

Inhaltsübersicht

Teil 1

Rechtliche und technische Hinführung 19

A. Einführung und Gang der Arbeit.....	19
I. Informationskriminalität und § 202a – kriminologischer Anriss	19
II. Gang der Arbeit.....	24
B. Derzeitiges Verständnis des § 202a StGB	26
I. Rechtsgut des § 202a StGB	27
II. Rechtsgutsträger.....	60
III. Tatobjekt Daten	70
IV. Bestimmung der Daten.....	85
V. Tathandlung: Ausspähen von/Verschaffen des Zugangs zu Daten	89
VI. Besondere Sicherung – Auslegung nach dem derzeitigen Verständnis...	96
C. Phänomenologie der Ausspähtechniken – Das Wechselspiel von Angriff und Abwehr	103
I. Tätergruppen und Tatmotive.....	104
II. Exemplarische Ausspähtechniken/-werkzeuge	108

Teil 2

Begründung des Tatbestandsmerkmals der besonderen Sicherung 160

A. Besondere Sicherung als Dokumentation des besonderen Sicherungs- interesses	164
I. Allgemeine sozialpsychologische Erkenntnisse zur Privatheit und Sicherung.....	165
II. Herrschende Behauptung einer sicherungsinhärenten Dokumentation eines besonderen Geheimhaltebedürfnisses.....	179
III. Zwischenschluss und Fortgang der Untersuchung.....	264
IV. Untersuchung weiterer Sicherungsmittel	267
V. Ergebnis.....	319
B. Viktimodogmatik als Begründungsmodus	321
I. Allgemeine Darlegung und Kritik der Viktimodogmatik.....	321
II. Gesetzgeberische Motivlage der Alt- und Neufassung des § 202a StGB	327

III. Auswertung der Literatur zu § 202a StGB und zur Viktimodogmatik – besondere Thesen	332
IV. Abschließende Stellungnahme zur viktimodogmatischen Fundierung des § 202a StGB.....	355
C. Erhöhung des Handlungsunrechts, Vertiefung der Rechtsgutsverletzung oder Prävention als denkbare Begründungsmodi	357
I. Vergleich der Merkmale der besonderen Sicherungen in § 123 Abs. 1, § 202 Abs. 1, 2 und § 243 Abs. 1 S. 2 Nr. 1, 2 mit denen des § 202a ..	358
II. Erhöhung des Handlungsunrechts.....	365
III. Vertiefung der Rechtsgutsverletzung wegen der Sicherung des Rechtsguts.....	367
IV. Prävention.....	369
D. Schluss	387
Literaturverzeichnis	389
Sachwortverzeichnis	423

Inhaltsverzeichnis

Teil 1

Rechtliche und technische Hinführung	19
A. Einführung und Gang der Arbeit.....	19
I. Informationskriminalität und § 202a – kriminologischer Anriß	19
II. Gang der Arbeit	24
B. Derzeitiges Verständnis des § 202a StGB	26
I. Rechtsgut des § 202a StGB	27
1. Rechtsgutsbegriff und Funktion	27
2. Ansichten zum Rechtsgut des § 202a StGB	30
a) Information	30
b) Vermögen	32
c) Materielles Geheimnis	33
d) Formelles Geheimnis	34
3. Stellungnahme.....	35
a) Wortlaut	37
(1) Vermögen	38
(2) Materielles Geheimnis.....	38
(3) Formelles Geheimnis.....	39
b) Historisch-systematische Auslegung	39
(1) Vermögen	40
(2) Materielles Geheimnis.....	43
(3) Formelles Geheimnis.....	44
c) Telos	45
(1) Verfassungskonforme Auslegung	46
(2) Strafandrohung	49
d) Ergebnis	49
4. Alternative rechtsgutsbestimmende Tatbestandseinschränkungen	54
a) Materielles Geheimnis – de lege ferenda.....	54
b) Sonstige Alternativen – de lege ferenda.....	57
II. Rechtsgutsträger.....	60
1. Nichtgeeignetheit sachenerrechtlicher Parallelen	61
2. Informationsspezifische Kriterien.....	62
a) Erstmalig Speichernder – Skribent	62
b) Geistiger Urheber	64

c) Derivativer Erwerber	66
d) Inhaber/Eigentümer des Datenträgers	67
e) Inhaltlich Betroffener	68
f) Ergebnis	70
III. Tatobjekt Daten	70
1. Der Datenbegriff als relativer Rechtsbegriff	71
2. Nicht-unmittelbare Wahrnehmbarkeit der gespeicherten Daten	73
a) Speicherarten	73
(1) Physische Wahrnehmbarkeit und Syntax	75
(2) Zwischenergebnis	77
b) Sonderprobleme	77
(1) Daten(fern)übertragung	78
(2) Sonderfall: Gruppenspezifische (Nicht-)Wahrnehmbarkeit	82
c) Zusammenfassung	84
IV. Bestimmung der Daten	85
1. Derzeitige Auffassung	85
2. Kritik an Einschränkungsversuchen im Hinblick auf kupierte Datenüberlassungen	86
3. Trennung von Zugangssicherung und Bestimmung	88
4. Relevanz von Zweck- und Nutzungsbestimmungen	88
5. Zusammenfassung	89
V. Tathandlung: Ausspähen von/Verschaffen des Zugangs zu Daten	89
1. Begehnungsweisen	89
2. Problem des Verschaffens verschlüsselter Daten	93
a) Problematik	93
b) Ergebnis	96
VI. Besondere Sicherung – Auslegung nach dem derzeitigen Verständnis	96
C. Phänomenologie der Ausspähtechniken – Das Wechselspiel von Angriff und Abwehr	103
I. Tätergruppen und Tatmotive	104
1. Tätergruppen	104
2. Tatmotive	106
II. Exemplarische Ausspähtechniken/-werkzeuge	108
1. „Klassischer“ und moderner Passwortdiebstahl	112
a) Begriffsklärung	112
b) Ablesen notierter Zugangsdaten	114
c) Social Engineering	114
d) Keylogging	116
e) Schlichtes Ausprobieren und Raten – Guessing	117
f) Brute-Force/Dictionary Attack	117
g) Rechtliche Wertung	118

2. Durch die technische Infrastruktur des Internet ermöglichte Techniken.....	120
a) Historie des Internet und ihre Auswirkungen auf die heutige Sicherheitsarchitektur	120
b) Phishing	126
c) Pharming	130
d) Nutzen von System„löchern“ (Exploiting).....	131
(1) Footprinting und Mapping	132
(2) Ping-Scanning	133
(3) Port-Scanning	133
(4) Rechtliche Wertung	135
e) Bots/Würmer.....	135
f) Trojanische Pferde.....	137
g) Spyware	141
(1) Technische Phänomenologie	141
(2) Rechtliche Wertung de lege lata.....	141
h) Dialer	144
i) Viren.....	144
j) Trapdoors und Backdoors	146
k) Ausnutzen transitiven Vertrauens.....	148
l) Man-in-the-Middle.....	149
m) Session Hijacking.....	152
3. Methoden der Tarnung	152
a) Masquerading	153
b) Spoofing	154
c) Rootkits	155
d) Rechtliche Wertung	156
4. Verknüpfung der Techniken.....	156
5. Zusammenfassung	157

*Teil 2***Begründung des Tatbestandsmerkmals
der besonderen Sicherung**

160

A. Besondere Sicherung als Dokumentation des besonderen Sicherungs- interesses	164
I. Allgemeine sozialpsychologische Erkenntnisse zur Privatheit und Sicherung	165
1. Information und Privatheit als Gegenstand strafrechtlichen Schutzes	166
2. Privatheit	168
3. Überblick über spezifische Erkenntnisse der Verhaltensforschung...	169
4. Herstellung und Sicherung von Privatheit	175
5. Ergebnis	178

II. Herrschende Behauptung einer sicherungsinhärenten Dokumentation eines besonderen Geheimhaltebedürfnisses	179
1. Wirkungsweise, Anwendung und Zielrichtung der Passwortabfrage ..	180
2. Meinungsstand zur besonderen Sicherung am Beispiel des Passwortes	184
a) Einzelne Literaturansichten	188
b) Zusammenfassung der herrschenden Meinung	212
3. Grundsätzliche Kritik an der Konzeption der herrschenden Meinung am Beispiel des Passwortes	216
a) Zwecke der Passwortabfrage	217
(1) Selbst Zugangsschutz bedeutet nicht zwingend Geheimnisschutz	217
(2) Schutz bedeutet nicht zwingend Zugangsschutz	219
(a) Betriebssystemebene	219
(b) Onlinedienste	222
(3) Passwortabfrage bedeutet Identifikation – jedoch nicht zwingend Schutz	223
b) Eindeutige Dokumentation braucht Handlungsalternativen	230
c) Unspezifischer Schutz lässt nicht auf spezifische Bedeutungen schließen	232
d) Zusammenfassung	236
4. Vergleich mit Sicherungen aus § 202 Abs. 1, 2, § 123 Abs. 1 und § 243 Abs. 1 S. 2 Nr. 1, 2 StGB.....	237
a) Sicherungen des § 202 StGB	238
(1) Überblick	238
(2) Einsatzzweck der Sicherung	239
(a) Verschluss	239
(b) Verschlossenes Behältnis	240
(3) Handlungsalternative	242
(a) Verschluss	242
(b) Verschlossenes Behältnis	242
(4) Spezifität	243
(5) Zusammenfassung	244
b) § 123 StGB – Die Befriedung	245
(1) Rechtsgut	245
(2) Begründung des Tatbestandsmerkmals	248
(3) Einsatzzweck der Sicherung	250
(4) Handlungsalternative	250
(5) Spezifität	251
(6) Zusammenfassung	251
c) Sicherungen der § 243 Abs. 1 S. 2 Nr. 1 und 2 StGB	253
(1) Wirkung des Merkmals, Regelbeispieltechnik	253
(2) Begründung des Regelbeispiels	253

(3) Einsatzzweck der Sicherung	256
(4) Handlungsalternative	258
(5) Spezifität	259
(6) Zwischenzusammenfassung	259
d) Zusammenfassung und Ergebnis	260
5. Vergleich mit § 244 Abs. 1 Nr. 3 – Wohnungseinbruchsdiebstahl	261
6. Absenz des Sicherungserfordernisses des § 202b StGB	263
III. Zwischenschluss und Fortgang der Untersuchung	264
IV. Untersuchung weiterer Sicherungsmittel	267
1. Firewall	269
a) Ziel, Wirkungsweise und Anwendung	269
b) Rechtliche Wertung	270
2. Antivirenprogramme (VirensScanner)	272
a) Ziel, Wirkungsweise und Anwendung	272
b) Rechtliche Wertung	276
3. Sogenannter Kopierschutz	277
4. Sonstige Sicherungsmaßnahmen im weiteren Sinne	280
5. Zwischenergebnis	281
6. Nicht-digitale physische Maßnahmen	282
7. Hindernisse gegenüber dem Auffinden und Verstehen – Krypto- und Steganographie	287
a) Einführung	287
b) Kurzglossar	287
c) Verschlüsselung und Verstecken – nicht nur historisch Verwandte	288
d) Alternativlosigkeit von Kryptographie und Steganographie bei der Kommunikation	292
e) Digitales Verstecken im Allgemeinen	295
(1) Ziel, Anwendungstechnik und Gegenmaßnahmen	295
(2) Rechtliche Wertung	297
f) Moderne Steganographie i.e.S.	299
(1) Ziel, Anwendungstechnik und Gegenmaßnahmen	299
(2) Rechtliche Wertung	301
g) Kryptographie	303
(1) Anwendungstechnik und Gegenmaßnahmen	304
(2) Rechtliche Wertung	309
(a) Schutz vor dem intellektuellen Zugang zu Daten	309
(b) Wertung nach der Dokumentationstheorie	313
h) Erhöhter Schutz durch Kombination von Zugangsschutz, Verschlüsselung und Täuschung	315
(1) Grundsatz	315
(2) Moderner kombinierter Schutz von Daten am Beispiel von TrueCrypt	315
V. Ergebnis	319

B. Viktimodogmatik als Begründungsmodus	321
I. Allgemeine Darlegung und Kritik der Viktimodogmatik	321
1. Kurze Einführung in die Viktimodogmatik	321
2. Allgemeine Thesen für und wider die Viktimodogmatik	324
II. Gesetzgeberische Motivlage der Alt- und Neufassung des § 202a StGB	327
1. § 202a StGB in der Fassung von 1986	327
2. § 202a StGB in der Fassung von 2007	331
III. Auswertung der Literatur zu § 202a StGB und zur Viktimodogmatik – besondere Thesen	332
1. Schwerpunktmaßig viktimodogmatische Literatur	333
a) Allenfalls bedingte Übertragung der Thesen zum Betrug auf § 202a StGB	333
b) Suche nach übertragbaren Thesen	336
(1) <i>Amelungs</i> Nennung der §§ 201 ff. StGB als aus viktimodogmatischer Perspektive betrachtbar	336
(2) <i>Schünemanns</i> Entwicklung der Viktimodogmatik	336
(3) <i>R. Hassemers</i> Unterscheidung von Beziehungs- und Zugriffsdelikten	336
(4) <i>Arzts</i> Tatbestandsrestriktionen, insb. bei Geheimnisschutzdelikten	338
(5) <i>Bleis</i> Problemverlagerung und monistische Interpretation des § 298 Abs. 1 Nr. 2 StGB a.F.	341
(6) Zwischenzusammenfassung	343
2. Literatur mit dem Fokus § 202a StGB	344
a) Regelmäßig bloße Nennung viktimodogmatischer Erwägungen ..	344
b) Schünemanns allgemeines und besonderes Eintreten für die Viktimodogmatik bei § 202a StGB	347
IV. Abschließende Stellungnahme zur viktimodogmatischen Fundierung des § 202a StGB	355
C. Erhöhung des Handlungsunrechts, Vertiefung der Rechtsgutsverletzung oder Prävention als denkbare Begründungsmodi	357
I. Vergleich der Merkmale der besonderen Sicherungen in § 123 Abs. 1, § 202 Abs. 1, 2 und § 243 Abs. 1 S. 2 Nr. 1, 2 mit denen des § 202a ..	358
1. Sicherungen des § 202 Abs. 1 und 2 StGB	359
2. Begründung der Befriedung des § 123 Abs. 1 StGB	360
3. Begründung der Regelbeispiele des § 243 Abs. 1 S. 2 Nr. 1 und 2 StGB	362
4. Zusammenfassung	363
II. Erhöhung des Handlungsunrechts	365
III. Vertiefung der Rechtsgutsverletzung wegen der Sicherung des Rechtsguts	367
IV. Prävention	369
1. Prävention als anerkannter Strafzweck	369

2. Bruch der Sicherung als Beweis der besonderen Gefährlichkeit des Täters	372
3. Vorverlagerung präventiver Strafzumessungserwägungen auf Tatbestandsebene	374
4. Systematische Passung der Begründung	377
a) Begründungskonkordanz von Bereichssicherungen	378
b) Widerspruchsfreiheit mit dem Nichterfordernis der Sicherung in § 202b und § 244 Abs. 1 Nr. 3 StGB	378
(1) § 202b StGB	378
(2) § 244 Abs. 1 Nr. 3 StGB	379
c) Kollisionsfreiheit mit § 243 Abs. 1 S. 2 Nr. 6 StGB	379
d) Zusammenfassung	382
5. Ausgewählte praktische Folgen	382
D. Schluss	387
Literaturverzeichnis	389
Sachwortverzeichnis	423