

Inhaltsverzeichnis

Vorwort	V
Inhaltsübersicht	VII
Abkürzungsverzeichnis	XXIII

1

Ausgangssituation, Begrifflichkeiten und Rechtsentwicklung

I.	Einleitung, Gang der Untersuchung und Vorüberlegungen	1
A.	Gang der Untersuchung	6
B.	Die Omnipräsenz informationstechnischer Systeme	9
1.	Abstraktion und Repräsentation	9
2.	Digitalisierung und Automatisierung	10
3.	Universalität	11
4.	Virtualisierung, Ubiquität und immanente Transnationalität	12
5.	Entwicklungsdynamik durch Geschwindigkeit und Zunahme des Miniaturisierungsgrads	14
II.	Begriffe, Definitionsansätze, Abgrenzungen und Entwicklungen	15
A.	Zum Wesen und Begriff der »Computerkriminalität«	15
1.	Der Computer als End- oder Zwischenziel deliktischen Handelns	17
2.	Der eigene Definitionsansatz	19
3.	Täterorientierte Einteilung der Computerkriminalität	21
4.	Technik- und menschbezogene Typen der Computerkriminalität	23
5.	Computerkriminalität und Wirtschaftskriminalität	26
B.	Zum Begriff »Computerstrafrecht«	28
1.	»Computerstrafrecht im weiten Sinn«	31

2.	»Computerstrafrecht im engen Sinn«	32
3.	Vorfeldbereich und Kernbereich	35
4.	»Formelles Computerstrafrecht«	38
C.	Abgrenzungen und Sonderfälle	39
1.	Hardware-Angriffe	39
2.	»Zeitdiebstahl«	40
3.	»Software-Diebstahl«	40
D.	Überblick über die Entwicklung der Computerstrafrechtsdogmatik	41
1.	DSG 1978	41
2.	StRÄG 1987	44
3.	UrhG-Novelle 1993 und StGB-Novelle 1994	45
4.	TKG	46
5.	Notifikationsgesetz 1999	46
6.	DSG 2000	47
7.	ZuKG	49
8.	Cybercrime-Konvention des Europarates	49
9.	StRÄG 2002	51
10.	E-Commerce-Gesetz	52
11.	TKG 2003	52
12.	StRÄG 2004	53
13.	EU-Rahmenbeschluss über Angriffe auf Informationssysteme	53
14.	StRÄG 2008	54
15.	Zweites Gewaltschutzgesetz 2009	55
16.	DSG-Novelle 2010	55
17.	Strafgesetznovelle 2011	55
18.	Ratifikation der Cybercrime-Konvention	56
19.	Errichtung eines Europäischen Zentrums zur Bekämpfung der Cyberkriminalität	57
20.	Sexualstrafrechtsänderungsgesetz 2013	58
21.	Richtlinie 2013/40/EU über Angriffe auf Informationssysteme	58
22.	StRÄG 2015	60
E.	Datenbegriff im Strafrecht	60
1.	Daten in einem engen und weiten Verständnis	61
2.	Technischer Datenbegriff	66
3.	Problemfelder bezüglich des kernstrafrechtlichen Datenbegriffs	67

2**Dogmatische Betrachtung des Computerstrafrechts
im engen Sinn**

I.	Indiskretionsbezogene Computerdelikte	74
A.	Widerrechtlicher Zugriff auf ein Computersystem (§ 118a)	74
1.	Zum Tatobjekt »Computersystem«	75
2.	Verfügungsberechtigung	84
3.	Zur Tathandlung des Sich-Zugang-Verschaffens	86
4.	Überwinden einer spezifischen Sicherheitsvorkehrung	88
5.	Exkurs: Trojanische Pferde	89
a.	Logische Bomben	91
b.	Dialer	92
c.	Browser-Hijacker	92
d.	Keylogger	93
6.	Überwindung vs Verletzung	96
7.	Überwindung vs Umgehung	100
8.	Subjektive Tatseite	104
a.	Deliktstypus nach Bewertung der überschießenden Innentendenzen	106
b.	Bereicherungsabsicht	113
9.	Sonstiges	117
B.	Die nebenstrafrechtliche Bestimmung des § 51 DSG 2000	117
1.	Deliktstypisierung und überschießende Innentendenzen	121
2.	Tatsubjekt	124
3.	Sonderdelikt	126
4.	»Aufgedrängte Information«	129
5.	§ 51 DSG 2000 als Allgemeindelikt bei widerrechtlich verschafften Daten	130
6.	Objektive Bedingung der Strafbarkeit	136
7.	Tatobjekt »personenbezogene Daten« mit Geheimhaltungsinteresse	138
8.	Allgemeine Betrachtung des schutzwürdigen Geheimhaltungsinteresses	142
9.	Tathandlungen	145
10.	Subjektive Tatseite	153

11. Sonstiges	153
C. Verletzung des Telekommunikationsgeheimnisses	
(§ 119)	154
1. Tatobjekt »Vorrichtung«	156
2. Benützen einer Vorrichtung	161
3. Subjektive Tatseite	162
a. »Subjektives Bezugsobjekt« und Schutzobjekt	163
b. Nachrichten	164
c. Inhalt einer Nachricht	166
d. Mitteilung vs Nachricht	174
e. »Gedankeninhalte«	175
f. »Paketvermittelnde Transportdienste«	182
g. »Inhaltserforschung«	184
4. Nachrichten am Übertragungsweg	188
5. Telekommunikation vs Computersystem	193
6. Unbefugter	196
7. Sonstiges	198
D. Missbräuchliches Abfangen von Daten (§ 119a)	199
1. § 119a Abs 1 Fall 1	200
2. Schutzobjekt und Bezugsobjekt des erweiterten Vorsatzes	200
3. Exkurs: Sniffer und Sniffing-Methoden	201
4. § 119a Abs 1 Fall 2 (Missbräuchliches Auffangen elektromagnetischer Emission)	207
5. De lege ferenda-Empfehlung an den Gesetzgeber ..	212
6. Subjektive Tatseite	214
7. Sonstiges	215
E. Sonstige Verletzungen des	
Telekommunikationsgeheimnisses iSd § 120 Abs 2a ...	216
1. Tatobjekt und Schutzobjekt	217
2. Telekommunikation	219
3. Aufzeichnen	221
4. Zugänglichmachen	222
5. Veröffentlichen	225
6. Mischdelikt	231
7. Unbefugter	232
8. Subjektive Tatseite	235
9. Sonstiges	236

II.	Vermögensbezogene Computerdelikte	236
A.	Datenbeschädigung (§ 126a)	237
1.	Exkurs: Computerviren und Computerwürmer	241
a.	Bootsektorviren	243
b.	Dateiviren	244
c.	Polymorphe Viren	244
d.	Stealth-Viren	245
e.	Hybridviren bzw multipartite Viren	245
f.	Makro- bzw Skriptviren	246
g.	Speicherresidente- bzw TSR-Viren	246
h.	Proof-of-Content-Viren	247
i.	Computerwürmer	248
2.	Computerdaten	250
3.	Verfügungsberechtigung	253
4.	Begehungsweisen	253
a.	Verändern	256
b.	Löschen	258
c.	Unbrauchbarmachen	261
d.	Datenunterdrückung	263
5.	Mischdelikt	270
6.	Vermögensschaden	273
7.	Exkurs: Tauglichkeit des Versuchs	276
8.	Subjektive Tatseite	278
9.	Deliktsqualifikationen	278
10.	§ 126a als terroristische Straftat	282
11.	Privilegierungen	283
12.	Tätige Reue	285
13.	Sonstiges	286
B.	Störung der Funktionsfähigkeit eines Computersystems (§ 126b)	287
1.	Exkurs: DDoS-Angriffe	287
a.	Bot-Netzwerke	289
b.	DoS-Methoden	291
(i.)	Ping flooding bzw ICMP flooding	292
(ii.)	Ping of Death bzw Large Packet Ping	292
(iii.)	Teardrop	293
(iv.)	Smurf	294
(v.)	SYN-Flooding	294
(vi.)	Land-Attack	296

2. Tatobjekt »Computersystem«	297
3. Verfügungsberechtigter	299
4. Tathandlung	300
a. Eingeben von Daten	300
b. Übermitteln von Daten	303
5. Störung der Funktionsfähigkeit eines Computersystems und Schadensermittlung	306
6. Subjektive Tatseite	311
7. Problemfelder: Subsidiaritätsklausel und Deliktsqualifikation	311
8. Sonstiges	317
C. Missbrauch von Computerprogrammen oder Zugangsdaten (§ 126c)	317
1. Tatobjekt des § 126c Abs 1 Z 1	321
2. Tatobjekt des § 126c Abs 1 Z 2	325
3. Herstellen	328
4. Einführen	331
5. Vertreiben, Veräußern und Sonst-Zugänglichmachen	333
6. Sich-Verschaffen	333
7. Besitzen	338
8. Abstraktes Gefährdungsdelikt	339
9. Subjektive Tatseite	340
10. Exkurs: Technischer Hintergrund des »Skimming«	340
11. Sonderproblem: IT-Sicherheitsexperten	344
12. Tätige Reue	347
13. Sonstiges	347
14. § 10 Zugangskontrollgesetz	348
D. Betrügerischer Datenverarbeitungsmissbrauch (§ 148a)	353
1. Zum Tatobjekt »Ergebnis einer Datenverarbeitung«	354
2. Gestaltung des Computerprogramms	356
3. Manipulation mittels Computerdaten	357
4. Sonstige Einwirkungen	357
a. Outputmanipulation	358
b. Konsolenmanipulation	360

5.	»Beeinflussung« des Datenverarbeitungsergebnisses	361
a.	Kritik an der Sozialadäquanz der äußeren Tatseite	363
b.	»Betrugsähnlichkeit«	365
c.	Kritik an der Betrugsähnlichkeit unter Berücksichtigung des § 108	368
d.	»Missbräuchliches Beeinflussen«	374
e.	Vergeistigung des Gewahrsamsbegriffs bei Geldbehebungen aus Bankomaten	376
6.	Sonderproblem: Beendigung der Tat und strafbare Beteiligung	378
a.	Delikte mit überschießender Innentendenz	380
b.	Anschlussdelikte	389
7.	Subjektive Tatseite	390
8.	Qualifikationen	391
9.	Sonstiges	391
III.	Datenfälschung (§ 225a)	392
A.	Tatobjekt der Datenfälschung	393
B.	Falsche und verfälschte Daten	398
C.	Subjektive Tatseite	401
D.	Vertiefte Untersuchung des Phänomens »Phishing« anhand § 108 StGB iVm dem Grundrecht auf Datenschutz	404
1.	Exkurs: »Phishing« und »Pharming«	404
a.	Phishing per E-Mail	405
b.	Phishing per »Abbruchtrojaner«	406
c.	Pharming mittels Deep-linking bzw Framing ..	407
d.	Pharming mittels Trojaner	408
e.	Pharming mittels DNS-Cache-Poisoning	408
2.	Strafrechtliche Beurteilung der Phishing Phase	409
a.	§ 108 StGB iVm § 1 Abs 1 DSGVO 2000	410
b.	Die umstrittene Täuschungsbestimmung des § 108	411
c.	Das Grundrecht auf Datenschutz nach § 1 Abs 1 DSGVO 2000	413
d.	Zur Anwendbarkeit des § 108 StGB im Fall des Phishing	430
3.	Prüfung der »Verwertungsphase«	433

	a. Zum Widerrechtlichen Zugriff auf ein Computersystem (§ 118a)	434
	b. Zum Betrügerischen Datenverarbeitungsmissbrauch (§ 148a)	435
	c. Zum Betrug (§ 146)	437
	d. Zur Datenverwendung in Gewinn- oder Schädigungsabsicht (§ 51 DSG 2000)	438
IV.	Missbräuche im unbaren Zahlungsmittelverkehr	438
	A. Unbare Zahlungsmittel (§ 74 Abs 1 Z 10)	439
	B. Fälschung unbarer Zahlungsmittel (§ 241a)	443
	1. Fälschen oder Verfälschen	444
	2. Schlichtes Tätigkeits- oder Erfolgsdelikt?	446
	3. Subjektive Tatseite	447
	4. Deliktsqualifikationen	447
	C. Annahme, Weitergabe oder Besitz falscher oder verfälschter Zahlungsmittel (§ 241b)	448
	1. Vorbereitungsdelikt unterschiedlicher Intensität ..	449
	2. Übernehmen eines Falsifikats	449
	3. Sich- oder Einem-anderen-Verschaffen	451
	4. Befördern eines Falsifikats	452
	5. Einem-anderen-Überlassen	452
	6. Besitz des Falsifikats	453
	7. Mischdelikt	454
	D. Vorbereitung der Fälschung unbarer Zahlungsmittel (§ 241c)	455
	1. Deliktsspezifische Fälschungswerkzeuge	456
	2. Mischdelikt	457
	3. Subjektive Tatseite	458
	E. Die Tätige Reue-Bestimmung des § 241d	459
	F. Entfremdung unbarer Zahlungsmittel (§ 241e)	460
	1. Bereicherungsentfremdung und Fälschungsentfremdung	461
	2. Vorbereitungshandlungen	463
	3. Deliktsqualifikationen	464
	4. Unterdrückung des unbaren Zahlungsmittels	465
	G. Die Tätige Reue-Bestimmung des § 241g	468
	H. Annahme, Weitergabe oder Besitz entfremdeter unbarer Zahlungsmittel (§ 241f)	471
V.	Sexualbezogene Delikte mit IKT-Bezug	472

A.	Pornographische Darstellungen Minderjähriger	
	(§ 207a)	472
1.	Pornographische Darstellungen	475
2.	Mischdelikt	476
3.	Qualifikation des Abs 1	478
4.	Sich-Verschaffen und Besitzen	
	inkriminierter Bilder	479
a.	Gewahrsamserlangung und Körperlichkeit	480
b.	»Quasi-Gewahrsam«	486
c.	Besitzverbot	489
d.	Aufgedrängter Besitz	497
5.	Der »Zugriff« auf pornographische Darstellungen	
	Minderjähriger im Internet	499
a.	Internet vs Intranet	500
b.	Die »Stand-Alone PC«-Ausnahme	501
6.	Wissentliche Betrachtung pornographischer	
	Darbietungen Minderjähriger (§ 215a Abs 2a)	503
7.	Pornographische Darbietung	504
8.	Tathandlung »Betrachten«	506
9.	Subjektive Tatseite	509
10.	Sonstiges	510
B.	Exkurs: Pornographiegesetz	510
C.	Anbahnung von Sexualkontakten zu Unmündigen	
	(§ 208a) – »Cyber-Grooming«	515
1.	§ 208a Abs 1	517
a.	IKT-Begehungsweisen	518
b.	Konventionelle Kontaktaufnahme	519
c.	Subjektive Tatseite	521
2.	§ 208a Abs 1 a	522
a.	IKT-gebundene Verhaltensweise	523
b.	Zur Strafbarkeitslücke bezüglich	
	pornographischer Darbietungen	525
c.	Kontaktherstellung zur unmündigen Person ...	525
d.	Subjektive Tatseite	528
3.	Tätige Reue	530
4.	Sonstiges	530
VI.	Sonstige Delikte mit IKT-Begehungsweisen	531
A.	Anleitung zur Begehung einer terroristischen	
	Straftat (§ 278f)	531

1. Medienwerk	532
2. Tatbestandsmerkmal »Internet«	532
3. Tatbestandsmerkmal »Information«	535
4. Anbieten	536
5. »Einer-anderen-Person-Zugänglichmachen«	537
6. Die Datenbeschädigung als terroristische Straftat	538
7. Zur Begehung einer terroristischen Straftat »aufreizen«	543
8. Sonstiges	544
9. Sich-Verschaffen von inkriminierten Informationen	544
B. Cyber-Stalking oder die Beharrliche Verfolgung (via Internet) iSd § 107a	546
1. Zum Begriff »Stalking«	547
2. Unzumutbare Beeinträchtigung der Lebensführung	548
3. »Längere Zeit hindurch«	549
4. Deliktstypus	550
5. Aufsuchen der räumlichen Nähe	553
6. »Distanz-Stalking« iSd § 107a Abs 2 Z 2	554
a. Telekommunikation	555
b. Cyber-Stalking	557
c. »Spamming«	559
7. Stalking durch »Identitätsmissbrauch« (§ 107a Abs 2 Z 3)	561
a. Personenbezogene Daten	563
b. Datenverwendung	566
8. Die Veranlassung zur Kontaktaufnahme (§ 107a Abs 2 Z 4)	566
9. Subjektive Tatseite	571
10. Sonstiges	572

3**Schlussbetrachtungen**

I.	Zusammenfassung der wesentlichsten Erkenntnisse	573
A.	Thesen aus der Einleitung	573
1.	Zum Begriff der Computerkriminalität	573
2.	Zum Begriff des Computerstrafrechts	573
3.	Zum Datenbegriff des Strafrechts	574
B.	Thesen des Hauptteils	574
1.	Zum Widerrechtlichen Zugriff auf ein Computersystem (§ 118a)	574
2.	Zur Datenverwendung in Gewinn- oder Schädigungsabsicht (§ 51 DSG 2000)	576
3.	Zur Verletzung des Telekommunikationsgeheimnisses (§ 119)	578
4.	Zum Missbräuchlichen Abfangen von Daten (§ 119a)	580
5.	Zu sonstigen Telekommunikationseingriffen (§ 120 Abs 2a)	581
6.	Zur Datenbeschädigung (§ 126a)	582
7.	Zur Störung der Funktionsfähigkeit eines Computersystems (§ 126b)	584
8.	Zum Missbrauch von Computerprogrammen oder Zugangsdaten (§ 126c)	585
9.	Zum Betrügerischen Datenverarbeitungsmissbrauch (§ 148a)	588
10.	Zur Datenfälschung (§ 225a)	589
11.	Zum Phishing und § 108 StGB iVm § 1 DSG 2000 ...	589
12.	Zu unbaren Zahlungsmitteln (§§ 241a, 241b, 241c, 241d, 241e, 241f, 241g)	589
13.	Zu Pornographischen Darstellungen Minderjähriger (§ 207a)	591
14.	Zu Pornographischen Darbietungen Minderjähriger (§ 215a)	592
15.	Zur Anbahnung von Sexualkontakten zu Unmündigen (§ 208a)	592
16.	Zur Anleitung zur Begehung einer terroristischen Straftat (§ 278f)	594
17.	Zu § 126a als terroristische Straftat	595

	18. Zur Beharrlichen Verfolgung (§ 107a)	596
II.	Epilog oder fünf generelle abschließende Thesen	597
	A. Zur Bedeutung der Computerkriminalität	597
	B. Zur Transformation und Expansion der Rechtsgüter	598
	C. Zu traditionellen Rechtsinstituten der Strafrechtsdogmatik im Fokus der IKT	600
	D. Zur Unzulänglichkeit diverser Tatbestände und zur problembehafteten Gesetzestechnik	601
	E. Zur Rechtsterminologie	604

4

Ausblick »StRÄG 2015«

A.	Einführung einer Legaldefinition der »kritischen Infrastruktur« in § 74	607
B.	Schaffung von Qualifikationsbestimmungen betreffend die Kritische Infrastruktur	610
C.	Neufassung des Widerrechtlichen Zugriffs auf ein Computersystem (§ 118a)	611
D.	Erweiterung bzw Abänderung der Qualifikationen der Datenbeschädigung (§ 126a)	615
E.	Erweiterung bzw Abänderung der Qualifikationen der Störung der Funktionsfähigkeit eines Computersystems (§ 126b)	618
F.	Einführung eines neuen Straftatbestandes, die »Fortgesetzte Belästigung im Wege einer Telekommunikation oder eines Computersystems« (§ 107c)	619
G.	Einführung einer Qualifikation des Selbstmordes für die »Beharrliche Verfolgung« (§ 107a Abs 3)	622
H.	Einführung einer neuen Strafbestimmung »Ausspähen von Daten eines unbaren Zahlungsmittels« (§ 241h)	622
I.	Weitere Änderungen iZm Computerdelikten durch das StRÄG 2015	624
	1. Einführung des Erschwerungsgrunds des »Identitätsmissbrauchs«	624
	2. Neudefinition der »Gewerbsmäßigkeit«	625

3. Erweiterung der Aufzählung der Rechtsgüter in § 74 Abs 1 Z 5	626
4. Erweiterung des Qualifikationstatbestands des § 147 Abs 1 Z 1 bezüglich § 241h StGB	627
5. Erweiterung der Privilegierung des § 166 um die Delikte der §§ 241a ff	627
6. Erweiterung der Strafausschließungsgründe des § 207a Abs 5	628
7. Ergänzung einer Geldstrafdrohung als Alternative zur Freiheitsstrafe und Anhebung von bestehenden Geldstrafdrohungen	628
8. Erhöhung der Wertgrenzen	629

5

Quellenverzeichnis

A. Literaturverzeichnis	631
1. Monographien	631
2. Festschriften und Sammelbände	637
3. Beiträge in Festschriften und Sammelbänden	640
4. Beiträge in Zeitschriften	645
5. Beiträge in Gesetzeskommentaren	651
B. Judikaturverzeichnis	654
C. Normenverzeichnis	659
1. Gesetze (alphabetisch)	659
2. Gesetzesmaterialien (chronologisch aufsteigend)	662
3. Europarecht (chronologisch aufsteigend)	665
4. Vorarbeiten, Stellungnahmen und Mitteilungen von Organen der EU	666
5. EU-Rahmenbeschlüsse	667
6. Konventionen und Erläuterungen des Europarats (chronologisch aufsteigend)	667
7. Protokoll der Vereinten Nationen (UN)	668
D. Web-Verzeichnis	668