

Inhaltsverzeichnis

§ 1	Einleitung.....	15
§ 2	Entwicklung der Computerkriminalität und ihre strafrechtliche Verfolgung.....	21
A.	Erstes Auftauchen der Computerkriminalität in Deutschland	21
B.	Strafbarkeitslücken in der Bekämpfung der aufkommenden Computerkriminalität	22
C.	Ansichten innerhalb der Literatur bezüglich einzelner Deliktgruppen	25
I.	Computermanipulation.....	26
II.	Computerspionage.....	29
III.	Computersabotage.....	30
IV.	Zeitdiebstahl	32
V.	Urkundenfälschung	33
VI.	Zusammenfassung.....	33
D.	Gesetzgebungsgeschichte des 2. WiKG.....	34
I.	1. Phase: Diskussion des § 263 a und § 269 StGB	35
II.	2. Phase: Diskussion der Straftatbestände gegen Computerspionage und Computersabotage	40
III.	Schlussphase: Gesetzgebung und deren Würdigung	43
E.	Nach dem Inkrafttreten des 2. WiKG erlassene Straftatbestände mit Bezug auf die Computerkriminalität.....	45
I.	§§ 263 a Abs. 2 i.V.m. 263 Abs. 2 bis 7 StGB	45
II.	§§ 269 Abs. 3 i.V.m. 267 Abs. 3 und 4 StGB.....	46
III.	Urheberrechtsnovelle	47
F.	Internetkriminalität.....	48

G.	Kriminalitätsentwicklung.....	50
I.	Kriminalstatistik 1998.....	51
II.	Verlauf der Kriminalstatistiken 1987 - 1998	52
III.	Dunkelfeld.....	53
H.	Polizeiliche Strafverfolgung und strafprozessuale Eingriffsbefugnisse.....	58
§ 3	Weitergehende Kriminalisierung.....	63
A.	Erstellen von Computerviren.....	63
I.	Entwicklung und Gefahrenpotential der Computerviren.....	63
II.	Strafbarkeit der Programmierung von Computerviren	67
III.	Schlußfolgerung	71
B.	Datenhehlerei.....	72
C.	Fahrlässigkeitsstrafbarkeit.....	73
D.	Computererpressung und sonstige Delikte.....	74
§ 4	Status quo in der Informationstechnologie.....	77
A.	Sicherheit in der Informationstechnologie	77
B.	Informationstechnik als Teil der Risikogesellschaft	81
C.	Zukünftige Grundlagen eines Informationsstrafrechts.....	83
I.	Schutz des Eigentümers oder Besitzers	86
II.	Schutz des Betroffenen.....	88
III.	Informationszugangsrechte	90
IV.	Zusammenfassung.....	92

§ 5	Prävention von Computerkriminalität	95
A.	Strafrecht als "ultima ratio"	95
I.	Verzicht auf Strafrecht	96
II.	Schutz durch Strafrecht	97
	1. Relativierung des Grundsatzes der Subsidiarität wegen Beschränkung der Wirtschaftsfreiheit	97
	2. Steigende Kriminalitätsrate keine Begründung für verstärkten Einsatz des Strafrechts	99
III.	Kompromiß	100
B.	Soziale Kontrollmechanismen und technischer Selbstschutz	102
I.	Selbstregulierung	103
II.	Filter auf Seiten des Access-Providers	107
III.	Filterprogramme auf Seiten des Anwenders	107
IV.	Altersprüfsysteme	108
V.	Netiquette	109
VI.	Schlußfolgerung	109
C.	Kryptographie, Steganographie und Biometrie als Schutz des Rechtsguts des § 202 a StGB	110
I.	Rechtsgut des § 202 a StGB	111
II.	Tatbestandsmerkmal "besonders gesichert"	115
III.	Kryptographie	120
	1. Darstellung der Kryptographie	120
	2. Kryptokontroverse	123
	a) Bedrohung der ungehinderten Kommunikation ..	123
	b) Rechtliche Grundlagen für den Schutz der Kommunikation	125
	c) Lösung der Kontroverse	127
	d) Internationale Regelungen	131
	3. Kompromittierende Abstrahlung	134
IV.	Steganographie	135
V.	Biometrie	137

VI.	Schlußfolgerung	139
D.	Sicherungsmaßnahmen als Schutz der Rechtsgüter der §§ 303 a und 303 b StGB	140
I.	Rechtsgut des § 303 a StGB.....	140
II.	Rechtsgut des § 303 b StGB.....	142
III.	Sicherungsmaßnahmen.....	142
IV.	Zivilrechtliche Haftung für Datenlöschung, Datenverlust und Datenzerstörung.....	148
V.	Schlußfolgerung	150
E.	Digitale Signatur als Schutz des Rechtsguts des § 269 StGB.....	151
I.	Rechtsgut des § 269 StGB.....	151
II.	Zweck digitaler Signaturen	151
III.	Schutz des Rechtsguts des § 269 StGB durch digitale Signaturen.....	153
IV.	Schlußfolgerung	154
F.	Wirtschaftsrechtliche Präventivmaßnahmen.....	154
I.	Vorschreiben von technischen Sicherheitsmaßnahmen durch den Gesetzgeber	155
II.	Schaffen einer Anzeigepflicht.....	159
III.	Schlußfolgerung	161
§ 6	Schlußbetrachtung: Präventivmaßnahmen als ausreichende Möglichkeit der Eindämmung	163
§ 7	Literaturverzeichnis	167