bislang vermissen.

In Bezug auf die Begriffe des „Datenverarbeitungsanlage“ und der „Daten“ ergeben sich daraus keine größeren Probleme. Die hM zieht den Gesetzeszweck sowie die in § 202a Abs. 2 StGB beschriebenen Einschränkungen des Datenbegriffs heran, um den Anwendungsbereich beider Tatbestandsmerkmale auf ein elektronisches Umfeld zu beschränken. Bedenken in Bezug auf die Bestimmtheit einiger „Computerdelikte“ im StGB resultieren nicht auf Grund fehlender Legaldefinitionen in diesem Bereich, sondern vielmehr wegen unzureichend beschriebener Tathandlungen (beispielsweise im Fall des § 303a StGB, siehe Kapitel 3.3.5.1.2).

Gravierender wirkt sich hingegen die das Fehlen präziser Begriffsbestimmungen in Bezug auf „Dienstanbieter“ sowie „Verbindungsdaten“ aus. Für erhebliche Verunsicherung in diesem Bereich haben vor allem das TDG des Bundes und der MDStV der Länder gesorgt. Beide Gesetze beanspruchen auf Grund einer umfassenden Regelung zur „Verantwortlichkeit“ von Dienstanbietern auch auf dem Gebiet des Strafrechts Geltung. Dabei gelang es den Gesetzgebern jedoch nicht, die „Tele-“ bzw. „Mediendienste“ vom Telekommunikationsbereich definitorisch klar abzugrenzen. Als Konsequenz daraus ist auch eine Unterscheidung der Dienstanbieter in Computernetzen und ihrer jeweiligen strafrechtlichen Verantwortlichkeit auf der Grundlage beider Gesetze kaum durchführbar. Diese Problematik wirkt sich unmittelbar auf den rechtlichen Umgang mit den „Verbindungsdaten“ aus, da diese üblicherweise nicht beim Benutzer, sondern beim Dienstanbieter anfallen. Handelt es sich hierbei um den Leitungs- oder Zugangs- (engl. *access*) Anbieter, entstehen „Telekommunikationsverbindungsdaten“. Anderenfalls kommen „Teledienstenutzungsdaten“ in Betracht. Diese Unterscheidung hat erhebliche Bedeutung für den Zugriff der Ermittlungsbehörden im Strafverfahren. Wegen der diffusen Beschreibung der Tele- und Mediendienste ist auch hier eine klare Abgrenzung kaum möglich.

3. Für den materiellrechtlichen Teil ergibt sich folgende zusammenfassende Bewertung:

Art. 2 strebt einen grundsätzlichen Richtungswechsel dahingehend an, unter dem Begriff „Hacking“ umgangssprachlich zusammengefasste Handlungen zu kriminalisieren. Dabei bleibt die Vorschrift eine Definition dessen, was unter „Zugriff nehmen“ zu verstehen sei, schuldig. Dreh- und Angelpunkt im gesamten Vertragsentwurf ist stattdessen ein generalklau-

selartig verwendeter Begriff der „Unbefugtheit“ (engl. *„without right“*), ohne dass dadurch ein materieller Unwertgehalt bestimmter Verhaltensweisen definiert würde. Gerade die Ausführungen in Kapitel 1.7 (Phänomenologie der Netzwerkkriminalität) haben jedoch gezeigt, dass nicht jeder „Zugriff“ auf ein System kriminelle Energie des Täters erfordert. Oft stehen EDV-Anlagen auf Grund ihrer technischen Komplexität einer breiten Öffentlichkeit offen, ohne dass der Betroffene dies bemerkt. Darüber hinaus ist „Zugriff“ nicht gleich „Zugriff“. Echte Mehrbenutzersysteme bedienen sich eines ausgefeilten Rechtesystems, so dass nur die Erlangung der Kontrolle über geschützte Bereiche oder auf Administratoren-Rechte als strafwürdig erscheint. Eben diese Ansicht scheint auch der deutsche Gesetzgeber im 2. WiKG geteilt zu haben und verneinte die Strafbarkeit des „bloßen Eindringens in ein EDV-System“. Was darunter im Einzelnen zu verstehen sei, blieb wie in der Konvention ungeklärt.

Art. 3 knüpft an die gerade beschriebenen Defizite des Art. 2 an. Vor allem dadurch, dass er nicht auf besonders schutzwürdige Datenübertragungen beschränkt ist, sondern jegliche „nichtöffentliche“ Kommunikation erfasst, stellt sich die Problematik der Überkriminalisierung von Bagatellfällen. Um nicht mit den sprichwörtlichen „Kanonen auf Spatzen zu schießen“, wäre es wünschenswert gewesen, an den Einsatz zumutbarer Schutzvorkehrungen durch die gefährdeten Nutzer anzuknüpfen. Stattdessen wurde auch hier der Ausweg in dem wenig bestimmten Begriff der „Unbefugtheit“ gesucht.

Als weiterer Hauptkritikpunkt an den Delikten im ersten Titel der Konvention bleibt hervorzuheben, dass es den Verfassern des Übereinkommens ebenso wenig wie dem deutschen Gesetzgeber im 2. WiKG gelungen ist, ein taugliches Zuordnungskriterium für unkörperliche Daten zu beschreiben. Am deutlichsten wird dies bei Art. 4, der den Sachbeschädigungsdelikten in Bezug auf körperliche Gegenstände nachempfunden ist. Während dort die „Fremdheit“ einer Sache zur Bestimmung der Berechtigung an ihr herangezogen werden kann, ist dies bei unkörperlichen Daten gerade nicht möglich. Stattdessen kommt es auf computerspezifische Rechte an, die ein Benutzer hinsichtlich bestimmter Daten definieren kann. Als Beispiele für die Vergabe von Berechtigungen seien Betriebssysteme wie „Unix/Linux“ und „NovellNetware“ genannt.

Art. 5 korrespondiert weitgehend mit § 303b StGB, ohne jedoch auf Manipulationen an der Hardware anwendbar zu sein. Dafür werden im Unterschied zur deutschen Strafnorm auch die Computersysteme von Privatleuten geschützt. Spam-Emails werden von beiden Vorschriften nicht erfasst. Angriffen auf die Verfügbarkeit eines Computersystems – Dos/DDoS – kann in Abhängigkeit von ihrem technischen Ablauf[1157] durch beide Vorschriften nur in Ausnahmefällen begegnet werden. Im Übrigen bestehen Bedenken in Bezug auf die hinreichende Bestimmtheit von Art. 5, da es dem Tatbestand nicht gelingt, eine Verbotsmaterie erschöpfend zu beschreiben.

Zu Recht umstritten bleibt Art. 6. Weder aus dem Wortlaut der Konvention noch aus den Erläuterungen ist zu entnehmen, welche „Vorrichtungen“ gemeint sind, deren „Herstellung“ usw. als strafwürdig erachtet wird. Unbefriedigend ist auf jeden Fall der Ansatz, auf eine subjektive Verwendungsabsicht des Täters abzustellen. Entscheidend muss vielmehr sein, ob ein bestimmtes Hilfsmittel allein und ausschließlich zu strafbaren Zwecken benutzt werden kann. Nur in dieser Gestaltung läuft die Vorverlagerung der Strafbarkeit in den Bereich von Vorbereitungshandlungen nicht Gefahr, den „fragmentarischen Charakter“ des Strafrechts zu übergehen. Gerade auf diesen Ansatz haben die Verfasser der Konvention jedoch verzichtet.

[1157] Siehe Kapitel 1.7.3.

In Bezug auf die Delikte der „Computerurkundenfälschung“ und des „Computerbetrugs“ ergeben sich keine nennenswerten Besonderheiten gegenüber dem nationalen Strafrecht.

Hinsichtlich der Bekämpfung von Kinderpornografie im Internet hat der deutsche Gesetzgeber die einschlägigen Delikte im 13. Abschnitt des StGB mit Wirkung zum 01.04.2004 grundlegend reformiert. In Bezug auf die geächteten Inhalte unterscheidet sich Art. 9 nur in Bezug auf die Altersgrenze der Darsteller vom deutschen Strafrecht. Anders bei den Tatobjekten. Die Konvention stellt auf „visuelle Darstellungen“ ab, während hier zu Lande zwischen „Schriften“ im Sinne von § 11 Abs. 3 StGB und „Live“-Darbietungen unterschieden wird. In der Vergangenheit hat sich vor allem als problematisch erwiesen, wann beim Herunterladen pornografischer Bilder ein „Verbreiten“ angenommen werden kann. In Zukunft drohen Strafbarkeitslücken bei „Streaming Media“-Angeboten, die zeitverzögert, d.h. nicht „live“ und ohne längerfristige Speicherung übertragen werden. In diesem Fall handelt es sich weder um Schriften oder gleichgestellte Darstellungen, noch um die von § 184c StGB n.F. erfassten „Darbietungen“.

Besondere Beachtung durch den Europarat erfuhren die Urheberrechtsdelikte. Dabei dürfte es sich um einen der zukünftigen Brennpunkte im Bereich der Computerkriminalität handeln. Dies liegt im Wesentlichen an der stetig zunehmenden Bedeutung unkörperlicher Daten im „Informationszeitalter“ sowie geänderten technischen Rahmenbedingungen, die „Softwarepiraten“ durch Breitbandtechnologie, CD/DVD-Brenner und dergleichen die Verletzung geistigen Eigentums denkbar leicht gemacht haben. Das Schutzniveau orientiert sich in erster Linie an internationalen Abkommen auf dem Gebiet des Urheberzivilrechts. Auch in diesem Bereich ist der deutsche Gesetzgeber erst kürzlich tätig geworden und hat durch das „Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft“ vom 10.09.2003 das nationale Urheberrecht an europäische und internationale Vorgaben angepasst. In Bezug auf das Urheberstrafrecht ergeben sich nach der letzten Novellierung keine wesentlichen Unterschiede mehr zu Art. 10 der Konvention. Zu kritisieren bleibt allein die weiterhin verbreitete, unsachliche Begrifflichkeit der sog. „Raubkopie“, die eine Nähe zum Raubtatbestand suggeriert, obwohl beim Anfertigen rechtswidriger Vervielfältigungsstücke weder „Gewalt gegen eine Person“ noch eine „Drohung mit einer gegenwärtigen Gefahr“ angewendet werden.

Hinsichtlich der Art. 11 bis 13 verdient lediglich Art. 12 besondere Erwähnung, der einen internationalen und vor allem europäischen Trend zur Begründung einer Verbandsverantwortlichkeit aufgreift. Ansätze hierfür finden sich bereits im deutschen Ordnungswidrigkeitenrecht.

4. Der verfahrensrechtliche Teil weist in vielen Bereichen signifikante Abweichungen vom geltenden deutschen Recht auf:

Besonders hervorzuheben ist Art. 14 Abs. 2 lit. c). Wie bereits eingangs dieser Zusammenfassung dargestellt, zielt diese Regelung darauf ab, die verfahrensrechtlichen Bestimmungen der Konvention nicht nur für die im materiellrechtlichen Teil beschriebenen Delikte zur Anwendung zu bringen, sondern darüber hinaus für die Erhebung von Beweisen in „elektronischer Form“ in Bezug auf beliebige Straftaten. Im Ergebnis zielt diese Vorschrift damit auf eine grundlegende Änderung vor allem der Befugnisnormen der StPO ab.

Art. 15 stellt einen der Hauptkritikpunkte an der „Convention on Cybercrime“ dar. Zwar dient dieser Artikel grundsätzlich dem Schutz der von den Ermittlungsmaßnahmen im Sinne der Konvention Betroffenen. Die Norm geriet jedoch viel zu pauschal, da die einzelnen Befugnisnormen der Artikel 16 bis 21 lediglich auf sie verweisen und im Gegenzug auf detaillierte

Schutzbestimmungen in Bezug auf die konkrete Eingriffsmaßnahme verzichten. Es fehlen vor allem obligatorische Richtervorbehalte – etwa in Bezug auf Eingriffe in das Fernmeldegeheimnis – Fristen für die Speicherung von Daten, Beschlagnahmeverbote und dergleichen. Ein genereller Hinweis auf die Menschrechtskonvention oder den Verhältnismäßigkeitsgrundsatz und dergleichen kann keinen Ersatz für Detailregelung hinsichtlich der Eingriffstiefe im Einzelfall darstellen, wenn die Freiheits- und Bürgerrechte der Betroffenen in rechtsstaatlich gebotener Weise berücksichtigt werden sollen. In diesem Punkt bestehen gravierende Defizite.

Art. 16, 18 und 19 gehen in Bezug auf die Sicherstellung von Daten erheblich über die StPO hinaus. Dies liegt im Wesentlichen daran, dass sie sich auf Daten unabhängig vom Medium, auf dem sie gespeichert sind, beziehen. Das deutsche Strafprozessrecht kennt im sachlichen Beweisbereich nur körperliche „Gegenstände“ und „Papiere“, was die Datenträger jedoch nicht unmittelbar die darauf befindlichen Informationen erfasst. In der wissenschaftlichen Diskussion hier zu Lande behalf man sich daher mit einer „Erstreckung“ der Beweisbedeutung vom stofflichen Substrat auf die unkörperlichen Inhalte, da beide in einem untrennbaren Zusammenhang stünden. Sofern die Voraussetzungen einer Sicherstellungsanordnung in Bezug auf den Datenträger vorlagen, wurde argumentiert, dass sich diese unterschiedslos auf die unkörperlichen Inhalte erstrecke. Die Anfertigung von Kopien sei sogar der „mildere Eingriff“, da das Speichermedium beim Berechtigten verbleiben könne. Diese Ansicht wird vorliegend abgelehnt.

Richtig ist, dass die Anordnung einer Sicherstellung sich dort auf die Daten erstreckt, wo die Berechtigung an den gespeicherten Informationen und am Datenträger in derselben Person zusammenfallen. Dies wird in der Regel bei lokalen Datenträger der Fall sein, die nur eine begrenzte Kapazität aufweisen. Der technische Fortschritt hat jedoch zur Entwicklung großvolumiger Speichermedien geführt, bei deren Einsatz – vor allem in Computernetzwerken – die an den Daten und am Datenträger Berechtigten oftmals nicht übereinstimmen. Bei der Sicherstellung eines Netzwerklaufwerks wird daher in unterschiedlicher Weise in die Rechte verschiedener Personen eingegriffen. Während in Bezug auf den Eigentümer des Datenträgers vor allem dessen Eigentumsgrundrecht betroffen ist, greift das Kopieren von Daten in das Recht an der Information im Sinne der informationellen Selbstbestimmung ein. In beiden Fällen liegt eine völlig unterschiedlich zu beurteilende Art der Rechtsbeeinträchtigung vor. Es ist daher falsch, wie bisher angenommen, die Beweisbedeutung des Datenträgers unterschiedslos auf die gespeicherten Daten zu erstrecken. Vielmehr müssen die Eingriffsvoraussetzung in Bezug auf gespeicherten Informationen gesondert beurteilt werden. Die Schlussfolgerung, dass die Anfertigung von Kopien stets der mildere Eingriff sei, verbietet sich jedenfalls in dieser Pauschalität.

Für die Durchsuchung eines Datenträgers ergibt sich eine ähnliche Beurteilung, da die StPO auch in diesem Fall, anders als Art. 19 Abs. 1, von zu durchsuchenden „Gegenständen“ und nicht von unkörperlichen Daten ausgeht.

Ebenso wenig können die deutschen Ermittlungsbehörden, die in den Besitz beweisrelevanter Daten gelangen wollen, deren Herausgabe anordnen, so wie dies von Art. 18 vorgesehen ist. Nach hM bezieht sich eine Herausgabeanordnung nach § 95 StPO nur auf körperliche Gegenstände und beinhaltet darüber hinaus keine generelle Verpflichtung zur Erstellung von Kopien. Die Lösung dürfte vor allem in der Erweiterung der Herausgabebefugnisse auf Daten liegen, wie dies im Rahmen besonderer Datenarten – etwa den sog. Bestandsdaten von Kunden der Telekommunikationsdienstleister – bereits geschehen ist.

Ein Sonderproblem stellt der Zugriff auf Emails dar, während diese in sog. „Mailboxen“ ruhen. In diesem Fall wird auch hier zu Lande diskutiert, ob Daten, während sie sich auf einem Server befinden, sichergestellt werden können, oder ob der Vorgang vom Absenden bis zum Lesen durch den Empfänger einheitlich zu bewerten ist und dem Fernmeldegeheimnis unterliegt, in das nur durch eine Überwachung der Telekommunikation eingegriffen werden kann. Die Verfasser der Konvention haben keine eindeutige Entscheidung getroffen. In Deutschland wird bislang die Anwendung der §§ 100a f. StPO bejaht, obwohl der Zugriff auf „ruhende“ Daten jedenfalls vom Wortlaut her keine „Überwachung und Aufzeichnung der Telekommunikation“ darstellt.

Hinsichtlich der Überwachung der Inhalte und der äußeren Umstände einer Kommunikation unterscheiden sich die Art. 20 und 21 kaum von den § 100a f. und 100g f. StPO, was die inhaltliche Reichweite der Maßnahmen betrifft. Etwas anderes gilt in Bezug auf den Schutz der davon Betroffenen. Während § 100a StPO einen abschließenden Straftatenkatalog vorsieht, im Rahmen dessen eine Überwachung der Telekommunikation zulässig ist, spricht Art. 21 nur von einer „Reihe schwerer Straftaten“, ohne diese jedoch näher zu definieren. Ebenso wenig ist ein Richtervorbehalt, noch eine Höchstdauer der Überwachung normiert. Ähnliche Defizite bestehen auch im Rahmen der Verbindungsdaten, deren Überwachung von Art. 20 geregelt wird.

5. Art. 22 enthält Regelungen zum geographischen Anwendungsbereich der Art. 2 bis 11. Die entscheidende Frage in Bezug auf den Ort der Tat, den § 9 StGB im deutschen Strafrecht bestimmt, bleibt unbeantwortet. Die Konvention differenziert weder danach, wo der Täter handelte, noch wo der Erfolg seiner Tat eintrat. Die eigentliche Sachfrage bleibt damit offen.

6. Im Ergebnis muss die bereits im ersten Kapitel dieser Untersuchungen dargestellte Kritik von Datenschützern und Interessenverbänden an der „Cybercrime Convention“ bestätigt werden. Als Ausblick bleibt zu hoffen, dass der deutsche Gesetzgeber, sollte er die Konvention ratifizieren, besonderes Augenmerk auf die inhaltliche Präzisierung der materiellen Strafnormen sowie die Begrenzung der verfahrensrechtlichen Befugnisse des Übereinkommens legt. Anderenfalls droht ein Übergewicht staatlicher Strafverfolgungsinteressen zu Lasten privater Menschen- und Freiheitsrechte.

Literaturverzeichnis

Achenbach, Hans
Die „kleine Münze“ des sog. Computer-Strafrechts – Zur Strafbarkeit des Leerspielens von Geldspielautomaten, Jura 1991, 225-230

Albrecht, Hans-Jörg/Neumann, Ulfrid
Nomos-Kommentar zum Strafgesetzbuch, Baden-Baden, Loseblattausgabe
zit.: NK – Bearbeiter § Rn

Bär, Wolfgang
Der Zugriff auf Computerdaten im Strafverfahren, Köln, 1992, zugl. Bayreuth, Univ. Diss., 1991

Polizeilicher Zugriff auf kriminelle Mailboxen, CR 1995, 489-500

Auskunftsansprüche über Telekommunikationsdaten nach den neuen §§ 100g, 100h StPO, MMR 2002, 358-364

Bäumler, Helmut
Eine sichere Informationsgesellschaft – Zur europäischen Bekämpfung der Computerkriminalität, DuD 2001, 348-352

Bechthold, Stefan
Der Schutz des Anbieters von Informationen – Urheberrecht und Gewerblicher Rechtsschutz im Internet, ZUM 1997, 427-450

Binding, Karl
Lehrbuch des gemeinen deutschen Strafrechts, Besonderer Teil, Leipzig, 1904
zit.: *Binding, Lehrbuch Bes. Teil, S.*

Bohnert, Joachim
Kommentar zum Ordnungswidrigkeitenrecht, München, 2003

Bonner Kommentar zum Grundgesetz
siehe: Dolzer, Rudolf/Vogel, Klaus

Bornemann, Roland
Der Jugendmedienschutz-Staatsvertrag der Länder, NJW 2003, 787-791

Bortloff, Nils
Tonträgersampling als Vervielfältigung, ZUM 1993, 476-481

Boujong, Karl-Heinz
Karlsruher Kommentar zum Gesetz über Ordnungswidrigkeiten
2. Auflage, München, 2000
Online: http://beck-gross.digibib.net/bib/home.asp
zit.: KK/OWiG – Bearbeiter § Rn

Bühler, Christoph
Ein Versuch, Computerkriminellen das Handwerk zu legen: Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität, MDR 1987, 448-457

Cohen, Fred
Computer Viruses – Theory and Experiments, Ph.d. dissertation, University of Southern California, 1984, http://all.net/books/virus/index.html (01.04.2004)

Dolzer, Rudolf/Vogel, Klaus
Bonner Kommentar zum Grundgesetz, Heidelberg, Loseblattausgabe
zit.: BK – Bearbeiter Art. Rn

Dreier, Horst
Grundgesetz Kommentar, Tübingen, 1998
zit.: Dreier – Bearbeiter Art. Rn

Dreier, Thomas/Schulze, Gernot
Urheberrechtsgesetz Kommentar, München, 2004

Echterhölter, Rudolf
Die Europäische Menscherrechtskonvention im Rahmen der verfassungsmäßigen Ordnung, JZ 1955, 689-693

Die Europäische Menschenrechtskonvention in der juristischen Praxis, JR 1956, 142-146

Eckhardt, Jens
Telekommunikations-Überwachungsverordnung – Ein Überblick, CR 2001, 670-678

Eisenberg, Ulrich
Beweisrecht der StPO – Spezialkommentar, 4. Auflage, München, 2002

Eisenberg, Ulrich/Nischan, Anett
Strafprozessualer Zugriff auf digitale multimediale Videodienste, JZ 1997, 74-83

Emmert, Ulrich
Anti- Hacker-Gesetz: Strafbare Sicherheits-Tools? KES 2002/2, S. 6;
http://www.kes.info/_archiv/_onlinearch/02-02-6-zkdsg.htm (01.04.2004)

EMRK-Kommentar
siehe: Frowein, Jochen/Peukert, Wolfgang

Engel-Flechsig, Stefan/Maennel, Frithjof/Tettenborn, Alexander
Das neue Informations- und Kommunikationsdienstegesetz, NJW 1997, 2981-2992

Beck'scher IuKDG-Kommentar, München, 2001

Erichsen, Hans-Uwe/Ehlers, Dirk
Allgemeines Verwaltungsrecht, 12. Auflage, Berlin, 2002

European Committe on Crime Problems (CDPC)
siehe: Europarat

Europäisches Parlament/Schmid, Gerhard (Berichterstatter)
Bericht über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON) (2001/2098(INI)),
Nichtständiger Ausschuss des Europäischen Parlaments über das Abhörsystem Echelon, http://www.europarl.eu.int/tempcom/echelon/rrechelon_en.htm (01.04.2004)

Europarat
Explanatory Report (dt. Erläuternder Bericht), 2001
http://conventions.coe.int/Treaty/en/Reports/Html/185.htm (01.04.2004)

Computer-Related Crime: Recommendation No. R (89) 9 on computer-related crime and final report of the European Committee on Crime Problems; Strasburg, 1990

European Institute for the Media/Friedrich-Ebert-Stiftung (Hrsg.)
Twilight Zones in Cyberspace: Crimes, Risk, Surveillance and User-Driven Dynamics, Prof. Dr. Jo Groebel/ Dr. Verena Metze-Mangold/ Jowon van der Peet/ Dr. David Ward, http://library.fes.de/pdf-files/stabsabteilung/01102.pdf (01.04.2004)

Explanatory Report (dt. Erläuternder Bericht)
siehe: Europarat

Frech, Martin
Der Bedeutungswandel des Begriffs „Hacker" seit seiner Entstehung zu Beginn der 60er Jahre, Seminararbeit an der FU Berlin, http://userpage.chemie.fu-berlin.de/~frech/sicherheit/hacker.pdf (01.04.2004)

Freund, Georg
Grundfälle zu den Urkundendelikten, JuS 1993, 731-737, 1016-1022; JuS 1994, 30-36, 125-129, 207-212, 305-309

Fromm, Friedrich Karl/Nordemann, Wilhelm
Urheberrecht – Kommentar zum Urheberrechtsgesetz und zum Urheberrechtswahrnehmungsgesetz, 9. Auflage, Stuttgart, 1998
zit.: Fromm/Nordemann – Bearbeiter § Rn

Frowein, Jochen/Peukert, Wolfgang
EMRK-Kommentar, 2. Auflage, Kehl, 1996, *zit. Frowein/Peukert – Bearbeiter § Rn*

Fuhrberg, Kai
Sicherheit im Internet, Dokument des BSI, http://www.bsi.de/literat/doc/sinetdoc/sinetstd.htm (01.04.2004)
zit.: Fuhrberg, [Kapitelnummer]

Gampp, Markus
Die Beurteilung von „Musik-Tauschbörsen" im Internet nach US-amerikanischem Urheberrecht – Der Präzedenzfall Napster und seine Nachfolger, GRURInt 2003, 991-1002

Gercke, Marco
Die Entwicklung der Rechtsprechung zum Internetstrafrecht in den Jahren 2000 und 2001, ZUM 2002, 283-288

Gerhards, Thomas
Computerkriminalität und Sachbeschädigung, Mannheim, Univ. Diss., 1993

Germann, Michael
Gefahrenabwehr und Strafverfolgung im Internet, Berlin, 2000, zugl.: Erlangen-Nürnberg, Univ. Diss., 1999

Göhler, Erich
Ordnungswidrigkeitengesetz, 13. Auflage, München, 2002

Gössel, Karl Heinz
Strafrecht, besonderer Teil/1, Heidelberg, 1987

Gravenreuth, Günter von
Computerviren, Hacker, Datenspione, Crasher und Cracker, NStZ 1989, 201-207

Greiner, Arved
Die Verhinderung verbotener Internetinhalte im Wege polizeilicher Gefahrenabwehr, Univ. Diss., 2001

Groß, Thomas
Die Schutzwirkung des Brief-, Post- und Fernmeldegeheimnisses nach der Privatisierung der Post, JZ 1999, 326-336

Haft, Fritjof
Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität (2.WiKG), NStZ 1987, 6-10

Hamelink, C.
New Information and Communication Technologies, Social Development and Cultural Change, Discussion paper No. DP 86. Geneva: United Nations Research Institute for Social Development, http://www.unrisd.org/engindex/publ/list/dp/dp86/dp86-07.htm (01.04.2004)

Hänel, Frederike
Napster und Gnutella – Probleme bei der Übertragung von MP3-Dateien nach deutschem Urheberrecht, JurPC Web-Dok. 245/2000, Abs. 1-57, http://www.jurpc.de/

Haß, Gerhard
Der strafrechtliche Schutz von Computerprogrammen, in: Lehmann (Hrsg.), Rechtsschutz und Verwertung von Computerprogrammen, 2. Auflage 1993, 467-512

Hauptmann, Peter-Helge
Zur Strafbarkeit des sog. Computerhackens – Die Problematik des Tatbestandsmerkmals „Verschaffen" in § 202a STGB, JurPC 1989, 215-218

Haurand, Günter/Vahle, Jürgen
Computerkriminalität, RDV 1990, 128-134

Heghmanns, Michael
Musiktauschbörsen im Internet aus strafrechtlicher Sicht, MMR 2004, 14-18

Herzog, Roman
Die Rechtsprechung des Bundesgerichtshofs zu Art. 5 der Europäischen Menschenrechtskonvention, JZ 1966, 657-660

Hildebrandt, Ulrich
Die Strafvorschriften des Urheberrechts, Berlin, Univ. Diss., 2000

Hilgendorf, Eric
Grundfälle zum Computerstrafrecht, JuS 1996, 509-512; 702-706; 890-894; 1082-1084; JuS 1997, 130-136; 323-331

Hoeren, Thomas
Skriptum Internetrecht, Stand: Februar 2003; http://www.uni-muenster.de/Jura.itm/hoeren/INHALTE/lehre/lehrematerialien.htm (01.04.2004)

Hoeren, Thomas/Sieber, Ulrich
Handbuch Multimedia Recht, München, Loseblattausgabe, Stand: Aug. 2003
zit.: Hoeren/Sieber – Bearbeiter Teil Rn

Ilzhöfer Volker
Patent-, Marken- und Urheberrecht, 5. Auflage, München, 2002

International Federation of the Record Industry (Hrsg.)
IFPI Music Piracy Report June 2002
http://www.ifpi.org/site-content/publications/publications.html (01.04.2004)

Ipsen, Jörn
Staatsrecht II – Grundrechte, 6. Auflage, Neuwied, 2003

Jarass, Hans/Pieroth, Bodo
Grundgesetz für die Bundesrepublik Deutschland – Kommentar, 7. Auflage, München, 2004
zit.: Pieroth/Jarass – Bearbeiter Art. Rn

Jescheck, Hans-Heinrich/ u.a.
Leipziger Kommentar – Strafgesetzbuch; 10. und teilweise 11. Auflage, Berlin,
zit.: LK – Bearbeiter § Rn

Jescheck, Hans-Heinrich/Weigend, Thomas
Lehrbuch des Strafrechts, Allgemeiner Teil, 5. Auflage, Berlin, 1996

Jessen, Ernst
Zugangsberechtigung und besondere Sicherung im Sinne von § 202a StGB, Frankfurt am Main 1994, zugl.: Kiel, Univ. Diss., 1993

Joecks, Wolfgang/Miebach, Klaus
Münchner Kommentar zum Strafgesetzbuch, München, 2003
zit.: MK – Bearbeiter § Rn

Karlsruher Kommentar zum Gesetz über Ordnungswidrigkeiten
siehe: Boujong, Karl-Heinz

Karlsruher Kommentar zur Strafprozessordnung
siehe Pfeiffer, Gerd

Kienapfel, Diethelm
Urkunden und andere Gewährschaftsträger, Frankfurt a.M., 1979

Kienle, Michael
Internationales Strafrecht und Straftaten im Internet, Konstanz, Univ. Diss., 1998

Klesczewski, Diethelm
Das Ende des Auskunftsersuchens nach § 12 FAG, JZ 1997, 719-721

Köhler, Helmut/Piper, Henning
UWG, Gesetz gegen den unlauteren Wettbewerb, 3. Auflage, München, 2002
zit.: Köhler/Piper – Bearbeiter § Rn

Krempl, Stefan
Selbstkontrolle statt Cyber Polizei und Filter?, telepolis, 09.03.2001, http://www.heise.de/tp/deutsch/inhalt/te/7103/1.html

Krey, Volker
Grundzüge des Strafverfahrensrechts (4. Teil), JA 1983, 638-643

Kugelmann, Dieter
Die „Cyber-Crime" Konvention des Europarats, DuD 2001, 215-223

Völkerrechtliche Mindeststandards für die Strafverfolgung im Cyberspace, TMR 2002, 15-23

Kühne, Hans-Heiner
Strafprozeßrecht – Ein Lehrbuch zum deutschen und europäischen Strafrechtsverfahren, 5. Auflage, Heidelberg, 1999

Lackner, Karl/Kühl, Kristian
Strafgesetzbuch mit Erläuterungen, 24. Auflage, München, 2001
zit.: Lackner/Kühl – Bearbeiter § Rn

Laga, Gerhard
Internet im rechtsfreien Raum? Zur Anwendbarkeit bestehender Gesetze auf das Internet, Wien, Univ. Diss., 1998
Online: http://www.juridicum.at/forschung/laga/dissertation/diss.html (01.04.2004)

Lampe, Ernst-Joachim
Die strafrechtliche Behandlung der sog. Computer-Kriminalität, GA 1975, 1-23

Unvollkommen zweiaktige Rechtfertigungsgründe, GA 1978, S. 7-12

Langenfeld, Christine
Die Neuordnung des Jugendschutzes im Internet, MMR 2003, 303-310

Laufhütte, Heinrich
Viertes Gesetz zur Reform des Strafrechts, 2. Teil: Pornographische, gewaltverherrlichende und jugendgefährdende Schriften, JZ 1974, 46-52

Leicht, Armin
Pflicht zur Herausgabe von Datenträgern und Mitwirkungspflichten bei der Aufbereitung von Dateien im Strafverfahren, IuR 1986, 346-360

Computerspionage – Die „besondere Sicherung gegen unberechtigten Zugang" (§202a StGB), IuR 1987, 45-53

Leipziger Kommentar – Strafgesetzbuch
siehe Jescheck, Hans-Heinrich

Lenckner, Theodor/Winkelbauer, Wolfgang
Computerkriminalität – Möglichkeiten und Grenzen des 2. WiKG), CR 1986, 483-488; 654-661; 824-831

Leube, Jutta
Neuere Rechtsprechung zum Kartellordnungswidrigkeitenrecht, NStZ 1984, 41-48

Lewinski, Silke von
Die WIPO-Verträge zum Urheberrecht und zu verwandten Schutzrechten vom Dezember 1996, CR 1997, S. 438-444

Liesching, Marc
Das neue Jugendschutzgesetz, NJW 2002, 3281-3286

Loewenheim, Ulrich
Handbuch des Urheberrechts, München, 2003
zit.: Handbuch des Urheberrechts – Bearbeiter § Rn

Löwe, Ewald/Rosenberg, Werner
Die Strafprozessordnung und das Gerichtsverfassungsgesetz, siehe Rieß, Peter (Hrsg.)

Lütolf, Sandra Hilda
Strafbarkeit juristischer Personen, Zürich, Univ. Diss., 1996

Mack, Holger
Sicherheit in Java und ActiveX, DuD 1999, 192-206;
http://www.secorvo.de/publikat/javaactx.pdf (01.04.2004)

Magnin, Cédric
The 2001 Council of Europe Convention on cyber-crime: an efficient tool to fight crime in cyber-space?, LLM Dissertation, Santa Clara University http://www.magnin.org/Publications/home.htm (01.04.2004)

Mahrenholz, Ernst Gottfried
Brauchen wir einen neuen Pornographiebegriff?, ZUM 1998, 525-529

Mangoldt, Hermann von/Klein, Friedrich/Starck, Christian
Das Bonner Grundgesetz, 4. Auflage, München, 1999
zit.: von Mangoldt/Klein/Starck – Bearbeiter Art. Rn

Mattil, Friedrich
Zur Anwendung des Abschnittes I der Europäischen Menschenrechtskonvention – Zugleich ein Beitrag zur Transformationslehre, JR 1965, 167-171

Maunz, Theodor/Dürig, Günter
Grundgesetz Kommentar, München, Loseblattausgabe
zit.: Maunz/Dürig – Bearbeiter Art. Rn

Maurach, Reinhart/Schroeder, Friedrich-Christian/Maiwald, Manfred
Strafrecht Besonderer Teil, 9. Auflage, Heidelberg, 2003

Maurer, Hartmut
Allgemeines Verwaltungsrecht, 14. Auflage, München, 2002

Staatsrecht I – Grundlagen, Verfassungsorgane, Staatsfunktionen, 3. Auflage, München, 2003

Mayer-Schönberger, Viktor
The Cookie Concept, http://www.cookiecentral.com/content.phtml?area=2&id=1 (01.04.2004)

Mehrings, Josef
Information und Dokumentation (IuD) – Ein Stiefkind der Urheberrechtsnovelle?, GRUR 1983, 275-290

Meurer, Dieter
*Die Bekämpfung der Computerkriminalität in der Bundesrepublik Deutschland***,** in: Hans G. Leser/Isomura, Tamotsu (Hrsg.), Wege zum japanischen Recht **–** Festschrift für Zentaro Kitagawa zum 60. Geburtstag am 5. April 1992*,* Berlin 1992

Meyer, Dieter
Nochmals: Auslegung des Art. 6 Abs. 3 lit. c) und e) MRK, NJW 1974, 1174-1175

Meyer-Goßner, Lutz
Strafprozessordnung – Gerichtsverfassungsgesetz, Nebengesetze und ergänzende Bestimmungen, 46. Auflage, München, 2003

Möhrenschlager, Manfred
Das neue Computerstrafrecht, wistra 1986, 128-142

Computerstraftaten und ihre Bekämpfung in der Bundesrepublik, wistra 1991, 321-331

Morris, Robert T.
A Weakness in the 4.2BSD UNIX TCP/IP Software, Computing Science Technical Report # 117 , AT&T Bell Laboratories, Murray Hill, New Jersey, http://www.eecs.harvard.edu/~rtm/papers.html (01.04.2004)

Mühle, Kerstin
Hacker und Computer-Viren im Internet – eine strafrechtliche Beurteilung, Passau, Univ. Diss., 1998

Müller, Rudolf
Die Grenzen des Bankgeheimnisses, NJW 1963, 833-838

von Münch, Ingo/Kunig, Philip
Grundgesetzkommentar, 5. Auflage, München, 1999,
zit.: von Münch/Kunig – Bearbeiter Art. Rn

Münchner Kommentar zum Strafgesetzbuch
siehe: Joecks, Wolfgang/Miebach, Klaus

Naucke, Wolfgang
Strafrecht: eine Einführung, 10. Auflage, Neuwied, 2002

Nelles, Ursula
Strafprozessrecht: Spuren aus der Datensammlung, JuS 1987, 51-57

Oldfield, Paul
Von Viren, Würmern und Trojanern, Niederolm, 2001
Online: http://www.sophos.de/sophos/docs/deu/comviru/viru_bde.pdf (01.04.2004)

Oppermann, Thomas
Europarecht: ein Studienbuch, 2. Auflage, München, 1999

Organisation for Economic Cooperation and Development (OECD)
Computer-Related Crime : Analysis of Legal Policy, Paris, 1986

Palandt, Otto
Bürgerliches Gesetzbuch, 62. Auflage, München, 2003
zit.: Palandt – Bearbeiter § Rn

Palm, Fritz/Roy, Rudolf
Mailboxen: Staatliche Eingriffe und andere rechtliche Aspekte, NJW 1996, 1791-1797

Der BGH und der Zugriff auf Mailboxen, NJW 1997, 1904-1905

Pätzel, Claus
Zur Offenkundigkeit von Halterdaten, NJW 1999, 3246-3247

Pfeiffer, Gerd
Karlsruher Kommentar zur Strafprozessordnung, 5. Auflage, München, 2003
Online: http://beck-gross.digibib.net/bib/home.asp
zit.: KK – Bearbeiter § Rn

Pieroth, Bodo/Schlink, Bernhard
Grundrechte, 18. Auflage, Heidelberg, 2002

Plassmann, Clemens
Bearbeitungen und anderen Umgestaltungen in § 23 UrhG, Univ. Diss., 1996

Plate, Jürgen
Grundlagen Computernetze, Stand 31.01.2004
http://www.netzmafia.de/skripten/netze/index.html
zit.: Plate, Grundlagen Computernetze, [Kapitelnummer]

Internet – Möglichkeiten und Dienste, Stand: 07.01.2004
http://www.netzmafia.de/skripten/internet/index.html
zit.: Plate, Internet, [Kapitelnummer]

Plate, Jürgen/Holzmann, Jörg
Sicherheit in Netzen, Sicherheitsaspekte in lokalen Netzen und im Internet,
Stand: 21.05.2003, http://www.netzmafia.de/skripten/sicherheit/index.html
zit.: Plate/Holzmann, Sicherheit in Netzen, [Kapitelnummer]

Preuße, Thomas
Informationsdelikte im Internet, Hamburg, 2000, zugl. Hannover, Univ. Diss., 2000

Radtke, Henning
Rechtsbehelfe gegen die "Durchsicht" (§ 110 StPO) von EDV-Anlagen durch Strafverfolgungsbehörden, JurPC Web-Dok. 173/1999, Abs. 1–23
http://www.jurpc.de/aufsatz/19990173.htm#rfn0 (01.04.2004)

Rehbinder, Manfred
Urheberrecht, 13. Auflage, München, 2004

Rieß, Peter/u.a.
Die Strafprozessordnung und das Gerichtsverfassungsgesetz, 24. und teilweise 25. Auflage, Berlin, 1999

Rogall, Klaus
Buchbesprechung zu Bär, Wolfgang: Der Zugriff auf Computerdaten im Strafverfahren, ZStW 110, 745 (751)

Rötzer, Florian
Dürfen von Telediensten IP-Adressen von Flatrate-Kunden gespeichert werden?, telepolis, 16.01.2003,
http://www.heise.de/tp/deutsch/html/result.xhtml?url=/tp/deutsch/inhalt/te/13978/1.html&words=IP%20Adresse%20Speicherung (01.04.2004)

Roßnagel, Alexander
Handbuch Datenschutzrecht, München, 2003
zit.: Handbuch Datenschutzrecht – Bearbeiter Kapitel Rn

Recht der Multimedia-Dienste, München, Loseblattausgabe
zit.: Roßnagel – Bearbeiter Teil § Rn

Rudolphi, Hans-Joachim
Systematischer Kommentar Strafprozessordnung und Gerichtsverfassungsgesetz, Frankfurt am Main, Loseblattausgabe
zit.: SK/StPO – Bearbeiter § Rn

Rudolphi, Hans-Joachim
Systematischer Kommentar zum Strafgesetzbuch, Neuwied, Loseblattausgabe
zit.: SK – Bearbeiter § Rn

Ruef, Marc
Denial of Service (DoS)
http://www.computec.ch/dokumente/denial_of_service/denial_of_service/denial_of_service.html (01.04.2004)
zit.: Ruef, DoS, Kap.

Sachs, Michael
Grundgesetz – Kommentar, München, 2003

Schack, Haimo
Urheber- und Urhebervertragsrecht, 2. Auflage, Tübingen, 2001

Schäfer, Helmut
Der Computer im Strafverfahren, wistra 1989, 8-13

Schlüchter, Ellen
Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität, Heidelberg, 1987

Schmidt-Bleibtreu, Bruno/Klein, Franz
Kommentar zum Grundgesetz, 9. Auflage, Neuwied, 1999
zit.: Schmidt-Bleibtreu/Klein – Bearbeiter Art. Rn

Schmitt, Rudolf
Ordnungswidrigkeitenrecht, München, 1970

Schmitz, Roland
Ausspähen von Daten, § 202a StGB, JA 1995, 478- 483

Schnabl, Andrea
Strafprozessualer Zugriff auf Computerdaten und die „Cyber-Crime" Konvention, JURA 2004, 379-385

Schneider, Uwe/Werner, Dieter
Taschenbuch der Informatik, 3. Auflage, Leipzig, 2000
zit.: Taschenbuch der Informatik – Bearbeiter, Kap., S.

Schönke, Adolf/Schröder, Horst
Strafgesetzbuch, 26. Auflage, München, 2001
Online: http://beck-gross.digibib.net/bib/home.asp
zit.: Sch/Sch – Bearbeiter § Rn

Schricker, Gerhard
Urheberrecht – Kommentar, 2. Auflage, 1999
zit.: Schricker – Bearbeiter § Rn

Schroeder, Friedrich-Christian
Pornographie, Jugendschutz und Kunstfreiheit, Heidelberg, 1992

Die Revolution des Sexualstrafrechts 1992-1998, JZ 1999, 827-833

Das 27. Strafrechtsänderungsgesetz – Kinderpornographie, NJW 1993, 2581-2583

Strafprozessrecht, 3. Auflage, München, 2001

Schroth, Ulrich/Schneider, Jochen
Probleme der Sichtung von Datenträgern vor Ort, CR 1992, 173-175

Schulze-Heimig, Ingeborg
Der strafrechtliche Schutz der Computerdaten gegen die Angriffsformen der Spionage, Sabotage und des Zeitdiebstahls, Münster 1995, zugl. Univ. Diss., Münster, 1994

Schwarz, Mathias
Urheberrecht und unkörperliche Verbreitung multimedialer Werke, GRUR 1996, 836-842

Seidl-Hohenveldern, Ignaz/Stein, Torsten
Völkerrecht, 10. Auflage, München, 2000

Shannon, Claude Elwood/Weaver, Warren
The mathematical theory of communication, 1949, Urbana, Illinois
http://cm.bell-labs.com/cm/ms/what/shannonday/paper.html (01.04.2004)

Sieber, Ulrich

Computerkriminalität und Strafrecht, Köln, 1977, 2., um einen Nachtrag ergänzte Auflage, 1980

Informationsrecht und Recht der Informationstechnik, NJW 1989, 2569-2580

The International Emergence of Criminal Information Law, Köln, 1992

Mißbrauch der Informationstechnik und Informationsstrafrecht – Entwicklungstendenzen in der internationalen Informations- und Risikogesellschaft, ursprünglich CR 1995, 100ff., aktualisierte und ergänzte Fassung unter: http://www.jura.uni-muenchen.de/sieber/article/mitis/Com_tu32.htm (01.04.2004)

Strafrechtliche Verantwortlichkeit für den Datenverkehr in internationalen Computernetzen, JZ 1996, 429-442; 494-507

Sieg, Rainer

Strafrechtlicher Schutz gegen Computerkriminalität, Jura 1986, 352-363

Sondermann, Markus

Computerkriminalität – Die neuen Tatbestände der Datenveränderung gem. § 303a StGB und der Computersabotage gem. § 303b StGB, Münster, Univ. Diss., 1989

Spahn, Andreas Guido

Wegnahme und Missbrauch codierter Scheckkarten nach altem und neuem Recht, Jura 1989, 513-520

Stenger, Hans-Jürgen

Mailboxen – Problem der Beweissicherung im Strafsachen, CR 1990, 786-794

Straus, Joseph

Der Schutz der ausübenden Künstler und das Rom Abkommen von 1961 – Eine retrospektive Betrachtung, GRUR Int. 1985, 19-29

Systematischer Kommentar zum Strafgesetzbuch

siehe Rudolphi, Hans-Joachim

Systematischer Kommentar Strafprozessordnung und Gerichtsverfassungsgesetz

siehe Rudolphi, Hans-Joachim

Tiedemann, Klaus

Wirtschaftsstrafrecht und Wirtschaftskriminalität, Allgemeiner und Besonderer Teil, Hamburg, 1976

Computerkriminalität und Missbrauch von Bankomaten, WM 1983, 1326-1331

Tröndle, Herbert/Fischer, Thomas

Strafgesetzbuch und Nebengesetze, 51. Auflage, München, 2003

Vogel, Markus

Distributed Denial-of-Service (DoS): Vorgehen und Gegenmaßnahmen, Seminararbeit an der Ruhr Universität Bochum, 2000
http://www.etdv.ruhr-uni-bochum.de/dv/lehre/seminar/ddos/ddos.pdf (01.04.2004)
zit: Vogel, DDoS, [Kapitel], S.

Vogler, Theo

Die strafrechtlichen Konventionen des Europarats, JURA 1992, 586-593

Vossbein, Jörn/Vossbein, Reinhard

Lagebericht zur IT-Sicherheit (Teil 1 und 2), KES 2002 Nr. 3 und 4,
http://www.kes.info/studie2002/index.htm (01.04.2004)

Walther
Zur Anwendbarkeit der Vorschriften des strafrechtlichen Jugendmedienschutzes auf im Bildschirmtext verbreitete Mitteilungen, NStZ 1990, 523-526

Weber, Hellmuth von
Die strafrechtliche Bedeutung der europäischen Menschenrechtskonvention ZStW 1953 (Band 65), 334-350

Weber, Ulrich
Der strafrechtliche Schutz des Urheberrechts, Tübingen, Habil.-Schrift, 1976

Weck, Gerhard
Datensicherheit: Methoden, Maßnahmen und Auswirkungen, Stuttgart, 1984

Welp, Jürgen
Die strafprozessuale Überwachung des Post- und Fernmeldeverkehrs, Heidelberg, 1974

Datenveränderung (§ 303a StGB), IuR 1988, 443-449, Sonderheft 1988, 434-439

Strafrechtliche Aspekte der digitalen Bildbearbeitung (I), CR 1992, 291-296

Strafprozessualer Zugriff auf Verbindungsdaten des Fernmeldeverkehrs, NStZ 1994, 209-215

Verbindungsdaten – Zur Reform des Auskunftsrechts (§§ 100g, 100h StPO), GA 2002, 535-556

Wessels, Johannes/Hettinger, Michael
Strafrecht – Besonderer Teil/1, 26. Auflage, Heidelberg 2002

Wessels, Johannes/Hillenkamp, Thomas
Strafrecht – Besonderer Teil/2, 25. Auflage, Heidelberg 2002

Wilhelm, H.
Beschlagnahme von Gegenständen, die einem Rechtsanwalt (Verteidiger) von seinem Mandanten übergeben sind, NJW 1959, 1716-1717

Winkelbauer, Wolfgang
Computerkriminalität und Strafrecht, CuR 1985, 40-44

Wolf, Stefan/Häger, Dirk/ Schorn, Heine
Erkennung und Behandlung von Angriffen aus dem Internet, Themenschwerpunkt des BSI auf der CeBIT 1999, http://www.bsi.de/literat/tagung/cebit99/index.htm (01.04.2004)
zit.: Wolf/Häger/Schorn, [Kapitelnummer]

Wolffgang, Hans-Michael
AWR-Kommentar, Köln, Loseblattausgabe (Stand: 2. Ergänzungslieferung 2002)