

Inhaltsverzeichnis

Einleitung	15
-------------------------	----

Teil I

Grundlagen und Begriffsbestimmungen	19
§ 1 Überblick zur Normgenese	19
A. Vorgeschichte	19
B. Normtext	21
C. Zu den Motiven der Gesetzgebung	21
D. Verfassungsbeschwerde	23
§ 2 Rechtsgut	24
A. Der Begriff des Rechtsguts	25
I. Die Ansätze in der Literatur	26
1. Systemimmanenter Rechtsgutsbegriff	26
2. Systemkritischer Rechtsgutsbegriff	27
3. Ablehnung des Rechtsgutsbegriffs	28
II. Rechtsgutsbegriff und Verfassung	28
III. Konsequenzen: Bedeutung des Rechtsgutsbegriffs für die vorliegende Arbeit	29
B. Methodik zur Bestimmung des Rechtsguts	31
I. Die „Achillesferse“ der rechtsgutsbezogenen Auslegung	32
II. Subjektive und objektive Auslegung	35
C. Zusammenfassung: Hermeneutisch-methodischer (systemimmanenter) Rechtsgutsbegriff	37
§ 3 Anschlussdelikt	39
§ 4 Daten, Informationen und Geheimnisse	41
A. Computer- und Datenstrafrecht	41
B. Der Begriff der Daten im StGB	43
C. Informationsbegriffe	44
D. Daten und Informationen in der Informatik	46
E. Schlussfolgerungen	47
I. Semantische, syntaktische und strukturelle Informationen	47
II. Daten i. S. d. Datenschutzrechts	49

III. Daten und Datenträger	51
1. Datenträger als „notwendige Lebensbedingung“	51
2. Verkörperung und digitale Daten	52
F. Zur Zuordnung von Daten und Geheimnissen	54
I. Einführung	54
II. Mögliche Anknüpfungspunkte für die Zuordnung von Daten	56
III. Die strafrechtliche Diskussion über die Zuordnung von Daten bei § 303a StGB	57
1. Zum Tatbestand der Datenveränderung	57
2. Zuordnungskriterien	58
3. Unbeachtlichkeit semantischer Aspekte	60
4. Rechte am Datenträger	61
5. Skripturaktstheorie	62
a) Strenge Skripturaktstheorie	63
b) Modifizierte Skripturaktstheorie	64
6. Wertungen des UrhG	64
7. Stellungnahme	65
IV. Zuordnung über den Zugang: Geheimnisse	66
1. Geheimnisschutz	66
a) Zum Begriff des Geheimnisses	67
b) Die von Geheimnisschutznormen geschützten Rechtsgüter und die Zuordnung von Geheimnissen	68
2. Formeller Geheimnisschutz (§ 202 StGB)	69

Teil 2

Der Rechtsgüterschutz der Datenhehlerei	71
§ 5 Rechtsgutsbezeichnungen in der Begründung des Gesetzentwurfs	71
§ 6 Formelles Datengeheimnis	72
A. Das „formelle Datengeheimnis“ bei §§ 202a, 202b, 202c StGB	72
I. Rechtsgüterschutz bei § 202a StGB (Ausspähen von Daten)	72
1. Überblick	72
2. Merkmale des „formellen Datengeheimnisses“	76
a) Besondere Sicherung und Überwindung der Sicherung	76
b) § 202a StGB als „elektronischer Hausfriedensbruch“	77
c) Europa- und völkerrechtliche Vorgaben und Rahmenbedingun- gen	79
3. Missverständliche Begrifflichkeiten im Schrifttum	81
a) „Recht am gedanklichen Inhalt“	81
b) „Besitz“	83

Inhaltsverzeichnis	11
c) Zugänglichkeit der Information	83
4. Rechtsgutsträger und „Verfügungsbefugnis“: Zuordnung der Daten bei § 202a StGB	84
a) Ansichten im Schrifttum	84
b) Stellungnahme: Zuordnung des Geheimbereichs	85
aa) Unterschied zur Situation bei § 303a StGB	85
bb) Situation bei § 202 StGB	87
cc) Übertragung auf § 202a StGB	90
(1) Keine notwendige Reihenfolge von Datenspeicherung und Sicherung	90
(2) Kriterien für die Zuordnung des Geheimbereichs	94
(3) Übermittlung	95
5. Fazit	95
II. Rechtsgüterschutz bei § 202b StGB (Abfangen von Daten)	97
III. Rechtsgüterschutz bei § 202c StGB (Vorbereiten des Ausspähens und Abfangens von Daten)	99
IV. Fazit und Schlussfolgerungen	100
B. Schutz „vor einer Aufrechterhaltung und Vertiefung“ der Verletzung: Perpetuierungstheorie	101
C. Formelles Datengeheimnis als Rechtsgut der Datenhehlerei?	102
I. Zum Tatbestand des § 202d Abs. 1 StGB	102
1. Anhaltspunkte für formellen Geheimnisschutz?	103
a) Merkmale formellen Geheimnisschutzes in anderen Normen	103
b) Daten, „die nicht allgemein zugänglich sind“	103
aa) Wortlaut	103
bb) Hinweise in den Gesetzesmaterialien	104
(1) Begründung in früheren Entwürfen	104
(2) Begründung des späteren Gesetzentwurfs	106
cc) Datenschutzrechtliches Begriffsverständnis	107
dd) Fazit	108
c) Tathandlungen	109
aa) Verschaffen, Überlassen, Zugänglichmachen	109
bb) Verbreiten	109
cc) Vergleich mit § 202c StGB	111
d) Bereicherungs- oder Schädigungsabsicht	112
e) Fazit	112
2. Anhaltspunkte für einen Perpetuierungstatbestand?	113
a) Vergleich mit § 259 StGB	113
aa) Vortat	113
bb) Tathandlungen	114
b) Loslösung von der Vortat	114

3. Fazit	115
II. Zur Stellung im Gesetz	115
III. Zum Konzept formellen Geheimnisschutzes durch das Anschlussdelikt	115
1. Zur Verletzung des formellen Datengeheimnisses durch die Vortat ..	116
a) Ausführungen und Beispiele in der Begründung	116
b) Überprüfung der Annahmen	117
2. Zur Perpetuierbarkeit einer Verletzung des formellen Datengeheimnisses durch die Vortat	120
a) Ausführungen in der Begründung des Gesetzentwurfs	120
b) Überprüfung der Annahmen	121
aa) Geheimbereich der Vortat	122
bb) Zuordnung der durch die Vortat erlangten Daten	125
(1) Verfügungsbefugter der Vortat?	125
(2) Zur Phänomenologie von Datenschwarzmärkten	127
(3) Schlussfolgerungen	129
(4) Vergleich mit § 202 StGB	130
(5) Verfügungsbefugnis des von der semantischen Information Betroffenen	131
3. Konsequenzen	132
a) Gesetzesmaterialien und „Wille des Gesetzgebers“	132
b) Kontextualisierung des Fehlers der Begründung des Gesetzentwurfs	135
aa) Anderweitige Ausführungen in der Begründung des Gesetzentwurfs	135
(1) Siebers Gutachten zum 69. DJT	135
(2) „Schutzlücken“ bei § 17 Abs. 2 UWG a.F. und § 44 i.V.m. § 43 Abs. 2 Nr. 1, 3 BDSG a.F.	136
bb) Anhaltspunkte in der Genese des Gesetzes	138
IV. Ergebnis	140
§ 7 Allgemeine Sicherheitsinteressen	140
A. Argumente für und gegen die Gefährlichkeitstheorie bei § 259 StGB	141
B. Situation bei § 202d StGB	142
I. Strafmaß	142
II. Bereicherungsabsicht	143
III. Antragsdelikt	143
IV. Argumente in der Begründung des Gesetzentwurfs	143
C. Konsequenzen	144
§ 8 Materielles Datengeheimnis	145
A. Zum Tatbestand des § 202d Abs. 1 StGB	146
I. Daten	147

Inhaltsverzeichnis	13
II. Nicht allgemein zugänglich	147
III. Vortäter	150
IV. Tathandlung des „Verbreitens“	150
V. Bereicherungs- oder Schädigungsabsicht	151
B. Weitergabe und Verbreitung semantischer Informationen als Unrecht	151
C. Zum Konzept materiellen Informationsschutzes durch das Anschlussdelikt	152
I. Verletzter und Geheimhaltungsinteresse	152
II. Bezug zur Vortat	154
1. Vortaten	154
2. Unmittelbarkeit, Datenkreationen, Ersatzhehlerei und „Sachidentität“	155
a) Datenkreationen	156
b) „Sachidentität“	159
aa) Zu Wortlaut und Systematik	159
bb) Zum „Schokoriegel“-Vergleich	161
D. Ergebnis: Die Datenhehlerei als materielles Geheimnisschutzdelikt	164
§ 9 Schluss	165
Literaturverzeichnis	167
Stichwortverzeichnis	190