

# Computerstrafrecht im Rechtsvergleich – Deutschland, Österreich, Schweiz

Von

Daniel Schuh



Duncker & Humblot · Berlin

## Inhaltsübersicht

<b>A. Einleitung</b> .....	21
I. Problemstellung .....	21
II. Zielsetzung und Gang der Untersuchung .....	24
<b>B. Computerkriminalität und Internetkriminalität</b> .....	28
I. Definitionen .....	28
II. Überblick über die Entwicklung des Computerstrafrechts in Deutschland, Österreich und der Schweiz .....	29
<b>C. Internationale Rechtsinstrumente</b> .....	35
I. Die Cybercrime Convention .....	35
II. Der EU-Rahmenbeschluss .....	44
<b>D. Das 41. Strafrechtsänderungsgesetz – Überblick über die Änderungen und Vergleich mit der Cybercrime Convention und dem EU-Rahmenbeschluss</b> .....	49
I. Das Ausspähen von Daten, § 202a dStGB .....	49
II. Das Abfangen von Daten, § 202b dStGB .....	55
III. Das Vorbereiten des Ausspähens und Abfangens von Daten, § 202c dStGB .....	60
IV. Die Datenveränderung, § 303a dStGB .....	67
V. Die Computersabotage, § 303b dStGB .....	68
<b>E. Die Umsetzung der Cybercrime Convention und des EU-Rahmenbeschlusses in Österreich durch die Strafrechtsänderungsgesetze 2002 und 2008</b> .....	75
I. Widerrechtlicher Zugriff auf ein Computersystem, § 118a öStGB .....	75
II. Verletzung des Telekommunikationsgeheimnisses, § 119 öStGB .....	85
III. Missbräuchliches Abfangen von Daten, § 119a öStGB .....	92
IV. Missbrauch von Tonband- oder Abhörgeräten, § 120 Abs. 2a öStGB .....	98
V. Datenbeschädigung, § 126a öStGB .....	103
VI. Störung der Funktionsfähigkeit eines Computersystems, § 126b öStGB .....	111
VII. Missbrauch von Computerprogrammen oder Zugangsdaten, § 126c öStGB .....	123
<b>F. Die Strafbarkeit der Computerkriminalität in der Schweiz</b> .....	141
I. Unbefugte Datenbeschaffung gemäß Art. 143 sStGB .....	141
II. Unbefugtes Eindringen in ein Datenverarbeitungssystem gemäß Art. 143 <sup>bis</sup> sStGB .....	156
III. Datenbeschädigung gemäß Art. 144 <sup>bis</sup> sStGB .....	168

<b>G. Unterschiede zwischen den jeweiligen Regelungen – Ein Vergleich anhand ausgewählter Beispiele</b> .....	191
I. Computerspionage durch Auswertung von Hardware.....	191
II. Hacking.....	194
III. Computersabotage.....	209
IV. Spammails.....	227
V. Phishing.....	230
VI. Schwarzsurfen.....	238
<b>H. Änderungsvorschläge</b> .....	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
<b>I. Zusammenfassung der Thesen</b> .....	250
<b>Anhang – Gesetzestexte</b> .....	253
I. Deutschland.....	253
II. Österreich.....	254
III. Schweiz.....	257
IV. Auszug aus der Cybercrime Convention.....	258
V. EU-Rahmenbeschluss 2005/222/JI.....	262
<b>Literaturverzeichnis</b> .....	270
<b>Sachregister</b> .....	281