

Computerstrafrecht im Rechtsvergleich - Deutschland, Österreich, Schweiz

Von

Daniel Schuh



Duncker & Humblot • Berlin

Inhaltsverzeichnis

A. Einleitung	21
I. Problemstellung	21
II. Zielsetzung und Gang der Untersuchung	24
1. Zielsetzung	24
2. Gang der Untersuchung	25
B. Computerkriminalität und Internetkriminalität	28
I. Definitionen	28
II. Überblick über die Entwicklung des Computerstrafrechts in Deutsch- land, Österreich und der Schweiz	29
1. Deutschland	29
2. Österreich	32
3. Schweiz	33
C. Internationale Rechtsinstrumente	35
I. Die Cybercrime Convention	35
1. Entstehungsgeschichte	35
2. Rechtscharakter und Inkrafttreten im nationalen Recht	37
3. Grundlagen der Umsetzung	38
4. Ziele	38
a) Harmonisierung der materiell-strafrechtlichen Vorschriften	39
b) Schaffung gemeinsamer strafprozessualer Maßnahmen	39
c) Verbesserung der länderübergreifenden Kooperation	40
5. Aufbau und Regelungsgehalt	40
6. Kritikpunkte	40
a) Datenschutz	40
b) Intransparente Entstehung	43
7. Zusatzprotokoll	43
II. Der EU-Rahmenbeschluss	44
1. Entstehungsgeschichte	44
2. Rechtscharakter	45
3. Ziele	45
4. Aufbau und Regelungsgehalt	46
5. Ein Vergleich der Cybercrime Convention mit dem EU-Rahmen- beschluss	46

D. Das 41. Strafrechtsänderungsgesetz - Überblick über die Änderungen und Vergleich mit der Cybercrime Convention und dem EU-Rahmenbeschluss	49
I. Das Ausspähen von Daten, § 202a dStGB	49
1. Synopse	49
2. Änderungen	50
a) Geschütztes Rechtsgut	50
b) Zugangverschaffen	50
c) Überwinden einer besonderen Sicherung	51
3. Vergleich mit der Cybercrime Convention und dem EU-Rahmenbeschluss	52
a) Schutzobjekt	52
b) Überwinden der Zugangssicherung	54
II. Das Abfangen von Daten, § 202b dStGB	55
1. Gesetzestext	55
2. Ratio des § 202b dStGB	55
3. Vergleich mit der Cybercrime Convention	55
a) Daten im Sinne des § 202b dStGB und Computerdaten gemäß Art. 1 lit. b Cybercrime Convention	56
b) Datenübermittlung gemäß § 202b dStGB und Computerdatenübermittlung im Sinne der Cybercrime Convention	59
c) Abstrahlung einer Datenverarbeitungsanlage gemäß § 202b dStGB und Abstrahlung aus einem Computersystem im Sinne der Cybercrime Convention	59
III. Das Vorbereiten des Ausspähens und Abfangens von Daten, § 202c dStGB	60
1. Gesetzestext	60
2. Bisherige Rechtslage	60
3. Vergleich mit der Cybercrime Convention	61
a) Unterschiede im Hinblick auf den objektiven Tatbestand	61
b) Unterschiede im Hinblick auf den subjektiven Tatbestand	66
IV. Die Datenveränderung, § 303a dStGB	67
1. Synopse	67
2. Neuregelung	67
3. Vergleich mit der Cybercrime Convention und dem EU-Rahmenbeschluss	67
V. Die Computersabotage, § 303b dStGB	68
1. Synopse	68
2. Änderungen	69
a) Erweiterung auf Privatpersonen	69
b) Tathandlungen im Rahmen des § 303b Abs. 1 Nr. 2 dStGB	70
c) Nachteilszufügungsabsicht	70
d) Benannte Strafzumessungsregeln in § 303b Abs. 4 dStGB	71
e) Vorbereitungshandlungen	72

3. Vergleich von § 303b dStGB mit der Cybercrime Convention und dem EU-Rahmenbeschluss.	72
a) Datenverarbeitung von wesentlicher Bedeutung (§ 303b dStGB) - Betrieb eines Computersystems (Art. 5 Cybercrime Convention) bzw. Informationssystems (Art. 3 EU-Rahmenbeschluss)..	72
b) Erhebliche Störung (§ 303b dStGB) - Schwere Behinderung (Cybercrime Convention und EU-Rahmenbeschluss).	73
c) Nachteilszufügungsabsicht im Sinne des § 303b Abs. 1 Nr. 2 dStGB.	73
E. Die Umsetzung der Cybercrime Convention und des EU-Rahmenbeschlusses in Österreich durch die Strafrechtsänderungsgesetze 2002 und 2008.	75
I. Widerrechtlicher Zugriff auf ein Computersystem, § 118a öStGB.	75
1. Gesetzestext.	75
2. Vergleich mit der Cybercrime Convention und dem EU-Rahmenbeschluss.	76
a) Computersystem	76
b) Überwinden der Zugangssicherung	76
c) Überschießende Innentendenz	76
3. Vergleich mit § 202a dStGB.	78
a) Geschütztes Rechtsgut	78
b) Objektiver Tatbestand.	79
c) Subjektiver Tatbestand.	83
d) Mitgliedschaft in einer kriminellen Vereinigung, § 118a Abs. 3 öStGB.	84
II. Verletzung des Telekommunikationsgeheimnisses, § 119 öStGB.	85
1. Synopse.	86
2. Änderungen.	86
3. Vergleich des § 119 öStGB mit Art. 3 Cybercrime Convention	87
4. Vergleich des § 119 öStGB mit § 202b dStGB.	87
a) Geschütztes Rechtsgut	87
b) Objektiver Tatbestand.	88
c) Subjektiver Tatbestand.	91
III. Missbräuchliches Abfangen von Daten, § 119a öStGB.	92
1. Gesetzestext.	92
2. Vergleich mit der Cybercrime Convention.	93
3. Vergleich mit § 202b dStGB.	95
a) Geschütztes Rechtsgut	95
b) Objektiver Tatbestand.	95
c) Subjektiver Tatbestand.	97
IV. Missbrauch von Tonband- oder Abhörgeräten, § 120 Abs. 2a öStGB	98
1. Gesetzestext.	98
2. Anwendungsbereich.	98

3. Vergleich mit Art. 3 Cybercrime Convention	99
4. Vergleich mit § 202b dStGB	99
a) Geschütztes Rechtsgut	99
b) Objektiver Tatbestand	100
c) Subjektiver Tatbestand	103
V. Datenbeschädigung, § 126a ÖStGB	103
1. Gesetzestext	103
2. Vergleich mit der Cybercrime Convention und dem EU-Rahmen- beschluss	103
3. Vergleich des § 126a Abs. 1 öStGB mit § 303a dStGB.	104
a) Geschütztes Rechtsgut	104
b) Objektiver Tatbestand	105
c) Subjektiver Tatbestand	106
d) Deliktscharakter	106
4. Vergleich des § 126a Abs. 2 mit §§ 303a, 303b Abs. 1 Nr. 1,2 i.V.m. Abs. 4 S. 2 Nr. 1 und 2 dStGB	107
a) Objektiver Tatbestand	107
b) Subjektiver Tatbestand	110
VI. Störung der Funktionsfähigkeit eines Computersystems, § 126b ÖStGB	111
1. Gesetzestext	111
2. Vergleich mit der Cybercrime Convention und dem EU-Rahmen- beschluss	112
3. Vergleich von § 126b öStGB mit § 303b Abs. 1 Nr. 2 dStGB.	113
a) Geschütztes Rechtsgut	113
b) Objektiver Tatbestand	114
c) Subjektiver Tatbestand	122
VII. Missbrauch von Computerprogrammen oder Zugangsdaten, § 126c ÖStGB	123
1. Gesetzestext	123
2. Vergleich von § 126c öStGB mit Art. 6 Cybercrime Convention ...	124
3. Vergleich von § 126c öStGB mit § 202c dStGB.	127
a) Geschütztes Rechtsgut und Gesetzessystematik	127
b) Deliktscharakter	127
c) Objektiver Tatbestand	129
aa) Computerprogramme und vergleichbare Vorrichtungen gemäß § 126c öStGB - Computerprogramme gemäß § 202c dStGB	129
bb) Besondere Beschaffenheit gemäß § 126c ÖStGB - Zweck gemäß § 202c dStGB	130
cc) Computerpasswort, Zugangscode und vergleichbare Daten gemäß § 126c Abs. 1 Nr. 2 öStGB - Passwörter und sonst- ige Sicherungscodes gemäß § 202c Abs. 1 Nr. 1 dStGB ...	131

d) Subjektiver Tatbestand	134
e) Tatige Reue	138
f) Strafbarkeit des Versuchs und Rucktritt	140
F. Die Strafbarkeit der Computerkriminalitat in der Schweiz	141
I. Unbefugte Datenbeschaffung gema Art. 143 sStGB	141
1. Gesetzestext	141
2. Geschutztes Rechtsgut	142
3. Vergleich von Art. 143 sStGB mit Art. 3 Cybercrime Convention und daraus resultierender Umsetzungsbedarf	143
a) Objektiver Tatbestand	143
b) Subjektiver Tatbestand	147
4. Vergleich von Art. 143 sStGB und § 202a dStGB	147
a) Objektiver Tatbestand	147
b) Subjektiver Tatbestand	150
5. Vergleich von Art. 143 sStGB mit § 202b dStGB	150
a) Objektiver Tatbestand	150
b) Subjektiver Tatbestand	153
6. Vorschlag der Information Security Society Switzerland zur Anderung des Art. 143 sStGB	153
7. Eigener Vorschlag zur Umsetzung der Cybercrime Convention	155
II. Unbefugtes Eindringen in ein Datenverarbeitungssystem gema Art. 143 ^{bis} sStGB	156
1. Gesetzestext	156
2. Geschutztes Rechtsgut, gesetzessystematische Stellung und Delikts- charakter	156
a) Geschutztes Rechtsgut	156
b) Gesetzessystematische Stellung	157
c) Deliktscharakter	157
3. Vergleich des Art. 143 ^{bis} sStGB mit Art. 2 Cybercrime Convention und daraus resultierender Umsetzungsbedarf	158
a) Objektiver Tatbestand	158
b) Subjektiver Tatbestand	160
4. Vergleich von Art. 143 ^{bis} sStGB mit § 202a dStGB	160
a) Gesetzessystematische Stellung	160
b) Deliktscharakter	161
c) Objektiver Tatbestand	162
d) Subjektiver Tatbestand	164
5. Vorschlag des Eidgenossischen Justiz- und Polizeidepartements	165
6. Vorschlag der Information Security Society Switzerland	167
7. Eigener Vorschlag zur Umsetzung der Cybercrime Convention	168
• III. Datenbeschadigung gema Art. 144 ^{bis} sStGB	168
1. Gesetzestext	169

2. Geschütztes Rechtsgut	169
3. Deliktscharakter	170
4. Vergleich mit der Cybercrime Convention und daraus resultierenden Umsetzungsbedarf	170
5. Vergleich des Art. 144 ^{bis} Ziff. 1 sStGB mit §§ 303a Abs. 1, 303b Abs. 1, 2i. V.m. 4 S. 2 Nr. 1 dStGB	174
a) Geschütztes Rechtsgut	174
b) Tatbestand	175
aa) Objektiver Tatbestand	175
bb) Subjektiver Tatbestand	176
c) Fakultative Qualifikation	176
6. Vergleich des Art. 144 ^{bis} Ziff. 2 sStGB mit §§ 303a Abs. 3 i. V.m. 202c Abs. 1 Nr. 2 dStGB	179
a) Deliktscharakter	179
b) Tatbestand	179
aa) Objektiver Tatbestand	179
bb) Subjektiver Tatbestand	183
c) Qualifikation	185
d) Tätige Reue	185
7. Vorschlag der Information Security Society Switzerland	186
a) Datenbeschädigung, Art. 144 ^{bis} sStGB	186
b) Unbefugtes Eindringen in eine Datenverarbeitungseinrichtung, Art. 143 ^{bis} sStGB	187
8. Eigener Vorschlag zur Umsetzung der Cybercrime Convention	188
a) Vorbereiten einer Computerstraftat, Art. 143 ^{ter} sStGB	188
b) Datenbeschädigung, Art. 144 ^{bis} sStGB	189
c) Computersabotage, Art. 144 ^{ter} sStGB	189
G. Unterschiede zwischen den jeweiligen Regelungen - Ein Vergleich anhand ausgewählter Beispiele	191
I. Computerspionage durch Auswertung von Hardware	191
II. Hacking	194
1. Formen des Hackings	195
2. Beispiele	196
a) NASA - Hack	196
b) KGB - Hack	196
3. Strafbarkeit des Hackings	197
a) Ping-, Port-Scans und Traceroute	197
b) Trojanische Pferde	197
aa) Funktionsweise	197
bb) Strafbarkeit	198
(1) Deutschland	198
(2) Österreich	199

(3) Schweiz	201
(4) Zusammenfassendes Ergebnis	202
c) Backdoors	203
aa) Funktionsweise	203
bb) Strafbarkeit des Nutzens von Backdoors	203
(1) Deutschland	203
(2) Österreich	204
(3) Schweiz	205
(4) Zusammenfassendes Ergebnis	206
cc) Strafbarkeit des Öffnens von Backdoors	206
d) Masquerading und IP-Spoofing	207
III. Computersabotage	209
1. DoS-Attacken	209
a) Funktionsweise	209
b) Strafbarkeit	211
aa) Deutschland	211
bb) Österreich	213
cc) Schweiz	214
dd) Zusammenfassendes Ergebnis	215
2. Computerviren	216
a) Funktionsweise	216
b) Beispiele	217
c) Strafbarkeit	218
aa) Deutschland	218
bb) Österreich	219
cc) Schweiz	220
dd) Zusammenfassendes Ergebnis	220
3. Computerwürmer	221
a) Funktionsweise	221
b) Beispiele	221
c) Strafbarkeit	223
aa) Deutschland	223
bb) Österreich	224
cc) Schweiz	225
dd) Zusammenfassendes Ergebnis	226
IV. Spammails	227
1. Vorgehensweise	227
2. Strafbarkeit	228
V. Phishing	230
1. Entwicklungsgeschichte des Phishings	230
2. Vorgehensweise	231
3. Vermeidbarkeit	232

4. Strafbarkeit	233
a) Deutschland	233
aa) Verschaffen der Zugangsdaten	233
bb) Verschaffen des Zugangs zum Onlineaccount	234
b) Österreich	236
aa) Verschaffen der Zugangsdaten	236
bb) Verschaffen des Zugangs zum Onlineaccount	236
c) Schweiz	237
d) Zusammenfassendes Ergebnis	237
VI. Schwarzsurfen	238
1. Funktionsweise des WLAN und Vorgehensweise der Schwarzsurfer	238
2. Unterbindungsmöglichkeiten	239
a) WEP- und WPA-Verschlüsselung	239
b) Mac-Filtertabelle	239
c) Unterbindung der SSID-Ausstrahlung	240
d) Deaktivierung der DHCP-Funktion	240
3. Strafbarkeit	240
a) Deutschland	240
b) Österreich	242
c) Schweiz	242
d) Zusammenfassendes Ergebnis	243
H. Änderungsvorschläge	244
I. Änderung des § 202a dStGB	244
II. Änderung des § 202b dStGB	245
III. Änderung des § 202c dStGB	246
IV. Änderung des § 303a dStGB	248
V. Änderung des § 303b dStGB	248
I. Zusammenfassung der Thesen	250
Anhang - Gesetzestexte	253
I. Deutschland	253
1. Ausspähen von Daten, § 202a dStGB	253
2. Abfangen von Daten, § 202b dStGB	253
3. Vorbereiten des Ausspähens und Abfangens von Daten, § 202c dStGB	253
4. Datenveränderung, § 303a dStGB	254
5. Computersabotage, § 303b dStGB	254
II. Österreich	254
1. Widerrechtlicher Zugriff auf ein Computersystem, § 118a öStGB ..	254
2. Verletzung des Telekommunikationsgeheimnisses, § 119 öStGB	255
3. Missbräuchliches Abfangen von Daten, § 119a öStGB	255
4. Mißbrauch von Tonaufnahme- oder Abhörgeräten, § 120 öStGB ...	255
5. Datenbeschädigung, § 126a öStGB	256

6. Störung der Funktionsfähigkeit eines Computersystems, § 126b ÖStGB	256
7. Missbrauch von Computerprogrammen oder Zugangsdaten, § 126c öStGB	257
III. Schweiz	257
1. Unbefugte Datenbeschaffung, Art. 143 sStGB	257
2. Unbefugtes Eindringen in ein Datenverarbeitungssystem, Art. 143 ^{bis} sStGB	257
3. Datenbeschädigung, Art. 144 ^{bis} sStGB	258
IV. Auszug aus der Cybercrime Convention	258
V. EU-Rahmenbeschluss 2005/222/JI	262
Literaturverzeichnis	270
Sachregister	281