IT und Strafrecht

Christian Bergauer

Das materielle Computerstrafrecht

Jan Sramek Verlag

Christian Bergauer

Das materielle Computerstrafrecht

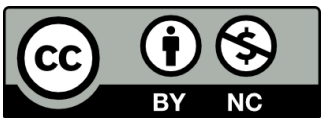
Jan Sramek Verlag

Veröffentlicht mit Unterstützung des Austrian Science Fund (FWF): PUB-Antragsnummer 300-V16

FWF Der Wissenschaftsfonds.

Die finanzielle Unterstützung des FWF ermöglicht auch den kostenfreien Zugriff auf dieses Dokument.

Creative Commons Licence Terms



You are free to share (copy, distribute and transmit) this work under the following conditions:

1. Attribution – You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).

2. Noncommercial – You may not use this work for commercial purposes.

Die vollständigen Creative Commons Lizenzbestimmungen in deutscher Sprache finden Sie online unter <http://creativecommons.org/licenses/by-nc/4.0/legalcode>

All übrigen Rechte, insbesondere das Recht auf Übersetzung oder die Nutzung des Layouts für Zwecke jenseits der Lizenzbestimmungen oder das Recht gedruckte Exemplare zu vertreiben, sind vorbehalten.

Produkthaftung:
Trotz sorgfältiger Bearbeitung und Kontrolle kann keine Garantie für die Vollständigkeit, Aktualität oder Fehlerlosigkeit des Werkes gegeben werden. Eine Haftung des Verlages, des/der Herausgeber/innen und/oder Autor/inn/en aus dem Inhalt dieses Werkes ist ausgeschlossen.

Eigensatz des Verlags
Schrift: Arnhem Pro

Eine auf hochwertigem Papier gedruckte Fassung mit Festeinband und Fadenheftung kann unter der ISBN 978-3-7097-0043-3 direkt beim Verlag <www.jan-sramek-verlag.at> oder im Buchhandel bestellt werden.

© Wien 2016, Jan Sramek Verlag KG

Vorwort

Die vorliegende Arbeit beruht im Wesentlichen auf der überarbeiteten Fassung meiner Habilitationsschrift, die im Herbst 2013 an der Rechtswissenschaftlichen Fakultät der Karl-Franzens-Universität Graz eingereicht und im Frühjahr 2014 angenommen wurde. Rechtsprechung und Literatur sowie Gesetzesänderungen (mit Ausnahme des StRÄG 2015, dem in der Arbeit noch ein »Ausblick« gewidmet wird) wurden bis 1. Juli 2015 berücksichtigt.

Mein Dank gilt allen, die mich in der Zeit des Verfassens der Habilitationsschrift und der Vorbereitung dieser Publikation unterstützt haben.

Mein wichtigster Dank kommt meiner Frau und meinen Kindern zu, die mir für mein Habilitationsvorhaben stets einen starken Rückhalt gegeben haben; ihnen ist dieses Buch herzlichst gewidmet.

Graz, im September 2015 *Christian Bergauer*

Das materielle Computerstrafrecht

1 Ausgangssituation, Begrifflichkeiten und Rechtsentwicklung 1

2 Dogmatische Betrachtung des Computerstrafrechts im engen Sinn 73

3 Schlussbetrachtungen 573

4 Ausblick »StRÄG 2015« 607

5 Quellenverzeichnis 631

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 DSG 2000 ... 410
b. Die umstrittene Täuschungsbestimmung des § 108 ... 411
c. Das Grundrecht auf Datenschutz nach § 1 Abs 1 DSG 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 1a ... 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 (§ 278 f) 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

Abkürzungsverzeichnis

aA	anderer Ansicht	**A**
AB	Ausschussbericht	
ABl	Amtsblatt der Europäischen Union	
Abs	Absatz	
aF	alte Fassung	
Alt	Alternative	
Anm	Anmerkung	
AnwBl	Österreichisches Anwaltsblatt (Fachzeitschrift)	
ARD	Aktuelles Recht zum Dienstverhältnis	
arg	argumento/argumentum (folgt aus)	
ARP	Adress Resolution Protocol	
ARPA	Advanced Research Projects Agency	
ARPANET	Advanced Research Projects Agency Network	
Art	Artikel	
ASCII	American Standard Code for Information Interchange	
AT	Allgemeiner Teil	
ausf	ausführlich	
Bd	Band	**B**
BG	Bundesgesetz	
BGBl	Bundesgesetzblatt	
BIOS	Basic Input Output System	
BlgNR	Beilagen zu den stenographischen Protokollen des Nationalrates	
BMJ	Bundesministerium für Justiz	
BReg	Bundesregierung	
bspw	beispielsweise	
BT	Besonderer Teil	
bzw	beziehungsweise	
CCC	Convention on Cybercrime	**C**
CD	Compact Disc	

	CDPC	European Committee on Crime Problems
	CETS	Council of Europe Treaty Series
	CPU	Central Processing Unit
	CR	Computer und Recht (Fachzeitschrift)
D	DF	Deliktsfall
	dh	das heißt
	DIN	Deutsche Industrie Norm
	DNS	Domain Name System
	DoS	Denial of Service
	DSK	Datenschutzkommission
	DSWR	Datenverarbeitung Steuern – Wirtschaft – Recht (Fachzeitschrift)
	DVD	Digital Versatile Disc
E	E	Entscheidung
	ecolex	Fachzeitschrift für Wirtschaftsrecht (Fachzeitschrift)
	EDVuR	EDV und Recht (Fachzeitschrift)
	EMV	Europay, Mastercard, Visa
	ER	Explanatory Report
	Erl	Erläuterung(en)
	ErlME	Erläuterungen zum Ministerialentwurf
	ErlRV	Erläuterungen zur Regierungsvorlage
	ErlStV	Erläuterungen zum Staatsvertrag
	ErwG	Erwägungsgrund
	etc	et cetera
	ETS	European Treaty Series
	EU	Europäische Union
	EuGH	Europäischer Gerichtshof
	EuGRZ	Europäische Grundrechte-Zeitschrift (Fachzeitschrift)
	EU-RB	Rahmenbeschluss der (damals noch) dritten Säule (polizeiliche und justizielle Zusammenarbeit in Strafsachen) der Europäischen Union.
F	f	folgende(r)
	ff	fortfolgende
	FN	Fußnote
	FS	Festschrift
	FTP	File Transfer Protocol

gem	gemäß	**G**
ggf	gegebenenfalls	
GMat	Gesetzesmaterialien	
GRC	Charta der Grundrechte der Europäischen Union	
GP	Gesetzgebungsperiode	
hA	herrschende Ansicht	**H**
hins	hinsichtlich	
hL	herrschende Lehre	
hM	herrschende Meinung	
Hrsg	Herausgeber	
HS	Halbsatz	
Http	Hypertext Transfer Protocol	
Html	Hypertext Markup Language	
idF	in der Fassung	**I**
idgF	in der geltenden Fassung	
idR	in der Regel	
idS	in diesem Sinn/e	
IEC	International Electrotechnical Commission	
ieS	im engen Sinn	
iHv	in Höhe von	
IKT	Informations- und Kommunikationstechnologie	
insb	insbesondere	
IP	Internet Protocol	
iSd	im Sinne des/der	
ISO	International Organization for Standardization	
ISP	Internet Service Provider	
iSv	im Sinne von/vom	
iVm	in Verbindung mit	
iwS	im weiten Sinn	
iZm	im bzw in Zusammenhang mit	
JA	Justizausschuss	**J**
JAB	Justizausschussbericht	
JAP	Juristische Ausbildung und Praxisvorbereitung (Fachzeitschrift)	
JBl	Juristische Blätter (Fachzeitschrift)	
JSt	Journal für Strafrecht (Fachzeitschrift)	

	jusIT	Zeitschrift für IT-Recht, Rechtsinformation und Datenschutz (Fachzeitschrift)
K	Kfz	Kraftfahrzeug
	krit	kritisch
L	LAN	Local Area Network
	LG	Landesgericht
	Lit	Literatur
	lit	litera
	LK	Leipziger Kommentar zum Strafgesetzbuch
M	MAC	Media Access Control
	ME	Ministerialentwurf
	mE	meines Erachtens
	MIT	Massachusetts Institute of Technology
	MM	Moduliertes Merkmal
	MR	Medien und Recht (Fachzeitschrift)
	MTA	Message Transfer Agent
	MTU	Maximum Transmission Unit
	mwN	mit weiteren Nachweisen
N	NFC	Near Field Communication
	NJW	Neue Juristische Wochenschrift
	Nov	Novelle
O	obj	objektiv(e)
	OECD	Organization for Economic Cooperation and Development
	OGH	Oberster Gerichtshof
	Ö	Österreich
	ÖJK	Österreichische Juristenkommission
	ÖJZ	Österreichische Juristen-Zeitung (Fachzeitschrift)
	österr	österreichisch(e)
P	PC	Personal Computer
	PIN	Persönliche Identifikationsnummer(n)
R	RAM	Random Acess Memory
	RB	Rahmenbeschluss

RdW	Österreichisches Recht der Wirtschaft (Fachzeitschrift)
ROM	Read Only Memory
Rs	Rechtssache EuGH
Rsp	Rechtsprechung
RV	Regierungsvorlage
RZ	Österreichische Richterzeitung (Fachzeitschrift)
Rz	Randzahl
S	Seite
SbgK	Salzburger Kommentar zum Strafgesetzbuch
Slg	Sammlung
SIAK	Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis (Fachzeitschrift)
SMTP	Simple Mail Transfer Protocol
sog	so genannte/r
SQL	Structured Query Language
StA	Staatsanwaltschaft
StF	Stammfassung
stRsp	ständige Rechtsprechung
StudB	Studienbuch
subj	subjektiv(e)
TAN	Transaktionsnummer(n)
TCP	Transmission Control Protocol
ua	unter anderem
uÄ	und Ähnliches
URL	Uniform Resource Locator
USB	Universal Serial Bus
usw	und so weiter
uU	unter Umständen
va	vor allem
VBA	Visual Basic for Application
verst Senat	verstärkter Senat
VfGH	Verfassungsgerichtshof
vgl	vergleiche
VoIP	Voice over IP

	Vorbem	Vorbemerkungen
	VwGH	Verwaltungsgerichtshof
W	WK	Wiener Kommentar zum Strafgesetzbuch
	WLAN	Wireless Local Aera Network
Z	Z	Ziffer
	zB	zum Beispiel
	ZfV	Zeitschrift für Verwaltung (Fachzeitschrift)
	ZIS	Zeitschrift für Internationales Strafrecht (Fachzeitschrift)
	ZStW	Zeitschrift für die gesamte Strafrechtswissenschaft (Fachzeitschrift)
	zT	zum Teil
	zusf	zusammenfassend
	zust	zustimmend
	ZVR	Zeitschrift für Verkehrsrecht (Fachzeitschrift)

1 Ausgangssituation, Begrifflichkeiten und Rechtsentwicklung

I. Einleitung, Gang der Untersuchung und Vorüberlegungen

Mit der Erfindung und Etablierung des PC und vor allem auch der Entwicklung des Internet wurde eine globale Durchdringung mit informationstechnischen Systemen (sog »Ubiquitous Computing«[1]) initiiert, die unsere Gesellschaft in vielen Bereichen verändert hat. So lässt sich ein Wandel der Kommunikationsweise und -formen ebenso erkennen wie eine in vielen Bereichen bereits unentbehrlich gewordene Technisierung des Alltags- und Berufslebens. Im Jahr 2014 ist die Zahl der Internetzugänge weltweit auf über drei Milliarden angestiegen.[2] Allein in Österreich verfügten damals bereits 81 %[3] der Haushalte[4] und 98 %[5] der Unternehmen[6] über einen Internetzugang.

Durch das enorme Potenzial digitalisierter Datenverarbeitung in jeglicher Hinsicht haben sich aber auch strafbare Handlungen in den letz-

1 Siehe grundlegend zur Begrifflichkeit *Weiser,* The Computer for the Twenty-First Century, Scientific American 1991, 66 ff; *Weiser,* Some Computer Science Problems in Ubiquitous Computing, Communications of the ACM 1993, 75 ff; siehe auch *Hödl,* Die Macht der klugen Dinge. Überlegungen zu ubiquitous computing, RFID-Chips und smart objects, juridikum 2007, 210.

2 Siehe *Internet World Stats,* World internet usage and population statistics, <www.internetworldstats.com/stats.htm> (03.03.2015).

3 Vgl *Statistik Austria,* IKT-Einsatz in Haushalten 2014, <www.statistik.at/web_de/statistiken/informationsgesellschaft/index.html> (03.03.2015).

4 Die Erhebungen betrafen Haushalte mit mindestens einem Mitglied im Alter von 16 bis 74 Jahren bzw Personen im Alter von 16 bis 74 Jahren.

5 Siehe *Statistik Austria,* IKT-Einsatz in Unternehmen 2014, <www.statistik.at/web_de/statistiken/informationsgesellschaft/index.html> (03.03.2015).

6 Die Erhebungen betrafen Unternehmen ab 10 Beschäftigten.

ten Jahren vermehrt in informationstechnische Systeme wie das Internet verlagert. Tatorte bilden hierbei nicht mehr nur physische Räume, sondern die unterschiedlichsten Bereiche des virtuellen Cyberspace. Tatmittel und Tatobjekte haben sich von körperlichen Gegenständen oder auch Menschen auf unkörperliche ubiquitäre Informationseinheiten, in Form digitaler Daten, ausgedehnt. Darüber hinaus darf nicht außer Acht gelassen werden, dass moderne informationstechnische Systeme auf einer Technologie beruhen, die sehr facettenreich und manipulationsträchtig ist und weder Ländergrenzen noch Entwicklungsgrenzen kennt. Das Entwicklungspotenzial der Technologie ist jedenfalls enorm, sodass sich am heutigen Tag keine seriöse Prognose abgeben lässt, wohin sich diese Technisierung noch bewegen wird. Meines Erachtens beschreiben die aktuellen Vorgänge aber lediglich den Anfang einer noch nie dagewesenen digitalen Revolution.

Die technischen Entwicklungen auf diesem Gebiet stellen große Herausforderungen für sämtliche Wissenschaftsdisziplinen dar, wobei im Bereich der Rechtswissenschaften – im hier interessierenden Zusammenhang – das Strafrecht und das Datenschutzrecht immanent mit dem gesellschaftlichen Zusammenleben in Theorie und Praxis verwoben sind.

Insbesondere indizieren die Informationstechnologie und ihre Möglichkeiten im strafrechtlichen Zusammenhang spezielle Problembetrachtungen in der Rechtspolitik, der Strafrechtsdogmatik, der Ermittlungstaktik und der Kriminaltechnik (wie insb Computer- bzw Datenforensik).

Spätestens dann, wenn die Sicherheit bzw das Zusammenleben der Gesellschaft und Rechtsgüter ernsthaft bedroht werden, ist ua der Gesetzgeber gefordert, auf solche Bedrohungen zu reagieren. Aufgrund der Transnationalität moderner Erscheinungsformen der »Computerkriminalität« ist dies nicht nur eine rein innerstaatliche Aufgabe der einzelnen Staaten, sondern erfordert ein »vernetztes« internationales Vorgehen, um Computerkriminalität wirksam bekämpfen zu können.[7] In Österreich hat der Gesetzgeber im Kernstrafrecht bereits im

7 Vgl dazu auch das »Haager Programm« von 2004 zur Stärkung von Freiheit, Sicherheit und Recht in der Europäischen Union und anschließend im »Stockholmer Programm« von 2009 und den dazugehörigen Aktionsplan [Aktionsplan des Rates und der Kommission zur Umsetzung des Haager Programms zur Stärkung von Freiheit, Sicherheit und Recht in der Europäischen Union, ABl C 2005/198, 1; Das Stockholmer Programm – Ein offenes und sicheres Europa im Dienste und

Jahr 1988 auf den informationstechnischen Paradigmenwechsel bezüglich ubiquitärer, digitaler unkörperlicher Daten reagiert, indem er die Tatbestände der Datenbeschädigung (§ 126a StGB[8]) und des betrügerischen Datenverarbeitungsmissbrauchs (§ 148a) schuf. Diese Maßnahme könnte – in der Sprache der modernen Informatik ausgedrückt – als ein (rein innerstaatliches) »Stand-Alone-Computerstrafrecht der ersten Generation« verstanden werden.

Auch viele andere europäische Staaten erkannten das Problem und auch die Schwierigkeit der Strafverfolgung iZm länderübergreifender Computerkriminalität, weshalb sowohl der Europarat als auch die Europäische Union zwei elementare einschlägige Rechtsakte setzten, zum einen die »Convention on Cybercrime« des Europarates[9] (in weiterer Folge: CCC) und zum anderen der EU-RB 2005/222/JI über Angriffe auf Informationssysteme[10]. Diese Regelungsvorgaben führten in Ö im Jahr 2002 neben der Aktualisierung der bisherigen Delikte gegen Computerkriminalität auch zu umfangreichen Erweiterungen[11], die in einem »Computerstrafrecht der zweiten Generation« mündeten.

Ziel der vorliegenden Arbeit ist es, die modernen Erscheinungsformen der Computerkriminalität technisch, aber mit dem Fokus auf Verständlichkeit für Juristinnen und Juristen (und nicht etwa für TechnikerInnen), darzustellen sowie legistische Bemühungen des Gesetzgebers, die bis dato entwickelten Literaturmeinungen und – soweit vorhanden – einschlägige Judikate aus rechtspolitischer und insb dogmatischer Sicht wissenschaftlich zu analysieren.[12]

▹▹ zum Schutz der Bürger, ABl C 2010/115, 1; Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – Ein Raum der Freiheit, der Sicherheit und des Rechts für die Bürger Europas – Aktionsplan zur Umsetzung des Stockholmer Programms, KOM (2010) 171 endg].

8 Paragraphenangaben ohne Kennzeichnung des Gesetzes oder der jeweiligen Fassung beziehen sich stets auf das Strafgesetzbuch (StGB), BGBl 60/1974 idF I 106/2014.

9 Convention on Cybercrime (ETS 185) vom 23.11.2001, <conventions.coe.int/Treaty/en/Treaties/Html/185.htm> (03.03.2015). Sie trat am 1. Juli 2004 mit der Ratifikation des fünften Staates (inkl zumindest dreier Mitgliedstaaten des Europarates) in Kraft. Österreich hat das »Übereinkommen über Computerkriminalität« bereits 2001 unterzeichnet, aber erst mit BGBl III 140/2012 formell ratifiziert.

10 Rahmenbeschluss 2005/222/JI des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme, ABl L 2005/69, 67.

11 Siehe zur Entwicklung des Computerstrafrechts gleich im Anschluss.

12 Die Zitierweise in dieser Arbeit folgt den »NZR«; siehe *Jahnel/Sramek,* NZR. Neue Zitierregeln (2012). Judikate werden nach ihrer Auffindbarkeit über ihr Aktenzei

Trotz Zunahme der Anzeigen im Bereich der Computerkriminalität fristet das Computerstrafrecht in der Strafrechtspraxis – obwohl die wesentlichen Computerdelikte zumindest schon zehn Jahre lang in Geltung stehen – noch immer ein eher untergeordnetes Dasein, was auch die Verurteilungszahlen hins einschlägiger Computerdelikte bestätigen.[13] Die starke Diskrepanz von Anzeigen und tatsächlichen Verurteilungen lässt sich neben den rein faktischen Problemen der Strafverfolgung in der Ausforschung international agierender Täter bzw Tätergruppen, in erster Linie auch mit den hohen Tatbestandsanforderungen einzelner Delikte begründen, die mE in vielen Fällen zu einer gravierenden Minderanwendbarkeit führen.

Auffällig ist allerdings, dass die Computerdelikte der »ersten Generation« – diese sind § 126a und § 148a StGB – als die wohl weiterhin am praxisrelevantesten zu betrachten sind.

▹▹ chen zitiert (vgl dazu *Staudegger,* Suche von Entscheidungen mit Aktenzeichen bzw »Geschäftszahl«, jusIT 2008/13, 33). Das bedeutet, dass selbst in Fachzeitschriften veröffentlichte E lediglich durch Entscheidungsdatum und Aktenzeichen genannt werden (in diesem Sinn *Pfersmann,* Bemerkenswertes aus der SZ 2006/I, ÖJZ 2008/98, der die Vorzüge des RIS entdeckt hat und dazu ausführt: »Hat man in ›seiner‹ Fachzeitschrift eine einschlägig interessierende E – ohne oder auch mit Kommentar – entdeckt, so kann man sich jetzt anhand des Aktenzeichens mittels einfachen Mausklicks aus dem RIS problemlos den Volltext auf den Bildschirm holen und auch ausdrucken«). Wurde die E allerdings glossiert, werden die »Meta-Daten« der E durch die Fundstelle und den Autor erweitert. Auch RIS-Rechtssatzdokumente werden in Form ihrer Rechtssatznummer angeführt, wobei dies in den Fällen erfolgt, in denen nicht auf die konkrete E selbst, sondern auf die konkrete Aussage des Rechtssatzes Bezug genommen wird *(Jahnel/Sramek,* NZR, 28 f). Darüber hinaus wird die Rechtssatznummer auch dann angegeben, wenn die im Rechtssatz extrahierte Aussage in vielen E getätigt wurde, welche sich für den Leser über die Rechtssatzabfrage im RIS einsehen lassen. Erstzitate von Gesetzen in den Fußnoten werden zwecks Leserfreundlichkeit bereits mit dem Kurztitel erfasst, der vollständige Titel des jeweiligen Gesetzes findet sich im Quellenverzeichnis. Erläuterungen zu Ministerialentwürfen oder Staatsverträgen werden mit »ErlME« bzw »ErlStV« angegeben.

13 Siehe unten die Statistik der Verurteilungszahlen. Zur generellen Kritik an den Statistiken siehe *Schmölzer,* Straftaten im Internet: eine materiell-rechtliche Betrachtung, ZStW 2011/123, 709 (715 ff).

Polizeiliche Anzeigenstatistik einschlägiger Delikte von 2003 bis 2013[14]:

Delikte	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013
§ 118a	12	26	16	31	40	41	62	79	172	229	391
§ 119	3	7	6	6	7	11	5	8	12	14	7
§ 119a	1	4	6	0	7	2	10	9	30	21	10
§ 126a	31	48	88	42	62	45	74	85	72	302	198
§ 126b	4	11	6	5	4	4	7	25	21	702	504
§ 126c	8	32	26	45	38	34	56	78	88	163	171
§ 148a	107	80	92	261	186	69	121	159	321	812	426
§ 225a	0	4	26	1	7	7	12	17	37	39	37

Nach Auskunft der Innenministerin sind Anstiege wie bspw des Phishing oder Bestellbetrugs sowie des Hacking festzustellen. Darüber hinaus ist auch bei Anzeigen bezüglich § 126a StGB (Datenbeschädigung), § 126b StGB (Störung der Funktionsfähigkeit eines Computersystems) und § 126c StGB (Missbrauch von Computerprogrammen und Zugangsdaten) ein starker Anstieg zu verzeichnen, welcher in erster Linie auf die vermehrte Verbreitung des sog »Polizei-Virus«[15] zurückzuführen sei.[16]

14 Die Statistik beruht auf dem Zahlenmaterial der parlamentarischen Anfragenbeantwortung der Innenministerin betreffend »Internetkriminalität – Strafdelikte durch IT-Medium im Jahr 2012« (13233/AB XXIV. GP, 1) und »Internetkriminalität – Strafdelikte durch IT-Medium im Jahr 2013« (1645/AB XXV. GP, 1).

15 Dabei wird ein Schadprogramm verschickt, das die infiltrierten Computersysteme sperrt und die Nutzer auffordert, für die Freigabe des Computers Geld zu überweisen (siehe zur »Ransomware« unten).

16 13233/AB XXIV. GP, 4.

Gerichtliche Kriminalstatistik[17] einschlägiger Delikte von 2003 bis 2013[18]:

Delikte	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013
§ 118a	0	0	0	0	0	0	1	0	0	1	2
§ 119	0	0	0	0	0	0	0	0	0	0	0
§ 119a	0	0	0	0	0	0	0	0	0	0	0
§ 126a	0	1	3	1	2	2	0	0	1	5	6
§ 126b	0	0	0	0	0	0	0	0	0	1	0
§ 126c	0	0	0	0	0	0	0	0	1	1	0
§ 148a	13	8	8	1	6	26	32	35	82	113	99
§ 225a	0	0	0	0	0	4	3	3	5	8	4

A. Gang der Untersuchung

Die vorliegende Arbeit setzt sich mit den Phänomenen der »Computerkriminalität« und mit dem »Computerstrafrecht« auseinander. Darüber hinaus thematisiert sie die Schnittstelle von Technik und Recht im Allgemeinen und materiellem Strafrecht und Informationstechnologie im Besonderen.

Zuerst werden die spezifischen Computerdelikte systematisch dargestellt und ausführlich besprochen, wobei es sich dabei nicht aus-

17 Diversionelle Erledigungen sind nicht erfasst.

18 Die konkrete Übersicht wurde aus den Daten der jährlich publizierten Gerichtlichen Kriminalstatistiken der Statistik Austria erstellt; siehe <www.statistik.at/web_de/statistiken/soziales/kriminalitaet/index.html> (03.03.2015).

schließlich um »echte« Computerdelikte handelt. Es werden nämlich auch grundsätzlich technikneutrale Bestimmungen analysiert, welche aber zumindest auch explizite, informationstechnologische Begehungsweisen enthalten (sog »unechte Computerdelikte«). Bei diesen letztgenannten Delikten wird daher – dem hier interessierenden Untersuchungsgegenstand Rechnung tragend – der Schwerpunkt der Ausarbeitung auf diese spezifischen Begehungsweisen gesetzt. Aufgrund der thematischen Nähe einzelner Nebenstrafbestimmungen, wie zB § 51 Datenschutzgesetz 2000 oder § 10 Zugangskontrollgesetz, werden auch diese Bestimmungen in die Untersuchung einbezogen. Daneben wird die Wirksamkeit des materiellen Strafrechts anhand ausgewählter Phänomene der Computerkriminalität untersucht.

Teil I der Arbeit befasst sich mit den informationstechnischen Infrastrukturen und technischen Entwicklungen sowie mit den Begrifflichkeiten »Computerkriminalität« und »Computerstrafrecht«. Außerdem wird der kernstrafrechtliche Datenbegriff aufgearbeitet, der eine wesentliche Rolle bei der Anwendung spezifischer Delikte spielt. Des Weiteren werden die legistischen Entwicklungen des Computerstrafrechts im engeren Sinn überblicksmäßig dargestellt. Was die informationstechnikspezifische Ausgangssituation anlangt, werden wesenstypische Elemente der Informations- und Kommunikationstechnologie wie Digitalisierung, Automatisierung, Abstraktion, Universalität, Virtualisierung, Ubiquität und Transnationalität sowie die Entwicklungsdynamik in Geschwindigkeit und Miniaturisierungszunahme angesprochen.

In weiterer Folge wird unter Berücksichtigung der vorhandenen Ansätze und modernen Erscheinungsformen der Begriff »Computerkriminalität« näher untersucht, wobei keiner dieser bisherigen Definitionsansätze vollends überzeugt.

Auch werden als Folge der hier getroffenen Definitionen bestimmte Fallbereiche und Sonderfälle (wie reine Hardware-Angriffe, Zeitdiebstahl, Urheberrechtsverletzungen bezüglich Software) für die gegenständliche Untersuchung weitgehend ausgeschieden und die dogmatischen Entwicklungen unter Einbeziehung internationaler und europäischer Vorgaben in einem Kurzüberblick festgehalten, bevor sich Teil II der vorliegenden Arbeit mit der dogmatischen Darstellung des Computerstrafrechts im engen Sinn beschäftigt.

Teil II umfasst den Hauptteil dieser Arbeit und widmet sich den einzelnen Computerdelikten. Diese werden nach den in Teil I angestellten Erwägungen identifiziert und bezüglich ihres thematischen

Kontexts gereiht und ausgewertet. Der Aufbau richtet sich in erster Linie nach den jeweiligen Rechtsgütern. Dabei wird mit den Individualrechtsgütern (wie zB der Privatsphäre, dem Kommunikations- bzw Übertragungsgeheimnis und dem Vermögen) der echten Computerdelikte begonnen und mit unechten Computerdelikten und deren Individualrechtsgüter- und Universalrechtsgüterschutz fortgesetzt. Mit einzelnen – eher schwach ausgeprägten – unechten Computerdelikten, endet der Kernbereich dieser Arbeit. Anzumerken ist, dass ausnahmsweise auch die einzige Strafbestimmung des Datenschutzgesetzes (§ 51 DSG 2000) ausführlich untersucht wird, obwohl es sich dabei um kein spezielles Computerdelikt handelt. Dies wird damit begründet, dass einerseits Verletzungen des Geheimhaltungsrechts personenbezogener Daten insb durch die IKT begründet und realisiert werden (was schon der Grundgedanke des Datenschutzgesetzes 1978 war[19]) und andererseits, weil der Schnittstelle von materiellem Strafrecht und Datenschutzrecht in dieser Arbeit ebenfalls besondere Aufmerksamkeit gewidmet werden soll. Der Umfang der Ausarbeitung der einzelnen echten und unechten Computerdelikte entspricht faktisch der Proportionalität ihrer IKT-Relevanz. Folglich wird – sachlich gerechtfertigt – den echten Computerdelikten mehr Platz eingeräumt, als den unechten, welche wenig IKT-Bezug aufweisen und daher auch am Ende des Hauptteils der vorliegenden Arbeit behandelt werden.

Im Zuge dieser Ausarbeitungen werden die entsprechenden Rechtsgüter untersucht, Tatbestände dargestellt und dogmatisch wie kriminalpolitisch analysiert. Da überschaubar wenige einschlägige Sachverhaltssubstrate von Gerichtsentscheidungen existieren, werden fiktive, aber durchaus realistische Lebenssachverhalte in dieser Arbeit verwendet und in ausgewählten Fällen einer hypothetischen strafrechtlichen Prüfung unterzogen. Darüber hinaus werden generell auch moderne Erscheinungsformen der Computerkriminalität (wie DoS, Phishing, Skimming, Cyber-Grooming und Cyber-Stalking, aber auch Malware, wie Computerwürmer, Computerviren und Trojanische Pferde usw) tech-

19 Vgl AB 1024 BlgNR XIV. GP, 1f: »Rechtspolitischer Grundgedanke der Beratungen war, die Persönlichkeitsphäre des Menschen auch in Anbetracht des Einsatzes moderner Informationstechnologie zu wahren und ihm Rechtsschutz gegen ungerechtfertigte Verwendung seiner Daten zu ermöglichen.«; weiters ErlRV 72 BlgNR XIV. GP, 8: »Die Diskussion über das Problem des ›Datenschutzes‹ entstand mit dem vermehrten Einsatz der elektronischen Datenverarbeitung für die Sammlung von Daten und Informationen«.

nisch erklärt, hins ihrer Sozialverträglichkeit untersucht und in weiterer Folge unter die abstrakten computerspezifischen Tatbilder subsumiert. Integralen Bestandteil dieser Arbeit bilden auch Verflechtungen des materiellen Strafrechts mit dem Grundrecht auf Datenschutz in praktischer Anwendung und Dogmatik sowie die Aufarbeitung der nebenstrafrechtlichen Strafbestimmung des § 51 DSG 2000. Besonderes Augenmerk wurde bei der Auseinandersetzung mit den IKT-spezifischen Delikten auf die bisherigen Lehrmeinungen und – sofern vorhanden – Judikate gelegt, welche einer ausführlichen Analyse zugeführt und kritisch hinterfragt werden. Daraus entwickelt sich in den meisten Fällen ein eigener Ansatz, der sich wiederum in vielen Aspekten von der hM deutlich unterscheiden kann. In anderen Fällen liegt der Mehrwert dieser Arbeit aber auch darin, dass bisher unbeachtete Problemfelder iZm den Computerdelikten erstmals aufgezeigt werden, deren Behandlung und bestenfalls Lösung – sofern sie nicht schon in der vorliegenden Arbeit ausgearbeitet werden – sich hervorragend für weiterführende Untersuchungen und wissenschaftliche Arbeiten eignen.

Nicht zuletzt werden in diesem Kapitel dogmatische Schwachstellen aufgezeigt, die für die starke Diskrepanz der Anzeigenstatistik und Verurteilungsstatistik mitverantwortlich sein könnten. Besondere Aufmerksamkeit wird ferner den daraus resultierenden Empfehlungen an den Gesetzgeber gewidmet.

In Teil III werden zusammenfassende Schlussbetrachtungen angestellt und wesentliche Erkenntnisse dieser Arbeit (Ergebnisse, eigene Thesen und Empfehlungen) in ihrem Kern überblickshaft aufgelistet.

B. Die Omnipräsenz informationstechnischer Systeme

1. Abstraktion und Repräsentation

Digitale Datenverarbeitungsprozesse basieren auf einem strengen Determinismus. Genau genommen gibt es nur zwei eindeutige (physikalische) Zustände, welche bei sämtlichen digitalen Verarbeitungsprozessen die Grundlage sind, nämlich Strom fließt oder fließt nicht[20],

20 Es könnte auch durch »hohe Spannung« und »niedere Spannung« beschrieben werden und muss nicht zwingend mit absoluten »ein-« bzw »aus-Werten« zu tun haben.

geladen oder ungeladen, magnetisiert oder nicht magnetisiert.[21] Zu jedem Zeitpunkt einer automationsunterstützten Datenverarbeitung sind diese Zustände klar determiniert. Alles, was der Mensch von einem Computersystem bearbeiten lassen will, muss letztlich auf diese Zustände rückführbar sein. Informationen werden daher von Daten repräsentiert, welche wiederum durch strukturierte Zeichen abgebildet werden, die letztlich durch codierte binäre Darstellungseinheiten[22] auf den zwei physikalischen Zuständen beruhen (Information – Daten – Zeichen). Dabei muss die Repräsentation stets so gewählt werden, dass sich die Information durch Interpretation der Repräsentation zurückgewinnen lässt (Abstraktion).[23] Im Wesentlichen beruht die Interaktion des Nutzers mit dem datenverarbeitenden Computersystem auf einer »funktionalen Abstraktion«, da er sich um das »Was er will« bemühen muss, nicht aber darum, »Wie«[24] das »Was« erreicht wird.[25] Der Informationsaustausch erfolgt lediglich über Umweltschnittstellen der Datenein- bzw Datenausgabe.

2. Digitalisierung und Automatisierung

Aufgrund der der automationsunterstützten Datenverarbeitung immanenten Digitalisierung, dh der Umwandlung analoger Daten in eine digitale Form, ist es möglich, bei reduziertem Speicherbedarf eine viel größere Datenmenge über physikalische Medien zu übertragen.[26]

Der Computer ist ein Werkzeug, das durch Automatisierungsfunktionalitäten in der Lage ist, Handlungsabläufe durch Verselbstständigung zu steigern, viel komplexere Berechnungen in relativ kurzer Zeit durchzuführen[27] und dadurch freie Ressourcen zu schaffen. Als eine Erscheinungsform der Computerkriminalität sind an dieser Stelle

21 Dafür hat sich die Darstellungsform 1 (Strom fließt) und 0 (Strom fließt nicht) durchgesetzt.
22 Das sind die kleinsten Darstellungseinheiten (»Bit« für »binary digit«).
23 Vgl *Gumm/Sommer,* Einführung in die Informatik[10] (2013) 4 bzw 34 f.
24 Damit haben sich die Programmierer der Anwendungsprogramme befasst.
25 Vgl *Balzert,* Lehrbuch Grundlagen der Informatik[2] (2005) 254.
26 Vgl *Mayer-Schönberger,* Information und Recht. Vom Datenschutz bis zum Urheberrecht (2001) 6.
27 Wofür ein begabter Mensch ohne Computerunterstützung oft ein Leben lang rechnen müsste.

DDoS-Attacken zu nennen, bei denen idR über sog »Botnets«[28] automatisierte Angriffe auf Zielsysteme durchgeführt werden. In vielen Fällen wird bereits das Bot-Netzwerk durch programmgesteuerte Automatisierungstechnik aufgebaut, indem bspw Software-Tools verwendet werden, die selbstständig port- bzw vulnerability-scans an den einzelnen Hosts[29] im Internet durchführen und geeignete Systeme in weiterer Folge mit entsprechenden »Backdoor«-Programmen[30] infiltrieren.

3. Universalität

Der Computer ist universell und multifunktional einsetzbar. Die Hardware ist nicht nur für die Durchführung bestimmter Aufgaben gebaut (wie dies etwa bei einem mechanischen Rechner der Fall ist), sondern für die Bewältigung aller Aufgaben ausgelegt, die von entsprechend programmierter Software bewältigt werden können. Die Problemlösungsvorschriften müssen daher von den Computerprogrammen kommen, welche nach den Universalrechnerprinzipien[31] von *von Neumann*[32] in Abhängigkeit bzw im Zusammenspiel mit der unverändert bleibenden Hardware für die programmgemäßen Handlungsschritte verantwortlich sind.[33]

---

28 »Botnet« ist das zusammengesetzte Kurzwort für »robot network«; »bot« wird im einschlägigen Jargon für »robot« (engl für »Roboter«; tschechisch: robota »Zwangsarbeit«) verwendet und beschreibt ein Computerprogramm bzw Computersystem, das weitgehend selbstständig Aufgaben ausführen kann; siehe *Tanenbaum,* Moderne Betriebssysteme[3] (2009) 772. Das Wort »Robot« geht auf den tschechischen Dramatiker *Karel Čapek* zurück, dessen Theaterstück vom Jahr 1921 den Titel »R.U.R.« (Rossum's Universal Robots) trug. Er leitete das Wort »robot« vom tschechischen Wort für Zwangsarbeit »robota« ab (siehe dazu *Nehmzow,* Mobile Robotik [2002] 7).

29 »Host« (engl für Gastgeber) bezeichnet jeden Computer, der an ein Netzwerk angeschlossen ist und mit anderen Systemen kommuniziert; siehe *Kersken,* IT-Handbuch für Fachinformatiker[5] (2011) 181.

30 Dabei handelt es sich um eine Unterkategorie der in der IKT als »Trojanische Pferde« bezeichneten Schadprogramme (siehe S 89 ff).

31 Nach dem theoretischen Modell eines Computers nach *von Neumann* besteht ein solcher aus fünf Funktionseinheiten (Eingabewerk, Ausgabewerk, Rechenwerk, Steuerwerk und Speicher); siehe *Burks/Goldstine/von Neumann,* Preliminary discussion of the logical design of an electronic computing instrument (1946) 92 ff; vgl auch *Kersken,* IT-Handbuch[5], 111; *Tanenbaum,* Computerarchitektur[5] (2006) 35.

32 Die Beschreibung der Funktionsweise eines Computers als »Universalrechner« nach *von Neumann* aus dem Jahr 1946, ist im Wesentlichen heute noch gültig.

33 Vgl *Schramm,* Informationstechnologie: Ausgewählte Themen, in Jahnel/Schramm/Staudegger (Hrsg), Informatikrecht[2] (2003) 1 (3).

Auf Grundlage dieser heute noch üblichen Grundkonzeption eines Computers (wie sie etwa in PCs, Hochleistungsrechnern, Smartphones und Tablet-PCs realisiert ist) konvergieren in dieser Funktionseinheit aus Hard- und Software für den Nutzer unmittelbar verwendbare Anwendungsprogramme ebenso wie mittelbare Übertragungsfunktionalitäten im Sinne einer virtuell bereitgestellten Infrastruktur für weitere digitale Dienste bzw Kommunikationsformen. Dies alles bei simultaner Nutzbarkeit der unterschiedlichsten Programme. Im Wesentlichen beschreiben solche Vorgänge, die dem Nutzer real vorhandene Ressourcen und Dienste bloß suggerieren, eine wesentliche Methode der Abstraktion, nämlich die Virtualisierung.

4. Virtualisierung, Ubiquität und immanente Transnationalität

Durch die Virtualisierung können physische Beschränkungen der Hardware überwunden und dem Nutzer Ressourcen zur Verfügung gestellt werden, die lediglich computerprogrammgesteuert in »entmaterialisierter« Form existieren. Digitale Daten und Programme können daher beliebig reproduziert und distribuiert werden. So können aufbauend auf der Hardware eines einzigen Computers (zB Apple-Plattform) weitere Computer- bzw Betriebssystemumgebungen[34] (zB Windows-Plattform, Linux-Plattform), Mikroprozessoren, Massenspeicher, flüchtige Speicher, Serveranwendungen (wie Application Service Providing) usw emuliert[35] und virtualisiert werden. Auch beim sog »Cloud Computing« werden über das Internet diverse IT-Ressourcen virtuell bereitgestellt.

Datensätze in computertechnisch verarbeitbarer Form (einschließlich Programme) können an unterschiedlichen Orten gleichzeitig sein. Darüber hinaus können räumliche Distanzen durch eine kaum ins Gewicht fallende Latenzzeit, dh quasi ohne Zeitverlust, überwunden werden. Jeder Teilnehmer in einem informationstechnischen Netzwerk ist – wie es auch der OGH sinngemäß zum Ausdruck bringt – der Nachbar jedes anderen.[36] Die Feststellung eines konkreten »Tatorts« (Ort des

34 Man spricht dabei von »Virtueller Maschine« (VM).

35 Ein Emulator ist eine Funktionseinheit, die die Eigenschaften einer Rechenanlage auf eine andere derart übertragen kann, dass Programme, die für die eine Rechenanlage konzipiert sind, auch auf der anderen ablaufen können (vgl DIN 44300).

36 OGH 16.11.2012, 6 Ob 126/12s = jusIT 2013/26, 52 *(Staudegger)* = ÖJZ EvBl-LS 2013/37, 239 *(Rohrer)*.

deliktischen Erfolgseintritts bzw physischer Handlungsort) in einer virtualisierten Umgebung eines globalen Netzwerks, kann sich als äußerst schwierig erweisen und bestenfalls aufgrund (ebenfalls manipulationsanfälliger) digitaler Spuren eruiert werden, wobei man nicht vergessen darf, dass Computerdaten[37] und Computerprogramme in ihrer funktionalen Erscheinungsform stets an Hardware gebunden sind.[38] Sie unterliegen in ihrer unmittelbaren Benutzbarkeit bzw Ausführbarkeit einem strengen Determinismus, da ihre binären Muster physikalische Zustände beschreiben, die zumindest kurzeitig auf einem permanenten Datenträger, flüchtigen Speicher oder auf diversen Übertragungsmedien Verkörperung finden müssen. Gerade die moderne Computerkriminalität steht in einem sehr engen Zusammenhang mit einer sich äußerst rasch weiterentwickelnden globalen Technisierung, die sehr vielseitig ist, aber auch leicht missbraucht werden kann.

Das Faktum der Virtualisierung führt zu einem Abstraktionsgrad jeder informationstechnischen Datenverarbeitung über das Internet, der eine immanente Transnationalität impliziert. Selbst wenn der in der Steiermark befindliche A seinem Hausnachbarn B ein E-Mail sendet, könnten die Daten im Hintergrund – bei kaum wahrnehmbarem Zeitverlust – im Zuge ihres paketvermittelten Transports »globale Distanzen« überwunden haben, um letztlich auf dem Computer von B angekommen zu sein. Die vernetzte Computertechnik bildet eine Instanz der singulären Grenzenlosigkeit bei nahezu zeitgleicher Nutzbarkeit eines virtuellen Handlungsraumes, jedoch mit grundsätzlicher Standort-Bestimmbarkeit jedes einzelnen Akteurs durch digitale Spuren. Die Computerkriminalität ist dementsprechend ein weltumspannendes Phänomen, das sich aufgrund der Internationalität ihrer Akteure idR nicht innerhalb der Grenzen autonomer Staatsgebiete zuträgt, weshalb auch nur eine breit angelegte Strategie zur Bekämpfung derselben zur Durchsetzung eines Strafanspruchs sinnvoll erscheint.[39]

---

37 Der hier verwendete Begriff »Computerdaten« wird im Sinn des Art 1 lit b CCC verstanden: »›computer data‹ means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function«.

38 Siehe *Brodowski/Freiling,* Computerkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft (2011) 23 f.

39 Vgl dazu die Erwägungen der CCC bzw ErlStV 1645 BlgNR XXIV. GP, 2 ff.

5. Entwicklungsdynamik durch Geschwindigkeit und Zunahme des Miniaturisierungsgrads

Computersysteme werden bei zunehmender Leistungsfähigkeit durch Funktionsintegration immer kleiner und schneller. Durch Miniaturisierung steigt zudem die Mobilisierungsrate, sodass in Hinkunft – wenn nicht schon heute realisiert – sämtliche gebräuchliche Alltagsgeräte (wie Kühlschränke, Waschmaschinen, Kraftfahrzeuge, intelligente Stromzähler, Fernsehapparate, Schlüsselanhänger, Fahrräder usw) mit Hochtechnologien als intelligente Systeme Teil des »Internet der Dinge« sein werden. Alltagsdinge, die den Menschen im Leben umgeben, konvergieren mit individualisierten Informationen und vernetzen[40] sich unbemerkt (sog »Pervasive Computing«[41]) zu einer Allgegenwärtigkeit der IKT (»Ubiquitous Computing«). Dadurch wird es möglich sowohl den »lifecycle« von solchen Gebrauchsgegenständen zu verfolgen als auch dessen Nutzung faktisch zu determinieren.[42] Darüber hinaus werden diese Gegenstände in der Lage sein selbstständig – vom Menschen faktisch unbemerkt – untereinander zu interagieren.[43]

Die Allgegenwart der IKT in der Vereinigung des Pervasive Computing wird in naher Zukunft nicht nur für das Strafrecht, sondern für sämtliche Rechtsdisziplinen eine große Herausforderung werden.

---

40 ZB durch RFID-Technik.

41 »Pervasive Computing« bezeichnet die Durchdringung von Alltagsgegenständen mit Datenverarbeitung bzw IKT. »Ubiquitous Computing« wird als Überbegriff der Allgegenwart von IKT verwendet (zu den Begrifflichkeiten siehe *Malaka/Butz/Hußmann,* Medieninformatik. Eine Einführung [2009] 275).

42 Siehe *Staudegger,* Sachenrechtliche Implikationen des »Internet der Dinge«, in Schweighofer/Geist/Staufer (Hrsg), Globale Sicherheit und proaktiver Staat – Die Rolle der Rechtsinformatik. Tagungsband des 13. Internationalen Rechtsinformatik Symposions IRIS 2010 (2010) 413 (413 ff).

43 Siehe dazu vertiefend *Hödl,* Ubiquitous Computing und soziale Gerechtigkeit, in Schweighofer/Geist/Staufer (Hrsg), Globale Sicherheit und proaktiver Staat – Die Rolle der Rechtsinformatik. Tagungsband des 13. Internationalen Rechtsinformatik Symposions IRIS 2010 (2010) 419 ff.

II. Begriffe, Definitionsansätze, Abgrenzungen und Entwicklungen

A. Zum Wesen und Begriff der »Computerkriminalität«[44]

Zu einer Zeit, in der universelle Rechenanlagen – wofür sich der Begriff »Computer« eingebürgert hat – bereits erfunden, aber bei weitem nicht für den Heimgebrauch und eine gesellschaftliche Durchdringung geeignet und gedacht waren, überlegte man schon, ob es sich bei der Vorstellung von »Computerkriminalität« um bloße Fantastereien oder ernst zu nehmende Realität handle.[45] Wenige Zeit später wurde jedoch auch empirisch nachgewiesen, dass die Computerkriminalität tatsächlich eine reale Bedrohung darstellt.[46]

Der Terminus »Computer« (lat computare[47]) hat sich aus dem Namensteil eines der ersten Einzelrechner »Electronic Numerical Integrator and Computer«[48] bald als Gattungsbegriff für elektronische Datenverarbeitungsanlagen etabliert, die in der Lage sind, (softwaregestützte) Rechenvorschriften abzuarbeiten. Die technisch

---

44 Engl »Computer Crime« oder »Computer-related Crime«, häufig auch »Cybercrime«. Der im heutigen Sprachgebrauch manifestierte Begriff(-steil) »Cyber« wird als Kurzwort für »Cybernetics« (griech Kybernetes = Steuermann) verstanden und wurde grundlegend ua von *Norbert Wiener* geprägt, der 1948 in »Cybernetics or Control and Communication in the Animal and the Machine« Modelle der Rückführung von Informationen und Bedeutung für die Selbstorganisation und Selbststeuerung von Menschen und Lebewesen vorstellte (die deutsche Übersetzung erschien 1968 unter dem Titel »Kybernetik. Regelung und Nachrichtenübertragung in Lebewesen und Maschine«); siehe zur Begrifflichkeit »Cyber« ausf *Faßler,* Cyber-Moderne. Medienevolution, globale Netzwerke und die Künste der Kommunikation (1999) 28 f; der Begriff »Cyberspace« wiederum wurde im Science-Fiction-Roman »Neuromancer« (1984) des amerikanisches Autors *William Gibson* verwendet, der damit eine künstliche Welt im Computer bezeichnete (vgl *Brush,* Cyberspace, in Jones [Ed], Encyclopedia of New Media [2003] 112 [112 ff]; weiters *Seifert,* Electronic-Commerce – Mobile-Commerce – Social-Commerce Guide. Lexikon mit den relevanten Definitionen und KPIs in der digitalen Welt [2013] 106).

45 Siehe etwa zur kontroversen Diskussion in Deutschland *Betzl,* Computerkriminalität – Dichtung und Wahrheit, DSWR 1972, 317 ff; *Betzl,* Computerkriminalität – Viel Lärm um Nichts, DSWR 1972, 475 ff; *Lampe,* Computerkriminalität – nur fauler Zauber, DSWR 1974, 242 f; *Sieben/von zur Mühlen,* Computerkriminalität – nicht Dichtung, sondern Wahrheit, DSWR 1972, 397 ff; *Sieben/von zur Mühlen,* Computerkriminalität – Viel Lärm um Nichts?, DSWR 1972, 252 ff.

46 Siehe zB bei *Sieber,* Computerkriminalität und Strafrecht[2] (1980).

47 »Rechnen«.

48 Siehe zur Geschichte des Computers *Tanenbaum,* Computerarchitektur[5], 30 ff.

bedingte wechselseitige Abhängigkeit von einem physikalisch materiellen, universell einsetzbaren Apparat (Hardware) und immateriellen Computerprogrammen und Daten (Software) wird in der Informatik als »Computersystem« bezeichnet.[49] »Universell« bedeutet in diesem Zusammenhang, dass ein solches System bei unveränderter Hardware prinzipiell alle programmierbaren Aufgaben bearbeiten kann.[50]

Der Begriffshof des Begriffs »Computer« als Wortteil im Begriff »Computerkriminalität« umfasst nicht nur Rechenanlagen (iSv Hardware) oder automationsunterstützt verarbeitbare Daten (iSv Software) im Einzelnen bzw Computersysteme in ihrer Gesamtheit (iSv Hard- und Software), sondern steht als – aus einer umgangssprachlichen Entwicklung hervorgegangenes – Synonym für sämtliche informations- und kommunikationstechnologischen[51] Vorgänge. Die in der Digitaltechnik fußende Konvergenz von Informationstechnologie und Kommunikationstechnologie führt im Großen und Ganzen zur Symbiose dieser Technologien, wobei der Computer bei allen technologischen Entwicklungen und Erscheinungsformen auf diesem Gebiet notwendigerweise das zentrale Element bleibt.

Der Begriff »Computerkriminalität« entstammt in Deutschland einer Studie von *von zur Mühlen,* der darunter jedes deliktische Handeln versteht, »bei dem der Computer Werkzeug oder Ziel der Tat ist«.[52] Dementsprechend sei der Begriff weit auszulegen und erfasse sämtliche Erscheinungsformen strafwürdigen bzw strafbaren Verhaltens, welche mit dem Computer in irgendeiner Weise zusammenhängen.[53] Dabei berühren die strafbaren Verhaltensweisen nicht nur einzelne Datenanwendungen, sondern die gesamte EDV-Landschaft.[54] So weit kann es mE aber nicht gehen, dass der Begriff der Computerkriminalität in

---

49 *Balzert,* Lehrbuch², 4 und 31; vgl Prinzipielles über die Funktionsweise eines Computers auch bei *Schramm* in Jahnel/Schramm/Staudegger, Informatikrecht³, 1 (2) bzw *Sonntag,* Informationstechnologie: Grundlagen, in Jahnel/Mader/Staudegger (Hrsg), IT-Recht³ (2012) 1 (6 ff).

50 Die Formulierung der Funktionsprinzipien des »Universalrechners« von 1946 gehen auf *John von Neumann* zurück; siehe dazu bspw *Tanenbaum,* Computerarchitektur⁵, 35.

51 In weiterer Folge »IT« bzw »IKT«.

52 Siehe *von zur Mühlen,* Computer-Kriminalität, Gefahren und Abwehrmaßnahmen (1972) 17.

53 Vgl *Uepping,* Computermißbrauch ... aus Sicht der Informatik – Betrachtungen zur Computerkriminalität, DSWR 1985, 323 (334).

54 Siehe *Uepping,* DSWR 1985, 323 (334).

eine Richtung verstanden wird, die auch Verhaltensweisen umfasst, bei denen bloß die Hardware eines Computers beschädigt oder weggenommen wird oder die bloß apparative Ausstattung eines Computers als Tatmittel, zB durch den Wurf eines Computers durch eine Fensterscheibe im Zuge eines Einbruchsdiebstahls, Verwendung findet. Enger formuliert es bereits *Sieber*[55], der darunter im Wesentlichen nur rechtswidrige Vermögensverletzungen[56] zusammenfasst, die durch Computermanipulation, Computersabotage, Computerspionage und Zeitdiebstahl[57] realisiert werden. Auch die OECD schränkte diesen Begriff in ihrer Untersuchung im Jahr 1986 auf informationstechnologische Verarbeitungsweisen ein, da sie von »any illegal, unethical, or unauthorized behaviour relating to the automatic processing and the transmission of Data« sprach.[58] In Österreich schloss man sich seit Aufkommen der Diskussion über diese modernen Kriminalitätsformen mehrheitlich dem Verständnis nach *von zu Mühlen* aus Deutschland an.[59]

1. Der Computer als End- oder Zwischenziel deliktischen Handelns

Jaburek/Schmölzer, die grundlegend die Diskussion in Österreich geprägt und begleitet haben, wollen dabei aber keine Unterteilung in Teilbereiche (zB Computermanipulation, Computersabotage, Computerspionage und Zeitdiebstahl) vornehmen, wie sie in Deutschland

55 Vgl *Sieber,* Computerkriminalität², 29 ff und 188; *Sieber,* The Handbook on Computer Crime, Computer-related Economic Crime and the Infringements of Privacy (1986) 31; *Sieber,* Der strafrechtliche Schutz der Information, ZStW 1991/103, 780 mwN; siehe *Uthemann,* Computerkriminalität, in Sieverts/Schneider (Hrsg), Handwörterbuch der Kriminologie. Bd 5 (1998) 265 (266).

56 Im Zusammenhang mit anderen Rechtsgütern spricht *Sieber* von der Computerkriminalität in einem weiteren Sinn *(Sieber,* Computerkriminalität², 29 f).

57 Siehe zu diesen Teilbereichen auch bereits *von zur Mühlen,* Computer-Kriminalität, 14 ff.

58 *OECD,* Computer-Related Crime: Analysis of Legal Policy, ICCP Series No 10 (1986) 7.

59 Siehe dazu *Tiegs,* Computerkriminalität – Probleme ihrer legistischen Erfassung, JBl 1986, 708; weiters vertiefend *Schick/Schmölzer,* Das österreichische Computerstrafrecht – eine Bestandsaufnahme EDVuR 1992, 107 mwN und Statistiken; weiters *Jaburek/Schmölzer,* Computer-Kriminalität (1985) 20 f; instruktiv *Schmölzer,* Entwicklung von Gesetzgebung und Rechtsprechung in Computer-Strafsachen, in BMJ (Hrsg), Strafrechtliche Probleme der Gegenwart. 16. Strafrechtliches Seminar 1988 (1989) 195 (195 ff); *Schmölzer,* Computer-Netzwerke und Strafrecht – eine internationale Herausforderung, in Terlitza/Schwarzenegger/Boric (Hrsg), Die internationale Dimension des Rechts, FS Posch (1996) 321 (323 f).

und der Schweiz[60] diskutiert wurde, sondern orientieren sich an der Zweiteilung des Computers als »End- oder Zwischenziel« deliktischen Handelns.[61] Sie begründen dies damit, dass sich die rechtlichen Schutzmöglichkeiten von Hardware, Software und Daten stark voneinander unterscheiden würden und ihnen daher eine solche Gliederung für die rechtswissenschaftliche Betrachtung geeigneter erscheine.[62] Der Computer sei demzufolge dann das Endziel, wenn durch eine Wechselwirkung des Täters mit dem Computer ein als strafwürdig empfundener Tathergang seinen Abschluss findet. Dient hingegen der Rechner nur als Hilfsmittel und wird die eigentlich schädigende Handlung zwar durch den Computer ausgelöst, nicht aber an diesem ausgeführt, so sei der Computer bloß das Zwischenziel der Handlung.[63] Anders als die Untergliederung von *von zur Mühlen*[64] in Zeitdiebstahl, Computermanipulationen, Computerspionage und Computersabotage knüpfen *Jaburek/Schmölzer* für eine weiterführende Einteilung an das Angriffsziel an, welches sie in den Bestandteilen eines Computersystems – Hardware, Software oder Daten[65] – konkretisieren.[66] *Schick/Schmölzer* führen dazu aus: »Erst wenn geklärt ist, welches Angriffsobjekt betroffen ist, kann es interessieren, durch welche Art von Tathandlung der Eingriff geschehen ist: ein Wegnehmen im Sinn eines Kopiervorganges etwa oder ein Verändern bzw Zerstören iS einer Software- oder Datenmanipulation bzw -sabotage. Erst aufgrund dieser Aufspaltung sollte dann die strafrechtliche Subsumtion erfolgen.«[67]

---

60 Vgl dazu ua *Rohner,* Computerkriminalität. Strafrechtliche Probleme bei »Zeitdiebstahl« und Manipulationen (1976) 4.

61 Siehe *Jaburek/Schmölzer,* Computer-Kriminalität, 22 f; weiters *Schmölzer,* Computer-Kriminalität: Probleme und Reformbestrebungen – national/international, in Arbeitsgemeinschaft für Datenverarbeitung (Hrsg), Quo vadis EDV? – Realität und Vision. 8. Internationaler Kongress Datenverarbeitung im Europäischen Raum (1987) 724 (725); *Schmölzer,* Computer-Kriminalität – kriminologische und kriminalpolitische Überlegungen, in Jehle/Maschke/Szabo (Hrsg), Strafrechtspraxis und Kriminologie², FS Göppinger (1990) 237 (242 f).

62 Siehe dazu die Matrix in *Jaburek/Schmölzer,* Computer-Kriminalität, 22.

63 Vgl *Jaburek/Schmölzer,* Computer-Kriminalität, 23.

64 Vgl grundlegend *von zur Mühlen,* Computer-Kriminalität, 14 ff.

65 Klarzustellen ist, dass die AutorInnen unter Software ausschließlich Programme verstehen und unter Daten »Information, deren Verarbeitung der Zweck der Computerinstallation ist, zB Buchhaltungskonten und deren Stände« vgl *Jaburek/Schmölzer,* Computer-Kriminalität, 18.

66 Siehe *Schick/Schmölzer,* EDVuR 1992, 107; *Schmölzer* in BMJ, Strafrechtliche Probleme der Gegenwart 1989, 195 (201).

67 Siehe *Schick/Schmölzer,* EDVuR 1992, 107.

Meines Erachtens sollte sich die Computerkriminalität gerade nicht über den »Computer als End- oder Zwischenziel« deliktischen Handelns definieren, sondern über IKT-spezifische Handlungsweisen bezüglich des »deliktischen Handelns« selbst. Meiner Auffassung nach sind es nämlich die »spezifischen Wesensmerkmale« der IKT, welche Computerkriminalität ausmachen.

2. Der eigene Definitionsansatz

Um den Begriff klar und sinnvoll zu determinieren, ist mE ausschließlich auf informationstechnisch[68] gebundene Vorgänge bzw Verhaltensweisen abzustellen, mit denen sich strafwürdige Handlungen bezüglich Computersystemen oder automationsunterstützt verarbeiteten (Computer-)Daten[69] realisieren lassen bzw auswirken. Dass bereits auf »strafwürdige« Verhaltensweisen abgestellt wird, hat den Sinn auch hins ihres Unrechtsgehalts als kriminell empfundene, neue Erscheinungsformen der Computerkriminalität diesem Kriminalitätsfeld thematisch zuzuordnen, selbst wenn nach geltendem Recht noch kein Straftatbestand dafür existiert und dieses Verhalten folglich formal nicht als »kriminell« zu bezeichnen wäre. Die Verquickung mit informations- und kommunikationstechnologisch unterstützten Begehungsweisen ist für das hier behandelte Kriminalitätsbild ein entscheidendes Kriterium für die Abgrenzung zu sonstigen Kriminalitätsformen, bei denen zB Computersysteme in oben beschriebener Weise als konventionelle Tatmittel bzw Handlungs- oder Angriffsobjekte bei strafwürdigen bzw strafbaren Verhaltensweisen relevant werden. Gleichwohl bedingt dies, dass Verhaltensweisen von dieser Begrifflichkeit auszunehmen sind, welche sich zwar an mit IKT in Zusammenhang stehenden Objekten im Ergebnis auswirken, die Handlungen aber in konventioneller – analoger – Weise ausgeführt werden. Die Wegnahme eines fremden Datenträgers, selbst wenn sich Daten darauf befinden mögen, fällt daher nicht unter »Computerkriminalität«.[70]

---

68 Darunter versteht man sämtliche »technische Mittel zur Verarbeitung und Übertragung von Informationen« siehe *Brodowski/Freiling,* Computerkriminalität, 15.

69 In diesem Zusammenhang ist darunter die technische Verarbeitungsform sämtlicher auf Computersystemen verarbeitbarer Daten (einschließlich Programmen) gemeint.

70 Andere Meinung *Jaburek/Schmölzer,* Computer-Kriminalität, 22, die den Fall des »Diebstahls einer Systemkomponente« ebenfalls der »Computerkriminalität« zuordnen; ebenso *Rohner,* Computer-Kriminalität, 5.

Für das Abziehen des Netzsteckers eines Computersystems, um dessen Stromversorgung zu unterbinden, gilt dasselbe.[71] Man denke bspw an die Unbrauchbarmachung von Computerprogrammen durch physische Zerstörung des jeweiligen Datenträgers oder an die Unterdrückung von Daten durch Wegnahme des Massenspeichers. Allerdings ist eine Datenunterdrückung, die durch digitale Verschlüsselungstechniken, wie zB im Fall der bereits angesprochenen »Ransomware«[72], realisiert wird, wiederum der Computerkriminalität zuzuordnen. Ein Computersystem kann folglich nur in seiner spezifischen Eigenschaft als eine datenverarbeitende Vorrichtung zum Ziel von diversen Erscheinungsformen der »Computerkriminalität« werden, nicht hingegen soweit seine rein physische Beschaffenheit betroffen ist. Für Computerdaten gilt eine solche Differenzierung in ähnlichem Maße, wobei zu unterscheiden ist, ob der Täter auf konventionellem oder automationsunterstütztem Weg Daten manipuliert oder mit ihnen als digitale Tatwerkzeuge gegen Computersysteme vorgeht. Die alleinige Abgrenzung des Computers bzw der Daten als Tatmittel oder Tatobjekt ist daher mE unzutreffend, vielmehr kommt es auf rein IKT-gebundene Verhaltensweisen an.[73] Löscht jemand Daten, über die er nicht verfügen darf, durch entsprechende informationstechnische Maßnahmen (Delete- oder Formatierungsbefehl usw), fällt dieses Vorgehen bereits unter den Begriff der Computerkriminalität. Es ist für diese Kategorisierung nicht notwendig, die anvisierten Computerdaten darüber hinaus noch als Tatobjekte zu identifizieren. Auch kommt es für das kriminologische Konstrukt der Computerkriminalität nicht darauf an, dass lediglich verpönte Schadprogramme (sog »Malware«[74]) als Tatmittel zum Einsatz gelangen. Sozial adäquate IKT-Nutzungen reichen prinzipiell dafür aus, sofern dadurch ein strafrechtliches Unrecht verwirklicht wird (zB ununterbrochenes Versenden unzähliger E-Mails an das

71 Siehe dazu unten zur Störung der Funktionsfähigkeit eines Computersystems (§ 126b).

72 Vgl das als »Polizei-Virus« bekanntgewordene Schadprogramm.

73 Dagegen wird in der Lehre vom Computer als »End- oder Zwischenziel« deliktischen Handelns gesprochen; vgl *Jaburek/Schmölzer,* Computer-Kriminalität, 19 ff; weiters *Schmölzer* in Arbeitsgemeinschaft für Datenverarbeitung, Quo vadis EDV?, 724 (725); ähnlich *Wegscheider,* Computerstrafrecht, in BMJ (Hrsg), Strafrechtliche Probleme der Gegenwart. 17. Strafrechtliches Seminar 1989 (1990) 127 (130).

74 »Malicious Software«; siehe dazu ausf *Bergauer,* Malware aus strafrechtlicher und verwaltungsstrafrechtlicher Sicht (Dissertation 2005) 8.

Opfer, um es zu belästigen[75], Übermitteln eines gefälschten E-Mails, um das Opfer zur Bekanntgabe sensibler Zugangsdaten zu veranlassen[76], widerrechtliche Benutzung einer entfremdeten Bankomatkarte samt ausspionierter PIN[77] an einer Bankomatkassa[78] oder an einem Bankomaten, computertechnisches Verschlüsseln fremder Daten[79]). In all diesen Fällen kann selbstverständlich weiter untersucht werden, ob die IKT als Tatmittel gebraucht oder als Tatobjekt anvisiert wurde. Eine solche Kategorisierung ist allerdings mE vernachlässigbar, weil gerade die spezifischen Eigenschaften der Informationstechnologie eine eindeutige Zuweisung in den unterschiedlichsten Erscheinungsformen der Computerkriminalität verhindert.

Die Einschränkung auf gewisse Individual- bzw Universalrechtsgüter (wie zB ausschließlich auf das »Vermögen«[80]) hat mE ebenso zu unterbleiben, solange an ihnen ein vom Strafrecht zu schützender Wert zu konstatieren ist[81] (zB Privatsphäre, Interesse am Fortbestand von Daten, Interesse an der Verfügbarkeit von Daten und Computersystemen, Vertrauen auf die Echtheit und Zuverlässigkeit elektronischer Dokumente, Vertrauen in die Sicherheit und Zuverlässigkeit des Zahlungsverkehrs mit unbaren Zahlungsmitteln).

3. Täterorientierte Einteilung der Computerkriminalität

Eine Fokussierung auf spezielle fachliche bzw persönliche Eigenschaften des Täters (zB gut ausgebildete Programmierer und Techniker, Hackergruppen, Systemverantwortliche) für eine kriminologische Einordnung von konkreten Straftaten, hat lediglich eine äußerst schwache Kennzeichnungsrelevanz und sollte daher vermieden werden. Ein nicht in IT-Angelegenheiten ausgebildeter oder interessierter Täter kann ebenso wie typische Hacker, Cracker, Script Kiddies[82] oder Viren-Programmierer Computerstraftaten begehen, etwa durch wider-

75 Vgl dazu »Cyber-Stalking«.
76 Vgl auch »Phishing«.
77 »Persönliche Identifikationsnummer«.
78 Sog »POS-Terminal« (Point of Sale-Terminal).
79 Vgl dazu die »informationstechnische Datenunterdrückung«.
80 Vgl *Sieber,* Computerkriminalität², 188.
81 Exakterweise würde man andernfalls nicht von »Kriminalität« sprechen können.
82 Siehe zu den einzelnen Begrifflichkeiten *Pfister,* Hacking in der Schweiz (2008) 77 ff und 90 ff; weiters *Russell/Cunningham,* Das Hacker-Buch (2001) 24 ff.

rechtliche Geldbehebung mit einer entfremdeten Bankomatkarte an einem Bankomaten oder durch Fälschung elektronischer Dokumente wie E-Mails oder anderer digitalisierter und ausstellerspezifischer Schriftsätze. Freilich könnte man anhand solcherart ausgewählter Persönlichkeitsmerkmale der Täter bzw Tätergruppen an eine Differenzierung zwischen »schlichter Computerkriminalität« und »qualifizierter Computerkriminalität« denken. Eine gewisse Graduierung nach Sozialschädlichkeit, krimineller Energie oder der Verwendung von Spezialtechnik, würde mE die Computerkriminalität zu sehr als reines Kriminalitätsbild für IKT-Spezialisten unbillig einschränken. Die IKT stellt eine massentaugliche informationstechnische Infrastruktur dar, deren Besonderheit gerade auch darin liegt, dass grundsätzlich jeder Nutzer Opfer wie Täter sein kann. Ein diesbezügliches »Profiling« iS einer täterorientierten Betrachtung nach speziellen Persönlichkeitsmerkmalen des Täters, sollte daher für eine weiterführende Phänomenuntergliederung vermieden werden.

Ganz idS soll der Begriff der Computerkriminalität daher insgesamt weit ausgelegt werden, um auch die stetigen technischen Weiterentwicklungen, die bis dato weitgehend nicht abzuschätzen sind, noch erfassen zu können. Bereits die jüngste Vergangenheit bzw Gegenwart zeigt, wie schnell neue Erscheinungsformen der Computerkriminalität zu Tage treten, aber auch wieder außer Mode geraten können. Es lässt sich daran denken, dass vermutlich nichts so schnelllebig ist wie Entwicklungen im Bereich der Informationstechnologie. Waren es bis vor Kurzem noch – neben den »Klassikern« wie »Hacking« und »Malware« (vgl zB Viren, Würmer, Trojanische Pferde) – Phänomene wie zB »Phishing«, »Pharming«, »Skimming« oder »Denial-of-Service-Angriffe«, so sind es heute bereits auch Erscheinungsformen wie »Cyber-Mobbing bzw -Stalking«, »Cyber-Grooming«, »Rache-Pornos«, »Sexting«, »Flaming«, »Cyberlocker«, »Happy Slapping«, »Internet-Trolle« oder »Scamming« und »Scareware« im Bereich des sog »Social Engineering«, Identitätsmissbräuche und der sog »Hacktivismus«, die hoch im Kurs stehen.[83]

83 Siehe dazu auch *Bergauer/Schmölzer,* Strafrecht, in Jahnel/Mader/Staudegger (Hrsg), IT-Recht[3] (2012) 635 (644 f); zur Phänomenologie ausf *Schmölzer,* ZStW 2011/123, 709 ff.

4. Technik- und menschbezogene Typen der Computerkriminalität

An dieser Stelle ist auch der Ansatz von *Gordon/Ford* anzuführen, welche die Computerkriminalität nach zwei Typen unterscheiden.[84] Auf der einen Seite stellen sie auf die »technikorientierte Cyberkriminalität« (Typ I) ab, welche drei wesentliche Merkmale besitzen soll:

1. Der Angriff besteht idR aus einem singulären Ereignis aus Sicht des Opfers.
2. In vielen Fällen wird dabei Crimeware[85] (Keylogger, Viren, Trojanische Pferde usw) auf den Computersystemen der Opfer zum Einsatz gebracht.
3. Die Infiltration der Systeme kann, muss aber nicht durch das Ausnützen von Sicherheitslücken realisiert werden.

Als Beispiele für diesen Typ I werden Phänomene wie »Phishing«, »Identitätsdiebstahl« und »DDoS-Attacken« angeführt.

Auf der anderen Seite steht als Typ II die »menschbezogene Cyberkriminalität«, die zwei wesentliche Charakteristika aufweise:

1. Für den Angriff wird nicht auf typische Schadsoftware zurückgegriffen, sondern es gelangen übliche Kommunikationsdienste oder Datenübertragungsprotokolle, wie zB Instant Messenger oder FTP, zum Einsatz.
2. Der Angriff stellt sich für das Opfer generell durch wiederholte Kontakte (mit dem Täter) oder Ereignisse dar.

Als Beispiele für Typ II werden zB »Cyberstalking« und »Cyberterrorismus« genannt.[86]

Eine solche Einteilung ist aus meiner Sicht allerdings aus folgenden Gründen abzulehnen:

---

84 Siehe im Folgenden *Gordon/Ford,* On the definition and classification of cybercrime. Journal in Computer Virology 2006, 13 ff: dem folgend offensichtlich *Brodowski/Freiling,* Computerkriminalität, 28 f.

85 Dabei handelt es sich um »Malware«, die zur Begehung einer strafbaren Handlung Verwendung findet; vgl *Gordon/Ford,* Journal in Computer Virology 2006, 13 (18).

86 Vgl *Gordon/Ford,* Journal in Computer Virology 2006, 13 (16).

Die Vielzahl moderner Erscheinungsformen der Computerkriminalität macht eine bloß theoretisch klar abtrennbare Kategorisierung in die hier generierten Typen I und II praktisch unmöglich. Zum einen, weil die Grenzen der Angriffsmethoden verschwimmen und zum anderen, weil die von *Gordon/Ford* aufgestellten Unterscheidungsmerkmale selbst äußerst schwache Kennzeichnungskraft besitzen. So lässt sich »Cyberstalking« (Typ II) auch mittels Crimeware im Zuge eines belästigenden DDoS-Angriffs über Bot-Netzwerke[87] (Typ I) realisieren.[88] Wie wären solche Angriffe zu klassifizieren?

Zu den Unterscheidungsmerkmalen des Typs I ist anzumerken, dass jedes einzelne Charakteristikum sehr vage definiert wird, wobei gerade diese beiden AutorInnen selbst auf die Wichtigkeit einer eindeutigen Begriffsklärung und Differenzierung hinweisen.[89] Die Unsicherheiten zeigen sich vor allem durch die unscharfe Diktion wie »generally« (Axiom 1) oder »often« (Axiom 2) und »can, but may not necessarily« (Axiom 3). Dadurch räumen die AutorInnen aber selbst ein, dass alle diese aufgestellten Kriterien gar nicht zutreffen müssen.

Das Phänomen »Cyberterrorismus« wiederum wird nach den Abgrenzungsmerkmalen von *Gordon/Ford* dem Typ II, der menschbezogenen Cyberkriminalität, zugeordnet, wobei sich auch hier wiederum die Frage stellt, ob eine solche Art Terrorismus tatsächlich auf »wiederholten Ereignissen« basieren muss, wie es Axiom 2 zu Typ II verlangt. Gerade Cyberterrorismus wird in erster Linie mit Malware bzw Crimeware verübt, man denke etwa an die Zwischenfälle mit »Stuxnet«[90] bzw anderer Malware oder DDoS-Tools mit denen zB computergesteuerte kritische Systeme, wie Stromversorgungsanlagen, Kommunikationsinfrastrukturen, Verkehrsleitsysteme, Flugsteuerungsprogramme, Kraftwerke, Gaspipelines manipuliert, zum Absturz gebracht oder fremdgesteuert werden können.

---

87 Siehe unten S 289 ff.

88 Siehe zu diesem Beispiel die Tabelle 1 bei *Gordon/Ford,* Journal in Computer Virology 2006, 13 (16).

89 Siehe *Gordon/Ford,* Journal in Computer Virology 2006, 13 (17).

90 »Stuxnet« ist eine Art »Wurm-Trojaner«, mit dem zB programmierbare Speicherbausteine ua der Pumpen- und Ventilsteuerungssysteme des iranischen Atomkraftwerks in Buschehr infiltriert wurden, um die Geschwindigkeit der Zentrifugen zu beeinflussen und darüber hinaus eine Fernzugriffsmöglichkeit für die Täter über das Internet zu ermöglichen. Siehe dazu *Kröner,* Cyberterrorismus – Definition, Arten, Gegenmaßnahmen (2011) 9 ff.

Abgrenzungsschwierigkeiten ergeben sich aber auch bei vermögensorientierten Angriffen, wie bspw widerrechtlichen Abbuchungen über Online-Banking-Systeme. Hier richtet sich der Angriff gegen ein Individualrechtsgut eines Menschen unter Verwendung technischer Hilfsmittel (zB Internetverbindung, E-Mail, Zugangsdaten, PIN), welche jedoch nicht der Crimeware zuzuordnen sind. Mangels Beeinflussung einer Person, dh sowohl des Opfers, als auch eines Menschen, der über die konkrete Giralgeldtransaktion entscheidet bzw diese ausführt, liegt hier ein nur betrugsähnliches (technikorientiertes) Verhalten vor. Es handelt sich dabei um eine Mischung aus »Phishing« (Typ I) und »Betrug« (Typ II). Der Betrug unter Rückgriff auf technische Mittel ist nach der Auffassung von *Gordon/Ford* in seinem Kern »people-related«.[91] Nun befassen wir uns aber hier mit einem Beispiel, das in seinem Wesen einem »personenbezogenen« Betrug entspricht, aber ohne dass eine Person tatsächlich als Tat- oder Handlungsobjekt in Erscheinung tritt, und das auch »mostly technological in nature« ist.[92]

Zusammenfassend ist zu diesem Ansatz festzuhalten, dass die aufgestellten Abgrenzungskriterien sehr schwammig erscheinen, was eine eindeutige Zuteilung aktueller Phänomene unmöglich macht. Neue Erscheinungsformen der Computerkriminalität, die möglicherweise auf einer noch weiterreichenden Verquickung von technikorientierten und menschbezogenen Verhaltensweisen beruhen, sollen hier noch gar nicht angesprochen werden. Nach *Gordon* und *Ford* liegt der Mehrwert einer solchen Klassifikation darin, dass man anhand dieser Einteilung unterschiedlich ausgebildete Kriminalisten zur Bearbeitung solcher Fälle heranziehen könne. Für Fälle des Typs I könne man daher speziell in IT ausgebildete Ermittlungsakteure einsetzen, währenddessen man für Typ II-Fälle eher auf klassische Ermittler zurückgreifen könne, die mit »menschbezogener Kriminalität« vertraut sind.[93]

Doch auch dieses Zielanliegen ist mE aufgrund der aufgezeigten Unschärfen der Thesen selbst wie auch der faktischen Gegebenheiten dieses technikspezifischen Kriminalitätsfeldes nicht wirklich gewinnbringend. Vielmehr ist zur Ausbildung entsprechender Ermittler an-

91 Vgl *Gordon/Ford,* Journal in Computer Virology 2006, 13 (15).

92 Siehe dazu ausf die strafrechtliche Betrachtung eines Phishing-Angriffs bzw die Unterscheidungsmerkmale des § 146 von § 148a unten.

93 Vgl *Gordon/Ford,* Journal in Computer Virology 2006, 13 (19); dem folgend auch *Brodowski/Freiling,* Computerkriminalität, 29.

zumerken, dass eine gewisse fachliche Qualifikation in beiden dieser kriminalistischen Ansätze gleichermaßen zur Verfolgung der Computerkriminalität sinnvoll wäre. KriminalbeamtInnen, StaatsanwältInnen und RichterInnen sollten zumindest mit ausreichendem technischen »Beurteilungswissen«[94] ausgestattet werden, um besser mit aktuellen und zukünftigen Phänomenen der Computerkriminalität in technischer, spezifisch dogmatischer und sozialer Hinsicht umgehen zu können. Es darf vorweggenommen werden, dass mE eine Sonderzuständigkeit für den Bereich des Computerstrafrechts beim Einzelrichter des Landesgerichts angebracht wäre, nicht auch zuletzt deshalb, weil viele der einschlägigen technikspezifischen Delikte aufgrund ihrer Strafdrohungen in die sachliche Zuständigkeit des Bezirksgerichts fallen, bei denen die Anklageseite »nur« von der Bezirksanwältin bzw dem Bezirksanwalt vertreten wird.

5. Computerkriminalität und Wirtschaftskriminalität

An dieser Stelle ist zu erwähnen, dass die Computerkriminalität nicht (vollständig) der Wirtschaftskriminalität untergeordnet werden kann.[95] Freilich können wirtschaftsbezogene Verhaltensweisen, hohe Schadensbeträge, wie auch ggf volkswirtschaftliche Beeinträchtigungen bzw ökonomische Motive hinter einzelnen Erscheinungsformen der Computerkriminalität stehen[96], doch erfasst diese vor allem auch Schädigungen von (höchstpersönlichen) Einzelinteressen[97], Verursachungen bloß geringer Schäden an Computerdaten bzw Computersys-

94 Siehe dazu grundlegend *Schramm* in Jahnel/Schramm/Staudegger, Informatikrecht², 1 (2) in Fortführung nunmehr *Sonntag* in Jahnel/Mader/Staudegger, IT-Recht³, 1 (2).

95 Vgl bereits *Lenckner,* Computerkriminalität und Vermögensdelikte (1981) 14; Eine Darstellung dieses Kriminalitätsfelds in der Fachliteratur zur Wirtschaftskriminalität – so etwa *Köck,* Wirtschaftsstrafrecht. Eine systematische Darstellung² (2010) 104; *Eder-Rieder,* Einführung in des Wirtschaftsstrafrecht³ (2014) 191 – ist solange unbedenklich, als sie nicht dazu führt, dass suggeriert wird, die Computerkriminalität ließe sich eindeutig der Wirtschaftskriminalität zu- bzw sogar unterordnen. Hingegen sieht *Rohner,* Computerkriminalität, 8 mwN, die Computerkriminalität tatsächlich als Teil der Wirtschaftskriminalität an.

96 Vgl ua *H. Steininger,* Typische Erscheinungsformen der Wirtschaftskriminalität und ihre Bekämpfung, ÖJZ 1982, 589; *Burgstaller,* Wirtschaftsstrafrecht in Österreich, JBl 1984, 577; *Rauch,* Korruptionsstrafrecht (2012) 17 und 19 ff.

97 ZB im Fall des Cyber-Stalking oder Cyber-Mobbing.

temen[98] und insb IKT-gebundene Verhaltensweisen[99], ggf auch unabhängig von einem computerspezifischen Rechtsgut[100].[101] Auf eine hohe Sozialschädlichkeit[102] ist daher ebenso wenig abzustellen wie auf die von *Liebscher*[103] geforderte Serienmäßigkeit und Internationalität zur Definition der Wirtschaftskriminalität. Letztere Kriterien vermögen es mE schon aufgrund der Tatsache, dass solche Merkmale der zur Computerkriminalität Bezug habenden IKT wesensimmanent sind, nicht, Entscheidendes für eine eindeutige Determinierung beizutragen. Es verbleiben daher als Schnittstelle zwischen Wirtschaftskriminalität und Computerkriminalität im Wesentlichen nur tatsächliche »IKT-gebundene Begehungsweisen« zur Realisierung von (echten) Wirtschaftsstraftaten. Aktuelle Phänomene, wie zB Cyberterrorismus, Cyber-Mobbing, Hacktivismus, »Happy Slapping«[104], »Rache-Pornos«[105],

98 Zu denken wäre an das Löschen von persönlichen Computerdaten (zB digitale Bilder oder Liebesbriefe), welche einen bloßen Affektionswert für den Verfügungsberechtigten besitzen. Dasselbe gilt sinngemäß für das Herbeiführen einer Funktionsstörung eines fremden Computersystems eines Heimanwenders (zB Notebook eines Studierenden) durch DoS-Attacken oder Computerwürmer.

99 Informationstechnisches Löschen oder Manipulieren von Computerdaten, Eingeben von Computerdaten zur Manipulation von Online-Banking-Systemen oder Geldautomaten, Fälschung elektronischer Dokumente, Abfangen bzw Ausspionieren von Daten am computer- bzw telekommunikationstechnischen Übertragungsweg, »Hacken« fremder Computersysteme usw.

100 ZB das Herunterladen von Kinderpornographie im Internet, das Beharrliche Verfolgen bzw Belästigen einer Person durch IKT-Mittel, das Chatten mit Unmündigen im Internet, um diese in weiterer Folge sexuell zu missbrauchen, das Verbreiten bzw Herunterladen von terroristischen Anleitungen via Internet.

101 Ebenso kritisch gegenüber der vollständigen Einordnung der Computerkriminalität unter die Wirtschaftskriminalität *Schmölzer* in FS Göppinger², 237 (243 f), die allerdings letztlich zwischen beiden Positionen vermittelnd den Kernbereich der Computerkriminalität als »ein neues, durch die ins Wirtschaftsleben integrierten technischen Entwicklungen bedingtes Phänomen der Wirtschaftskriminalität« anerkennt.

102 Wie es etwa *Schick* zur Typisierung der Wirtschaftskriminalität vorsieht, vgl *Schick,* Die Bekämpfung der Wirtschaftskriminalität in Österreich mit den Mitteln des Strafrechts, in BMJ (Hrsg), Strafrechtliche Probleme der Gegenwart. 5. Strafrechtliches Seminar 1977 (1978) 98 (98 ff).

103 Vgl *Liebscher,* Grundfragen des Wirtschaftsstrafrechts, JBl 1979, 225.

104 Engl für »fröhliches Schlagen«; Beim »Happy-Slapping« werden (konventionelle) Straftaten – wie zB Beleidigung, Körperverletzung, Raufhandel, Nötigung, Vergewaltigung – mit einem Videoaufnahmesystem (wie zB Mobiltelefon, Digitalkamera) aufgezeichnet und im Wege der Telekommunikation bzw mittels Computersystemen anderen Personen zugänglich gemacht bzw im Internet veröffentlicht; vgl 82/ME XXIV. GP, 7.

105 Ohne Zustimmung des Ex-Partners werden Nackfotos bzw Filme von geschlechtlichen Handlungen ins Internet gestellt, um den Ex-Partner bloßzustellen.

informationelle Verbreitung von Kinderpornographie bzw nationalsozialistischer Propaganda haben allerdings per se nichts mit dem Wirtschaftsleben gemein.

Darüber hinaus gibt es in Ö – zumindest zurzeit und soweit überschaubar – nur eine einzige eindeutig wirtschaftsspezifische Strafbestimmung die dem Bereich des Computerstrafrechts zugeordnet werden kann, nämlich § 10 ZuKG, wodurch sämtliche Handhabungen von Umgehungsvorrichtungen zu geschützten Diensten (zB Pay-TV), welche sowohl körperliche Gerätschaften (Hardware) als auch unkörperliche Computerprogramme (Software) sein können, erfasst werden. Soweit nun jemand Computerprogramme als solche Umgehungsvorrichtungen im informationstechnischen Weg zB herstellt, verbreitet oder auch nur durch Speicherung auf einem Datenträger innehat, handelt es sich dabei um Computerkriminalität ebenso wie (zumindest nach einigen Definitionsansätzen) um Wirtschaftskriminalität. Dies nicht zuletzt, weil § 10 ZuKG ausschließlich die gewerbsmäßige Begehung pönalisiert. Andere Bestimmungen wiederum lassen sich – mangels mehr oder minder IKT-gebundener Verhaltensweisen – wohl treffender dem Immaterialgüterstrafrecht (zB § 91 UrhG, § 42 GMG, § 60 MSchG) oder dem Wettbewerbs(straf)recht (zB § 4 UWG) zuordnen.

Formen der Computerkriminalität, die ein gewisses Maß an sozialer Unverträglichkeit überschreiten und sich generell an vom Strafrecht zu schützenden Rechtsgütern orientieren, müssen mit strafgesetzlichen Mitteln bekämpft werden. Die strafrechtsdogmatische Erfassung solcher (strafwürdiger) Phänomene ist nun Aufgabe des sog »Computerstrafrechts«.

B. Zum Begriff »Computerstrafrecht«

Selbst wenn es mittlerweile eine (wachsende) Vielzahl von Publikationen zum Computerstrafrecht in der österr Fachliteratur gibt, sind kaum[106] Versuche unternommen worden, die Begrifflichkeit des »Computerstrafrechts« zu untersuchen. Aus diesem Grund soll eine den strafrechtlich zu begegnenden Erscheinungsformen der Computerkriminalität adäquate Definition bzw Begriffsklärung gefunden werden,

106 Siehe aber *Bergauer/Schmölzer* in Jahnel/Mader/Staudegger, IT-Recht[3], 635 (644 f).

ist doch das Computerstrafrecht nichts anderes, als die strafgesetzgeberische Reaktion auf strafwürdiges Verhalten, das der Computerkriminalität zuzuordnen ist.

Der Begriff »Computerstrafrecht« umschreibt bereits seit seinen Anfängen in abstrakter Art und Weise eine Spezialbetrachtung des Strafrechts im Hinblick auf seine spezifischen informationstechnologiebezogenen Bestimmungen sowie die Subsumtion strafwürdiger Sachverhalte mit einem Bezug zur Informations- und Kommunikationstechnologie[107] unter allgemeine Tatbestände. Aus diesem Grund kann man von einer Querschnittsmaterie innerhalb des Strafrechts sprechen. Ein eigenständig kodifiziertes Sondergesetz innerhalb des Strafrechts existiert nicht und ist auch nicht indiziert.[108]

In Ö gibt es keine einzige Strafbestimmung, die ausschließlich auf einen Computer an sich abstellt, und dennoch wurde bereits sehr früh von einem »Computerstrafrecht« gesprochen.[109] Im Schrifttum werden – vermeintlich der technischen Entwicklung Rechnung tragend – iSd Mottos: »Jede populäre Entwicklungsstufe der Technologie braucht in der strafrechtlichen Bewertung ihren eigenen Begriff« neue Termini vorgeschlagen (wie zB Internetstrafrecht[110], Informationsstrafrecht[111], multimediale Kriminalität[112], Cyberstrafrecht[113], Datennetzkriminali-

107 Siehe zur Begrifflichkeit auch *Kersken,* IT-Handbuch[5], 25.

108 Siehe dazu bereits *Bergauer/Schmölzer* in Jahnel/Mader/Staudegger, IT-Recht[3], 635 (644 f).

109 Siehe *Schmölzer,* Das neue Computer-Strafrecht (Strafrechtsänderungsgesetz 1987), EDVuR 1988, 20; *Wegscheider* in BMJ, Strafrechtliche Probleme der Gegenwart 1990, 127 (127 ff); siehe zur Entstehung auch *Schmölzer,* ZStW 2011/123, 709 (721).

110 Vgl *Hilgendorf/Valerius,* Computer- und Internetstrafrecht[2] (2012) Rz 7; auch *Reindl-Krauskopf,* Computerstrafrecht im Überblick[2] (2009) 4.

111 Siehe *Sieber,* Computerkriminalität und Informationsstrafrecht, CR 1995, 100 ff; weiters *Hilgendorf/Valerius,* Computer- und Internetstrafrecht[2], Rz 6.

112 Siehe etwa *Vassilaki,* Multimediale Kriminalität – Entstehung, Formen und rechtspolitische Fragen der »Post-Computerkriminalität«, CR 1997, 297 ff.

113 Vgl bereits die Überschriften bei *Salimi,* Zahnloses Cyberstrafrecht? Eine Analyse der gerichtlichen Straftatbestände zum Daten- und Geheimnisschutz, ÖJZ 2012/115, 998; *Salimi,* Zahnloses Cyberstrafrecht? Eine Analyse der gerichtlichen Straftatbestände zum Daten- und Geheimnisschutz, in Landesgruppe Österreich der Internationalen Strafrechtsgesellschaft (AIDP) und Juristenverband (Hrsg), Cyber Crime – Zunehmende Bedrohung der Informationsgesellschaft (2012) 32 (32 ff); *Lee,* Die Verhältnismäßigkeit im Cyberstrafrecht – Überprüfung des Strafrechtseingriffs im Cyberspace anhand des Verhältnismäßigkeitsgrundsatzes (2010) 1 ff.

tät[114], Kommunikationsstrafrecht[115]). Dabei wird aber gerne übersehen, dass derartige Termini ebenso unscharf[116] wie »Modeerscheinungen« sind. Ein »Internetstrafrecht« etwa ist terminologisch auf das Medium »Internet« beschränkt, das trotz seiner Breite nur einen Ausschnitt der Informationstechnologie darstellt (bereits strafbare Handlungen in einem »Intranet« fallen – streng genommen – nicht darunter). Der Begriff des Internetstrafrechts[117] kann daher nicht synonym für Computerstrafrecht verwendet werden.[118]

Die Beibehaltung von etablierten, hinreichend aussagekräftigen (und dogmatisch ohnehin unbeachtlichen Beschreibungen) sollte daher gefördert werden. Zum einen, um an einer mittlerweile allgemein verbreiteten und akzeptierten Vorstellung festzuhalten und zum anderen, weil es in der wissenschaftlichen Befassung nicht darum gehen kann, reines »Wording« zu betreiben.[119] Darüber hinaus hat man mit solchen Bezeichnungen auch nichts gewonnen, da es sich lediglich um informelle Beschreibungen handelt, denen keinerlei dogmatische Bedeutung zukommt. Auswirkungen in der Praxis könnten allenfalls für die behördeninterne Geschäftsverteilung (zB bei Staatsanwaltschaften oder Kriminalpolizei) denkbar sein.

Daher macht es meiner Meinung nach lediglich Sinn – vom Stand der technischen Entwicklungen weitgehend unabhängig – das Computerstrafrecht in einem engen und weiten Begriffsverständnis zu verstehen, das aber bloß eine Spezialbetrachtung des Strafrechts aus einem ganz bestimmten Blickwinkel, nämlich der IKT-Bezogenheit, beschreibt und demnach eine ganz bestimmte Kategorie von Straftaten meint. Eine vom materiellen Kernbereich des StGB völlig losgelöste Computerstrafrechtsdogmatik ist damit aber nicht intendiert.

Dem »ultima ratio«-Gedanken des Strafrechts generell entsprechend sollte sich die Schaffung neuer Computerdelikte an der Frage orientieren, ob die sozialschädlichen Erscheinungsformen der Com-

---

114 Vgl zB *Hilgendorf,* Die Neuen Medien und das Strafrecht, ZStW 2001/113, 650 (653).

115 Siehe zB *Tiedemann/Valerius* in Laufhütte/Rissing-van Saan/Tiedemann (Hrsg), Leipziger Kommentar StGB[12]. Bd 9/1 (2012) § 263a Rz 2 (Stand Oktober 2011).

116 Siehe dazu auch *Schmölzer,* ZStW 2011/123, 709 (720 f), die kritisiert, dass der festzustellende Wandel der Begrifflichkeiten, auf unklaren und uneinheitlichen Inhalten und Abgrenzungen beruhe.

117 Dasselbe gilt für den Begriff »Cyberstrafrecht«.

118 So auch *Brodowski/Freiling,* Computerkriminalität, 31.

119 Vgl bereits *Bergauer/Schmölzer* in Jahnel/Mader/Staudegger, IT-Recht[3], 635 (644 f).

puterkriminalität eine derartige Intensität annehmen, dass für Beeinträchtigungen und Bedrohungen von (wenn auch neuen) Rechtsgütern kein anderes – als das strafrechtliche – Instrumentarium[120] mehr angemessen und ausreichend erscheint. Eine Überreglementierung durch Anlassgesetzgebung sollte aber jedenfalls – auch in diesem Bereich – vermieden werden.[121] Der Rechtsgüterschutz wird und muss daher auch in dieser Materie ein fragmentarischer bleiben.

1. »Computerstrafrecht im weiten Sinn«

Unter dem (materiellen) Computerstrafrecht im weiten Sinn ist mE die Gesamtheit der Rechtsvorschriften des Kriminalstrafrechts zu verstehen, die auf IKT-Sachverhalte angewendet werden (können).[122] Deshalb fallen unter das Computerstrafrecht iwS neben speziell geschaffenen Computerdelikten[123] auch klassische[124] (und traditionelle) Strafbestimmungen, sofern das Substrat der Rechtsanwendung auf Sachverhalten mit (wesentlichem) Bezug zur Informationstechnologie beruht.[125] Dieses Verständnis korrespondiert mit dem weiten Begriff der Computerkriminalität, der nach der hier vertretenen Auffassung lediglich darauf abstellt, dass strafbare Handlungen unter Verwendung der IKT begangen werden.[126] Als klassische bzw traditionelle (technikneutrale) Strafnormen sind dabei zB Inhaltsdelikte[127], hier insb Ehrenbeleidigungs-

120 ZB des Zivilrechts oder des Verwaltungsrechts.

121 Vgl auch *Bergauer/Schmölzer* in Jahnel/Mader/Staudegger, IT-Recht[3], 635 (643 f).

122 Siehe dazu bereits *Bergauer/Schmölzer* in Jahnel/Mader/Staudegger, IT-Recht[3], 635 (644 f).

123 Zur Begrifflichkeit des »Computerdelikts« siehe gleich im Anschluss.

124 Darunter können Strafbestimmungen verstanden werden, die völlig ohne Bezug zu informationstechnischen Methoden oder Zielen begangen werden können; vgl dazu auch *Gildemeister,* Cyber Crime – Herausforderungen in der Praxis, in Landesgruppe Österreich der Internationalen Strafrechtsgesellschaft (AIDP) und Juristenverband (Hrsg), Cyber Crime – Zunehmende Bedrohung der Informationsgesellschaft (2012) 23 (23).

125 Die Formulierung ist angelehnt an die Definition des von der »Rechtsinformatik« im weiten Sinn umfassten »IT-Rechts« (bzw Informatikrechts) nach *Schramm* (vgl *Schramm,* Zum Beispiel: Der Lehrgang für Rechtsinformatik an der Karl-Franzens-Universität Graz, in Mayer-Schönberger/Schneider-Manns-Au (Hrsg), Der Jurist am Info-Highway. Über die Zukunft eines Berufsstandes (1997) 161 (161 und 163 f).

126 Siehe oben.

127 Vgl zB verbotene Inhalte auf Websites, wie etwa kinderpornographische Darstellungen, rassistisches oder nationalsozialistisches Gedankengut.

delikte[128], aber auch Gemeingefährdungsdelikte[129] usw anzuführen, sofern ein überwiegend informationstechnologisches Geschehen Ausgangspunkt der juristischen Betrachtung ist. Daneben finden sich strafrechtliche Tatbestände, die in ihrem Anwendungsbereich ebenso Praktiken erfassen, die dem Computerstrafrecht iwS zugeordnet werden können, in den unterschiedlichsten – auf speziellen Wertentscheidungen und spezifischen Begrifflichkeiten beruhenden – Nebengesetzen (vgl zB § 91 UrhG[130], § 108 TKG 2003[131], § 51 DSG 2000[132]). Das Computerstrafrecht iwS dient aber lediglich einer groben Abgrenzung zu anderen Strafrechtsspezialisierungen und erweist sich aufgrund seines weitgehend uferlosen Umfangs für weitere wissenschaftliche Untersuchungen, empirische Analysen und Statistiken als nicht sonderlich nutzbringend.

2. »Computerstrafrecht im engen Sinn«

Das (materielle) Computerstrafrecht im engen Sinn erfasst nun die spezifischen Delikte des Kern- und Nebenstrafrechts, die explizit dafür geschaffen wurden, computer- bzw datengestützte Begehungsweisen oder Tatmittel (computer- oder datengestützte Ausrichtung)[133] und informationstechnische Angriffe auf IKT-Systeme bzw Daten als Tatobjekte (computer- bzw datenorientierte Ausrichtung)[134] zu erfassen (sog »Computerdelikt«)[135], um der Computerkriminalität entgegen zu wirken.[136] Dazu zählen etwa die Datenbeschädigung (§ 126a), die Störung der Funktionsfähigkeit eines Computersystems (§ 126b), der Missbrauch von Computerprogrammen oder Zugangsdaten (§ 126c),

128 Vgl zB die üble Nachrede oder Beleidigung in E-Foren; siehe auch *Bergauer,* Ehrenbeleidigungen im Web 2.0 aus strafrechtlicher Sicht, in Gögele/Unger (Hrsg), IT-Sicherheit aus rechtlicher, wirtschaftlicher und technologischer Perspektive (2010) 6 (6 ff).

129 Vgl zB *Bergauer,* Computerwürmer und Gemeingefährdungsdelikte im Strafrecht, jusIT 2008/2, 2.

130 Urheberrechtsgesetz, BGBl 111/1936 idF I 99/2015.

131 TKG 2003, BGBl I 70/2003 idF I I 44/2014.

132 DSG 2000, BGBl I 165/1999 idF I 83/2013.

133 Computer bzw Daten als Tatwerkzeuge.

134 Computer bzw Daten als Angriffsziele.

135 Zum Begriff »Computerdelikt« siehe auch ErlRV 1166 BlgNR XXI. GP, 23.

136 Im Zusammenhang mit dem Begriff »Computerkriminalität« sprechen *Jaburek/Schmölzer* vom Computer als »End- oder Zwischenziel« deliktischen Handelns (vgl *Jaburek/Schmölzer,* Computer-Kriminalität, 20 ff); ähnlich *Wegscheider* in BMJ, Strafrechtliche Probleme der Gegenwart 1990, 127 (130).

der widerrechtliche Zugriff auf ein Computersystem (§ 118a), das missbräuchliche Abfangen von Daten (§ 119a), der Betrügerische Datenverarbeitungsmissbrauch (§ 148a), aber auch bspw die Datenfälschung (§ 225a). Darüber hinaus sind auch Delikte mit IKT-gebundenen Begehungsweisen dem Computerstrafrecht zugehörig. Als Beispiele dafür sind § 107a Abs 2 Z 2, § 207a Abs 3a, § 208a Abs 1 Z 1 und Abs 1a, § 278f Abs 1 und 2 zu nennen. Am besten lassen sich »Computerdelikte« daher in zwei Kategorien einteilen: solche die ausschließlich bzw überwiegend auf IKT-Begehungsweisen abstellen (hier als »echte Computerdelikte« bezeichnet)[137], und solche, die grundsätzlich technikneutraler Natur sind, aber in einzelnen Begehungsweisen auch über IKT-Mittel realisiert werden können, was explizit als Handlungsalternative unter Strafe gestellt wurde (hier: »unechte Computerdelikte«).[138]

In der Lit findet man auch eine andere Begriffsbestimmung, bei der das »Computerstrafrecht« dem »Internetstrafrecht«[139] gegenüber gestellt wird. Dabei werden jene Delikte, die iZm einem einzelnen Rechner stehen, zum Computerstrafrecht (im eigentlichen Wortsinn) gezählt und jene, die von vornherein auf die Kommunikation in Rechnernetzen ausgerichtet sind, zum Internetstrafrecht.[140] Eine solche Differenzierung wäre zwar grundsätzlich denkbar, da etwa unter dem Begriff »Computersystem« nach der Legaldefinition des § 74 Abs 1 Z 8, einzelne, aber auch verbundene Vorrichtungen, die der automationsunterstützten Datenverarbeitung dienen, verstanden werden, ist aber technologiebedingt mE nicht sonderlich zweckmäßig und ergiebig. So existiert im öStGB genau genommen kein einziges Computerdelikt, das sich ausschließlich mit einem einzelnen Computer befasst. Die Definition der einschlägigen Tatbestände umfasst hierbei meist ein »Computersystem« (iSd § 74 Abs 1 Z 8), wie zB in §§ 118a, 126b, oder »Daten« (zB §§ 119a, 126a, 148a iSd § 74 Abs 2) bzw Nachrichten, die ua im Wege eines Computersystems übertragen werden (siehe §§ 119, 120a). Auch der Betrügerische Datenverarbeitungsmissbrauch (§ 148a) beschränkt sich nicht auf ei-

137 Echte Computerdelikte sind demnach zB § 126a oder § 126b.

138 Unechte Computerdelikte sind zB § 107a oder § 207a.

139 Vgl auch *Reindl-Krauskopf,* Computerstrafrecht², 4; weiters *Altenhain,* IT-Strafrecht – Entstehung eines Rechtsgebiets, in Weiß (Hrsg), Rechtentwicklungen im vereinten Deutschland (2011) 117 (133 f).

140 Ohne vertiefte Begründung und für das deutsche Strafrecht *Hilgendorf/Valerius,* Computer- und Internetstrafrecht², Rz 7. Ebenso verwenden diese Autoren »Informationsstrafrecht« als unscharfen Überbegriff.

nen einzelnen Rechner, denn unter Datenverarbeitung versteht man die Summe der im Ablauf logisch verbundenen Datenverwendungsschritte, die zur Erreichung eines bestimmten Ergebnisses zur Gänze oder auch nur teilweise automationsunterstützt erfolgen.[141] Das kann ebenso eine Datenverarbeitung sein, die über ein Netzwerk abgewickelt wird. Deshalb hat man sich im Gesetzwerdungsprozess bewusst dafür entschieden, in der Deliktsbezeichnung des § 148a auf das Wort »Computer« (wie zB »Computerbetrug«) zu verzichten.[142] Aber auch für die Datenbeschädigung nach § 126a, bei der automationsunterstützt verarbeitete, übermittelte oder überlassene Daten das Tatobjekt bilden, deren Verarbeitung genauso gut über Computernetzwerke erfolgen kann, wird nicht auf einen konkreten »Computer« abgestellt. Der nicht ausreichend umrissene Terminus »Internetstrafrecht« wiederum bringt nun die beachtliche Einschränkung mit sich, dass lediglich strafrechtlich relevante Handlungen im Medium »Internet« erfasst sind. Genau genommen würden Tatbegehungen in einem »Intranet« uÄ dieser Kategorie nicht unterliegen. Daher wäre es in diesen Fällen wohl exakter, wenn man zB von einem »Computernetzwerkstrafrecht« sprechen würde, was jedoch aus meiner Sicht vernachlässigbar und nicht weiter zu verfolgen ist.

Was das Verständnis von »Computer«-Strafrecht im echten Wortsinn anlangt, ist zu beachten, dass gewisse Erscheinungsformen, wie zB die Datenfälschung, das Herstellen bzw Verbreiten von Malware, das Klonen von SIM-Karten oder Mikrocontrollern oder das informationstechnische Hantieren mit pornographischen Darstellungen Minderjähriger, mangels »Computer«-Bezogenheit nicht davon erfasst wären. Derartige Handlungen werden aber generell auch einem »Internetstrafrecht« nicht unterzuordnen sein. Abschließend ist noch anzumerken, dass bei einer derartigen Aufteilung in ein Computer- bzw Internetstrafrecht sämtliche Delikte mit »telekommunikationstechnischen Begehungsweisen« gar nicht oder zumindest nicht vollständig erfasst werden können. Daher wäre es in diesem Fall indiziert an eine weitere Gruppierung zu denken, wie zB ein »Kommunikationsstrafrecht[143]«, welches jedoch genau, wie die beiden anderen Kategorien Unschärfen und Abgrenzungsprobleme mit sich brächte.

---

141 Vgl *Kirchbacher/Presslauer* in WK² § 148a Rz 15 (Stand November 2009).

142 Vgl JAB 359 BlgNR XVII. GP, 18.

143 Siehe zur tatsächlichen Verwendung auch eines solchen Begriffs *Tiedemann/Valerius* in LK¹² § 263a Rz 2.

Eine Einteilung des Computerstrafrechts, die sich »ausschließlich« und streng am Computersystem bzw an Daten als Tatmittel oder als Tatobjekt orientiert, ist abzulehnen. Bei sehr vielen in Frage kommenden Delikten, aber auch in einschlägigen Sachverhalten, treffen nämlich beide Unterscheidungskriterien kumulativ zusammen. So sieht bspw § 119a Abs 1 erster Deliktsfall zwar als Schutzobjekt (automationsunterstützt verarbeitete) Daten vor, der Täter muss aber zur Erfüllung des objektiven Tatbestands ebenso eine Vorrichtung, zB ein Computerprogramm[144], als Tatmittel benützen. Bei DDoS-Angriffe treten idR gleichermaßen informationstechnische Tatmittel wie auch Computersysteme als Tatobjekte in Erscheinung. Eine eindeutige Zuordnung nach den genannten Differenzierungsmerkmalen wäre hier unpraktikabel und weitgehend auch gar nicht möglich. Derartige Unterscheidungskriterien erweisen sich als unpräzise und nicht sonderlich zweckmäßig, weshalb sie allenfalls in einer Unterkategorie eines »Computerstrafrechts im engen Sinn« nach obigem Verständnis eine mehr oder weniger sinnvolle Rolle spielen könnten.

3. Vorfeldbereich und Kernbereich[145]

Reindl-Krauskopf erachtet eine Einteilung des Computerstrafrechts über die EDV als Tatmittel oder Tatobjekt als wenig zielführend, da insb bei der Gruppe, wo die EDV als Tatmittel das Kriterium bildet, unterschiedliche Deliktstypen und die verschiedensten Rechtsgüter betroffen seien.[146] Sie teilt das »Computerstrafrecht« daher in einen Vorfeldbereich und einen Kernbereich ein und orientiert sich dabei an den Rechtsgütern und der jeweiligen Beeinträchtigungsnähe. Beispielsweise werden §§ 118a, 119, 119a, 126c, 241a ff und § 10 ZuKG von *Reindl-Krauskopf* als Vorfelddelikte angeführt.

Als wirkliche Vorbereitungsdelikte können dabei aber streng genommen bloß § 126c, §§ 241a ff sowie § 10 ZuKG qualifiziert werden. Der Gesetzgeber hat dabei eindeutige und besonders gefährliche Vorbereitungshandlungen als eigenständige Tatbestände unter Strafe gestellt.[147]

---

144 Als Beispielsfall aus der Praxis könnte die Datenspionage mittels eines Keyloggers dabei in Betracht kommen.

145 Diese Einteilung geht auf *Reindl-Krauskopf* zurück (vgl daher *Reindl-Krauskopf,* Computerstrafrecht², 8 f).

146 Vgl *Reindl-Krauskopf,* Computerstrafrecht², 8.

147 Siehe zu den Vorbereitungsdelikten *Fuchs,* Strafrecht. Allgemeiner Teil I⁸ (2012) Rz 28/15 ff.

Warum *Reindl-Krauskopf* nun auch die Strafbestimmungen der §§ 118a, 119, 119a dem Vorfeldbereich zuordnet, ist – mangels näherer Begründung[148] – unklar. Eine klare Definition und Abgrenzung des Vorfeldbereichs fehlen.

Beim Versuch eine solche Begründung zu finden, könnte man bei der Zuordnung zu Vorfelddelikten auf die Tathandlungen abstellen, wie bspw im Fall des § 118a auf die widerrechtliche Zugangsverschaffung zu einem fremden Computersystem, die dem System- und Datenzugriff (Rechtsgüter sind der Schutz der Privatsphäre und ein abstrakter Datenschutz)[149] vorausgeht. Auch muss bei den Delikten §§ 119, 119a erst eine Vorrichtung benützt werden, damit die Kenntnisverschaffung von Nachrichteninhalten (§ 119) oder Daten (§ 119a) materiell realisiert werden kann. In diesem Fall wäre bei einer derartigen Betrachtung ein gewisser Abstand zur Rechtsgutverletzung schon erkennbar, da die tatsächliche Kenntnisnahme zB der Nachrichteninhalte iSd § 119 vom objektiven Tatbestand gar nicht verlangt wird. Nach diesem Verständnis muss aber streng genommen auch § 126b dem Vorfeldbereich zugeordnet werden, da dieser als Tatobjekt ein »Computersystem« schützt, die Bestimmung aber zur Datenbeschädigung (§ 126a), welche elektronische Daten behandelt, ausdrücklich subsidiär ist. In diesem Sinn lässt sich in der Pönalisierung der Herbeiführung einer Funktionsstörung eines (vermögenswerte) Daten führenden Computersystems, was die vorrangig interessierenden Daten als zu schützende Information anlangt, eine Vorverlagerung des Rechtsgüterschutzes erkennen.[150]

Streng genommen müsste man einer solchen Einteilung folgend auch diverse Organisationsdelikte (zB §§ 278a ff) dem Vorbereitungsbereich zurechnen, die aufgrund der Eigenständigkeit des strafrechtlichen Unrechts selbstständig vertypte Vorbereitungsdelikte darstellen und Tätigkeiten erfassen, die mit terroristischen Vereinigungen und dem Computerstrafrecht in Verbindung stehen.[151]

Der Kernbereich des Computerstrafrechts umfasst nach *Reindl-Krauskopf* neben Schadensdelikten (zB §§ 126a, 126b), Bereicherungs-

148 Vgl *Reindl-Krauskopf,* Computerstrafrecht², 8 f.

149 Siehe zur Begrifflichkeit *Thiele* in SbgK § 118a Rz 15 f (Stand März 2007).

150 Siehe dazu *Bergauer/Schmölzer* in Jahnel/Mader/Staudegger, IT-Recht³, 635 (651).

151 Siehe dazu auch *Kienapfel/Höpfel/Kert,* Strafrecht Allgemeiner Teil I¹⁴ (2012) Z 21 Rz 6 und 9; vgl auch *Plöchl* in WK² § 278b Rz 2 (Stand Jänner 2014); weiters *Triffterer* in SbgK § 278a Rz 10 (Stand Juni 1997).

delikten (zB § 148a) und Inhaltsdelikten (zB § 78, §§ 111 ff, § 207a sowie § 1 PornG, §§ 3d, 3h VerbotsG) auch Urkundendelikte (zB § 225a).[152]

Auch hins dieser Kategorie ist nicht ganz schlüssig, warum etwa die Datenfälschung nach § 225a als Kerndelikt erachtet wird, ist doch idZ gerade der Gebrauch von Datenfalsifikaten – anders als bei Urkunden nach § 223 Abs 2 – gar nicht pönalisiert. Erfasst ist daher lediglich das Fälschen oder Verfälschen von Daten. Dass die Strafbarkeit – vergleichbar mit echten Vorbereitungsdelikten – schon in einem sehr frühen Stadium einsetzt, wird auch indirekt durch die Bestimmungen über die Tätige Reue nach § 226 indiziert.[153] Interessanterweise nennt schließlich *Reindl-Krauskopf* selbst an einer anderen Stelle § 225a als eine »weitere Vorfeldtat«.[154]

Nützlich wäre es wohl, wenn bei einer solchen Einteilung zumindest auch die konkreten Rechtsgüter namentlich genannt würden, um die jeweilige Klassifizierung nachvollziehbarer zu gestalten. Dies löst andernfalls bei Mischdelikten, die unterschiedliche Rechtsgüter schützen, wie auch bei § 118a[155], eine Zuordnungsproblematik aus. Auch wäre es aus meiner Sicht notwendig, sämtliche Delikte, die nach Ansicht *Reindl-Krauskopfs* in den Bereich eines Computerstrafrechts fallen, in ihrer Darstellung und Systematik abschließend zu berücksichtigen. Eine nur beispielhafte Veranschaulichung reicht gerade in Anbetracht der von ihr konstatierten Vielschichtigkeit der Rechtsgüter wohl nicht aus. Dass aber eine Vollständigkeit einer Deliktszuordnung im Bereich des Computerstrafrechts mit seinem weiten Anwendungsfeld[156] faktisch kaum realisierbar ist, stellt diesen Ansatz wohl ebenso in Frage.

Zusammenfassend ist mE davon auszugehen, dass durch eine Systematik, die Delikte in einen Vorfeldbereich und einen Kernbereich unterteilt, nichts gewonnen ist, vielmehr noch trägt sie zu einer gewissen Unübersichtlichkeit bei, die für das Verständnis von einem »Computerstrafrecht« und dessen Anwendung entbehrlich erscheint.

---

152 Vgl *Reindl-Krauskopf,* Computerstrafrecht², 8; Vgl auch *Reindl,* Das neue Computerstrafrecht – ein Überblick, in BMJ (Hrsg), Vorarlberger Tage 2003. Bd 115 (2003) 63 (64 f).

153 Vgl dazu *Thiele* in SbgK § 225a Rz 46 (Stand März 2007).

154 Siehe *Reindl-Krauskopf,* Computerstrafrecht², 66.

155 ZB »Privatsphäre« und »formeller Datenschutz« siehe dazu S 74 f.

156 Tatsächlich müsste man bei einer umfassenden Darstellung die meisten Delikte des Strafrechts zuordnen, da auch traditionelle (technik- und medienneutrale) Delikte in besonderen Sachverhalten anwendbar sind.

Meines Erachtens kann es nur sinnvoll sein, das Computerstrafrecht dahingehend zu verstehen, dass es sich dabei um eine Spezialbetrachtung des Strafrechts handelt, die auf spezifische IKT-bezogene Strafbestimmungen im Besonderen (Computerstrafrecht ieS) sowie auf die Subsumtion sämtlicher strafbarer IKT-bezogener Sachverhalte im Allgemeinen (Computerstrafrecht iwS) fokussiert. Eine rechtsgutorientierte Kategorisierung ist mE aufgrund der Vielzahl und Verschiedenheit der relevanten Rechtsgüter unzweckmäßig. Das Augenmerk sollte auf »IKT-gebundene Verhaltensweisen« gerichtet werden, die darauf abzielen, entweder IKT zu schädigen oder IKT als Tatmittel Verwendung finden zu lassen. In weiterer Folge ist mit der Bezeichnung »Computerstrafrecht« das »Computerstrafrecht im engen Sinn« gemeint.

4. »Formelles Computerstrafrecht«

Von einem formellen Computerstrafrecht kann mE im Bereich des Strafprozessrechts gesprochen werden, soweit Ermittlungsmaßnahmen durch informations- und kommunikationstechnologische Methoden durchgeführt werden bzw der Erlangung und Überwachung automationsunterstützt verarbeitbarer Daten dienen.[157] Dabei sind bspw die Datenauskunft (§ 135 Abs 2 StPO[158]), die Nachrichtenüberwachung (§ 135 Abs 3 StPO), aber auch die optische und akustische Überwachung von Personen unter Verwendung technischer Mittel zur Bild- oder Tonübertragung (§ 136 StPO) und der automationsunterstützter Datenabgleich (§ 141 StPO) zu nennen, ebenso wie die hitzig diskutierte, umstrittene Online-Durchsuchung[159]. Auf ein solches formelles Computerstrafrecht wird in dieser Arbeit nicht vertieft eingegangen.

157 Siehe solche Maßnahmen zusammengefasst in *Bergauer/Schmölzer* in Jahnel/Mader/Staudegger, IT-Recht[3], 635 (710 ff).

158 Siehe folgend StPO 1975, BGBl 631/1975 (WV) idF I 85/2015.

159 Siehe dazu vertiefend *Bergauer,* Online-Durchsuchung: Rechtliche und technische Überlegungen, jusIT 2008/19, 47.

C. Abgrenzungen und Sonderfälle

1. Hardware-Angriffe

Sofern sich konventionelle – dh IKT-neutrale – strafbare Handlungen ausschließlich gegen Hardware (zB Gehäuse, Monitor, Tastatur) richten, ergeben sich für eine strafrechtliche Beurteilung keine großen Schwierigkeiten. Ihre Zerstörung oder Beschädigung wird unter die Sachbeschädigung (§§ 125 f), ihre Wegnahme unter den Diebstahl (§§ 127 ff) oder die Dauernde Sachentziehung (§ 135) zu subsumieren sein. Alle diese Fälle lassen sich nach der hier vertretenen Auffassung nicht einmal der »Computerkriminalität« zuordnen, weil IKT-gebundene Verhaltensweisen fehlen.[160]

Hingegen fallen strafbare IKT-gebundene Verhaltensweisen, selbst wenn dadurch lediglich Hardware geschädigt wird, sehr wohl unter dieses Kriminalitätsbild. Man denke dabei an Computerviren, die mit einer Überlastungsroutine für Festplatten-Schreib-/Leseköpfe ausgestattet sind und damit einen sog (physikalischen) »Headcrash«[161] verursachen können.

Eine strenge Abgrenzung zwischen reinen Hardware-Komponenten und Systemen, bestehend aus Hard- und Software, lässt sich aber in der Praxis kaum noch bewerkstelligen. Zu nennen sind an dieser Stelle etwa durch Mikrocontroller[162] gesteuerte Geräte wie Grafikkarten, Netzwerkadapter, USB-Speichersticks udgl, deren Chips mit »in Hardware gegossener Software« (sog »Firmware«) gesteuert werden. Zu nennen sind idZ auch die sog »Embedded Systems«, wie zB einfache Automaten (Getränke- oder Fahrkartenautomaten), Chipkarten (zB Bankomatkarte, e-card, SIM-Karte), Digitalkameras, Multimediageräte (zB MP3-Player), Multifunktionsdrucker, aber auch moderne Kühlschränke

160 Vgl *Bergauer/Schmölzer* in Jahnel/Mader/Staudegger, IT-Recht[3], 635 (646).

161 Dabei berührt ein grundsätzlich auf einem Luftpolster über der rotierenden Plattenoberfläche schwebender Schreib-/Lesekopf die Plattenoberfläche.

162 Dabei handelt es sich um vollständige Computersysteme (sog »Ein-Chip-Computersysteme«), die mit Prozessor, Speicher, Ein-/Ausgabeeinheiten und entsprechender Systemsoftware ausgestattet sind (vgl *Piller,* die Chipkarte in Österreich, in Arbeitsgemeinschaft für Datenverarbeitung [Hrsg], Quo vadis EDV? – Realität und Vision. 8. Internationaler Kongress Datenverarbeitung im Europäischen Raum [1987] 374 [374 ff]). Vorwiegend werden diese Chips in eingebetteten Systemen (Embedded Systems) verwendet. Siehe *Tanenbaum,* Computerarchitektur[5], 48 ff; weiters *Rankl/Effing,* Handbuch der Chipkarten[5] (2008) 87.

und Waschmaschinen oder Kfz-Komponenten und hochtechnisierte Waffensysteme.[163]

Sachbeschädigungen an solchen körperlichen Bauteilen können daher ggf sowohl als Computerkriminalitätsfälle behandelt werden als auch mit speziellen Computerdelikten in echte Konkurrenz treten.

2. »Zeitdiebstahl«

Der sog »Zeitdiebstahl« – dh die bloße unbefugte Inbetriebnahme oder Verwendung eines fremden Computers für eigene Zwecke – ist strafrechtlich nicht subsumierbar und in Anbetracht der »ultima ratio«-Funktion des Strafrechts idR auch nicht strafwürdig.[164]

3. »Software-Diebstahl«[165]

Die in der Praxis wohl häufigste unerlaubte Handlung iZm kommerziellen Computerprogrammen betrifft das unerlaubte Kopieren von urheberrechtlich geschützten Programmen, wie Anwendungssoftware oder Computerspiele. Mangels einer »körperlichen (beweglichen) Sache« iSd § 285 ABGB entfällt hierbei allerdings die Anwendbarkeit des Diebstahls (§ 127). Darüber hinaus würde auch das verlustfreie Reproduzieren (Kopieren) von Computerprogrammen keine unmittelbare Vermögensverschiebung darstellen, weil dadurch weder Gewahrsam gebrochen noch über- bzw zugeführt würde, was jedoch für den Diebstahl als »Vermögensverschiebungsdelikt« charakteristisch ist.[166]

---

163 Siehe dazu auch S 79.

164 Vgl dazu bereits *Schmölzer,* Legistische Tendenzen im Computer-Strafrecht, RZ 1986, 178; *Schmölzer* in BMJ, Strafrechtliche Probleme der Gegenwart 1989, 195 (201); *Wegscheider* in BMJ, Strafrechtliche Probleme der Gegenwart 1990, 127 (144 ff); *Fuchs,* Zum Entwurf von Strafbestimmungen gegen die Computerkriminalität, RdW 1985, 330; *Reindl,* E-Commerce und Strafrecht (2003) 195 ff.

165 Diese Begrifflichkeit ist im Sinne der Strafrechtsdogmatik verfehlt und daher nur umgangssprachlich zu verstehen (dasselbe gilt für den Begriff der »Raubkopie«).

166 Siehe hierfür *Bergauer/Schmölzer* in Jahnel/Mader/Staudegger, IT-Recht[3], 635 (647).

D. Überblick über die Entwicklung der Computerstrafrechtsdogmatik

Anhand einiger Eckdaten lässt sich die Entwicklung nachzeichnen, die an die Veränderung der ursprünglich rein als körperlich erachteten Tatmittel bzw Tatobjekte hin zu mittlerweile längst ubiquitären, virtuellen Werkzeugen oder Handlungs- bzw Angriffsobjekten anknüpft. Auch die Einflüsse internationaler wie europäischer Vorgaben bestätigen die globale Betroffenheit von neuen, modernen Erscheinungsformen der Kriminalität und spiegeln eine in jüngerer Zeit gewachsene Harmonisierungsidee und geeinte Entschlossenheit zur Bekämpfung derartiger Phänomene wider. Die wichtigsten Entwicklungen sollen daher chronologisch gereiht hervorgehoben werden:

1. DSG 1978

Der Gesetzgeber hat mit der Normierung des Grundrechts auf Datenschutz in § 1 Datenschutzgesetz (1978)[167] personenbezogene Daten als Schutzobjekte in Verfassungsrang determiniert. Bereits damals wurde darauf abgestellt, dass es für das verfassungsgesetzlich gewährleistete subjektive Recht auf Geheimhaltung personenbezogener Daten unbeachtlich sei, auf welchem Datenträger diese Daten verkörpert werden bzw welche physikalische Eigenschaft sie besitzen.[168] Im Gegensatz zu § 1 Abs 1 und 2 DSG 1978, die nicht auf automationsunterstützte Datenverarbeitung abstellten und daher sämtliche Formen personenbezogener Daten als Grundrechtsobjekt qualifizierten, erfassten Abs 3 und 4 lediglich automationsunterstützt verarbeitete Daten, weshalb die Rechte auf Auskunft, Richtigstellung und Löschung auf automationsunterstützt verarbeitete personenbezogene Daten beschränkt waren. Unter dem Begriff »Daten« wurden im Entwurf zum DSG 1978 »Zeichen oder Zeichenketten verstanden, die in einem Entscheidungsprozess relevante Bedeutung für den Entscheider haben und deren semantische Bedeutung mit Hilfe von Interpretationsregeln, die dem Entscheider bekannt sind, zu vollständigen

167 DSG 1978, BGBl 565/1978 aufgehoben durch BGBl I 165/1999; im Folgenden wird diese historische Fassung des DSG mit »DSG 1978« bezeichnet.

168 Siehe ErlRV 72 BlgNR XIV. GP, 22.

Aussagen ergänzt werden kann«.[169] Vom DSG ausgenommen sollte jedoch grundsätzlich der Schutz von Programmen sein.[170] Auch galt diese Einschränkung nach der bereits erwähnten Legaldefinition von Daten (§ 3 Z 1 DSG 1978) für die gesamte Bezug habende einfachgesetzliche Ausgestaltung des Datenschutzrechts.

Im DSG 1978 wurde bereits festgelegt, dass Daten natürlicher und juristischer Personen gleichermaßen Schutz genießen.[171]

Wesentliches Element des Grundrechts war (und ist) ein allgemeiner Geheimhaltungsschutz von personenbezogenen Daten, der von mehreren zusätzlichen Nebenrechten (Recht auf Auskunft, Richtigstellung und Löschung) für die Betroffenen begleitet wurde.[172] Das Grundrecht auf Datenschutz umfasst daher genauer gesagt bereits seit dem DSG 1978 vier Rechte: das Recht auf Geheimhaltung, das Recht auf Auskunft, das Recht auf Richtigstellung und das Recht auf Löschung.

Da Grundrechte traditionellerweise staatsgerichtet sind, aber die Gefährdung der Privatsphäre durch die Dezentralisierung der ursprünglich über Zentralserver und Großrechenanlagen konzipierten Datenverarbeitungen hin zu Einzelplatzsystemen für jedermann nunmehr auch von Privaten ausging[173], wurde dieses Grundrecht (als derzeit einziges)[174] im § 1 DSG 1978 mit einer unmittelbaren Drittwirkung versehen.[175] Im Gegensatz zur mittelbaren Drittwirkung, bei der durch einfache Gesetze die Grundrechtswirkung zwischen Privaten vermittelt wird (zB die Bestimmungen zum Schutz von Leib und Leben im StGB oder auch § 879 ABGB hins der Einhaltung der »guten Sitten« bei privatrechtlichen Verträgen), lassen sich aus der unmittelbaren Drittwirkung, die dem Grundrecht vom Verfassungsgesetzgeber explizit

169 Vgl ErlRV 72 BlgNR XIV. GP, 22; *Garstka,* Grundbegriffe für den Datenschutz, in Kilian/Lenk/Steinmüller (Hrsg), Datenschutz. Juristische Grundfragen beim Einsatz elektronischer Datenverarbeitungsanlagen in Wirtschaft und Verwaltung (1973) 209 (210 ff).

170 Vgl ErlRV 72 BlgNR XIV. GP, 22.

171 Siehe die ErlRV 72 BlgNR XIV. GP, 21 f; *Duschanek,* Datenschutzgesetz (1978) 20.

172 Vgl *Jahnel,* Handbuch Datenschutzrecht (2010) Rz 2/1.

173 Mit der DSG-Nov 1986 (BGBl 370/1986) wurde ua auf die massentauglichen »Homecomputer« Bezug genommen; vgl *Dohr,* Datenschutz in nationaler und internationaler Perspektive, in Arbeitsgemeinschaft für Datenverarbeitung (Hrsg), Quo vadis EDV? – Realität und Vision. 8. Internationaler Kongress Datenverarbeitung im Europäischen Raum (1987) 703 (706).

174 Siehe dazu *Berka,* Lehrbuch Verfassungsrecht[5] (2013) Rz 1264 f.

175 Vgl *Jahnel,* Handbuch, Rz 1/11.

beigemessen werden muss[176], direkt Ansprüche zwischen Privaten ableiten.[177] Anzumerken ist schließlich, dass der Staat – auch wenn er privatwirtschaftlich agiert – stets an die Grundrechte gebunden ist (sog »Fiskalgeltung«[178]).

Als Strafbestimmungen wurden bereits mit dem DSG 1978 § 48 Abs 1 (Geheimnisbruch) und § 49 (unbefugte Eingriffe in Verarbeitungen) eingeführt[179], wovon beinahe jede Indiskretion bezüglich geschützter Daten, die aus einer beruflichen Tätigkeit heraus bekannt waren, pönalisiert, aber auch bereits das Löschen[180], Verfälschen oder Sonst-Verändern und Sich-Verschaffen von automationsunterstützt verarbeitbaren Daten erfasst wurden.

Mit Schaffung dieser Delikte hat der Gesetzgeber bereits sehr früh – dh bevor der Personal Computer (PC) als Heimcomputer so richtig massentauglich wurde[181] – auf Datenmanipulationen bzw Datenspionage zumindest hins personenbezogener Daten reagiert.

Angesichts des Straftatbestands des § 48 DSG 1978 stand der Gesetzgeber durch die Verlagerung von zentralen EDV-Großrechneranlagen zu völlig dezentralen, selbstständig lauffähigen Heimarbeitsplätzen, vor einer neuen Herausforderung. § 48 DSG 1978 konnte in dieser Form nicht mehr sachlich gerechtfertigt werden, zumal dieser Straftatbestand durch seinen vergleichsweise unspezifischen Unrechtsgehalt geeignet war, über das ursprüngliche Ziel hinausschießend, ungerechtfertigt Bevölkerungsteile zu kriminalisieren.[182] Dies wurde jedoch durch das DSG 2000[183] korrigiert.

---

176 Konkret wurde diese unmittelbare Drittwirkung »originär« in § 1 Abs 6 DSG 1978 durch die Rechtswegklausel »Soweit Rechtsträger in Formen des Privatrechts tätig sind, ist das Grundrecht auf Datenschutz im ordentlichen Rechtsweg geltend zu machen« eingeräumt.

177 Zur »Drittwirkung« siehe vertiefend *Berka,* Verfassungsrecht[5], Rz 1263 ff.

178 Siehe *Berka,* Verfassungsrecht[5], Rz 1258 ff.

179 Mittlerweile findet sich im DSG 2000 nur mehr die Strafbestimmung des § 51 DSG 2000 (Datenverwendung in Gewinn- oder Schädigungsabsicht).

180 Die Tathandlungen des Löschens, Verfälschens oder Sonst-Veränderns des § 49 DSG 1978 wurden durch die Einführung des § 126a StGB durch das StRÄG 1987 (BGBl 605/1987) entfernt und die Deliktsbezeichnung in »Unbefugte Eingriffe im Datenverkehr« abgeändert.

181 Siehe *Dohr* in Arbeitsgemeinschaft für Datenverarbeitung, Quo vadis EDV?, 703 (706).

182 Vgl ErlRV 1613 BlgNR XX. GP, 54.

183 BGBl I 165/1999.

2. StRÄG 1987

Der Entwurf einer Strafgesetznovelle von 1985 sowie eine E[184] des OGH im Jahre 1986, in der das Löschen eines Computerprogramms als »Sachbeschädigung durch Unbrauchbarmachen«[185] beurteilt wurde, bildeten den Anstoß zu regen Diskussionen in der Lehre um die Sacheigenschaft von Computerprogrammen und die diesbezügliche Anwendbarkeit der klassischen Sachbeschädigung (§ 125). Inzwischen hatte der Gesetzgeber seine diesbezüglichen legistischen Bestrebungen finalisiert und reagierte mit dem StRÄG 1987 auf diese neuen Kriminalitätsformen durch Füllung der dogmatischen Lücke mit dem neuen Straftatbestand des § 126a bezüglich »gespeicherter« Daten.[186] In der Lehre wurde mehrfach die Meinung vertreten, dass etwa hins einer »Beschädigung« von Daten gar keine Lücke bestehe.[187] In den GMat[188] wird dazu erläutert, dass es zweifelhaft sei, ob es sich bei gespeicherten Daten überhaupt um (körperliche) Sachen iSd StGB handle. Aus diesem Grund sei es in Anbetracht von automationsunterstützt übermittelten Daten notwendig, den Schutz gegen unbefugte Eingriffe – gerade auch in der Phase ihrer Verarbeitung – gehörig zu gewährleisten und den strafrechtlichen Schutz vor einer unbefugten Datenbeschädigung durch einen neuen Straftatbestand deutlich klarzustellen. Ebenso wird bereits auf den Datenbegriff des DSG 1978 verwiesen, wobei über die dort erforderliche Personenbezogenheit der Daten hinaus in § 126a Abs 2 idF BGBl 605/1987 der deliktsspezifische Legalbegriff der Daten bereits näher definiert wurde. Darunter verstand man schon damals sowohl personenbezogene und nicht personenbezogene Daten als auch Programme.

Mit dem Inkrafttreten des StRÄG 1987[189] am 1. März 1988 wurden letztendlich zwei – nach den GMat abschließende[190] – Strafbestimmun-

184 Siehe OGH 12. 2. 1986, 9 Os 2/86.
185 Siehe unten S 239.
186 Vgl idS JAB 359 BlgNR XVII. GP, 17.
187 Zur Diskussion in der Lehre vgl *Fuchs,* RdW 1985, 330; *Jaburek/Schmölzer,* Computer-Kriminalität, 53 ff*; Seiler,* Kritische Anmerkungen zum StRÄG 1987 betreffend den Besonderen Teil des StGB, JB1 1989, 746; *Seiler* in SbgK § 125 Rz 6 (Stand August 1994); *Triffterer* in SbgK § 126a Rz 3 (aF Stand Dezember 1992); vgl weiters *Komenda/Madl* in SbgK § 126a Rz 3 (Stand Juni 2013); *Schmölzer,* EDVuR 1988, 20.
188 Vgl JAB 359 BlgNR XVII. GP, 17.
189 StRÄG 1987, BGBl 605/1987.
190 Siehe JAB 359 BlgNR XVII. GP, 16.

gen, nämlich die Datenbeschädigung (§ 126a) und der Betrügerische Datenverarbeitungsmissbrauch (§ 148a) im StGB normiert und die angesprochene Diskussion dadurch weitgehend abgebrochen.[191]

Mit der Einführung des § 148a wurde eine grundsätzlich unbestrittene[192] echte Strafbarkeitslücke geschlossen, da nunmehr auch Verhaltensweisen erfasst werden, die unter den klassischen Betrug nicht subsumierbar waren, aber dem Unwert eines Betruges entsprachen.[193] Bei der (betrügerischen) Manipulation von Datenverarbeitungsprozessen fehlte es bis dato an der erforderlichen Täuschung einer Person, um § 146 anwenden zu können. Zudem wurden mit diesem Schritt Daten erstmals als »eigenständiges schützenswertes Vermögensobjekt« anerkannt.[194]

3. UrhG-Novelle 1993[195] und StGB-Novelle 1994[196]

Die ansteigende Verlagerung von traditionellen Begehungsweisen auf informationstechnologisch gestützte bzw orientierte (Tat-)Handlungen brachte Modernisierungen und gemeinschaftsrechtliche Harmonisierungen[197] mit sich, die zunehmend computerstrafrechtliche Betrachtungen (iwS) für weitere Rechtsmaterien eröffneten. So ist etwa § 91 UrhG[198], zB iZm der widerrechtlichen digitalen Verwertung von geschützter Software, als Beispiel für die ins (Computer-)Nebenstrafrecht einzuordnenden Begehungsweisen ebenso zu nennen wie die durch die StGB-Nov 1994 im Kernstrafrecht normierte und damals mit

191 Siehe dazu vertiefend *Schick/Schmölzer,* EDVuR 1992, 107; weiters *Schmölzer,* Strafrecht, in Jahnel/Schramm/Staudegger (Hrsg), Informatikrecht² (2003) 335 (350); *Reindl,* E-Commerce, 103.

192 Außer bereits der Ablehnung zum Entwurf von *Fuchs,* RdW 1985, 330.

193 Vgl auch *Seiler,* JB1 1989, 746; ebenso *Schmölzer,* EDVuR 1988, 20; siehe aber krit zur Definition des Tatbestandes *Schmölzer* in Jahnel/Schramm/Staudegger, Informatikrecht², 335 (350); die Diskussionen darüber zusammenfassend *Reindl,* E-Commerce, 34 ff.

194 Siehe zuletzt *Schmölzer,* ZStW 2011/123, 709 (723) mwN;

195 UrhG-Nov 1993, BGBl 93/1993.

196 StGB-Nov 1994, BGBl 622/1994.

197 Siehe bspw die RL 91/250/EWG des Rates vom 14. Mai 1991 über den Rechtsschutz von Computerprogrammen, ABl L 1991/122, 42 in der kodifizierten Fassung RL 2009/24/EG des Europäischen Parlaments und des Rates vom 23. April 2009 über den Rechtsschutz von Computerprogrammen (kodifizierte Fassung), ABl L 2009/111, 16.

198 Urheberrechtsgesetz, BGBl 111/1936 idF I 99/2003.

»pornographische Darstellungen mit Unmündigen«[199] betitelte Bestimmung des § 207a[200] als Beispiel für Tatbegehungen ua auch mittels informationstechnischer modi operandi.

4. TKG

In § 102 TKG[201] wurde noch der Geheimnismissbrauch normiert, dessen Regelungsinhalt mit dem StRÄG 2002 ins Kernstrafrecht (§ 120 Abs 2a) überstellt wurde. Daneben existierte bereits in § 103 TKG die Strafbestimmung »Verletzung von Rechten der Benützer«, die inhaltlich nach wie vor Bestand hat.[202]

5. Notifikationsgesetz 1999[203]

Aufgrund europarechtlicher Vorgaben wurde es erforderlich auch »Dienste der Informationsgesellschaft« in das Notifikationsverfahren einzubeziehen. Dabei handelt es sich um Dienstleistungen, die drei wesentliche Kriterien erfüllen. Sie müssen 1. im Fernabsatz, 2. elektronisch und 3. auf individuellen Abruf des Empfängers erbracht werden.

Nach den GMat handle es sich bei Dienstleistungen, die im Fernabsatz erbracht werden, um solche, bei denen Erbringer und Empfänger nicht gleichzeitig physisch anwesend sind. Das treffe bspw auf die Online-Buchung eines Flugtickets zu, nicht aber auf die Buchung eines Flugtickets über ein Netzwerk, wenn sie zB in einem Reisebüro in Anwesenheit des Kunden vorgenommen wird.[204]

»Elektronisch« bedeutet idZ, dass die Dienstleistung über ein elektronisches Verarbeitungs- und Speicherungssystem derart erbracht werden muss, dass sowohl beim Sender als auch beim Empfänger eine elektronische Verarbeitung und Speicherung erfolgt. Daher sind Dienste, die zwar mit elektronischen Geräten, aber in materieller Form

199 Seit dem StRÄG 2004 (mehr dazu gleich im Anschluss) mit der Bezeichnung »Pornographische Darstellung Minderjähriger« betitelt.
200 StGB, BGBl 60/1974 idF 622/1994.
201 Telekommunikationsgesetz (1997), BGBl I 100/1997 aufgehoben durch BGBl I 134/2002.
202 Siehe S 52 f.
203 Notifikationsgesetz 1999, BGBl I 183/1999.
204 Siehe dazu ErlRV 1898 BlgNR XX. GP, 12.

erbracht werden (zB die Ausgabe von Geld oder Fahrkarten über Automaten), nicht von dieser Regelung betroffen.[205]

Auf individuellen Abruf des Empfängers wird eine Dienstleistung erbracht, wenn sie nur auf individuelle Anforderung erfolgt. Massenkommunikationen iSv »Punkt zu Mehrpunkt-Übertragungen« sind daher nicht erfasst.[206]

6. DSG 2000

Eine Aktualisierung des Datenschutzrechts in Österreich wurde erst durch die europäische Datenschutzrichtlinie[207] (in weiterer Folge: Datenschutz-RL) eingeleitet. Das Ergebnis bildete letztlich das DSG 2000[208], das am 1. Jänner 2000 in Kraft getreten ist.

Neben grundlegenden Veränderungen[209] des Grundrechts, wie zB der richtlinienkonformen Ausdehnung der Begleitgrundrechte auf Auskunft, Richtigstellung und Löschung bezüglich manuell geführter Dateien, wurde auch die Zuständigkeit in allen Fällen[210] der Durchsetzung des Auskunftsrechts bei der Datenschutzkommission[211] (DSK) festgemacht.[212]

Das Grundrecht auf Datenschutz ist systematisch eng mit dem Recht auf Achtung der Privatsphäre (Art 8 EMRK) verknüpft, was sich auch im ausdrücklichen Verweis darauf in § 1 Abs 2 DSG 2000 offenbart. Gleichwohl reicht das nationale Grundrecht auf Datenschutz, das

---

205 Vgl ErlRV 1898 BlgNR XX. GP, 12 mit weiteren Beispielen.

206 Vgl ErlRV 1898 BlgNR XX. GP, 12.

207 Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl L 1995/281, 31.

208 DSG 2000, BGBl I 165/1999.

209 Nachzulesen bei *Jahnel,* Handbuch, Rz 1/12 ff; ebenso *Dohr/Pollirer/Weiss/Knyrim,* DSG. Datenschutzrecht² § 1 Anm 3 (Stand 4.6.2013).

210 Sowohl bei Auftraggebern des öffentlichen Bereichs als auch bei denen, die in Formen des Privatrechts eingerichtet sind.

211 Mit der DSG-Novelle 2013 (BGBl I 57/2013) wurde – nach dem Urteil des EuGH [EuGH 16.10.2012, C-614/10 (Kommission/Österreich) = jusIT 2012/100, 211 *(Pachinger)* = AnwBl 2013, 71 *(Winkler)* = ZfRV 2014/7, 52 *(Bresich/Riedl/Souhrada-Kirchmayer)* = ÖZW 2013, 21 *(Pabel)]* – *die* vollständige Unabhängigkeit der DSK iSd Art 28 Abs 1 Datenschutz-RL sichergestellt. Mit der DSG-Novelle 2014 (BGBl I 83/2013) wurde mit 1. Jänner 2014 – im Wesentlichen aufgrund der Verwaltungsgerichtsbarkeits-Nov 2012 (BGBl I 51/2012) – die DSK aufgehoben und eine »Datenschutzbehörde« eingesetzt (siehe dazu teils krit *Jahnel,* Gesetzgebungsmonitor Datenschutz: DSG-Novellen 2013 und 2014 kundgemacht, jusIT 2013/66, 142).

212 Siehe § 1 Abs 5 DSG 2000.

durch Art 8 GRC[213] im Geltungsbereich des EU-Rechts ergänzt wurde, weiter als Art 8 EMRK, da durch die Formulierung »insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens« im ersten Satzteil des § 1 Abs 1 DSG 2000 ausgedrückt wird, dass der Geheimhaltungsanspruch nicht ausschließlich auf den Schutz der Privatsphäre abzielt.[214] Dadurch reicht das Grundrecht auf Datenschutz bis in den Bereich des wirtschaftlichen und politischen Lebens hinein.[215] Darüber hinaus sieht § 1 DSG 2000 weitere Begleitgrundrechte (auf Auskunft, Richtigstellung und Löschung) zur Durchsetzung des zentralen Grundrechts auf Geheimhaltung (§ 1 Abs 1 DSG 2000) vor.[216]

Im Zuge der Novellierung der einfachgesetzlichen Bestimmungen wurde die Legaldefinition von »personenbezogenen Daten« in § 4 Z 1 DSG 2000 richtlinienkonform angepasst, sodass die Wendung »auf einem Datenträger festgehaltene«[217] entfallen musste.

Im DSG 2000 wirkten sich aber ebenso nationale dogmatische Modernisierungstendenzen des StGB aus, nämlich derart, dass § 49 DSG 1978 überhaupt – mangels praktischer Anwendbarkeit[218] – beseitigt wurde und eine gerichtliche Strafbarkeit lediglich dann vorliegen soll, wenn eine rechtswidrige Verwendung von Daten in besonders verwerflicher Gewinnerzielungs- oder Schädigungsabsicht gegeben ist. Als einzige Strafbestimmung wurde daher § 51 DSG 2000 unter der Deliktsbezeichnung »Datenverwendung in Gewinn- oder Schädigungsabsicht« geschaffen. Um dabei nicht mit inzwischen normierten gerichtlichen Straftatbeständen ähnlicher Regelungszwecke zu konkurrieren,

213 Charta der Grundrechte der Europäischen Union, ABl C 2007/303, 1 idF C 2012/326, 391.

214 *Jahnel,* Das Grundrecht auf Datenschutz nach dem DSG 2000, in Akyürek/Baumgartner/Jahnel/Lienbacher/Stolzlechner (Hrsg), Staat und Recht in europäischer Perspektive, FS Schäffer (2006) 313 (321); *Berka,* Geheimnisschutz – Datenschutz – Informationsschutz im Lichte der Verfassung, in Studiengesellschaft für Wirtschaft und Recht (Hrsg), Geheimnisschutz – Datenschutz – Informationsschutz (2008) 53 (63); *Kotschy,* Grundrechte und staatliche EDV-Register, in OJK (Hrsg), Grundrechte in der Informationsgesellschaft (2001) 88 (89).

215 Vgl *Dohr/Pollirer/Weiss/Knyrim,* DSG² § 1 Anm 5.

216 Vgl *Wiederin* in Korinek/Holoubek (Hrsg), Bundesverfassungsrecht. Bd III Art 8 EMRK Rz 136 (Stand 2002).

217 In der Stammfassung des DSG 1978 wurde in § 3 Z 1 die Wortfolge »auf einem Datenträger gespeicherte Angaben« verwendet. Die DSG-Nov 1986 (BGBl 370/1986) änderte diese Formulierung in »auf einem Datenträger festgehaltene Angaben«.

218 »§ 49 wiederum enthält einen Tatbestand, dessen Verwirklichung sich als praktisch unmöglich erwiesen hat, sodaß er schon aus diesem Grunde zu beseitigen ist« (vgl ErlRV 1613 BlgNR XX. GP, 32).

wurde als Tathandlung die Benützung sowie die Weitergabe von Daten, insb ihre Veröffentlichung, unter Strafe gestellt.[219]

Anstelle des vormals gerichtlich strafbaren Geheimnisbruchs gem § 48 DSG 1978 wurden in Folge weitere Tatbestände in den Katalog der Verwaltungsübertretungen des § 52 DSG 2000 aufgenommen, deren Definitionen sich ua im hier interessierenden Kontext an der Verletzung des Datengeheimnisses wie auch an der Verschaffung eines vorsätzlich widerrechtlichen Zugangs zu einer Datenanwendung oder der Aufrechterhaltung eines erkennbar widerrechtlichen Zugangs orientieren.

7. ZuKG

Das zunehmende wirtschaftliche Interesse an illegalen Vorrichtungen, die den Empfang von Internet- oder Rundfunkdiensten, Pay-TV oder sonstigen online-Dienstleistungen ohne Genehmigung des Diensteanbieters ermöglichen, war der Hintergrund der gemeinschaftsrechtlichen Vorgaben[220], die die Ursache der Schaffung der Strafbestimmung des § 10 Zugangskontrollgesetzes[221] bildeten. Darin werden gewerbsmäßige Tathandlungen derartige Umgehungsvorrichtungen betreffend pönalisiert.[222]

8. Cybercrime-Konvention des Europarates

Der Europarat hatte es sich bis Ende des Jahres 2000 zum Ziel gesetzt, ein Übereinkommen über Computerkriminalität (»Convention on Cybercrime«[223]) auszuarbeiten, da er ua von der Notwendigkeit überzeugt war, »eine gemeinsame Strafrechtspolitik zu verfolgen, die den Schutz

219 Vgl ErlRV 1613 BlgNR XX. GP, 54.

220 Richtlinie 98/84/EG über den rechtlichen Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten, ABl L 1998/320, 54; sowie Richtlinie 2001/29/EG zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft, ABl L 2001/167, 10 idF L 2002/6, 71.

221 ZuKG, BGBl I 60/2000 idF I 32/2001.

222 Vgl ErlRV 99 BlgNR XXI. GP, 6.

223 Convention on Cybercrime (ETS 185) vom 23.11.2001, <conventions.coe.int/Treaty/en/Treaties/Html/185.htm> (01.04.2014). Sie trat am 1. Juli 2004 mit der Ratifikation des fünften Staates (inkl zumindest dreier Mitgliedstaaten des Europarates) in Kraft. Österreich hat das »Übereinkommen über Computerkriminalität« erst mit BGBl III 140/2012 formell ratifiziert.

der Gesellschaft vor Computerkriminalität, unter anderem durch die Annahme geeigneter Rechtsvorschriften und die Förderung der internationalen Zusammenarbeit, zum Ziel hat«.[224]

Dazu wurde bereits im Jahr 1996 vom European Committee on Crime Problems (CDPC) das »Committee of Experts on Crime in Cyberspace« eingesetzt.[225] Am 23.11.2001 wurde die »Convention on Cybercrime« in Budapest von vielen[226] Mitgliedstaaten des Europarats unterzeichnet, darunter Österreich[227], aber auch von Nichtmitgliedstaaten wie etwa Kanada und Südafrika, die die CCC zumindest unterzeichnet haben, und die USA und Japan, wo die CCC jeweils bereits auch ratifiziert wurde.[228]

Die CCC ist das erste völkerrechtliche (und damit richtungsweisende) Instrument auf dem Gebiet der Bekämpfung der Computerkriminalität. Sie dient als Leitlinie für jeden Staat, der eine umfassende nationale Gesetzgebung gegen Computerkriminalität ausarbeiten möchte, und bietet einen Rahmen für die internationale Zusammenarbeit zwischen den Vertragsstaaten des Übereinkommens.[229]

In erster Linie erfasst die CCC Handlungen gegen die Vertraulichkeit, Unversehrtheit und Verfügbarkeit von Computersystemen, Netzwerken und Computerdaten sowie den Missbrauch solcher Systeme und Daten, wobei auch strafprozessuale Maßnahmen harmonisiert bzw das Rechtshilfesystem für länderüberschreitende Kooperationen verbessert werden sollen.[230]

---

224 Siehe Präambel der CCC.

225 European Committee on Crime Problems (CDPC), CDPC/103/211196.

226 Der Europarat hat aktuell 47 Mitgliedstaaten (einschließlich aller EU-Mitgliedstaaten); Russland und San Marino haben bis heute die CCC nicht unterzeichnet; einige EU-Mitgliedstaaten haben die CCC zwar unterzeichnet, bis heute aber nicht ratifiziert (wie Griechenland, Luxemburg, Polen, Schweden, Tschechien).

227 Österreich hat die CCC am 23.11.2001 unterzeichnet, mit dem StRÄG 2002 faktisch umgesetzt, aber erst mit BGBl III 140/2012 formell ratifiziert (siehe dazu *Bergauer,* Gesetzgebungsmonitor Computerstrafrecht: Ratifikation des Übereinkommens über Computerkriminalität, jusIT 2012/95, 205).

228 Zum aktuellen Stand der Ratifikationen der CCC (ETS 185) siehe <conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG> (01.04.2014).

229 Siehe ErlStV 1645 BlgNR XXIV. GP, 2.

230 Siehe die Entstehungsgeschichte zusammenfassend *Schuh,* Computerstrafrecht im Rechtsvergleich – Deutschland, Österreich, Schweiz (2012) 35 ff; vgl ErlStV 1645 BlgNR XXIV. GP, 2.

Da zwischen den Staaten nicht in allen Punkten – wie etwa was rassistische Straftaten anlangt – Einigkeit bestand, musste ein Zusatzprotokoll[231] zur CCC geschaffen werden, um eine Unterzeichnung und Ratifikation der CCC zB durch die USA zu ermöglichen.[232] Österreich hat dieses Zusatzprotokoll am 30. Jänner 2003 unterzeichnet, formell ratifiziert wurde es bis heute nicht.[233]

9. StRÄG 2002

Mit der (Teil-)Umsetzung der CCC hat der nationale Gesetzgeber im Bereich des Computerstrafrechts ieS umfangreiche legistische Maßnahmen gegen die moderne Computerkriminalität gesetzt. Durch das StRÄG 2002[234] wurden dabei spezifische Computerdelikte verankert, wie zB §§ 118a, 119, 119a, 126b, 126c, 225a.

Im Hinblick darauf, dass nunmehr nicht bloß in zwei Strafbestimmungen (nämlich §§ 126a, 148a) der Begriff »Daten« Verwendung findet, wurde in § 74 Abs 2 eine generelle »Begriffsbestimmung«[235] für das Strafgesetzbuch normiert. Dies nicht zuletzt deshalb, weil auch im DSG 2000 keine allgemeine Definition des Datenbegriffs vorgesehen ist, die Daten als Informationen[236], die zur automationsunterstützten Verarbeitung aufbereitet wurden, erfasst.[237]

231 Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS 189), <conventions.coe.int/Treaty/en/Treaties/Html/189.htm> (01.04.2014); Es trat am 1. März 2006 durch die fünfte Ratifikation in Kraft.

232 Siehe *Schuh,* Computerstrafrecht, 44 mwN.

233 Siehe den aktuellen Stand der Ratifikationen des Zusatzprotokolls (ETS 189) siehe <conventions.coe.int/Treaty/Commun/ChercheSig.asp?CL=GER&CM=&NT=189&DF=&VL> (01.04.2014); vgl auch *Bergauer,* Gesetzgebungsmonitor Computerstrafrecht: Ratifikation des Übereinkommens über Computerkriminalität, jusIT 2012/95, 205.

234 StRÄG 2002, BGBl I 134/2002.

235 Genauer gesagt handelt es sich dabei bloß um eine inhaltliche Konkretisierung und keine Definition (siehe dazu S 60 ff).

236 Als Information versteht man im Wesentlichen »Daten mit Bedeutungsinhalt«.

237 Vgl ErlRV 1166 BlgNR XXI. GP, 23.

10. E-Commerce-Gesetz

Mit Umsetzung der RL 2000/31/EG[238] wurde das ECG[239] geschaffen, welches rechtliche Aspekte des elektronischen Geschäfts- und Rechtsverkehrs (insb Informationspflichten) und darüber hinaus auch Haftungsprivilegien für diverse Diensteanbieter (Provider[240]) behandelt. Generell erfasst der Anwendungsbereich des ECG »Dienste der Informationsgesellschaft«, welche in der Regel gegen Entgelt elektronisch im Fernabsatz auf individuellen Abruf des Empfängers bereitgestellt werden (§ 3 Z 1 ECG iVm § 1 Abs 1 Z 2 NotifG 1999). Gleichwohl gelten die Haftungsbegünstigungen auch für unentgeltliche elektronische Dienste (§ 19 Abs 2 ECG).[241] Das ECG berücksichtigt zudem – über die Richtlinie hinaus – noch die Verantwortlichkeit von Suchmaschinenbetreibern (§ 14 ECG) und die Linkhaftung (§ 17 ECG). Für das (internationale) Strafrecht kann das Herkunftslandprinzip (§§ 20 ff ECG) relevant werden, das für (kommerziell handelnde) Provider vorgibt, dass diese den rechtlichen Anforderungen des Mitgliedstaates unterliegen, in dem sie niedergelassen sind.

11. TKG 2003

In § 108 TKG 2003[242] findet sich weiterhin die (nunmehr einzige) Strafbestimmung des TKG über die »Verletzung von Rechten der Benützer«, welche ausschließlich Betreiber eines öffentlichen Kommunikationsnetzes oder -dienstes und alle Personen, die an der Tätigkeit eines solchen mitwirken, zur Geheimhaltung der Tatsachen oder der Inhalte des Telekommunikationsverkehrs bestimmter Personen verpflichtet (§ 108 Abs 1 Z 1 TKG 2003). Darüber hinaus dürfen sie gegenüber dem

238 Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt (»Richtlinie über den elektronischen Geschäftsverkehr«), ABl L 2000/178, 1.

239 E-Commerce-Gesetz, BGBl I 152/2001 idF I 34/2015.

240 Darunter versteht man Internet Service Provider (ISP), wie Access-, Caching- oder Host-Provider.

241 Siehe zur Providerhaftung im Strafrecht etwa *Bergauer,* Das Betreiben eines Anonymisierungsdienstes im Internet als strafbarer Beitrag zur Verbreitung von Kinderpornografie? Zugleich eine Anmerkung zu LG für Strafsachen Graz 30.6.2014, 7 Hv 39/14p, jusIT 2014/77, 161.

242 BGBl I 70/2003.

Empfangsberechtigten keinerlei Veränderungen an der Nachricht vornehmen oder sie ihm vorenthalten (§ 108 Abs 1 Z 2 TKG 2003).

12. StRÄG 2004

Mit dem StRÄG 2004[243] wurde in erster Linie der EU-RB[244] vom 28. Mai 2001 zur Bekämpfung von Betrug und Fälschung iZm unbaren Zahlungsmitteln (zB Kreditkarte, Bankomatkarte, Wechsel, Scheck, Reisescheck) ins nationale Recht umgesetzt. Daneben wurden kleinere Anpassungen an den hier interessierenden speziellen Computerdelikten (insb die Erweiterung der Tathandlungen des § 126c um das »Sich-Verschaffen« und »Besitzen« und die Ergänzung des § 148a als eines der Hauptdelikte in § 126c Abs 1 Z 1) vorgenommen. Ebenso wurde § 207a in erster Linie auf Grundlage internationaler und europarechtlicher Vorgaben[245] in mehrfacher Hinsicht novelliert, weshalb dieses Delikt im Bereich des Computerstrafrechts in Form von kinderpornographischen Realdarstellungen bei entsprechenden Tathandlungen über die Dienste der IKT bzw bei computergenerierter »virtueller Pornografie«[246] in Erscheinung tritt.

13. EU-Rahmenbeschluss über Angriffe auf Informationssysteme

Auf EU-Ebene wurde am 24. 02. 2005 der Rahmenbeschluss[247] 2005/222/JI über Angriffe auf Informationssysteme erlassen. Der RB stellt darauf

---

243 StRÄG 2004, BGBl I 15/2004.

244 Rahmenbeschluss 2001/413/JI zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln vom 28. 5. 2001, ABl L 2001/149, 1. »EU-RB« steht in weiterer Folge für einen Rahmenbeschluss der (damals noch) dritten Säule (polizeiliche und justizielle Zusammenarbeit in Strafsachen) der Europäischen Union und soll der schnelle Abgrenzung zu Rechtsakten internationaler Organisationen – wie dem Europarat – dienen.

245 Convention on Cybercrime (ETS 185), <conventions.coe.int/Treaty/en/Treaties/Html/185.htm> (01. 04. 2014); weiters Rahmenbeschluss 2004/68/JI des Rates vom 22. Dezember 2003 zur Bekämpfung der sexuellen Ausbeutung von Kindern und der Kinderpornografie, ABl L 2004/13, 44; ebenso VN-Fakultativprotokoll zum Übereinkommen über die Rechte des Kindes betreffend den Verkauf von Kindern, die Kinderprostitution und die Kinderpornografie, BGBl III 93/2004.

246 Vgl *Hinterhofer* in SbgK § 207a Rz 43 ff (Stand November 2006); *Schick* in WK² § 207a Rz 14 (aF Stand Mai 2007).

247 Rahmenbeschluss 2005/222/JI des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme, ABl L 2005/69, 67.

ab, durch Angleichung der einzelstaatlichen Strafrechtsvorschriften für Angriffe auf Informationssysteme die Zusammenarbeit zwischen den Justiz- und sonstigen zuständigen Behörden, einschließlich der Polizei und anderer spezialisierter Strafverfolgungsbehörden der Mitgliedstaaten, zu verbessern. Dabei soll das Strafrecht – was den Bereich der Angriffe auf Informationssysteme betrifft – angeglichen werden, um eine möglichst effiziente polizeiliche und justizielle Zusammenarbeit bei Straftaten iVm Angriffen auf Informationssysteme sicherzustellen und einen Beitrag zur Bekämpfung der organisierten Kriminalität und des Terrorismus zu leisten.[248]

Da sich in vielen Bereichen die Vorgaben aus der CCC mit jenen des EU-RB 2005/222/JI überschneiden und die CCC großteils bereits mit dem StRÄG 2002 in innerstaatliches Recht umgesetzt wurde, war hins des RB nur ein geringer Anpassungsbedarf gegeben, welcher mit dem StRÄG 2008[249] realisiert wurde.[250] Mittlerweile liegt bereits ein Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Angriffe auf Informationssysteme und zur Aufhebung des EU-RB 2005/222/JI des Rates vor.[251]

14. StRÄG 2008

Im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen der EU wurde der RB 2005/222/JI über Angriffe auf Informationssysteme gefasst, der jedoch aufgrund der bereits vollzogenen Umsetzung der CCC eine Transferierung in nationales Recht lediglich in einem geringen Umfang erforderte. Mit dem StRÄG 2008[252] wurden daher in erster Linie rahmenbeschlusskonform weitere Qualifikationen von einschlägigen Delikten (wie zB § 126b Abs 2) geschaffen, Tatbestände

248 Siehe dazu die Erwägungsgründe zum Rahmenbeschluss 2005/222/JI des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme, ABl L 2005/69, 67.

249 StRÄG 2008, BGBl I 109/2007.

250 Siehe ErlRV 285 BlgNR XXIII. GP, 3.

251 Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Angriffe auf Informationssysteme und zur Aufhebung des Rahmenbeschlusses 2005/222/JI des Rates, KOM (2010) 517 endg.

252 StRÄG 2008, BGBl I 109/2007.

neben kleineren dogmatischen Anpassungen[253] auch hins einer Tatbegehung durch Mitglieder einer kriminellen Vereinigung konkretisiert (zB § 118a Abs 3, § 126a) und dabei Strafdrohungen angehoben.

15. Zweites Gewaltschutzgesetz 2009

Durch das zweite Gewaltschutzgesetz[254] wurden ua eine Sexualstraftäterdatei[255] eingeführt und ein neuer Abs 3a in § 207a geschaffen, der nunmehr auch denjenigen pönalisiert, der im Internet wissentlich auf eine pornographische Darstellung Minderjähriger zugreift.

16. DSG-Novelle 2010

Durch die DSG-Novelle 2010[256] wurden neben weiteren Adaptierungen – insb der Berücksichtigung von speziellen Vorschriften über die Videoüberwachung und Anpassungen bzw Ergänzungen der Verwaltungsstraftatbestände des § 52 DSG 2000 – auch eine etwas abgeänderte Strafbestimmung des § 51 DSG 2000 kodifiziert, die nun durch Entfall des vorher existenten Abs 2 von einem Ermächtigungsdelikt zu einem reinen Offizialdelikt erhoben wurde, was deutlich auf eine generelle Aufwertung des Datenschutzes in der Gesetzgebungstendenz schließen lässt.[257]

17. Strafgesetznovelle 2011

Insbesondere in Umsetzung des Übereinkommens des Europarates zum Schutz von Kindern vor sexueller Ausbeutung und sexuellem

253 Wesentlich ist dabei die Änderung der Definition des Tatbestands des § 118a Abs 1 dahingehend, dass anstelle des Erfordernisses der »Verletzung« einer spezifischen Sicherheitsvorkehrung, nun die »Überwindung« derselben schon als strafbarkeitsbegründend ausreichend ist.

254 2. GeSchG, BGBl I 40/2009.

255 Darunter wird die besondere Kennzeichnung einer strafbaren Handlung gegen die sexuelle Integrität und Selbstbestimmung im Strafregister für Zwecke der (neugeschaffenen) Sonderauskunft zu Sexualstraftätern verstanden; siehe § 2 Abs 1a und § 9a Strafregistergesetz 1968, BGBl 1968/277 idF I 107/2014.

256 DSG-Novelle 2010, BGBl I 133/2009.

257 Zu den einzelnen Modifikationen des § 51 DSG 2000 durch die DSG-Nov 2010 siehe ausf *Bergauer,* Änderungen der strafrechtsrelevanten Bestimmungen des DSG 2000 durch die Novelle 2010, in Jahnel (Hrsg), Datenschutzrecht. Jahrbuch 2010 (2010) 73 (73 ff).

Missbrauch (CETS 201)[258] wurden mit der Strafgesetznovelle 2011[259] neue Strafbestimmungen zum Schutz von Kindern geschaffen.

Die Novellierung greift zudem den Umsetzungen der Richtlinie 2011/93/EU des Europäischen Parlaments und des Rates vom 13. Dezember 2011 zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie sowie zur Ersetzung des Rahmenbeschlusses 2004/68/JI des Rates[260], und zum Teil auch der Richtlinie 2011/36/EU zur Verhütung und Bekämpfung des Menschenhandels und zum Schutz seiner Opfer sowie zur Ersetzung des Rahmenbeschlusses 2002/629/JI des Rates[261] vor.[262]

Hervorzuheben ist die Normierung der neuen Straftatbestände gegen die Anbahnung von Sexualkontakten zu Unmündigen[263] (§ 208a[264]) und die wissentliche Betrachtung pornographischer Darbietungen Minderjähriger (§ 215a Abs 2a[265]).

18. Ratifikation der Cybercrime-Konvention

Die CCC wurde im Jahr 2012, elf Jahre nach ihrer Unterzeichnung und zehn Jahre nach ihrer faktischen Teilumsetzung, in Ö ratifiziert. Das Übereinkommen über Computerkriminalität trat gem Art 36 Abs 4 CCC für Ö mit 1. Oktober 2012 in Kraft. Mit BGBl III 140/2012 wurde die Ratifikation des Übereinkommens über Computerkriminalität kundgemacht, weshalb grundsätzlich erst mit diesem Formalakt innerstaatlich

258 Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201) <conventions.coe.int/Treaty/en/Treaties/Html/201.htm> (01.04.2014); BGBl III 96/2011.

259 BGBl I 130/2011.

260 Richtlinie 2011/93/EU des Europäischen Parlaments und des Rates vom 13. Dezember 2011 zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie sowie zur Ersetzung des Rahmenbeschlusses 2004/68/JI des Rates, ABl L 2011/335, 1 idF L 2012/18.

261 Richtlinie 2011/36/EU des Europäischen Parlaments und des Rates vom 5. April 2011 zur Verhütung und Bekämpfung des Menschenhandels und zum Schutz seiner Opfer sowie zur Ersetzung des Rahmenbeschlusses 2002/629/JI des Rates, ABl L 2011/101, 1.

262 Vgl ErlRV 1505 BlgNR XXIV. GP, 4.

263 Auch als »Grooming«-Bestimmung bekannt.

264 Eingeführt mit BGBl I 130/2011 und um Abs 1a ergänzt durch BGBl I 116/2013.

265 Eingeführt mit BGBl I 130/2011.

ein verbindlicher Staatsvertrag vorliegt.[266] Das Zusatzprotokoll (ETS 189) wurde aber nach wie vor (noch) nicht ratifiziert.

19. Errichtung eines Europäischen Zentrums zur Bekämpfung der Cyberkriminalität

Trotz der europäischen Bestrebungen der effizienten Untersuchung von Cyberstraftaten und der wirksamen Verfolgung der Täter auf EU-Ebene bestehen noch immer Hindernisse: wie etwa »Grenzen der Gerichtsbarkeit, unzureichende Möglichkeiten für den Austausch sachdienlicher Erkenntnisse, technische Probleme bei der Ermittlung der Täterherkunft, ungleiche Kapazitäten für Untersuchungen und computerforensische Maßnahmen, Mangel an Fachpersonal und uneinheitliche Zusammenarbeit mit anderen für die Sicherheit im Internet zuständigen Stellen«.[267] Um diesen Herausforderungen zu begegnen, hat die Kommission die Einrichtung eines Europäischen Zentrums zur Bekämpfung der Cyberkriminalität zu einem vorrangigen Ziel der EU-Strategie der inneren Sicherheit erhoben.[268] Das »Europäische Zentrum zur Bekämpfung der Cyberkriminalität (EC3)« mit seinem Sitz beim Europäischen Polizeiamt (Europol) in Den Haag wurde am 11.01.2013 offiziell eröffnet[269] und soll nun als zentrale Anlaufstelle für den europaweit geführten Kampf gegen die Cyberkriminalität dienen. Überwiegender Zweck dieser Einrichtung ist es, Fachwissen zu bündeln, strafrechtliche Untersuchungen zu unterstützen und EU-weite Lösungen zu fördern sowie in der ganzen Union das Bewusstsein für die Problematik der Cyberkriminalität zu schärfen.[270]

---

266 Siehe *Bergauer,* jusIT 2012/95, 205.

267 Mitteilung der Kommission an den Rat und das Europäische Parlament Kriminalitätsbekämpfung im digitalen Zeitalter: Errichtung eines Europäischen Zentrums zur Bekämpfung der Cyberkriminalität, KOM (2012) 140 endg.

268 Mitteilung der Kommission an das Europäische Parlament und den Rat EU-Strategie der inneren Sicherheit: Fünf Handlungsschwerpunkte für mehr Sicherheit in Europa, KOM (2010) 673 endg.

269 Siehe <www.europol.europa.eu/ec3> (01.04.2014).

270 Siehe die Mitteilung der Kommission an den Rat und das Europäische Parlament Kriminalitätsbekämpfung im digitalen Zeitalter: Errichtung eines Europäischen Zentrums zur Bekämpfung der Cyberkriminalität, KOM (2012) 140 endg.

20. Sexualstrafrechtsänderungsgesetz 2013[271]

Art 6 Abs 2 Richtlinie 2011/93/EU[272] sieht einen Tatbestand vor, der bisher in keiner internationalen Vorgabe enthalten war. Demnach haben die Mitgliedstaaten sicherzustellen, dass der Versuch eines Erwachsenen, mit Mitteln der Informations- und Kommunikationstechnologie eine Straftat nach Art 5 Abs 2 und 3 zu begehen, indem er Kontakt zu einer unmündigen Person aufnimmt, um kinderpornografische Darstellungen dieser Person zu erhalten, strafbar ist.[273] Aus diesem Grund wurde § 208a um den Abs 1a erweitert, der denjenigen pönalisiert, der zu einer unmündigen Person, in der Absicht, eine strafbare Handlung nach § 207a Abs 3 oder 3a StGB in Bezug auf eine pornographische Darstellung (§ 207a Abs 4 StGB) dieser Person zu begehen, im Wege einer Telekommunikation oder unter Verwendung eines Computersystems Kontakt herstellt.

21. Richtlinie 2013/40/EU über Angriffe auf Informationssysteme

Da nicht alle EU-Mitgliedstaaten[274] die CCC ratifiziert haben[275] und die Computerkriminalität ein Vorgehen auf EU-Ebene erfordere, um dem gegenwärtigen Trend zu groß angelegten Computerattacken in Europa und weltweit entgegenzuwirken, sollen entsprechende Maßnahmen auf EU-Ebene durchgeführt werden.[276] Die Mitgliedstaaten seien nämlich allein nicht in der Lage, die Bürger wirksam vor Cyberangriffen zu

271 BGBl I 116/2013.

272 Richtlinie 2011/93/EU des Europäischen Parlaments und des Rates vom 13. Dezember 2011 zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie sowie zur Ersetzung des Rahmenbeschlusses 2004/68/JI des Rates, ABl L 2011/335, 1 idF L 2012/18.

273 Vgl ErlRV 2319 BlgNR XXIV. GP, 18.

274 Die EU selbst hat das Übereinkommen ebenfalls nicht unterzeichnet.

275 Siehe zum aktuellen Stand der Ratifikationen der CCC (ETS 185) <conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG> (01.04.2014).

276 Vgl dazu auch in die »Digitale Agenda für Europa« – die erste Leitinitiative, die im Rahmen der Strategie Europa 2020 angenommen wurde – und in der die Notwendigkeit festgehalten wird, dem Aufkommen neuer Formen der Kriminalität, insbesondere der Cyberkriminalität, auf europäischer Ebene Einhalt zu gebieten [Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – Eine Digitale Agenda für Europa, KOM (2010) 245 endg/2].

schützen.[277] Anstelle des RB wurde daher eine Richtlinie über Angriffe auf Informationssysteme[278] ausgearbeitet, die das materielle Strafrecht und die Verfahrensvorschriften der Mitgliedstaaten stärker als bisher angleichen soll. Nach Meinung der Kommission werden durch das Regelungsinstrument einer Richtlinie die Ziele des Vorschlags (und schließlich auch die Bekämpfung der Computerkriminalität) besser erreicht. Straftäter würden auf diese Weise davon abgehalten werden, sich in Mitgliedstaaten zu begeben, in denen Cyberangriffe weniger hart bestraft werden. Des Weiteren würden einheitliche Definitionen den Austausch von Informationen und die Erhebung und den Abgleich relevanter Daten für die Strafverfolgung fördern und die Wirkung von Präventivmaßnahmen in der EU sowie die internationale Zusammenarbeit verstärken.[279] Die Kommission berichtete bereits im Jahr 2008[280], dass der EU-RB 2005/222/JI nicht auf Bedrohungen durch sog »Botnets« ausgerichtet war, welche aber in jüngster Zeit insb durch massive gleichzeitige Angriffe auf Informationssysteme in Erscheinung traten. Die Richtlinie sollte daher diesen »neuen« Methoden der Internetkriminalität Rechnung tragen.

Am 14.08.2013 wurde die Richtlinie 2013/40/EU über Angriffe auf Informationssysteme und Ersetzung des Rahmenbeschlusses 2005/222/JI[281] kundgemacht, welche am 03.09.2013 in Kraft getreten ist und bis zum 04.09.2015 von den Mitgliedstaaten umgesetzt werden muss.[282]

Ein etwaiger Umsetzungsbedarf wurde auch von der Arbeitsgruppe »StGB 2015« untersucht und in ihrem Abschlussbericht angemerkt.[283]

---

277 Siehe dazu den Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Angriffe auf Informationssysteme und zur Aufhebung des Rahmenbeschlusses 2005/222/JI des Rates KOM (2010) 517 endg 9.

278 Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Angriffe auf Informationssysteme und zur Aufhebung des Rahmenbeschlusses 2005/222/JI des Rates KOM (2010) 517 endg.

279 Siehe dazu KOM (2010) 517 endg 9.

280 Bericht der Kommission an den Rat auf der Grundlage von Artikel 12 des Rahmenbeschlusses des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme, KOM (2008) 448 endg.

281 Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates vom 12. August 2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates, ABl L 2013/218, 8.

282 Siehe dazu weiterführend *Sonntag,* Die EU-Richtlinie über Angriffe auf Informationssysteme, jusIT 2014/2, 8.

283 Bericht des Bundesministers für Justiz über die Fortschritte der Reformgruppe zum Strafgesetzbuch aufgrund der Entschließung des Nationalrates vom 29.4.2014, E 17-NR/XXV. GP; »StGB 2015« Bericht der Arbeitsgruppe, III-104 BlgNR

Schließlich soll diesem mit dem StRÄG 2015[284], welches am 01.01.2016 in Kraften treten soll, Rechnung getragen werden.

22. StRÄG 2015

Mit der RV zum StRÄG 2015[285] werden gravierende Änderungen insb auch im Bereich des Computerstrafrechts vorgeschlagen. Insbesondere werde neben inhaltlichen Ausdehnungen der §§ 118a, 126a und 126b und einer Neudefinition der »Gewerbsmäßigkeit«, generell die Wertgrenzen der Qualifikationstatbestände von derzeit € 3.000,– auf € 5.000,– und von € 50.000,– auf € 300.000,– angehoben. Darüber hinaus wird auch ein neuer Erschwerungsgrundes in § 33 Abs 1 Z 8 eingeführt, der auf die Tatbegehung unter Missbrauch der personenbezogenen Daten einer anderen Person abstellt, wenn dadurch das Vertrauen eines Dritten gewonnen wurde, wodurch dem rechtmäßigen Identitätseigentümer ein Schaden zugefügt wird. Daneben wird die Einführung einer Qualifikationsbestimmung hins des Selbstmordes in § 107a StGB sowie von neuen Tatbeständen, nämlich § 107c StGB »Fortgesetzte Belästigung im Wege einer Telekommunikation oder eines Computersystems« für Erscheinungsformen des sog »Cybermobbing« und § 241h »Ausspähen von Daten eines unbaren Zahlungsmittels«, angestrebt. Da die RV zum StRÄG 2015 erst kurz vor Drucklegung im NR (mit einigen Abänderungen) beschlossen wurde, finden die wesentlichsten Änderungen zusammengefasst nur mehr in Kapitel IV »Ausblick ›StRÄG 2015‹« Berücksichtigung.

E. Datenbegriff im Strafrecht

> § 74[286] [Auszug] (2) Im Sinne dieses Bundesgesetzes sind Daten sowohl personenbezogene und nicht personenbezogene Daten als auch Programme.

XXV. GP, <www.parlament.gv.at/PAKT/VHG/XXV/III/III_00104/imfname_366604.pdf> (03.03.2015).

284 RV 689 BlgNR XXV. GP in der Fassung des Beschlusses des Nationalrates vom 07.07.2015 (204/BNR XXV. GP).

285 RV 689 BlgNR XXV. GP in der Fassung gem der Änderungen im Plenum des NR gegenüber dem ursprünglichen Entwurf (9403 BlgBR XXV. GP).

286 BGBl 60/1974 idF I 61/2012.

Mit dem StRÄG 2002 hat der Gesetzgeber eine »Legaldefinition«[287] des Begriffs »Daten« mit § 74 Abs 2 im Strafgesetzbuch normiert. Davor war lediglich für § 126a Abs 2 idF BGBl 605/1987 klargestellt worden, dass sich »der Schutz auch auf nicht personenbezogene Daten und auf Programme erstreckt«.[288]

1. Daten in einem engen und weiten Verständnis

Unter »Daten« versteht man aktuell im kernstrafrechtlichen Sinn sowohl personenbezogene und nicht personenbezogene Daten als auch Programme. Es handelt sich dabei aber nicht tatsächlich um eine Definition, sondern um eine (semantisch/pragmatische[289]) Umfangbeschreibung des Anwendungsbereichs bzw inhaltliche Abgrenzung, welche Inhalte von dem in einem Tatbestand verwendeten Begriff »Daten« erfasst werden. Gemeint ist daher eine Abgrenzung den Informationswert bzw die Information selbst betreffend (Daten im weiten Sinn) und – die angeführten »Programme« ausgenommen[290] – nicht die elektronische Verarbeitungs- bzw Darstellungsform der Information, die hier als »Daten im engen Sinn« bzw generell als »Computerdaten«[291] bezeichnet werden.

Die Menge der möglichen Bedeutungen einer Information bestimmt sich im Übrigen nach dem jeweiligen Abstraktionsgrad. Das bedeutet, dass ein einzelnes Zeichen in einem entsprechenden Kontext bereits eine oder mehrere Bedeutungen besitzen kann, was ebenso für ein aus mehreren solchen Zeichen eines vordefinierten Zeichensatzes gebildetes Wort gilt. Ein Satz aus mehreren solchen Worten kann wieder eine oder mehrere Bedeutungen haben usw. Darüber hinaus lassen sich solche Daten idR für den Verwender bzw Empfänger bestimmten Zwecken zuordnen.

---

287 Siehe zur Kritik gleich im Anschluss.

288 Vgl JAB 359 BlgNR XVII. GP, 17.

289 Die Semantik behandelt die Beziehung zwischen Zeichen und ihren Bedeutungen. Die Pragmatik untersucht die Beziehungen bzw Wirkungen zwischen den Zeichen und den Verwendern (dh Zweckgebundenheit der Zeichen); vgl dazu *Reisinger,* Strukturwissenschaftliche Grundlagen der Rechtsinformatik (1987) 127.

290 Siehe gleich im Anschluss.

291 Vgl Art 1 lit b CCC: »›computer data‹ means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function.«

Alle diese abgestuften Schichten besitzen daher bereits syntaktische, semantische und pragmatische Elemente, die sich für unterschiedliche Bezugssysteme auf unterschiedlichen semiotischen[292] Instanzen ergeben können.[293] Ordnet nun der Mensch den Sinn solcher Daten in einen für ihn relevanten Gesamtzusammenhang ein, lässt sich die Intention bzw der Zweck der Information erkennen.

Zum leichteren Verständnis der hier untersuchten Problematik wird in weiterer Folge von einer technischen Ebene (Daten im engen Sinn) und einer inhaltlichen Ebene (Information bzw Daten im weiten Sinn) gesprochen. Anzumerken ist aber, dass Computersysteme ausschließlich (in Bitmuster konvertierte) Repräsentationen von Informationen verarbeiten können.

Auffällig ist daher insb, dass im Zuge der Umsetzung der CCC vom Gesetzgeber dennoch eine andere Definition für Daten als die dort formulierte gewählt wurde.[294] Nach den Erl[295] der CCC orientierten sich die Konventionsverfasser bei ihrer Definition von Daten im technischen Sinn an den internationalen ISO-Standards[296]. Art 1 lit b CCC definiert idS »Computerdaten« wie folgt:

> »computer data« means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function.

---

292 Zur Abgrenzung des technischen Informationsbegriffs vom umgangssprachlich verwendeten Begriff der Information kann auf die wesentlichen Begriffe der Semiotik bzw Linguistik zurückgegriffen werden: Syntax, Semantik, Pragmatik (vgl dazu generell auch *Koller,* Theorie des Rechts. Eine Einführung[2] [1997] 203 f).

293 ZB ist die Aussage »01000001« nicht nur eine syntaktisch geordnete Aneinanderreihung von Zeichen (0, 1), die wiederum mehrere Bedeutungen haben können (zB die Repräsentation der physikalischen Zustände »Strom fließt nicht« bzw »Strom fließt«), sondern hat bereits für ein Computersystem eine gewisse Bedeutung (Semantik). Für den Menschen wird sich eine solche erst nach einer weiteren Abstraktion ergeben, nämlich zB in der Darstellung des Großbuchstabens »A« des Alphabets. Handelt es sich dabei um eine konventionell gültige Semantik bezüglich eines bestimmten Bedeutungszusammenhangs, kann weiter untersucht werden, welchen Zweck bzw welche Wirkung der Mensch mit diesem Zeichen konkret verbindet – wie etwa A für »Austria« der Kfz-Kennzeichen (Pragmatik).

294 Siehe auch ErlStV 1645 BlgNR XXIV. GP, 3.

295 Vgl ER (ETS 185) Pkt 25, <conventions.coe.int/Treaty/EN/Reports/Html/185.htm> (01.04.2014).

296 ISO/IEC 2382–1:1993 Information technology –Vocabulary – Part 1: Fundamental terms.

Mit anderen Worten: Der Konventionsbegriff stellt auf die automationsunterstützte Verarbeitungsform von Informationen im technischen Zusammenhang (»Daten im engen Sinn«) ab, wie sie durch die binär codierte Darstellungsweise repräsentiert werden, also in concreto auf Daten, die ausschließlich und unmittelbar automationsunterstützt verarbeitet werden können. Daten können demnach als eine einer entsprechenden Syntax folgenden Zeichenfolge begriffen werden, die unmittelbar zur Verarbeitung über Datenverarbeitungssysteme verwendet werden können. Insbesondere soll die Verwendung der Bezeichnung »Computerdaten« dies unmissverständlich zum Ausdruck bringen.[297] Darüber hinaus fand eine nahezu gleichlautende Definition in Art 1 lit b des EU-RB 2005/222/JI[298] Eingang. Auf eine Fixierung bzw Verkörperung auf einen Datenträger kommt es für den Datenbegriff aber nicht an.[299]

Obwohl daher die vom nationalen Gesetzgeber in § 74 Abs 2 vorgenommene Begriffsbestimmung im Vergleich zu den abweichenden Definitionen von Computerdaten der europäischen und internationalen Vorgaben wie »Äpfel und Birnen« anmutet, ist der Datenbegriff des StGB deutlich weiter gefasst. § 74 Abs 2 beschreibt nämlich nicht ausschließlich reine Computerdaten, obwohl der Gesetzgeber den eigens bestimmten Datenbegriff hauptsächlich in den Tatbeständen der speziellen Computerdelikte verwendet.[300] Der sehr weitgefasste Wortlaut schließt grundsätzlich sämtliche »Informationen«, ungeachtet ihrer Verarbeitungs- bzw Darstellungsform und ihres Inhalts, mit ein und erfasst expressis verbis auch Programme.[301] Wobei sich der Begriff »Programme« als unpräzise erweist, letztlich aber wohl im hier interessierenden Zusammenhang und unter Berücksichtigung einer konventionsgerechten[302] und rahmenbeschlusskonformen[303] Interpretation ausschließlich in Hinblick auf »Computerprogramme« verstanden werden muss. Computerprogramme werden nach der DIN 44300 Teil 4

297 Vgl ER (ETS 185) Pkt 25.
298 Rahmenbeschluss 2005/222/JI des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme, ABl L 2005/69, 67.
299 AA *Haft,* Das neue Computerstrafrecht, DSWR 1986, 255 (256).
300 Siehe dazu auch *Jerabek/Reindl-Krauskopf/Schroll* in WK² § 74 Rz 65 (Stand Juli 2013); weiters ErlStV 1645 BlgNR XXIV. GP, 3.
301 Vgl auch ErlStV 1645 BlgNR XXIV. GP, 3.
302 Vgl die CCC.
303 Vgl EU-RB 2005/222/JI.

(1988) als vollständige Arbeitsvorschrift zur Lösung einer Aufgabe definiert. Wesentlich ist aber, dass sie eine »Doppelnatur«[304] aufweisen, nämlich die formale Notation der Handlungsanweisungen (Quellcode) auf der einen Seite und die von der Maschine im funktionalen Sinn verarbeitbare binäre Form desselben (Maschinencode[305]) auf der anderen Seite. »Ein Computerprogramm ist eine endliche Anzahl von Zeichen in geeigneter Anordnung, die, in (zB elektromagnetische) Impulse umgewandelt, mittels (zB elektronischer) Schaltungen im Rechner den Ablauf von logischen und mathematischen Operationen bewirken, um ein erwünschtes Resultat zu erzielen.«[306] Die Arbeitsanweisungen[307] eines lauffähigen Computerprogramms in binärer Übersetzung[308] sind zwangsläufig auch (Computer-)Daten. Es ist darauf hinzuweisen, dass der Gesetzgeber den Begriff »Programm« zwar im Tatbestand des § 148a verwendet, bei § 126c aber konkret vom »Computerprogramm« spricht. Es wäre jedenfalls sinnvoll die Terminologie zu vereinheitlichen und generell den eindeutigeren Begriff »Computerprogramm« zu benutzen.

Dass damit im kernstrafrechtlichen Verständnis – anders als bspw im Urheberrecht[309] – ausschließlich die Darstellungsform eines Computerprogramms im sog »Maschinencode« oder in Form eines unmittelbar per Interpreter ausführbaren »Source Code«[310], jedenfalls daher die in-

304 Siehe dazu *Wiebe,* Know-how-Schutz von Computersoftware (1993) 424 ff.

305 Sog »Object Code«.

306 Vgl *Lackner,* Softwareschutz in Österreich durch Urheberrecht? (Dissertation 1991) 66.

307 Vgl auch bereits DIN 44300 Nr 40 (1972).

308 Dh in Maschinensprache bzw Maschinencode (Object Code) übersetztes Programm.

309 Im Urheberrecht werden unter »Computerprogramm« alle Ausdrucksformen verstanden, dh der Maschinencode und Quellcode, wie auch das Material zur Entwicklung des Computerprogramms (vgl § 40a Abs 2 UrhG; siehe auch OGH 12.07.2005, 4 Ob 45/05d = ecolex 2005/445, 924 *(Braunböck)* = MR 2005, 379 *(Walter);* jüngst EuGH 02.05.2012, C-406/10 (SAS Institute Inc/World Programming Ltd) = ecolex 2012/257, 627 *(Anderl)* = jusIT 2012/45, 97 *(Staudegger)* = MR-Int 2012, 61 *(Appl);* siehe auch EuGH 22.12.2010, C-393/09 (Bezpečnostní softwarová asociace – Svaz softwarové ochrany/Ministerstvo kultury) = MR-Int 2011, 11 *(Savelka)* = MR 2011, 36 *(Marko/Hofmarcher)* = jusIT 2011/20, 44 *(Staudegger/Thiele)* = ÖBl-LS 2011/84, 164 *(Bücherle);* weiters zB *Staudegger,* Software-Erstellung: Vertragstyp und Quellcodeherausgabe, JBl 2006, 195; siehe zusammenfassend *Staudegger,* Die Rechtsprechung des EuGH in Urheberrechtssachen im Jahr 2012, in Staudegger/Thiele (Hrsg), Geistiges Eigentum. Jahrbuch 2012 (2013) 1 (9 ff).

310 Dabei wird der entsprechende Algorithmus einer formalen Notation eines Computerprogramms einer speziellen Programmiersprache (Quellcode) zeilenweise in Laufzeit analysiert und von einem eigenen Computerprogramm, dem sog »In-

formationstechnische Verarbeitungsform gemeint sein muss, lässt sich über eine rahmenbeschlusskonforme[311] bzw konventionsgerechte[312] Interpretation ermitteln, da beide Vorgaben von einem Programm ausgehen, »das die Ausführung einer Funktion durch ein Computersystem auslösen kann«. Daraus kann geschlossen werden, dass lediglich die unmittelbar operative Ausdrucksform, dh der technisch-funktionale Aspekt, eines Programms gemeint ist und nicht etwa dessen formalsprachlich verfasster Quellcode. »Daten« im informationstechnischen Verständnis sind also gleichermaßen Objekte, mit denen Computerprogramme arbeiten[313], und Computerprogramme selbst. Man könnte Computerprogramme in ihrer technischen Beschreibung als »aktive Daten« bzw »Programmdaten« bezeichnen, da mit ihnen Problemlösungen durch Handlungsanweisungen der Programmlogik durchgeführt bzw eingeleitet[314] werden. Mittels Computerprogrammen lassen sich aber aufgrund ihrer Ergebnisausgabe auch neue Informationen erzeugen. Alle anderen binär codierten Darstellungseinheiten, mit denen keine Algorithmen[315] operativ ausgeführt werden, wären dagegen »passive Daten« bzw »Nutzdaten«. Die technische (binäre) Repräsentation[316] des (abstrakten) Informationsgehalts aktiver und passiver Daten für die automationsunterstützte Verarbeitung – und somit auch für Computerprogramme – ist jedoch stets dieselbe. Computerprogramme sind ebenfalls der Kategorie der »Daten im engen Sinn« zuzuordnen.[317]

---

terpreter«, in den Maschinencode (Object Code) übersetzt. Das Ergebnis wird unmittelbar am Bildschirm anzeigt. Als Echtzeit-Übersetzer fungiert dabei ein Interpreter-Programm, wie zB ein Internetbrowser, der den Quellcode einer Webpage interpretiert und visualisiert (zB HTML, Javascript, PHP). Mit dieser Übersetzer-Technologie erreicht man eine höhere »Abstraktionsschicht«, da die zur Problemlösung auszuführenden Programme nicht auf den jeweiligen Prozessortyp abgestimmt sein müssen. Ebenso gibt es in diesem Bereich Mischformen aus Compiler- und Interpreterkomponenten (zB Java).

311 Vgl Art 1 lit b letzter HS EU-RB 2005/222/JI.

312 Vgl Art 1 lit b letzter HS CCC.

313 Siehe auch *Jaburek/Schmölzer,* Computer-Kriminalität, 18.

314 Man kann dies so verstehen, dass das unkörperliche Computerprogramm die exakte Vorgabe bereitstellt, welche Schaltungen wie zu schalten sind. Die Schaltungen selbst sind Hardware, die in der entsprechenden Reihenfolge betätigt werden (vgl anstatt vieler *Tanenbaum,* Computerarchitektur[5], 25)

315 Rechenvorschrift oder Handlungsanweisung zur Lösung mathematischer Probleme (siehe zu Algorithmen allgemein *Kersken,* IT-Handbuch[5], 33 f bzw 91).

316 Im Sinne der konkreten Form der Darstellung.

317 Insoweit verwirrend *Jerabek/Reindl-Krauskopf/Schroll* in WK² § 74 Rz 66, wenn sie bei Programmen von »Daten im weiten Sinn« sprechen, da sie nicht primär der

Den GMat zufolge umfasse aber die kernstrafrechtliche Begrifflichkeit auch die technische Darstellung der Computerdaten[318], weshalb der (innerstaatliche) strafrechtsspezifische Legalbegriff der »Daten« tatsächlich viel weiterreicht, als jener der CCC. Daten iSd § 74 Abs 2 erfassen – in Abgrenzung zum DSG 2000[319] – nicht nur die Information selbst, sondern auch die damit korrespondierende digitale Repräsentation (zB in Form des entsprechenden Bitmusters). Von einer tatsächlichen Definition des Begriffs »Daten« im technischen Sinn hat der Gesetzgeber bewusst Abstand genommen, da er die Abgrenzung des Datenbegriffs zu dem des DSG 2000 als ausreichend erachtet.[320]

In den GMat zum DSG 1978 wurde allerdings im Zusammenhang mit Daten ganz konkret von Zeichen oder Zeichenketten gesprochen, die in einem Entscheidungsprozess relevante Bedeutung für den Entscheider haben[321] und deren semantische Bedeutung mit Hilfe von Interpretationsregeln, die dem Entscheider bekannt sind, zu vollständigen Aussagen ergänzt werden können.[322]

2. Technischer Datenbegriff

In der Informatik wurde der Datenbegriff mittlerweile mehrfach modifiziert. Mit der DIN[323] 44300 Nr 19 (1972) wurde festgehalten, dass »Daten« »nur solche [sind], die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden«.

In geringer Weiterentwicklung dieser Definition wurde daraus in der DIN 44300 Teil 2 (1988) Folgendes: »Daten sind Gebilde aus Zeichen oder kontinuierliche Funktionen, die aufgrund bekannter oder unterstellter Abmachungen Information darstellen, vorrangig zum Zwecke der Verarbeitung und als deren Ergebnis«.

Auch diese technische Normierung wurde durch den internationalen Technologiestandard ISO/IEC 2382-1 (1993) wiederum abgelöst,

---

Darstellung von Aussagen, Tatsachen oder vergleichbaren Informationen dienen würden und daher keine Daten ieS seien.

318 Vgl ErlStV 1645 BlgNR XXIV. GP, 3.

319 Siehe ErlRV 1166 XXI. GP, 23.

320 Vgl ErlRV 1166 XXI. GP, 23.

321 Vgl Pragmatik.

322 Siehe ErlRV 72 BlgNR XIV. GP, 22 mwN insb den Verweis auf DIN 44300 Nr 19 (1972); vgl auch *Löschnigg,* Datenermittlung im Arbeitsverhältnis (2009) 132.

323 »Deutsche Industrie Norm«.

sodass es sich bei »Daten« nunmehr um »a reinterpretable representation of information in a formalized manner, suitable for communication, interpretation or processing« handelt.

Im Wesentlichen geht es bei der technischen Beschreibung von (digitalen) Daten also nicht um Bedeutungsinhalte, sondern um deren Verarbeitungs- bzw Darstellungsform (zB Bitmuster).[324] Erst durch Abstraktion[325] sämtlicher interpretierfähigen Daten kann man auf die »Information« (dh den semantischen Dateninhalt)[326] schließen. Die Information wird gemäß der technischen Norm ISO/IEC 2382-1 (1993) definiert als »knowledge concerning objects, such as facts, events, things, processes, or ideas, including concepts, that within a certain context has a particular meaning«. Folglich stellt der Informationsbegriff[327] in der Informationstechnik auf das Wissen oder die Kenntnisse der konkreten Vorgänge und Bedeutung in der realen Welt ab. Daten sind lediglich Träger eines transzendierenden Sinns, der sich für den Menschen in einer Information darstellt.

3. Problemfelder bezüglich des kernstrafrechtlichen Datenbegriffs

§ 107a Abs 2 Z 3 und 4 beziehen sich auf »personenbezogene Daten«, die in dieser Form aber im StGB nicht näher definiert werden. Wählt man den Weg der Interpretation von »Daten« über die Legaldefinition des § 74 Abs 2, so zeigt sich ein Widerspruch. § 74 Abs 2 bestimmt nämlich, dass iSd StGB »Daten« sowohl personenbezogen oder nicht personenbezogen als auch sogar Programme sein können. Mit der Formulierung in

---

324 Siehe auch *Sonntag* in Jahnel/Mader/Staudegger, IT-Recht[3], 1 (5 f).

325 »Abstraktion« beschreibt in der Informatik den Prozess der Rückgewinnung der Information aus Daten (vgl *Gumm/Sommer,* Informatik[10], 4). Man kann auch von »Interpretation« sprechen.

326 Der Informationsbegriff ist nicht unumstritten. Manche Autoren teilen den hier verwendeten Informationsbegriff noch weiter auf bzw verwenden abgewandelte Abgrenzungen und Begrifflichkeiten (zB Daten – Information – Wissen). Beispielsweise spricht *Werner,* Information und Codierung. Grundlagen und Anwendungen[2] (2008) 1 von Daten, wenn Syntax plus Semantik gegeben ist, *Richter,* IT-gestütztes Wissensmanagement[2] (2008) 15 bereits dann, wenn Zeichen einer Syntax folgend vorliegend. Für die hier gegenständlichen Zwecke, ist eine tiefere Auseinandersetzung mit dem Informationsbegriff aber entbehrlich. Vielmehr soll in diesem Kontext der Fokus auf eine möglichst verständliche Darstellung gelegt werden.

327 Zur Begrifflichkeit vgl zB *Werner,* Information, 1 ff; weiters *Mayer-Schönberger,* Information, 16 f.

§ 107a Abs 2 Z 3 und 4 sind jedoch »personenbezogenen Daten« iSd Datenschutzgesetzes 2000 gemeint[328], weshalb zumindest ein entsprechender Verweis auf das spezielle Sachgesetz im Gesetzestext angebracht wäre. Der Terminus »personenbezogene Daten« wird ausschließlich in § 4 Z 1 DSG 2000 gesetzlich dahingehend definiert, dass es sich dabei um Angaben über Betroffene handelt, deren Identität bestimmt bzw bestimmbar ist. Die konkrete Verarbeitungsform der Daten – dh ob sie etwa manuell oder automationsunterstützt verarbeitet werden – spielt im konkreten Zusammenhang der Begriffsklärung keine Rolle.

Der Wortlaut des § 225a (Datenfälschung) ist in diesem Zusammenhang ebenfalls unpräzise, da lediglich die »Eingabe, Veränderung, Löschung oder Unterdrückung von Daten« angesprochen ist und die Begriffsbestimmung von »Daten« in § 74 Abs 2 – wie gerade ausgeführt – gerade keine Aussage darüber trifft, in welcher Form die Daten verarbeitet werden müssen. Dadurch wären über die Wortinterpretation des § 74 Abs 2 grundsätzlich auch konventionelle Daten, zB auf Papier, genauso von § 225a mitumfasst. Gleichwohl liegt eine Computerdatenfälschung dann nicht vor, wenn bloß syntaktische Änderungen in der Darstellungsweise elektronischer Daten vorgenommen werden[329], ohne den Informationswert der Daten zu verändern. Richtigerweise muss daher die Information – dh die für den Menschen relevanten Dateninhalte – bspw verfälscht werden. Im informationstechnischen Verständnis könnte man daher bei § 225a von »Informationsverarbeitung« – im Gegensatz zur Datenverarbeitung wie zB bei § 126a und § 148a – sprechen.

Dass diese Besonderheiten nicht bedacht wurden und unsachlich erscheinen, ist offensichtlich, wie auch die späteren Ausführungen zu § 225a zeigen werden.[330] Die Problematik tritt aber nur deshalb in Erscheinung, weil der Gesetzgeber einerseits weder in der allgemeinen Begriffskonkretisierung des § 74 Abs 2, noch im konkreten Tatbestand des § 225a eine Einschränkung auf »automationsunterstützt verarbeitete, übermittelte oder überlassene Daten« (Computerdaten)[331] vorgenommen hat und andererseits die semantische Ebene des Da-

328 Vgl den Hinweis als Klammerausdruck in *Schwaighofer* in WK² § 107a Rz 26.

329 Als Beispiel könnte daran gedacht werden, dass jemand einem E-Mail lediglich ein neues Zeichen zB ein Leerzeichen an einer unbeachtlichen Stelle hinzufügt, ohne aber den Hinweis auf den konkreten Aussteller zu manipulieren.

330 Siehe dazu S 393 ff.

331 Vgl zB § 126a Abs 1.

tenbegriffs in diesem deliktischen Zusammenhang nicht besonders berücksichtigt hat.

Die Tatbestände des § 278[332] (Kriminelle Vereinigung) und § 278f[333] (Anleitung zur Begehung einer terroristischen Straftat) spitzen die terminologische Problematik weiter zu, da sie nun ua ausdrücklich »Informationen« erfassen.[334] Der Begriff der »Information« [335] wird aber nicht gesetzlich definiert, weder in Form einer allgemeinen Legaldefinition noch in den Delikten selbst.

Plöchl führt dazu aus, dass Informationen insb Mitteilungen, Auskünfte oder Hinweise seien, »die der Vereinigung oder der Ausführung der vorgesehenen Vereinigungstaten nützlich sein könnten (zB Beschaffen von Plänen, Hinweise zur Deaktivierung der Alarmanlage, Bekanntgabe der von der Sicherheitsbehörde oder privaten »Security-Unternehmen« festgelegten Überwachungsrayone samt den entsprechenden Inspektionsintervallen, zweckdienliche Hinweise zur Fahrtroute und der Bewachung eines Geldtransportes etc)«.[336]

Im Wesentlichen beziehen sich Informationen auf den für Menschen relevanten Bedeutungsinhalt von Daten (hier: Daten im weiten Sinn). Sie fallen daher in das »semantisch/pragmatische« Verständnis von Daten[337], gleich wie »personenbezogene Daten« oder »nicht personenbezogene Daten«. Auf die Verarbeitungsform der Informationen (hier: Daten im engen Sinn) kommt es bei § 278 – im Gegensatz zu § 278f Abs 1 und 2[338] – nicht an. Gerade deshalb, weil innerhalb von systematisch ähnlich gelagerten Delikten auf unterschiedliche (technische) Darstellungsformen abgestellt wird, der Relevanzzusammenhang des Bedeutungsgehalts aber vergleichbar ist, erscheint es unverständlich, weshalb nicht auch in diesen Bestimmungen auf den (inhaltlich abgegrenzten) Datenbegriff des § 74 Abs 2 zurückgegriffen wurde. Vielmehr noch wird durch die zusätzliche dogmatisch relevante

332 Eingeführt mit dem StRÄG 2002, wo aber auch »Daten« bezüglich einer allgemeinen Begriffsabgrenzung in § 74 Abs 2 aufgenommen wurden.
333 Eingeführt mit BGBl I 103/2011.
334 Auch § 278 Abs 3 erfasst ua »die Bereitstellung von Informationen«.
335 Zum technischen Informationsbegriff siehe oben.
336 Vgl *Plöchl* in WK² § 278 Rz 38 (Stand Jänner 2014).
337 Dh »Daten im weiten Sinn« bzw »Information«.
338 Durch den tatbestandlichen Hinweis, dass es sich um Information im (Abs 1) bzw aus (Abs 2) dem Internet handeln muss, wird die Verarbeitungsform dieser »Informationen« auf informationstechnische Darstellungen (Computerdaten) eingeschränkt.

Einführung des Begriffs der »Information« der Eindruck erweckt, als handle es sich dabei gerade im strafrechtlichen Verständnis bei »Daten« auf der einen und »Informationen« auf der anderen Seite um Verschiedenes. Wie jedoch festgestellt wurde, ist in beiden Fällen der Informationsgehalt gemeint und nicht der (technische) Datenbegriff. Von einer konstanten und sinnvollen Begriffsverwendung kann daher nicht gesprochen werden.

Insgesamt muss gesagt werden, dass für die Abbildung eines adäquaten Rechtsgüterschutzes eine genaue Differenzierung äußert bedeutsam ist. Die allgemeine inhaltliche Absteckung bzw Ausdehnung des Datenbegriffs in § 74 Abs 2 ist jedenfalls mE – anders als es die GMat gerade in diesem Zusammenhang zum Ausdruck bringen[339] – nicht ausreichend und findet insoweit auch äußerst inkonsequent Verwendung.

Daher wäre seitens des Gesetzgebers stets zu überlegen, ob sich der Tatbestand einer einschlägigen Strafbestimmung an der technischen Verarbeitungsform (wie zB in §§ 119a, 126a, 148a) und/oder den Inhalten von Daten[340] (wie zB bei §§ 107a, 118a, 119[341], 120 Abs 2a, 126c Abs 1 Z 2, 207a Abs 3 und 3a, 225a, 278 Abs 3, 278f) orientiert.

Geht es um »Bedeutungsinhalte«, so erfüllt etwa die elektronisch verarbeitbare Information unabhängig vom Träger und ihrer Darstellungsform ihren Zweck, welcher grundsätzlich durch Reproduktion und Transmission in seiner abstrakten Erscheinungsform (aber mit konkretem Inhalt) nicht verändert wird. Fokussiert man nun auf die Phase der automationsunterstützten Verarbeitung und nicht auf die (verbotenen[342] bzw geschützten[343]) Inhalte, wird das Abstellen auf die die Information repräsentierenden (Computer-)Daten wohl sinnvoller sein.

Eine zweckmäßige weiterführende Konkretisierung des Datenbegriffs in § 74 Abs 2 könnte wie folgt aussehen:[344]

---

339 Siehe ErlRV 1166 BlgNR XXI. GP, 30.

340 Im Sinne von »Information«.

341 Das gilt analog auch für die strafrechtsautonomen Begrifflichkeiten »Nachricht« (= technische Repräsentation der Information) und »Inhalt einer Nachricht« (= Information) in § 119 und § 120 Abs 2a.

342 ZB digitale kinderpornographische Bilddateien.

343 ZB Dateien mit personenbezogenen Inhalten.

344 Freilich müsste die Terminologie in einzelnen Tatbeständen dementsprechend harmonisiert werden.

»Im Sinne dieses Bundesgesetzes sind Daten

a) personenbezogene und nicht personenbezogene Informationen sowie

b) deren computertechnische Darstellung (Computerdaten) einschließlich unmittelbar ausführbarer Computerprogramme.«

Das diesbezügliche Abstellen auf »Informationen« ist mE zum einen schon deshalb treffender, weil eine Begriffsbestimmung ohne den zu bestimmenden Begriff vorgenommen werden soll[345], und zum anderen, weil mit diesem Begriff insb auf »Inhalte« hingewiesen wird. Die entsprechende Terminologie der einzelnen Bestimmungen des StGB wäre freilich idS zu adaptieren.

Was den Begriff »Computerprogramme« anlangt, könnte es sehr hilfreich sein, bereits in der Begriffsbestimmung auf die für das Kernstrafrecht relevante Ausdrucksform eines »Computerprogramms« abzustellen, gerade weil sich diese in anderen Sachgesetzen (wie etwa dem UrhG) unterschiedlich zeigt.

Insgesamt bezieht sich der vorliegende Definitionsvorschlag somit in lit a auf »Daten im weiten Sinn« und betrifft die für den Menschen relevante »Information« bzw die semantische Ebene von Daten. Lit b hingegen stellt auf »Daten im engen Sinn« ab und beschreibt Daten als reinen Träger einer (etwaigen) Information auf technischer Ebene.

345 *Thiele* spricht von einer Tautologie (vgl *Thiele* in SbgK § 118a Rz 60), tatsächlich ist es sogar eine Zirkeldefinition.

2 Dogmatische Betrachtung des Computerstrafrechts im engen Sinn

Unter dem materiellen Computerstrafrecht im engen Sinn werden – nach der im Vorangegangenen herausgearbeiteten Definition – die materiell-rechtlichen spezifischen Delikte des Kern- und Nebenstrafrechts verstanden, die explizit dafür geschaffen wurden, um computer- bzw datengestützte Begehungsweisen (einschließlich Tatwerkzeuge solcher Art) einerseits und/oder informationstechnische Angriffe auf IKT-Systeme bzw Computerdaten andererseits zu erfassen, um der Computerkriminalität entgegenzuwirken. Die nachfolgenden, überwiegend rechtspolitischen und dogmatischen Betrachtungen dieser Materie befassen sich daher mit »Computerdelikten«, also solchen strafbaren Handlungen, die entweder im Wesentlichen auf IKT-Begehungsweisen abstellen (hier: »echtes Computerdelikt«) oder grundsätzlich technikneutraler Natur sind, aber in einzelnen Begehungsweisen auch über IKT-Mittel realisiert werden können, was allerdings explizit auch als Handlungsalternative unter Strafe gestellt worden sein muss[346] (hier: »unechtes Computerdelikt«). Die einschlägigen Delikte werden in erster Linie nach den jeweiligen von ihnen geschützten Rechtsgütern gereiht, wobei zunächst mit den echten Computerdelikten der Anfang gemacht wird, welche das Individualrechtsgut der Privatsphäre (einschließlich Kommunikations- bzw Übertragungsgeheimnis und Datengeheimnis) schützen und bestimmte Indiskretionen in Bezug auf Daten und Übertragungen pönalisieren. Aus diesem Grund werden die nun im Anschluss untersuchten und diesbezüglich einschlägigen

346 Ist ein solcher IKT-Bezug nicht ausdrücklich im Unrechtstatbestand erfasst, wäre dieses Delikt dem Computerstrafrecht im weiten Sinn zuzuordnen (wie zB § 111 Abs 1, § 115 Abs 1).

echten Computerdelikte unter der Bezeichnung »Indiskretionsbezogene Computerdelikte« zusammengefasst.

I. Indiskretionsbezogene Computerdelikte

A. Widerrechtlicher Zugriff auf ein Computersystem (§ 118a)

> § 118a (1) Wer sich in der Absicht, sich oder einem anderen Unbefugten von in einem Computersystem gespeicherten und nicht für ihn bestimmten Daten Kenntnis zu verschaffen und dadurch, dass er die Daten selbst benützt, einem anderen, für den sie nicht bestimmt sind, zugänglich macht oder veröffentlicht, sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen, zu einem Computersystem, über das er nicht oder nicht allein verfügen darf, oder zu einem Teil eines solchen Zugang verschafft, indem er spezifische Sicherheitsvorkehrungen im Computersystem überwindet, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.
>
> (2) Der Täter ist nur mit Ermächtigung des Verletzten zu verfolgen.
>
> (3) Wer die Tat als Mitglied einer kriminellen Vereinigung begeht, ist mit Freiheitsstrafe bis zu drei Jahren zu bestrafen.[347]

In Umsetzung von Art 2 CCC (Illegal access) und Art 7 Abs 1 des EU-RB 2005/222/JI[348] wurde mit dem StRÄG 2002 § 118a zur Erfassung von Handlungen normiert, die man herkömmlich als »Hacking« bezeichnet.[349] Von dieser Bestimmung wird in erster Linie das Rechtsgut »Privatsphäre« geschützt, was sich bereits aus der systematischen Einordnung im 5. Abschnitt des StGB (Verletzungen der Privatsphäre und bestimmter Berufsgeheimnisse) ergibt. *Thiele* spricht darüber hinaus

347 BGBl 60/1974 idF I 109/2007.

348 Hinsichtlich der Schaffung einer Qualifikation bezüglich der Tatbegehung im Rahmen einer kriminellen Vereinigung mit einer Strafdrohung von bis zu 3 Jahren Freiheitsstrafe (vgl § 118a Abs 3).

349 Siehe ErlRV 1166 BlgNR XXI. GP, 23; ErlStV 1645 BlgNR XXIV. GP, 3.

das »formelle Datengeheimnis« als eines der Rechtsgüter hinter § 118a an.[350] Die Privatsphäre eines Menschen wird nämlich nicht nur innerhalb seiner eigenen Wohnstätte als schützenswert erachtet,[351] weshalb es auch irrelevant ist, wo sich ein Computersystem, das persönliche Daten verarbeitet, räumlich[352] befindet. Der Anspruch des Einzelnen auf Respektierung seines privaten Lebens, seiner privaten Interessen und Neigungen und seiner privaten Aktivitäten besteht jedenfalls unabhängig davon.[353] Aus diesem Grund lässt sich ein widerrechtlicher Zugriff auf ein fremdes Computersystem – gleichgültig, wo dessen Standort ist – durchaus als »virtueller Hausfriedensbruch« bezeichnen.[354] § 118a Abs 1 hat den unerlaubten Zugang zu einem Computersystem oder einem Teil davon als Regelungszweck und verkörpert eine Art »virtuelles Hausrecht«.[355] Nach Kapitel II Abschnitt 1 Überschrift 1 der CCC, die »Offences against the confidentiality, integrity and availability of computer data and systems« lautet, soll auch vom unter dieser Überschrift positionierten Art 2 (Illegal access) die Sicherheit (iSd Vertraulichkeit, Unversehrtheit und Verfügbarkeit) von Computerdaten und -systemen geschützt werden.[356]

1. Zum Tatobjekt »Computersystem«

Die Legaldefinition des § 74 Abs 1 Z 8 beschreibt den Begriff »Computersystem« als sowohl einzelne als auch verbundene Vorrichtungen, die der automationsunterstützten Datenverarbeitung dienen.[357] Art 1 lit a CCC definiert ein Computersystem »as any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data«. Dazu wird in den Erl[358] ausgeführt, dass es sich dabei um ein Gerät handelt, das aus Hard- und

350 Vgl *Thiele* in SbgK § 118a Rz 16; weiters *Schmölzer,* ZStW 2011/123, 709 (728).
351 Siehe dazu auch ErlRV 173 BlgNR XXII. GP, 17.
352 Dazu zählen zB auch mobile Endgeräte wie Notebooks, Smartphones.
353 Siehe ErlRV 173 BlgNR XXII. GP, 17.
354 Vgl auch *Salimi,* ÖJZ 2012/115, 998.
355 Zum virtuellen Hausfriedensbruch bzw virtuellen Hausrecht siehe auch *Thiele* in SbgK § 118a Rz 13; ebenso *Reindl,* E-Commerce, 147; zust auch *Seling,* Schutz der Privatsphäre durch das Strafrecht (2010) 76; weiters *Salimi,* ÖJZ 2012/115, 998.
356 Siehe dazu ER (ETS 185) Pkt 44.
357 Vgl ErlStV 1645 BlgNR XXIV. GP, 3.
358 Vgl ER (ETS 185) Pkt 23.

Software besteht und für die automatische[359] Datenverarbeitung entwickelt wurde, wobei es unbeachtlich ist, ob es sich dabei um einen Einzelrechner (Stand-Alone) oder um einem Verbund von Computersystemen handelt. Dies ergibt sich indirekt auch aus den Erl[360] zu Art 2 und Art 19 CCC, wonach hervorgeht, dass der Begriff Computersystem auch ein »Local Area Network« (LAN) umfasst.

Die RL 2013/40/EU[361] spricht zwar in Art 2 lit a von einem »Informationssystem«, definiert ein solches allerdings in dieselbe Richtung, nämlich als »eine Vorrichtung oder eine Gruppe miteinander verbundener oder zusammenhängender Vorrichtungen, die einzeln oder zu mehreren auf der Grundlage eines Programms die automatische Verarbeitung von Computerdaten durchführen, sowie die von ihr oder ihnen zum Zwecke des Betriebs, der Nutzung, des Schutzes und der Pflege gespeicherten, verarbeiteten, abgerufenen oder übertragenen Computerdaten;«.

Mit anderen Worten, ein Computersystem kann als Summe aller elektronischen Bauteile (Hardware) und unkörperlichen Programme (Software) bezeichnet werden, die gemeinsam der automationsunterstützten Datenverarbeitung dienen.[362] Dies entspricht in etwa dem Begriffsverständnis der Informatik, wenn dort unter Computersystem »das technische Gerät Computer[363] und die Programme zur Steuerung des Computers« gemeint sind.[364]

Ein System kann im Wesentlichen als eine Sammlung von Gegenständen, die in einem inneren Zusammenhang stehen, samt den Be-

359 »Automatisch« wird idZ dahingehend verstanden, dass keine direkte menschliche Intervention erforderlich ist.

360 Siehe ER (ETS 185) Pkt 46 und 188.

361 So auch schon Art 1 lit a EU-RB 2005/222/JI, der unter dem Ausdruck »›Informationssystem‹ eine Vorrichtung oder eine Gruppe miteinander verbundener oder zusammenhängender Vorrichtungen, die einzeln oder zu mehreren auf der Grundlage eines Programms die automatische Verarbeitung von Computerdaten durchführen sowie die von ihr oder ihnen zum Zwecke des Betriebs, der Nutzung, des Schutzes und der Pflege gespeicherten, verarbeiteten oder übertragenen Computerdaten« versteht.

362 Vgl dazu *Fuchs/Reindl-Krauskopf,* Strafrecht. Besonderer Teil I[4] (2014) 123; siehe für das Begriffsverständnis in der Informatik *Balzert,* Lehrbuch[2], 31.

363 Ein technisches Gerät, das umfangreiche Informationen mit hoher Zuverlässigkeit und großer Geschwindigkeit automatisch, durch Programme gesteuert, verarbeiten und aufbewahren kann. Siehe dazu *Balzert,* Lehrbuch[2], 29.

364 Siehe *Balzert,* Lehrbuch[2], 4.

ziehungen zwischen diesen Gegenständen beschrieben werden.[365] Daher können sowohl Verbindungen im Mikrobereich, wie zB der Zusammenschluss eines Mikroprozessors mit weiteren Systemkomponenten als ein Computersystem qualifiziert werden (zB Tastatur und Bildschirm[366]) als auch lokale Netzwerke samt entsprechenden Verbindungskomponenten.[367]

Der Definition des § 74 Abs 1 Z 8 entsprechend sind nicht nur selbstständig lauffähige Einzelrechner, sondern auch ein Verbund von zusammengeschlossenen selbstständig oder unselbstständig[368] lauffähigen Systemen als »ein Computersystem« iSd Strafrechts zu werten. Folglich kann ein solches Computersystem auch über Eigentums- und Zuständigkeitsbereiche hinweg bestehen, was eine Abgrenzung in der Strafrechtspraxis erschweren kann. Das Tatobjekt Computersystem und seine Teilkomponenten müssen daher in einem konkreten Sachverhalt stets dynamisch beurteilt werden. Diese Teilkomponenten beschränken sich aber nicht auf rein körperliche Hardware, sondern umfassen auch die mit dieser verbundenen unkörperlichen Software (also Daten und Programme).[369]

Durch die ausdrückliche Bezugnahme der Definition des § 74 Abs 1 Z 8 auf eine automationsunterstützte »Datenverarbeitung«, kann – da es dabei um keinen strafrechtsspezifischen Legalbegriff handelt – über das Prinzip der »Einheit der Rechtssprache«[370], Interpretationsanleihe beim Datenschutzgesetz genommen werden. Gleichwohl kommt es im Strafrecht, im Gegensatz zum DSG 2000, nicht auf einen rein personenbezogenen Charakter der Datenverarbeitung an.[371]

---

365 Vgl *Goos/Zimmermann,* Vorlesungen über Informatik. Band I. Grundlagen und funktionales Programmieren[4] (2006) 18.

366 Siehe *Reindl-Krauskopf* in WK² § 118a Rz 6 (Stand September 2008).

367 Siehe auch *Reindl,* E-Commerce, 149; *Reindl-Krauskopf,* Computerstrafrecht², 12.

368 In diesem Zusammenhang ist zB an Client-Server-Systeme zu denken, bei denen die zwar prozessorgesteuerten aber unselbstständigen Clients nur iVm einem Server und den dort bereitgestellten Diensten bestimmungsgemäß lauffähig sind.

369 Siehe auch *Reindl-Krauskopf* in WK² § 118a Rz 8.

370 Das Prinzip der Einheit der Rechtssprache besagt, dass im Allgemeinen davon auszugehen ist, dass die in der Rechtssprache geprägten Begriffe auch die gleiche Bedeutung haben (siehe insb VwGH 25.02.1992, 88/07/0107; OGH 18.09.1991, 1 Ob 22/91; weiters VwGH 31.03.1992, 90/13/0131; VwGH 25.02.1993, 92/04/0231; VwGH 24.11.2006, 2006/02/0235).

371 Insofern siehe § 74 Abs 2.

In § 3 Z 5 DSG 1978[372] wurde noch ausdrücklich die »Datenverarbeitung« in den Begriffsbestimmungen genannt. Mit Einführung des DSG 2000[373] wurde daraus – fast wortgleich – in § 4 Z 7 DSG 2000 die »Datenanwendung«.[374] Darunter versteht man aber nach wie vor die Summe der in ihrem Ablauf logisch verbundenen Verwendungsschritte, die zur Erreichung eines inhaltlich bestimmten Ergebnisses (des Zweckes der Datenanwendung) geordnet sind und zur Gänze oder auch nur teilweise automationsunterstützt, also maschinell und programmgesteuert, erfolgen (automationsunterstützte Datenanwendung).

Es muss daher ein durch die Datenverarbeitung »inhaltlich bestimmtes Ergebnis« hervorgebracht werden. Ein konkreter »personenbezogene Daten« betreffender Zweck, wie im DSG 2000, ist aufgrund der Klarstellung bezüglich der Dateninhalte in § 74 Abs 2 für das strafrechtliche Datenverständnis nicht gefordert.

Probleme können bspw dann auftreten, wenn der Täter mit seinem Computer (als Tatwerkzeug) selbst berechtigter Nutzer desselben Netzwerks des Zielcomputers[375] ist. Dies wäre bspw bei Verwendung eines Sniffers[376] der Fall, wo der Datenverkehr gar nicht am bzw im Zielcomputer selbst, sondern im gemeinsam verwendeten Netzwerk abgefangen wird.[377] In einem derartigen Fall wird nicht der Computer des Auszuspionierenden als Tatobjekt zu werten sein, sondern eben das gesamte LAN. Man kann daher von einer einzelfallbezogenen »Skalierung des Tatobjekts« sprechen. Da in einem solchen Fall der Täter zwar ebenfalls ein Nutzungsberechtigter dieses Netzwerks ist, nicht aber alleine darüber verfügen darf, ist der Tatbestand durch die bloße (Mit-) Benützungsberechtigung noch nicht ausgeschlossen.

---

372 DSG 1978, BGBl 565/1978 idF 370/1986.

373 DSG 2000, BGBl I 165/1999.

374 Siehe dazu ErlRV 1613 BlgNR XX. GP, 38.

375 Als Zielsystem wird das System bezeichnet, in das der Täter eindringen will.

376 Bei einem Sniffer handelt sich um ein spezielles Computerprogramm oder Gerät, das zur Datenaufzeichnung in einem Netzwerk verwendet wird. Zu Sniffer-Programmen und deren rechtlichen Beurteilung siehe *Bergauer,* Sniffer-Tools – unwillkommene Spyware: Ein Sniffer-Angriff unter § 118a StGB subsumiert, RdW 2006/391, 412.

377 ZB in Form eines »Man-in-the-Middle«-Angriffs; siehe ua *Kurose/Ross,* Computernetzwerke[4], 83; weiters *Borges/Schwenk/Stuckenberg/Wegener,* Identitätsdiebstahl und Identitätsmissbrauch im Internet. Rechtliche und technische Aspekte (2011) 48 ff.

▹ **Automat, Konsole, Mikrocontroller, Embedded Systems**

Dass nicht jeder Automat mit einem Computersystem gleichzusetzen ist, liegt auf der Hand. Dies muss auch bei der Einordnung unter die Legaldefinition berücksichtigt werden. Doch ist eine derartige Abgrenzung angesichts der raschen technologischen Entwicklung nicht immer leicht zu vollziehen. Grundsätzlich unterscheiden sich Automaten von Computersystemen dadurch, dass sie lediglich eindeutig festgelegte Funktionen, die durch die bauliche Konstruktion bereits vorgegeben sind, erfüllen.[378] So lässt sich etwa ein Zigarettenautomat nicht dazu verwenden, einen trinkfertigen Kaffee auszugeben.[379] Dagegen sind Computersysteme grundsätzlich universell einsetzbare Anlagen, die zu unterschiedlichsten automatischen Datenverarbeitungen herangezogen werden können.[380] Die Vorschriften[381], wie bei der programmgesteuerten Datenverarbeitung konkret vorgegangen wird, können daher jeweils neu programmiert und auch geändert werden, ohne die jeweilige Hardware verändern zu müssen. Die unterschiedlichen Problemlösungen werden jeweils durch die Software erzielt. So lassen sich auf ein und demselben physikalisch-materiell unveränderten Computersystem sowohl Textverarbeitungen durchführen, Computerspiele ausführen und Websites im Internet besuchen.

Anzumerken ist aber, dass auch ein Automat softwaregesteuert funktionieren kann und in dieser Konzeption sehr wohl auch Datenverarbeitungsprozesse ausführt (zB Bankomat, moderner Fahrkartenautomat).[382]

Ein moderner Automat bildet idR ein mit einem Mikrocontroller[383] ausgestattetes »Embedded System«, das nach den angeführten Definitionsansätzen und Hintergründen ebenfalls als ein selbstständiges

---

378 Siehe *Balzert,* Lehrbuch², 3.

379 Das Beispiel aus *Balzert,* Lehrbuch², 3.

380 Vgl *Schramm* in Jahnel/Schramm/Staudegger, Informatikrecht², 1 (2 f).

381 Diese Vorschriften, die Handlungsanweisungen oder Arbeitsanweisungen darstellen, werden als Algorithmen bezeichnet, die nach einem strengen Formalismus beschrieben werden müssen und ein Computerprogramm bilden. Ein Algorithmus ist eine Problemlösungsbeschreibung, die festlegt, wie ein Problem zu lösen ist (siehe dazu *Balzert,* Lehrbuch², 4 und 29).

382 Vgl dazu das sog »Ubiquitous Computing«.

383 Dabei handelt es sich um ein vollständiges Computersystem (sog »Ein-Chip-Computersystem«), das mit Prozessor, Speicher, Ein-/Ausgabeeinheiten und entsprechender Systemsoftware ausgestattet ist. Vorwiegend werden diese Chips in eingebetteten Systemen (Embedded Systems) verwendet. Siehe *Tanenbaum,* Computerarchitektur⁵, 48 ff; weiters *Rankl/Effing,* Handbuch⁵, 87.

Computersystem iSd § 74 Abs 1 Z 8 zu betrachten ist. Freilich ergibt dies für das Tatobjekt des § 118a Abs 1 nur dann Sinn, wenn sich überhaupt auszuspionierende Daten in einem derartigen System bzw auf einem mit diesem verbundenen Speicher befinden. Als weitere Beispiele für Mikrocontroller gesteuerte Geräte können Chipkarten[384] (zB Bankomatkarte, E-Card[385], SIM[386]-Karte), Digitalkameras, Multimediageräte[387], Multifunktionsgeräte[388] sowie moderne Kühlschränke[389] und Waschmaschinen oder Waffensysteme (wie Marschflugkörper oder Interkontinentalraketen) genannt werden.[390]

Doch innerhalb der Mikrocontroller gesteuerten Geräte lassen sich ebenfalls Unterschiede festhalten. So gibt es die Gruppe der Universalcontroller, die tatsächlich »normale Computer« verkörpern, wohingegen die sog »Spezialcontroller« in Architektur und Befehlssatz auf ganz bestimmte Anwendungen gerichtet sind.[391]

Dieser Festlegung folgend müssten streng genommen auch einzelne Peripheriegeräte, wie zB ein USB-Stick oder eine externe Fest-

384 Vgl auch *Rankl,* Chipkarten-Anwendungen (2006) 5.

385 Auf dem Chip der E-Card werden zurzeit folgende Daten gespeichert: »Alle am Kartenkörper aufgedruckten Daten sowie das Geschlecht und das Geburtsdatum sind zusätzlich am Chip gespeichert. Vor- und Familienname sind mit und ohne diakritische Zeichen gespeichert. Informationen über den Versicherungsstatus – das heißt, ob und bei welchem Krankenversicherungsträger ein Patient versichert ist – oder eine eventuelle Rezeptgebührenbefreiung werden durch die Anspruchsprüfung beim Einlesen der E-Card überprüft«. Siehe dazu <www.chipkarte.at/portal27/portal/ecardportal/channel_content/cmsWindow?action=2&p_menuid=51909&p_tabid=4> (01.04.2014).

386 Subscriber Identity Module für das mobile Telefonieren in Telekommunikationsnetzen, wobei Speicherbereiche jedenfalls für Kontakte auf diesem Chip für den Nutzer vorgesehen sind. Als Beispielsfall könnte an das Entfernen einer SIM-Karte aus einem unbeaufsichtigten fremden Mobiltelefon eines Unternehmers gedacht werden, wobei sich der Täter als Wettbewerber über ein manipuliertes Chipkartenlesegerät Kenntnis von den im SIM-Adressbuch gespeicherten Geschäftskontakten verschaffen will.

387 ZB MP3-Player oder digitale Bildbetrachter.

388 Dabei handelt es sich um ein kombiniertes Gerät, das je nach Konzeption die Funktionen eines Scanners, Kopierers, Druckers und/oder Fax in einem Gerät vereint und sowohl über einen angeschlossenen PC als auch als unabhängiges, selbstständiges Gerät bedient werden kann.

389 Siehe dazu *Pressetext-Austria,* Internet-Kühlschrank als Informationszentrum im Haushalt, <pressetext.at/news/010214032/internet-kuehlschrank-als-informationszentrum-im-haushalt> (01.04.2014); weiters *PC-Welt,* Internet-Kühlschrank im Test, <www.pcwelt.de/news/Internet-Kuehlschrank-im-Test-158989.html> (01.04.2014).

390 Weitere Beispiele finden sich in *Tanenbaum,* Computerarchitektur[5], 48.

391 Siehe dazu ausf *Balzert,* Lehrbuch[2], 49.

platte als jeweils ein Computersystem (iSd § 74 Abs 1 Z 8) beurteilt werden, sofern sie nicht zur Tatzeit mit dem Tatobjekt verbunden, dh am Ziel-PC angeschlossen waren. Andernfalls würden diese Geräte als Peripheriegeräte[392] über die unmittelbare Anbindung bzw mittelbare Kommunikation mit dem Prozessor an den Datenverarbeitungsprozessen des »führenden Systems« teilnehmen und so zu dessen »Teil« werden. Dabei sind an sich bereits als selbstständige Computersysteme zu beurteilende (Mikrocontroller gesteuerte) Speichermedien ebenfalls Teil des PCs, und als tatbildliches Computersystem anzusehen.[393] Daher gilt, dass einzelne Teile eines Computersystems, die ihrerseits selbstständige Computersysteme darstellen würden[394], sinnvoller Weise aber nicht immer gesondert auch als eigenständige Computersysteme iSd § 74 Abs 1 Z 8 behandelt werden sollten. In bestimmten Fällen wäre es sachgerechter, sie weiterhin nur als Teil eines im Einzelfall festzustellenden (geeigneteren) Computersystems zu betrachten.[395] Als Beispiel könnte ein Hackerangriff auf ein lokales Netzwerk genannt werden, bei dem der Täter Sicherheitsvorkehrungen der Netzwerkanmeldung umgeht, dann aber auf Daten eines mit diesem Netzwerk verbundenen ungesicherten PCs zugreift.[396] In diesem Fall würden das Netzwerk als tatbildliches Computersystem und der konkrete Zielcomputer als bloßer Teil desselben beurteilt werden müssen. Daher kann es auch in diesem Beispielsfall für die Tatbestandsmäßigkeit der Handlung keine Rolle spielen, dass der Zielcomputer selbst nicht gesondert mit einer spezifischen Sicherheitsvorkehrung[397] ausgestattet ist.

---

392 Siehe dazu auch ER (ETS 185) Pkt 23: »A computer system usually consists of different devices, to be distinguished as the processor or central processing unit, and peripherals«.

393 Zu denken wäre an einen Hackerangriff, bei dem sich der Täter widerrechtlich Zugriff auf einen PC verschafft und sich die auszuspionierenden Daten auf einer bei diesem angeschlossenen externen Festplatte befinden.

394 Beispielsweise können in einem konkreten Sachverhalt, in dem ein Netzwerk ausspioniert wurde, diverse Netzwerkkomponenten, wie Switches oder Router, als Teile des Computersystems »lokales Netzwerk« betrachtet werden; ebenfalls ist eine mit einem PC dauerhaft verbundene Festplatte, ausgenommen in Fall eines externen und zum Zeitpunkt der Tathandlung nicht mit dem PC verbundenen Datenträgers, als Teil des Computersystems des »PC« zu beurteilen.

395 In diesem Sinne auch *Reindl,* E-Commerce, 149; vgl zudem *Reindl-Krauskopf,* Computerstrafrecht², 12.

396 Ähnlich doch lediglich auf unselbstständige Systeme bezogen *Thiele* in SbgK § 118a Rz 29.

397 Zur spezifischen Sicherheitsvorkehrung siehe S 88 f.

Es ist für die Tatbestandlichkeit der Verhaltensweise von entscheidender Bedeutung, ob dem Angriffsobjekt eine Sicherheitsvorkehrung zuzurechnen ist.[398] Würde nämlich im selben Beispielsfall der Täter nicht über das gesicherte Netzwerk Zugriff auf die Daten des PCs erlangen, sondern sich diesen Zugriff vor Ort durch bspw eine offengelassene Bürotür verschaffen, so wäre die Netzwerksicherheitsvorkehrung nun nicht dem Zielsystem zuzuordnen und der PC selbst als das tatbildliche Computersystem iSd § 118a Abs 1 zu qualifizieren. Mangels Überwindung einer spezifischen Sicherheitsvorkehrung wäre gerade in diesem Beispiel der objektive Tatbestand nicht erfüllt.[399]

Es muss daher im Einzelfall geprüft werden, ob der Weg der Datenübertragung im Fall eines Zugriffs über ein Netzwerk ausschließlich über den (gesicherten) Weg zum konkreten Zielsystem führt oder (ungesicherte) Umwege existieren. Im ersten Fall würde die Sicherheitsvorkehrung, die im Netzwerk dermaßen angebracht ist, dass jeder Zugriff von außerhalb diese Schutzvorrichtung auch passieren muss, diesem gesamten Netzwerk als tatbildliches Computersystem zugerechnet werden, ganz gleichgültig, welche Netzwerkkomponente (auch PC, Switch, Router usw) vom Spionagezugriff konkret betroffenen wäre. Im zweiten Fall, wenn der Täter ein nicht umfassend gesichertes Netzwerk über einen Umweg infiltriert, »umgeht« er eine Sicherheitsvorkehrung, »überwindet« sie aber nicht. Im Ergebnis wäre diese Sicherheitsvorkehrung nicht ausreichend, um dem konkreten Spionageobjekt als eine derartige Vorrichtung zugerechnet zu werden.[400]

Thiele führt auf Grundlage einer Wortinterpretation hins »Teil eines solchen« aus, dass als Teil eines Computersystems nur etwas in Frage kommt, das selbst kein (funktionsfähiges) Computersystem darstellt.[401] Dem ist jedoch entgegenzuhalten, dass bei einer derartigen (engen) Auslegung jeder durch einen Mikrocontroller gesteuerte Bauteil eines PC per se als ein eigenes Computersystem beurteilt werden müsste. Des Weiteren könnte dieser Argumentation zufolge ein lokales Netzwerk kein selbstständiges Computersystem darstellen, da jedes damit verbundene System (PC, Router, Switch) jeweils

398 Siehe dazu auch *Bergauer,* RdW 2006/391, 412.
399 Im Ergebnis übereinstimmend auch *Thiele* in SbgK § 118a Rz 40.
400 Abgesehen davon, dass am konkreten Spionageobjekt nicht selbst eine Sicherheitsvorkehrung implementiert ist.
401 *Thiele* in SbgK § 118a Rz 29.

ein eigenständiges Computersystem darstellt. Bei einem Hackerangriff auf ein Netzwerk würde daher jede von diesem Angriff betroffene Netzwerkkomponente als Tatobjekt in Frage kommen. Doch wie oben bereits angemerkt, intendiert auch die CCC, dass selbst ein LAN als ein »Computersystem« qualifiziert werden kann. Dasselbe würde dann auch für den USB-Stick und die externe Festplatte gelten, weshalb das führende übergeordnete System auch hins einer etwa dort implementierten Sicherheitsvorkehrung nicht für die Beurteilung des Zugriffs auf als selbstständiges Computersystem zu qualifizierendes Gerät heranzuziehen wäre. Selbstständig funktionsfähige Geräte müssten demnach stets mit eigenen spezifischen Sicherheitsvorkehrungen ausgestattet sein; die Zurechnung einer übergeordneten Sicherung wäre ausgeschlossen. Es ist nicht zu übersehen, dass eine derartige Interpretation doch eher lebensfremd und rechtspolitisch wohl unerwünscht wäre.

Auch lässt sich die Argumentation *Thieles* nicht auf die Begriffsbestimmung des § 74 Abs 1 Z 8 stützen, denn dort zählen sowohl einzelne als auch verbundene Vorrichtungen, die der automationsunterstützten Datenverarbeitung dienen, als »ein Computersystem«. Daher ist nicht zu erkennen, warum solche Vorrichtungen nur selbstständige Systeme sein müssen, zielt doch die Definition ausdrücklich darauf ab, dass diese Vorrichtungen der automationsunterstützten Datenverarbeitung bloß »dienen« müssen. Allein nach dem Wortlaut der Begriffsbestimmung kann daher schon nicht gefordert sein, dass eine solche Vorrichtung in der Lage sein müsse, eine automationsunterstützte Datenverarbeitung selbstständig durchzuführen.[402] Vielmehr ist mE diese Definition dahingehend zu interpretieren, dass es sich bei einem Computersystem iSd Strafrechts um eine auf eine gemeinsame automatische Datenverarbeitung gerichtete Funktionseinheit handeln muss, deren Umfang je nach bestimmungsgemäß vorgesehener Datenverarbeitung abzugrenzen ist. Wird auf einen PC vor Ort durch Umgehung der dort implementierten Sicherheitsvorkehrung widerrechtlich zugegriffen, so besteht die betroffene Funktionseinheit lediglich aus der Hard- und Software des PC, samt denn damit ggf verbundenen (selbstständig oder unselbstständigen) zusätzlichen Peripheriegeräten.[403]

402 AA *Schuh,* Computerstrafrecht, 192.

403 Wobei es keinen Unterschied macht, ob diese Peripheriegeräte selbst als eigenständige Computersysteme qualifiziert werden können.

Betrifft der Hackerangriff ein Netzwerk, wie zB ein gesichertes WLAN[404], so ist dieses LAN mit sämtlichen untergeordneten (und selbst als eigenständige datenverarbeitende Funktionseinheiten zu qualifizierenden) Systemen als das gegenständliche Computersystem iSd § 74 Abs 1 Z 8 zu beurteilen. Man muss daher in der Strafrechtspraxis zur Konstatierung des tatsächlichen Tatobjekts eine einzelfallbezogene, spezifische Skalierung des für den Angriff wesentlichen Computersystems vornehmen.

Insgesamt ist somit bei der Legaldefinition des § 74 Abs 1 Z 8 generell von einem weiten Begriffsverständnis auszugehen.[405] Nicht zuletzt deshalb ist dabei auf die (nationalen wie europäischen[406]) GMat zu rekurrieren, nach denen bezugnehmend auf die CCC der Begriff »Computersystem« (insb auch iZm §§ 119, 119a) sehr weit zu verstehen sei. Es werden davon nämlich auch Kommunikationsformen erfasst, die über eine Telekommunikation hinausgehen.[407]

Selbstverständlich muss ein Computersystem als Tatobjekt eines widerrechtlichen Zugriffs auf ein Computersystem (§ 118a) jedenfalls auch tatsächlich in der Lage sein, Daten, von denen sich der Täter Kenntnis verschaffen will, zu speichern. Daher kommen Computersysteme, die zB durch Spezialcontroller gesteuert werden und keine Datenspeicherung ermöglichen, bzw Geräte, in denen überhaupt keine Sicherheitsvorkehrung werkseitig vorgesehen oder individuell angebracht werden kann, nicht als Tatobjekte iSd § 118a Abs 1 in Betracht.

2. Verfügungsberechtigung

Der Täter muss hins der anvisierten Daten ein Unbefugter sein. Auch bezüglich des Computersystems darf er keine (alleinige) Verfügungsberechtigung haben. Auf Eigentumsverhältnisse kommt es dabei nicht an. Selbst derjenige, der Eigentümer der Hardware eines Computersys-

404 Wireless Local Area Network (auch WiFi genannt) siehe dazu *Kersken,* IT-Handbuch[5], 204 ff; weiters auch *Lichtenstrasser/Mosing/Otto,* Wireless LAN – Drahtlose Schnittstelle für Datenmissbrauch?, ÖJZ 2003/14, 253.

405 Siehe *Thiele* in SbgK § 118a Rz 28.

406 Vgl die Erwägungen zum EU-RB 2005/222/JI wie auch zur diesen ersetzenden RL 2013/40/EU.

407 Vgl ErlRV 1166 BlgNR XXI. GP, 25; insofern verkennen die Autoren *Lichtenstrasser/Mosing/Otto,* ÖJZ 2003/14, 253, dass der Begriff »Computersystem« weiter reicht, als jener der »Telekommunikation«.

tems ist, kommt daher als Täter in Frage, wenn er bezüglich der darauf verarbeiteten bzw gespeicherten Software (Programme bzw Dateien) keine bzw keine alleinige Verfügungsberechtigung besitzt.[408] Fraglich ist, ob es tatsächlich sinnvoll ist, die Verfügungsberechtigung auf das Computersystem bzw einen Teil davon zu beziehen. Immerhin muss es dem Täter, um sich strafbar zu machen, immer auf die (nicht für ihn bestimmten) Daten ankommen (vgl überschießende Innentendenzen), auch wenn er selbst Eigentümer der Hardware wäre. Verschafft sich jemand Zugang zu einem Computersystem über das er (neben dem Eigentümer bzw Betreiber) nicht allein verfügen darf, aber auf dem ausschließlich in seine alleinige Verfügungsberechtigung fallende Daten gespeichert sind, so käme auch dieser an den Daten Berechtigte als Täter iSd § 118a Abs 1 in Betracht.[409] Man denke etwa an den Fall der Nutzung eines Online- bzw »Cloud-Speichers«[410] im Internet, auf dem die Kunden gegen Entgelt ihre Daten abspeichern können. Vergisst nun jemand bspw sein Passwort, um auf das Service zugreifen zu können und verschafft sich durch die Überwindung der installierten spezifischen Sicherheitsvorkehrung, welche sein eigenes Nutzerkonto vor widerrechtlichen Zugriffen schützen soll[411], den Zugang dazu, so ist die objektive Tatbestandsmäßigkeit hergestellt, weil er nicht über die Hardware (allein) verfügen darf. Lediglich der Entfall des erweiterten Vorsatzes in dem Sinn, dass dieser Täter nicht in der Absicht handelt, »sich oder einem anderen Unbefugten« in Kenntnis der dort gespeicherten Daten zu setzen, lässt den (subjektiven) Tatbestand entfallen. So wäre es mE sachgerechter jede Person als Täter zu erfassen, die nicht (allein) über die Daten, die auf dem Computersystem gespeichert sind, verfügen darf. Hingegen nicht auch jene, die zwar die alleinige Berechtigung bezüglich der Daten besitzt, aber gerade nicht über das Computersystem selbst (allein) verfügen darf. Letzteres dient hierbei lediglich als Mittel zum Zweck der konkreten Datenverarbeitung.

---

408 Vgl auch *Birklbauer/Hilf/Tipold,* Strafrecht BT I² (2012) § 118a Rz 4; weiters *Reindl-Krauskopf* in WK² § 118a Rz 10 und 15; auch *Thiele* in SbgK § 118a Rz 31 f.

409 In diesem Sinne wohl auch *Reindl-Krauskopf* in WK² § 118a Rz 14.

410 Das Problem zeigt sich aber prinzipiell bei allen Formen der Virtualisierung und Abstraktion des verwendeten Dienstes von der Hardware, wie zB beim »Cloud Computing« uÄ.

411 Ggf hat dieser Nutzer die Sicherheitsvorkehrung sogar selbst dort installiert.

3. Zur Tathandlung des Sich-Zugang-Verschaffens

Als Tathandlung verlangt § 118a Abs 1, dass sich der Täter Zugang zu einem Computersystem verschaffen muss. Die Formulierung »Zugang zu einem Computersystem zu verschaffen« ist wohl etwas verwirrend, da sie auf den ersten Blick den physischen Zugang zu einem Computersystem suggeriert. Ein solcher Zugang ist aber nicht gemeint, was schon durch die erforderliche Sicherheitsvorkehrung zum Ausdruck gebracht wird, die »im«[412] System überwunden werden muss. Treffender wäre es mE den Wortlaut im Sinne der Deliktsbezeichnung anzupassen und auf den »Zugriff auf« ein Computersystem abzustellen.

»Zugang« zu einem Computersystem hat man sich nach deliktsspezifischem Verständnis dann verschafft, wenn man in der Lage ist, innerhalb des Computersystems tatsächlich tätig zu werden und dadurch Systemressourcen bzw -funktionalitäten nutzen kann. Der Täter muss also mit Soft- oder Hardware des fremden Systems in informationstechnischer Weise operieren können.[413] Wesentlich ist dabei, dass diese Verwendungsmöglichkeit »automationsunterstützt« erfolgen muss, sodass Daten, die im System gespeichert sind überhaupt verarbeitet werden können. Jemand der sich bloß »physischen« Zugang zur Hardware eines Computersystems verschafft, in dem er zB mit der Tastatur oder Maus eines ausgeschalteten oder in den Ruhemodus versetzten Systems vor Ort hantiert[414], verschafft sich noch keinen Zugang zum Computersystem, da dadurch kein Datenverarbeitungsprozess in Gang gesetzt wird und eine Kenntnisverschaffung von automationsunterstützt verarbeitbaren Daten folglich auch gar nicht möglich wäre. Weiters verschafft man sich durch das bloße Versenden eines E-Mails oder einer Datei an das Zielsystem keinen Zugang.[415]

Auf eine bestimmte Datenqualität der im Computersystem gespeicherten Informationen kommt es ebenfalls nicht an. Vielmehr sind

412 Diese Klarstellung findet sich auch ausdrücklich in die GMat (vgl ErlRV 1166 BlgNR XXI. GP, 24).

413 Siehe auch *Bergauer,* RdW 2006/391, 412.

414 Ausschließlich im Kontext des Begriffs »Zugang verschaffen« wäre hier denkbar, dass eine Person ein im Ruhemodus befindlich geglaubtes System durch eine Mausbewegung oder einen Tastenanschlag reaktivieren will, um Kenntnis von dort gespeicherten Daten zu erlangen, das System jedoch ausgeschaltet bzw überhaupt nicht funktionsfähig ist.

415 Vgl ER (ETS 185) Pkt 46.

der Konturierung des Datenbegriffs des § 74 Abs 2 folgend personenbezogene, nicht personenbezogene Daten, aber auch Programme erfasst, auf die sich die Spionageabsicht des Täters richten muss. Für eine Strafbarkeit müssen daher nicht unbedingt Daten ausspioniert werden, die zur Privatsphäre des Opfers zählen. Es würde ausreichen, wenn sich die Spionageabsicht auf reine Systemdateien oder andere Daten ohne jeglichen Personenbezug erstreckt. Damit sich das weitgefasste (subjektive) Tatbestandsmerkmal »Daten« nicht zu weit vom geschützten Rechtsgut »Privatsphäre« entfernt, sieht man im Schrifttum dieses Rechtsgut bereits dann als verletzt an, wenn eine abstrakte Gefährdung desselben eintritt.[416] Bedient man sich des oben angesprochenen Vergleichs mit dem (virtuellen) Hausrecht, so kommt es bereits aufgrund des Wortlauts dieser Tatbestände (§§ 109 bzw 118a) nicht darauf an, welche Gegenstände bzw Daten(-inhalte) sich in der Wohnstätte bzw im Computersystem befinden, sondern allein darauf, dass sich ein Unberechtigter Zugang zu einem grundsätzlich[417] schützenswerten Objekt, das eng mit der Privatsphäre verbunden ist, verschaffen will.[418] Dieser Vergleich hinkt aber in Bezug auf die oben angesprochene Verfügungsberechtigung, da kein Hausfriedensbruch nach § 109 Abs 1 vorliegt, wenn sich der Mieter einer Wohnung mit Gewalt Zutritt zum (Mehrparteien-)Haus verschafft, in dem sich die Mietwohnung befindet[419], wohl aber derjenige als Täter nach § 118a Abs 1 in Betracht kommt, der eine spezifische Sicherheitsvorkehrung überwindet, um sich Zugriff auf ein Computersystem, oder einen Teil davon – über das er nicht allein verfügen darf – zu verschaffen, auf dem ausschließlich »seine« Daten gespeichert sind.[420]

§ 118a Abs 1 lässt allerdings nicht jede Zugangsverschaffung ausreichen, sondern nur eine solche, bei der eine spezifische Sicherheitsvorkehrung überwindet wird. Es handelt sich bei § 118a Abs 1 folglich um ein verhaltensgebundenes Erfolgsdelikt.

---

416 Siehe dazu *Seling,* Privatsphäre, 77 mwN.

417 Dass das Objekt auch für Dritte als schützenswert ersichtlich wird, soll durch entsprechende Sicherheitsvorkehrungen im Computersystem zum Ausdruck gebracht werden. Vgl dazu § 109, der ein Eindringen in die Wohnstätte eines anderen mit Gewalt oder durch Drohung mit Gewalt verlangt. Das Betreten einer Wohnung durch eine offenstehende Tür etwa, stellt auch keinen (realen) Hausfriedensbruch dar (siehe dazu vertiefend *Bertel* in WK² § 109 Rz 2 ff).

418 Siehe *Seling,* Privatsphäre, 77.

419 ZB, weil er den Haustorschlüssel vergessen hat.

420 Man denke erneut an das Beispiel mit dem Online-Speicher im Internet.

4. Überwinden einer spezifischen Sicherheitsvorkehrung

Nur gesicherte Computersysteme, oder Teile davon, genießen den strafrechtlichen Schutz des § 118a.[421] Der Gesetzgeber hat dabei von den nach der CCC zulässigen Tatbestandseinschränkungen insofern Gebrauch gemacht, als nicht jeder widerrechtliche Zugriff auf ein Computersystem strafbar sein sollte. Daher macht sich nur strafbar, wer zu diesem Zweck spezifische Sicherheitsvorkehrungen überwindet.[422]

Mit anderen Worten, die Sicherheitsvorkehrung verkörpert das besondere Interesse des Verfügungsberechtigten am System bzw an den darin gespeicherten Daten. Es ist folglich davon auszugehen, dass der Gesetzgeber lediglich in der Überwindung der spezifischen Sicherheitsvorkehrung die sozial inadäquate Gefährlichkeit der Tathandlung erachtet, und nicht schon in der bloßen Zugangsverschaffung auf ein fremdes Computersystem. Verschafft sich der Täter Zugang zu einem fremden Computersystem, ohne spezifische Sicherheitsvorkehrungen zu überwinden, dann stellt dies noch ein strafrechtlich gebilligtes Verhalten dar.

Die Diktion des Gesetzestextes selbst gibt keinen Hinweis auf Art und Umfang der Sicherheitsvorkehrung. Nach den GMat[423] seien Sicherheitsvorkehrungen dann als spezifisch anzusehen, wenn sie im Computersystem angebracht worden sind, um sicherzustellen, dass nur berechtigte Personen auf das System zugreifen können und unberechtigten Personen der Zugriff auf dieses System dadurch verwehrt wird. Als Beispiele nennen die Erl etwa Computerpasswörter und Zugangscodes. Nicht im direkten Zusammenhang mit dem Zugriff auf ein Computersystem stehende allgemeine Maßnahmen oder Vorrichtungen gelten nicht als spezifische Sicherheitsvorkehrungen (wie zB das Versperren der Türe zum Computerraum oder eine Alarmanlage).[424]

Daher ist der Zugriff auf Daten eines Magnetstreifens einer Bankomatkarte im Zuge des sog »Skimming«[425] ebenfalls nicht erfasst, da die bloße Speicherung von Daten auf einem Datenträger noch keine

421 Vgl *Reindl,* E-Commerce, 153 ff; *Reindl* in BMJ, Vorarlberger Tage 2003, 63 (76 f); *Reindl-Krauskopf,* Computerstrafrecht², 15.
422 Siehe ErlRV 1166 BlgNR XXI. GP, 24.
423 Vgl ErlRV 1166 BlgNR XXI. GP, 24.
424 Siehe ErlRV 1166 BlgNR XXI. GP, 24; weiters *Maleczky,* Das Strafrechtsänderungsgesetz 2002, JAP 2002/2003, 115; auch *Reindl-Krauskopf,* Computerstrafrecht², 15.
425 Siehe mehr dazu S 340 ff.

besondere Sicherungsfunktion gegen unerlaubten Zugriff erfüllt. Darüber hinaus würde die Möglichkeit des bloßen Auslesens der Daten selbst noch keine Überwindung einer Sicherheitsvorkehrung darstellen, denn die erforderliche PIN-Eingabe schützt nicht vor dem Zugriff auf die Daten des Magnetstreifens oder Mikrochips, sondern vor widerrechtlicher Verwendung derselben.

Spezifisch ist eine Sicherheitsvorkehrung dann, wenn sie den Zweck hat, den Zugang Unbefugter zu den geschützten Daten, die im Computersystem verarbeitet werden, zu verhindern oder zumindest erheblich zu erschweren.[426] Die Zugriffsmöglichkeit muss an eine gesicherte Zugangsart gebunden werden, womit ein Zugang außerhalb dieses vorgegebenen Zugriffszenarios weitgehend verhindert wird. Eine spezifische Sicherheitsvorkehrung muss objektiv geeignet und ganz konkret auf bestimmte Zugriffsszenarien abgestimmt sein[427], um ggf diese auch verhindern zu können. Sie muss daher in der Lage sein, den individuellen Zugriff eines Täters in einem konkreten Sachverhalt wirksam zu unterbinden. So reicht es zur Erfüllung des Tatbestandes nicht aus, eine Antiviren-Software als Sicherheitsvorkehrung zu implementieren, um unmittelbare Zugriffe auf das System durch den Täter vor Ort zu verhindern. Eine derartige Sicherheitsmaßnahme kann nämlich nie einen wirksamen Schutz gegen solche Angriffe leisten. Anders jedoch wäre dieses Schutzprogramm zu qualifizieren, wollte der Täter bspw ein Trojanisches Pferd ins System einschleusen, um sich von den Daten Kenntnis zu verschaffen.

5. Exkurs: Trojanische Pferde

Die Bezeichnungen »Trojanisches Pferd« bzw in darauffolgender synonymer Verwendung »Trojaner«[428] stammen ursprünglich aus der griechischen Mythologie um den Trojanischen Krieg.[429]

426 Siehe *Thiele* in SbgK § 118a Rz 39.

427 IdS auch *Reindl-Krauskopf* in WK² § 118a Rz 25; vgl auch *Reindl-Krauskopf,* Computerstrafrecht², 15; AA offenbar *Thiele* in SbgK § 118a Rz 39, der nicht auf die Wirksamkeit im Einzelnen oder auf eine »Geheimtechnik« abstellen will.

428 Im einschlägigen Jargon hat sich das Kurzwort »Trojaner« verbreitet, was aber eigentlich eine Verkehrung der Analogie bedeutet, da sich die Trojaner selbst vom Holzpferd der Griechen täuschen haben lassen.

429 Siehe zur Etymologie des Begriffs »Trojanisches Pferd« bei *Schmeh,* Das Trojanische Pferd. Klassische Mythen erklärt (2007) 30 f.

Ähnliche Wirkung wie das Holzpferd in der Geschichte um Troja erzielt das Trojanische Pferd auch in der Datenwelt des Computers. Ein Computerprogramm wird möglichst unbemerkt in ein fremdes Computersystem eingeschleust, damit es dort bestimmte Aufgaben ausführen kann. Eine dieser Aufgabe ist zB die Bereitstellung einer Hintertüre zum Zielsystem, sog »Backdoor Trojan« oder »Remote Access Trojan« (RAT).[430]

Ein Trojanisches Pferd ist ein Computerprogramm, das sich prinzipiell hinter einer für einen Nutzer nützlich erscheinenden Funktionalität versteckt.[431] Wenn zB ein Programm, das eine Festplatte formatieren[432] soll, die Festplatte formatiert, dann handelt es sich offensichtlich um kein Trojanisches Pferd. Wird aber das Formatieren der Festplatte vom Nutzer nicht erwartet, dann handelt es sich um einen Trojaner. Es geht daher darum zu vergleichen, was ein Programm tut und was der Nutzer vom Programm erwartet.[433]

Trojanische Pferde verbergen sich idR in seriös wirkenden Webpages, E-Mail-Anhängen oder hinter nützlichen Programmeigenschaften diverser Software. Sie sollen den Nutzer respektive das Opfer dazu verleiten, sich das Schadprogramm durch aktives Mitwirken selbst (unbemerkt) im System zu implementieren.[434] Diese Interaktion führt letzt-

---

430 Vgl etwa *Kersken,* IT-Handbuch[5], 1064 f; weiters *Solomon,* Elements of Computer Security (2010) 344; auch *Winterer,* Windows 7 Sicherheit (2011) 149 ff.

431 Siehe etwa *Kersken,* IT-Handbuch[5], 1064 f; siehe aber auch ErwG 65 RL 2009/136/EG: »Computerprogramme, die heimlich zugunsten Dritter das Verhalten des Nutzers überwachen oder die Funktionsweise seines Endgerätes beeinträchtigen (›Spähsoftware‹) sind genauso wie Viren eine ernste Bedrohung für die Privatsphäre des Nutzers. Ein hoher und einheitlicher Schutz der Privatsphäre der Nutzer muss unabhängig davon gewährleistet werden, ob unerwünschte Spähprogramme oder Viren versehentlich über elektronische Kommunikationsnetze heruntergeladen werden oder aber versteckt in anderer Software, die auf externen Speichermedien wie CD, CD-ROM oder USB-Speicherstift verbreitet wird, ausgeliefert und installiert werden. Die Mitgliedstaaten sollten zur Bereitstellung von Information an Endnutzer über mögliche Schutzvorkehrungen auffordern und die Endnutzer auffordern, die notwendigen Maßnahmen zu ergreifen, um ihre Endgeräte vor Viren und Spähsoftware zu schützen«.

432 Dabei wird auf der Festplatte ein magnetisches Muster aufgebracht, das Spuren und Sektoren festlegt (vgl etwa *Gumm/Sommer,* Informatik[10], 50).

433 Vgl auch *von Gravenreuth,* Computerviren – Technische Grundlagen und rechtliche Gesamtdarstellung[2] (1998) 11 f; weiters *Clough,* Principles of Cybercrime (2010) 34.

434 Siehe dazu auch *Slade,* Software Forensics. Collecting Evidence from the scene of a digital crime (2004) 101 ff; weiters *Eckert,* IT-Sicherheit. Konzepte – Verfahren – Protokolle[9] (2014) 73 ff; auch *Moore,* Cybercrime: Investigating High-Technology Computer Crime[2] (2011) 38.

lich dazu, dass der Nutzer an seiner Schädigung selbst mitwirkt (sog »[Computer Based] Social Engineering«[435]).

Würde man Schadprogramme in hierarchische Kategorien fassen wollen, so sind Trojanische Pferde unter dem Sammelbegriff »Malware«[436] in erster Linie der Spyware[437] (Spionagesoftware) zuzuordnen. Neben den klassischen Remote Access Trojanern gibt es noch weitere schädigende Programmfunktionalitäten[438], die den Trojanischen Pferden zuzuordnen sind.

a. Logische Bomben

Logische Bomben sind Computerprogramme, die den mitgeführten Payload[439] erst nach Eintritt einer bestimmten Bedingung (sog »Trigger[440]-Funktion«) aktivieren.[441] Unter dem Payload versteht man im Bereich der Malware die konkrete schädigende Funktion, also den Aktionscode, eines jeweiligen Schadprogramms (zB das Öffnen einer Hintertüre, das Formatieren eines Datenträgers).[442] Der Trigger bildet den Auslösemechanismus ab, der bestimmt, wann der Payload letztlich ausgeführt werden soll. Beispielsweise wartet das Programm auf den Eintritt einer bestimmten Bedingung, wie etwa ein bestimmtes Datum (zB 1. April) oder der Payload wird erst aktiviert, wenn ein Datenträger zu mehr als die Hälfte ausgelastet ist.[443]

---

435 Siehe dazu *Lipski,* Social Engineering – Der Mensch als Sicherheitsrisiko in der IT (2009) 9; vgl auch *Borges/Schwenk/Stuckenberg/Wegener,* Identitätsdiebstahl, 96 ff; ebenso *Feiler,* Technische Aspekte der Online-Durchsuchung, in Zankl (Hrsg), Auf dem Weg zum Überwachungsstaat? (2009) 173 (173 f).

436 Zusammengesetztes Kurzwort für »malicious software« und bezeichnet jegliche Arten von Schadprogrammen in informationstechnischen Systemen (siehe dazu auch *Slade,* Software Forensics, 95).

437 Siehe dazu *Clough,* Cybercrime, 36.

438 Auch »Malicious Code« genannt.

439 Engl für Nutzlast, Ladegut.

440 Engl für Auslöser, Abzug.

441 Vgl *Janowicz,* Sicherheit im Internet[3] (2007) 218.

442 Siehe dazu *Harley/Slade/Gattiker,* Anti-Viren-Buch, 37 bzw 130 f; weiters *Slade,* Software Forensics, 98 und 100.

443 Siehe dazu *Winterer,* Viren, Würmer & Trojanische Pferde (2002) 194 f; weiters *Harley/Slade/Gattiker,* Anti-Viren-Buch, 130 f; weiters *Slade,* Software Forensics, 100.

b. Dialer

Die Begriffe Dialer-Software bzw Dialer Trojans sind nach dem derzeitigen Begriffsverständnis[444] deutlich negativ besetzt. Man verbindet damit unerwünschte kostenpflichtige Einwahlprogramme ins Internet.[445] Beispielsweise werden dabei vordefinierte Einwahlprogramme (zB des Telefonmodems oder der ISDN-Karte) zum jeweils verwendeten Internet Service Provider (ISP) durch eigene Programme der Täter ersetzt. Dies führt dazu, dass die Internetverbindungen unbemerkt über einen anderen – allerdings kostenpflichtigen – Mehrwertdienst zustande kommen.[446] Mit dem Aufkommen von Breitband-Internetanschlüssen sind Dialer-Programme mittlerweile auf andere Systeme als PCs, wie zB Mobiltelefone und Smartphones, ausgewichen. Man verwendet diesen Begriff inzwischen als Überbegriff für sämtliche »Trickbetrügereien«, die elektronische Dienste zu hohen Minuten- bzw SMS-Preisen anbieten.[447]

c. Browser-Hijacker

»Browser-Hijacker« manipulieren das Verhalten des verwendeten Internet Browsers. Dabei werden zum Teil schwerwiegende Systemeingriffe vorgenommen, die auch von versierten Nutzern kaum mehr rückgängig gemacht werden können. Beispielsweise werden unaufgefordert »Pop-Up-Seiten«[448] erzeugt oder Browser-Startseiten auf andere Webpages, die mit Werbung oder »Malicious Code« versehen sind, umgeleitet.[449] Über aktive Inhalte[450] dieser Webpages kann es den Hijackern schließlich auch gelingen, Zugriff auf das Zielsystem zu nehmen. Damit das Wiederherstellen der ursprünglichen Einstellungen weitge-

444 Ursprünglich wurden Dialer als seriöse Bezahldienste im Bereich des (unkörperlichen) Softwareerwerbs durch Download verwendet. Der Käufer konnte die entsprechende Software nur über einen kostenpflichtigen Mehrwert-Zugang herunterladen. Die Bezahlung erfolgte dadurch unmittelbar durch die Download-Zeit über die kostenpflichtige Telefonnummer (siehe *Winterer,* Viren, 229 f).

445 Siehe dazu *Janowicz,* Sicherheit[3], 258.

446 Vgl *Winterer,* Viren, 229 ff.

447 Siehe *Janowicz,* Sicherheit[3], 258.

448 Darunter versteht man plötzlich auftauchende Browser-Fenster oder Bildschirmmeldungen.

449 Siehe auch *Pfister,* Hacking, 33.

450 ZB ActiveX-Komponenten.

hend unterbunden wird, werden Hijacking-Trojaner dauerhaft ins System implementiert, die das »Browser-Hijacking« bei jedem Neustart des Zielsystems neu veranlassen.

d. Keylogger

Keylogger werden dazu eingesetzt, sämtliche Tastatur-Eingaben des Nutzers unbemerkt aufzuzeichnen und dem Täter zukommen zu lassen. Man unterscheidet zwischen Software- und Hardware-Keylogger[451], wobei Letztere eigenständige sehr kleine Computersysteme[452] darstellen, die mit dem zu überwachenden System in physische Verbindung gebracht werden müssen. Beispielsweise kann ein als Verbindungsstecker getarnter Hardware-Keylogger zwischen Tastatur und PC angeschlossen werden, der in weiterer Folge sämtliche Tastaturanschläge des Nutzers speichert.[453] Die aufgezeichneten Daten können – je nach Ausstattung der Schnüffelsoftware – zB per Funkverbindungen (zB Bluetooth) dem Täter in entsprechenden Abständen automatisiert übermittelt werden, oder die Geräte müssen – wie bereits beim Anbringen derselben – vor Ort manuell demontiert werden, um die Daten auswerten zu können. Sie unterscheiden sich von Keylogger-Programmen ua dadurch, dass ein Zugriff auf bzw über die Software des Zielsystems zur Installation des Schnüffelgeräts, aber auch für dessen Funktionsfähigkeit nicht erforderlich ist. Daher sind auch software-basierende Standard-Schutzmaßnahmen, wie Antivirenprogramme, Firewalls etc wirkungslos.

Software-Keylogger hingegen werden möglichst unbemerkt in das Zielsystem eingeschleust und verrichten ihre Arbeit zwischen Betriebssystem und Anwendungsprogrammen, wo sie zuerst sämtliche Tastaturanschläge einlesen und speichern und im Anschluss an das Betriebssystem zur Weiterverarbeitung weiterleiten.[454] Die aufgezeich-

---

451 Werden umgangssprachlich auch als »Hardware-Wanzen« bezeichnet; siehe dazu allgemein auch *Winterer,* Windows, 170 f.

452 Bestehend aus Hardware- und Software-Komponenten.

453 Siehe dazu auch *Feiler* in Zankl, Überwachungsstaat, 173 (183).

454 Siehe dazu *Emigh/Ramazan,* Overview of Crimeware, in Jacobsson/Ramzan (Eds), Crimeware. Understanding New Attacks and Defenses (2008) 2 (8 ff); weiters *Winterer,* Viren, 198 f; siehe auch *Bergauer,* Ausgewählte Aspekte der strafrechtlichen Betrachtung von Spyware, in Schweighofer/Liebwald/Drachsler/Geist (Hrsg), e-Staat und e-Wirtschaft aus rechtlicher Sicht – Tagungsband des 9. Internationalen Rechtsinformatik Symposions IRIS 2006 (2006) 327 (327 ff).

neten Daten werden dabei idR über bestimmte TCP[455]-Dienste[456] in regelmäßigen Abständen an den Täter übermittelt. Zur Installation dieser Schadprogramme ist aber ein Zugriff auf das Zielsystem notwendig. Für das Implementieren der Software am Zielsystem stehen dem Täter, neben der Vor-Ort-Manipulation[457], viele Möglichkeiten des Fernzugriffs über das Internet offen.

(Exkurs Ende)

Ein Virenschutzprogramm wäre grundsätzlich ein taugliches Instrument, um derartige Schadprogramme als Tatwerkzeuge des Täters aufzuspüren und abzufangen. Das Versenden eines E-Mails, das ein Schadprogramm im Anhang mitführt, reicht allerdings zur Verwirklichung des Tatbestandes nicht aus, um Daten eines »ungeschützten« Systems selbst nach Ausführung des Trojanischen Pferdes dem Täter zu übermitteln. Ein derartiger Fall wäre bei personenbezogenen Daten insb nach § 51 DSG 2000 bzw bei Daten, die sich gerade am Übertragungsweg befinden (zB unter Verwendung eines Keyloggers oder Sniffers[458]), nach §§ 119, 119a zu beurteilen. Darüber hinaus läge nicht einmal eine Versuchsstrafbarkeit iSd §§ 15, 118a Abs 1 vor, wenn keine Sicherheitsvorkehrung installiert ist und das Schadprogramm auch nicht in der Lage wäre, auf eine Sicherheitsvorkehrung entsprechend zu reagieren bzw diese gar zu deaktivieren.

Es kann für einen Betreiber eines Computersystems notwendig werden, mehrere spezifische Vorkehrungen zu treffen, um einen umfassenden technischen wie strafrechtlichen Schutz für sein Computersystem iSd § 118a zu erlangen. Als spezifische Sicherheitsvorrichtungen kommen sowohl Hardware-Maßnahmen (zB biometrische Verfahren der Zugangskontrolle, Hardwarefirewall[459]), aber auch Software-Vorkehrungen (wie zB Passwortkontrollen und Firewall-Programme[460]) in

455 Transmission Control Protocol (vgl *Gumm/Sommer,* Informatik[10], 638 ff).

456 ZB E-Mail und FTP.

457 ZB im Fall einer systematisierten Überwachung der Mitarbeiter auf den einzelnen Arbeitsplatzrechnern; oder die Programme befinden sich bereits ab »Werk« auf den Computersystemen, Smartphones.

458 Siehe dazu *Bergauer,* RdW 2006/391, 412; zu Sniffer-Vorrichtungen siehe auch *Kurose/Ross,* Computernetzwerke[4], 81 f.

459 Siehe *Bergauer,* RdW 2006/391, 412; vgl auch generell für das schweizerische Strafrecht *Pfister,* Hacking, 108 ff.

460 Siehe *Reindl,* E-Commerce, 153 ff; vgl *Bergauer,* RdW 2006/391, 412.

Betracht.[461] Auch könnte Antivirensoftware eine derartige Sicherungsvorkehrung sein, um Spionagezugriffe mittels Schadprogrammen, wie etwa Trojanischen Pferden, zu identifizieren und abzuwehren. Tatbildlich würde daher ein Täter agieren, der mittels solcher Spionagetools die Virenschutzsoftware überwinden bzw aus technischer Sicht wohl eher verletzen würde. Datenverschlüsselungen mittels kryptografischer Schlüssel etwa, sind keine spezifischen Sicherheitsvorkehrungen iSd § 118a Abs 1. Sie schützen ausschließlich vor der Erfassung des Bedeutungsinhalts der Daten, nicht vor dem Zugriff auf das System bzw die (verschlüsselten) Daten an sich.

Auch muss die spezifische Sicherheitsvorkehrung prinzipiell wirksam sein.[462] Das heißt, es würde bspw nicht ausreichen, bloß eine Passwortabfrage zu simulieren[463] oder ein System mit passwortgestützter Zugangssoftware auszustatten, wenn das entsprechende Passwort leicht[464] für jedermann zugänglich wäre oder ausdrücklich bekanntgegeben wurde.[465] *Reindl-Krauskopf* spricht dabei vom geheimen Charakter von Zugangscodes.[466] Der BGH hat iZm der zivilrechtlichen (Störer-)Haftung einer Privatperson wegen des Betriebs eines ungesicherten WLAN-Routers bei (Urheber-)Rechtsverletzungen durch Dritte festgehalten, dass einer Privatperson lediglich die im privaten Bereich marktüblichen Sicherungsmaßnahmen eines solchen Geräts zumutbar sind, wobei die Wahl eines persönlichen, ausreichend langen und sicheren Passworts anstelle der werkseitigen Standardeinstellungen des WLAN-Routers jedenfalls üblich und zumutbar ist.[467] Die Anforderungen sind aber für die Anwendbarkeit des § 118a Abs 1 und die Frage, ob eine spezifische Sicherheitsvorkehrung vorliegt, die das Schutzinteresse an den im System gespeicherten Daten zum Ausdruck bringt, wohl nicht zu streng anzusetzen, sodass etwa ein sehr einfaches und leicht zu eruierendes Passwort (zB 123456), aber auch ein vordefiniertes generelles Hersteller- bzw Master-Passwort (zB 0000) für das Vorhan-

461 Vgl *Thiele* in SbgK § 118a Rz 39.
462 Siehe *Reindl-Krauskopf* in WK² § 118a Rz 25.
463 ZB sind »Fake-Programme« oder ähnliche »digitale Attrappen«, die nur den Eindruck vermitteln es handle sich um gesicherte Systeme keine wirksamen tatbildlichen Sicherheitsvorkehrungen.
464 Als Beispiel ließe sich ein auf ein Stück Papier aufgeschriebenes Passwort anführen, das unmittelbar neben bzw auf dem Monitor oder PC vorzufinden ist.
465 Vgl *Reindl-Krauskopf,* Computerstrafrecht², 15; siehe auch *Reindl,* E-Commerce, 155.
466 Siehe *Reindl-Krauskopf,* Computerstrafrecht², 16.
467 BGH 12.05.2010, I ZR 121/08 = jusIT 2010/63, 138 *(Staudegger)*.

densein einer wirksamen Sicherheitsvorkehrung spricht und der Anwendung des § 118a Abs 1 nicht entgegensteht.[468]

Thiele will nicht auf die Wirksamkeit im Einzelnen abstellen. Das würde aber dazu führen, dass auch eine völlig untaugliche Sicherheitsvorkehrung, die nicht in der Lage ist einen konkreten individuellen Zugriff zu verhindern, ebenfalls für die Tatbildlichkeit ausreichen würde. Wie im oben geschilderten Fall wäre nach *Thiele* die Installation eines Virenschutzprogramms ausreichend, um vor Zugriffen eines Täters vor Ort und ohne Verwendung eines entsprechenden Computerprogramms als Tatmittel[469] schützen zu können. Da der Täter in diesem Fall kein Schadprogramm verwendet, wäre das Virenschutzprogramm, da es für völlig andere Zwecke geschaffen wurde, als Schutz gegen derartige Zugriffe völlig ungeeignet und wirkungslos. In anderen Fällen, nämlich wenn sich der Täter über ein Netzwerk mittels eines Trojanischen Pferdes Zugang zu diesem System verschaffen wollte, könnte das Antivirenprogramm jedoch sehr wohl als taugliches Schutzprogramm agieren. Die Aktualität des Virenschutzprogramms kann jedoch mE keine entscheidende Rolle für die Qualifizierung als spezifische und grundsätzlich wirksame Sicherheitsvorkehrung sein, da es in der Natur der Sache liegt, dass bei neu auftretenden Schadprogrammen, deren Signatur bzw Muster des Programmcodes noch unbekannt ist, die Antivirensoftware-Hersteller stets der Aktualisierung der Virendefinitionsdatensätze hinterher hinken. Vielmehr muss die Vorrichtung nur individuell für diese Art des Angriffs konzipiert sein. Auf eine grundsätzliche Wirksamkeit der Sicherheitsmaßnahme wird jedoch idR abzustellen sein, zumal bei völliger Untauglichkeit nicht einmal von einer Überwindung gesprochen werden kann.

6. Überwindung vs Verletzung

Wurde noch in der originären Definition des § 118a Abs 1 idF des StRÄG 2002[470] auf die »Verletzung« der Sicherheitsvorkehrung abgestellt, ist mit dem StRÄG 2008[471] diese Diktion auf das Erfordernis der »Über-

468 In diesem Sinn auch *Birklbauer/Hilf/Tipold,* Strafrecht BT I² § 118a Rz 5; aA *Reindl-Krauskopf* in WK² § 118a Rz 25; auch *Pfister,* Hacking, 110.
469 Erneut sei hierbei auf ein Trojanisches Pferd verwiesen.
470 BGBl I 134/2002.
471 BGBl I 109/2007.

windung« abgeändert worden, womit die Strafbarkeit insgesamt ausgeweitet wurde. Zu dieser Entwicklung ist am Rande anzumerken, dass bereits im ME[472] zum StRÄG 2002 das Kriterium der Überwindung vorgesehen war, doch wurde dieses in einigen Stellungnahmen im Zuge des Begutachtungsverfahrens als zu weitreichend erachtet.[473] Der Gesetzgeber schloss sich diesen Anregungen im Rahmen des Begutachtungsverfahrens schließlich an, indem die Verletzung der spezifischen Sicherheitsvorkehrung in § 118a Abs 1 aF tatbildlich wurde. Dies nicht zuletzt auch deshalb, weil diese Formulierung näher am Begriff »infringing« des Originaltexts der CCC[474] wäre.[475] Unter der Verletzung der spezifischen Sicherheitsvorkehrung wird nach den GMat das Eingreifen in die Daten- bzw Sachsubstanz derselben verstanden.[476] Eine derartige Handlung musste daher eine konkrete Einwirkung auf den spezifischen Schutzmechanismus der Sicherheitsvorkehrung bedeuten, der durch eine bewusste Manipulation außer Kraft gesetzt oder doch zumindest nachteilig modifiziert wird (zB das Löschen eines Firewallprogramms). Damit war in der aF eindeutig mehr als nur die »Überwindung« gefordert.[477]

In Zusammenschau mit den in der Praxis gemachten Erfahrungen und Stellungnahmen im Begutachtungsverfahren zum ME[478], aber auch in Hinblick auf die diesbezügliche Rechtsentwicklung in Deutschland zu § 202a dStGB[479] dehnte der Gesetzgeber die Strafbarkeit auf die bloße Überwindung der spezifischen Sicherheitsvorkehrung in § 118a Abs 1 idgF aus, sodass eine Beeinträchtigung der Daten- bzw Sachsubstanz nicht mehr erforderlich ist. Dabei muss ein gewisses Mindestmaß an krimineller Energie zur Überwindung vorliegen, »so dass etwa die Verwendung eines von der berechtigten Person – wenn auch unbefugterweise – mitgeteilt erhaltenen Passworts auch nicht unter den Begriff der ›Überwindung‹ einer Sicherheitsvorkehrung zu subsumieren sein wird«.[480]

---

472 ME zum StRÄG 2002, 308/ME XXI. GP, 7.
473 Siehe dazu ErlRV 285 BlgNR XXIII. GP, 7.
474 Vgl Art 2 CCC.
475 Siehe ErlRV 1166 BlgNR XXI. GP, 24.
476 Siehe ErlRV 1166 BlgNR XXI. GP, 24 und ErlRV 285 BlgNR XXIII. GP, 7.
477 Siehe *Fabrizy,* StGB und ausgewählte Nebengesetze[11] (2013) § 118a Rz 2; siehe auch die Anmerkungen dazu in den ErlRV 285 BlgNR XXIII. GP, 8.
478 ME zum StRÄG 2008, 92/ME XXIII. GP.
479 Mit der Deliktsbezeichnung »Ausspähen von Daten«.
480 Vgl ErlRV 285 BlgNR XXIII. GP, 7.

Man denke zB an den Fall, dass sich ein versierter Systembetreiber selbst eine grundsätzlich taugliche – aber fehlerbehaftete – Passwortzugangssoftware programmiert hat, die jedoch ungewollt jedes eingegebene Passwort für eine Zugangsfreigabe akzeptiert. Es wäre nicht zu verstehen, warum eine derartige – wenn auch mangelhafte – Vorkehrung nicht geeignet sein soll, das Schutzinteresse des Systemberechtigten vor unbefugten Zugriffen Dritter zum Ausdruck zu bringen. Nach außen hin würde man dieses Programm auch als eine Sicherheitsmaßnahme (vergleichbar mit einem »Einfahrt verboten – Ausgenommen Berechtigte« Verkehrszeichen) wahrnehmen können. Ob in solchen Fällen aber auch ein tatbestandliches Überwinden vorliegen würde, ist in einem anderen Zusammenhang zu prüfen. *Reindl-Krauskopf* verlangt ein bestimmtes Maß an »aktivem Zutun« (iS einer gewissen Anstrengung) des Täters, um die Schwelle der Strafbarkeit zu überschreiten.[481] Dieses Zutun würde daher entfallen, wenn der Täter ohne aktiven Aufwand Kenntnis vom Passwort erlangen würde, weil zB der Systemberechtigte selbst dem Täter das Passwort mitgeteilt hat. Diesem Erfordernis folgend dürfte daher im bloßen Eingabeversuch eines Passworts, der im Beispielsfall mit der fehlerhaften Zugangssoftware bereits zu einem Zugang führen würde, ebenfalls mangels »Überwindung« keine Tatbestandsmäßigkeit vorliegen. Das bloße Tippen auf einer fremden Tastatur wäre als noch sozial adäquate Handlung strafrechtlich unbeachtlich. Die Vorgehensweise des Täters ist vergleichbar mit dem Drücken einer Türklinke, um zu sehen, ob eine Türe versperrt ist oder nicht; ist diese nicht versperrt besteht keine wirksame Sicherung. Dass darin bereits eine gewisse Anstrengung[482] gesehen werden kann, um mit einer Schwierigkeit fertig zu werden, ist mE zu verneinen, ist doch wohl eine Sicherheitsvorkehrung wie ein Hindernis zu betrachten, das idR auch im Stande sein muss, Widerstand gegen einen entsprechenden Zugriff zu leisten.

Ähnlich wäre ein Sachverhalt zu beurteilen, in dem als Vorbereitungshandlung das neben dem Computersystem auf Papier geschriebene Passwort, das daher vom Systemverantwortlichen dem Täter nicht ausdrücklich mitgeteilt wurde und auch nicht allgemein bekannt ist, durch Ablesen eruiert wird und in weiterer Folge ohne be-

481 Siehe *Reindl-Krauskopf* in WK² § 118a Rz 28.

482 Vgl *Reindl-Krauskopf* in WK² § 118a Rz 26, die auf die Definition des Begriffs »überwinden« nach dem Duden verweist.

rücksichtigungswürdigenden Aufwand dem Täter durch Eingabe des passenden Kennworts den Zugriff auf das fremde Computersystem ermöglicht. Es handelt sich dabei nämlich um das tatsächliche Passwort, das vom Täter ohne einer gewissen Anstrengung errechnet[483] oder verschafft wurde.

Die bloße Eingabe eines offen einsehbaren – ggf gleich neben dem System befindlichen – Passworts kann für einen vernünftig denkenden Menschen nicht mit der Bewältigung einer gewissen Schwierigkeit verglichen werden.[484] Die im System angebrachte passwortbasierende Zugangssoftware ist zwar als spezifische Sicherheitsvorkehrung iSd § 118a Abs 1 zu werten, doch wird diese mangels gehöriger Anstrengung (hier: bloße Eingabe eines vom Berechtigten nicht gehörig geheim gehaltenen Passworts) in einem solchen Fall nicht überwunden. In diesem Sinn urteilte wohl auch der OGH iZm § 129, wenn er einen zufällig passenden Schlüssel von einem nachgemachten Schlüssel unterscheidet.[485]

Eine Subsumtion dieser Vorbereitungshandlung unter das Vorbereitungsdelikt des § 126c Abs 1 Z 2 (iSd »Sich-Verschaffen von Zugangsdaten«) wäre darüber hinaus ebenfalls nicht unproblematisch.[486]

Anders wäre der Fall jedoch zu beurteilen, wenn der Täter intensivere Anstrengungen unternehmen muss, um die Sicherheitsvorkehrung des gesicherten Servers zu passieren, indem er zB mittels »Brute Force«[487]-Programmen das Passwort ermittelt, durch das Übermitteln

483 Siehe zu sog »Brute Force«-Programmen gleich im Anschluss.

484 Siehe dazu auch *Reindl-Krauskopf,* Computerstrafrecht[2], 16.

485 Vgl OGH 29.07.1981, 11 Os 70/81.

486 Siehe dazu die Ausführungen zu § 126c (S 317 ff).

487 »Rohe Gewalt«; dabei handelt es sich um Computerprogramme, die alle möglichen Kombinationen vordefinierter Zeichenketten (wie etwa »abcdefghijklmnopqrstuvwxyz« und »0123456789«) durchprobieren, um so das »passende« Passwort ermitteln zu können. Dahinter steckt ein systematisches Abarbeiten von endlichen Zeichenfolgen, welche bei Verwendung aller als Passwort möglichen Zeichen, nach einer kurz oder lang andauernden Zeitspanne, die Berechnung des konkreten Kennworts durch Permutation mathematisch garantiert. Die Zeitdauer eines solchen Angriffs ist allerdings unter Berücksichtigung des derzeitigen Stands der Technik bei Verwendung eines sinnvollen Zeichensatzes unverhältnismäßig lang. Eine weitere Angriffsmöglichkeit würde die sog »Dictionary-Attack« bieten, bei der eine Liste mit sehr häufig als Passwort verwendeten Zeichenfolgen programmgesteuert durchgearbeitet wird. In dieser Variante werden eigene Sammlungen (bei Passwort-Hash-Werten auch »Regenbogentabellen« genannt) von potentiellen und häufig verwendeten Passwörtern durchprobiert, wobei dies zwar die Geschwindigkeit des Angriffs erhöht, jedoch zu Lasten der Trefferquote geht (vgl dazu *Gollmann,* Computer Security[3] [2011] 52 ff).

von Datenpaketen (DoS) die Software bzw den Zugangsdienst außer Funktion setzt oder sich Zugangsdaten im Wege des Phishing verschafft. In solchen Fällen, die zB bei »Brute Force«-Attacken in weiterer Folge zur Ermittlung und letztlich Eingabe eines passenden Kennworts führen, liegt – im Gegensatz zu den Fällen des freiwillig mitgeteilten bzw nicht gehörig geheim gehaltenen Kennworts – bereits ein tatbestandliches Überwinden vor. So wird wohl auch das oben angeführte Beispiel der GMat gemeint sein, dass in einem Fall, in dem ein passendes Kennwort für den Systemzugriff unbefugt verwendet wird, das mittels ins Gewicht fallender krimineller Energie (rechtswidrig) erlangt wurde, eine Sicherheitsvorkehrung tatbestandlich überwunden werde.[488]

7. Überwindung vs Umgehung

Ein Überwinden ist aber mehr als ein bloßes Umgehen.[489] Würden zwei unterschiedliche Datenübertragungswege, nämlich einer davon durch eine spezifische Sicherheitsvorkehrung gesichert, der andere ungesichert, die Verbindung zum konkreten Zugriffsobjekt ermöglichen, so würde der Täter im zweiten Fall die Sicherheitsvorkehrung bloß umgehen.[490]

Ein Überwinden erfordert mE die Konfrontation des Täters mit der spezifischen Sicherheitsvorkehrung, etwa durch Ausarbeitung eines Überwindungsplans und die anschließende direkte Bezwingung. In Anlehnung an die Begrifflichkeit in § 109 Abs 3 Z 2 oder § 129 Z 4 könnte man auf das Überwinden eines Widerstandes der Sicherheitsvorkehrung schließen.[491] Auch hat der OGH iZm § 129 Z 1 hins des Begriffs »einsteigen« festgestellt: »[…] die größere verbrecherische Energie zur Überwindung von Hindernissen und Widerständen, die andere Diebe scheuen oder umgehen, macht diesen Täter gefährlicher und darum strafwürdiger […]«.[492] Ebenso legt »eine solche größere verbrecherische

488 Vgl ErlRV 285 BlgNR XXIII. GP, 7.

489 Vgl *Bergauer/Schmölzer* in Jahnel/Mader/Staudegger, IT-Recht[3], 635 (658).

490 Abgesehen davon kann davon ausgegangen werden, dass der Täter in einem derartigen Fall die Überwindung der Sicherheitsvorkehrung nicht in seinen Vorsatz aufgenommen hat, weshalb die Tatbestandsmäßigkeit zudem am subjektiven Tatbestand scheitert würde.

491 In den genannten Bestimmungen zum Hausfriedensbruch oder Einbruchsdiebstahl geht es darum, »[…] den Widerstand einer Person zu überwinden […]«.

492 Vgl OGH 30.09.1976, 9 Os 101/75.

Energie ein Dieb an den Tag, der einen Schlüssel nachmacht, das heißt sich eigenmächtig einen für das betreffende Schloss passenden Schlüssel entweder nach dem Originalschlüssel dieses Schlosses oder nach einem Abdruck desselben etc anfertigt oder anfertigen lässt, indem er sich das Original oder den Abdruck verschafft hat oder der sich den Originalschlüssel widerrechtlich aneignet und damit aufsperrt, nicht aber ein Dieb, der bloß den Umstand nützt, dass er zufällig über einen passenden, an sich aber zu einem anderen Schloss gehörenden Schlüssel verfügt und mit diesem aufsperrt«.[493]

Auch aus dieser Aussage, die im Wesentlichen auf die kriminelle Energie Bezug nimmt, lässt sich ableiten, dass ein Überwinden mehr an krimineller Energie erfordert als das bloße Umgehen. In diesem Sinn erläutert der OGH auch in einer weiteren E, dass die Umgehung des Zündschlosses eines PKW durch Kurzschließen (der Zündkabel) nicht die Voraussetzungen der Überwindung einer Sperrvorrichtung iSd § 129 Z 3 darstellt.[494]

Der Täter muss somit auch iZm § 118a Abs 1 auf die im System installierte Sicherheitsvorkehrung entsprechend reagieren, um dieses Hindernis direkt bezwingen zu können. Eröffnet sich daher eine zusätzliche Möglichkeit für einen Zugriff, ohne auf ein Hindernis zu stoßen, so liegt kein tatbestandliches Überwinden vor. Zu denken wäre bspw an ein Netzwerk, zu dem man sich über zwei unterschiedliche Remote Access Server (RAS) anmelden kann, wovon jedoch nur einer mit Zugangssoftware gesichert ist. Verwendet der Täter den ungesicherten Zugang, so würde zwar eine im System angebrachte Sicherheitsvorkehrung umgangen, nicht jedoch in Form eines Hindernisses überwunden werden. Wählt der Täter den anderen (gesicherten) Weg, weil er etwa von der zweiten Variante nichts wusste, so kommt ihm die zwar ebenfalls möglich gewesene ungesicherte Zugriffsmöglichkeit nicht zu gute.[495] Man könnte aber in diesem Fall auch so weit gehen, die Eigenschaft der Sicherheitsvorkehrung als eine spezifische anzuzweifeln, da ein System, das über mehrere Zugänge verfügt, eben an allen diesen Zugangsmöglichkeiten entsprechend gesichert sein muss, andernfalls keine »spezi-

493 Siehe OLG Linz 07.01.1997, 7 Bs 350/96 mit Verweis auf OGH 21.04.1977, 12 Os 9/77 verst Senat; OGH 29.10.1985, 10 Os 124/85; OGH 12.01.1993, 14 Os 156/92.

494 Siehe OGH 29.07.1981, 11 Os 70/81.

495 Siehe dazu den annähernd vergleichbar iZm dem Einbruchsdiebstahl *Bertel* in WK² § 129 Rz 11 (Stand Dezember 2008).

fische« – weil nicht geeignete – Schutzmaßnahme besteht.[496] Meines Erachtens ist nämlich die Sicherheitsvorkehrung so auszugestalten, dass sie jeden Zugreifenden ausschließlich über einen gesicherten Zugangsweg zum System führen muss. Ist dies nicht der Fall, liegt auch keine geeignete und wirksame Sicherheitsvorkehrung vor.

Allerdings besteht dabei das Problem in der Abgrenzung der Systemkomponenten und der damit einhergehenden Beurteilung der gegenständlichen technischen Infrastruktur als tatbildliches Computersystem, weshalb in derartig gelagerten Sachverhalten[497] die Frage der Zuordnung einer Sicherheitsvorkehrung zum tatgegenständlichen Computersystem eine zentrale Bedeutung einnimmt.[498]

Auch das durchaus realistische Beispiel von *Reindl-Krauskopf*[499], in dem eine mit einem ausführbaren Betriebssystem selbstständig lauffähige CD-ROM[500] verwendet wird, ohne das Betriebssystem des Zielsystems samt etwaiger Zugangssoftware ausführen zu müssen, um an die Daten desselben zu gelangen, ist mE – in Anlehnung an die oben beschriebenen Fälle, aber entgegen der Ansicht *Reindl-Krauskopfs* – bloß eine Umgehung der Sicherheitsvorrichtung und daher keine Überwindung. In concreto liegen ebenfalls zwei unterschiedliche Zugriffswege vor, von denen nur einer gesichert ist[501], der andere – vom Täter geschaffene – nicht. Die bloße Umgehung ist dort zu erblicken, wo das Hindernis des technischen Widerstandes der Sicherheitsvorkehrung eben nicht berührt wird, sondern dieser Hürde ausgewichen wird. Lässt eine Sicherheitsvorkehrung einen Umweg zu, so ist sie nach den oben getroffenen Aussagen weder spezifisch noch wirksam gegen diesen konkreten Zugriffsversuch konzipiert.[502] Es ist für den Systemverantwortlichen technisch leicht realisierbar, die »Boot-Funktion« für externe Medien im System zu unterbinden und die diesbezüglichen Einstell-

496 Siehe dazu bereits oben.
497 Insbesondere iZm Datenverarbeitungen über Netzwerke.
498 Siehe dazu auch *Bergauer,* RdW 2006/391, 412.
499 Siehe die aA *Reindl-Krauskopf,* Computerstrafrecht², 17.
500 Aktueller wäre das Beispiel wohl mit einem bootfähigen und mit einem lauffähigen Betriebssystem ausgestatteten USB-Stick anstelle einer CD-ROM.
501 Gesichert, und daher mit einer spezifischen Sicherheitsvorkehrung ausgestaltet, wäre der Zugang zum System nur über das dort installierte Betriebssystem.
502 Vgl den Virenscanner, der zwar gegen Zugriffe mittels Schadprogrammen als Sicherheitsvorkehrung geeignet wäre, nicht aber gegen vor Ort-Zugriffe des Täters ohne diese Tatwerkzeuge.

möglichkeiten im System[503], ebenfalls mit einer Passwortabfrage vor Veränderungen zu schützen. Auch wäre es möglich lediglich zB die interne Festplatte[504] mit entsprechendem Zugriffsschutz zu versehen, sodass erst diese Festplattensicherung die tatbildliche Sicherheitsvorkehrung darstellte. Mit einer solchen Schutzvorkehrung könnte ein Zugriff über externe Boot-Medien wirksam unterbunden werden.

Ein derartiger Sachverhalt ist mit dem oben angeführten Fall des »Kurzschließens« eines PKW insoweit vergleichbar[505], als hierbei nur eine Umgehung und nicht eine Überwindung der Sperrvorrichtung vorliegt.[506] In diesem Sinn ist auch »die Umgehung eines Fahrrad-Schlosses« durch Abmontieren des Gepäckträgers zu verstehen.[507]

Eine derartige Vorgehensweise mittels externer Boot-Medien[508] stützt sich – im Gegensatz zu den in den GMat[509] angesprochenen Angriffsmethoden der »Code Injection«[510], »SQL[511] Injection«[512] oder »Race Conditions«[513] – gerade nicht auf Systemschwachstellen der installierten (Software-)Sicherheitsvorkehrung, sondern nützt generell die unzureichende Systemsicherung durch den Systembetreiber aus.

---

503 Gemeint ist zB die Konfiguration der »BIOS-Einstellungen« (BIOS = Basic Input Output System).

504 Grundsätzlich ist iSd von Neumann-Architektur jede Festplatte ein externes Gerät. An dieser Stelle ist allerdings mit der Bezeichnung »intern« eine im Gehäuse des Computers eingebaute Festplatte gemeint.

505 Man beachte das Analogieverbot, doch dient dieser Vergleich lediglich der Interpretation des Begriffs »überwinden«.

506 Siehe OGH 10.10.1978, 11 Os 144/78; OGH 29.07.1981, 11 Os 70/81.

507 Vgl OGH 28.06.1994, 14 Os 78/94.

508 Denkbar wäre auch, dass der Täter die Festplatte des Zielsystems ausbaut, um die Passwortabfrage des BIOS im Zuge des Bootens des Rechners zu »umgehen«.

509 Siehe dazu ErlRV 285 BlgNR XXIII. GP, 7.

510 »Code Injection« ist der generelle Überbegriff für Handlungen, bei denen der Täter versucht eigenen (schädigenden) Code ins Zielsystem einzuschleusen, vgl etwa »Cross-Site-Scripting« (XSS), »SQL Injection«, »PHP Injection« uÄ.

511 »Structured Query Language«.

512 Dabei versucht der Angreifer über eine Benutzereingabeaufforderung oder URL-Requests zur Abfrage einer SQL-Datenbank eigenen SQL-Code einzuschleusen, um Zugriff auf die Datenbank zu erhalten; siehe dazu ausf *Clarke,* SQL Injection. Attacks and Defense (2012) 6 ff.

513 Hierbei bleiben mehrere Prozesse im Wartezustand gefangen, weil sie wechselseitig auf sich oder auf dieselben Ressourcen zugreifen wollen. Das »Wettrennen« um den Zugriff wird »Race Condition« genannt, wobei eine solche Situation auch zu einem »Deadlock« führen kann, wenn sich dabei beide Programme gegenseitig sperren oder anderwärtig behindern. Ein solcher Deadlock führt zumindest zum Absturz der betroffenen Prozesse, wenn nicht sogar zum Absturz des Gesamtsystems (vgl *Kersken,* IT-Handbuch[5], 301).

Mit dem Erlangen des Zugangs zu einem Computersystem durch Überwindung einer spezifischen Sicherheitsvorkehrung im Computersystem ist der tatbestandliche Erfolg eingetreten (Erfolgsdelikt), der objektive Tatbestand daher erfüllt und die Tat – entsprechenden deliktsspezifischen Vorsatz vorausgesetzt – auch formell vollendet.[514]

8. Subjektive Tatseite

Der subjektive Tatbestand des § 118a Abs 1 ist äußerst komplex. Er verlangt neben dem Tatbildvorsatz, der sich zumindest in Form des dolus eventualis (§ 5 Abs 1 zweiter HS) auf das Eindringen in ein fremdes Computersystem durch die Überwindung einer spezifischen Sicherheitsvorkehrung richten muss, auch hohe Absichtsanforderungen in einem erweiterten Vorsatz des Täters. Folglich muss dieser im Zeitpunkt der Handlungsvornahme eine »doppelte« Absicht[515] (iSd § 5 Abs 2) verfolgen.

Zum einen handelt es sich um die Datenspionageabsicht – sich oder einem anderen Unbefugten von den im Computersystem gespeicherten Daten Kenntnis zu verschaffen –, zum anderen um eine Gewinn- bzw Schädigungsabsicht – sich oder einem anderen durch die Datenverwendung[516] einen Vermögensvorteil zuzuwenden (= Gewinnabsicht) oder zumindest einem anderen einen Nachteil zuzufügen (= Schädigungsabsicht). Der Nachteil muss nicht unbedingt vermögensrechtlicher Natur sein, doch muss er jedenfalls über die bloße Verletzung der Geheimhaltung hinausreichen.[517]

---

514 Materiell beendet ist die Tat erst bei Realisierung der überschießenden Innentendenzen.

515 Siehe zur entsprechenden Begründung der hier vertretenen »doppelten Absicht« gleich im Anschluss; des Weiteren – allerdings ohne Begründung – für eine »doppelte« Absicht: *Bertel/Schwaighofer,* Österreichisches Strafrecht. Besonderer Teil I (§§ 75 bis 168b StGB)[12] (2012) § 118a Rz 3; *Bergauer,* RdW 2006/391, 412; *Kienapfel/Schroll,* Grundriss des österreichischen Strafrechts. Besonderer Teil I[5] (2003) 401; wohl auch *Schmölzer,* ZStW 2011/123, 709 (729); *Eder-Rieder,* Wirtschaftsstrafrecht[3], 200; *Bergauer,* Viren, Würmer, Trojanische Pferde – Computerstrafrecht auf dem Prüfstand, in BMJ (Hrsg), 35. Ottensteiner Fortbildungsseminar aus Strafrecht und Kriminologie (2007) 27 (35); für eine »dreifache« Absicht (iS einer Datenspionageabsicht, einer Datenverwendungsabsicht und einer Gewinn- bzw Schädigungsabsicht): *Thiele* in SbgK § 118a Rz 57; *Seling,* Privatsphäre, 78; *Fuchs/Reindl-Krauskopf,* BT I[4], 124; *Reindl-Krauskopf,* Computerstrafrecht[2], 17 f; *Reindl,* E-Commerce, 160.

516 Im Sinne eines Selbst-Benützen, Einem-anderen-Zugänglichmachen oder Veröffentlichen.

517 Vergleichbar *Flora,* Das Bankgeheimnis im gerichtlichen Strafverfahren (2007) 33.

Die Formulierung der überschießenden Innentendenzen ist jedoch nicht sonderlich stimmig. Bekanntlich definiert eine überschießende Innentendenz einen weiteren Unrechtsteil als Anforderung an die Tat, der über den äußeren (objektiven) Tatbestand (erster Unrechtsteil) hinausreicht.

Der objektive Tatbestand des § 118a Abs 1 lässt sich zusammenfassen als das Zugangverschaffen zu einem fremden Computersystem durch Überwindung einer Sicherheitsvorkehrung dieses Systems. Der erste Teil des erweiterten Vorsatzes, die Spionageabsicht, verlangt aber nur, dass der Täter im Tatzeitpunkt in der Absicht handelt, sich oder einem anderen Unbefugten Kenntnis von in »einem« Computersystem gespeicherten und nicht für ihn bestimmten Daten zu verschaffen. Daraus wird ersichtlich, dass sich die subjektive Zielvorstellung des Täters dem Wortlaut nach nicht ausschließlich auf die Daten des Systems richten muss, auf das sich der Täter objektiv widerrechtlich Zugriff verschafft hat.

Beispiel: Der Informatikstudent A betreibt in seiner Wohnung zwei Computersysteme, denen er die Systemnamen Bit und Byte gegeben hat. Bit ist mit einem Passwortschutz ausgestattet, Byte (noch) nicht. Der Nachbar B will sich Zugriff auf Byte verschaffen. Um A von Byte abzulenken, überwindet er mittels des zuvor durch ein »Brute Force«-Programm ermittelten Passworts die Sicherheitsvorkehrung vom System Bit. A wendet sich daraufhin von Byte ab, um das Sicherheitsproblem bei Bit zu lösen, woraufhin B über das Netzwerk Zugriff auf die Daten des ungesicherten Byte nimmt.

B hat sich vorsätzlich widerrechtlichen Zugriff auf ein Computersystem (Bit) verschafft, indem er spezifische Sicherheitsvorkehrungen im Computersystem (Bit) überwunden hat. Der objektive Tatbestand ist daher erfüllt.

Darüber hinaus hat B auch in der Absicht gehandelt, sich von in einem Computersystem (Byte) gespeicherten und nicht für ihn bestimmten Daten Kenntnis zu verschaffen. Würde B weiters die Zielvorstellung verfolgen, diese Daten zu verwenden, um sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen, wäre auch der subjektive Tatbestand gänzlich erfüllt.

Sinnvoller Weise wird man wohl die überschießenden Innentendenzen an den objektiven Tatbestand insoweit anschließen müssen, dass sich die Absicht, sich von den Daten Kenntnis zu verschaffen, ausschließlich auf die Daten des Computersystems beziehen muss, zu

dem sich der Täter auch (objektiv) Zugang verschafft hat. Der subjektive Tatbestand ist daher entsprechend teleologisch zu reduzieren.

a. Deliktstypus nach Bewertung der überschießenden Innentendenzen

Betrachtet man die Struktur der überschießenden Innentendenzen, so ergeben sich auch dort gewisse Besonderheiten. Die erste überschießende Innentendenz lässt § 118a Abs 1 als sog »kupiertes Erfolgsdelikt«[518] (= Absichtsdelikt ieS[519]) in Erscheinung treten, da die Kenntniserlangung der Daten bloß einen – über den objektiven Tatbestand hinausreichenden – anvisierten Erfolg darstellt. Die Erreichung dieses Erfolgs ist aber nicht (mehr) tatbestandsmäßig. Hat der Täter somit den objektiven Tatbestand erfüllt, ist die Tat formell bereits vollendet, sofern die überschießenden Innentendenzen zum Tatzeitpunkt vorliegen. Die Strafbarkeit wurde insoweit vom Gesetzgeber vorverlagert. Werden auch diese rein anvisierten Ziele in weiterer Folge tatsächlich realisiert, ist die Tat auch in materieller Hinsicht beendet.

Die Rechtsgutbeeinträchtigung hält somit grundsätzlich auch nach formeller Vollendung des objektiven Tatbestands weiter an[520], weil der Täter in diesem Fall auf äußerer Tatseite noch nicht alles getan hat, um sein anvisiertes Endziel zu erreichen. Mit der widerrechtlichen Zugriffsverschaffung (Zwischenerfolg) hat er idR noch nicht Kenntnis von den Daten erlangt, weshalb der Erfolg der Kenntnisverschaffung noch nicht eingetreten ist. Dieser kann nun aber unmittelbar ohne ein weiteres Zutun des Täters eintreten, wenn etwa nach der Überwindung der spezifischen Sicherheitsvorkehrung (zB durch Manipulation der Passwortabfrage) bereits geöffnete Dokumente am Zielsystem für den Täter unmittelbar einsehbar sind, oder durch weiteres Zutun, wenn der Täter gewünschte Daten des Computersystems zur Kenntnisnahme einem Dritten vermittelt. Auch wäre es denkbar, dass nach Zugriffsverschaf-

518 Siehe zur Begrifflichkeit allgemein *Fuchs,* AT I[8] Rz 10/60; vgl auch *Triffterer,* Österreichisches Strafrecht. Allgemeiner Teil [2] (1994) 67.

519 Da in diesem Zusammenhang auch tatsächlich »Absicht« iSd § 5 Abs 2 in Bezug auf den angestrebten Erfolg vorliegen muss.

520 Sofern nicht der Täter die Tat nach Erfüllung des objektiven Tatbestands aufgegeben hat oder aufgeben musste, bevor die Endziele tatsächlich erreicht wurden.

fung durch den unmittelbaren Täter ein Dritter hinzutritt und sich von auf diesem System gespeicherten Daten selbst Kenntnis verschafft.

Die zweite kumulativ erforderliche Innentendenz zielt darauf ab, dass diese Daten vom Täter verwendet werden, um sich oder einem anderen einen Vermögensvorteil zu verschaffen bzw einem anderen einen Nachteil zuzufügen. Da der Täter hierbei den angestrebten Enderfolg selbst durch die Datenverwendung realisieren will, liegt – strafrechtsdogmatisch betrachtet – sowohl ein »verkümmert mehraktiges Delikt«[521] als auch ein kupierter Erfolg vor. Bei Vornahme des objektiven Tatbestands strebt der Täter bereits eine weitere Handlung (Datenverwendung) an, die er selbst durchführen will (arg »er die Daten selbst benützt«). Es spielt – anders als bei § 51 DSG 2000, wo es mE ausschließlich auf die Dateninhalte ankommt – keine Rolle, ob der Täter die Dateninhalte dabei verwertet oder die Daten als elektronisch verarbeitbare Einheiten unabhängig von ihrem Informationswert[522] gebraucht. Dieses anvisierte weitere Handeln soll aber letztlich zu einem spezifischen Enderfolg führen (arg »dadurch«), nämlich sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen. Die Bindung der angestrebten Handlung an diese (alternativen) angepeilten Endziele lassen diese Variante der überschießenden Innentendenz als eine Einheit in Erscheinung treten[523], bei der zumindest geprüft werden muss, ob die auf der subjektiven Tatseite (angestrebte) Handlung objektiv geeignet ist, den (anvisierten) Enderfolg herbeizuführen.

Bezüglich des zweiten Unrechtsteils des subjektiven Tatbestands ist § 118a Abs 1 somit ein »verkümmert zweiaktiges Delikt mit spezifischem kupiertem Enderfolg«.

Führt man beide kumulativ zu erfüllenden Unrechtsteile des erweiterten Vorsatzes zusammen, so lassen sich unter Berücksichtigung des objektiven Tatbestands insgesamt drei Erfolge erkennen:

---

521 Siehe zur Begrifflichkeit allgemein *Fuchs,* AT I[8] Rz 10/59; vgl auch *Triffterer,* AT[2], 67.

522 ZB würde das Öffnen einer Datei, selbst wenn diese keinen Informationswert führen würde, bereits ein Benützen der Daten im Sinne des § 118a Abs 1 darstellen (nicht so bei § 51 DSG 2000; siehe unten).

523 Darum ist es mE auch zutreffender von einer »doppelten« Absicht – als von einer dreifachen – zu sprechen, die jeweils ein anvisiertes Endziel verfolgen. Zum einen sich oder einem anderen Kenntnis von den Daten zu verschaffen und zum anderen durch die Verwendung dieser Daten, sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen.

1. Die Erfüllung des objektiven Tatbestands führt tatbestandlich betrachtet zum Zwischenerfolg des Zugriffverschaffens auf ein fremdes Computersystem.

2. Der anvisierte erste Enderfolg der Datenspionageabsicht.

3. Der beabsichtigte zweite Enderfolg der Vermögensvorteilsverschaffung bzw Nachteilszufügung muss ebenfalls nur in der Vorstellung des Täters angestrebt werden.

§ 118a Abs 1 stellt daher ein verkümmert zweiaktiges Delikt mit einem Taterfolg und zwei spezifischen kupierten Enderfolgen dar.

Aus dem objektiven Tatbestand lässt sich ein vom Gesetzgeber intendierter Zugangsschutz zu Computersystemen erkennen, der auf das Rechtsgut »Privatsphäre«, ähnlich einem (virtuellen) Hausfriedensbruch, fokussiert. Aus den überschießenden Innentendenzen ergibt sich ua ein vorverlagerter »Datenschutz«, der aber wiederum an weitere Voraussetzungen geknüpft ist und nicht generell besteht.[524]

Unklar ist, warum der Gesetzgeber in einem Delikt, das das Rechtsgut »Privatsphäre« schützt, überhaupt (auch) eine Gewinnabsicht vorsieht.[525] Man könnte darauf schließen, dass der Gesetzgeber lediglich versucht hat einen »dishonest intent«[526] zu formulieren, wie es in Art 2 CCC als eine Alternative zur ausdrücklich genannten Datenspionageabsicht unsubstanziiert normiert wurde[527] und auch im Begutachtungsverfahren zum ME[528] mehrfach angeregt wurde. Doch will die CCC lediglich ein Mindestschutzniveau im Bereich des Computerstrafrechts sicherstellen, weshalb die einzelnen nationalen Rechtsordnungen (hier: Mitgliedstaaten des Europarats) ihre Regelungen nicht unter den Mindestanforderungen der CCC ausgestalten dürfen. Eine Gewinnabsicht iZm den Vorgaben der CCC zu Maßnahmen gegen »illegal access« wird daher weder in der Konvention selbst noch in den Erl[529] explizit erwähnt, geschweige denn als notwendig erachtet. Das

524 So auch *Schmölzer,* ZStW 2011/123, 709 (728).
525 Wenn auch alternativ zu einer Schädigungsabsicht.
526 Es lässt sich aus den Erl erkennen, dass dort bei diesem Ausdruck von einem erweiterten Vorsatz (»special intent«) ausgegangen wird und nicht vom allgemeinen Tatbildvorsatz (»general intent«).
527 »[…] with the intent of obtaining computer data or other dishonest intent, […]«.
528 ME zum StRÄG 2002, 308/ME XXI. GP.
529 Vgl ER (ETS 185) Pkt 50.

hohe Absichtserfordernis der österr Umsetzung in § 118a Abs 1 ist daher »hausgemacht« und mE völlig überschießend.[530]

Nach den GMat[531] liegen sämtliche Daten iSd § 74 Abs 2 im Schutzbereich des Art 2 CCC und nicht nur etwa »Nachrichten«[532] (wie – im weiteren Sinn – bei den §§ 118, 119 und 120 Abs 2a). Auch (sonst) besonders schutzwürdige, wie zB personenbezogene Daten oder auch nur »gewöhnliche«, dem geringsten strafrechtlichen Schutz zugedachte, Daten sind umfasst, was sich auf den korrespondierenden § 118a auswirken muss.

In diesem Sinn wurde der subjektive (Grund-)Tatbestand des § 118a Abs 1 am unterschiedlichen Schutzniveau der jeweiligen Datenqualität ausgerichtet. Da nunmehr aber nach den GMat die Schutzbestimmungen zu Gunsten von Nachrichten, die durch weniger hohe (subjektive) Anforderungen ausgestaltet sind, ohnehin weiterhin bestehen bleiben sollen, ist für die sonstigen (gewöhnlichen) Daten noch ein weiters (subjektives) Element zu ergänzen.[533] Dabei wird jedoch übersehen, dass es Fälle gibt, in denen diese Schutzbestimmungen für Nachrichten (wie zB § 119) nicht greifen und § 118a Abs 1 nunmehr auch für Nachrichten lediglich unter den erhöhten subjektiven Erfordernissen anwendbar wäre. So ein Fall liegt etwa dann vor, wenn Nachrichten nicht am elektronischen Übertragungsweg abgefangen, sondern

530 Siehe dazu bereits krit *Bergauer,* RdW 2006/391, 412.

531 Vgl ErlRV 1166 BlgNR XXI. GP, 24.

532 Zum strafgesetzlichen Begriffsverständnis siehe S 164 ff.

533 »Nach geltendem österreichischem Recht wird nun aber schon bei Nachrichten eine besondere Absicht, nämlich sich (bzw. einem anderen Unbefugten) Kenntnis zu verschaffen, verlangt (vgl. §§ 118 Abs. 2, 119 und 120 Abs. 1); und selbst bei (sonst) besonders schutzwürdigen Daten muss, wenn nicht überhaupt nur die Offenbarung oder Verwertung strafbar ist (vgl. § 121 StGB in Bezug auf die Verletzung von Berufsgeheimnissen, § 51 des Datenschutzgesetzes 2000 in Bezug auf personenbezogene Daten), jedenfalls ein (besonderer) erweiterter Vorsatz vorliegen (vgl. § 123 StGB für die Auskundschaftung eines Geschäfts- oder Betriebsgeheimnisses). Der Entwurf schlägt daher nunmehr vor, von der Möglichkeit der Beschränkung der Strafbarkeit auf einen »dishonest ident« im Form folgender Kombination Gebrauch zu machen: Zunächst soll der Täter – wie in Bezug auf Nachrichten – die Absicht verfolgen müssen, sich oder einem anderen Unbefugten Kenntnis von den Daten zu verschaffen. Da die Schutzbestimmungen zu Gunsten von Nachrichten aber ohnehin weiterhin bestehen bleiben sollen, soll für die sonstigen (gewöhnlichen) Daten noch ein Element hinzukommen.« (ErlRV 1166 BlgNR XXI. GP, 24); Anmerkung: es wird wohl »dishonest intent« iSd Art 2 CCC gemeint sein.

durch Hacking ausspioniert werden.[534] In einem derartigen Fall wäre § 119 nicht anwendbar.[535] Im Gegensatz dazu ist aber die Anwendung des § 118a Abs 1 durchaus denkbar, sofern der Täter spezifische Sicherheitsvorkehrungen des Computersystems überwindet, um sich Kenntnis von den Nachrichten zu verschaffen. Diese Spionageabsicht, wie sie zB in § 119 oder auch § 120 Abs 2a formuliert ist[536], reicht aber zur Verwirklichung des § 118a alleine nicht aus, da eben trotz der erhöhten Datenqualität einer »Nachricht« weitere Vorsatzanforderungen bestehen. Insofern liegt in diesem Fall eine nicht systemkonforme Strafbarkeitslücke vor. Die GMat[537] zum erhöhten Vorsatzerfordernis bei § 118a Abs 1 lassen darin schon allein aus diesem Grund auf kein angemessenes, rechtspolitisch durchdachtes Konstrukt schließen. Die hohe Schwelle für den Eintritt der gerichtlichen Strafbarkeit aufgrund der objektiven, aber vor allem hins der sehr hohen subjektiven Anforderungen an die Tat ist kriminalpolitisch nicht zu vertreten und führt zu einer gravierenden Minderanwendbarkeit dieser Strafbestimmung, was auch die eingangs angeführten Verurteilungszahlen nahelegen.[538]

Doch wird in den GMat übersehen, dass es – wie zur »Datenqualität« bezüglich der Spionageabsicht bereits ausgeführt – eben nicht auf den Inhalt (also den Informationswert) im Fall des § 118a Abs 1 ankommt. Vielmehr soll das Rechtsgut »Privatsphäre«, das durch das Computersystem als Tatobjekt gegenständlich repräsentiert wird, vor unbefugten Zugriffen geschützt werden. Wollte man den Gedanken der unterschiedlichen Schutzwürdigkeit der Daten tatsächlich in diesem Delikt zum Ausdruck bringen, so wäre mE eine Aufgliederung des Delikts in mehrere Deliktsfälle oder auch Qualifikationen mit entsprechend differenzierten Vorsatzanforderungen – dem Schutzniveau der Daten entsprechend – eindeutig sinnvoller.

Diese Unklarheit entsteht auch dadurch, dass in den GMat darauf verwiesen wird, dass sich die Formulierung dieser Absichtskombina-

534 Zu denken wäre etwa an das Ausspionieren von E-Mails, die sich nicht gerade am Übertragungsweg befinden, aber auf der Festplatte des Opfers abgespeichert sind (zB im Posteingang oder bei den gesendeten Objekten des lokalen E-Mail-Clientprogramms).

535 Zu § 119 siehe S 154 ff.

536 Beide Bestimmungen behandeln den »Inhalt von Nachrichten« als Bezugsobjekt des erweiterten Vorsatzes; darüber hinaus erfasst § 120 Abs 2a eine »Nachricht« auch als Tatobjekt.

537 Siehe ErlRV 1166 BlgNR XXI. GP, 24.

538 Siehe S 6.

tion an § 51 DSG 2000[539] sowie an § 121 Abs 2 orientiert hat.[540] Betrachtet man nun § 121 Abs 2 (aber auch § 122 Abs 2) genauer, so erkennt man in Abs 2 eine »Qualifikation« lediglich im Fall der Tatbegehung mit einem überschießenden Vorsatz, der im Stärkegrad der Absicht ua auf einen Vermögensvorteil[541] gerichtet sein muss. Diese überschießende Innentendenz findet aber im Grunddelikt keine Entsprechung. Es ist daher nicht zu verstehen, warum eine Gewinnabsicht – wenn auch alternativ zur Schädigungsabsicht – in § 118a Abs 1 bereits in den Grundtatbestand aufgenommen wurde.[542] Auch dieser Vergleich mit § 121 Abs 2 spricht für einen Qualifikationstatbestand hins einer Gewinnabsicht im Fall des § 118a. Doch selbst wenn man § 51 DSG 2000 aF in diesem Zusammenhang analysiert, muss angemerkt werden, dass dieser zunächst eine Bestimmung des Nebenstrafrechts darstellt, die einem eigenständigen Sachgesetz mit einer sondergesetzlichen Wertentscheidung und Begrifflichkeit zugeordnet ist. Daraus folgt, dass hier besondere Merkmale und Maßstäbe einer rechtlich zu erfassenden Spezialmaterie vorliegen, die auch angesichts eigenständiger kriminalpolitischer Überlegungen und spezieller Sachterminologie gewisse Differenzierungen zum Kernstrafrecht zulassen und sogar erfordern.

Dass sich der historische Gesetzgeber bei der Formulierung des § 118a ua an einem Spezialtatbestand des Datenschutzgesetzes orientiert haben dürfte[543], der als Zweck ausschließlich »personenbezogene Daten« unter entsprechenden Einschränkungen[544] schützt, erweist sich mE hins des Regelungszweckes des § 118a Abs 1 als wenig sachgerecht. Dies nicht zuletzt, weil § 51 DSG 2000 aF gerade auch im subjektiven Tatbestand diverse Unklarheiten enthält. So umfasst die vom Täter verlangte Bereicherungsabsicht auf der einen Seite lediglich die Verschaffung

539 Gemeint war § 51 Abs 1 DSG 2000 idF I 165/1999, also vor der DSG-Nov 2010.

540 Vgl ErlRV 1166 BlgNR XXI. GP, 24 f.

541 Die Qualifikation enthält keinen über das Grunddelikt hinausreichenden (objektiven) Qualifikationstatbestand (siehe *Lewisch* in WK² § 121 Rz 16 [Stand September 2008]).

542 Ebenso *Seling,* Privatsphäre, 80.

543 Vgl ErlRV 1166 BlgNR XXI. GP, 24 f.

544 ZB das Vorliegen eines schutzwürdigen Geheimhaltungsinteresses und die Einschränkung des Tatobjekts auf ausschließlich personenbezogene Daten, die auf Grund einer berufsmäßigen Beschäftigung anvertraut oder zugänglich geworden sind oder die widerrechtlich verschafft wurden.

eines Vermögensvorteils[545] zu dessen Gunsten, und nicht auch etwa die Vermögensvermehrung eines anderen, was vermutlich jedoch auf ein Redaktionsversehen zurückgeht[546], das nunmehr in der Fassung nach der DSG-Nov 2010 – jedoch ohne entsprechenden Hinweis darauf – behoben wurde. Interessant ist allerdings die diesbezügliche Anmerkung in den GMat, dass man die Formulierung des Bereicherungsvorsatzes des § 51 DSG 2000 (idgF) terminologisch dem StGB angleichen will.[547] Dabei wird in den GMat ausdrücklich – mE jedoch völlig unverständlich – in einer beispielhaften Aufzählung auf die Bestimmungen des § 129 (Diebstahl mit Einbruch oder Waffen) und § 146 (Betrug) verwiesen.[548] Daraus ergibt sich aber ein nicht schlüssiger Zirkelverweis aus den GMat[549] zu § 118a und § 51 DSG 2000, selbst wenn man auf andere korrespondierende Bestimmungen des Kernstrafrechts, zB auf §§ 118a, 119a, Bezug nimmt. Orientierte sich offenbar der historische Gesetzgeber ursprünglich noch – im Zuge der Normierung des § 118a – aufgrund von Ähnlichkeiten im Regelungszweck hins des Gewinn- und Schädigungsvorsatzes ua an § 51 DSG 2000 aF, so sieht er mit der DSG-Nov 2010 die Notwendigkeit gegeben, § 51 DSG 2000 terminologisch wiederum an das StGB anzugleichen. Es ist nicht klar, wie diese Aussage gewertet werden soll, da eben gerade iZm der Frage nach einer »unrechtmäßigen« Bereicherung insb bei »Geheimnisschutzdelikten« ebenfalls Bestimmungen im StGB existieren, die diese Unrechtmäßigkeit nicht erfordern (wie bspw §§ 118a Abs 1, 119a Abs 1, 121 Abs 2, 122 Abs 2). Man wird sich folglich nicht darauf verlassen können, dass mit der Aussage in den GMat, § 51 DSG 2000 aF terminologisch an das StGB anpassen zu wollen, in erster Linie die Konkretisierung des subjektiven Tatbestands um eine unrechtmäßige Bereicherung gemeint war.

---

545 Unter einem Vermögensvorteil versteht man jede Vergrößerung der Aktiven oder Verringerung der Passiven (siehe statt vieler *Kirchbacher* in WK² § 146 Rz 120 [Stand September 2011]).

546 Eine gegenteilige Auslegung dieses erweiterten Vorsatzes, dh iS einer Vermögensvermehrung auch zu Gunsten eines anderen, war jedoch aufgrund des eindeutigen Wortlauts in § 51 DSG 2000 aF nicht zulässig (siehe *Hinterhofer,* Geheimnisschutz – Datenschutz – Informationsschutz im Strafrecht, in Studiengesellschaft für Wirtschaft und Recht (Hrsg), Geheimnisschutz – Datenschutz – Informationsschutz [2008] 169 [188]).

547 Siehe ErlRV 472 BlgNR XXIV. GP, 21.

548 Siehe dazu *Bergauer* in Jahnel, Jahrbuch 2010, 73 (74).

549 ErlRV 1166 BlgNR XXI. GP, 24 und ErlRV 472 BlgNR XXIV. GP, 21.

b. Bereicherungsabsicht

In Betrachtung der Bereicherungsabsicht des § 118a Abs 1 fällt *Seling* auf, dass die Unrechtmäßigkeit der Vermögensvermehrung nicht tatbildlich ist.[550] Unrechtmäßig ist eine angestrebte Bereicherung dann, wenn der Täter keinen Anspruch darauf hat oder zu haben glaubt.[551] Dadurch wäre auch eine vom Täter gewollte rechtmäßige Bereicherung vom subjektiven Tatbestand erfasst, was doch ungewöhnlich erschiene. *Seling* bezweifelt daher die Gleichwertigkeit von Gewinn- und Schädigungsvorsatz und schlägt vor, die Gewinnabsicht ersatzlos zu streichen.[552]

Inzwischen hat der Gesetzgeber – wie bereits oben ausf erörtert – tatsächlich den subjektiven Tatbestand des § 51 DSG 2000 terminologisch an das StGB angepasst. Nunmehr enthält diese nebengesetzliche Strafbestimmung – anders als noch in der aF – expressis verbis auch die »unrechtmäßige Bereicherung« in ihrem Tatbestand.

Fraglich ist mE aber, ob das Erfordernis der Unrechtmäßigkeit der Bereicherung im erweiterten Vorsatz des § 118a Abs 1 – wie es *Seling* verlangt – überhaupt notwendig erscheint. Zum einen zeugt bereits die Kombination der unterschiedlichen überschießenden Innentendenzen von sehr hoch angelegten Strafbarkeitsvoraussetzungen, weshalb die Strafbarkeit nicht auch noch durch die Konkretisierung der Gewinnabsicht durch das normative Tatbestandsmerkmal »unrechtmäßig« (arg »unrechtmäßige Bereicherung)« weiter eingeschränkt werden sollte. Und zum anderen ist der Schutz der Privatsphäre (siehe den angesprochenen Vergleich mit dem »virtuellen Hausrecht«) und nicht der Schutz des Vermögens der Zweck dieser Bestimmung. Der Gesetzgeber erfasst die von ihm als gerade noch strafwürdig angesehene Intention eines Täters iZm einer objektiven gegen die Rechtsordnung verstoßenden Handlung im jeweiligen Delikt, sodass jeweils auch unter Bezugnahme auf das dahinterstehende Rechtsgut unterschiedliche Anforderungen in den subjektiven Tatbeständen – den Regelungszwecken entsprechend – gerechtfertigt und notwendig sind. So ist mE der Ver-

---

550 Siehe *Seling,* Privatsphäre, 81 unter Bezugnahme auf *Hinterhofer,* Geheimnisschutz, 187 zu § 51 Abs 1 DSG 2000 aF und § 101 Abs 1 BWG.

551 Siehe zB zum Betrug *Kirchbacher* in WK² § 146 Rz 121 mwN; zum Diebstahl *Bertel* in WK² § 127 Rz 38 (Stand Dezember 2008); zur Veruntreuung *Kienapfel,* Grundriß des österreichischen Strafrechts. Besonderer Teil II³ (1993) § 133 Rz 85 mwN.

552 Vgl *Seling,* Privatsphäre, 81 f.

gleich der subjektiven Anforderungen an die Tat mit Vermögensdelikten – wie zB § 146 – gar nicht sachgerecht, weil die Unrechtmäßigkeit der anvisierten Bereicherung dort regelmäßig als Unrechtsmäßigkeitskorrektiv (zum Erfolg der äußeren Tatseite) eingesetzt wird.

Im Übrigen ist die Formulierung einer überschießenden Innentendenz bezogen auf eine Bereicherung im Sinne eines Vermögensvorteils, der nicht auch unrechtmäßig sein muss, in den Tatbeständen zum Schutz von Geheimnissen durchaus systemkonform (siehe dazu im Kernstrafrecht § 121 Abs 2, § 122 Abs 2, aber insb auch § 101 Abs 1 BWG[553], § 27 Abs 3 BHAG-G[554], § 28 E-Geldgesetz 2010[555], § 252 Abs 2 FinStrG[556], § 9 InfoSiG[557], § 94 Abs 3 WAG 2007[558] oder § 66 Abs 2 ZaDiG[559]). Eine objektive Geheimnisverletzung allein reicht in all diesen Fällen einer Geheimnisverletzung für die Strafbarkeit nicht aus, vielmehr muss ein – je nach Bestimmung entsprechend graduierter – Bereicherungs- oder Schädigungsvorsatz hinzutreten.[560] Auch findet man vergleichbare Formulierungen bspw bei den Delikten gegen Ehe und Familie (§ 194 Abs 2[561]) oder gegen die sexuelle Integrität und Selbstbestimmung (§ 213 Abs 2[562], § 214 Abs 2[563], § 215a Abs 1[564]). Hingegen wird lediglich bei zentralen Vermögens- bzw Bereicherungsdelikten (wie zB §§ 127, 132, 134, 142, 144, 146, 148a) aber auch bei diversen Delikten zum Schutz unbarer Zahlungsmittel (§ 241e Abs 1[565], § 241f[566]) die »unrechtmäßige Bereicherung«[567] verlangt. Diese Betrachtung verdeutlicht, dass die Textierung eines erweiterten Vorsatzes eine Vermögensvermehrung betreffend, die nicht ausschließlich auf eine unrecht-

553 Bankwesengesetz, BGBl 532/1993 idF I 69/2015.
554 Buchhaltungsagenturgesetz, BGBl I 37/2004 idF I 183/2013.
555 E-Geldgesetz 2010, BGBl I 107/2010 idF I 68/2015.
556 Finanzstrafgesetz, BGBl 129/1958 idF I 105/2014.
557 Informationssicherheitsgesetz, BGBl I 23/2002 idF I 10/2006.
558 Wertpapieraufsichtsgesetz 2007, BGBl I 60/2007 idF I 69/2015.
559 Zahlungsdienstegesetz, BGBl I 66/2009 idF I 68/2015.
560 Siehe auch § 51 DSG 2000, wo auf subjektiver Tatseite entweder ein Bereicherungsvorsatz oder eine Schädigungsabsicht bezüglich des Geheimhaltungsanspruchs des Betroffenen vorliegen muss.
561 Verbotene Adoptionsvermittlung.
562 Kuppelei.
563 Entgeltliche Vermittlung von Sexualkontakten mit Minderjährigen.
564 Förderung der Prostitution und pornographischer Darbietungen Minderjähriger.
565 Entfremdung unbarer Zahlungsmittel.
566 Annahme, Weitergabe oder Besitz entfremdeter unbarer Zahlungsmittel.
567 Jedoch genügt bei den Bereicherungsdelikten idR zumindest dolus eventualis (§ 5 Abs 1 zweiter HS), Absicht (§ 5 Abs 2) ist nicht gefordert.

mäßige Bereicherung abstellt, außerhalb des Vermögensstrafrechts nichts Ungewöhnliches ist. Angesichts der hinter diesen Delikten stehenden und zu schützenden Rechtsgüter ist dies auch nachvollziehbar und sachgerecht, weshalb mE der diesbezüglichen Argumentation[568] nicht zu folgen ist. Das Erfordernis, dass der Bereicherte daher keinen Anspruch auf die Vermehrung seines Vermögens haben darf, ist gerade im hier gegenständlichen Zusammenhang (mit dem Schutz unkörperlicher Informationen bzw Geheimnisse) wohl vernachlässigbar.

Aber auch die von *Seling*[569] aufgeworfene Frage nach der Gleichwertigkeit der Vorsatzalternativen der »Bereicherungs-« und »Schädigungsabsicht« ist mE nur von geringer Relevanz. *Seling* ist dabei zwar zu konzedieren, dass für sich allein genommen das Bestreben, sich »rechtmäßig« zu bereichern, keinen adäquaten Unrechtsgehalt zur Vorsatzalternative »des Einem-anderen-einen-Nachteilzufügens« besitzt. So fehlt es bei einem Vorsatz, sich oder einem anderen einen (rechtmäßigen) Vermögensvorteil zuzuwenden, an einem sozial inadäquaten Element. Gerade im Bereich der Delikte zum Schutz der Privatsphäre oder von Geheimnissen wäre die Realisierung einer Bereicherung auch ohne eine korrelierende Vermögensschädigung des Opfers denkbar. Anders als bei der widerrechtlichen Zueignung einer vermögenswerten körperlichen Sache ist mit einer »bloßen« Kenntnisverschaffung von (unkörperlichen) Daten aber noch keine Vermögensverschiebung verbunden, weshalb der Berechtigte dadurch (noch) nicht in seinem Vermögen geschädigt wird. Im Gegensatz zu den klassischen Vermögens- bzw Bereicherungsdelikten (wie zB § 146) stellt daher in concreto die angestrebte Bereicherung nicht das Korrelat zur Schadenszufügung dar. Die Absicht einer – insb auch rechtmäßigen – Bereicherung kann nicht als die Kehrseite des dem Opfer entstandenen Vermögensnachteils gesehen werden, zumal es beim Ausspionieren und auch bei der Verwendung von Daten nicht zwangsläufig auch zu einem (Vermögens-)Nachteil[570] des Opfers kommt.

Aber eine solche unrechtsbezogene Gleichwertigkeit der Vorsatzalternativen ist im gegenständlichen Fall gar nicht notwendig. Den GMat

568 Vgl *Seling,* Privatsphäre, 81; weiters *Hinterhofer,* Geheimnisschutz, 187.

569 Siehe *Seling,* Privatsphäre, 81.

570 Da für die im Computersystem gespeicherten Daten gem § 118a Abs 1 keine Geheimhaltungsinteressen bestehen müssen, muss nicht auch eine unberechtigte Verwendung, wie zB eine Veröffentlichung, gleichsam einen Nachteil bedeuten.

zufolge wollte man doch schließlich nur zur – auf äußerer Tatseite als sozial inadäquat qualifizierten – widerrechtlichen Zugangsverschaffung zum fremden Computersystem zusätzliche subjektive »strafbarkeitseinschränkende Elemente« in unterschiedlicher Ausgestaltung verankern.[571] Das bloße Geschehen in der Außenwelt muss daher von einer darüber hinausgehenden subjektiven Zielrichtung des Täters getragen sein.[572] Das in objektiver Hinsicht sozial inadäquate Verhalten des Täters, muss – um gerichtliche Strafbarkeit begründen zu können – mit überschießenden Innentendenzen des Täters ausgeführt worden sein. Es geht daher nicht um die tatsächliche Bereicherung iSd Vermögensstrafrechts, weshalb seitens des Gesetzgebers vermutlich auch nicht auf die diesbezüglichen Formulierungen der einschlägigen Bereicherungsdelikten zurückgegriffen wurde, sondern um die Abbildung missbilligter Absichten in verschiedene unrechtsthematische Richtungen, die erst kumulativ mit dem objektiven Tatbestand das strafrechtliche Unrecht dieser Tat ausmachen.

In diesem Sinn kann daher argumentiert werden, dass eine »Datenspionageabsicht« deshalb verlangt wird, um den erhöhten Anforderungen für besonders geschützte Daten (zB Nachrichten[573]) und dem Schutz der Privatsphäre gerecht zu werden. Kumulativ dazu[574] muss durch die Datenverwendung entweder eine Schädigungsabsicht (arg »einem anderen einen Nachteil zufügen«) oder eine Bereicherungsabsicht hinzutreten, die einen weiterführenden – lediglich in der Vorstellung des Täters zu konstatierenden – Sachverhalt in Bezug auf die vermögensorientierte Verwendung von widerrechtlich erlangten Daten beschreibt, ohne aber auf diverse damit verbundene Vermögensverschiebungsabsichten[575] abzustellen. Es spielt dafür deliktsspezifisch keine Rolle, ob sich der Täter rechtmäßig oder unrechtmäßig bereichern will. Ob diese Absicht daher eine rechtmäßige oder unrechtmäßige Bereicherung beinhaltet, ist schon deshalb irrelevant, weil es eben darauf ankommt, dass der Täter sich die hierfür zu verwendenden Daten widerrechtlich verschaffen will

571 Vgl die Erwägungen zum »dishonest intent« ErlRV 1166 BlgNR XXI. GP, 24.

572 Siehe zum erweiterten Vorsatz allgemein statt vieler *Kienapfel/Höpfel/Kert,* AT[14] Z 11 Rz 23 ff.

573 Reicht die bloße Spionageabsicht – dh ohne Bereicherungs- bzw Schädigungsabsicht – aus, kann man von reinen Indiskretionsdelikten sprechen (siehe *Hinterhofer,* Geheimnisschutz, 187 mwN).

574 Wohl um ein zu weitreichendes Kriminalisierungspotenzial abzufangen.

575 Man denke dabei an das verlustfreie Vervielfältigen von (unkörperlichen) Daten.

und keine Verfügungsberechtigung über die Daten hat. Wäre der Täter dazu berechtigt, entfiele nämlich bereits der objektive Tatbestand.

Insgesamt führen meiner Meinung nach die strengen Kriterien der objektiven Tatbestandsmerkmale iVm den hohen Absichtsanforderungen der subjektiven Tatseite zu einer gravierenden Minderanwendbarkeit[576] dieser Norm.[577] Das scheint keinesfalls sachgerecht.

9. Sonstiges

§ 118a Abs 3 sieht eine Deliktsqualifikation vor, wenn die Tat als Mitglied einer kriminellen Vereinigung (§ 278 Abs 2) begangen wird. In einem solchen Fall ist mit Freiheitsstrafe bis zu drei Jahren zu bestrafen.

§ 118a Abs 2 konzipiert sämtliche strafbaren Handlungen nach § 118a als Ermächtigungsdelikte iSd § 92 StPO.

Gem § 30 Abs 1 StPO fällt das Grunddelikt des § 118a Abs 1 in die sachliche Zuständigkeit des Bezirksgerichts, die Deliktsqualifikation des § 118a Abs 3 fällt gem § 31 Abs 4 Z 1 StPO in die sachliche Zuständigkeit des Einzelrichters am Landesgericht.

B. Die nebenstrafrechtliche Bestimmung des § 51 DSG 2000

> § 51 Wer mit dem Vorsatz, sich oder einen Dritten dadurch unrechtmäßig zu bereichern, oder mit der Absicht, einen anderen dadurch in seinem von § 1 Abs. 1 gewährleisteten Anspruch zu schädigen, personenbezogene Daten, die ihm ausschließlich auf Grund seiner berufsmäßigen Beschäftigung anvertraut oder zugänglich geworden sind oder die er sich widerrechtlich verschafft hat, selbst benützt, einem anderen zugänglich macht oder veröffentlicht, obwohl der Betroffene an diesen Daten ein schutzwürdiges Geheimhaltungsinteresse hat, ist, wenn die Tat nicht nach einer anderen Bestimmung mit strengerer Strafe bedroht ist, vom Gericht mit Freiheitsstrafe bis zu einem Jahr zu bestrafen.[578]

576 *Salimi* spricht von unüberwindbaren subjektiven Hürden (vgl *Salimi,* ÖJZ 2012/115, 998); vgl auch in diese Richtung *Reindl* in BMJ, Vorarlberger Tage 2003, 63 (79).

577 Siehe bereits *Bergauer,* RdW 2006/391, 412.

578 BGBl I 165/1999 idF I 133/2009.

Das von § 51 DSG 2000 geschützte Rechtsgut besteht in erster Linie[579] in der aus dem Rechtsgut der Privatsphäre stammenden »informationellen Selbstbestimmung«[580], die auf dem Interesse des Betroffenen an der Geheimhaltung oder alleinigen Verwendung seiner schützenswerten personenbezogenen Daten aufbaut.[581] Vor allem durch die unbefugte Datenverwendung durch Dritte wird dieses Rechtsgut beeinträchtigt. Anders als das Grundrecht auf Geheimhaltung des § 1 Abs 1 DSG 2000 selbst[582] stellt die Strafbestimmung des § 51 DSG 2000 nicht schon auf die rechtswidrige Ermittlung der Daten ab, sondern erst auf die anschließende Verwendung[583] – welche allerdings mit dem Ermittlungsvorgang zusammenfallen kann.[584]

Die einzige gerichtliche Strafbestimmung des DSG 2000 wurde durch die DSG-Nov 2010[585] in mehrfacher Hinsicht modifiziert.[586] Die Definition des subjektiven Tatbestandes wurde dabei derart abgeändert, dass über den erweiterten Vorsatz ein interessantes Mischdelikt entstanden ist, da neben einem Bereicherungsvorsatz auch die »bloße« Schädigungsabsicht bezüglich des Geheimhaltungsanspruchs nach § 1 Abs 1 DSG 2000 berücksichtigt wurde. Durch diese alternative Zusammenführung verschiedener subjektiver Unrechtsmerkmale, besitzt § 51 DSG 2000 sowohl Relevanz für vermögensrechtliche Bereicherungen als auch für beabsichtigte Verletzungen des Geheimhaltungsrechts. Man könnte insofern von einem »Kombinationsdelikt« sprechen, da die Un-

579 Zu einem gewissen Maß ist § 51 DSG 2000 auch ein Vermögensdelikt (siehe gleich im Anschluss).

580 Der Begriff stammt ursprünglich aus Deutschland und wird dort als eine Ausprägung des allgemeinen Persönlichkeitsrechts (iSd Art 2 Abs 1 GG iVm Art 1 Abs 1 GG) verstanden. Das informationelle Selbstbestimmungsrecht wurde 1983 vom deutschen Bundesverfassungsgericht im sog »Volkszählungsurteil« (BVerfG 15.12.1983, 1 BvR 209/83 ua) als Grundrecht anerkannt.

581 Siehe dazu auch *Triffterer* in SbgK § 126a Rz 39 (aF Stand Dezember 1992).

582 Siehe allgemein zum Ermittlungsschutz des Grundrechts auf Geheimhaltung (§ 1 Abs 1 DSG 2000) *Wiederin,* Privatsphäre und Überwachungsstaat (2003) 62; weiters *Jahnel,* Handbuch Rz 2/15 mwN; ErlRV 72 BlgNR XIV. GP, 21; siehe auch VfSlg 12.228/1989, 12.880/1991, 16.369/2001; weiters DSK 05.04.2002, K120.766/004-DSK/2002.

583 Siehe auch *Reindl-Krauskopf,* Strafrechtliche Aspekte der Datenverwendung, in Brodil (Hrsg), Datenschutz im Arbeitsrecht. Mitarbeiterüberwachung versus Qualitätskontrolle (2010) 73 (74); weiters *Bergauer,* Der Handel mit Patientendaten – eine (datenschutzrechtliche) Straftat?, ÖJZ 2013/113, 958.

584 Mehr dazu unten (S 132 ff).

585 BGBl I 133/2009.

586 Siehe dazu ausf *Bergauer* in Jahnel, Jahrbuch 2010, 73 (73 ff).

rechtsmerkmale der überschießenden Innentendenzen eine Bereicherungsintention[587] (iS eines Vermögensdelikts) mit einer (alternativen) Indiskretionsabsicht in »einer« formal ausgewiesenen Strafbestimmung zusammenführen. Auffällig ist, dass die Bereicherungstendenz schwerer wiegt, weil eine Tatbestandsmäßigkeit über diese subjektive Alternative des Bereicherungsvorhabens (1. DF) bereits bei einem bedingten Vorsatz hergestellt ist. Die (erweiterte) Vorsatzalternative, welche auf Verletzung des Geheimhaltungsrechts gerichtet sein muss (2. DF), erfordert hingegen das höchstmögliche Maß an Vorsatz, nämlich die Absicht iSd § 5 Abs 2. Der soziale Sinngehalt der beiden Vorsatzziele ist ebenso wie die unterschiedlichen Vorsatzgraduierungen, nicht als rechtlich gleichwertig einzustufen. Im Übrigen stimmen auch die – zwar für die formelle Vollendung unbeachtlichen – »materiellen Beendigungszeitpunkte«, wie sich gleich im Anschluss bei der »Deliktstypisierung unter Einbeziehung der überschießenden Innentendenzen« zeigen wird – nicht überein. § 51 DSG 2000 enthält somit zwei selbstständige, untereinander nicht austauschbare Deliktsfälle über die konkrete Berücksichtigung des jeweiligen erweiterten Vorsatzes, die diese Strafbestimmung – bezogen auf die subjektive Tatseite – als kumulatives Mischdelikt begreifen lässt. Offensichtlich wurden zwei Deliktsfälle nur aus gesetzestechnischen Gründen unter einer einzigen Bezeichnung und mit derselben Strafdrohung zusammengefasst. Bei der Deliktsgestaltung wäre mE eine Struktur, wie sie § 241e Abs 1 durch Satz 1 und Satz 2 besitzt, zu bevorzugen. Dort wurden ebenfalls zwei Deliktsfälle, die sich lediglich über die jeweilige überschießende Innentendenz voneinander abgrenzen, in einem Absatz – jedoch in zwei getrennten Sätzen – bei gleicher Strafdrohung zusammengefasst. Doch auch die gemeinsame Strafdrohung dieser beiden selbstständigen Deliktsfälle des § 51 DSG 2000, ist mE unangemessen. Folglich sollten die Taten den unterschiedlichen Unrechtsintensitäten der überschießenden Innentendenzen entsprechend sanktioniert werden. So wäre etwa denkbar, die Strafdrohung des Deliktsfalls mit der (bloßen) Schädigungsabsicht hins des Geheimhaltungsrecht auf eine Freiheitsstrafe von bis zu 6 Monaten zu reduzieren und den anderen Deliktsfall mit dem bisherigen Strafsatz – Freiheitsstrafe bis zu einem Jahr – zu belassen.

587 § 51 DSG 2000 ist allerdings nicht als (reines) Vermögensdelikt zu sehen, obwohl der Gesetzgeber durch die Bereicherungsintention den personenbezogenen Daten mittelbar einen Vermögenswert zuspricht.

Zusammenfassend ist die innere Tatseite des § 51 DSG 2000 erfüllt, wenn zum (zumindest bedingten) Tatbildvorsatz[588] entweder ein (erweiterter) Bereicherungsvorsatz (ebenfalls zumindest dolus eventualis) hinzukommt oder wenn der Täter im erweiterten Vorsatz mit der Absicht (iSd § 5 Abs 2) handelt, einen anderen in seinem von § 1 Abs 1 DSG 2000 gewährleisteten Anspruch zu schädigen. Bei dieser zweiten Vorsatzalternative der Schädigungsabsicht muss es dem Täter gerade auf die Verletzung des Geheimhaltungsanspruchs des Betroffenen nach § 1 Abs 1 DSG 2000 ankommen. Durch den Entfall der Formulierung »Wer in der Absicht, sich einen Vermögensvorteil zu verschaffen oder einem anderen einen Nachteil zuzufügen« der aF des subjektiven Tatbestands stellt der Gesetzgeber in der geltenden Fassung klar, dass die Absicht jemandem »bloß« einen Nachteil zuzufügen, nicht mehr tatbildlich ist. Vielmehr wird dieser »Nachteil« nun auf die Verletzung des Geheimhaltungsrechts konkretisiert. Handelt daher jemand objektiv tatbildlich und mit entsprechendem Vorsatz, einem anderen einen Vermögensschaden zuzufügen, ohne sich jedoch selbst oder einen anderen bereichern zu wollen, ist § 51 DSG 2000 nicht anwendbar, sofern der Täter nicht mit Schädigungsabsicht hins des Geheimhaltungsanspruchs gehandelt hat.

Der neu formulierte Bereicherungsvorsatz wurde der Terminologie des Kernstrafrechts angepasst, wobei in den GMat beispielhaft auf die Bestimmungen des § 129 (Diebstahl mit Einbruch oder Waffen) und § 146 (Betrug) Bezug genommen wird.[589] Dieser Verweis ist aber nicht nachvollziehbar, da de facto die konkrete Bestimmung eher mit § 118a (Widerrechtlicher Zugriff auf ein Computersystem) bzw § 119a (Missbräuchliches Abfangen von Daten) korrespondiert. Eine Ausrichtung an Vermögens- bzw Bereicherungsdelikten ist mE verfehlt, schützt doch § 51 DSG 2000, welcher im spezifischen Sachgesetz des Datenschutzgesetzes eingebettet ist, vor allem den Geheimhaltungsanspruch und die Selbstbestimmung bezüglich personenbezogener Daten. Eine Anlehnung an diverse Indiskretionsdelikte wäre daher – trotz Nähe der ersten überschießenden Innentendenz zum Vermögensstrafrecht – zutreffender. Darüber hinaus ist es außerhalb der zentralen Vermögens- bzw Bereicherungsdelikte – wie oben bereits

588 Das ergibt sich auch für das Nebenstrafrecht idR aus § 7 Abs 1 StGB.
589 Vgl ErlRV 472 BlgNR XXIV. GP, 21.

ausgeführt[590] – eher unüblich, auf eine »unrechtmäßige« Bereicherung abzustellen, da ein Erfordernis in die Richtung, dass der Bereicherte keinen Anspruch auf die Vermehrung seines Vermögens haben darf, gerade im hier gegenständlichen Zusammenhang vernachlässigbar ist. Die besonders verwerfliche »Gewinn(erzielungs)absicht«[591] – wie sie auch in der Deliktsbezeichnung zu finden ist – stellt auf die reine innere Einstellung des Täters ab und nicht auf sein äußeres Verhalten, das im Wesentlichen die »rechtswidrige Datenverwendung« in Anlehnung an das zu schützende deliktsspezifische Rechtsgut als sozial inadäquates Element abstrakt abbildet. Daher sei auch zur Deliktsbezeichnung noch angemerkt, dass diese wohl besser in die Richtung »Datenverwendungsmissbrauch« lauten sollte, um das sozial inadäquate Verhalten, das durch diesen Deliktstypus erfasst wird, transparenter zu machen.

1. Deliktstypisierung und überschießende Innentendenzen

Die Typisierung des § 51 DSG 2000 fällt kompliziert aus, da die äußere Betrachtung der Tathandlungen selbst und diese wiederum in Verbindung zur entsprechenden subj Absichtsanforderung unterschiedliche Deliktstypen indizieren. Bezieht man nämlich die Inhalte der überschießenden Innentendenzen als fiktive Erfolge in die Betrachtungen mit ein, so weist die Tathandlung des »Selbst-Benützens«[592] iVm der subjektiven Alternative des Bereicherungsvorsatzes darauf hin, dass § 51 erster Fall erste subj Alt DSG 2000 ein kupiertes Erfolgsdelikt (= Absichtsdelikt iwS[593]) darstellt.[594] Der Eintritt der Bereicherung beschreibt einen über den objektiven Tatbestand hinausreichenden vom Täter (bloß) gewünschten Erfolg als Endziel. Die Erreichung des Endziels ist aber nicht (mehr) tatbestandsmäßig. Der Täter hat auf äußerer Tatseite alles getan, um das geplante Endziel zu erreichen. Mit dieser Konzeption wird der formelle Vollendungszeitpunkt auf die äußere

590 Siehe S 113 ff.
591 Vgl ErlRV 1613 BlgNR XX. GP, 54.
592 Prinzipiell handelt es sich dabei um eine schlichte Tätigkeit, die keinen Erfolg verlangt (siehe *Salimi* in WK² DSG § 51 Rz 9 [Stand Mai 2012]).
593 Da es sich bezüglich des Stärkegrades der überschießenden Innentendenz iZm dieser subj Alternative nur um zumindest dolus eventualis handeln muss.
594 Vgl aber *Salimi* in WK² DSG § 51 Rz 9, der idZ von einem schlichten Tätigkeitsdelikt ausgeht.

Tathandlung (mit dem Ziel einer Bereicherung) vorverlagert.[595] Mit anderen Worten ist das sozial inadäquate Verhalten in § 51 DSG 2000 schon in der rechtswidrigen Verwendung schutzwürdiger personenbezogener Daten zu sehen, worauf sich auch der (zumindest bedingte) Tatbildvorsatz erstrecken muss. Es mangelt folglich dem objektiven Tatbestand an einer generellen sozial inadäquaten Verhaltensbeschreibung. Daher fehlt eine hinreichende Abgrenzung zwischen strafwürdigem und straffreiem Verhalten in der äußeren Beschreibung der Tat.

Im Zeitpunkt jeder Datenverwendung wird bereits in die grundrechtlich geschützte Interessensphäre des Betroffenen nach § 1 Abs 1 DSG 2000 eingegriffen. Gerichtlich strafbar wird dieser Eingriff aber erst, wenn noch zumindest eine der geforderten erweiterten Vorsatzanforderung zum objektiven Verhalten als weiteres Unrechtselement hinzutritt. Für das strafrechtliche Unrecht – im Gegensatz zum datenschutzrechtlichen – ist somit lediglich der Inhalt des konkreten Vorsatzes ausschlaggebend. Im Grunde genommen liegt in Anbetracht der tatsächlichen Rechtsgutbeeinträchtigung eine »Rückverlagerung« der Strafbarkeit vor, die darüber hinaus auch nur bei entsprechender Innentendenz des Täters grundsätzlich begründet wird.

Dass sich das Unrecht der Tat ausschließlich erst durch die Verbindung mit den tatsächlichen Innentendenzen (bzw überhaupt erst auf Rechtswidrigkeitsebene) ergibt, wird im Übrigen auch iZm § 148a thematisiert und kritisiert.[596] Daher wird an dieser Stelle bloß erneut darauf hingewiesen, dass der Gesetzgeber angehalten ist, die Formulierung von objektiven Tatbeständen ohne sozial inadäquate Merkmale zu vermeiden.

Die zweite Vorsatzalternative bezüglich der Schädigungsabsicht hins des Geheimhaltungsanspruchs schutzwürdiger personenbezogener Daten eines anderen unterscheidet sich deutlich von der Bereicherungsalternative. Da bereits mit rechtswidriger Datenverwendung der Anspruch auf Geheimhaltung verletzt ist, liegt dann, wenn es dem Täter geradezu darauf ankommt (iSd § 5 Abs 2), mit dieser Datenverwendung (verbis »dadurch« iSd Selbst-Benützens, Zugänglichmachens oder Veröffentlichens) den Betroffenen in seinem Geheimhaltungsanspruch zu schädigen, schon die strafrechtliche Rechtswidrigkeit in den

595 Vgl *Bergauer/Thiele,* Rezension zu *Farsam Salimi* in WK² DSG § 51. Auszug aus *Höpfel/Ratz* (Hrsg), Wiener Kommentar zum Strafgesetzbuch, jusIT 2012/74, 158.

596 Siehe S 364 f.

einzelnen Tathandlungen selbst vor.[597] Die Verwirklichung der äußeren Tatseite wird idR mit der Realisierung des Inhalts des erweiterten Vorsatzes in Form der angestrebten Schädigung zeitlich zusammenfallen. Folglich fällt bei dieser Vorsatzvariante zum einen das strafrechtliche Unrecht stets mit dem datenschutzrechtlichen zusammen und zum anderen wird die Tat regelmäßig zeitgleich formell vollendet und materiell beendet, was wohl bei der Bereicherungsalternative idR nicht der Fall sein dürfte.

Da bei dieser zweiten subj Alternative der Enderfolg (hier: Schädigung des Geheimhaltungsanspruchs) ohne weiteres Zutun eintreten soll, liegt auch in diesem Fall ein kupiertes Erfolgsdelikt (= Absichtsdelikt ieS) vor. Die über den Tatbildvorsatz, der sich auf sämtliche objektiven Tatbestandsmerkmale zumindest in Form eines dolus eventualis beziehen muss, hinausreichende zusätzliche Absichtsanforderung[598], den Geheimhaltungsanspruch zu verletzen, stellt einen quantitativen Wollenszuwachs dar, der das vom Täter anvisierte Endziel repräsentiert, das in seiner Vorstellung ohne weiteres Zutun erreicht werden soll. Mit anderen Worten, die (objektive) Tathandlung ist das Substrat mit dem der Inhalt des erweiterten Vorsatzes umgesetzt wird.

Verwirklicht man § 51 DSG 2000 durch die Begehungsweisen des Zugänglichmachens oder des Veröffentlichens, liegt tatbestandlich betrachtet aber bereits ein Erfolgsdelikt vor.[599] Da in beiden Fällen die Möglichkeit des Zugriffs auf die Daten für einen bestimmten Empfänger bzw unbestimmten Empfängerkreis tatbestandsmäßig ausreichend ist, führen beide Tathandlungen bloß eine »konkrete Gefährdung« des Rechtsguts herbei, die aber nach hM als Gefährdungserfolg für die Konstatierung eines Erfolgsdelikts genügt.[600] Versendet der Täter zB ein E-Mail mit berufsmäßig anvertrauten schutzwürdigen personenbezogenen Daten des Betroffenen an einen Dritten, so ist mit Zustellung der Nachricht (= Tathandlung des Zugänglichmachens) lediglich die konkrete Gefahr eingetreten, dass der Dritte das E-Mail mit den Daten lesen wird (= Gefährdungserfolg). Löscht der Empfänger das E-Mail, ohne es zu lesen, ist der Tatbestand erfüllt, ohne dass ein

597 Siehe dazu auch LG Salzburg 29.04.2011, 49 Bl 17/11v = jusIT 2011/89, 185 *(Thiele)*.

598 Im Sinne des § 5 Abs 2.

599 Siehe dazu auch *Salimi* in WK² DSG § 51 Rz 9 (Stand Mai 2012).

600 Vgl dazu auch *Bergauer,* OGH: Die üble Nachrede – ein Erfolgsdelikt?, jusIT 2012/26, 60; vgl weiters auch *Kienapfel/Schmoller,* Studienbuch Strafrecht. Besonderer Teil III² (2009) Vorbem §§ 169 ff Rz 16.

»Verletzungserfolg« eingetreten ist. Was die Einbeziehung der jeweiligen überschießenden Innentendenzen in diese Betrachtungen anlangt, so kann auf die obigen Ausführungen verwiesen werden.[601] Ähnliches gilt für die Veröffentlichung im Internet, denn auch dort besteht grundsätzlich lediglich die (konkrete) Gefahr, dass jemand die Daten wahrnimmt. Die Tatbestandsmäßigkeit wird aber bereits mit der bloßen Möglichkeit der Wahrnehmung durch Dritte hergestellt.

2. Tatsubjekt

Das Normtext einleitende »Wer« deutet grundsätzlich auf ein Allgemein- bzw Jedermannsdelikt hin, doch wird dies dadurch relativiert, dass nach dem Wortlaut des § 51 DSG 2000 nur personenbezogene Daten erfasst sind, die dem Täter ausschließlich auf Grund seiner berufsmäßigen Beschäftigung anvertraut oder zugänglich geworden sind oder die er sich widerrechtlich verschafft hat. Daten, die dem Täter außerhalb seiner berufsmäßigen Beschäftigung anvertraut oder zugänglich wurden, sind nicht deliktstauglich, sofern sie nicht widerrechtlich verschafft wurden.[602] § 51 DSG 2000 ist daher in Bezug auf die Modalitäten iZm der berufsmäßigen Beschäftigung als ein echtes Sonderdelikt zu verstehen.[603] Hinsichtlich »widerrechtlich verschaffter« Daten ist § 51 DSG 2000 ein Allgemeindelikt.[604] Die Ansicht des OGH[605], dass durch die Einschränkung des Begriffs »Betroffener« auf vom Auftraggeber verschiedene Personen (vgl § 4 Z 3 DSG 2000) die personenbezogenen Daten des Auftraggebers selbst aus dem strafrechtlichen Schutz, wie etwa gegenüber seinem eigenen Dienstleister, ausgeklammert wären, ist differenziert zu betrachten.

---

601 Auf die überschießenden Innentendenzen bezogen stellt § 51 DSG 2000 daher stets ein »kupiertes Erfolgsdelikt« dar.

602 Vgl auch *Hinterhofer,* Geheimnisschutz, 183.

603 Anders noch § 48 Abs 1 DSG 1978 (BGBl 565/1978, außer Kraft getreten mit BGBl I 165/1999), wo es sich ausschließlich um ein echtes Sonderdelikt gehandelt hatte, da davon nur personenbezogene Daten erfasst waren, die dem Täter »ausschließlich kraft seiner berufsmäßigen Beschäftigung mit Aufgaben der Verarbeitung anvertraut worden oder zugänglich geworden sind«.

604 Vgl *Bergauer,* ÖJZ 2013/113, 958; Mehr dazu gleich im Anschluss.

605 Vgl als obiter dictum in OGH 05.04.1991, 16 Os 6/91 (16 Os 7/91), allerdings in concreto noch zu § 48 Abs 1 DSG 1978 (BGBl 565/1978, außer Kraft getreten mit BGBl I 165/1999).

Zum einen ist diese Schlussfolgerung in Bezug auf die datenschutzrechtliche Rollenverteilung unzutreffend. Richtig ist vielmehr, dass die Verarbeitung eigener personenbezogener Daten solange datenschutzrechtlich irrelevant ist, wie kein Dritter hins dieser Datenverwendung in Erscheinung tritt.[606] So dürfte dies auch der (historische) Gesetzgeber sehen, wenn in den GMat ausgeführt wird, dass die Daten des Auftraggebers selbst gegenüber einer Datenverarbeitung des Auftraggebers evidentermaßen keines Schutzes iSd vorliegenden Gesetzes bedürfen.[607] Verwendet nun ein Dienstleister (iSd § 4 Z 5 DSG 2000) zwar anfangs die eigenen Daten des Auftraggebers in datenschutzrechtlich zulässiger Weise, will diese aber dann (unberechtigterweise) für seine eigenen Zwecke weiterverarbeiten, so kommt es zu einem funktionalen Rollenwechsel. Bezüglich dieses (nicht mehr von der Aufgabe eines Dienstleisters gedeckten) neuen Zwecks ist der Dienstleister zum Auftraggeber geworden und der »Erstverarbeiter«[608] zum Betroffenen.[609] Dadurch fallen auch »eigene Daten« – bei jeder Form der Einbeziehung eines Dritten durch zweckwidrige Verwendung – grundsätzlich in den Schutzbereich des § 51 DSG 2000.

Zum anderen ist jedoch – nur im Ergebnis – dem OGH zu konzedieren, dass der strafrechtliche Schutz in einem derartigen Fall lediglich dann gegeben ist, wenn es sich dabei um Daten handelt, die dem Dienstleister ausschließlich auf Grund seiner berufsmäßigen Beschäftigung anvertraut oder zugänglich geworden sind (bzw er sie sich widerrechtlich verschafft hat). Hat daher eine Privatperson[610] als Dienstleister für den Erstverarbeiter den deliktsspezifischen Vorsatz erst nach dem rechtmäßigen Erhalt der Daten gefasst, so wurden dieser Person diese Daten weder aus beruflichen Gründen anvertraut oder zugänglich, noch hat sie sich diese widerrechtlich verschafft.

---

606 Siehe dazu auch *Jahnel,* OGH: Kein Schutz von Unternehmensdaten nach dem DSG?, RdW 2005/244, 200; auf Grundlage unzutreffender Schlussfolgerungen auch OGH 04.05.2004, 4 Ob 50/04p = RdW 2005/244, 200 *(Jahnel)* = ecolex 2004, 873 *(Knyrim*).

607 Vgl ErlRV 554 BlgNR XVI. GP, 12.

608 Auf die Begrifflichkeit des Auftraggebers iSd § 4 Z 4 DSG 2000 wird bewusst verzichtet, da über die Definition des Betroffenen (§ 4 Z 3 DSG 2000) e contrario zum Ausdruck gebracht wird, dass es sich beim datenschutzrechtlichen Auftraggeber um eine vom Betroffenen verschiedene (natürliche oder juristische) Person handeln muss.

609 Vgl dazu sinngemäß *Jahnel,* RdW 2005/244, 200.

610 Dh jemand, der keine berufliche Verbindung zur konkreten Datenverwendung hat.

Beispiel 1: A führt ein elektronisches Tagebuch in einer Datei, in dem viele intime Ereignisse über ihn festgehalten sind. Seinem vermeintlich besten Freund B überlässt A die Tagebuchdatei, damit ihm dieser ein Inhaltsverzeichnis und Sachregister für seine Erlebnisse einrichten möge. Während des Indizierens des Textes kommt B die Idee, das Tagebuch im Internet zu veröffentlichen, um A in seinem Geheimhaltungsanspruch zu schädigen.

Beispiel 2: Z würde gerne für eigene Zwecke Aktbilder von sich selbst besitzen. Sie bittet daher ihren Freund Y, diese von ihr anzufertigen, was dieser auch tut, wobei die Fotos auf seiner Digitalkamera bzw Festplatte gespeichert bleiben. Einen Monat später wird die Beziehung auf Initiative von Z beendet. Y veröffentlicht daraufhin in Schädigungsabsicht bezüglich des Geheimhaltungsrechts von Z die Bilder im Internet via Facebook.

Da sich in beiden Beispielsfällen B bzw Y die Daten nicht widerrechtlich verschafft haben, wurde § 51 DSG 2000 nicht verwirklicht. Zivilrechtliche Ansprüche bleiben davon freilich unberührt.

3. Sonderdelikt

Anders wäre der Sachverhalt allerdings zu beurteilen, wenn Y nicht der Freund, sondern ein professioneller Fotograf wäre. In einem solchen Fall sind ihm die Daten aufgrund seiner beruflichen Beschäftigung zugänglich bzw anvertraut worden. Auf eine »Widerrechtlichkeit« des Zugänglichwerdens kommt es in diesem Fall nicht an. Würde Y die Daten mit entsprechendem Vorsatz später veröffentlichen, handelt er bereits tatbestandsmäßig. Dies selbst dann noch, wenn er inzwischen den Beruf gewechselt hätte, in Pension gegangen wäre oder aus anderen Gründen den Beruf, durch den ihm diese schutzwürdigen Daten zugänglich wurden, nicht mehr ausübt.[611] Anzumerken ist jedoch, dass bei der (zulässigen) Datenverwendung in Ausübung einer beruflichen Beschäftigung noch keine sozial inadäquate Handlung vorliegt, sofern sich eine solche innerhalb der Regelungen über das Datengeheimnis nach § 15 Abs 1 DSG 2000[612] bewegt, weshalb ein (straf-)rechtlich missbilligtes Ri-

611 Vgl auch *Hinterhofer,* Geheimnisschutz, 186.

612 § 15 Abs 1 DSG 2000: »Auftraggeber, Dienstleister und ihre Mitarbeiter – das sind Arbeitnehmer (Dienstnehmer) und Personen in einem arbeitnehmerähnlichen (dienstnehmerähnlichen) Verhältnis – haben Daten aus Datenanwendungen,

siko fehlt.[613] § 51 DSG 2000 beschreibt in dieser Konstellation (arg »die ihm ausschließlich auf Grund seiner berufsmäßigen Beschäftigung anvertraut oder zugänglich geworden sind«) ein echtes unrechtsgeprägtes Sonderdelikt[614]. Eine etwaige strafbare Beteiligung daran (iSd § 12 zweiter oder dritter Fall) ist nach den Gesichtspunkten des § 14 Abs 1 zu prüfen, wobei gem § 14 Abs 1 Satz 1 bei wenigstens einem Beteiligten die besondere Täterqualität vorliegen muss.[615] Auf den ersten Blick deutet zumindest die Tathandlung des Selbst-Benützens auf ein eigenhändiges Delikt iSd § 14 Abs 1 Satz 2 Fall 1 hin, bei dem der Qualifizierte (Intraneus) die tatbestandsmäßige Ausführungshandlung selbst setzen muss (arg »Daten, die ihm ausschließlich aufgrund seiner berufsmäßigen Beschäftigung anvertraut oder zugänglich geworden sind […], selbst benützt«). Qualifiziertes Tatsubjekt und Tathandlung können in dieser Handlungsalternative aber sehr wohl getrennt werden, weil das »Selbst-Benützen« im deliktsspezifischen Verständnis lediglich ein Benützen zu eigenen Zwecken[616] bedeutet.[617] So könnte der Qualifizierte einen Dritten (Extraneus) anleiten, die schutzwürdigen Daten vom dienstlichen Computersystem auf einen persönlichen Datenträger des Qualifizierten zu kopieren, um sie dort für eigene Zwecke des Qualifizierten zu speichern.

Richtigerweise handelt es sich daher bei § 51 DSG 2000 in der Variante als echtes Sonderdelikt, um ein »Sonderpflichtdelikt« iSd § 14 Abs 1 Satz 2 Fall 2, da demjenigen, dem personenbezogene Daten Dritter beruflich überantwortet werden, eine besondere Rechtspflicht trifft, nämlich das Datengeheimnis (§ 15 DSG 2000) zu wahren.[618] Aus diesem Grund muss der Qualifizierte jedenfalls in der im Tatbild vorgesehenen besonderen Weise – Bruch des Datengeheimnisses der beruflich anvertrauten bzw zugänglichen personenbezogenen Daten – an der

---

die ihnen ausschließlich auf Grund ihrer berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich geworden sind, unbeschadet sonstiger gesetzlicher Verschwiegenheitspflichten, geheim zu halten, soweit kein rechtlich zulässiger Grund für eine Übermittlung der anvertrauten oder zugänglich gewordenen Daten besteht (Datengeheimnis)«.

613 Vgl *Bergauer,* ÖJZ 2013/113, 958.

614 Vgl auch *Salimi* in WK² DSG § 51 Rz 14.

615 In diesem Sinn zu § 48 Abs 1 DSG (1978) wohl auch OGH 05.04.1991, 16 Os 6/91 (16 Os 7/91).

616 Was einen Verstoß gegen die strenge datenschutzrechtliche Zweckbindung darstellt.

617 Mehr dazu weiter unten.

618 Vgl allerdings noch zu § 48 DSG (1978) *Triffterer* in SbgK § 126a Rz 38 f (aF Stand Dezember 1992).

Verwirklichung mitwirken. Verwendet der Qualifizierte daher die ihm beruflich anvertrauten oder zugänglichen Daten mit deliktsspezifischem Vorsatz zweckwidrig weiter (iSd Selbst-Benützens, Einem-anderen-Zugänglichmachens oder Veröffentlichens), so bricht er das ihm übertragene Datengeheimnis. Ein Nichtqualifizierter (Extraneus) kann bei diesem Sonderdelikt nur Bestimmungs- oder Beitragstäter sein.

Unmittelbarer Täter im Sinn dieser Rechtspflicht kann nur derjenige sein, der das ihm aus beruflichen Gründen überantwortete Datengeheimnis als seine persönliche Sonderpflicht bricht, sprich der Qualifizierte selbst. Es wäre zwar denkbar, dass der Qualifizierte einem Dritten (Extraneus) das Passwort zu seinem Computersystem in seinem Büro nennt, damit sich dieser die schutzwürdigen Daten auf einen Datenträger überspielen kann. Doch selbst in diesem Fall ist hier der Qualifizierte durch seine »verbotenen Hinweise« unmittelbarer Täter des Datengeheimnisbruchs. Die verbotenen Hinweise könnten darüber hinaus auch als Tathandlung des Zugänglichmachens der Daten an einen Dritten verstanden werden. Dieser Dritte hat sich aber lediglich durch einen sonstigen Beitrag (faktisches Überspielen der Daten) an der Tat beteiligt.[619]

Der objektive Tatbestand dieses Sonderpflichtdelikts ist aber mE viel zu weit gefasst, denn er beschriebt diesbezüglich kein sozial inadäquates Verhalten: »Wer […] personenbezogene Daten, die ihm ausschließlich auf Grund seiner berufsmäßigen Beschäftigung anvertraut oder zugänglich geworden sind […] selbst benützt, einem anderen zugänglich macht oder veröffentlicht […]«. Man denke an den Fall, dass eine Person ein Zeitungsinserat aufgeben will und dem zuständigen Redakteur den Anzeigentext samt seinen Kontaktdaten (zB Name, Anschrift, Telefonnummer usw) für eine Veröffentlichung in der Zeitung übermittelt. Der Redakteur veröffentlicht in weiterer Folge (grundsätzlich) schutzwürdige personenbezogene Daten und verwirklicht dadurch bereits den objektiven Tatbestand. Es ist daher das gesetzliche Tatbild unter Hinzufügung eines weiteren, ungeschriebenen Tatbestandsmerkmals dahingehend zu verstehen, dass nur eine missbräuchliche Datenverwendung – nämlich eine, die das Datengeheimnis verletzt – vom objektiven Tatbestand erfasst ist.[620] Methodologisch handelt

619 Siehe in Anlehnung an den Beispielsfall bei *Fuchs,* AT I[8], Rz 35/15.

620 Man vergleiche das Erfordernis des »Missbrauchens der Befugnis« bei weiteren klassischen Sonderpflichtdelikten va § 153 Abs 1 bzw § 302 Abs 1.

es sich dabei um eine teleologische Reduktion, da der überschießende Normtext im Sinne der ratio legis eingeschränkt wird bzw werden muss.

4. »Aufgedrängte Information«

Zu einem kriminalpolitisch unbefriedigenden Ergebnis kommt man in den Fällen, in denen dem »Täter« die schutzwürdigen Daten – außerhalb einer beruflichen Beschäftigung – »zugespielt« wurden, ohne dass sich dieser die Daten aktiv verschafft hat.

Zu denken wäre dabei an Fälle »aufgedrängter Information«, in denen zB jemandem per E-Mail die Daten eines Betroffenen unaufgefordert übersendet werden bzw ein Datenträger mit den schützenswerten Daten in die Sphäre des ursprünglich Vorsatzlosen gelangt ist. Man könnte sich dabei eine Variante des Beispielsfalls 2 vorstellen, in der Y die digitalen Aktbilder unberechtigterweise seinem besten Freund X unaufgefordert per E-Mail zuschickt. X fasst erst nach Erhalt der Daten den Entschluss, die Bilder – nachdem er sie durch Betrachten bzw Abfragen selbst benützt hat – im Internet zu veröffentlichen. Da sich aber X die personenbezogenen Daten der Z nicht widerrechtlich verschafft hat, entfällt bereits der Anwendungsbereich des § 51 DSG 2000.

Obwohl die widerrechtliche Verschaffung selbst[621] grundsätzlich[622] (noch) nicht deliktsgegenständlich ist, sondern erst die anschließende Verwendung[623], werden durch die vorausgesetzte Einengung des Tatobjekts unerträgliche Ergebnisse zugelassen. Der Gesetzgeber könnte diese Lücke durch das Hinzufügen weiterer objektiver Kriterien bezüglich des Tatobjekts schließen, indem er neben dem Erfordernis, dass die Daten widerrechtlich verschafft worden sein müssen, auch eine Art »Auffanganforderung« normiert, wie zB »oder sonst unzulässiger Weise innehat«. Es wäre nach dem Vorbild des § 120 Abs 2a und insb in Anbetracht des Schutzes der Privatsphäre und des Geheimhaltungscharakters personenbezogener Daten auch sinnvoll, demjenigen, der – wenn auch ohne sein Zutun – in Besitz von fremden personenbezogenen Daten gelangt ist, an denen ein schutzwürdiges Geheimhaltungsinte-

621 Es handelt sich dabei neben der näheren Beschreibung des Tatobjekts idR gleichzeitig auch (noch) um eine Vorbereitungshandlung.

622 Man beachte aber ein etwaiges Zusammentreffen des widerrechtlichen Sich-Verschaffens mit der Tathandlung des Selbst-Benützens (siehe gleich im Anschluss).

623 Siehe auch *Reindl-Krauskopf* in Brodil, Datenschutz, 73 (74); weiters *Salimi* in WK² DSG § 51 Rz 44.

resse besteht, die Pflicht aufzuerlegen, sich der Daten umgehend zu entledigen. Wird ein solcher »aufgedrängter Besitz« nicht durch die sofortige[624] »Gewahrsamsaufgabe«[625] beendet, würde durch die (weitere) bewusste Speicherung der Daten – deliktsspezifischer Vorsatz vorausgesetzt – zumindest Tatbestandsmäßigkeit iSd Selbst-Benützen des § 51 DSG 2000 gegeben sein. Freilich darf in einem solchen Fall das Löschen bzw Vernichten der Daten (iSd Aufzählung des § 4 Z 9 DSG 2000[626]) nicht als ein tatbestandliches Selbst-Benützen gewertet werden. De lege lata führt diese Strafbarkeitslücke zur Perpetuierung von Unrecht[627] bzw auch Sanierung von Unrecht[628], welche sich gerade in Anbetracht von ubiquitären (personenbezogenen) Daten im Rahmen des Geheimhaltungsgrundrechts als äußerst sachwidrig und rechtspolitisch untragbar darstellt. Es ist darüber hinaus nicht zu verstehen, weshalb zwar die Weitergabe einer telekommunikationstechnischen Nachricht (zB E-Mail) durch einem Unberechtigten, der zufällig in Besitz derselben gelangt ist, mit entsprechendem Vorsatz nach § 120 Abs 2a strafbar ist, nicht aber die Weitergabe von schutzwürdigen personenbezogenen Daten (wie etwa gar sensibler Daten iSd § 4 Z 2 DSG 2000).

5. § 51 DSG 2000 als Allgemeindelikt bei widerrechtlich verschafften Daten

Da das Datengeheimnis des § 15 Abs 1 DSG 2000 expressis verbis nur für (datenschutzrechtliche) Auftraggeber, Dienstleister und ihre Mit-

624 Siehe diverse Überlegungen zu gewissen Erfordernissen einer solchen Besitzaufgabe, wie etwa einer bestimmten Überlegungsfrist usw – bei *Hochmayr,* Besitz als strafbare Handlung, in BMJ (Hrsg), 33. Ottensteiner Fortbildungsseminar aus Strafrecht und Kriminologie. Bd 118 (2005) 87 (101).

625 Zur Problematik des strafrechtlichen Begriffs des »Gewahrsams« iZm unkörperlichen Daten siehe ausf S 480 ff.

626 »Verarbeiten von Daten: das Ermitteln, Erfassen, Speichern, Aufbewahren, Ordnen, Vergleichen, Verändern, Verknüpfen, Vervielfältigen, Abfragen, Ausgeben, Benützen, Überlassen (Z 11), Sperren, Löschen, Vernichten oder jede andere Art der Handhabung von Daten mit Ausnahme des Übermittelns (Z 12) von Daten«.

627 In Form des Geheimnisbruchs.

628 Ursprünglich schutzwürdige personenbezogene Daten können durch eine derartige Handlung zu »allgemein verfügbaren Daten« iSd § 1 Abs 1 DSG 2000 werden (was im datenschutzrechtlichen Schrifttum teilweise vertreten wird; siehe dazu unten). ME können systemgerecht nur zulässigerweise veröffentlichte Daten als »allgemein verfügbare Daten« iSd § 1 Abs 1 DSG 2000 in Betracht kommen (aM *Kotschy,* Das Grundrecht auf Geheimhaltung personenbezogener Daten, in Jahnel [Hrsg], Datenschutzrecht und E-Government. Jahrbuch 2012 [2012] 28 [45 f]).

arbeiter gilt, denen die Daten »ausschließlich auf Grund ihrer berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich geworden sind«, normiert § 51 DSG 2000 in der Variante Daten, »die er [Anm: der Täter] sich widerrechtlich verschafft hat« ein Datenweiterverarbeitungsverbot für »jedermann«. Der Gesetzgeber hatte wohl – den GMat zufolge – bei der Einführung des DSG 2000 darauf Bedacht genommen, dass eine »›berufsmäßige Beschäftigung mit Aufgaben der (Daten)Verarbeitung‹ nicht mehr einigen wenigen Berufsbildern vorbehalten [ist], sondern eine allgemein verbreitete Begleiterscheinung der modernen Arbeitswelt«.[629]

Da der Täterkreis dennoch wieder eingeschränkt wird, nämlich auf Personen, die sich die schutzwürdigen personenbezogenen Daten vor der eigentlichen Tat verschafft haben, könnte man an ein eigenhändiges Delikt denken. Hierbei muss der Qualifizierte selbst die Ausführung der Tat vornehmen. In Anbetracht der Systematik und Konzeption des Datenschutzrechts ergibt sich, dass es nicht darauf ankommt, dass der Täter in seiner Person selbst sich die Daten widerrechtlich verschafft bzw in weiterer Folge selbst verwendet. Dies leitet sich auch aus der Definition des Auftraggebers nach § 4 Z 4 erster Satz DSG 2000 ab, wenn es dort heißt, »natürliche oder juristische Personen, […] wenn sie allein […] die Entscheidung getroffen haben, Daten zu verwenden (Z 8), unabhängig davon, ob sie die Daten selbst verwenden (Z 8) oder damit einen Dienstleister (Z 5) beauftragen«. Darüber hinaus prägt diese täterbezogene Einschränkung nicht das Unrecht der Tat[630], was sich auch dadurch beweisen lässt, dass in einem Fall, in dem sich jemand ausschließlich schutzwürdige personenbezogene Daten verschafft, nicht einmal noch das Versuchsstadium des § 51 DSG 2000 betreten wird und es sich angesichts dieses Deliktstypus noch um eine straflose Vorbereitungshandlung handelt.

Für das »Sich-Verschaffen« der Daten wird schon begrifflich ein aktives Tun des Täters verlangt, weshalb die bloße Kenntnis bzw der faktische Besitz nicht tatbildlich ist.[631] Ein Sich-Verschaffen wird in An-

629 Siehe dazu ErlRV 1613 BlgNR XX. GP, 32.

630 Dazu gleich im Anschluss mehr.

631 Siehe auch *Salimi* in WK² DSG § 51 Rz 21 mwN; weiters OLG Wien 14.11.2013, 23 Bs 351/13 f = MR 2014, 246 *(Bauer)* = jusIT 2015/3, 9 *(Bergauer)* bzw *Bergauer,* Heimliche Nacktaufnahmen und deren Veröffentlichung im Internet in Anbetracht der Strafbestimmung des § 51 DSG 2000 – zugleich eine Anmerkung zu OLG Wien 14.11.2013, 23 Bs 351/13 f = jusIT 2015/3, 9.

betracht des Rechtsguts der informationellen Selbstbestimmung und der Reichweite des § 1 Abs 1 DSG 2000[632] bezüglich sämtlicher Verarbeitungsformen wohl iSd Verständnisses des (dort) als Tathandlung normierten Sich-Verschaffens iSd § 126c Abs 1 zu verstehen sein.[633] Es kommt somit nicht auf eine Gewahrsamsverschaffung an körperlichen Gegenständen an.[634] Die bloße unberechtigte Kenntniserlangung der Dateninhalte reicht bereits aus.

Ob das Verschaffen auch »widerrechtlich« erfolgte, ist in Anbetracht der Gesamtrechtsordnung zu werten. Zu prüfen ist dabei, ob sich jemand ohne rechtlich anerkannten Grund bzw durch einen Verstoß gegen eine Rechtsvorschrift diese geschützten Daten verschafft.[635] Es spielt dabei keine Rolle, ob sich dieser rechtliche Grund auf die Daten selbst bezieht (zB Verstoß gegen das Datenschutzgesetz 2000) oder auf ihren Träger (zB Wegnahme eines USB-Sticks mit den deliktischen Daten iSd § 127). Zu beachten ist folglich, dass ein beruflich indiziertes Verschaffen von Daten, die allerdings vom Arbeitgeber nicht datenschutzkonform verwendet werden sollen, ebenfalls ein widerrechtliches Verschaffen – weil Verstoß gegen das DSG 2000 – darstellen kann.[636] Aber nicht nur rechtliche Gebote bzw Verbote indizieren eine Widerrechtlichkeit, sondern ggf auch ein Sich-Verschaffen gegen den ausdrücklich oder schlüssig erklärten Willen des Berechtigten.[637]

In bestimmten Sachverhaltskonstellationen kann jedoch das widerrechtliche Verschaffen der Daten bereits mit der Tathandlung des »Selbst-Benützens« zusammenfallen bzw dieser unmittelbar vorangehen.[638] So führt das LG Salzburg in seiner E aus: »[...] das widerrechtliche Fotografieren der Toilettenbesuche der Genannten mittels iPhone, stellt daher eine – vom erforderlichen Vorsatz getragene – widerrechtliche Benützung von personenbezogenen Daten der Genannten, an denen sie ein schutzwürdiges Geheimhaltungsinteresse haben, dar«.[639] Ähnliches gilt für den Sachverhalt mit dem sich das OLG Wien be-

632 »Bloßes Wissen« der schutzwürdigen Daten, ohne jegliche Aufzeichnung bzw Verkörperung der Daten, fällt ebenfalls (nur) unter das Grundrecht nach § 1 Abs 1 DSG 2000 (vgl *Jahnel,* Handbuch, Rz 3/72 mwN).

633 Vgl dazu auch die Ausführungen zu § 126c bzw § 207a Abs 3.

634 Siehe dazu ausf *Bergauer,* jusIT 2015/3, 9.

635 Siehe auch *Hinterhofer,* Geheimnisschutz, 183.

636 Vgl idS wohl auch *Salimi* in WK² DSG § 51 Rz 19.

637 Vgl zur Widerrechtlichkeit im Tatbild auch ErlRV 1316 BlgNR XXII. GP, 4.

638 AA offenbar *Reindl-Krauskopf,* Cyberstrafrecht im Wandel, ÖJZ 2015/19, 112.

639 LG Salzburg 29.04.2011, 49 Bl 17/11v = jusIT 2011/89, 185 *(Thiele)*.

fassen musste, in dem der Täter im Badezimmer einer Wohngemeinschaft heimlich eine Mini-Digitalkamera installiert hat, um seine unbekleideten Mitbewohnerinnen damit zu filmen. Darüber hinaus soll der Täter die Videoaufnahmen anschließend auf eine Porno-Plattform ins Internet gestellt haben.[640]

Das »Sich-Verschaffen« iZm § 51 DSG 2000 kann datenschutzrechtsakzessorisch und jedenfalls auch sachgerecht als »Erheben bzw Ermitteln oder Erfassen für eigene Zwecke« verstanden werden. Die GMat halten etwa zum Begriff des Ermittelns[641] fest, dass nur das bloße »Wahrnehmen«, das kein gezieltes »Beobachten« darstellt, kein Ermitteln von Daten sei.[642] Will der Täter gezielt an eine schutzwürdige personenbezogene Information, liegt foglich bereits ein datenschutzrelevantes »Erheben« von Daten vor[643]. Hat er darüber hinaus vor, diese Information in einer Datenanwendung weiterzuverwenden, handelt es sich um ein »Ermitteln«. Wird die Information in weiterer Folge tatsächlich zur Weiterverwendung auf einem Datenträger festgehalten, spricht man vom »Erfassen«.[644] Alle diese Handhabungsmöglichkeiten von Daten werden vom Überbegriff des Verarbeitens von Daten (§ 4 Z 9 DSG 2000) ebenso umfasst wie von Art 2 lit b Datenschutz-RL.

Um zu vermeiden, dass jedes Sich-Verschaffen von Daten gleichzeitig auch ein datenschutzrechtliches Erheben bzw Ermitteln iSd Tathandlung des § 51 DSG des »Selbst-Benützens« darstellt, muss erneut darauf hingewiesen werden, dass es im Anwendungsbereich des DSG 2000 wohl ausschließlich auf Dateninhalte, nämlich den entsprechenden personenbezogenen Charakter, ankommt (hier: Daten im weiten Sinn). Für die begriffliche Klarstellung ist es mE erforderlich, beim datenschutzrechtlich relevanten »Sich-Verschaffen« auf die Information selbst abzustellen.

---

640 OLG Wien 14.11.2013, 23 Bs 351/13f = MR 2014, 246 *(Bauer)* = jusIT 2015/3, 9 *(Bergauer)*.

641 Es ist darauf hinzuweisen, dass das »Ermitteln« in der Stammfassung des DSG 2000 (BGBl I 165/1999) unter § 4 Z 10 DSG 2000 aF eigens definiert wurde. In den GMat wird aber ausgeführt, dass diese eigene Definition des Begriffs Ermitteln in Z 10 – allein schon im Hinblick auf die Datenschutz-RL – entbehrlich erscheint (vgl ErlRV 472 BlgNR XXIV. GP, 8).

642 ErlRV 472 BlgNR XXIV. GP, 7.

643 Vgl diesbezüglich auch iZm einer Video-Echtzeitüberwachung VwGH 28.05.2013, 2011/17/0066 (2011/17/0067).

644 Siehe dazu ausf *Bergauer,* jusIT 2015/3, 9.

In diesem Sinn verschafft sich ein Täter, dem es nicht auf die personenbezogenen Daten ankommt, widerrechtlich bloß eine Festplatte mit gespeicherten personenbezogenen Daten[645], ohne Letztere aber dadurch bereits gleichzeitig auch ermittelt zu haben. Beim Ermitteln muss es dem Täter bei der Wegnahme des Datenträgers auf die personenbezogenen Inhalte ankommen und die diesbezüglichen Daten schließlich iSd Lesens, Abfragens, Speicherns usw verarbeiten wollen. Im Zusammenhang mit der Sicherstellung eines Computers hatte in diesem Sinne auch die DSK in Zweifel gestellt, dass man durch Übernahme der rein faktischen Verfügungsgewalt über einen Computer von einem »Erheben« der darauf gespeicherten Daten sprechen kann.[646]

Das Sich-Verschaffen eines Datenträgers impliziert also grundsätzlich (noch) nicht das Erheben der darauf gespeicherten personenbezogenen Daten. In den oben zitierten E liegt aber durch das Abfotografierens bzw Filmens gleichermaßen ein widerrechtliches Sich-Verschaffen wie auch datenschutzrechtlich relevantes Ermitteln vor, an das sich unmittelbar – dh ohne eine ins Gewicht fallende Verzögerung – auch das Speichern der Daten auf dem jeweiligen Speichermedium (Speicherchip des iPhones bzw der Mini-Digitalkamera) für die Zwecke des Täters anschließt.

Selbst wenn man – wie *Salimi*[647] – davon ausgehen mag, dass das Ermitteln nicht vom Selbst-Benützen erfasst sein könne, liegt jedenfalls in einem derartigen Sachverhalt mit der bloßen Kenntnisnahme (Abfragen, Ausgeben, in den Arbeitsspeicher einlesen, Speichern usw) der Daten durch den Täter wohl ein Selbst-Benützen vor. Mit anderen Worten, es ist eine Abgrenzung von drei Szenarien indiziert:

---

645 Dass die Wegnahme eines Datenträgers oder Computersystems auch ein widerrechtliches Sich-Verschaffen der darauf gespeicherten personenbezogenen Daten bedeutet, befindet auch *Salimi* in WK² DSG § 51 Rz 23.

646 Siehe DSK 26.10.2006, K121.218/0017-DSK/2006, wobei letztlich entschieden wurde, dass im vorliegenden Fall die Absicht der handelnden Sicherheitsorgane nur darauf gerichtet war, mit dem sichergestellten PC die darin enthaltenen Datenträger als Beweisgegenstände gegen jede mögliche Zerstörung oder Veränderung zu sichern und ihre Beseitigung zu verhindern, nicht aber die Daten in einer Datenanwendung zu verarbeiten.

647 »Das Ermitteln der Daten kann keine Form des Benützens sein, da der Gesetzgeber von einem Umgang mit Daten ausgeht, die bereits beim Täter vorhanden sind – entweder, weil diese ihm aufgrund berufsmäßiger Beschäftigung zugegangen sind oder weil er sich diese zunächst widerrechtlich verschafft hat« *(Salimi* in WK² DSG § 51 Rz 44).

1. Daten, die der Täter bereits (rechtmäßig) innehat[648] und anschließend weiterverwendet,
2. Daten, die sich der Täter widerrechtlich verschafft hat, um sie in weiterer Folge verwenden zu wollen und
3. Daten, die sich der Täter widerrechtlich verschafft und deren Inhalte dem Täter gleichzeitig mit dem Verschaffungsakt zugänglich werden bzw dieser durch zB automatische Speicherung verarbeitet.

Die Grenzziehung lässt sich dabei nur schwer bewerkstelligen, und selbst das Erfordernis einer solchen ist wohl aus rechtspolitischen Gründen zu hinterfragen.

Bei Daten, von denen der Täter aus beruflichen Gründen bereits Kenntnis hat, kommt es nach hM[649] nicht ausschließlich auf das enge Verständnis des Geheimhaltungsschutzes iSv Preisgabe und Weitergabe an Dritte an, sondern wird auch ein Ermittlungsschutz vom Geheimhaltungsanspruch nach § 1 Abs 1 DSG 2000 mit eingeschlossen. So stellt auch eine Zweckänderung der Datenverwendung – nämlich zB die Ermittlung von Daten für andere Zwecke – einen Eingriff in den Geheimhaltungsanspruch des Betroffenen dar. Nach der datenschutzrechtlichen Rollenverteilung wird der Täter durch eine Zweckänderung[650] hins der Datenverwendung zum datenschutzrechtlichen Auftraggeber.[651] Dem Täter fehlt in seinem nunmehrigen deliktischen Verhalten bereits die rechtliche Befugnis zur Verwendung der Daten zu diesem geänderten (neuen) Zweck. Hat der Täter schon vor beruflicher Anvertrauung oder Zugänglichwerdung der Daten seinen Tatplan gefasst und wartet er nun lediglich darauf, dass er diese Daten verwenden kann, so erfüllt bereits der Zugriff auf die Daten die Tathandlung des »Selbst-Benützens« und, aus datenschutzrechtlicher Sicht, die Datenverarbeitungsvariante des »Ermittelns« (§ 4 Z 9 erster Fall DSG 2000).

---

648 Weil sie ihm zB aufgrund einer beruflichen Beschäftigung zugänglich wurden, oder er sich diese auf zulässige Weise verschafft hat bzw ihm verschafft wurden.

649 Vgl statt vieler *Jahnel,* Handbuch, Rz 2/15 mwN; weiters *Wiederin,* Privatsphäre, 62; siehe auch VfSlg 12.228/1989, 12.880/1991, 16.369/2001; DSK 05.04.2002, K120.766/004-DSK/2002; auch findet sich bereits in den GMat zum DSG 1978 (ErlRV 72 BlgNR XIV. GP, 22) der Hinweis, dass auch Daten, die ohne Mitwirkung des Betroffenen ermittelt wurden, dem DSG unterliegen.

650 Neuer Zweck: Die Daten werden nunmehr für seine eigenen Zwecke verwendet.

651 Siehe dazu S 428 f.

Aus datenschutzrechtlicher Sicht muss jede Zweckänderung gesondert auf ihre Zulässigkeit geprüft werden, was sich aus dem strengen Zweckbindungsprinzip ergibt. Dieses sieht vor, dass Daten nur für festgelegte, eindeutige und rechtmäßige Zwecke ermittelt und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverwendet werden dürfen (vgl § 6 Abs 1 Z 2 DSG 2000). Daraus folgt, dass auch Daten, die in ein und demselben Unternehmen verarbeitet werden, verschiedenen Zwecken dienen können. In diesem Fall würde eine ursprünglich datenschutzkonforme Verwendung von Daten für einen festgelegten Zweck bei nunmehriger Weiterverwendung dieser Daten für einen anderen Zweck grundsätzlich eine datenschutzrechtliche Übermittlung iSd § 4 Z 12 DSG 2000 darstellen, welche auf ihre datenschutzrechtliche Zulässigkeit gesondert zu prüfen ist. *Jahnel* bringt es auf den Punkt, wenn er ausführt, dass Daten zu »besitzen« nicht automatisch auch bedeutet, diese verwenden zu dürfen.[652]

6. Objektive Bedingung der Strafbarkeit

Die täter- bzw tatobjektbezogene Umschreibung »[Daten], die er sich widerrechtlich verschafft hat« iZm § 51 DSG 2000 als Allgemeindelikt[653] schränkt die Strafbarkeit insoweit ein, dass nur solche schutzwürdigen personenbezogenen Daten als Tatobjekt überhaupt in Frage kommen, die der Täter durch Zweckentfremdung je nach seinem Vorsatz weiterverwenden will. Da der objektive (strafbarkeitsbegründende) Tatbestand – wie oben angemerkt – kein sozial inadäquates Verhalten beschreibt und dadurch ein hohes Kriminalisierungspotenzial schon durch die äußere Tatbeschreibung begründet wird, könnte man dieses konkretisierende Element als »objektive Bedingungen der Strafbarkeit« ansehen, die nicht vom Tatbildvorsatz umfasst sein müssen (sog »Tatbestandsannex«).[654] Eine solche Interpretation bietet sich auch an, um Beweisschwierigkeiten im Bereich eines diesbezüglichen Tatbildvorsatzes, Kausalitätsproblemstellungen oder eine ggf doppelte Rechtswidrigkeitsprüfung zu vermeiden. Wobei man im Vorfeld – au-

652 Vgl *Jahnel,* Handbuch, Rz 4/103.

653 Dies gilt nicht für die Variante des § 51 DSG 2000 als (echtes) Sonderdelikt, da die berufsmäßige Zugänglichkeit in diesem Fall das Unrecht der Tat mitbestimmt.

654 Siehe zur Begrifflichkeit *Triffterer,* AT², 191 ff; zum »Tatbestandsannex« weiters *Triffterer,* AT², 194.

ßerhalb der Tatbestandprüfung des § 51 DSG 2000 – dennoch die Widerrechtlichkeit und den spezifischen Verschaffungsakt überprüfen muss. Im Übrigen ist das »widerrechtliche Verschaffen« der Daten (im Fall des § 51 DSG 2000 als Allgemeindelikt) kein Erfolgserfordernis. Es nimmt daher in dieser Variante keinen Einfluss auf den Unrechtsgehalt der Tat, schränkt aber den Anwendungsbereich der Strafvorschrift auf die strafwürdigen Fälle ein, denn bestraft wird nach § 51 DSG 2000 als Allgemeindelikt nur unter der Bedingung, dass die Daten vorher widerrechtlich verschafft wurden. Dies macht auch im Vergleich zur Variante des § 51 DSG 2000 als Sonderdelikt Sinn, denn – wie bereits oben angemerkt – fokussiert § 51 DSG 2000 nicht auf den Verschaffungsakt der tatbildlichen Daten, sondern auf deren (anschließende) Verwendung.[655] Da »jede« Datenverwendung von schutzwürdigen personenbezogenen Daten bereits einen Eingriff in des Grundrecht auf Datenschutz (§ 1 Abs 1 DSG 2000) darstellt, sollen aber für die Festsetzung des strafrechtlichen Unrechts (iSd tatsächlichen kriminalpolitischen Strafbedürfnisses) weitere rein objektive Kriterien hinzutreten, um eine überschießende Strafbarkeit zu verhindern. Eine solche Interpretation ergibt sich aus spezifischen Sinn- und Zwecküberlegungen bezüglich des konkreten Deliktstypus. Die Strafbarkeit wird daher vom Vorliegen weiterer äußerer Umstände abhängig gemacht. Insoweit stellt eine (unechte) objektive Bedingung (rein objektiv) der Strafbarkeit auch das Gegenstück einer überschießenden Innentendenz (rein subjektiv) dar, obwohl beide Elemente die Strafbarkeit einschränken. Es ist aber bei der objektiven Bedingung der Strafbarkeit die subjektive Einstellung des Täters unbeachtlich.

Wer ein fehlgeleitetes E-Mail mit schutzwürdigen personenbezogenen Daten irrtümlich erhält und diese Daten in weiterer Folge mit entsprechender Schädigungsabsicht im Internet veröffentlicht, macht sich nicht nach § 51 DSG 2000, sondern nach dem Ermächtigungsdelikt des § 120 Abs 2a strafbar.[656]

655 Dazu schon *Reindl-Krauskopf* in Brodil, Datenschutz, 73 (74).
656 Siehe dazu S 216 ff.

7. Tatobjekt »personenbezogene Daten« mit Geheimhaltungsinteresse

Als Tatobjekt des § 51 DSG 2000 werden ausschließlich personenbezogene Daten (iSd § 1 Abs 1 DSG 2000 bzw § 4 Z 1 DSG 2000) geschützt. Personenbezogene Daten, die automationsunterstützt verarbeitet werden, kommen dabei aber ebenso in Betracht, wie konventionell (oder auch nur zum Teil automationsunterstützt) verarbeitete Daten[657], da sich § 51 DSG 2000 am Grundrecht nach § 1 Abs 1 DSG 2000 orientiert. Personenbezogen sind Daten gem § 4 Z 1 DSG 2000 dann, wenn es sich um Angaben eines Betroffenen handelt, dessen Identität bestimmt oder bestimmbar ist.[658] Beim Tatobjekt des § 51 DSG 2000 kommt es foglich auf Dateninhalte, dh die Information selbst, an und nicht auf eine konkrete Darstellungsform derselben. Insoweit ist der Begriff »Daten« historisch bedingt nicht mehr treffsicher. Ursprünglich wurden »Daten« in der allgemeinen Begriffsbestimmung des § 3 Z 1 DSG 1978 als »auf einem Datenträger gespeicherte Angaben […]« definiert. Mit der DSG-Nov 1986[659] wurde diese Formulierung leicht in »auf einem Datenträger festgehaltene Angaben« modifiziert und mit Umsetzung der Datenschutz-RL musste die Einschränkung »auf einem Datenträger festgehaltene« überhaupt entfallen (vgl § 4 Z 1 DSG 2000). Art 2 lit a Datenschutz-RL versteht unter dem Begriff »personenbezogene Daten« alle »Informationen« über eine bestimmte oder bestimmbare natürliche Person. Die »Daten« des DSG 2000 sind daher mit (personenbezogenen) »Informationen« gleichzusetzen. So auch der OGH wenn er zu § 1 Abs 1 DSG 2000 ausführt, dass unter personenbezogenen Daten »Informationen (im weitesten Sinn)« zu verstehen sind, die mit einer Person in Verbindung stehen oder gebracht werden können.[660] Darüber hinaus umfassen auch die Schutzgewährleistungen des europäischen Gemeinschaftsgrundrechts des Art 8 Abs 1 GRC und des nationalen Grundrechts auf Geheimhaltung des § 1 Abs 1 DSG 2000 personenbezogenen »Daten«, unabhängig ihrer Darstellungsform. § 51 DSG 2000 verweist nun in der zweiten Alternative seiner überschießenden Innentendenzen expressis verbis auf den Geheimhal-

657 Siehe dazu ausf *Jahnel,* Die Meldung von Gesundheitsdaten an die Führerscheinbehörde aus datenschutzrechtlicher Sicht, jusIT 2008/8, 18; auch DSK 05.04.2002, K120.766/004-DSK/2002.

658 Siehe dazu auch S 563 ff.

659 BGBl 370/1986.

660 OGH 24.11.2014, 17 Os 40/14 g (17 Os 41/14d) = jusIT 2015/30, 76 *(Bergauer*).

tungsanspruch des § 1 Abs 1 DSG 2000, weshalb auch das dort gegenständliche Datenverständnis maßgebend ist.

Dass daher lediglich der (unkörperliche) Informationscharakter ausschlaggebend ist, macht bezüglich des zu schützenden Rechtsguts jedenfalls Sinn. Die personenbezogenen Daten – wenn auch als reine Information verstanden – stellen nur das mittelbare Schutzobjekt dar, da originär die Persönlichkeit eines konkreten menschlichen Individuums, dessen Integrität und Entfaltungsmöglichkeiten das zentrale Schutzanliegen bilden.[661]

Personenbezogene Informationen fallen bei flüchtigen Ereignissen, die gleich wieder in Vergessenheit geraten können, ebenso an, wie beim schlichten Faktum der Existenz einer Person durch ihr äußeres Erscheinungsbild in der Außenwelt. Auf ein Festhalten auf einem (Daten-)Träger kommt es dabei nicht an.[662]

Innerhalb der Kategorie der deliktsrelevanten direkt personenbezogenen Daten unterscheidet man einerseits Daten, die einer Person so zugeordnet sind, dass deren Identität ohne zusätzliche Informationen bestimmt werden kann, und andererseits Daten, die erst unter Rückgriff auf weitere Zusatzinformationen auf die Identität einer Person schließen lassen.[663] Wesentlich ist folglich, dass es beim Tatobjekt des § 51 DSG 2000 auf Dateninhalte, dh die Information, ankommt.

§ 51 DSG 2000 liegt – wie auch § 1 Abs 1 DSG 2000 – ein nur relativer Geheimnisbegriff zugrunde. Geschützt sind demnach personenbezogene Daten nur, sofern an ihnen ein »schutzwürdiges Geheimhaltungsinteresse« besteht.

Das schutzwürdige Geheimhaltungsinteresse und der Geheimhaltungsanspruch, sind anhand der Verfassungsbestimmung des § 1 Abs 1 DSG 2000[664] zu ermitteln.[665] Da es nicht um die Frage geht, wann schutzwürdige Geheimhaltungsinteressen als verletzt erachtet werden, sondern lediglich darum, ob überhaupt solche Interessen an den

661 *Berka,* Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit, 18. ÖJT Band I/1 (2012) 69.

662 Siehe dazu *Bergauer,* jusIT 2015/3, 9.

663 Siehe *Jahnel,* Begriff und Arten von personenbezogenen Daten, in Jahnel (Hrsg), Datenschutzrecht und E-Government. Jahrbuch 2008 (2008) 27 (32 ff).

664 Was die allgemeine Verfügbarkeit bzw mangelnde Rückführbarkeit der Daten auf eine Person anlangt.

665 Siehe *Bergauer,* ÖJZ 2013/113, 958; weiters *Kmetic,* Grundzüge des Computerstrafrechts (2014) 26.

verwendeten Daten bestehen, ist es für die Tatbestandsmäßigkeit des § 51 DSG 2000 nicht erforderlich, ein solches Geheimhaltungsinteresse nach Art 8 EMRK iZm der Gesamtrechtsordnung, insb auch nach den §§ 7 bis 9 DSG 2000, zu beurteilen.[666] Ausgeschlossen ist ein schutzwürdiges Geheimhaltungsinteresse nach der Verfassungsbestimmung des § 1 Abs 1 DSG 2000 explizit somit nur dann, wenn Daten infolge ihrer allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen (sog »anonyme Daten«) nicht Gegenstand des Geheimhaltungsanspruchs sind.

Der OGH führt diesbezüglich in einer E[667] aus, dass ein großzügiger Maßstab anzulegen ist und ein schützwürdiges Geheimhaltungsinteresse grundsätzlich immer dann angenommen wird, wenn es nicht iSd § 1 Abs 1 zweiter Satz DSG 2000 auszuschließen ist. Von einer »allgemeinen Verfügbarkeit« ist nach dem OGH nur dann auszugehen, wenn im Zeitpunkt der in Rede stehenden Verwendung von Daten diese tatsächlich (noch) jedermann zugänglich sind, was etwa bei Daten zutrifft, die in öffentlichen Registern oder Büchern, in Kundmachungen oder in sonstigen öffentlich abrufbaren Informationsquellen, wie etwa dem Telefonbuch oder dem Internet, auffindbar sind. Dagegen bedeutet (einmal hergestellte) Öffentlichkeit nicht in jedem Fall auch allgemeine Verfügbarkeit. Denn neben der jeweiligen Reichweite unterschiedlicher Arten von Öffentlichkeit (etwa in Form eines Gesprächs vor mehreren Anwesenden, einer Berichterstattung durch Massenmedien oder der Abrufbarkeit im Internet) ist – unter dem Aspekt fortdauernder Verfügbarkeit – die zeitliche Komponente zwischen (einmaliger) Veröffentlichung und Verwendung der Daten zu berücksichtigen. Nach diesen Kriterien sind daher nach Meinung des OGH in einer öffentlichen Verhandlung vorgekommener Daten – ohne qualifizierte Berichterstattung in Massenmedien oder dem Internet – nicht allgemein verfügbar.

Grundsätzlich wird aber die »allgemeine Verfügbarkeit« weder im DSG 2000 noch in dessen GMat[668] näher erläutert[669]. Allerdings hat

666 So aber *Dohr/Pollirer/Weiss/Knyrim,* DSG² § 51 Anm 8.

667 OGH 24.11.2014, 17 Os 40/14g (17 Os 41/14d) = jusIT 2015/30, 76 *(Bergauer*).

668 Siehe ErlRV 1613 BlgNR XX. GP, 35; dort ist von der »allgemeinen Zugänglichkeit« die Rede.

669 Zur detaillierten Auseinandersetzung mit dieser Thematik siehe *Jahnel,* Dreifacher Datenschutz?, in Bergauer/Staudegger (Hrsg), Recht und IT. Zehn Studien (2009) 33 (51f); ebenso *Jahnel* in FS Schäffer, 313 (321f).

mittlerweile auch der EuGH[670] zu »allgemein verfügbaren Daten« Stellung genommen und klargestellt, dass auch »veröffentlichte personenbezogene Daten« in den Anwendungsbereich der Datenschutz-RL[671] fallen.[672] Das Geheimhaltungsinteresse des Betroffenen lebt daher durch Änderung der ursprünglichen Zweckbindung von zulässigerweise veröffentlichten Daten datenschutzrechtlich wieder auf.

In diese Richtung verweisen auch die GMat (iZm § 8 Abs 2 DSG 2000), wenn dort ausgeführt wird: »Da im Übrigen auch eine andere Form der Aufbereitung veröffentlichter Daten neue – nicht veröffentlichte – Informationen liefern kann, kann nicht ausgeschlossen werden, daß in besonderen Konstellationen schutzwürdige Geheimhaltungsinteressen doch berührt werden, […]«.[673]

Anzumerken ist an dieser Stelle, dass der Wortlaut des § 1 Abs 1 DSG 2000 allgemein verfügbare Daten per se vom Grundrechtsschutz ausschließt. Dieser zu rigorose Ausschluss, stellt ein Versäumnis des nationalen Gesetzgebers dar, der die unionsrechtlichen Vorgaben bislang nicht gehörig umgesetzt hat.[674]

In diesem Zusammenhang sei ergänzend auf das Recht auf Datenschutz nach Art 8 GRC hingewiesen, welches in seinem Wortlaut weder auf ein etwaiges schutzwürdiges Interesse abstellt, noch eine Ausnahme für veröffentlichte Daten vorsieht.[675]

Beispiel: A speichert auf einem Datenträger (zB USB-Stick) personenbezogene Daten von unterschiedlichen Personen, die im Internet – zB von A selbst – zulässigerweise auf verschiedenen Webpages veröffentlicht wurden. A kombiniert diese für sich allgemein verfügbaren Daten in einer Datensammlung. Diese gesammelten Daten stellen nun aber durch ihren neuen Informationsgehalt neue personenbezogene Daten dar, die in dieser Form nicht allgemein verfügbar sind. Die Datensammlung verfolgt nämlich einen anderen Zweck und dieser deckt sich wiederum nicht mit dem Zweck, der der Veröffentlichung der ein-

670 EuGH 16.12.2008, C-73/07 (Tietosuojavaltuutettu/Satakunnan Markkinapörssi Oy und Satamedia Oy) = MR-Int 2009, 14 *(Wittmann)*.

671 RL 95/46/EG.

672 Vgl *Bergauer,* OGH: Verletzung des Grundrechts auf Datenschutz unter Missbrauch der Amtsgewalt, jusIT 2012/13, 30.

673 Siehe ErlRV 1613 BlgNR XX. GP, 41.

674 Siehe zum diesbezüglichen (aber nicht beschlossenen) Vorhaben § 1 Abs 1 DSG 2000 idF RV 472 BlgNR XXIV. GP.

675 Vgl sinngemäß ErlRV 472 BlgNR XXIV. GP, 6.

zelnen Datensätze zugrunde gelegen ist.[676] Falls sich B den USB-Stick, auf dem diese Datensammlung gespeichert ist, widerrechtlich verschafft und die Daten – entsprechenden Vorsatz vorausgesetzt – verwendet (bspw durch die Veröffentlichung im Internet), ist § 51 DSG 2000 verwirklicht.

Auf Tatbestandsebene ist somit lediglich zu prüfen, ob an den deliktsgegenständlichen Daten überhaupt ein schutzwürdiges Geheimhaltungsinteresse iSd § 1 Abs 1 DSG 2000 nach objektiven Gesichtspunkten besteht. Bejahendenfalls kann erst bei der Rechtswidrigkeitsprüfung das Unrecht der Tat noch entfallen, wenn nämlich zwar an sich schutzwürdige Daten verwendet werden, aber dieser Eingriff bzw diese Beschränkung des grundrechtlich geschützten Interesses nach § 1 Abs 2 DSG 2000 – bzw den einfachgesetzlichen Bestimmungen des §§ 8 und 9 DSG 2000 – gerechtfertigt ist.[677]

Eine solche Rechtfertigung wird daher insb gem § 8 Abs 2 erster Satz zweite Alt (für nicht-sensible Daten) und gem § 9 Z 2 DSG 2000 (für sensible Daten) bei der Verwendung bloß »indirekt personenbezogener Daten«[678] vorliegen.

8. Allgemeine Betrachtung des schutzwürdigen Geheimhaltungsinteresses

Was das schutzwürdige Geheimhaltungsinteresse anlangt, so kommt es dafür – wie oben ausgeführt – auf eine objektive (datenschutzrechtliche) Betrachtung an, weshalb die Daten nicht absolut geheim sein müssen.[679] Ein begrenzter Kreis von (berechtigten) Geheimnisträgern beeinträchtigt dieses Interesse daher noch nicht.[680] In diesem Sinn führt – wie bereits angemerkt – der OGH aus, dass das schutzwürdige Interesse an der Geheimhaltung personenbezogener Daten auch dann nicht ausgeschlossen werde, wenn der Betroffene selbst geschützte Da-

676 Vgl idS EuGH 16.12.2008, C-73/07.
677 Vgl dazu auch *Salimi* in WK² DSG § 51 Rz 64.
678 Siehe dazu *Bergauer,* Indirekt personenbezogene Daten – datenschutzrechtliche Kuriosa, in Jahnel (Hrsg), Datenschutzrecht. Jahrbuch 2011 (2011) 55 (55 ff); generell zur Begrifflichkeit *Jahnel* in Jahnel, Jahrbuch 2008, 27 (36 ff).
679 AA *Salimi* in WK² DSG § 51 Rz 45.
680 Siehe dazu noch *Jahnel,* Datenschutzrecht, in Jahnel/Schramm/Staudegger (Hrsg), Informatikrecht² (2003) 241 (250); weiters OGH 03.09.2002, 11 Os 109/01.

ten einem (begrenzten) Personenkreis offenbart.[681] Selbst ein begrenzter Kreis von berechtigten »Geheimnisträgern« steht daher dem Geheimhaltungsinteresse nicht entgegen. Dies resultiert auch aus dem allgemeinen Gebot der restriktiven Interpretation einer Einschränkung von Grundrechten.[682] Darüber hinaus ist – anders als noch in § 48 Abs 1 DSG 1978 – nicht mehr die »Offenbarung« der Daten tatbildlich, die sich dadurch definierte, dass der Täter die schutzwürdigen Daten jemandem mitteilen musste, dem sie bisher nicht oder nicht sicher bekannt waren.[683]

Dass diese Daten niemandem außer dem Betroffenen bekannt sein dürfen, ist daher nicht gefordert. Dies ist schon deshalb anzunehmen, da die Frage, ob an den Daten schutzwürdige Geheimhaltungsinteressen bestehen, ausschließlich anhand objektiver (datenschutzgesetzlicher) Kriterien zu beantworten ist. Für eine Strafbarkeit nach § 51 DSG 2000 kommt es idZ darauf an, dass die Daten vom Täter – mit entsprechendem Vorsatz – rechtswidrig (im datenschutzrechtlichen Verständnis) verwendet werden. Es ist davon auszugehen, dass, hätte der Gesetzgeber dies – entgegen der hier vertretenen Ansicht – anders berücksichtigen wollen, der objektive Tatbestand um das Merkmal »Unbefugten« – wie es auch in § 120 Abs 2a Eingang gefunden hat – einfach ergänzt hätte werden können, was aber nicht gemacht wurde. Damit wäre aber klargestellt worden, dass nur pönalisiert wird, wer einem (aus datenschutzrechtlicher Sicht) »Unbefugten« diese Daten zugänglich macht. Daher bestätigt die geltende Formulierung des Tatbestands die Meinung, dass es überhaupt nicht auf den Kenntnisstand oder eine etwaige Befugnis des Datenempfängers ankommt.

Für eine grundsätzliche Strafbarkeit des Zugänglichmachens von schutzwürdigen Daten kommt es demnach nicht darauf an, ob dem Übermittlungsempfänger die Daten bereits (rechtmäßig oder unrechtmäßig) bekannt sind oder nicht. Ein »Offenbarungszwang« für eine Strafbarkeit in der Form, dass geheim zuhaltende Daten einem bislang unwissenden Dritten zur Kenntnis gebracht werden müssen, besteht

681 Vgl OGH 03.09.2002, 11 Os 109/01.
682 So auch OGH 03.09.2002, 11 Os 109/01.
683 Siehe OGH 05.04.1991, 16 Os 6/91 (16 Os 7/91); weiters *Bertel* in WK² § 310 Rz 7 (Stand Mai 2010).

für die Tatbildmäßigkeit nicht (mehr[684]).[685] So sieht dies auch *Popp,* der ausführt, dass der zum »Offenbaren« gehörende Erfolg erst (und nur dann) eingetreten ist, wenn auf der Empfängerseite mindestens eine Person am Ende um die geheime Tatsache weiß und sie der von dieser Tatsache betroffenen Person zuordnen kann.[686] Das »interne Täterverhalten«, ohne die Daten außenwirksam zu verwenden, reicht somit schon aus.[687] Zu diesem Schluss muss man wohl kommen, wenn man sich die faktische Existenz der Tathandlung des »Selbst-Benützens« vor Augen führt, da gerade diese Handlung keine tatsächliche Aufhebung des Geheimhaltungsschutzes im engeren Sinn impliziert. Der Täter ist ja bereits (rechtmäßig oder nicht) in Kenntnis der Daten. In diesem Sinn führt auch der OGH aus, dass das schutzwürdige Interesse an der Geheimhaltung personenbezogener Daten auch dann nicht ausgeschlossen werde, wenn der Betroffene selbst geschützte Daten einem (begrenzten) Personenkreis offenbart.[688]

Ebenso kommt es für die Strafbarkeit nicht auf das enge Verständnis des Geheimhaltungsschutzes an (iSd ausschließlichen Schutz gegenüber Preisgabe und Übermittlung an Dritte). Nach einhelliger datenschutzrechtlicher Meinung beinhaltet der Geheimhaltungsschutz auch einen Ermittlungsschutz.[689] Dem Täter fehlt in Verwirklichung des Delikts bereits die rechtliche Befugnis zur Verwendung der Daten, selbst wenn er diese für die Ausübung seiner beruflichen Tätigkeit innehat. Aus datenschutzrechtlicher Sicht muss jede Zweckänderung gesondert auf ihre Zulässigkeit geprüft werden, was sich aus dem strengen Zweckbindungsprinzip ergibt. Im Gegensatz etwa zum kernstrafrechtlichen § 120 Abs 2a, wo die erste Tathandlung des Aufzeich-

---

684 Siehe aber die Vorgängerbestimmung des § 48 Abs 1 DSG 2000 mit seiner Tathandlung des »Offenbarens« (vgl auch OGH 05.04.1991, 16 Os 6/91[16 Os 7/91]).

685 Vgl dazu auch die Tathandlung des »Offenbarens« iZm der Verletzung des Amtsgehemnisses (§ 310), wo gefordert wird, dass das Amtsgeheimnis jemandem mitgeteilt wird, der es bisher nicht oder nicht sicher gekannt hat (vgl *Bertel* in WK² § 310 Rz 7; *Leukauf/Steininger,* StGB³ § 310 Rz 10; *Fabrizy,* StGB¹¹ § 310 Rz 3a).

686 Vgl *Popp,* IT-Outsourcing und Cloud Computing – zwei neue Herausforderungen für die Criminal Compliance, JSt 2012, 30.

687 AA *Salimi* in WK² DSG § 51 Rz 45, der meint, dass jede Tathandlung – auch das Benützen – geeignet sein müsse, die Geheimhaltungsinteressen des Opfers zu verletzen, was eine Außenwirkung voraussetze.

688 Vgl OGH 03.09.2002, 11 Os 109/01.

689 Vgl *Wiederin,* Privatsphäre, 62; weiters *Jahnel,* Handbuch, Rz 2/15 mwN; *Jahnel* in FS Schäffer, 313 (320); VfSlg 12.228/1989, 12.880/1991, 16.369/2001; DSK 05.04.2002, K120.766/004-DSK/2002.

nens einer Nachricht noch eine abstrakte Gefährdung des Rechtsguts bedeutet, ist mit dem »Selbst-Benützen« schutzwürdiger Daten iSd § 51 erster Fall zweite subj Alt DSG 2000 – entsprechende Absicht vorausgesetzt – bereits das Rechtsgut der »Geheimhaltung personenbezogener Daten«) bzw der »informationellen Selbstbestimmung« verletzt. Insbesondere bei der (erweiterten) Schädigungsabsicht kommt es nämlich (lediglich) darauf an, den »Anspruch« auf Geheimhaltung nach § 1 Abs 1 DSG 2000 zu schädigen, was sich daher gerade nicht daran orientieren kann, ob die Daten rein faktisch absolut geheim sind oder nicht.

9. Tathandlungen

Die Tathandlungen des § 51 DSG 2000 sind das Selbst-Benützen, Einem-anderen-Zugänglichmachen und das Veröffentlichen der tatbildlich näher konkretisierten personenbezogenen Daten.

Mit »Benützen« der Daten werden wohl sämtliche Handlungsalternativen der Datenverwendung iSd § 4 Z 8 DSG 2000 gemeint sein, wie es auch die Deliktsbezeichnung zum Ausdruck bringt.[690] Dass der Gesetzgeber ausschließlich das Benützen im datenschutzrechtlichen Sinn, nämlich als eine der vielen Alternativen des § 4 Z 9 DSG 2000 (neben dem Zugänglichmachen und Veröffentlichen) pönalisieren wollte[691], ist mE bereits aufgrund der Tatsache, dass wohl auch das »Zugänglichmachen« keinen ausdrücklichen datenschutzgesetzlichen terminus technicus einer Datenverwendungsmodalität darstellt, nicht anzunehmen. Als ein weiteres Indiz kann der Ausdruck des »widerrechtlichen Verschaffens« herangezogen werden, denn auch das »Verschaffen« ist kein Begriff, der aus der Datenschutzterminologie stammt. Zudem soll nach den GMat die rechtswidrige »Verwendung« von Daten in besonders verwerflicher Absicht von der Strafnorm erfasst sein.[692] Da diesbezüglich von der Datenverwendung gesprochen wird, ist anzunehmen, dass alle Arten der Handhabung von Daten gemeint sind. Daher wäre die Formulierung einer Tathandlung des »Verarbeitens« (§ 4 Z 9 DSG 2000) wohl sachgerechter.

690 Wobei anzumerken ist, dass das »Verarbeiten von Daten« eine Unterform der »Verwendung von Daten« iSd § 4 Z 8 darstellt; siehe dazu nun auch ErlRV 689 BlgNR XXV. GP, 21.

691 Wie es auch *Thiele* in SbgK, Vorbem zu den §§ 118 – 124 StGB Rz 61 interpretiert.

692 Siehe dazu ErlRV 1613 BlgNR XX. GP, 53.

Den GMat[693] ist weiters zu entnehmen, dass die Tathandlung des »Benützens« gewählt wurde, um nicht zu einer Konkurrenz mit anderen gerichtlichen Straftatbeständen zu gelangen (zB § 126a). Diese Sorge war und ist – nun nach der Novellierung des § 51 DSG 2000 noch viel mehr – aus mehreren Gründen nicht nachvollziehbar. § 51 DSG 2000 idgF stellt nun ebenso wie § 126a ein (reines) Offizialdelikt dar und geht als lex specialis hins personenbezogener Daten der Datenbeschädigung ggf vor. Wobei anzumerken ist, dass als Tatobjekt des § 51 DSG 2000 nicht nur automationsunterstützte Daten (wie ua bei § 126a) in Frage kommen, sondern auch solche, die mittels anderer Verarbeitungs- und Darstellungsformen verarbeitet werden.

Aufgrund der höheren Strafdrohung des § 51 DSG 2000 würde in diesem Verhältnis zum Grunddelikt des § 126a Abs 1 auch die Subsidiaritätsklausel des § 51 DSG 2000 nicht greifen. Zudem repräsentiert § 126a nach hM ein Vermögens- bzw Erfolgsdelikt, das auf den Eintritt eines Vermögensschadens abstellt. Da durch die DSG-Nov 2010 nunmehr klargestellt wurde, dass sich die »Schädigungsabsicht« in § 51 DSG 2000 lediglich auf den »Geheimhaltungsanspruch« nach § 1 Abs 1 DSG 2000 bezieht und nicht auf einen Vermögens- oder auch »Gefühlsschaden«, würde sich bei Änderung der Handlungsmodalität vom »Benützen« zum »Verarbeiten« in § 51 DSG 2000 keine ernsthafte Konkurrenzproblematik gegenüber dem Anwendungsbereich des § 126a mehr ergeben. Denn sofern jemand Daten zB widerrechtlich löscht[694], um dem Verfügungsberechtigten einen Vermögensschaden zuzufügen, ist § 51 DSG 2000 ohnedies nicht anwendbar, da der Täter weder mit Bereicherungsvorsatz agierte, noch mit Schädigungsabsicht bezüglich des Geheimhaltungsanspruchs des Betroffenen gehandelt haben kann. Die »besonders verwerfliche Absicht«, die der Gesetzgeber in § 51 DSG 2000 berücksichtigt wissen wollte und die aktuell durch alternativ zu erfüllende überschießende Innentendenzen in Form eines Bereicherungsvorsatzes und einer Schädigungsabsicht des Geheimhaltungsanspruchs des Betroffenen realisiert ist, verhindert ohnedies eine über das Ziel hinausschießende Kriminalisierung der Bevölkerung (strafbarkeitseinschränkende Funktion[695]). Zudem wird de lege lata – wie bereits erörtert – auch das Tatob-

693 Vgl ErlRV 1613 BlgNR XX. GP, 53.

694 Das Löschen ist neben dem Benützen einer der vielen Handlungsalternativen des »Verarbeitens von Daten« gem § 4 Z 9 DSG 2000.

695 Siehe dazu *Hinterhofer,* Geheimnisschutz, 191.

jekt dermaßen eng definiert, dass eine vollständige Erfassung sämtlicher Formen des Verarbeitens iSd § 4 Z 9 DSG 2000 als Tathandlungen, die für sich allein genommen (noch) nicht den »strafrechtlichen Unwert« darstellen, jedenfalls gerechtfertigt und auch sachdienlicher wäre. Bereits aus praktischer Sicht ist ein »Benützen von Daten«, ohne in Berührung mit den anderen Handlungsalternativen des § 4 Z 9 DSG 2000 zu gelangen, kaum vorstellbar. In der einschlägigen Lit wird unter »Benützung« insb das Gebrauchen und Verarbeiten von Daten für die vorgegebenen Zwecke verstanden.[696] Das bedeutet, dass das Benützen mit dem Überbegriff des »Verarbeitens von Daten« definiert wird, obwohl »das Benützen« neben vielen anderen nur eine einzige Handlungsalternative des Verarbeitens im engen datenschutzrechtlichen Begriffsverständnis nach § 4 Z 9 DSG 2000 darstellt und das Verarbeiten von Daten wiederum eine Unterkategorie der Datenverwendung nach § 4 Z 8 DSG 2000 ist.[697] Darüber hinaus verwirklicht der Täter diese Tathandlung gerade dann, wenn er die Daten nicht nach den »vorgegebenen Zwecken« verwendet, sondern für seine eigenen. Auch streng nach dem Wortsinn interpretiert, impliziert das »Benützen« eine aktive Handhabung der Daten, wie das Abfragen, Ausgeben, Löschen, Kopieren, Verknüpfen usw. Nichts anderes wird unter dem Ausdruck »Gebrauchen« von Daten zu verstehen sein, welcher ebenfalls für die nähere Umschreibung des Benützens herangezogen wird.[698] Es fragt sich, warum nicht – in Klarstellung einer nicht deckungsgleichen Definition der Begrifflichkeiten zum DSG 2000 – die konkrete Tathandlung als zB »Selbst-Gebrauchen« beschrieben wird. Die Aufnahme einer Begrifflichkeit (hier: Benützen) als Tatbestandsmerkmal in einen Straftatbestand eines speziellen Sachgesetzes, das in seinen spezifischen Begrifflichkeiten selbst diesen Terminus anders verwendet, ist zu vermeiden. Die Rechtsanwendung wird dadurch unnötig erschwert. Es ist aber mE – im Gegensatz etwa zum rein subjektiv angestrebten Selbst-Benützen der Daten des § 118a Abs 1 – auf das Benützen der »Dateninhalte« abzustellen.

---

696 *Dohr/Pollirer/Weiss/Knyrim,* DSG² § 4 Anm 10; vgl auch *Jahnel,* Handbuch, Rz 3/110.

697 Zu beachten ist allerdings, dass sich die österreichische Terminologie des DSG 2000 in diesem Zusammenhang von der Begrifflichkeit der Datenschutz-RL unterscheidet. In Art 2 Datenschutz-RL umfasst bereits der Begriff der »Verarbeitung« auch die Weitergabe von Daten durch Übermittlung, Verbreitung oder jede andere Form des Bereitstellens (siehe ausf *Jahnel,* Handbuch, Rz 3/108).

698 Siehe dazu *Dohr/Pollirer/Weiss/Knyrim,* DSG² § 4 Anm 10; vgl auch *Jahnel,* Handbuch, Rz 3/110.

Im Unterschied zu den Handlungsalternativen der Datenweitergabe entfaltet jedoch das Benützen der Daten keine unmittelbare Außenwirkung.[699] Werden die Daten nämlich durch das Benützen durch den Täter selbst einem anderen zugänglich, so liegt eine Form der Weitergabe bzw Übermittlung der Daten vor. Dies führt aber bei näherer Betrachtung dazu, dass bereits das »widerrechtliche Verschaffen« der Daten selbst ein Benützen indiziert, zumindest sofern der Täter dabei bereits (inhaltliche) Kenntnis von den Daten nimmt bzw nehmen kann (vgl »ermitteln«).[700] Verschafft sich also der Täter widerrechtlich diese Daten, ist ein Benützen im weiteren Sinn derselben (wie das Ermitteln, Speichern, Vervielfältigen, Auslesen usw) eingeschlossen.[701] Anders wäre es freilich, wenn der Täter durch einen Dritten (Bestimmungstäter) gegen Entgelt veranlasst würde, sich eine automationsunterstützt verarbeitete Datei, deren Inhalt er nicht kennt, widerrechtlich zu verschaffen. In diesem Fall geht mit dem widerrechtlichen Verschaffen kein Benützen der personenbezogenen Daten einher, da der Täter die personenbezogenen »Inhalte« dieser Datei nicht benützt oder in einer anderen datenschutzrelevanten Form verarbeitet.

Auch erscheint auf den ersten Blick anstelle der Tathandlung des Benützens, die des – bereits in der Vorgängerbestimmung des § 48 Abs 1 DSG 1978[702] verwendeten – »Verwertens« sinnvoll, da prinzipiell jede Form der Datenverwendung davon erfasst wäre, die einen wirtschaftlichen Nutzen für den Täter eröffnen würde. Unter dem »Verwerten« versteht man im Strafrecht prinzipiell eine Handlung, bei der der Täter das Geheimnis (hier: Daten, an denen ein Geheimhaltungsinteresse besteht), ohne es anderen zu offenbaren, sich selbst wirtschaftlich nutzbar macht.[703] Diese Handlungsmodalität könnte aber lediglich bei der Deliktsvariante mit der Bereicherungsintention des Täters Sinn machen, denn bei der Alternative bezüglich der Schädigungsabsicht hins des Geheimhaltungsanspruchs wäre sie jedenfalls unpassend, da

699 Siehe dazu auch LG Salzburg 29.04.2011, 49 Bl 17/11v = jusIT 2011/89, 185 *(Thiele);* aA *Salimi,* ÖJZ 2012/115, 998.

700 Siehe S 132 f.

701 Siehe dazu auch LG Salzburg 29.04.2011, 49 Bl 17/11v = jusIT 2011/89, 185 *(Thiele);* aA *Salimi* in WK² DSG § 51 Rz 44, wenn er meint: »Das Ermitteln der Daten kann keine Form des Benützens sein«.

702 BGBl 565/1978.

703 Siehe zB *Lewisch* in WK² § 121 Rz 7 mwN.

dabei auf keinen darüber hinausreichenden wirtschaftlichen Nutzen oder Schaden mehr abgestellt wird.

Wesentlicher Teil dieser Tathandlung ist die Beifügung des Wortes »selbst«. Damit wird klargestellt, dass der Täter die Daten selbst, dh für eigene Zwecke, verarbeiten muss. Sie können dabei – müssen es aber nicht – bloß intern, ohne Außenwirkung für Selbstzwecke des Täters verarbeitet werden.[704] Die anderen Tathandlungen des Zugänglichmachens oder Veröffentlichens verlangen dagegen, dass der Täter die Daten anderen mit Außenwirkung zugänglich macht.[705] Mit der Übermittlung oder Veröffentlichung erschöpft sich aber bereits der datenschutzrechtliche Zweck der Datenverwendung für den Täter. Diese Erwägungen führen dazu, dass die Tathandlung des »Selbst-Benützens« aufgrund des unterschiedlichen sozialen Sinngehalts und des Vollendungszeitpunkts den anderen Tathandlungen gegenüber rechtlich ungleichwertig ist.[706]

Die Tathandlung des Zugänglichmachens wird nicht bloß in der Übermittlung der Daten, also in der Weitergabe von Daten an andere Empfänger als den Betroffenen, den Auftraggeber oder einen Dienstleister zu sehen sein, sondern insb auch in der Veröffentlichung von Daten.[707] Die Verwendung von Daten für ein anderes Aufgabengebiet des Auftraggebers könnte bei entsprechendem Vorsatz ebenfalls tatbildlich sein. Die Normierung der Tathandlung des Veröffentlichens von Daten lässt demzufolge auf den ersten Blick aus rein datenschutzrechtlicher Sichtweise bloß auf eine verstärkende Redundanz schließen, da das Veröffentlichen bereits Handlungsalternative des »Übermittelns von Daten« iSd § 4 Z 12 DSG 2000 ist und somit auch in der Tathandlung des Zugänglichmachens bereits enthalten ist. Zu diesem Ergebnis tragen aus dem strafrechtlichem Verständnis heraus auch die GMat bei, wenn in diesen ausgeführt wird: »Ein Zugänglichmachen liegt vor, wenn einem anderen – auf welche Art auch immer – die Möglichkeit zur Kenntnisnahme verschafft wird (z.B. Bild auf einer Internet-Homepage).«[708] Eine solche Ansicht bietet aber faktisch keinen Raum für eine Abgrenzungsmöglichkeit zum Veröffentlichen.

704 Siehe dazu auch LG Salzburg 29.04.2011, 49 Bl 17/11v = jusIT 2011/89, 185 *(Thiele);* aA *Salimi,* ÖJZ 2012/115, 998.
705 Vgl auch *Salimi* in WK² DSG § 51 Rz 46.
706 In diesem Zusammenhang auch *Salimi* in WK² DSG § 51 Rz 10.
707 Siehe § 4 Z 12 DSG 2000.
708 Siehe ErlME 82/ME XXIV. GP, 8.

Wenn sich das »Veröffentlichen« nur aufgrund eines größeren Personenkreises durch Zugänglichmachen (!) von der Tathandlung des »einem anderen Zugänglichmachens« abgrenzen soll, wie es die GMat darstellen[709], so würde doch wohl die letztgenannte Tathandlung im äußeren Tatbestand – stellvertretend für sämtliche Handlungen, die das Tatobjekt anderen zugänglich machen – vollkommen ausreichen. Die Tathandlung des Veröffentlichens wäre folglich entbehrlich und ginge – sofern man von einer rechtlichen Gleichwertigkeit ausgehen mag[710] – wohl vollständig im Zugänglichmachen auf. Es machte somit keinen Unterschied, ob der Täter die Daten bloß einer anderen Person oder unzähligen Personen zur Kenntnis bringt. Abgrenzungsmerkmal der beiden Tathandlungen ist lediglich die Mindestpublizität, die sich an § 69 orientiert.[711] Dabei stellt die Formulierung »einem anderen zugänglich machen« auf das Zugänglichmachen für einen »konkreten Empfänger« ab. Ein konkreter Empfänger ist dabei eine ganz bestimmte Person. Das Zugänglichmachen stellt in diesem Fall einen Akt der »Individualkommunikation«[712] dar, bei der sich die Kommunizierenden mit der Identität des jeweiligen Gegenübers auseinandersetzen (müssen). Es kann sich also auch um die Weitergabe der Daten im privaten Umfeld des Täters handeln, ohne Öffentlichkeitswirkung. Paradebeispiel für das Zugänglichmachen für einen anderen ist die Übermittlung der Daten per E-Mail an einen konkreten Empfänger. A sendet B ein E-Mail, wobei A den B mittels dessen E-Mail-Adresse »individualisieren« muss. Der sprachliche Ausdruck »einem« ist nicht als Zahlwort, sondern als (unbestimmter) Artikel zu verstehen, und weist daraufhin, dass es sich um einen empfängerorientiert-konkreten Adressatenkreis handeln muss. Wird diese Personenanzahl iSd § 69 überschritten, liegt ein Veröffentlichen vor.

Die Nennung der beiden mit Außenwirkung beladenen Tathandlungen nebeneinander, indiziert aber, dass der Gesetzgeber beide Tathandlungen für unentbehrlich erachtet. So kann daraus – wie zu § 120 Abs 2a ausgeführt – gerade für den Datenschutz mit seiner Einbettung in den Schutz der Privatsphäre geschlossen werden, dass auch diese

709 Vgl ErlME 82/ME XXIV. GP, 8.
710 Siehe dazu krit gleich im Anschluss.
711 Siehe dazu insb die Ausführungen zu § 120 Abs 2a.
712 Zur Begrifflichkeit siehe auch *Gaderer* in Kucsko (Hrsg), urheber.recht § 18a Pkt 4.1 (Stand Dezember 2007).

beiden Tathandlungen unterschiedliche Wertigkeiten besitzen.[713] Den besonderen Wertvorstellungen des Datenschutzes Rechnung tragend, handelt es sich daher mE bezüglich aller Tathandlungen des § 51 DSG 2000 um ein kumulatives Mischdelikt.[714]

Eine Veröffentlichung von geheim zuhaltenden personenbezogenen Daten im Internet bzw für einen unbestimmten Empfängerkreis intensiviert die Rechtsgutbeeinträchtigung gegenüber dem Zugänglichmachen doch deutlich und stellt deshalb auch einen größeren sozialen Störwert dar.[715] In diese Richtung ist wohl auch der Wille des historischen Gesetzgebers zu interpretieren, wenn in den GMat ausgeführt wird, dass als Tathandlung die »Benützung sowie die Weitergabe von Daten, insbesondere ihre Veröffentlichung« unter Strafe gestellt werden solle.[716]

Gerade in Anbetracht moderner Informationstechnologie, ubiquitärer Daten und informationstechnischer Durchdringung steigt das Potential der Gefährdung bzw die Verletzung der Privatsphäre durch die Anzahl der Datenempfänger und Zugriffsmöglichkeiten unverhältnismäßig stark an.

Das Rechtsgut ist daher umso stärker beeinträchtigt, je mehr Personen das Tatobjekt zugänglich wird (insb einer sukzessiven Öffentlichkeit im Internet). Die Öffentlichkeit eines Verhaltens ist daher bereits dann anzunehmen, wenn keine Gewähr dafür besteht, dass die Daten nicht über einen relativ kleinen oder zumindest sehr geschlossenen und unter Geheimhaltungspflicht stehenden Kreis hinaus gelangt.[717] So schreibt auch *Jahnel,* dass die Prüfung der datenschutzrechtlichen Zulässigkeit einer Veröffentlichung von besonderer Bedeutung ist, weil die Konsequenzen gravierend seien.[718]

Zusammenfassend ist daher festzuhalten, dass die Zugänglichmachung der tatbildlichen Daten an bis zu 10 Personen noch unter die Tathandlung »einem anderen zugänglich machen« fällt, darüber hin-

713 AA *Salimi* in WK² DSG § 51 Rz 10, der – ohne nähere Begründung – die Tathandlungen des Zugänglichmachens und des Veröffentlichens als gleichwertig erachtet und somit diesbezüglich von einem alternativen Mischdelikt ausgeht.

714 Vgl *Bergauer,* ÖJZ 2013/113, 958.

715 Vgl *Bergauer,* ÖJZ 2013/113, 958.

716 Siehe ErlRV 1613 BlgNR XX. GP, 54.

717 In diesem Sinne LG Klagenfurt 10.01.2008, 7 Bl 121/07y = jusIT 2008/44, 95 *(Bergauer)*.

718 Vgl *Jahnel,* Handbuch, Rz 3/120.

aus liegt ein – was den sozialen Sinngehalt anlangt – ungleichwertiges Veröffentlichen vor.

Das Zugänglichmachen oder Veröffentlichen der Daten erfordert aber meist auch das Benützen durch den Täter selbst, um die Daten überhaupt erst, zB via E-Mail, versenden zu können oder zwecks Veröffentlichung auf eine Website zu stellen.

Aus all diesen Erwägungen ergibt sich durch die ausdrückliche Nennung dieser Begehungsweisen nebeneinander eine begriffliche Anlehnung an die abweichende Terminologie des Strafrechts, was zum Teil zu einer Vermischung von Rechtsbegriffen führt, die in den genannten Gesetzen (StGB bzw DSG 2000) auch unterschiedlich verstanden werden. Im Strafrecht versteht man unter »Veröffentlichen« prinzipiell das Zugänglichmachen für einen unbestimmten[719] bzw breiten[720] Personenkreis. Die Tathandlung des Zugänglichmachens ist, wie oben erwähnt, ohnedies bereits dem Strafrecht entnommen, und unter dem strafrechtsakzessorischen »Selbst-Benützen« ist wohl das »Verarbeiten« bzw »Gebrauchen« der Daten und daher jede Art der Handhabung von Daten[721] durch den Täter selbst gemeint.

Die unterschiedliche Bedeutung der Tathandlungen wird aber auch nicht vom ungleichen Datenbegriff des StGB bedingt. Zwar werden nach § 74 Abs 2[722] »Daten« iSd StGB viel weiter verstanden als im DSG 2000, da nicht nur personenbezogene, sondern auch nicht personenbezogene Daten sowie Programme darunter fallen, jedoch sind die tatsächlichen Verwendungsmodalitäten von Daten – zumindest in automationsunterstützt verarbeitbarer Form als Computerdaten – des DSG 2000 und von Daten im weiten Begriffsverständnis des Strafrechts kongruent. Die faktischen Handhabungsmöglichkeiten von Daten orientieren sich eben nicht an deren Inhalten[723]. Dass der Strafgesetzgeber nämlich grundsätzlich sehr wohl auf datenschutzrechtliche Terminologie zurückgreift, zeigen etwa im materiellen Strafrecht § 107a Abs 1 Z 3 und 4, aber auch §§ 74, 75 StPO.

---

719 Siehe zB *Lewisch/Reindl-Krauskopf* in WK² § 120 Rz 12 (Stand September 2008).

720 Siehe *Reindl-Krauskopf,* Computerstrafrecht², 27.

721 Was wiederum eher dem Verarbeiten von Daten iSd § 4 Z 9 DSG 2000 entsprechen würde, da das »einem Dritten Zugänglichmachen« oder »veröffentlichen« in der strafrechtlichen Terminologie gesondert betrachtet eher dem »Übermitteln von Daten« iSd § 4 Z 12 gleichkommt.

722 Siehe dazu *Jerabek/Reindl-Krauskopf/Schroll* in WK² § 74 Rz 64 bzw *Nittel* in SbgK § 74 Rz 177 (Stand November 2006).

723 Siehe zum Datenbegriff ausf S 60 ff.

Nicht nur in Anbetracht des Prinzips der Einheit der Rechtssprache, sondern gerade auch was die Rechtssicherheit anlangt, wäre eine konsequente Verfolgung einer einheitlichen Terminologie äußerst wünschenswert.

10. Subjektive Tatseite

Bezüglich sämtlicher objektiver Tatbestandsmerkmale des § 51 DSG 2000 wird Tatbildvorsatz im Mindeststärkegrad eines dolus eventualis gefordert.

Darüber hinaus ist das Delikt mit zwei alternativ zu erfüllenden überschießenden Innentendenzen ausgestattet, die § 51 DSG 2000 zu einem kumulativen Mischdelikt auf subjektiver Tatseite machen.[724] Dies bedeutet, dass faktisch zwei selbstständige Delikte mit demselben objektiven Tatbestand und derselben Strafdrohung unter § 51 DSG 2000 zusammengefasst wurden. Wie bereits eingangs zu dieser Bestimmung erwähnt, muss der Täter im Tatzeitpunkt entweder einen Bereicherungsvorsatz oder eine Schädigungsabsicht haben. Für den Bereicherungsvorsatz reicht dolus eventualis aus, die Schädigungsvariante verlangt Absicht iSd § 5 Abs 2. Es muss dem Täter gerade darauf ankommen, den Betroffenen in seinem Geheimhaltungsanspruch nach § 1 Abs 1 DSG 2000 zu schädigen. Die beiden alternativ vom Täter angestrebten Ziele müssen jeweils durch die Tathandlungen unmittelbar erreicht werden wollen (arg »dadurch«).[725]

11. Sonstiges

§ 51 DSG 2000 ist seit der DSG-Nov 2010 ein reines Offizialdelikt[726], das mit einer Subsidiaritätsklausel zu anderen Bestimmungen, die mit strengerer Strafe bedroht sind, ausgestattet wurde. Es fällt gem § 30 Abs 1 StPO in die sachliche Zuständigkeit des Bezirksgerichts.

724 Siehe *Bergauer,* ÖJZ 2013/113, 958.
725 Vgl auch *Salimi* in WK² DSG § 51 Rz 57 f.
726 Davor handelte es sich um ein Ermächtigungsdelikt.

C. Verletzung des Telekommunikationsgeheimnisses (§ 119)

> § 119 (1) Wer in der Absicht, sich oder einem anderen Unbefugten vom Inhalt einer im Wege einer Telekommunikation oder eines Computersystems übermittelten und nicht für ihn bestimmten Nachricht Kenntnis zu verschaffen, eine Vorrichtung, die an der Telekommunikationsanlage oder an dem Computersystem angebracht oder sonst empfangsbereit gemacht wurde, benützt, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.
>
> (2) Der Täter ist nur mit Ermächtigung des Verletzten zu verfolgen.[727]

Nach Art 3 CCC soll die widerrechtliche Überwachung von nicht öffentlichen Übertragungen von Computerdaten zu und von Computersystemen oder auch innerhalb eines solchen Systems pönalisiert werden. In Umsetzung dieser Vorgabe durch das StRÄG 2002 wurde die Strafbestimmung der »Verletzung des Fernmeldegeheimnisses« (§ 119 aF[728]) entsprechend adaptiert. Dabei wurde ua in Anbetracht der mittlerweile veralteten Terminologie auch auf die aktuelle Begrifflichkeit des Telekommunikationsgesetzes rekurriert.[729] Die Deliktsbezeichnung wurde auf »Verletzung des Telekommunikationsgeheimnisses« und die tatbildliche »Fernmeldeanlage«, die noch aus dem Fernmeldegesetz 1993[730] stammte, auf »Telekommunikationsanlage« und »Com-

727 BGBl 60/1974 idF I 56/2006.

728 In der Fassung BGBl 60/1974, die lautete:
§ 119 (1) Wer in der Absicht, sich oder einem anderen Unbefugten von einer durch eine Fernmeldeanlage übermittelten und nicht für ihn bestimmten Mitteilung Kenntnis zu verschaffen, eine Vorrichtung an einer Fernmeldeanlage anbringt oder sonst empfangsbereit macht, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.
(2) Ebenso ist zu bestrafen, wer eine Vorrichtung, die an einer Fernmeldeanlage angebracht oder sonst empfangsbereit gemacht worden ist, in der im Abs. 1 bezeichneten Absicht benützt.
(3) Der Täter ist nur auf Verlangen des Verletzten zu verfolgen. Wird die Tat jedoch von einem Beamten in Ausübung seines Amtes oder unter Ausnützung der ihm durch seine Amtstätigkeit gebotenen Gelegenheit begangen, so hat der öffentliche Ankläger den Täter mit Ermächtigung des Verletzten zu verfolgen.

729 Siehe ErlRV 1166 BlgNR XXI. GP, 25.

730 Fernmeldegesetz 1993, BGBl 908/1993: § 2 Z 2 »Fernmeldeanlage« alle technischen Anlagen zur Aussendung, zur Übertragung oder zum Empfang von Nachrichten, sei es auf dem Leitungs- oder Funkweg, auf optischem Wege oder mittels anderer elektromagnetischer Systeme.

putersystem« abgeändert. Wobei in der Fassung des § 119 nach dem StRÄG 2002[731] der Klammerausdruck nach Telekommunikation »(§ 3 Z 13 TKG)« noch einen ausdrücklichen Verweis auf das TKG[732] lieferte.[733] Mit dem BGBl I 56/2006 ist – spät, aber doch[734] – dieser Verweis entfallen, weshalb sich im aktuellen Gesetzeswortlaut[735] kein Bezug mehr auf das TKG findet.[736] In den GMat wird jedoch expressis verbis darauf hingewiesen, dass dadurch eine inhaltliche Änderung des Begriffes »Telekommunikation« nicht eintrete. Diese sei weiterhin als technischer Vorgang des Aussendens, Übermittelns und Empfangens von Nachrichten jeglicher Art in der Form von Zeichen, Sprache, Bildern oder Tönen mittels dazu dienender technischer Einrichtungen zu verstehen.[737] Aus technischer Sicht handelt es sich bei einer »Kommunikation« um den Austausch von Informationen (die ihrerseits wiederum Inhalte einer Nachricht sind). Von einer »Telekommunikation« spricht man, wenn solche Kommunikationen über beliebige Entfernungen stattfinden.[738]

Auch wurde anstelle der Tathandlungen des Anbringens oder Sonst-Empfangsbereitmachens einer Vorrichtung das »Benützen« einer derartigen Vorrichtung normiert, weshalb das Anbringen oder Sonst-Empfangsbereitmachen nach dem StRÄG 2002 keine eigene Strafbarkeit mehr begründet.[739] Zu Recht weist *Seling* darauf hin, dass die Rücknahme der Strafbarkeit in diesem Zusammenhang überrascht, wurde doch zu § 119 aF[740] noch vorgebracht, dass das Anbringen oder Empfangsbereitmachen von entsprechenden Vorrichtungen »objektiv besonders gefährlich« sei und es daher nötig und gerechtfertigt sei, schon für diese Handlungen eine Strafdrohung vorzusehen.[741]

731 BGBl I 134/2002.
732 TKG (1997), BGBl I 100/1997.
733 Siehe auch *Lewisch* in WK² § 119 Rz 5b (Stand September 2008).
734 § 3 TKG, auf den in § 119 StGB ausdrücklich referenziert wurde, ist zusammen mit dem gesamten TKG (1997) am 19.03.2003 außer Kraft getreten. Mit dem TKG 2003 (BGBl I 70/2003), das am 20.08.2003 in Kraft getreten ist, wird nun keine Legaldefinition von »Telekommunikation« mehr vorgenommen, weshalb das Klammerzitat nicht mehr zutreffend war.
735 BGBl I 134/2002 idF I 56/2006.
736 Siehe ErlRV 1325 BlgNR XXII. GP, 6.
737 Vgl ErlRV 1325 BlgNR XXII. GP, 6; weiters aber auch ErlRV 1505 BlgNR XXIV. GP, 6.
738 Siehe *Freyer,* Nachrichten-Übertragungstechnik⁶ (2009) 13.
739 Siehe dazu *Lewisch* in WK² § 119 Rz 3; weiters *Reindl,* E-Commerce, 162 (FN 509).
740 Vor dem StRÄG 2002, BGBl 60/1974.
741 Siehe *Seling,* Privatsphäre, 155; vgl auch ErlRV 30 BlgNR XIII. GP, 255.

Eine weitere markante Änderung ist in § 119 Abs 2 zu erkennen, da die ehemals als Privatanklagedelikt (Abs 3 aF) ausgestaltete Strafbestimmung mit dem StRÄG 2002 zu einem Ermächtigungsdelikt aufgewertet wurde.

Nunmehr pönalisiert § 119 ausschließlich das Benützen einer Vorrichtung, die an einer Telekommunikationsanlage oder an einem Computersystem angebracht oder sonst empfangsbereit gemacht wurde, um sich oder einem anderen Unbefugten vom Inhalt von im Wege einer Telekommunikation oder eines Computersystems übertragenen Nachrichten Kenntnis zu verschaffen.

1. Tatobjekt »Vorrichtung«

Unter »Vorrichtung« ist jedes technische Hilfsmittel (auch Computerprogramme[742]) zu verstehen, das dem Außenstehenden eine Kenntnisnahme über die Telekommunikationsanlage bzw über das Computersystem erlaubt.[743] Jedoch fallen nach hM nur Vorrichtungen darunter, die entweder speziell zum Spionagezweck hergestellt oder adaptiert wurden.[744] Dies stützt sich auf die GMat, nach denen nur solche Vorrichtungen erfasst sein sollen, die entweder speziell zu Abhörzwecken hergestellt oder zu solchen Zwecken adaptiert wurden.[745] Vorrichtungen, die a priori einem erlaubten Zweck dienen können oder überhaupt standardisiertes Softwarezubehör darstellen, sind demnach keine tauglichen Tatobjekte des § 119.[746]

742 Siehe unten zu § 126c bzw § 74 Abs 1 Z 8; weiters *Reindl-Krauskopf* in WK² § 119a Rz 4; ebenso *Thiele* in SbgK § 119 Rz 44 f (Stand März 2007); siehe auch Art 7 lit a des Vorschlags für eine Richtlinie des Europäischen Parlaments und des Rates über Angriffe auf Informationssysteme und zur Aufhebung des Rahmenbeschlusses 2005/222/JI des Rates, KOM (2010) 517 endg.

743 Siehe dazu *Lewisch* in WK² § 119 Rz 4 f.

744 Vgl *Reindl,* E-Commerce, 163 mwN; *Reindl-Krauskopf,* Computerstrafrecht², 29; insb auch *Thiele* in SbgK § 119 Rz 46 mwN; weiters *Lewisch* in WK² § 119 Rz 4a mwN.

745 Siehe ErlRV 30 BlgNR XIII. GP, 255; vgl dazu auch *Leukauf/Steininger,* StGB³ § 119 Rz 12.

746 Siehe zu diesem Problem auch die krit Auseinandersetzung mit den Tatobjekten des § 126c Abs 1 Z 1 (S 321 ff) bzw *Bergauer,* Kritische Anmerkungen zu § 126c StGB, ÖJZ 2007/45, 532; weiters *Thiele* in SbgK § 119 Rz 46.

So sind etwa das Abhören von Funkverkehr mittels eines gewöhnlichen Radioapparats oder das Mithören fremder Gespräche infolge bloßer Fehlschaltungen von Telefonen nicht tatbildlich.[747] Dass überhaupt »Vorrichtungen« verlangt werden, ist nachvollziehbar und auch zweckmäßig, wenn dadurch eine zu weitgehende Kriminalisierung verhindert wird.[748] Doch mE führt diese zu massive Strafbarkeitsbeschränkung insb in den Fällen, in denen der Täter Standard-Komponenten der Betriebssystemsoftware als eine derartige Vorrichtung benützt, die eben nicht explizit für tatbildliche Spionagehandlungen geschaffen oder adaptiert wurde, zu kriminalpolitisch unerwünschten Ergebnissen. Personen, die zur Datenspionage Standard-Programme verwenden, welche im Lieferumfang von Betriebssystemen enthalten sind[749], machen sich – mangels Verwendung einer deliktsspezifischen Vorrichtung – nicht strafbar. Auch die Verwendung eines herkömmlichen Netzwerkadapters, der in einen entsprechenden Empfangsmodus gesetzt wurde (sog »Promiscuous Mode«), ermöglicht den Empfang von nicht an dieses Computersystem adressierten Datenpaketen auf einer konkreten Netzwerkebene innerhalb eines LAN. Daher könnte das System des »Täters« in die Lage versetzt werden, den gesamten ankommenden Datenverkehr an der Netzwerkschnittstelle innerhalb eines konkreten Netzwerksegments (zB Subnet) aufzufangen.[750] Soll ein WLAN[751]-Adapter zur Datenspionage Verwendung finden, so muss dieser – im Gegensatz zum Promiscuous Mode, der lediglich auf das konkret verbundene Netzwerk beschränkt bleibt – im sog »Monitor Mode«[752] betrieben werden, um alle am Adapter ankommenden »Frames«[753] eines beliebigen WLAN aufzeichnen zu können.[754]

---

747 Siehe ErlRV 30 BlgNR XIII. GP, 255; weiters JAB 959 BlgNR XIII. GP, 25; vgl *Lewisch* in WK² § 119 Rz 4a.

748 Siehe dazu auch ER (ETS 185) Pkt 53.

749 Wie etwa das Programm »Telnet«, das eine netzwerkfähige Terminalemulation ermöglicht, die ein lokales Terminal (zB den Computer des Täters) in die Lage versetzt, einen entfernten Rechner so zu bedienen, als säße man selbst direkt davor (siehe dazu ua *Hein/Reisner,* TCP/IP – Ge-packt² [2004] 312 f).

750 Siehe dazu genauer *Bergauer,* RdW 2006/391, 412.

751 Wireless Local Area Network.

752 Zur Funktionsweise siehe *Dhanjani/Clarke,* Network Security Tools (2005) 262.

753 »Ethernet- bzw WLAN-Frames«; darunter versteht man Datenpakete auf Netzwerkebene siehe *Kersken,* IT-Handbuch⁵, 197; auch *Hunt,* TCP/IP. Netzwerk-Administration³ (2002) 10.

754 Siehe dazu *Rey/Thumann/Baier,* Mehr IT-Sicherheit durch Pen-Tests (2005) 170.

Eine Netzwerkschnittstelle oder der implementierte Empfangsmodus sind aber nicht für widerrechtliche Abhörzwecke geschaffen worden und dienen nicht ausschließlich illegalen Zwecken.[755] Aus diesem Grund verneint *Lewisch* auch die Deliktstauglichkeit von WLAN-Adaptern zur Datenspionage, da sie lediglich »allgemeine Zugangsschlüssel« für diese Übertragungstechnik darstellen.[756]

Bezüglich des WLAN-Adapters ist zudem anzumerken, dass dieser – selbst wenn er in den entsprechenden Empfangsmodus gesetzt wurde – nicht an einem Computersystem (oder an einer Telekommunikationsanlage) »angebracht« wird[757], da im Unterschied zu kabelgebundenen Netzwerken eine physische Verbindung mit dem Netzwerk nicht hergestellt wird.[758]

Viel eher wird dies vom Auffangbegriff des »Sonst-Empfangsbereitmachens« erfasst sein.

Eine Vorrichtung wird angebracht, wenn eine »mechanische Verbindung« zwischen der Vorrichtung und der Telekommunikationsanlage oder dem Computersystem hergestellt wird.[759] Aufgrund des Wortlauts, dass die Vorrichtung »an der Telekommunikationsanlage oder an dem Computersystem angebracht« sein muss, stellt sich die Frage, ob davon Software-Vorrichtungen (zB Keylogger-Programme), die »in« einem Computersystem implementiert sind, ebenfalls erfasst werden. Davon zu unterscheiden sind wiederum »Hardware-Keylogger«, die an externen Schnittstellen – wie handelsüblichen Peripheriegeräten bzw zwischen[760] externen Geräten und dem Zielcomputer – angeschlossen werden. Nur solche werden aber wohl als Vorrichtung an einem Computersystem physisch angebracht. Im Fall eines implementierten unkörperlichen Schnüffelprogramms wird man dann wohl vom »Sonst-Empfangsbereitmachen« ausgehen müssen, da keine »mecha-

755 In erster Linie sind derartige Modi für Test- und Analysezwecke implementiert.

756 Siehe *Lewisch* in WK² § 119 Rz 4a; aA *Lichtenstrasser/Mosing/Otto,* ÖJZ 2003/14, 253; in Bezug auf »WarDriving« eine Strafbarkeit auch eher bejahend *Thiele* in SbgK § 119 Rz 54.

757 Wird allerdings ein Computersystem des Täters, das zum Aufzeichnen des Netzwerkverkehrs ausgestattet ist (zB Packet-Sniffer), physisch an einen Netzwerkknotenpunkt (zB Switch, Router) des Zielnetzwerks angeschlossen, so kann man vom »Anbringen« der tatbestandlichen Vorrichtung an einem Computersystem sprechen.

758 Siehe dazu *Thiele* in SbgK § 119 Rz 49.

759 Vgl ErlRV 30 BlgNR XIII. GP, 255.

760 ZB zwischen Tastaturanschlussstecker und PC-Schnittstelle.

nische« – wohl aber zumindest virtuelle – Verbindung zum konkret zu überwachenden Computersystem vor Ort hergestellt wird.[761]

Unter Empfangsbereitmachen der Vorrichtung ist die Herstellung eines Zustandes zu verstehen, der es dem Täter »unverzüglich ermöglicht, die Vorrichtung zu dem verpönten Zweck zu benützen«.[762] Beispielsweise kann eine Vorrichtung, ohne unmittelbare Verbindung zur Telekommunikationsanlage oder zum Computersystem, in einen Zustand gebracht werden, in dem sie das Telekommunikations- bzw Übertragungsgeheimnis verletzen kann.[763]

Das bloße Aufbewahren einer deliktsspezifischen Vorrichtung ist noch nicht erfasst, solange sie nicht einsatzbereit gemacht wurde.[764] Wird bspw ein Hardware-Sniffer an einem Computersystem angebracht, der jedoch erst in einem weiteren Schritt zur Datenaufzeichnung per Softwareansteuerung aktiviert werden muss, so stellt sich die Frage, ob das »Benützen« einer bereits angebrachten, aber noch nicht empfangsbereit gemachten Vorrichtung überhaupt von der Tathandlung des § 119 erfasst ist. Liegt die »Benützung des Sniffers« nun darin, diesen erst bloß zur Kenntniserlangung der Mitteilungen zu aktivieren, so benützt der Täter keine »empfangsbereite, angebrachte« Vorrichtung, sondern eine, die bloß angebracht wurde. Aus der Formulierung »oder sonst empfangsbereit gemacht« ergibt sich nämlich, dass auch die »angebrachte« Vorrichtung bereits empfangsbereit sein muss. Das alleinige Aktivieren, Empfangsbereitmachen bzw Einschalten einer bereits angebrachten tatbestandlichen Vorrichtung, ist daher grundsätzlich[765] noch eine straflose Vorbereitungshandlung zu § 119.

Dem Wortlaut des Tatbestands zufolge geht der Gesetzgeber aber ganz offensichtlich davon aus, dass mit dem Anbringen einer Vorrichtung, diese auch zwangsläufig bereits empfangsbereit ist.[766] Die angesprochene Formulierung »sonst empfangsbereit« deutet grundsätzlich

761 Vgl ErlRV 30 BlgNR XIII. GP, 255.
762 Vgl ErlRV 30 BlgNR XIII. GP, 255.
763 ZB bei der Verwendung von Richtstrahlern, die nur räumlich an das Strahlenbündel der Ferngespräche herangebracht werden müssen; siehe ErlRV 30 BlgNR XIII. GP, 255.
764 Siehe ErlRV 30 BlgNR XIII. GP, 255.
765 In den Fällen aber, in denen mit der Aktivierung gleichzeitig auch die Kenntnisverschaffungsmöglichkeit der Mitteilungen ohne weiteren Zwischenschritt gegeben ist, liegt in der Aktivierung nun bereits eine ausführungsnahe Handlung (siehe in diese Richtung auch *Reindl-Krauskopf* in WK² § 119a Rz 3).
766 Diese Formulierung findet sich bereits in der StF des § 119 (BGBl 60/1974).

auf einen Auffangbegriff bezogen auf »angebracht« hin[767], doch schließt dieser mE jenen bereits in sich ein, da auch eine angebrachte Vorrichtung bereits empfangsbereit sein muss. Es spielt daher für eine Strafbarkeit nach § 119 keine Rolle, ob eine empfangsbereite, angebrachte Vorrichtung vom Täter benützt wird oder ob dieser eine andere Vorrichtung verwendet, die ohne physische Verbindung zum Zielsystem bereits empfangsbereit ist. Es handelt sich vielmehr (mittlerweile) um eine vermeidbare Redundanz, die aus der historischen Zweiteilung der Tathandlung herrührt, in der noch das Anbringen oder Sonst-Empfangsbereitmachen (Abs 1) neben dem Benützen (Abs 2) der Vorrichtung selbstständig strafbar war.[768] Ein tatbestandliches Abstellen auf eine Vorrichtung, die lediglich empfangsbereit gemacht wurde, reicht zur Erfassung sämtlicher intendierter verpönter Handlungen völlig aus.

Das bloße Anbringen einer Vorrichtung ist grundsätzlich[769] noch als straflose Vorbereitungshandlung zu beurteilen.[770] Wer die Vorrichtung angebracht hat, ist gleichgültig.[771] Es ist für eine Strafbarkeit nach § 119 nicht erforderlich, dass die Vorrichtung unberechtigterweise angebracht oder sonst empfangsbereit gemacht wurde. Auch das Benützen einer ursprünglich rechtmäßig zur Kommunikationsüberwachung angebrachten oder sonst empfangsbereiten Vorrichtung in der entsprechenden inkriminierten Absicht ist von § 119 erfasst.[772]

Nach der alten Rechtslage (§ 119 aF[773]) war neben dem Benützen (Abs 2) einer inkriminierten Vorrichtung auch das Anbringen oder Sonst-Empfangsbereitmachen (Abs 1) einer solchen ausdrücklich und selbstständig unter Strafe gestellt. Dies mit der Begründung, dass »die bezeichneten Verhaltensweisen [Anm: Anbringen und Empfangsbe-

767 Siehe *Thiele* in SbgK § 119 Rz 49.

768 Siehe § 119 idF BGBl 60/1974.

769 Doch beachte man §§ 118a und § 126c, aus denen sich dennoch eine Strafbarkeit ergäben könnte.

770 Siehe ErlRV 1166 BlgNR XXI. GP, 26; aA offensichtlich *Lewisch* in WK² § 119 Rz 5a und *Hinterhofer,* Geheimnisschutz, 172, die auch das »Anbringen einer Vorrichtung« zur Kenntniserlangung von E-Mails unter § 119 subsumieren. *Lewisch* verweist dabei auch auf *Reindl-Krauskopf* in WK² § 119a Rz 4, doch ist dort nichts dergleichen zu finden. Vielmehr ist *Reindl-Krauskopf* – aber dem entgegengesetzt – zuzustimmen, wenn sie ausdrücklich erklärt: »Das Anbringen und/oder Empfangsbereitmachen der Abhöreinrichtung alleine bewirkt noch keine Strafbarkeit.«

771 Siehe dazu ErlRV 1166 BlgNR XXI. GP, 26; ebenso *Bertel/Schwaighofer,* BT I¹² § 119 Rz 2.

772 Siehe ErlRV 30 BlgNR XIII. GP, 256.

773 BGBl 60/1974.

reitmachen] aber technisch an die Ausführung der Tat heranreichen, diese jederzeit möglich machen und damit objektiv besonders gefährlich sind«.[774] Da diese »Vorbereitungshandlungen« – wie oben ausgeführt – nicht mehr selbstständig strafbar sind, fragt sich, ob sich an der expressis verbis in den GMat erwähnten »besonderen Gefährlichkeit« dieser Handlungen inzwischen etwas geändert hat. Offensichtlich wurde die Anhebung der Strafbarkeitsschwelle durch Art 3 CCC inspiriert, da dort keine Strafbarkeit für das bloße Anbringen oder Sonst-Empfangsbereitmachen vorgesehen ist. Gleichwohl liefe es aber der CCC nicht zuwider, würde der Gesetzgeber einen höheren Schutz, dh auch für die Vorbereitungshandlungen, vorsehen, da sich die Intention der Konvention nur auf ein gewisses Mindestschutzniveau bezieht.[775] Dass sowohl in Echtzeit arbeitende Vorrichtungen als auch Aufnahmegeräte bzw -programme tatbildlich sind, ergibt sich aus dem Wortlaut des § 119, in dem lediglich auf die Benützung einer Vorrichtung zur Kenntnisverschaffung von Nachrichten abgestellt wird. Ob sich nun der Täter in Echtzeit Kenntnis verschaffen will oder ob er dies erst durch einen späteren Abruf einer Aufzeichnung tun möchte, ist unbeachtlich. Auch die CCC gibt zu dieser Auslegung Anlass, da im ER (ETS 185) iZm den »technischen Mitteln« von einer direkten oder indirekten Kenntnisnahme gesprochen wird und dabei expressis verbis angemerkt wird: »Interception may also involve recording«.[776] Unter Aufzeichnen versteht man das nicht bloß flüchtige Festhalten einer Nachricht auf einem Trägermedium.[777]

2. Benützen einer Vorrichtung

Das Benützen einer Vorrichtung verlangt das tatsächliche Verwenden derselben.[778] Dazu ist aber festzuhalten, dass nur das Benützen der Vorrichtung zu dem verpönten Zweck der Kenntnisverschaffung gemeint

774 Siehe ErlRV 30 BlgNR XIII. GP, 255.

775 Siehe *Seling,* Privatsphäre, 156; vgl auch *Plöckinger,* Internet und materielles Strafrecht – Die Convention on Cyber-Crime, in Plöckinger/Duursma/Helm (Hrsg), Aktuelle Entwicklungen im Internet-Recht (2002) 113 (113).

776 Siehe ER (ETS 185) Pkt 53; vgl auch *Lewisch* in WK² § 119 Rz 5; ebenso *Thiele* in SbgK § 119 Rz 44.

777 Siehe *Lewisch/Reindl-Krauskopf* in WK² § 120 Rz 31b; weiters *Thiele* in SbgK § 120 Rz 57 (Stand Mai 2010).

778 Siehe *Lewisch* in WK² § 119 Rz 7.

sein kann. Die sozial inadäquate Gefährlichkeit der Handlung lässt sich daher nur aus dem Tatbildvorsatz samt überschießender Innentendenz feststellen. Das »Benützen« der Vorrichtung für andere Zwecke, wie bspw die Kontaktaufnahme des Täters mit seiner Schnüffelsoftware über ein Netzwerk, die bis dahin noch nicht mit der Nachrichtenerfassung begonnen hat[779] oder das bloße Empfangsbereitmachen einer Vorrichtung (im Vorfeld des Versuchsstadiums), ist freilich nicht erfasst.[780] Unter dem Benützen einer Vorrichtung ist jedes tatsächliche Gebrauchen zu Abhör- bzw Aufzeichnungszwecken einer konkreten Kommunikation bzw Übertragung zu verstehen. Da das bloße Benützen der Vorrichtung zur Datenspionage für eine Strafbarkeit bereits ausreicht, stellt § 119 Abs 1 tatbestandlich betrachtet ein schlichtes Tätigkeitsdelikt dar.

3. Subjektive Tatseite

Auf der inneren Tatseite ist neben dem (zumindest bedingten) Tatbildvorsatz noch ein erweiterter Vorsatz gefordert, der sich im Stärkegrad der Absichtlichkeit (iSd § 5 Abs 2) auf die Kenntnisverschaffung richten muss (Spionageabsicht). Der Gesetzgeber hat in diesem Zusammenhang zur Wahrung des bestehenden Geheimnisschutzes von der Möglichkeit der Beschränkung der Strafbarkeit mittels eines »dishonest intent« nach Art 3 CCC Gebrauch gemacht.[781]

Wegen des höheren Schutzbedürfnisses hins Nachrichteninhalte wird in § 119 die überschießende Innentendenz dahingehend ausgestaltet, dass der Täter – im Gegensatz etwa zu § 119a – lediglich in der Absicht handeln muss, sich oder einem anderen Unbefugten Kenntnis zu verschaffen. Was die Kenntnisverschaffung von allen anderen Daten iSd § 119a betrifft, wird dadurch, dass vom Täter in subjektiver Hinsicht mehr verlangt wird, die Schwelle zur Strafbarkeit deutlich angehoben.[782] Der Inhalt des erweiterten Vorsatzes zeigt – bei beiden Delikten – eine Vorverlagerung des Rechtsgüterschutzes an, da es in Wahrheit nicht um das Benützen einer Vorrichtung geht, sondern im Fall des § 119 Abs 1 um das Kenntnisverschaffen von Nachrichteninhalten.[783]

779 ZB will der Täter diesen noch entsprechend parametrisieren, um die richtigen Datenpakte in weiterer Folge dann abzufangen.
780 Vgl dazu auch ErlRV 1166 BlgNR XXI. GP, 26.
781 Siehe ErlRV 1166 BlgNR XXI. GP, 26; weiters ErlStV 1645 BlgNR XXIV. GP, 4.
782 Siehe zum erweiterten Vorsatz des § 119a siehe S 214 f.
783 Vgl auch *Schmölzer,* ZStW 2011/123, 709 (729).

Da die Kenntniserlangung der Daten einen über den objektiven Tatbestand hinausreichenden vom Täter lediglich anvisierten Erfolg darstellt, der außerhalb des objektiven Tatbestands angesiedelt ist und für die formelle Vollendung des Delikts gar nicht eintreten muss, kann man unter Einbeziehung dieser überschießenden Innentendenz bei § 119 Abs 1 von einem kupierten Erfolgsdelikt ausgehen.

a. »Subjektives Bezugsobjekt« und Schutzobjekt

»Bezugsobjekt des erweiterten Vorsatzes« und daher auch Schutzobjekt der Bestimmung ist der »Inhalt einer Nachricht«.[784] Der Terminus »Schutzobjekt« wird zwar – offenbar traditionell – von einem Teil der Rsp[785] und Lehre[786] mit Rechtsgut gleichgesetzt[787], doch ist die Bezeichnung mE durchaus geeignet, den geschützten Gegenstand eines Delikts zu umschreiben, der nicht das Tatobjekt (= ein Gegenstand der Außenwelt[788]) – an dem oder mit Bezug auf den die Tathandlung verwirklicht wird[789] –, aber auch nicht das rein ideelle Rechtsgut erfasst, sondern das »abstrakte Angriffsobjekt« eines Tatbilds.[790] Im hier gegenständlichen Fall ist nämlich die tatbestandliche »Vorrichtung« Tatobjekt, diese verkörpert aber weder das Rechtsgut, noch gilt ihr das Schutzanliegen. Das »geschützte Objekt« der Bestimmung ergibt sich nun lediglich aus dem erweiterten Vorsatz, denn dieser fokussiert auf den »Inhalt einer Nachricht« als Bezugsobjekt und unterscheidet sich wiederum deutlich vom rein abstrakten Rechtsgut des »Kommunikations- bzw Übertragungsgeheimnisses«.

---

784 Ungenau daher *Birklbauer/Hilf/Tipold,* Strafrecht BT I² §§ 119, 119a, 120 Abs 2a Rz 8, wenn sie dabei (generell) von »Nachrichten« sprechen.

785 Vgl OGH 11.01.1983, 10 Os 159/82.

786 Zur Problematik des Begriffes »Schutzobjekt« instruktiv *Triffterer,* AT², 46 f.

787 Siehe *Leukauf/Steininger,* Kommentar zum österreichischen StGB³ (1992) Vorbem § 1 Rz 47; auch *Triffterer,* AT², 46 mwN, der die synonyme Verwendung dieser Begriffe aber insoweit kritisiert, als der Wortteil »Objekt« eine Realitätsnähe suggeriere, die bei rein abstrakten Rechtsgütern nicht vorhaben sei.

788 Vgl *Kienapfel/Höpfel/Kert,* AT¹⁴ Z 10 Rz 2.

789 Siehe OGH 11.01.1983, 10 Os 159/82; dazu auch *Leukauf/Steininger,* StGB³ Vorbem § 1 Rz 47.

790 Mit Bezugnahme auf das Schrifttum siehe dazu auch *Leukauf/Steininger,* StGB³ Vorbem § 1 Rz 47.

b. Nachrichten

Art 3 CCC liefert hins des Nachrichtenbegriffs keine derartige Vorgabe, da dieser lediglich von »non-public transmissions of computer data« spricht. Art 1 lit b CCC versteht unter Computerdaten »any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function« Da jedoch § 119a auf alle von der CCC fokussierten Daten abstellt, wird den Verpflichtungen aus der CCC nur durch das Normenpaket §§ 119 und 119a gehörig Rechnung getragen. Die CCC will lediglich ein Mindestschutzniveau[791] sicherstellen, weshalb es auch den Vertragsstaaten unbenommen bleibt, strengere Schutzmaßnahmen, wie etwa für den Bereich der Inhaltsdaten, vorzusehen. Doch ist § 119 historisch betrachtet nicht (nur) die Reaktion auf internationale Vorgaben, sondern rekurriert bereits seit seiner Stammfassung[792] auf die verfassungsrechtliche Grundlage des Art 10a StGG[793].[794] Zweck des Art 10a ist der Schutz aller »nicht für die Öffentlichkeit bestimmten, im Wege des Fernmeldeverkehrs übermittelten Nachrichten oder Mitteilungen«.[795] Daher werden von Art 10a StGG jedenfalls Inhaltsdaten geschützt. Ob darüber hinaus auch Verkehrsdaten erfasst sind, ist strittig. Nach der überwiegenden verfassungsrechtlichen Lehre sind die Daten, die den Informationsverkehr betreffen, außerhalb des Schutzbereichs angesiedelt[796], wobei erst jüngst der VwGH in einem obiter dictum den Anwendungsbereich auch auf

791 Siehe *Plöckinger* in Plöckinger/Duursma/Helm, Aktuelle Entwicklungen, 113 (113).

792 Siehe dazu die Fassung BGBl 60/1974.

793 RGBl 142/1867 verfassungsrechtlich verankert mit BGBl 8/1974.

794 Strafrechtliches und grundrechtliches Rechtsgut sind im Kern identisch, weshalb die Erl zu Art 10a StGG ausdrücklich einladen, für dessen Auslegung auch die GMat zu § 119 StGB heranzuziehen; siehe *Wiederin* in Korinek/Holoubek (Hrsg), Bundesverfassungsrecht. Bd III Art 10a StGG Rz 12 (Stand 2001).

795 Siehe JAB 960 BlgNR XIII. GP, 2.

796 Siehe dazu *Berka,* Verfassungsrecht[5], Rz 1428; weiters *Wessely,* Das Fernmeldegeheimnis – ein unbekanntes Grundrecht?, ÖJZ 1999, 491; auch *Wiederin* in Korinek/Holoubek, Bundesverfassungsrecht Art 10a StGG Rz 12 mwN; jüngst auch VfGH 29.06.2012, B 1031/11; siehe die Meinungen zusammenfassend auch *Kalteis,* Polizeiliche Ermittlung von IP-Adressen nur mit richterlicher Genehmigung?, ZfV 2013/246, 184.

Verkehrsdaten erstreckt sieht.[797] Die hM im Strafrecht sieht jedenfalls Verkehrsdaten als davon mitumfasst an.[798]

Bereits in den GMat[799] der historischen Fassung[800] wird ausdrücklich angeregt, die Terminologie an die Begrifflichkeiten des damaligen Fernmeldegesetzes[801] anzupassen. Obwohl der Strafgesetzgeber seither in den unterschiedlichen Fassungen dieser Bestimmung stets auf das TKG expressis verbis Bezug genommen hat und die Definition der »Telekommunikation« noch iS dieser historischen Definition des TKG verstanden wissen will, definiert er den Begriff »Inhalt einer Nachricht« im deliktsspezifischen Zusammenhang völlig autonom, als die »Vermittlung von Gedankeninhalten«.[802] Diese Begriffsbestimmung entspricht im Wesentlichen dem technischen Verständnis aus der Nachrichten-Übertragungstechnik, wo der Inhalt einer Nachricht als »Information« bezeichnet wird.[803]

Auf den ersten Blick lassen die Anführungszeichen im ersten Satz der Erl[804] »Wie schon derzeit in § 102 TKG soll Schutzobjekt der Inhalt von ›Nachrichten‹ sein. Darunter wird – wie auch im aktuell verwendeten Begriff der ›Mitteilung‹ – die Vermittlung von Gedankeninhalten zu verstehen sein« den Eindruck entstehen, dass sich der zweite Satz auf diesen hervorgehobenen Begriff der Nachrichten bezieht. Richtig ist aber, dass diese nähere Beschreibung dem Begriff »Inhalt von Nach-

797 Vgl VwGH 27.05.2009, 2007/05/0280; siehe aber auch in diese Richtung der Lit *Damjanovic/Holoubek/Kassai/Lehofer/Urbantschitsch,* Handbuch des Telekommunikationsrechts (2006) 243.

798 Siehe grundlegend *Schmölzer,* Prozessuale Zwangsmittel im Fernmeldewesen – Beschlagnahme oder Überwachung, RZ 1988, 247; *Schmölzer,* Rückwirkende Überprüfung von Vermittlungsdaten im Fernmeldeverkehr, JBl 1997, 211; weiters *Schmölzer/Mayer-Schönberger,* Das Telekommunikationsgesetz 1997 – Ausgewählte rechtliche Probleme, ÖJZ 1998, 378; weiters *Reindl,* Telefonüberwachung zweimal neu?, JBl 2002, 69; *Reindl,* Die nachträgliche Offenlegung von Vermittlungsdaten des Telefonverkehrs im Strafverfahren (»Rufdatenrückerfassung«), JBl 1999, 791; siehe zusammenfassend auch *Reindl-Krauskopf/Tipold/Zerbes* in WK-StPO § 134 Rz 28 mwN (Stand Oktober 2009); Als Beispiele für die Rsp sind OGH 17.06.1998, 13 Os 68/98; OGH 06.12.1995, 13 Os 161/95 zu nennen.

799 Vgl ErlRV 30 BlgNR XIII. GP, 255.

800 § 401 StG-Entwurf des Jahres 1912 diente zunächst als Vorbild des § 119 aF (siehe dazu ErlRV 30 BlgNR XIII. GP, 255; weiters *Thiele* in SbgK § 119 Rz 1 f).

801 FG (StF: BGBl 170/1949) wurde vom FernmeldeG 1993 (StF: BGBl 908/1993) abgelöst, dieses wiederum durch das TKG (1997) (BGBl I 100/1997) außer Kraft gesetzt, und selbiges in weiterer Folge ebenso durch das TKG 2003 (BGBl I 71/2003).

802 Siehe ErlRV 1166 BlgNR XXI. GP, 26; *Leukauf/Steininger,* StGB[3] § 119 Rz 3.

803 Vgl *Freyer,* Nachrichten-Übertragungstechnik[6], 13.

804 Vgl ErlRV 1166 BlgNR XXI. GP, 26 mit Bezug auf *Leukauf/Steininger,* StGB[3] § 119 Rz 3.

richten« gilt und es sich beim »Inhalt einer Nachricht« ausschließlich um den zur Übertragung bestimmten, vom Sender intendierten Gedankeninhalt (= Information) handelt.

Klargestellt wird darüber hinaus, dass der Schutz nicht einem etwaigen zu bewahrenden Geheimnis gilt, das im Inhalt einer Nachricht liegen mag, sondern einer unbeobachteten und unabgehörten Kommunikation im Wege einer Telekommunikation oder eines Computersystems.[805] Zentrales Element ist daher die Vertraulichkeit jedes Inhalts während einer technischen Kommunikation.[806] Dies wird auch im ER (ETS 185)[807] expressis verbis so verstanden: »The term ›non-public‹ qualifies the nature of the transmission (communication) process and not the nature of the data transmitted.«

c. Inhalt einer Nachricht

In den GMat wird ausdrücklich[808] darauf hingewiesen, dass der »Inhalt einer Nachricht« im kernstrafrechtlichen Begriffsverständnis anders definiert werde, als es im TKG 2003 der Fall ist. Im TKG 2003 werden – im Gegensatz zum StGB – die Begriffe »Inhaltsdaten« (§ 92 Abs 3 Z 5 TKG 2003) und »Nachricht« (§ 92 Abs 3 Z 7 TKG 2003) legaldefiniert, wobei diese Begriffsbestimmungen – trotz der thematischen Nähe des § 119 zum TKG – für das strafrechtliche Verständnis ungeeignet sind.

Der – terminologisch wohl in erster Linie naheliegende – Begriff der »Inhaltsdaten« verweist in seiner Definition des § 92 Abs 3 Z 5 TKG 2003 auf Nachrichten nach Z 7, die lautet: »›Inhaltsdaten‹ die Inhalte übertragener Nachrichten (Z 7)«. Mit dem Rückgriff auf diese Begrifflichkeit wäre zwar die Ausgrenzung der äußeren Kommunikationsdaten als Bestandteil der telekommunikationsrechtlichen Nachricht realisiert, nicht aber die dadurch verbleibende Lücke, was »private« und nicht gewerbliche Übertragungen und entsprechende Dienstleistun-

805 Siehe *Reindl-Krauskopf,* Computerstrafrecht², 30; auch *Hinterhofer,* Geheimnisschutz, 172; siehe idS auch für Deutschland *Gercke/Brunst,* Praxishandbuch Internetstrafrecht (2009) 71; zu Art 10a StGG auch *Wiederin* in Korinek/Holoubek, Bundesverfassungsrecht Art 10a StGG Rz 3.

806 Siehe zu Art 10a StGG *Wiederin* in Korinek/Holoubek, Bundesverfassungsrecht Art 10a StGG Rz 3; *Reindl-Krauskopf* spricht idZ vom »Übertragungsgeheimnis« (siehe *Reindl-Krauskopf,* Computerstrafrecht², 29).

807 Vgl ER (ETS 185) Pkt 54.

808 Siehe ErlRV 1166 BlgNR XXI. GP, 26.

gen anlangt, die als Dienste der Informationsgesellschaft (§ 1 Abs 1 Z 2 NotifG 1999[809]) zu qualifizieren sind.

Folglich sind nach telekommunikationsrechtlichem Verständnis nur jene »Inhaltsdaten« erfasst, die in Form von »Nachrichten« iSd TKG 2003 übermittelt werden. Die Legaldefinition von Nachrichten nach § 92 Abs 3 Z 7 TKG 2003 (wortgleich mit Art 2 RL 2002/58/EG)[810] lautet nunmehr:

> ›Nachricht‹ jede Information, die zwischen einer endlichen Zahl von Beteiligten über einen öffentlichen Kommunikationsdienst ausgetauscht oder weitergeleitet wird. Dies schließt nicht Informationen ein, die als Teil eines Rundfunkdienstes über ein Kommunikationsnetz an die Öffentlichkeit weitergeleitet werden, soweit die Informationen nicht mit dem identifizierbaren Teilnehmer oder Nutzer, der sie erhält, in Verbindung gebracht werden können;

Nach ErwG 15 RL 2002/58/EG und der damit verbundenen richtlinienkonformen Interpretation des TKG 2003 kann eine Nachricht daher alle Informationen über Namen, Nummern oder Adressen einschließen, die der Absender einer Nachricht oder der Nutzer einer Verbindung für die Zwecke der Übermittlung der Nachricht bereitstellt. In diesem Sinn ist davon auszugehen, dass nicht nur der Inhalt (sog »Body«) eines E-Mails[811], sondern auch weitere Meta-Daten, wie zB die Informationen im E-Mail-Header[812], als Teil der Nachricht zu werten sind. Daher wäre eine Gleichsetzung des »Geheimnisumfangs« von § 119 und § 93 Abs 1 TKG 2003[813] (Kommunikationsgeheimnis) unzutreffend.[814]

---

809 Notifikationsgesetz 1999, BGBl I 183/1999.

810 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, ABl L 2002/201, 37.

811 Übermittlungen auf Basis des »Simple Mail Transfer Protocols« (SMTP) nach den entsprechenden Requests for Comments (zB RFC 821 für SMTP, RFC 822 [aktualisiert durch RFC 2822, und RFC 5322] für das E-Mail-Format).

812 Sog »Briefkopf« siehe zum Aufbau eines E-Mails *Balzert,* Lehrbuch², 41 f; weiters *Kersken,* IT-Handbuch⁵, 263.

813 § 93 Abs 1 TKG 2003: »Dem Kommunikationsgeheimnis unterliegen die Inhaltsdaten, die Verkehrsdaten und die Standortdaten. Das Kommunikationsgeheimnis erstreckt sich auch auf die Daten erfolgloser Verbindungsversuche«.

814 Siehe dazu ausdrücklich OGH 13.04.2011, 15 Os 172/10y (15 Os 173/10w) = jusIT 2011/44, 93 *(Karel)* = MR 2011, 153 *(Hasberger)* = JBl 2011, 726 *(Reindl-Krauskopf)*.

Mit anderen Worten, die telekommunikationsrechtliche Definition der »Inhaltsdaten« erfasst zwar – wie auch die strafrechtliche Umschreibung des »Inhalts einer Nachricht« – die reine Information, die zwischen den Kommunikationsteilnehmern ausgetauscht wird, doch ergibt sich aus dem TKG 2003, dass nur solche Informationen gemeint sein können, die mittels Nachrichten iSd TKG 2003 übertragen werden. Dort liegen aber gerade die Einschränkungen, die den entsprechenden strafrechtlichen Zwecken entgegenstehen.

Würde man nämlich tatsächlich für eine kernstrafrechtliche Interpretation der grundrechtsbezogenen Strafnorm des § 119 bezüglich der Begriffe »Inhaltsdaten« und »Nachricht« auf § 92 Abs 3 Z 5 bzw Z 7 TKG 2003 abstellen, so entstünde eine nach Art 10a StGG – aber auch nach Art 8 EMRK[815] – Regelungslücke, was Nachrichten betrifft, die nicht über einen »öffentlichen Kommunikationsdienst ausgetauscht oder weitergeleitet« werden. Unter einem derartigen Dienst versteht das TKG 2003 eine »gewerbliche Dienstleistung, die ganz oder überwiegend in der Übertragung von Signalen über Kommunikationsnetze besteht, einschließlich Telekommunikations- und Übertragungsdienste in Rundfunknetzen, jedoch ausgenommen Dienste, die Inhalte über Kommunikationsnetze und -dienste anbieten oder eine redaktionelle Kontrolle über sie ausüben. Ausgenommen davon sind Dienste der Informationsgesellschaft iSv § 1 Abs. 1 Z 2 des Notifikationsgesetzes, BGBl. I Nr. 183/1999, die nicht ganz oder überwiegend in der Übertragung von Signalen über Kommunikationsnetze bestehen« (§ 3 Z 9 TKG 2003). Betreiber von privaten Netzwerken oder Unternehmen, die ihren Mitarbeitern den Zugang zur Telekommunikation verschaffen, bieten nämlich idR keinen öffentlichen Kommunikationsdienst an, noch machen sie dies grundsätzlich gewerblich[816].[817] Und zwar selbst dann nicht, wenn sie faktisch als Provider agieren.[818] Es kann daher generell gesagt werden, dass der »Inhalt einer Nachricht« das Schicksal einer »Nachricht«

815 BGBl 210/1958 aktuell idF III 30/1998, durch BGBl 59/1964 wurde die EMRK in den Verfassungsrang erhoben.

816 Es muss eine auf Gewinnerzielung gerichtete Kommunikationsdienstleistung vorliegen.

817 Siehe dazu OGH 13.06.2002, 8 ObA 288/01p = ASoK 2012, 172 *(Rauch)* = ASoK 2012, 300 *(Trattner)* = ÖJZ EvBl 2012/86, 604 *(Rohrer)* = DRdA 2013/16, 160 *(Eichinger)* = ZAS 2013/12, 75 *(Majoros)*.

818 Siehe dazu für den Bereich des Arbeitsrechts *Rebhahn,* Mitarbeiterkontrolle am Arbeitsplatz (2009) 72 f.

teilt.[819] Auf diese Fälle wäre § 119 bei Rückgriff auf eine telekommunikationsgesetzliche Interpretation des Nachrichtenbegriffs schlicht nicht anwendbar, obwohl der ER (ETS 185) ausdrücklich erläutert: »Communications of employees, whether or not for business purposes, which constitute ›non-public transmissions of computer data‹ are also protected against interception without right under Article 3 (see e.g. ECHR Judgement in Halford v. UK case, 25 June 1997, 20605/92)«.[820]

Wenngleich daher Privatgespräche von Arbeitnehmern ebenfalls den strafrechtlichen Schutz des § 119 genießen[821], billigt die (strafrechtliche) hM die Kontrolle der Einhaltung eines ausdrücklichen Verbots der privaten Nutzung durch den Arbeitgeber.[822]

Auch was ein Chat-Forum betrifft ist anzumerken, dass in diesem Fall »Dienste der Informationsgesellschaft« iSd § 3 Z 1 ECG[823] nicht mit Kommunikationsdiensten iSd § 3 Z 9 TKG 2003 verwechselt werden dürfen, die die Übertragung von Signalen über Kommunikationsnetze zum Gegenstand des Dienstes haben. Die Abgrenzung kann sich freilich in der Praxis auf Grund des Zusammenwachsens verschiedener Technologien als schwierig erweisen. Darüber hinaus ist auch eine Verschränkung nicht ungewöhnlich, sodass etwa ein sog »Access-Provider« sowohl dem ECG als auch dem TKG 2003 unterliegen kann.[824] Doch hat ein Chat-Forum nicht – oder jedenfalls nicht überwiegend – die Übertragung von Signalen über Kommunikationsnetze zum Gegenstand. Eine solche Übertragung erbringt für die Chat-Teilnehmer idR der jeweilige Internet-Zugangsanbieter[825]. Beim Betreiber eines Chat-Forums handelt es sich daher auch nicht um einen Betreiber eines (öffentlichen) Telekommunikationsdienstes iSd § 3 Z 9 TKG 2003.[826]

---

819 Das bedeutet, dass es für die Beurteilung des Nachrichteninhaltsschutzes darauf ankommt, ob die Nachricht selbst überhaupt in einen entsprechenden Anwendungsbereich eines speziellen Gesetzes (zB TKG 2003 oder StGB) fällt.

820 Vgl ER (ETS 185) Pkt 54.

821 Siehe ausdrücklich auch ErlRV 30 BlgNR XIII. GP, 255; weiters JAB 959 BlgNR XIII. GP, 25.

822 Siehe dazu *Reindl-Krauskopf* in Brodil, Datenschutz, 78 unter Hinweis auf *Lewisch* in WK² § 119 Rz 10 mwN; auch *Hinterhofer,* Geheimnisschutz, 173; ebenso weiters JAB 1973, 25.

823 BGBl I 152/2001.

824 Vgl ErlRV 817 BlgNR XXI. GP, 18.

825 Sog »Access-Provider«.

826 Siehe dazu ausf VwGH 27.05.2009, 2007/05/0280, worin insb untersucht wurde, ob § 53 Abs 3a SPG idF BGBl I 158/2005 die Sicherheitsbehörden berechtigt auch von einem Betreiber eines Chat-Forums Auskunft über Name, Anschrift und Teil-

Doch auch § 134 Z 3 StPO verweist iZm der Überwachung[827] von Nachrichten im Klammerausdruck auf die entsprechende Nachrichten-Definition des § 92 Abs 3 Z 7 TKG 2003. Da diese Begriffsbestimmung wiederum auf einen Kommunikationsdienst nach § 3 Z 9 TKG 2003 verweist, dieser aber »Dienste der Informationsgesellschaft« ausdrücklich nicht erfasst, wurden in § 134 Z 3 StPO diese Dienste mit Verweis auf § 1 Abs 1 Z 2 Notifikationsgesetz[828] expressis verbis ebenfalls berücksichtigt.

Daraus folgt einerseits, dass – wie bereits dargestellt – der Begriff »Nachricht« nach dem TKG 2003 keine Nachricht mitumfasst, die mittels eines Dienstes der Informationsgesellschaft[829] übermittelt wird.[830] Andererseits wird dadurch auch offensichtlich, dass bei der »Überwachung von Nachrichten« (§ 134 Z 3 StPO) nur Inhalte von Nachrichten erfasst sind, die entweder über ein Kommunikationsnetz (§ 3 Z 11 TKG 2003) oder einen Dienst der Informationsgesellschaft (§ 1 Abs 1 Z 2 NotifG 1999) ausgetauscht oder weitergeleitet werden, was jedoch nicht alle Nachrichtenübermittlungen einschließt.[831]

Wesentliches Element dieser Beobachtung ist, dass die materiellrechtliche Strafbestimmung der »verbotenen Veröffentlichung« nach § 301[832] ua auf § 134 StPO Bezug nimmt. Gem § 301 Abs 3 macht sich nämlich strafbar, »wer auf eine im Abs. 1 bezeichnete Weise eine Mitteilung über den Inhalt von Ergebnissen aus einer Auskunft über Vorratsdaten oder Daten einer Nachrichtenübermittlung oder einer Über-

---

nehmernummer eines bestimmten Anschlusses zu verlangen, wenn sie diese Daten als wesentliche Voraussetzung für die Erfüllung der ihnen übertragenen Aufgaben benötigen. Grundlegend DSK 03.10.2007, K121.279/0017-DSK/2007. Siehe auch OGH 22.06.2012, 6 Ob 119/11k = jusIT 2012/61, 134 *(Mader)* = ecolex 2012, 904 *(Anderl)* = ÖJZ EvBl-LS 2012/157, 974 *(Rohrer)* = ZIR 2013, 56 *(Briem)*.

827 Darunter versteht die StPO das Ermitteln des »Inhalts von Nachrichten«.

828 BGBl I 183/1999.

829 Die Dienstleistung der Dienste der Informationsgesellschaft muss drei wesentliche Merkmale aufweisen: ihre Erbringung muss 1. im Fernabsatz (lit a), 2. elektronisch (lit b) und 3. auf individuellen Abruf des Empfängers (lit c) erfolgen (siehe § 1 Abs 1 Z 2 NotifG 1999; vgl ErlRV 1898 BlgNR XX. GP, 12); zu einzelnen Beispielen von Diensten, die nicht davon erfasst sind siehe Anlage 1 der RV 1898 BlgNR XX. GP, 7. Auch § 3 Z 1 ECG verweist bezüglich der Definition des Dienstes der Informationsgesellschaft auf § 1 Abs 1 Z 2 NotifG 1999.

830 Zu diesem Ergebnis kommend wohl auch *Reindl-Krauskopf/Tipold/Zerbes* in WK-StPO § 134 Rz 41 ff.

831 Siehe dazu *Reindl-Krauskopf/Tipold/Zerbes* in WK-StPO § 134 Rz 43.

832 Sowohl idF BGBl I 93/2007 als auch idF BGBl I 66/2011; nach der alten Rechtslage iVm § 149a Abs 1 Z 1 StPO (zB idF BGBl I 134/2002).

wachung von Nachrichten oder aus einer optischen oder akustischen Überwachung von Personen unter Verwendung technischer Mittel (§ 134 Z 5 StPO) veröffentlicht«.[833]

Durch diese Bezugnahme wird auch die in § 134 Z 3 StPO normierte (auf die ins TKG 2003 verweisende) Definition von Nachrichten (§ 92 Abs 3 Z 7 TKG 2003) mittelbar ins materielle Kernstrafrecht übernommen. Obwohl § 134 Z 3 StPO auch Nachrichten berücksichtigt, die über einen Dienst der Informationsgesellschaft ausgetauscht oder weitergeleitet werden, und daher die Regelungen über die Überwachung von Nachrichten über Nachrichten, die dem Regime des TKG 2003 unterliegen, hinausreichen, entspricht der hier gegenständliche Nachrichtenbegriff im Wesentlichen[834] der Definition des § 92 Abs 3 Z 7 TKG 2003.

Insgesamt lässt sich daher festhalten, dass der Nachrichtenbegriff nach § 301 iVm § 134 Z 3 StPO iSd TKG 2003 zu interpretieren ist, wobei darüber hinaus auch Dienste der Informationsgesellschaft (§ 1 Abs 1 Z 2 NotifG 1999) umfasst sind.

Daraus folgt, dass innerhalb des Kernstrafrechts der Begriff »Nachricht« je nach Bestimmung unterschiedlich zu interpretieren ist.

Aus der in dieser Arbeit vorgenommenen Untersuchung lassen sich daher zusammenfassend folgende unterschiedliche Bedeutungen des Begriffs »Nachrichten« im StGB erkennen:

Für § 119 und § 120 Abs 2a[835] gilt, dass der Nachrichtenbegriff »autonom« zu verstehen ist und nicht unter Bezugnahme auf das TKG 2003 definiert wird. Obwohl gerade § 119 und zu einem Teil auch § 120 Abs 2a ausdrücklich auf den »Inhalt einer Nachricht« abstellen, muss in erster Linie der Begriff der »Nachricht« inhaltlich verstanden werden, da der Inhalt einer Nachricht auch das Schicksal der übergeordneten Nach-

833 Man beachte dabei, dass die Bestimmungen zur Auskunft über Vorratsdaten mit Erkenntnis des VfGH 27.06.2014, G 47/2012 ua als verfassungswidrig aufgehoben wurden.

834 Durch die Beifügung in § 134 Z 3 StPO »[…] oder einen Dienst der Informationsgesellschaft […]« wird die Bezugnahme innerhalb der Nachrichtendefinition des § 92 Abs 3 Z 7 TKG 2003 auf »öffentlichen Kommunikationsdienst« (iSd § 3 Z 9 TKG 2003) genau genommen verdrängt, da in letztgenannter Legaldefinition »Dienste der Informationsgesellschaft« ausdrücklich ausgenommen werden. Dies wird auch dadurch ersichtlich, dass der Bezug zu einem »Kommunikationsnetz«, auf das aus § 3 Z 9 TKG 2003 wiederum verwiesen wird, neben dem Hinweis auf die Dienste der Informationsgesellschaft, die Nachricht näher konkretisiert.

835 Siehe unten S 216 ff.

richt teilt.[836] Der »Inhalt einer Nachricht« wird dabei jedenfalls auf den zu vermittelnden Gedankeninhalt (hier: als Mitteilung bezeichnet) beschränkt, folgt aber der Bewertung der in Übertragungszustand versetzten »Nachricht«.

Die Unterschiede des Nachrichtenbegriffs in §§ 119 und 120 Abs 2a können in drei Punkte gegliedert werden:

1. Durch diese Bestimmungen werden auch private Nachrichtenübermittlungen geschützt.
2. Es werden auch Übertragungen erfasst, die nicht gewerblich erfolgen.
3. Grundsätzlich sind alle Formen der Nachrichtenübermittlung, und nicht nur jene, die den Regelungen des TKG 2003 folgen[837], tatgegenständlich.

Für § 301 Abs 3 iVm § 134f StPO gilt hingegen nunmehr, dass der Begriff der »Nachricht« grundsätzlich nach dem TKG 2003 definiert wird. Die tatbestandliche Ergänzung, dass auch deren Austausch oder Weiterleitung durch Dienste der Informationsgesellschaft (§ 1 Abs 1 Z 2 NotifG 1999) umfasst ist, ändert daran grundsätzlich nichts und erweitert lediglich die Begriffsklärungen »Auskunft über Daten einer Nachrichtenübermittlung« (§ 134 Z 2 StPO) und »Überwachung von Nachrichten« (§ 134 Z 3 StPO). Das heißt, dass eine Nachricht, die über nicht-öffentliche Kommunikationsdienste übertragen wird, mangels Vorliegens einer tatbestandlichen »Nachricht« nicht nach § 134f StPO überwacht werden darf.[838] § 301 Abs 3 wäre daher in diesem Zusammenhang gar nicht anwendbar.

Die Klarstellung in den GMat, dass der Begriff »Inhalt einer Nachricht« nach § 119 – anders als nach dem TKG 2003 – im Sinne der »Vermittlung von Gedankeninhalten« zu verstehen sei, erweist sich terminologisch als missverständlich und inkonsequent.[839] Äußere Ge-

836 Man kann sich eine Nachricht (insb eine, die über elektronische Datennetze geleitet wird) zum leichteren Verständnis bildlich als einen Brief vorstellen, auf dessen Umschlag sich für den Transport zusätzliche Informationen befinden, die gedankliche Botschaft, die dem Empfänger mitgeteilt werden soll, sich innerhalb des Umschlags befindet.

837 Also auch jene, die zB als Dienst der Informationsgesellschaft erbracht werden.

838 Siehe auch *Reindl-Krauskopf/Tipold/Zerbes* in WK-StPO § 134 Rz 43.

839 Siehe ErlRV 1166 BlgNR XXI. GP, 26; *Leukauf/Steininger,* StGB[3] § 119 Rz 3.

sprächsdaten der geführten (technischen) Kommunikation (zB Verkehrsdaten einschließlich Zugangsdaten[840] und Standortdaten[841]) fallen – wie oben ausgeführt, entgegen der Intention des TKG 2003 iVm RL 2002/58/EG[842] – nicht in den Anwendungsbereich von § 119. Solche »Daten« werden aber dann von § 119 erfasst, wenn sie selbst Teil des »gedanklichen« Inhalts der Nachricht sind. Man stelle sich vor, jemand teilt seinem Kommunikationspartner zB die eigene IP-Adresse bewusst mit. In diesem Fall wäre die IP-Adresse als Inhaltsdatum und Teil des Nachrichteninhalts zu qualifizieren. Das gilt freilich gleichermaßen für Standortdaten oder Zugangsdaten, sofern diese Teil des vermittelten Mitteilungsinhalts sind.

Nach diesen Betrachtungen ergibt sich, dass einerseits das Abstellen auf die gegenüber dem TKG 2003 einschränkende Funktion des Nachrichtenbegriffs des § 119, was iZm der Formulierung »Inhalt von Nachrichten« das Abstellen auf die rein inhaltliche Mitteilung ohne weitere damit verbundenen Meta-Daten (»äußere Gesprächsdaten«) betrifft[843], sinnvoll ist. Andererseits ist die in den GMat zum Ausdruck gebrachte über die Definition des TKG 2003[844] hinausreichende Vorstellung, dass sich diese Gedankenvermittlung nicht aus öffentlichen oder privaten, entgeltlichen oder unentgeltlichen Kriterien ergeben müsse, und darüber hinaus auch Nachrichteninhalte erfasst werden sollen, die durch Dienste der Informationsgesellschaft übermittelt werden, auffallend sachgerecht.

Dies nicht zuletzt, weil damit den internationalen Vorgaben entsprochen wird und ein derartiges Begriffsverständnis in Hinblick auf die korrespondierenden Grundrechte[845] (vgl Art 10a StGG, Art 8 EMRK) mehr als angebracht erscheint.

---

840 § 92 Abs 3 Z 4 TKG 2003: Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden.

841 § 92 Abs 3 Z 6 TKG 2003: Daten, die in einem Kommunikationsnetz verarbeitet werden und die den geografischen Standort der Telekommunikationsendeinrichtung eines Nutzers eines öffentlichen Kommunikationsdienstes angeben.

842 Siehe dazu auch *Feiler,* Die SPG-Novelle 2007, in Zankl (Hrsg), Auf dem Weg zum Überwachungsstaat? (2009) 43 (53).

843 Dh der Inhalt einer Nachricht nach § 119 ist nicht mit dem Inhalt einer Nachricht nach dem TKG 2003 gleichzusetzen, was auch die GMat ausdrücklich einräumen (ErlRV 1166 BlgNR XXI. GP, 26).

844 Aber auch was die Dienste der Informationsgesellschaft nach dem ECG betrifft.

845 Siehe dazu *Wessely,* ÖJZ 1999, 491.

Zur Wahrung der Einheit der Rechtsordnung[846] und Rechtsprache sowie zur Vermeidung der aufgezeigten Interpretationsschwierigkeiten sollte der Gesetzgeber anstelle des Begriffs »Nachrichten« in § 119 einen Terminus verwenden, der nicht rechtstechnisch-begrifflich »vorbelastet« ist.

§ 119 muss daher, um seinen Vorgaben gerecht zu werden, bezüglich des Tatobjekts »Inhalt von Nachrichten« – trotz seiner Nähe zum TKG – eine vom TKG 2003 unabhängige Definition bilden, die aus den dargestellten Erwägungen heraus, in der Wahl einer anderen Terminologie umzusetzen wäre. Die Lösung wäre einfach, nämlich den vor dem StRÄG 2002 in § 119 aF[847] verwendeten Begriff der »Mitteilung« wieder aufleben zu lassen, um so eine entsprechende Abgrenzung zu realisieren. Denn auch die »Mitteilung« stellte im selben Sinn auf den Gedankeninhalt[848] ab und legt aktuell nicht unbedingt[849] eine (unzutreffende) Interpretation nach dem TKG 2003 nahe. Eine »Mitteilung« ist daher – im Gegensatz zur Nachricht – ohne Rücksicht auf etwaige technische (Verarbeitungs-)Formen zu verstehen. Zentraler Anknüpfungspunkt des strafrechtlichen Begriffsverständnisses des § 119 ist also ausschließlich eine als »Inhalt« verstandene Information und nicht etwa eine Information, die als Vorgang einer Kommunikation (zB Vermittlungsdaten[850] bzw Verkehrsdaten[851]) beschrieben wird.[852]

d. Mitteilung vs Nachricht

Neben der nicht näher substantiierten Aussage des JA[853] zu Art 10a StGG, dass der Schutz allen »im Wege des Fernmeldeverkehrs übermittelten Nachrichten oder Mitteilungen« gilt, könnte auch die sprach-

---

846 Siehe dazu auch OGH 17.06.1998, 13 Os 68/98.

847 IdF BGBl 60/1974.

848 Siehe dazu *Leukauf/Steininger,* StGB[3] § 119 Rz 3; so auch *Schmölzer* in Jahnel/Schramm/Staudegger, Informatikrecht[2], 335 (355); weiters ErlRV 1166 BlgNR XXI. GP, 26; Interessanterweise verwendet der Justizausschuss die Begriffe »Nachrichten« und »Mitteilung« nebeneinander, und – soweit überschaubar – synonym (JAB 960 BlgNR XIII. GP, 2).

849 Trotz Verweis auf das TKG iZm der »Telekommunikationsanlage« bzw »Fernmeldeanlage« in den historischen Fassungen.

850 Vgl noch TKG 1997.

851 Vgl TKG 2003.

852 Siehe *Damjanovic/Holoubek/Kassai/Lehofer/Urbantschitsch,* Telekommunikationsrecht, 242.

853 Siehe JAB 960 BlgNR XIII. GP, 2.

bzw kommunikationswissenschaftliche Sicht Indizien dafür liefern, dass es einen Bedeutungsunterschied zwischen den Termini »Mitteilung« und »Nachricht« gibt. So wandelt etwa der Sender die seinem Geist entsprungene »Mitteilung« in entsprechende Signale (iSv Zeichen in einer entsprechenden Syntax) um und übermittelt diese über einen bestimmten Trägerkanal als »Nachricht«[854] dem Empfänger.[855] Erst durch Decodierung der Nachricht erschließt sich für den Empfänger im Fall der Kenntnis der verwendeten Semantik und des Kontexts die ursprüngliche Mitteilung. Das im Geist Entstandene und zur Übertragung Bestimmte wird also als »Mitteilung« bezeichnet, zur »Nachricht« wird sie, wenn sie in einen übertragungsfähigen codierten Zustand[856] gebracht wird.

e. »Gedankeninhalte«

Thiele schließt Inhalte, die zusammenhanglos oder sinnlos sind[857], als Schutzobjekte des § 119 aus.[858] Dasselbe gelte zB auch für ein automatisch generiertes E-Mail, das den Administrator über die Systemauslastung der letzten Tage informiert, oder zumindest grundsätzlich[859] für den Aufruf einer Internetadresse.[860]

Dem ist aber mE entgegenzuhalten, dass es grundsätzlich – wie oben ausf angesprochen – nicht um die Qualität des Inhalts geht. Vielmehr muss die Kommunikation, sei es im Wege einer Telekommunikation oder im Wege eines Computersystems, eine Übertragung eines vom Menschen – zur Übermittlung bestimmten – geistigen Produkts

854 Außerhalb der telekommunikationsrechtlichen Begrifflichkeit, könnte man hier auch von »Daten«, als die übertragungsfähige Repräsentation der Information bzw Mitteilung sprechen.

855 Siehe in diese Richtung *Hansen,* Sprachliches Handeln und Transaktionsanalyse. Die Psychologie im Sprechakt (2008) 135.

856 Die »Mitteilung« wird in eine einer bestimmten Ordnung (Syntax) folgende Zeichenfolge umgewandelt (= Mitteilung oder Information in einer übertragungsfähigen Codierung), die über einen Kommunikationskanal (= geeignetes Medium) vom Sender an den Empfänger übertragen wird.

857 Siehe auch bereits für § 119 aF *Leukauf/Steininger,* StGB[3] § 119 Rz 3.

858 Siehe *Thiele* in SbgK § 119 Rz 34.

859 Wobei *Thiele* in SbgK § 119 Rz 34 auch ausdrücklich Ausnahmen von diesem Ausschluss nennt.

860 *Thiele* in SbgK § 119 Rz 35.

beinhalten. Auch die Übermittlung einer »leeren«[861] SMS oder eines E-Mails[862] kann eine gedankliche Mitteilung sein, nämlich dann, wenn der Kommunikationspartner etwa eine Zustimmungserklärung durch das bloße Absenden einer Nachricht ohne ausdrücklichen Inhalt verlangt.[863] Der Absender und Empfänger dieser Mitteilung müssen auch in einem solchen Fall darauf vertrauen können, dass der »Inhalt« – in concreto eben ein nicht augenscheinlich schriftlich ausgewiesener – während der Übertragungsphase nicht kompromittiert wird. In diesem Fall ist der mangelnde »augenscheinliche Inhalt« dennoch der »Gedankeninhalt« der Übertragung. Der gedankliche Inhalt erschließt sich daher erst aus der (subjektiv) kontextbezogenen Verarbeitung der Nachricht durch den Empfänger. Ein Kommunikationsprozess ist nach *Reisinger* dadurch charakterisiert, dass der Sender Signale[864] über ein Übertragungsmedium an den Empfänger sendet, wobei nicht die Transmission von Signalen intendiert ist, sondern die von Nachrichten[865] bzw Botschaften[866]. Der Bedeutungsinhalt von bloßen übermittelten strukturierten Daten zu einer »Nachricht« erschließt sich aber den Kommunizierenden nur, sofern eine gemeinsam bekannte Syntax und Semantik (gemeinsamer Code[867]) verwendet wird.[868] In unserem Beispiel wurde die Modalität der Datenübertragung und die entsprechende Decodierung der Übermittlung im Vorhinein ausreichend festgelegt (= syntaktische Ebene), sodass der Empfänger der »inhaltsleeren« SMS den Bedeutungsgehalt – nämlich die Zustimmung des Absenders – aus der »leeren« SMS selbst interpretieren kann (= semantische Ebene). In diesem Fall bildet die »leere« SMS für die Kommunizierenden (Sender und Empfänger[869]) ein zum gewöhnlichen

861 Will man sich lieber einen Inhalt vorstellen, so lässt sich die Argumentation auch auf die Übertragung zB einer einzigen Zahl zB »1« als Inhalt stützen.

862 Das heißt, es werden nur die spezifizierten E-Mail-Rahmendaten über SMTP übermittelt.

863 Man denke etwa an eine akkordierte geheime Anweisung an einen Broker, an der Börse entsprechende Handlungen zu setzen.

864 Darunter versteht man die physikalische Repräsentation einer Nachricht, wie etwa den Verlauf einer Spannung oder elektrischen Feldstärke uÄ; siehe dazu *Rohling/May,* Informations- und Codierungstheorie, in Rechenberg/Pomberger (Hrsg), Informatik Handbuch[4] (2006) 211 (214).

865 Vgl *Reisinger,* Rechtsinformatik, 127.

866 Anstelle des Terminus »Nachricht« verwendet *Grimm* in synonymer Bedeutung den Terminus »Botschaft« (vgl *Grimm,* Digitale Kommunikation [2005] 91 ff).

867 Im Sinne einer gemeinsamen Zuordnungsvorschrift.

868 Siehe dazu *Reisinger,* Rechtsinformatik, 127.

869 Oder Kommunikator und Rezipient.

konventionalisierten Zeichenvorrat der gewohnten Sprache zusätzliches Zeichen, das über die speziell vereinbarte Semantik[870] (in concreto eine Zustimmungserklärung) zur Nachricht/Information wird. Die Syntax dieses Zeichens wäre eine den technischen Spezifikationen entsprechende SMS-Nachricht ohne zusätzlichen Text im Body-Teil. Die Semantik dieses erweiterten Zeichens ist konventionell und in concreto somit nur für die tatsächlich (eingeweihten) Kommunizierenden bedeutsam. Insofern hat die »leere SMS« lediglich für die Kommunizierenden auch eine pragmatische Bedeutung[871], da nur diese – auf Grund ihrer ausdrücklichen und sinnvollen Vereinbarung – die Botschaft dieses Zeichens verstehen. Ein echter Informationswert ergibt sich in diesem Fall lediglich für die eingeweihten Kommunizierenden.[872] Für Dritte, die mit dieser besonderen Sprachkonvention nicht vertraut sind, würde sich möglicherweise ein »zusammenhangloser« bzw »sinnloser« Inhalt ergeben, da für sie – aus situationsunabhängiger Sichtweise und auch unabhängig von der Perspektive der tatsächlich Kommunizierenden – keine bzw eine andere (somit beliebige) semantische Bedeutung erkennbar ist, dennoch wird der »Inhalt einer Nachricht« übertragen. Man kann dies auch mit der klassischen Kryptografie vergleichen, bei der grundsätzlich[873] nur derjenige in der Lage ist, die Daten zu entschlüsseln, der in Kenntnis des zur Decodierung erforderlichen Schlüssels (Code) ist. Dass die Allgemeinheit keine Bedeutung in einer bestimmten Übertragung erkennen kann, bedeutet nicht, dass es überhaupt niemand kann. Jede Form der entsprechenden Übertragung von »Inhalten mit Erklärungswert«, unabhängig von der gewohnten Bedeutung der sie repräsentierenden Zeichen, muss nach § 119 geschützt sein.

Daraus ergibt sich folgende Vorgehensweise für die Ausforschung, ob einen gedankliche Mitteilung oder sonstige Daten vorliegen:

---

870 Behandelt die Beziehungen zwischen den Zeichen und ihren Bedeutungen (Vgl *Reisinger,* Rechtsinformatik, 124).

871 Im Sinne von Verbindung mit Kontext und Erfahrungen der Beteiligten; siehe zu den drei semiotischen Ebenen Syntax, Semantik und Pragmatik auch *Grimm,* Digitale Kommunikation, 7 ff.

872 Siehe zur Pragmatik und Information zB *Rohling/May* in Rechenberg/Pomberger, Informatik[4], 211 (214); weiters *Reisinger,* Rechtsinformatik, 126).

873 Vgl die »Kryptanalyse«, das ist die Kunst einen verschlüsselten (Geheim-)Text ohne Kenntnis des Schlüssels zu entziffern (siehe *Wobst,* Abenteuer Kryptologie. Methoden, Risiken und Nutzen der Datenverschlüsselung[3] [2001] 29).

In einem ersten Schritt ist die gegenständliche Übertragung in Anbetracht der gewohnten Sprache in syntaktischer und semantischer Hinsicht zu überprüfen. Dabei gilt es zu beachten, dass auch nur diese beiden Elemente in Form von Zeichen und Daten letztlich objektiv[874] auf einem Übertragungsmedium feststellbar sind. Lässt sich aus dieser Betrachtung heraus aus Sicht der Allgemeinheit bereits erkennen, dass eine gedankliche Mitteilung vorliegt, kann die Prüfung zu diesem Zeitpunkt beendet werden.

Ergibt sich jedoch aus dieser Betrachtungsweise kein eindeutiges Ergebnis, muss in weiterer Folge die Intention des Senders ausgeforscht werden. Dazu muss auf die verwendete Syntax und die dazugehörige intendierte Semantik (iS einer Sondersprache, wie zB der »Gaunersprache«[875]) eingegangen werden, die eine Übertragung als bewusst vorgenommene Nachricht des Senders an den Empfänger offenlegt. Mit anderen Worten: Es muss erkundet werden, was der Sender im konkreten Fall als eine Mitteilung bestimmt hat. Zur Aufklärung kann in der Praxis freilich auch der »eingeweihte« Empfänger beitragen. Ob die Mitteilung überhaupt für den Empfänger Relevanz besitzt, also ob aus der Nachricht eine (neue) Information für den Empfänger resultiert, ist dabei wohl unbeachtlich. Um generell aus einer entsprechenden Syntax bzw Daten Informationen gewinnen zu können, müssen sie in einem vordefinierten Bedeutungskontext betrachtet werden.

Daher findet sich mE im gegenständlichen Zusammenhang das Substrat für die Entscheidung, ob eine Nachricht (§ 119) oder (nicht gedankliche, sonstige) Daten (§ 119a) vorliegen, in der Unterscheidung von technisch bedingter Syntax und intendierter[876] Semantik einer konkreten Übertragung. Die Unterscheidung von Semantik und Pragmatik ist bei dieser Untersuchung nicht von vordringlichem Interesse, kann aber mE bei speziellen Problemen im Einzelfall durchaus Bedeutung haben.[877]

---

874 Man beachte den Unterschied zwischen »speicherbaren Daten bzw Nachrichten« und »verstandenen Informationen« (siehe zu diesen Überlegungen auch *Engelmann/Großmann,* Was wissen wir über Information?, in Hildebrand/Gebauer/Hinrichs/Mielke (Hrsg), Daten- und Informationsqualität² (2011) 3 (5 f).

875 ZB Jargon einer bestimmten Gruppe, wie etwa Rotwelsch.

876 Die bewusst als Nachricht des Senders übermittelte Botschaft an den Empfänger.

877 Siehe etwa S 184 ff.

Gesetzt den Fall, ein Täter, der sich durch irgendwelche Umstände die gegenständlich verwendete Sondersprache und Vereinbarung über die Nachrichtenübertragung angeeignet hat, benützt eine Vorrichtung, um sich die »Inhalte« (Information) dieser Übermittlung zur Kenntnis zu bringen. In diesem Fall kann zwar die Allgemeinheit keine (semantische) Bedeutung und keine (pragmatische) Relevanz der konkreten Datentransmission erkennen, dennoch hat sich der (eingeweihte) Täter vom Inhalt einer Nachricht Kenntnis verschafft. Aus dem Schutzzweck des Grundrechts nach Art 10a StGG und dem demselben Rechtsgut dienenden einfachgesetzlichen (grundrechtsbezogenen) § 119 ergibt sich, dass es nicht auf konkrete Inhalte ankommt, sondern rein auf die Vertraulichkeit nicht für die Öffentlichkeit bestimmter Übertragungen. Dabei geht es eben nicht um die Meta-Daten, die in diesem Fall tatsächlich und technisch ausschließlich den (stofflichen, verdinglichten) Gegenstand der Übertragung bilden. Für die konkreten Kommunikationspartner geht es gerade um den im Bewusstsein liegenden Kern der Übertragung (geistige Ebene), die beim Empfänger – und in concreto auch beim unberechtigten Täter – durch Decodierung ermittelt wird. Insoweit kommt es nicht ausschließlich auf den objektiven Charakter des für die Allgemeinheit erkennbaren Bedeutungsgehalts einer Nachricht an, sondern auch auf deren subjektive Bestimmung als eine gedankliche Mitteilung.[878] Ob nun das »Abfangen« von Nachrichteninhalten (§ 119) oder sonstiger Daten (§ 119a) vom Täter intendiert war, hängt ebenso – neben der vom Sender der Nachricht als gedankliche Botschaft bestimmten Übertragung – von der konkreten Person des Täters und dessen diesbezüglichem »Kenntnisstand«[879] bzw »Erfahrungshintergrund« ab.

878 Siehe idS zu Art 10a StGG unter Bezugnahme auf den verwandten Schutz des Briefgeheimnisses auch *Wiederin* in Korinek/Holoubek, Bundesverfassungsrecht Art 10a StGG Rz 7; zur Beschreibung einer »Mitteilung« siehe *Kruspel,* Auf dem Weg zu einem tragfähigen Massenkommunikationsbegriff: Nachricht als vermittelte Mitteilung (2008) 6.

879 Im Sinne einer im Einzelfall zu konstatierenden Vertrautheit des Täters mit der syntaktischen Modalität der Übertragung, deren semantischen Deutung und der ggf daraus ableitbaren pragmatischen Relevanz.

Beispiel 1:
A übermittelt B per E-Mail die Nachricht »Der Strauch treibt aus«.

Sender/Kommunikator ist A.
Empfänger/Rezipient ist B.

Trägermedium ist das E-Mail via SMTP[880] samt technisch zur Transmission notwendiger Infrastruktur.

Als Syntax wird ein allgemein bekannter Zeichenvorrat (Alphabet) in konventionalisierter grammatikalischer Ordnung verwendet. Der semantische Gehalt der Nachricht ergibt sich aus der Bedeutung der Zeichen in der konkreten Syntax. Die Allgemeinheit würde situationsunabhängig und ohne Beachtung der Sender- und Empfängerperspektive wohl daraus schließen, dass es um eine Pflanze geht, die gerade neue Triebe bildet.

Der pragmatische Gehalt für den Sender- und Empfänger könnte aber jener sein, dass es sich dabei nicht um Botanik, sondern um eine vereinbarte Sondersprache mit abgeänderter Semantik handelt, die zum Ausdruck bringt, dass zB mit einer illegalen Machenschaft begonnen wurde. Der Wissensstand des Empfängers wurde daher um eine neue (pragmatische) Information erweitert.

Die Prüfung, ob es sich dabei um den Inhalt einer Nachricht iSd § 119 handelt, kann in diesem Fall kurz und prägnant ausfallen und wird eindeutig mit ja zu beantworten sein.

Die verwendete Syntax lässt iZm der dazugehörigen konventionellen semantischen Bedeutung bereits auf (irgend-)eine gedankliche Mitteilung (Information) schließen. Die Pragmatik (für die Beteiligten) ist dabei unbeachtlich, da bereits auf einer darunterliegenden Ebene (Semantik) ein »gedanklicher Inhalt« aus den Daten bzw der Nachricht abstrahiert werden kann. Eine objektive ex post-Betrachtung reicht in diesem Fall aus, um einen gedanklichen Inhalt zuzuerkennen. Eine qualitative Bewertung desselben ist nicht vorzunehmen und für die hier interessierende Abgrenzung unbeachtlich.

880 Simple Mail Transfer Protocol.

Beispiel 2:
A übermittelt B per E-Mail die Nachricht/Daten »123AB045«.

Sender/Kommunikator ist A.
Empfänger/Rezipient ist B.

Trägermedium ist erneut das E-Mail über das SMTP samt der technisch zur Transmission notwendigen Infrastruktur.

In diesem Fall wird zwar offensichtlich eine Folge konventioneller Zeichen verwendet, doch scheint die spezielle Ordnung und eine etwaige spezielle Semantik (für die Allgemeinheit) unbekannt. Daraus folgt, dass zwar nach allgemeiner Ansicht die tatsächlich verwendeten Zeichen für sich allein genommen eine gewisse Bedeutung haben können, doch lässt sich daraus nicht zwingend schließen, dass es sich bei dieser Zeichenfolge um eine gedankliche Mitteilung handelt. Hier bereits die Prüfung abzubrechen und von sonstigen Daten iSd § 119a auszugehen, wäre aber verfrüht. Kommt man aus einer objektiven Betrachtung heraus zu keinem eindeutigen Ergebnis, so muss weiters auf die Sichtweise der jeweiligen Kommunizierenden iSd »Eindruckstheorie«[881] eingegangen werden, um das Wesen der Übertragung zu ermitteln. In diesem Fall muss aber auf die Person (insb bezüglich der Vertrautheit mit gegenständlichen Sprachkonventionen) des Täters, der diese Nachricht/Daten abgefangen hat, eingegangen werden, um ihm die »Absicht« der Kenntnisverschaffung von »Inhalten« überhaupt nachweisen zu können. Stellt sich dabei heraus, dass es sich bei den Kommunizierenden um Geschäftspartner handelt, die über eine vereinbarte Kommunikationsmethodik zB »Insider-Wissen« kommunizieren und der Täter ein Kontrahent und ehemaliger Mitarbeiter eines dieser Kommunizierenden, der mit dieser »Sondersprache« vertraut ist, so ergibt sich daraus, dass es sich bei dieser Übertragung, sehr wohl um eine Mitteilung gedanklichen Inhalts handelt, deren widerrechtliches Abhören nach § 119 zu beurteilen wäre. Zum selben Ergebnis kommt man auch im mehrfach angesprochenen Fall der »leeren« SMS.

881 Siehe grundlegend *Burgstaller,* Über den Verbrechensversuch, JBl 1969, 521; *Burgstaller,* Der Versuch nach § 15, JBl 1976, 113; allgemein *Fuchs,* AT I[8], Rz 30/18 ff sowie *Kienapfel/Höpfel/Kert,* AT[14], Z 24 Rz 12 ff.

Diesem Beispiel folgend wäre auch die Übermittlung einer PIN, als bloße Zahlenabfolge, als Tatobjekt des § 119 zu beurteilen, wenn der Sender diesen bewusst zur Kenntniserlangung an den Empfänger übermittelt.[882] Der pragmatischen Relevanz für die Kommunizierenden ist somit ggf eine wichtige Bedeutung zuzumessen. § 119 muss in einem übergeordneten Verhältnis jede Form der Übertragung gedanklicher Inhalte (Informationen) schützen, selbst wenn diese für die Allgemeinheit nicht gleich als solche kenntlich sind. Erst wenn ein solcher Gedankeninhalt letztlich nicht nachweisbar ist, muss § 119a aushilfsweise herangezogenen werden.

An dieser Stelle sei angemerkt, dass bei personenbezogenen Daten als Gegenstand der kompromittierten Übertragung stets auch § 51 DSG 2000 berücksichtigt werden muss.

f. »Paketvermittelnde Transportdienste«

Doch auch in Anbetracht der technischen Grundlagen einer Übertragung über informationstechnische Systeme[883], wie das Internet, ergibt sich, dass auf Ebene einer paketvermittelnden[884] Übertragungsmodalität »fragmentarische« oder »zusammenhanglose« Inhalte auftauchen können. Würde zB eine Schnüffelsoftware[885] einen Nachrichtenverkehr in einem Netzwerk aufgrund der paketvermittelnden Übertragung nur fragmentarisch mitlesen bzw aufzeichnen, würde dies nichts am Charakter der gedanklichen Mitteilung ändern. Zum einen handelt der Täter in der Absicht, sich vom Inhalt einer Nachricht Kenntnis zu verschaffen, und zum anderen wird auch eine Nachricht übermittelt. Ob der Täter aber tatsächlich Kenntnis vom Inhalt erlangt, ist für eine Strafbarkeit nach § 119 ebenso unbeachtlich, wie das technische Verfahren des Kommunikationsvorgangs selbst.

---

882 AA offensichtlich *Reindl-Krauskopf* in WK² § 119a Rz 8.

883 Unter einem informationstechnischen System wird hier jedes technische Mittel verstanden, das der automationsunterstützten Verarbeitung von Informationen bzw Daten dient.

884 Sog »Packet Switching«: Die zu versendenden Daten werden in Datenpakete zerteilt und über unterschiedliche Wege zum Empfänger geleitet (sog »Routing«). Der Empfänger nimmt die Pakete entgegen und interpretiert sie je nach Daten- und Übertragungsart iSd jeweiligen Protokollspezifikationen (siehe *Kersken,* IT-Handbuch⁵, 170 f); auch die Internettelefonie über VoIP-Dienste basiert auf dieser Grundlage.

885 Spezielles Spionageprogramm.

Daher ist auch die Verwendung eines Keyloggers, der einzelne Tastaturanschläge – die der Bearbeitung einer gedanklichen Mitteilung dienen – mitprotokolliert, vom Tatbild erfasst.[886] Selbst dann, wenn der Hard- oder Software-Keylogger als Vorrichtung im Zielsystem unbemerkt nur Zeichenfolgen in Echtzeit aufzeichnet und daher keine vollständige »Gedankenerklärung« als Mitteilungspaket abfängt, haben wir es mit Inhaltsdaten zu tun. Die Tasten werden dabei idR vom Opfer gezielt in einer entsprechenden Reihenfolge gedrückt, weshalb die Übermittlung des jeweiligen Tastenzeichens vom Sender intendiert ist. Auch wenn sich letztlich – mangels Vollständigkeit der Zeichenaufzeichnung – kein Bedeutungsgehalt für den Täter erschließen mag, liegt dennoch eine Nachrichtenübermittlung[887] vor. Das gilt selbstverständlich auch dann, wenn nur eine einzige Taste gedrückt wird.[888] Die Bedeutung des Inhalts als Mitteilung ergibt sich aber lediglich für denjenigen, der mit der konkreten Übertragungsmodalität vertraut ist. Als etwaige äußere Daten dieser Nachrichtenübermittlung könnten zB die jeweiligen Scancodes[889] der Tastatur genannt werden, die keinen gedanklichen Inhalt dieser Übertragung darstellen. Ist somit der Täter nachweislich mit der die Nachricht konstituierenden Konvention vertraut, hat er »Nachrichten« abgefangen (iSd § 119). Kann man ihm das jedoch nicht nachweisen, macht er sich zumindest nach § 119a bezüglich sonstiger Daten strafbar, sofern er die entsprechenden Anforderungen auf subjektiver Tatseite erfüllt. Demzufolge ist es unbeachtlich, ob verschlüsselte Botschaften ausgetauscht werden oder ob aufgrund der paketvermittelnden Datenübertragung in Netzwerken oder aus der Konzeption eines technischen Schnüffelprogramms heraus nur Inhaltsfragmente erfasst werden, solange dem Täter die Decodierungsmöglichkeit der Inhalte und die entsprechende Absicht nachgewiesen werden können.

Dies gilt auch für übermittelte Internet-Adressen und automatisch generierte Informationen – sofern sie eine per Datensatz zum Aus-

886 Vgl *Winterer,* Viren, 198 f.

887 In diesem Fall würde eine Übertragung »im Wege eines Computersystems« (nämlich innerhalb eines Computersystems, zB von Tastatur über CPU zum Bildschirm) vorliegen.

888 Vgl das Beispiel mit der »leeren« SMS.

889 Unter einem Scancode, versteht man eine Nummer, die vom Tastaturcontroller an die CPU gesendet wird und eine bestimmte Taste samt ihrem Zustand (iSv gedrückt oder losgelassen) kennzeichnet; siehe *Schiffmann/Bähring/Hönig,* Technische Informatik 3. Grundlagen der PC-Technologie (2011) 277.

druck gebrachte Intention des Absenders transportieren.[890] Wird etwa eine Internetbestellung per Webshop durchgeführt, auf welche ein automatisch generiertes E-Mail als Bestellbestätigung repliziert wird, so hat dieses mE sehr wohl einen Gedankeninhalt, nämlich den, dass der Webshop-Betreiber – wenn auch durch eine automatisch generierte Information als sein »Werkzeug« – seine dadurch manifestierten »Gedanken« (zB Kontrahierungswillen) zum Ausdruck bringt, die er ohne technische Unterstützung auch selbst getätigt hätte.[891] So ist – im Sinne der oben angeführten Kritik an *Selings* Definition einer Telekommunikation[892] und in Anbetracht der Übertragungsmöglichkeit über ein »Computersystem« iSd § 119 – nicht einzusehen, warum Gedankeninhalte, die zwar von einer Person ausgehen, aber ausschließlich über Maschinen übertragen werden, nicht schutzwürdig erscheinen sollten.[893] Dabei wird doch wohl wiederum ein Datensatz als »technisch verarbeitbare Verkörperung« einer von Menschen getätigten gedanklichen Intention übertragen, die einen »gedanklichen Inhalt« darstellt.[894] Inhalt der Übermittlung wäre in diesem Fall jedoch nur jener Teil, der vom Menschen tatsächlich »durch Eingabe geäußert« wurde. Mit anderen Worten: Äußere Daten der Informationsübertragung (zB Zeit und Ort einer Transaktion), die nicht vom Kommunikator beeinflusst sind[895], sind nicht als Gedankeninhalte zu werten, sehr wohl aber jene Übertragungsteile, die vom Kommunikator als »bewusst intendiert« (und ggf vom intendierten Empfänger verstanden werden sollen) zu qualifizieren sind.

g. »Inhaltserforschung«

Da sich aus der Datenform ein unterschiedliches strafrechtliches Schutzniveau ergibt, ist streng nach »gedanklichen Inhalten« einerseits (§ 119) und anderen übermittelten »Daten« (§ 119a) zu unterschei-

890 AA daher *Seling,* Privatsphäre, 156; weiters teilweise aA *Thiele* in SbgK § 119 Rz 35.

891 ZB »Die Bestellung konnte nicht durchgeführt werden, da die Ware nicht mehr verfügbar ist« oder »Danke für Ihre Bestellung. Die Ware wird unmittelbar nach Zahlungseingang versandt«.

892 Siehe *Seling,* Privatsphäre, 156.

893 Siehe dazu das Bespiel mit Geldautomaten bei *Seling,* Privatsphäre, 156.

894 ZB Auszahlung von € 100,– von Konto A, am 25.03.2010, um 10 Uhr, über Bankomat XY.

895 So stellt bei einem E-Mail auch der genannte Betreff und nicht nur der »Body-Teil« eine etwaige gedankliche Mitteilung dar; aA offensichtlich *Thiele* in SbgK § 119 Rz 35.

den. Dass eine derartige Unterscheidung in vielen Fällen nicht einfach zu realisieren ist, zeigen gerade die oben angesprochenen Beispiele für die Übertragung von Inhalten[896]. Wie lässt sich aber eine Abgrenzung in schwierigen Fällen durchführen?

Meines Erachtens kommt es nicht ausschließlich darauf an, welche Bedeutung einer konkreten Übertragung aus Sicht der Allgemeinheit (iS einer objektiven Betrachtung) beigemessen werden kann. Dies einerseits deshalb, weil – wie oben dargelegt – der Mitteilungscharakter nicht immer aus sich heraus erkennbar sein muss. Andererseits ist eben nicht ein besonderes Geheimnis oder ein bestimmter Inhalt geschützt, sondern generell die Vertraulichkeit jeder Übertragung. Folglich muss bei sämtlichen Kommunikationsformen über Telekommunikationsanlagen oder Computersysteme geprüft werden, welches qualitative Ausmaß (dh ob Gedankeninhalte vermittelt werden oder nicht) für eine bestimmte Übertragung konkret intendiert war. Dazu könnte man sich im Zweifelsfall eines Gedankenmodells bedienen, indem jede Übertragung auf eine Kommunikation zwischen zweier Menschen umgedeutet würde. In dieser Fiktion muss geprüft werden, welche Teile der Summe aller Übertragungsgegenstände als bewusste Mitteilung bzw Information vom Sender an den Empfänger ausdrücklich gewollt war. Lässt sich aus der Art der »Inhalte« für die Allgemeinheit ein Bedeutungsgehalt nicht ableiten, ist in einem nächsten Schritt auf einen – mit den entsprechenden Übertragungs- und Codierungsmodalitäten vertrauten – »Kommunikationspartner« abzustellen.

Im Fall der »leeren« SMS wurden im Body-Teil keine Nutzdaten übermittelt, weshalb »kein Inhalt« gerade der intendierte Inhalt war. Legt man diesen Fall auf das Gedankenmodell um, so wäre deutlich erkennbar, dass gerade diese inhaltsleere Übermittlung der gedankliche Inhalt der Übertragung war. Jene Daten, die dabei für die Form bzw Modalität der Übertragung angefallen sind und übermittelt werden (SMS-Header, Übertragungswege, Quell- und Zieladressen, Protokollinformation, Standortdaten usw) und eben nicht ausdrücklich vom Absender für die zu verteilende Information beabsichtigt und bezweckt waren, fallen nicht unter den Nachrichten(inhalts)begriff des § 119.

896 Siehe etwa die Beispiele der »leeren« SMS oder der Geldausgabeautomaten.

Im Fall des Aufrufs einer Internetadresse würde der Absender der Adressanfrage (nach vorliegendem Gedankenmodell) »per Brief« den Empfängern (vgl Diensteanbietern) den gewünschten URL[897] mitteilen, der hier den intendierten Gedankeninhalt repräsentiert, und zwar gleichgültig, ob sich daraus schlüssige Hinweise auf den Inhalt der Website ergeben oder nicht. Wie bspw im Fall »<www.einszweidrei.org>«, wo die (gedankliche) Erklärung des Absenders nicht in der Zeichenfolge der Zieladresse, sondern in der »Information« liegt, »diese konkrete Website aufzurufen«.[898] Die Besonderheit von Internet-Adressen liegt im sog »Domain-Name-System« (DNS) verborgen, welches es erlaubt, den für eine Kommunikation im Internet[899] notwendigen IP-Adressen[900] zur leichteren Handhabung bei der Verwendung durch Menschen gewisse – einfacher zu merkende – Namen zuzuordnen. Diese Domainnamen werden über sog »Nameserver« in einem hierarchischen Domainnamensystem verwaltet.[901] Aus diesen Namen-Zuordnungen ergibt sich aber, dass den konkreten Domain-Namen bereits inhaltliche Information der aufzurufenden Websites immanent sein können, wie zB »<www.aids-hilfe.net>« Doch ist mE eben der »gedankliche Inhalt« der Übertragung nicht ausschließlich in der deskriptiven DNS-Adresse festzumachen, sondern in der umfassenderen Botschaft, dass der Nutzer diese Website mit diesem Inhalt aufrufen will. Die schützenswerte Mitteilung liegt also darin, dass der »konkrete Nutzer« mit dem Inhalt dieser Website in Verbindung gebracht wird. Dies obwohl der Inhalt der Kommunikation in diesem Fall sehr eng mit dem

---

897 »Uniform Resource Locator«.

898 Siehe zur Untermauerung dieser Ansicht – iZm der Umsetzung der Vorratsdatenspeicherungs-RL 2006/24/EG – § 102a Abs 7 TKG 2003 (BGBl I 27/2011): »Der Inhalt der Kommunikation und insbesondere Daten über im Internet aufgerufene Adressen dürfen auf Grund dieser Vorschrift nicht gespeichert werden«. Man beachte allerdings die Ungültigerklärung der Vorratsdatenspeicherungs-RL mit Urteil des EuGH 08. 04. 2014, C-293/12, C-594/12 (Digital Rights Ireland Ltd bzw Kärntner Landesregierung ua/Bundesregierung ua) = ÖJZ 2014/54, 337 *(Lehofer)* = ecolex 2014, 397 *(Wilhelm)* = ecolex 2014, 576 *(Zankl)* = jusIT 2014/49, 96 *(Klaushofer)* = AnwBl 2014, 371 *(Schrott)* = NLMR 2014, 95 *(Heißl)* = ÖJZ 2014/74, 474 *(Lehofer)* = MR-Int 2014, 17 *(Otto)*.

899 In Netzwerken auf Grundlage der TCP/IP Protokollfamilie (siehe *Balzert,* Lehrbuch², 36; weiters *Hein/Reisner,* TCP/IP², 14 ff).

900 Derzeit noch eine rein nummerische Adresse nach dem IPv4 (nach RFC 791): zB 123.123.123.123 (siehe instruktiv *Kersken,* IT-Handbuch⁵, 220 ff); für die bereits angedachte neue Version IPv6 (nach RFC 2460) zB 4A29:30B4:0031:0000:0000:0092:1A3B:3394 siehe ebenfalls *Kersken,* IT-Handbuch⁵, 233 ff.

901 Siehe *Kersken,* IT-Handbuch⁵, 252 ff.

Vorgang der Kommunikation (hier: Internet-Adresse, die einerseits ein durch § 119 geschütztes Inhaltsdatum repräsentiert und andererseits gleichzeitig auch ein Verkehrsdatum darstellt) verknüpft ist. Die auf die Anfrage folgende Übermittlung des Seiteninhalts einer konkreten Website, ist jedoch grundsätzlich nicht geschützt, da dieser – außer bei geschlossenen Benutzergruppen und individualisierten Inhalten[902] – für die Öffentlichkeit bestimmt ist.[903]

Zur Untermauerung dieser Ansicht ist der Fokus auf den – in Umsetzung der Vorratsdatenspeicherungs-RL[904] – geschaffenen § 102a Abs 7 TKG 2003[905] zu richten, der besagt, dass Inhalte der Kommunikation und insb Daten über im Internet aufgerufene Adressen nicht gespeichert werden dürfen. In den Erl wird verdeutlicht: »[…] damit soll kein Zweifel offen bleiben, dass auch die Umsetzung der Vorratsdatenspeicherungs-RL nicht dazu führt, dass Inhaltsdaten erfasst werden. Nur demonstrativ wird dabei der wichtigste Fall angeführt, nämlich die aufgerufenen Web-Seiten. Erfasst sind aber alle Formen von Kommunikationsinhalten, etwa die Betreffzeile eines E-Mails, Informationen zu Newsgroup-Diensten oder zu Chaträumen, wie IRC-Channels.«[906] Dadurch wird wohl der Inhaltscharakter von Internet-Adressen bestätigt.

Etwaige Verkehrsdaten, Standortdaten usw, die bloß technische Begleiterscheinungen für die tatsächliche Abrufbarkeit darstellen und selbst nicht als Teil der von Menschen beabsichtigten gedanklichen Sendung sind, bleiben daher unberücksichtigt. Diese »äußeren Übertragungsdaten« werden aber prinzipiell von § 119a erfasst.[907]

---

902 Siehe eigenes privates Profil auf diversen sozialen Plattformen oder Abruf des eigenen Kontos über Online-Banking usw.

903 Siehe ähnlich *Wiederin* in Korinek/Holoubek, Bundesverfassungsrecht Art 10a StGG Rz 7.

904 Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, ABl L 2006/105, 54; man beachte allerdings die Ungültigerklärung der Vorratsdatenspeicherungs-RL mit Urteil des EuGH 08.04.2014, C-293/12, C-594/12 (Digital Rights Ireland Ltd bzw Kärntner Landesregierung ua/Bundesregierung ua) = ÖJZ 2014/54, 337 *(Lehofer)* = ecolex 2014, 397 *(Wilhelm)* = ecolex 2014, 576 *(Zankl)* = jusIT 2014/49, 96 *(Klaushofer)* = AnwBl 2014, 371 *(Schrott)* = NLMR 2014, 95 *(Heißl)* = ÖJZ 2014/74, 474 *(Lehofer)* = MR-Int 2014, 17 *(Otto)*.

905 BGBl I 27/2011.

906 Vgl ErlRV 1074 BlgNR XXIV. GP, 26.

907 Siehe S 199 ff.

All diese Überlegungen haben gemein, dass die Übertragung selbst durch das Kommunikations- bzw Übertragungsgeheimnis geschützt ist und es nicht auf die Qualität der Inhalte einer vom Menschen – wenn auch zB mittelbar durch Maschinen – veranlassten Übertragung ankommt.

4. Nachrichten am Übertragungsweg

Der verfassungsrechtliche Schutz der Telekommunikation durch Art 10a StGG und Art 8 EMRK reicht weiter als der Schutz des Kernstrafrechts, da Letzterer mit dem Ende der Kommunikation aufhört.[908] Nach der strafrechtlichen hM[909] ist der Nachrichteninhalt durch § 119 nur solange geschützt, als er sich gerade auf dem »Übertragungsweg« befindet.[910] Demnach sind im Computersystem abgespeicherte Nachrichten (E-Mails, SMS[911], MMS[912], Chat[913]-Protokolle usw), die sich gerade nicht (bzw nicht mehr) am Übertragungsweg befinden, keine tauglichen »Tatobjekte«.[914]

Wird ein E-Mail jedoch gerade verfasst oder ein abgespeichertes E-Mail vom Berechtigten geöffnet, um es zu lesen, so wird es über externe Busleitung von der CPU zum Arbeitsspeicher und zum Bildschirm des Computersystems geladen, weshalb wiederum eine Nachrichtenübertragung »innerhalb des Computersystems« stattfindet. Mit anderen Worten, eine gerade in Bearbeitung befindliche Nachricht, sei es um diese gerade zu verfassen oder nur zu betrachten, ist unabhän-

---

908 Siehe *Thiele* in SbgK § 119 Rz 11.

909 Siehe *Bergauer/Schmölzer* in Jahnel/Mader/Staudegger, IT-Recht[3], 635 (660); weiters *Lewisch* in WK[2] § 119 Rz 9a; auch *Reindl-Krauskopf,* Computerstrafrecht[2], 3; weiters *Seling,* Privatsphäre, 157; die Meinungen zusammenfassend auch *Thiele* in SbgK § 119 Rz 37.

910 Siehe dazu auch *Venier,* Die Online-Durchsuchung. Oder: Die Freiheit der Gedanken, AnwBl 2009, 480; siehe idS auch *Zerbes,* Spitzeln, Spähen, Spionieren. Sprengung strafprozessualer Grenzen durch geheime Zugriffe auf Kommunikation (2010) 21.

911 Short Message Service.

912 Multimedia Messaging Service.

913 Engl für plaudern, sich unterhalten; dabei handelt es sich um eine elektronische Kommunikationsform, die synchron (= in Echtzeit, zB Live-Chat bzw Instant Messaging) oder asynchron (= mit zeitlicher Verzögerung, zB Internetforum oder auch E-Mail) stattfinden kann, siehe dazu auch *Betsch,* Körperlichkeit im Chat (2007) 6 ff.

914 Siehe zu den einzelnen Lehrmeinungen *Thiele* in SbgK § 119 Rz 37.

gig von der Zuordnung zu technischen Kommunikations- bzw Übertragungsformen (zB E-Mail, SMS)[915] ebenfalls geschützt.[916] Dies trifft für jede elektronische Datei zu, die mit einem gedanklichen Inhalt ausgestattet ist und im Wege eines Computersystems übermittelt wird. Dies gilt zB auch für einen Sachverhalt, in dem der Sender (Person A) und der Empfänger (Person B) in gleichzeitiger Anwesenheit vor demselben Computersystem sitzen und A dem B ein Word-Dokument oder ein abgespeichertes E-Mail mit entsprechendem gedanklichen Inhalt am lokalen Bildschirm zur Kenntnisnahme öffnet. Während der Dauer der Betrachtung dieser »Nachricht« wird dieselbe im Wege eines Computersystems übertragen, weshalb § 119 anwendbar ist. »Telekommunikation« ist – wie bereits mehrfach angeführt – jeder technische Vorgang des Aussendens, Übermittelns und Empfangens von Nachrichten jeglicher Art in der Form von Zeichen, Sprache, Bildern oder Tönen mittels dazu dienender technischer Einrichtungen. Das Aussenden der Nachricht geschieht dadurch, dass der »Sender« das Dokument mit der entsprechenden Nachricht für den »Empfänger« am Bildschirm anzeigt. Die dazu dienende technische Einrichtung bildet dabei das Computersystem.

Das soeben Gesagte muss natürlich auch für den Fall sog »Toter Briefkästen«[917] gelten. In Analogie zur herkömmlichen Verwendung von Astlöchern oder Mauernischen werden Nachrichten vom Urheber in Webmail-Programmumgebungen als »Entwurf« verfasst und gespeichert, nicht aber versendet. Der Empfänger, der sich selbst in Kenntnis der Zugangsdaten zu diesem Mail-Service befindet, meldet sich an diesem Server an und liest den vom Sender erstellten Entwurf. Die Mitteilung geht auf diesem Weg, ohne dass sich die Kommunizierenden kennen müssen, dem Rezipienten zu und wird nicht wie üblich kommunikationstechnisch von A nach B übermittelt. Dennoch ist die Mitteilung von § 119 geschützt, nämlich ausschließlich in der Zeit ihres Transportes, wenn sie für das Abrufen oder Weiterbearbeiten über

915 Auch unabhängig der Unterscheidung der Modalität der Übertragung iS eines Kommunikationsdienstes oder Dienstes der Informationsgesellschaft.

916 Siehe mehr dazu gleich im Anschluss.

917 Zur Beschreibung von »toten Briefkästen« in der DDR siehe *Müller-Enbergs,* Inoffizielle Mitarbeiter des Ministeriums für Staatssicherheit. Teil 2: Anleitungen für die Arbeit mit Agenten, Kundschaftern und Spionen in der Bundesrepublik Deutschland.[2] (1998) 185 ff und 740 ff.

technisch bedingte Transportwege[918] (arg »im Wege eines Computersystems«) geleitet wird.

Seling wendet jedoch ein, dass nur solche Informationsübertragungen geschützt seien, bei denen »zwei oder mehrere Personen in Kontakt treten, um miteinander zu kommunizieren«, denn nur in solchen Fällen ginge es um die Übermittlung eines Gedankeninhalts.[919] Dem ist entgegen zu halten, dass sich für eine derartige Konkretisierung weder Hinweise bezüglich der Übertragung im Wege einer Telekommunikation noch für die Übermittlung im Wege eines Computersystems finden.[920] Aus den von *Seling* mit dem Hinweis »in diese Richtung auch« zitierten Quellen[921] lässt sich mE jedenfalls nicht auf diese Einschränkung schließen. Völlig konträr zur Aussage *Selings* stellt der ER (ETS 185) gerade nicht auf ein derart enges Verständnis ab: »The communication in the form of transmission of computer data can take place inside a single computer system (flowing from CPU to screen or printer, for example), between two computer systems belonging to the same person, two computers communicating with one another, or a computer and a person (e.g. through the keyboard)«.[922]

Dass sich auch der nationale, historische Gesetzgeber an diesem weiten Verständnis orientiert hat, belegen wohl neben den Erl[923] auch die ergänzende Formulierung des Gesetzeswortlauts betreffend Übermittlungen »im Wege eines Computersystems«. Dadurch werden auch Übertragungen von Nachrichteninhalten von § 119 erfasst, die grundsätzlich nicht unter eine Telekommunikation (iSd TKG) fallen.[924] Dass das Erfordernis des Gedankeninhalts – nach *Seling*[925] – nur aus einer Kommunikation resultieren kann, bei der zwei oder mehrere Personen in Kontakt treten, ist daher mE nicht zutreffend. Auch aus dem bereits angesprochenen Legalbegriff von »Nachricht« in § 92 Abs 3 Z 7 TKG 2003 ergibt sich nur, dass es sich um eine Information handeln

---

918 Bussysteme dienen ua der Kommunikation zwischen Bestandteilen innerhalb eines Computersystems (siehe *Kersken,* IT-Handbuch[5], 115 und 133 ff).

919 Vgl *Seling,* Privatsphäre, 156.

920 Siehe dazu vielmehr den Begriff »Mensch-Maschine-Kommunikation« in der Informatik bei *Blaschek,* Mensch-Maschine-Kommunikation, in Rechenberg/Pomberger (Hrsg), Informatik Handbuch[4] (2006) 839 (839 ff).

921 Siehe *Seling,* Privatsphäre, 156 (FN 762).

922 Siehe ER (ETS 185) Pkt 55.

923 Siehe dazu ErlRV 1166 BlgNR XXI. GP, 25.

924 Siehe ErlRV 1166 BlgNR XXI. GP, 25.

925 Vgl *Seling,* Privatsphäre, 156.

muss, die zwischen einer endlichen Zahl von Beteiligten ausgetauscht oder weitergeleitet wird. Dabei kommt es lediglich darauf an, dass die Teilnehmer oder Nutzer der Nachricht identifizierbar sein müssen. Nicht vom Nachrichtenbegriff des TKG 2003 erfasst sind daher Informationen, die über einen Rundfunkdienst oder ein Kommunikationsnetz an die Öffentlichkeit übertragen werden. Dass es aber zumindest zwei »Personen« sein müssen, wie *Seling* es darstellt, ergibt sich mE auch daraus nicht. Zudem sei im wiederholten Mal darauf hingewiesen, dass – wie oben ausf dargelegt – der Begriff und das Schutzobjekt des § 119 (arg »Inhalt einer Nachricht«) losgelöst von der telekommunikationsrechtlichen Terminologie zu betrachten sind und autonomen Charakter besitzen. Richtig ist vielmehr, dass jeder »Transmissionsprozess« eine aus Sender, Sendung und Empfänger bestehende Struktur beschreibt.[926] Diese Elemente haben allerdings ausschließlich einen funktionalen Charakter, sodass die Funktionen des Senders und Empfängers grundsätzlich[927] auch in ein und derselben Person zusammentreffen können.

Das Übermitteln eines E-Mails mit einem gedanklichen Inhalt, das sich der Absender selbst adressiert[928], muss wohl ebenfalls vom Telekommunikations- bzw Übertragungsgeheimnis geschützt sein. Auch hier bedient sich der Versender der elektronischen Übertragung zur Nachrichtenübermittlung. Doch selbst wenn man *Selings* Aussage ausschließlich auf den Begriff der Telekommunikation beziehen würde[929], sodass diese dadurch definiert würde, dass stets zwei oder mehrere Personen in Kontakt treten müssen, wäre sie auch deshalb schon falsch, da ein Erfordernis multipler Personen, für einen »Schutz des Übertragungsvorganges« unbedeutend ist.[930] Auch solche am Übertra-

926 Siehe *Reisinger,* Rechtsinformatik, 126.

927 Sofern technisch möglich.

928 ZB weil der Versender gerade in seiner Freizeit einen Einfall hatte, den er sich zur weiteren Bearbeitung an seine vom Arbeitsplatz abrufbare E-Mail-Adresse geschickt hat, oder sich eine Mitteilung einer anderen Person an seine E-Mail-Adresse, die von zuhause aus abrufbar ist, weitergeleitet hat, um sie auf dem privaten PC zu archivieren.

929 Was jedoch nicht in seinem Sinn ist, da er dabei generell von »Informationsübertragungen« spricht und im Folgenden als Beispiele »Telefonate und E-Mails zwischen zwei Personen« nennt und daher sowohl auf die Telekommunikation als auch auf die Übertragung im Wege eines Computersystems Bezug nimmt (siehe *Seling,* Privatsphäre, 156).

930 Ebenso liefert die mehrfach angesprochene Definition der Telekommunikation, die der Gesetzgeber darunter wohl verstanden wissen will, keinen Anhaltspunkt

gungsweg befindliche Nachrichten werden von § 119 erfasst, die sich der Inhaber eines Anrufbeantworters[931] selbst von einem externen Anschluss aus auf diesen spricht.[932] Die obigen Ausführungen haben deutlich aufgezeigt, dass gerade die Vertraulichkeit solcher Übertragungen im Wege einer Telekommunikation oder über ein Computersystem geschützt sein soll. Dasselbe gilt natürlich auch für Inhaltsdaten[933], die der Berechtigte für sich selbst in einen externen Online-Speicher[934] als Nachricht[935] an sich selbst überträgt. Während des Übertragungsvorgangs genießen daher auch solche Nachrichten den Schutz des § 119. Freilich muss dabei geprüft werden, ob tatsächlich eine »Nachricht« als Übermittlung eines gedanklichen Inhalts vorliegt. Das Übertragungsmedium – dh ob im Wege einer Telekommunikation oder eines Computersystems – spielt dabei nur eine sehr untergeordnete Rolle, da beide Übertragungswege tatbestandlich erfasst sind. Man kann daher in diese Richtung argumentieren, dass für eine »Kommunikation« stets ein Anfang und ein Ende (Ursprung und Ziel) determiniert sein muss, weshalb zumindest zwei »funktionale« Anschlüsse (wie zB Sender und Empfänger) für eine Übertragung notwendig sind. Dabei ist es unbeachtlich, wem diese Anschlüsse zuzuordnen sind.[936] Zur Unterstützung dieser Argumentation kann auch § 94 Abs 4 erster Satz TKG

---

für eine derartige Auffassung. »Telekommunikation« ist als technischer Vorgang des Aussendens, Übermittelns und Empfangens von Nachrichten jeglicher Art in der Form von Zeichen, Sprache, Bildern oder Tönen mittels dazu dienender technischer Einrichtungen zu verstehen (Vgl ErlRV 1325 BlgNR XXII. GP, 6; ausdrücklich auch in ErlRV 1505 BlgNR XXIV. GP, 6).

931 Grundsätzlich genießen Anrufbeantworter, Mailboxen sowie in Übertragungsnetze eingebundene Computer als Endgeräte Schutz nach Art 10a StGG (siehe *Wiederin* in Korinek/Holoubek, Bundesverfassungsrecht Art 10a StGG Rz 6 mwN); siehe dazu auch den Hinweis in FN 49 zu Inhalten einer Telekommunikation bei *Schmölzer,* Überwachung von Nachrichten und Auskunft über Daten einer Nachrichtenübermittlung nach altem und nach neuem Recht. Von der Fernmelde- zur Telekommunikations-Überwachung – eine problemorientierte Genealogie, in Moos/Jesionek/Müller (Hrsg), Strafprozessrecht im Wandel, FS Miklau (2006) 467 (475).

932 ZB um ihn als eine Art »Gedankenspeicher« zu nutzen.

933 Im Sinne von elektronischen Dokumenten mit gedanklichem Inhalt.

934 Online-Speicherplatz oder -Backup; siehe dazu für viele Anbieter <www.a1.net/hilfe-support/online-festplatte> (01.04.2014).

935 ZB in Form eines Word-Dokuments, das den Kommunikator (der in diesem Fall selbst auch der Rezipient ist) an diverse Termine, Aufgaben oder Ereignisse erinnern soll. Als Beispiel kann weiters die Übermittlung einer Word-Einkaufsliste vom PC an das eigene Smartphone des Urhebers genannt werden.

936 Siehe dazu die angeführten Beispiele des selbst geschickten E-Mails und dem Telefonat mit seinem eigenen Anrufbeantworter.

2003 herangezogen werden, wo ausdrücklich der »Sender und Empfänger« erwähnt wird. Ebenso wird zu den (mittlerweile durch den VfGH[937] als verfassungswidrig aufgehobenen) Vorratsdaten in § 102a Abs 4 Z 3 und 4 TKG 2003 idF BGBl I 27/2011 auf den »Absender und Empfänger« eines E-Mails abgestellt. In den Erl[938] wird dazu klargestellt:

»Absender ist die letztübermittelnde Kommunikationseinrichtung mit einer zugeordneten öffentlichen IP-Adresse, die nicht notwendigerweise mit der IP-Adresse des Absenders des E-Mails übereinstimmt, und, – z. B. bei Webmail – auch mit der IP-Adresse des versendenden Mailservers ident sein kann. Die Absender E-Mail-Adresse ist nicht notwendigerweise einem bestimmten Teilnehmer zuordenbar, da im E-Mail-Protokoll die dynamische Erzeugung einer Absender-Adresse durch den Endbenutzer ohne Mitwirkung des Betreibers möglich ist.«

5. Telekommunikation vs Computersystem

Die tatbestandliche Festlegung auf Nachrichten, die entweder im Wege einer Telekommunikation oder mittels eines Computersystems übertragen werden, mag verwirren, erfasst doch die Telekommunikation als technischer Vorgang bereits das Aussenden, Übermitteln und Empfangen von Nachrichten jeglicher Art in der Form von Zeichen, Sprache, Bildern oder Tönen mittels dazu dienender technischer Einrichtungen.[939] Wie oben bereits ausgeführt bleibt dieses Begriffsverständnis auch nach dem notwendig gewordenen Entfall[940] des ausdrücklichen Verweises auf das TKG[941] weiterhin aufrecht.[942]

So fallen die klassische Sprachtelefonie über Fest- oder Mobilfunknetze, Nachrichten per Fernschreiber und Telegrafen[943], Fax[944] und

937 VfGH 27.06.2014, G 47/2012 ua.
938 Siehe ErlRV 1074 BlgNR XXIV. GP, 24.
939 Vgl ErlRV 1325 BlgNR XXII. GP, 6.
940 § 3 TKG, auf den in § 119 StGB ausdrücklich Bezug genommen wurde, ist zusammen mit dem gesamten TKG (1997) am 19.03.2003 außer Kraft getreten. Mit dem TKG 2003 (BGBl I 70/2003), das am 20.08.2003 in Kraft getreten ist, wird nun keine Legaldefinition von »Telekommunikation« mehr vorgenommen, weshalb das Klammerzitat nicht mehr zutreffend war.
941 TKG (1997), BGBl I 100/1997.
942 Siehe ErlRV 1325 BlgNR XXII. GP, 6.
943 Siehe *Thiele* in SbgK § 119 Rz 39 mit weiteren Beispielen.
944 Vgl ER (ETS 185) Pkt 51.

auch die IP-Telefonie[945] sowie diverse Datenübertragungen (zB per E-Mail, SMS, MMS) bereits unter den Begriff der »Telekommunikation«.[946] Daher wurde auch der ursprünglich engere Begriff des »Fernmeldeverkehrs«, der grundsätzlich auf die Sprachtelefonie abstellte, in den die neuen Kommunikationsformen einschließenden Begriff der Telekommunikation abgeändert.[947] In Umsetzung des Art 3 CCC, indem ausdrücklich von »non-public transmissions of computer data to, from or within a computer system« gesprochen wird, hat der Gesetzgeber auch die Übertragung im Wege eines Computersystems in den Gesetzeswortlaut aufgenommen. Er weist insb darauf hin, dass der Begriff »Computersystem« nach der CCC sehr weit verstanden wird. Daher werden auch Kommunikationsformen davon erfasst, die über eine Telekommunikation iSd TKG hinausgehen.[948] Daraus kann einerseits geschlossen werden, dass auch moderne digitale Telekommunikationsvorgänge bereits von der umfassenderen Übertragungsform und daher der Formulierung »im Wege eines Computersystems« erfasst werden[949], wie auch der Datentransfer[950] im Internet. Andererseits werden aber von dieser Übertragungsmodalität auch Transmissionen tatbestandlich erfasst, die sich innerhalb eines Computersystems zutragen können. Im Zusammenhang mit Keylogger-Programmen ist festzuhalten, dass auch eine Übertragung innerhalb eines Computersystems tatbildlich ist (wie bspw zwischen CPU[951] und Bildschirm oder Drucker, aber auch zwischen dem User und dem Computer über die Tastatur).[952] Dies geht

945 Auch Internet-Telefonie oder Voice-over-IP (VoIP) genannt; dabei wird ein Gespräch in digitalisierter Form in Echtzeit über ein paketvermittelndes Datennetz mittels des (TCP/)IP-Protokolls übertragen; siehe dazu *Hein/Reisner,* TCP/IP², 499 f.

946 Vgl auch ErlRV 1316 BlgNR XXII. GP, 5.

947 Siehe dazu zutreffend *Schmölzer* in FS Miklau, 467 (471).

948 Siehe ErlRV 1166 BlgNR XXI.GP, 25.

949 Siehe zur Konvergenz von Kommunikationstechnologie und Informationstechnologie auch S 15 ff.

950 Siehe dazu *Reindl-Krauskopf* in WK² § 119a Rz 6.

951 Central Processing Unit; siehe dazu *Tanenbaum,* Computerarchitektur⁵, 71 ff.

952 Siehe den ausdrücklichen Wortlaut von Art 3 CCC: »[…] within a computer system […]«; siehe dazu ER (ETS 185) Pkt 55: »The communication in the form of transmission of computer data can take place inside a single computer system (flowing from CPU to screen or printer, for example), between two computer systems belonging to the same person, two computers communicating with one another, or a computer and a person (e.g. through the keyboard). Nonetheless, Parties may require as an additional element that the communication be transmitted between computer systems remotely connected.«

aus § 119 – anders als in Art 3 CCC – nicht ausdrücklich hervor. Werden daher, wie bei der Verwendung eines Keyloggers, Nachrichten während ihrer Übertragungsphase über externe Busleitungen[953] vom Spionageprogramm mitprotokolliert, ist § 119 prinzipiell anwendbar. Aber auch Nachrichtenübertragungen zwischen zwei Computersystemen ein und derselben Person[954] sowie die Übertragung in einem Computernetzwerk (zB LAN) generell werden davon umfasst.[955] Zusammenfassend ist davon auszugehen, dass sämtliche Übertragungen (einschließlich Telekommunikationsvorgänge) über technische Systeme von § 119 berücksichtigt werden. Hier kann auf ER (ETS 185) Pkt 206 verwiesen werden, wo richtigerweise bereits erkannt wurde: »The distinction between telecommunications and computer communications, and the distinctiveness between their infrastructures, is blurring with the convergence of telecommunication and information technologies«.

Was jedoch von § 119 nicht erfasst wird, ist das Ausspionieren von Nachrichteninhalten durch die Rekonstruktion der elektromagnetischen Abstrahlung eines Computersystems. Eine solche Abstrahlung stellt einerseits keine spezifizierte Datenübertragung oder Telekommunikation dar, und andererseits sind »elektromagnetische Wellen« auch keine Computerdaten im eigentlichen Sinn.[956] Der Gesetzgeber verzichtet in diesem Fall auf den höheren Schutz von Nachrichteninhalten durch geringere Vorsatzanforderungen und überlässt eine solche Spionage von Inhalten, die über das Abfangen elektromagnetischer Wellen eines Computersystems dem Täter zugänglich werden, ausschließlich dem § 119a Abs 1 zweiter Deliktsfall.[957]

---

953 Interne Busleitungen werden verwendet, um Daten innerhalb der CPU zu transportieren, externe Busse verbinden zB die CPU mit den Eingabe/Ausgabe-Geräten und dem Arbeitsspeicher; siehe *Tanenbaum,* Computerarchitektur[5], 195 f; weiters *Hellwagner,* Arbeitsspeicher- und Bussysteme, in Rechenberg/Pomberger (Hrsg), Informatik Handbuch[4] (2006) 363 (372); *Gumm/Sommer,* Informatik[10], 41.

954 Vgl dazu ER (ETS 185) Pkt 55.

955 Siehe zum Begriff »Computersystem« ab S 75.

956 Siehe dazu ER (ETS 185) Pkt 57: »The creation of an offence in relation to ›electromagnetic emissions‹ will ensure a more comprehensive scope. Electromagnetic emissions may be emitted by a computer during its operation. Such emissions are not considered as ›data‹ according to the definition provided in Article 1. However, data can be reconstructed from such emissions. Therefore, the interception of data from electromagnetic emissions from a computer system is included as an offence under this provision«.

957 Siehe dazu gleich im Anschluss ab S 207.

Es ist allerdings nicht hinreichend verständlich, warum der Gesetzgeber iZm dem Abfangen von elektromagnetischer Emission nicht weiterhin dem Regime des unterschiedlichen Schutzniveaus der anvisierten »Informationsqualität« – Nachrichtenspionage (§ 119) oder Datenspionage (§ 119a) – treu bleibt. Es kann letztlich aus Sachlichkeitserwägungen heraus die Frage nicht abschließend beantwortet werden, warum gerade Inhaltsdaten, von denen sich ein Unbefugter im Wege der Rekonstruktion von aufgefangenen elektromagnetischen Wellen Kenntnis verschaffen will, nicht dem Regelungsmodell des § 119 entsprechend geschützt werden.[958]

6. Unbefugter

Der Täter muss ein Unbefugter sein, weshalb jemand, zu dessen Kenntnisnahme die Mitteilung bestimmt ist, nicht als Täter in Betracht kommt. Als Unbefugter ist aber auch der Inhaber einer Kommunikationsinfrastruktur iZm der Übertragung von Mitteilungen, anderer Personen zu qualifizieren, sofern die Nachrichten nicht für ihn bestimmt sind.[959] Als befugt wird folglich jeder rechtmäßig beteiligte Kommunikationsteilnehmer[960] iSv (Ab-)Sender und Empfänger(n) zu werten sein. Greift jemand »befugterweise« auf die Kommunikationsinhalte zu, der selbst kein Kommunikationspartner ist – wie etwa ein Systemadministrator, wenn er im Zuge einer Fehlersuche auf den Inhalt eines (nicht für ihn bestimmten) E-Mails[961] zugreift – so kann unter gewissen Umständen dieser Zugriff befugt erfolgen, weshalb bereits der objektive Tatbestand ausgeschlossen ist. So weitreichend wie die Befugnis eines Systemadministrators in den Erl offenbar begriffen wird, darf sie mE in den meisten Fällen bei weitem nicht reichen: »Fallkonstellationen, in denen bspw Systemadministratoren befugterweise (den Inhalt von) E-Mails analysieren, sind – ohne dass dies ausdrücklich[962] gesagt werden müsste – von der Strafbarkeit ausgenommen«.[963]

---

958 Mehr dazu zu § 119a Abs 1 zweiter Deliktsfall.

959 Siehe *Lewisch* in WK² § 119 Rz 9b; weiters *Thiele* in SbgK § 119 Rz 43; dazu bereits auch JAB 959 BlgNR XIII. GP, 25.

960 In diesem Sinne *Leukauf/Steininger,* StGB³ § 119 Rz 22; vgl weiters ErlRV 1166 BlgNR XXI. GP, 26.

961 Dazu *Thiele* in SbgK § 119 Rz 42; vgl auch ErlRV 1166 BlgNR XXI. GP, 26.

962 Das »s« wurde vom Autor ergänzt, da es im Original fehlt.

963 Vgl ErlRV 1166 BlgNR XXI. GP, 26.

Warum sollte der Inhalt von übermittelten Nachrichten von einem Administrator eingesehen werden dürfen? Auch ein Postbote darf einen Brief nicht öffnen, um etwa Zustelladressen zu überprüfen udgl. Was den Übermittlungsdienst einer Nachrichtenübermittlung betrifft, zB Briefzustellung durch Postboten oder Provider für eine elektronische Nachricht, ist das »Fernmeldegeheimnis« mit dem Briefgeheimnis vergleichbar.[964] Der Übermittlungsdienst garantiert die Integrität des Übertragungsweges, und auf diesem sind die Nachrichten geschützt. Einen Systemadministrator von vornherein als Befugten anzusehen, ist mE eine völlige Fehleinschätzung.[965] Selbst wenn ein Systemadministrator über das Computersystem[966] eines Kommunikationsteilnehmers verfügen darf, bedeutet dies nicht, dass dieser Nachrichteninhalte, die eben nicht für ihn bestimmt sind, von vornherein einsehen darf. Die diesbezügliche Aussage in den GMat müsste viel differenzierter ausfallen. Vergleichbar wäre ein derartiger Sachverhalt in etwa mit einem Gespräch, das jemand über eine Telefonanlage führt, die diesem nicht alleine gehört.[967] In diesem Fall darf der andere Verfügungsberechtigte nicht allein aus der Tatsache heraus, dass er auch ein (Mit-)Berechtigter ist, ableiten, zum heimlichen Abhören mittels einer Wanze befugt zu sein. Auch bei einer E-Mail-Kommunikation muss man darauf vertrauen können, dass kein Administrator die Nachricht mitliest. Eine Administratoreneigenschaft kann keinen Freibrief zur Ermittlung von Kommunikationsinhalten darstellen. Andernfalls würde der Gesetzgeber die Funktionsfähigkeit eines Computersystems oder eine Telekommunikationsanlage über das durch Grundrechte eingeräumte Übertragungs- bzw Kommunikationsgeheimnis (Art 10a StGG)[968] bzw den Schutz der Privatsphäre (Art 8 EMRK) stellen. Ein Administrator muss in Ausübung seiner Tätigkeit äußerst zurückhaltend[969] vorge-

964 *Zerbes,* Spitzeln, 21.

965 Siehe auch *Lewisch,* der ebenso meint: »Befugt greift auch etwa der Systemadministrator auf Nachrichten zu« und für Einzelheiten auf *Reindl-Krauskopf* bezüglich § 118a verweist (siehe *Lewisch* in WK² § 119 Rz 9b). Gleichwohl betrifft aber § 118a Abs 1 die Verfügungsbefugnis über ein Computersystem, nicht einen ggf Befugten im Rahmen von Kommunikationsinhalten während der Übertragung.

966 Was nicht automatisch bedeutet, dass er auch über das Computersystem des bzw der anderen Kommunikationspartner(s) verfügen darf.

967 Siehe wenige Sätze oberhalb. Vgl dazu *Lewisch* in WK² § 119 Rz 9b; weiters *Thiele* in SbgK § 119 Rz 43; dazu bereits auch JAB 959 BlgNR XIII. GP, 25.

968 Beachte, dass Art 10a StGG unter Richtervorbehalt steht.

969 Was streng im Einzelfall zu prüfen sein wird.

hen und wird nur dann auf Inhalte Zugriff nehmen dürfen, wenn zur Fehleranalyse eines Netzwerks die Benützung einer Vorrichtung, die eine Kenntnisverschaffung der übermittelten Nachricht ermöglicht, unvermeidbar ist. Zu diesem Zweck müssen doch wohl die Kommunikationspartner über derartige Maßnahmen im Vorfeld entsprechend informiert werden, was ggf auch die Übertragungsrichtung der Kommunikation betrifft.[970] Wird eine derartige Maßnahme notwendig, so kann der Telekommunikationsteilnehmer, der vom Administrator angemessen über das Benützungsvorhaben einer entsprechenden Vorrichtung vorab informiert wurde, selbst entscheiden, ob er während dieser Fehleranalyse den »überwachten« Dienst zur Kommunikation nutzen will. Doch auch wenn beide Übertragungsrichtungen betroffen wären, müsste der andere Kommunikationspartner, der eben von der IT-Maßnahme nicht im Vorhinein informiert werden konnte, zumindest im Nachhinein aufgeklärt werden. Hinsichtlich der Kommunikationsinhalte ist der Systembetreuer daher grundsätzlich ein Unbefugter. Würde man von vornherein eine Befugnis jedes Systemadministrators ableiten, schlösse dies bereits den Tatbestand aus. Darüber hinaus kann sich für einen Administrator auf Tatbestandsebene die Straflosigkeit mangels tatbestandlicher Vorrichtung[971] oder wegen Nichterfüllung des subjektiven Tatbestands ergeben.

7. Sonstiges

§ 119 ist entsprechend der Systematik der Tatbestände zum Schutz der Privatsphäre im Kernstrafrecht[972] durch Abs 2 als Ermächtigungsdelikt iSd § 92 StPO ausgestaltet. Dies ist damit zu begründen, dass bei strafbaren Handlungen, die die Privatsphäre eines Menschen gefährden, dieser letztlich entscheiden kann, ob die Strafverfolgungsbehörden weitere Ermittlungen in seiner Privatsphäre durchführen sollen. Will er dies nicht, kann der Verletzte die Ermächtigung verweigern.[973]

Die Kriminalpolizei oder die Staatsanwaltschaft haben gem § 92 Abs 1 StPO nämlich unverzüglich bei der gesetzlich berechtigten Per-

970 Gemeint ist damit, ob nur ausgehende oder auch eingehende E-Mails davon betroffen sind.

971 Siehe dazu die obigen Ausführungen.

972 Beachte im Nebenstrafrecht das Delikt des § 51 DSG 2000, das erst jüngst in ein reines Offizialdelikt umgewandelt wurde (S 117 ff).

973 Vgl *Birklbauer/Hilf/Tipold,* Strafrecht BT I² §§ 119, 119a, 120 Abs 2a Rz 19.

son anzufragen, ob sie die Ermächtigung erteilt. Wird diese verweigert, so ist jede weitere Ermittlung gegen die betreffende Person unzulässig und das Verfahren einzustellen. Die Ermächtigung gilt als verweigert, wenn die berechtigte Person sie nicht binnen vierzehn Tagen nach Anfrage erteilt.

Spätestens jedoch muss die Ermächtigung gem § 92 Abs 2 StPO bei Einleitung diversioneller Maßnahmen oder Einbringen der Anklage vorliegen und kann bis zum Schluss des Beweisverfahrens erster Instanz auch zurückgenommen werden.

Als Verletzte werden im Sinn dieser Bestimmung zunächst diejenigen verstanden, zu deren Kenntnisnahme die Nachricht bestimmt ist. Schließlich kommt im Fall des Kompromittierens einer Nachrichtenübertragung auch der Absender der Nachricht als ein Verletzter in Betracht.[974]

Aufgrund der Strafdrohung ist sachlich das Bezirksgericht zuständig (§ 30 Abs 1 StPO).

D. Missbräuchliches Abfangen von Daten (§ 119a)

> § 119a (1) Wer in der Absicht, sich oder einem anderen Unbefugten von im Wege eines Computersystems übermittelten und nicht für ihn bestimmten Daten Kenntnis zu verschaffen und dadurch, dass er die Daten selbst benützt, einem anderen, für den sie nicht bestimmt sind, zugänglich macht oder veröffentlicht, sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen, eine Vorrichtung, die an dem Computersystem angebracht oder sonst empfangsbereit gemacht wurde, benützt oder die elektromagnetische Abstrahlung eines Computersystems auffängt, ist, wenn die Tat nicht nach § 119 mit Strafe bedroht ist, mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.
>
> (2) Der Täter ist nur mit Ermächtigung des Verletzten zu verfolgen.[975]

974 Siehe dazu ErlRV 1166 BlgNR XXI. GP, 26 mit Verweis auf *Leukauf/Steininger,* StGB[3] § 119 Rz 22.

975 BGBl 60/1974 idF I 56/2006.

Gemeinsam mit § 119 bildet § 119a das Umsetzungspaket von Art 3 CCC. § 119a hat in dieser Systematik in mehrfacher Hinsicht Auffangcharakter.[976] Zum einen schützt § 119a Abs 1 erster Fall vor Spionagehandlungen, die nicht schon von § 119 hins »Nachrichteninhalten« erfasst werden[977], und fokussiert darüber hinaus auf alle sonstigen Daten iSd § 74 Abs 2 als Schutzobjekt. Zum anderen wird aber auch das widerrechtliche Auffangen von elektromagnetischer Abstrahlung eines Computersystems tatbildlich behandelt, die zur Rekonstruktion von Computerdaten, aber auch von Nachrichten herangezogen werden kann. In diesem Deliktsfall liegen weder Formen der spezifizierten Tele- und Computerkommunikationen noch Daten (einschließlich Nachrichten) iSd § 74 Abs 2 vor, weshalb eine eigenständige Tatbestandsvariante, die sowohl Nachrichteninhalte als auch sonstige Daten gleichermaßen erfasst, in § 119a Abs 1 zweiter Fall geschaffen wurde.

1. § 119a Abs 1 Fall 1

§ 119a Abs 1 Fall 1 schützt das Übertragungsgeheimnis[978] bzw die Vertraulichkeit der nichtöffentlichen Computerdatenübertragung an sich[979]. Diesbezüglich kann auf das oben zu § 119 Abs 1 Gesagte sinngemäß verwiesen werden. Nur die wesentlichen Unterschiede und Besonderheiten, werden daher im Folgenden behandelt. Die Tathandlung (Benützen einer Vorrichtung) und das Tatobjekt (Vorrichtung) sind in beiden Bestimmungen ident.

2. Schutzobjekt und Bezugsobjekt des erweiterten Vorsatzes

§ 119a Abs 1 erster DF behandelt das missbräuchliche Abfangen von Daten iSd § 74 Abs 2 und macht dabei keinen Unterschied, ob es sich um personenbezogene, nicht personenbezogene Daten oder Computerprogramme einerseits handelt, oder andererseits, ob »Mitteilungen« gedanklichen Inhalts oder »sonstige Übertragungsdaten« jeglichen

976 Siehe dazu ErlRV 1166 BlgNR XXI. GP, 27.
977 Durch die ausdrückliche Subsidiaritätsklausel des § 119a Abs 1.
978 Siehe *Reindl-Krauskopf* in WK² § 119a Rz 2.
979 Siehe *Thiele* in SbgK § 119a Rz 7 (Stand März 2007).

Inhalts vorliegen. Wie bereits bei § 119 hins der Nachrichten müssen sich auch die Daten in § 119a gerade am Übertragungsweg befinden.[980]

§ 119a Abs 1 erfasst daher auch die nicht vom Nutzer veranlasste Datenübertragung im Wege eines Computersystems. Über ein Netzwerk verbundene Computersysteme tauschen untereinander permanent Daten aus, die für den Betrieb des Netzwerkes bzw diverser Software-Dienste erforderlich sind. Fängt der Täter über eine tatbildliche Vorrichtung, die an einem solchen Computersystem angebracht oder empfangsbereit gemacht wurde, Daten – wie IP-Adressen und TCP-Port-Nummern usw – von lediglich kommunizierenden Computersystemen respektive Diensten ab, liegt objektiv betrachtet ebenfalls ein Eingriff in eine Computerdatenübertragung vor. Dies selbst dann, wenn die Inhaber der Systeme von diesen Übertragungen nichts wissen. Es kommt bloß darauf an, dass der Täter ein Unbefugter sein muss und die Daten nicht zu seiner Kenntnis bestimmt sein dürfen. Vorrichtungen, die für solche Zwecke – wie dem Abfangen des Datenverkehrs in Netzwerken – Verwendungen finden können, werden als sog »Sniffer« bezeichnet. Anders als bei Trojanischen Pferden ist es nicht erforderlich, dass die inkriminierte Vorrichtung im konkreten Zielsystem des Opfers implementiert wird, sondern es reicht aus, dass eine physische Verbindung mit dem entsprechenden Netzwerksegment besteht.

3. Exkurs: Sniffer und Sniffing-Methoden

Sniffer können als Computerprogramme, die zB auf einem Notebook oder PC installiert sind, oder auch eigenständige Systeme, bestehend aus Hard- und Softwarekomponenten, ausgestaltet sein. Ihre Bezeichnung beruht auf ihrer Fähigkeit, sämtliche Datenpakete[981] in einem Netzwerk »erschnüffeln« zu können.[982] Man nennt sie daher auch »Packet-Sniffer«.[983] Vorauszuschicken ist, dass Sniffer grundsätzlich äußerst nützliche Werkzeuge für Netzwerkadministratoren zur Systemanalyse und Netzwerkpflege darstellen. Sie können sowohl in kabelgebundenen als auch drahtlosen Netzwerken eingesetzt werden und sind nur sehr schwer auszuforschen. Sie befassen sich mit den

980 Vgl *Thiele* in SbgK § 119a Rz 17.
981 Sog »Frames«.
982 Siehe auch *Lichtenstrasser/Mosing/Otto,* ÖJZ 2003/14, 253.
983 Siehe dazu *Moore,* Cybercrime², 34; weiters *Kurose/Ross,* Computernetzwerke⁴, 82.

einzelnen Paketen[984] der unterschiedlichsten Netzwerkprotokolle und Ebenen[985]. Damit ein Sniffer nicht – wie für prinzipiell alle Hosts[986] in einem Netzwerk vorgesehen – nur den an das eigene System adressierten Datenverkehr lesen kann, muss sein Netzwerkadapter in einen entsprechenden Empfangsmodus gesetzt werden, den sog »Promiscuous Mode«[987]. Erst dieser versetzt die Vorrichtung in die Lage, den gesamten Datenverkehr – der über die Netzwerkschnittstelle übertragen wird – anzunehmen, indem die Regel, dass Datenpakete, die nicht für das jeweilige System bestimmt sind, zu verwerfen sind, ignoriert wird. Daher werden auch Ethernet-Frames eines LAN, die vom physikalischen Übertragungsmedium weitergeleitet werden, vom Sniffer angenommen, die nicht für diesen bestimmt sind. Doch reicht die Manipulation des Empfangsmodus allein nur in sehr einfach gestalteten Netzwerken (zB über sog »Hubs«[988]) tatsächlich aus.

Beim ARP-Spoofing[989] oder ARP-Cache-Poisoning[990] wird auf das »Adress Resolution Protocol«[991] gesetzt, das die Aufgabe hat, (Software-)IP-Adressen in die jeweiligen (Hardware-)MAC-Adressen[992] umzuwandeln. Das Internet Protokoll arbeitet auf der Internet-Schicht der

---

984 Übertragene Byte-Ströme nach dem zB TCP-Schichtenmodell werden folgend genannt: Streams (Application Layer), TCP-Segments (Transport Layer), IP-Datagrams (Internet Layer) und Ethernet-Frames (Network Layer); mehr dazu unter *Hunt,* TCP/IP³, 10.

985 Siehe statt aller zum OSI-7-Schicht-Modell *Hunt,* TCP/IP³, 7; zum TCP/IP-Referenzmodell siehe *Hunt,* TCP/IP³, 10 ff.

986 »Host« (engl für Gastgeber) bezeichnet jeden Computer, der an ein Netzwerk angeschlossen ist und mit anderen Systemen kommuniziert (siehe *Kersken,* IT-Handbuch⁵, 181).

987 Siehe dazu *Kersken,* IT-Handbuch⁵, 197; weiters *Hunt,* TCP/IP³, 146; weiters bereits *Bergauer* in BMJ, 35. Ottensteiner Fortbildungsseminar, 27 (33 ff).

988 Die einfachste Form eines zentralen Verteilers in Ethernet-Netzwerken (siehe *Kersken,* IT-Handbuch⁵, 201): An einem Port des Hub einlangende Daten, werden an alle anderen Ports weitergeleitet. Das angeschlossene System, an das diese Datenpakete adressiert sind, nimmt diese zur Weiterverarbeitung an, die anderen Systeme verwerfen die Daten.

989 Unter »Spoofing« versteht man generell das Vortäuschen einer Tatsache; siehe zum ARP-Spoofing bereits *Bergauer,* RdW 2006/391, 412; weiters *Bergauer* in BMJ, 35. Ottensteiner Fortbildungsseminar, 27 (34 f).

990 Auch als ARP-Poisoning bezeichnet; »Poisoning« lehnt sich dabei an der Methode an, dass der ARP-Pufferspeicher eines Hosts durch manipulierte ARP-Pakete »vergiftet« wird.

991 Spezifiziert in RFC 826.

992 Media Access Control-Adressen (auch Hardware-Adressen) sind weltweit eindeutige und festvergebene Identifikationsnummern jeder Netzwerkkarte bzw überhaupt jedes Netzwerkadapters (siehe *Kersken,* IT-Handbuch⁵, 197).

TCP/IP-Protokollhierarchie und ist in der Lage die verschiedensten Datennetze mit den unterschiedlichsten Adressierungsmechanismen zu unterstützen[993], doch können zur Verarbeitung der Datenpakete auf der darunterliegenden Netzzugangsschicht[994] die IP-Adressen nicht ausgewertet werden. Aus diesem Grund versieht das ARP auf dieser Schicht seinen Dienst, um die IP-Adressen der IP-Datagramme in die Ethernet-Adressen (= MAC-Adressen der physischen Schicht) umzuwandeln.[995] Dazu wird von der ARP-Software eine idR dynamische Übersetzungstabelle verwaltet, die in Form eines Pufferspeichers (sog »ARP-Cache«) automatisch vom Protokoll selbst aufgebaut wird. Erhält das ARP die Aufforderung, eine IP-Adresse in die korrespondierende MAC-Adresse aufzulösen, sucht es zuerst in dieser Tabelle nach einem entsprechenden Eintrag. Wird ein Eintrag gefunden, kann das Datenpaket an das System mit der konkreten MAC-Adresse weitergereicht werden. Kann die Adresse im ARP-Cache nicht gefunden werden, sendet das ARP einen ARP-Request als sog »Broadcast-Paket«[996] mit der IP-Adresse, für welche die MAC-Adresse gesucht wird, an alle verbundenen Hosts. Erkennt eines dieser Systeme die ihm zugeordnete IP-Adresse, antwortet es mit einem ARP-Reply-Paket, das seine MAC-Adresse enthält. Das ARP legt daraufhin diese Zuordnung im ARP-Cache an und leitet das Datenpaket an den konkreten Host weiter.[997] Jeder Host im LAN verwaltet einen solchen ARP-Cache, um nicht ständig MAC-Adressen auflösen zu müssen. Um Inkonsistenzen zu vermeiden, werden die einzelnen Tabelleneinträge idR periodisch aktualisiert bzw gelöscht.[998]

Beim ARP-Cache-Poisoning wird nun das Computersystem, das Daten über das Internet an eine Empfangsstation versenden will, dazu veranlasst, die Datenpakete anstatt wie üblich zB über das Standard-Gateway des Subnetzes an das System des Täters zu leiten. Nachdem der Täter die Datenpakete erhalten und gespeichert hat, leitet er diese

993 Siehe *Hein/Reisner,* TCP/IP², 22 f.
994 ZB Ethernet; Die Netzzugangsschicht ist die unterste Schichte des TCP/IP-Protokollhierarchie.
995 Siehe *Hunt,* TCP/IP³, 46 f.
996 Unter Broadcast (engl für Ausstrahlung, Rundfunk) versteht man eine an alle Hosts eines konkreten Netzwerks adressierte Meldung (siehe *Kersken,* IT-Handbuch⁵, 222).
997 Siehe *Hunt,* TCP/IP³, 47.
998 Siehe statt aller *Hunt,* TCP/IP³, 43.

in weiterer Folge tatsächlich über das Standard-Gateway[999] zum Empfänger weiter.[1000] Um sich anstelle des Standard-Gateways in Position zu bringen, sendet der Angreifer dem auszuspionierenden System unaufgefordert ARP-Reply-Pakete, die diesem System die Adresse des Angreifer-Computers als Adresse des Standard-Gateways vortäuscht.[1001] Da die ARP-Spezifikation erlaubt, dass auch unaufgeforderte ARP-Replys im ARP-Cache gespeichert werden, wird bei einer konkreten Datenübermittlung des Zielsystems in weiterer Folge ungeprüft die im ARP-Cache gespeicherte Adresse des vermeintlichen Gateways zum Datentransfer ins Internet verwendet. Tatsächlich aber werden die Datenpakete über die verdeckte Zwischenstation des Täters geleitet, der sie erst nach lokaler Speicherung ins Internet per IP-Forwarding weiterleitet. Man nennt solche Angriffe auch »Man-in-the-Middle-Attack«[1002]. Das Opfer bemerkt grundsätzlich von diesen Vorgängen im Hintergrund nichts.

In Netzwerksegmenten, deren zentraler Verteiler (zB Switch[1003]) eine virtuelle Punkt-zu-Punkt-Verbindung zwischen den einzelnen Kommunikationspartnern herstellen kann, muss allerdings zusätzlich die Arbeitsweise des Switchs manipuliert werden. Ein Switch speichert in einer »Switch-Tabelle«[1004] nicht nur die MAC-Adressen seiner angeschlossenen Hosts dynamisch, sondern merkt sich dazu auch den jeweiligen Hardware-Port, an dem dieser Host am Switch angeschlossen ist. Aus diesem Grund findet über die anderen Ports prinzipiell auch kein fremder Datenverkehr statt. Datenpakete werden direkt an den Port weitergeleitet, mit dem die gewünschte MAC-Adresse verbunden ist.[1005]

---

999 Auch als »Default-Gateway« oder »Standard-Router« bezeichnet, nimmt alle Daten entgegen, die weder für das lokale Netzwerk noch für ein Netzwerk mit einem bestimmten Router adressiert sind (siehe *Kersken,* IT-Handbuch[5], 237).

1000 Siehe *Thome/Sollbach,* Grundlagen und Modelle des Information Lifecycle Management (2007) 229 f.

1001 Siehe dazu *Eckert,* IT-Sicherheit[9], 124.

1002 Siehe dazu allgemein *Borges/Schwenk/Stuckenberg/Wegener,* Identitätsdiebstahl, 48 ff.

1003 Ein Switch speichert die MAC-Adressen aller angeschlossenen Schnittstellen (individuelle Nummer eines Netzwerkadapters der angeschlossenen Systeme) eines Netzwerksegments, sodass an die verbundenen Systeme nur jene Daten gelangen, für die diese auch bestimmt sind. Dies ermöglicht jedem angeschlossenen Computersystem – im Gegensatz zu einem »Hub« – die volle Bandbreite zu nutzen; siehe ua dazu *Kersken,* IT-Handbuch[5], 201.

1004 Wird auch als »MAC-Adressen-Tabelle« bezeichnet.

1005 Siehe dazu *Kurose/Ross,* Computernetzwerke[4], 523.

Damit nun auch der Angreifer auf dem Port des Switches, an dem sein Sniffer angeschlossen ist, den gesamten Datenverkehr des Netzwerksegments mitlesen kann, sendet er viele modifizierte Ethernet-Frames, die jeweils eine andere MAC-Adresse als Quelladresse vortäuschen, an den Switch.[1006] Dadurch wird für jedes Paket ein neuer Eintrag mit MAC-Adresse und Port in der Switch-Tabelle gespeichert. Ist die Speicherkapazität der Tabelle erschöpft, leitet der Switch – um den Netzwerkbetrieb aufrechtzuerhalten – jedes weitere Datenpaket an alle Ports des Switches weiter. Dadurch »fluten« diese Pakete das komplette Netzwerksegment und sind somit auch auf dem Port, an dem der Sniffer angeschlossen ist, ersichtlich.[1007] Der Sniffer kann nun durch den speziellen Empfangsmodus seines Netzwerkadapters ungehindert den gesamten Netzwerkverkehr aufzeichnen.

(Exkurs Ende)

Im Verhältnis von § 119a zu § 119 ist auch auf die tatbestandlichen »Übertragungswege« einzugehen. Werden in § 119 Übermittlungen erfasst, die im Wege einer »Telekommunikation« oder eines »Computersystems« erfolgen, so wird in § 119a Abs 1 erster Fall nur mehr auf die Übertragung im Wege eines Computersystems abgestellt.[1008] Einerseits hat sich wohl der historische Gesetzgeber diesbezüglich am sehr weiten Begriffsverständnis der CCC orientiert. Es sollen demnach auch Kommunikationsformen erfasst werden, die über eine Telekommunikation hinausgehen.[1009] Etwa iZm Keylogger-Vorrichtungen, die heimlich Tastaturanschläge während der Übertragung des Scan-Codes der gedrückten Taste vom Keyboard-Controller zum Betriebssystem abfangen, ist festzuhalten, dass auch solche Übertragungen innerhalb eines Computersystems tatbildlich sind (wie bspw zwischen Prozessor und Bildschirm oder Drucker, aber auch zwischen User und Computer über die Tastatur).[1010]

1006 Diese Vorgehensweise ist auch als »MAC-Flooding« oder »Switch-Jamming« bekannt.
1007 Siehe dazu *Thome/Sollbach,* Grundlagen, 227.
1008 Zur Unterscheidung siehe oben ab S 193.
1009 Siehe ErlRV 1166 BlgNR XXI. GP, 25.
1010 Vgl ER (ETS 185) Pkt 55.

Wie bei § 119 Abs 1 besteht die Tathandlung im Benützen der Vorrichtung zur Kenntnisverschaffung, weshalb insofern auf das oben zu § 119 Abs 1 Gesagte verwiesen werden kann.

Obwohl im Fall des klassischen »Skimming«[1011] (engl für Abschöpfen) das vom Täter meist an Bankomaten unbemerkt angebrachte Lesegerät[1012] eine tatbildliche Vorrichtung iSd § 119a Abs 1 Fall 1 darstellt, werden die Daten des auf der Bankomatkarte befindlichen Magnetstreifens[1013] von dieser Vorrichtung[1014] bereits vor Auslösung der Datenverarbeitung durch den Berechtigten ausgelesen, weshalb sich die Daten, auf die es der Täter abgesehen hat, nicht am Übertragungsweg befinden. Schiebt das Opfer seine Zahlungskarte durch das vom Täter angebrachte Aufsatzgerät in das originale Karteneinschubfach, so werden die Daten des Magnetstreifens bereits während des manuellen Einführens der Zahlungskarte in den Bankomaten kopiert. § 119a Abs 1 muss daher ausscheiden.

Anders wäre der Sachverhalt allerdings zu beurteilen, wenn der Täter ein Lesegerät zum Ausspionieren von in Europa mittlerweile standardisierten »EMV-Chip«-Karten[1015] innerhalb des Karteneinschubs anbringen würde (sog »EMV-Skimmer«). In diesem Fall leitet der Skimmer die über das Bedienfeld eingegebenen Daten wie eine Vermittlungsstation (sog »Man-in-the-Middle«[1016]) unbemerkt an das System weiter. Die Daten (insb PIN) werden während der vom Kartenberechtigten eingeleiteten Datenverarbeitung – im Zuge ihrer Verarbeitung und Übermittlung zwischen Terminal und Chip – mitgelesen und gespeichert.[1017] Die Funktionalität entspricht faktisch einem Hardware-

---

1011 Siehe dazu auch *Marberth-Kubicki,* Computer- und Internetstrafrecht[2] (2010) Rz 77 ff; weiters *Seidl,* Debit Card Fraud: Strafrechtliche Aspekte des sog. »Skimmings«, ZIS 2012, 415; zur technischen Vorgangsweise siehe S 340 ff; der Begriff »Skimming« wird aber mittlerweile auch für das Kopieren von Chip-Karten verwendet siehe dazu *Rankl/Effing,* Handbuch[5], 1059.

1012 Auch »Skimmer« genannt.

1013 Zu Magnetstreifenkarten siehe ausf *Rankl/Effing,* Handbuch[5], 18 ff.

1014 IdR wird dafür ein Aufsatzgerät verwendet, das vor dem Karteneinschubfach angebracht wird.

1015 Innerhalb Europas sind die Zahlungskarten und Bankomaten mittlerweile mit dem EMV-Standard ausgestattet, weshalb Kartenduplikate durch die Verwendung des Mikrochips grundsätzlich erkannt werden. EMV steht dabei für Europay, Mastercard und Visa (siehe dazu auch S 341).

1016 Mehr zu diesen Begriffen ab S 201 ff.

1017 Siehe *Heuse,* PIN-Skimming bei Chipkarten möglich, <heise.de/-209205> (01.04.2014).

Keylogger, was die Tastatureingaben des Nutzers betrifft (sog »PIN-Skimming«) und einem Sniffer, was die Kommunikation zwischen Bankomat und Chip der Zahlungskarte anlangt. Der Tatbestand des § 119a Abs 1 wäre in diesem Fall erfüllt.

4. § 119a Abs 1 Fall 2 (Missbräuchliches Auffangen elektromagnetischer Emission)

Grundsätzlich emittiert jedes elektronische Gerät während seines Betriebes elektromagnetische Wellen, weshalb auch Computerkomponenten wie Monitore, Festplatten, Tastaturen usw physikalisch bedingt elektromagnetische Wellen[1018] aussenden. Mit entsprechenden Geräten und Know-how ausgestattet, wäre es möglich, diese Emission über eine erhebliche räumliche Distanz aufzufangen und eine Datenrekonstruktion vorzunehmen.[1019]

▹ **Van Eck Phreaking[1020] und TEMPEST**

So lässt sich etwa das auf einem Computerbildschirm[1021] ersichtliche Bild, auf einem entfernten System, das in keinerlei Verbindung mit diesem Computersystem oder Bildschirm steht, aus der aufgefangenen kompromittierenden Abstrahlung reproduzieren.[1022] Eines der wohl bekanntesten Forschungsprojekte auf diesem Gebiet ist »TEMPEST«[1023]

1018 Siehe dazu ausf *Freyer,* Nachrichten-Übertragungstechnik[6], 60 ff.

1019 Siehe dazu auch *Reindl,* E-Commerce, 167 mwN; weiters *Thiele* in SbgK § 119a Rz 25; auch *Hinterhofer,* Geheimnisschutz, 182.

1020 Der Begriff »Phreaking« stellt ein zusammengesetztes Kunstwort aus »Phone« und »freaking« dar und beschreibt seit den frühen 1960er Jahren Hacker, die sich an Telefonanlagen zu schaffen machten. In weiteren Kunstwörtern des Hacker-Jargons findet sich das »Ph« in Anlehnung an diese frühe Hacker-Generation, wie etwa bei »Phishing« und »Pharming« (siehe zur Entstehungsgeschichte des »Phreaking« *Schwabach,* Internet and the law[2] [2014] 192 f; weiters *Moore,* Cybercrime[2], 42 ff).

1021 ZB ein gewöhnlicher CRT-Monitor oder auch ein Laptop-Monitor, der allerdings besser abgeschirmt ist; siehe dazu auch *Feiler* in Zankl, Überwachungsstaat, 173 (183).

1022 Der niederländische Wissenschaftler *Wim van Eck* hat sich bereits 1985 mit dieser Abstrahlung von elektromagnetischen Wellen befasst: siehe *Van Eck,* Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?, Computer & Security, Vol. 4, 1985, <cryptome.org/jya/emr.pdf> (10.07.2013).

1023 Die US-Regierung wies darauf hin, dass es sich dabei um kein Akronym, sondern um einen Codenamen handelt (siehe *NSA,* TEMPEST: a signal problem – The story of the discovery of various compromising radiations from communications and Comsec equipment, <www.nsa.gov/public_info/_files/cryptologic_spectrum/

der NSA[1024], das mittlerweile als Zertifizierungsstandard für die elektromagnetische Abschirmung von Computerequipment Verwendung findet.[1025]

Nach Art 3 CCC soll auch das Abfangen der elektromagnetischen Abstrahlung, die nicht unter den Begriff der »Computerdaten« des Art 1 lit b CCC subsumiert werden kann, unter Strafe gestellt werden.[1026] Die emittierte Abstrahlung besitzt also selbst keine Datenqualität nach der CCC, da nur ISO[1027]-spezifizierte Daten darunter fallen, die direkt zur Datenverarbeitung in Computersystemen geeignet sein müssen.[1028] Aus der aufgefangenen Emission können aber durch spezielle technische Verfahren und Vorrichtungen, (konventionsgemäße) »Daten« rekonstruiert werden.[1029]

Elektromagnetische Wellen sind daher auch keine Daten iSd § 74 Abs 2, obwohl der Datenbegriff des StGB prinzipiell weiter gefasst ist als jener der Computerdaten der CCC.[1030]

Abgesehen von der fehlenden Daten- bzw Nachrichtenqualität ist auch die »Abstrahlung« elektromagnetischer Wellen als bloßer »Nebeneffekt« von elektronischen Geräten kein geschützter und intendierter »Übertragungsvorgang«, der jedoch für die Anwendung der § 119 Abs 1 und § 119a Abs 1 erster DF erforderlich wäre.

Wesentlich ist für die Verwirklichung des § 119a Abs 1 zweiter Fall, dass es (tatbestandlich)[1031] keinerlei Vorrichtung bedarf, weshalb es auch unbeachtlich ist, welche technischen Mittel zum Abfangen der Emission wie eingesetzt werden.[1032]

Die »elektromagnetische Abstrahlung« tritt als Tatobjekt dieses Deliktsfalls in Erscheinung.

---

tempest.pdf> (01.04.2014); siehe dazu auch *Koops,* The Crypto Controversy: A Key Conflict in the Information Society (1998) 211 ff.

1024 National Security Agency/USA.

1025 *Gülmen,* TEMPEST-Zertifizierung – der Weg zum abhörsicheren Gerät, <blog.gdsys.de/blog/2012/09/13/tempest-zertifizierung-der-weg-zum-abhorsicheren-gerat/> (01.04.2014).

1026 Siehe ER (ETS 185) Pkt 57.

1027 »International Organization for Standardization«.

1028 Siehe ER (ETS 185) Pkt 25.

1029 Vgl ER (ETS 185) Pkt 57.

1030 Siehe zum Datenbegriff des § 74 Abs 2 S 60 ff.

1031 In praxi ist freilich eine Vorrichtung zur Realisierung dieser Abhörmethode erforderlich (siehe dazu idS auch *Thiele* in SbgK § 119a Rz 28).

1032 Siehe *Thiele* in SbgK § 119a Rz 28 mit Verweis auf *Reindl-Krauskopf* in WK² § 119a Rz 10.

Die Tathandlung umfasst lediglich das »Auffangen« der Abstrahlung. Darunter ist jede Handlung zu verstehen, die geeignet ist, elektromagnetische Wellen zu empfangen.[1033] Ob eine Rekonstruktion in weiterer Folge gelingt, ist irrelevant.[1034] Auch sind Nachrichteninhalte und sonstige Daten gleichermaßen (mittelbares)[1035] Tatobjekt.[1036]

Richtig merkt *Reindl-Krauskopf*[1037] an, dass nur jene elektromagnetischen Wellen gemeint sein sollen, die als Nebeneffekt des Betriebs der einzelnen Computerkomponenten anfallen, und nicht auch jene, die in dieser Form eine gezielte Datenübertragung in kabellosen Systemen repräsentieren, wie bei WLAN, Bluetooth, RFID[1038], NFC[1039] usw. Da solche drahtlosen Datenübertragungen, sofern sie in unverschlüsselter Form durchgeführt werden, ggf sehr weitreichend ausgestrahlt und relativ einfach mitgelesen werden können, wirft *Reindl-Krauskopf* die Frage nach einer allfälligen Strafbarkeit nach § 119a Abs 1 Fall 2 auf. Sie untersucht dabei den Begriff der »Abstrahlung« und hält dazu fest, dass es sich um kein Synonym für »Übertragung« handle. *Reindl-Krauskopf* führt sinngemäß weiter aus, dass, würde man die Strafbarkeit in einem solchen Fall bejahen, sich für Übertragungen in kabelgebundenen Netzwerken (LAN) ein minderer Schutz als bei Verwendung drahtloser Netzwerke (WLAN) ergäbe, da nur im LAN (über § 119a Abs 1 Fall 1) die Benützung einer speziellen Vorrichtung tatbildlich gefordert sei. Beim WLAN wäre die Schwelle zur Strafbarkeit im Fall des § 119a Abs 1 Fall 2 daher deutlich schneller überschritten, was einen Wertungswiderspruch darstelle.[1040]

Der Argumentation *Reindl-Krauskopf* ist dabei lediglich entgegenzuhalten, dass Art 3 CCC diesbezüglich überhaupt nicht weiter differenziert und folglich die elektromagnetische Emission als »Computerdatenübertragung« mitumfasst wird.[1041]

1033 Vgl *Thiele* in SbgK § 119a Rz 27.

1034 Dazu auch *Reindl-Krauskopf* in WK² § 119a Rz 10.

1035 Datenrekonstruktion aus aufgefangenen elektromagnetischen Wellen. Die Abstrahlung selbst besitzt keine Datenqualität.

1036 Ähnlich *Seling,* Privatsphäre, 159.

1037 Vgl *Reindl-Krauskopf* in WK² § 119a Rz 10.

1038 »Radio Frequency Identification«.

1039 »Near Field Communication« als Erweiterung der RFID-Technik.

1040 Siehe *Reindl-Krauskopf* in WK² § 119a Rz 10.

1041 Art 3 CCC: »Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, inclu-

Denkt man diese Argumentation zu Ende, so muss man zum Ergebnis kommen, dass für das Auffangen der Abstrahlung elektromagnetischer Wellen während einer Kommunikation oder Datenübertragung der hier untersuchte Deliktsfall gar nicht angedacht sein kann. In der Praxis ist es mE wohl faktisch unmöglich, eine Filterung der Emissionen innerhalb der korrespondierenden, rekonstruierbaren Daten vorzunehmen, welche sich gerade auf dem Transportweg befunden haben und welche nicht. Im letzteren Fall wäre nämlich die Bestimmung gar nicht anwendbar und im ersteren, was Datenübertragungen in Funknetzwerken anlangt, schlicht überflüssig, weil ein derartiger Sachverhalt bereits von § 119 bzw § 119a Abs 1 Fall 1 erfasst wäre. Sinnvollerweise müsste der Tatbestand auf das Auffangen von elektromagnetischer Abstrahlung »gespeicherter« und nicht am Transport befindlicher Daten abzielen.[1042] Man würde aber in diesem Fall in die Nähe der »Strafbarkeit von widerrechtlicher Datenreproduktion« durch Manipulation elektromagnetischer Emission kommen. Bislang war dem Kernstrafrecht[1043] der »Datenklau«[1044] von abgespeicherten, aber nicht gerade am EDV-Transport befindlichen Daten fremd. Auffallend ist aber, dass – würde der Strafgesetzgeber tatsächlich das widerrechtliche Reproduzieren von Daten für sich allein genommen bereits unter Strafe stellen wollen – für den hier untersuchten Tatbestand keine weiteren objektiven Kriterien zur Strafbarkeitseinschränkung vorgesehen sind. So verlangt der Tatbestand etwa kein Erfordernis einer besonderen Sicherung der Daten[1045], wie bspw solche, die dem Vorbild der spezifischen Sicherheitsvorkehrung des § 118a Abs 1 entsprechen würde. Zu denken wäre dabei auch an die hier angesprochene TEMPEST-Zertifizierung. Der Gesetzgeber könnte zB nur Systeme schützen, deren Komponenten eine bestimmte TEMPEST-Klassifizierung

---

ding electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system«.

1042 In diesem Sinn auch *Gercke/Brunst,* Internetstrafrecht, 72 mwN.

1043 Sofern es sich um personenbezogene Daten handelt, könnte ggf § 51 DSG 2000 zur Anwendung gelangen.

1044 Der umgangssprachlich in diesem Zusammenhang oft gebraucht Begriff des »Datendiebstahls« ist nach der Strafrechtsterminologie nicht korrekt, da es für einen »Diebstahl« nach § 127 an der »Körperlichkeit« des Tatobjekts (arg »fremde bewegliche Sache«) mangelt, aber auch beim Kopieren von Daten keine »Vermögensverschiebung« stattfindet.

1045 Siehe auch *Thiele* in SbgK § 119a Rz 29.

der Emissions-Abschirmung besitzen. Wer also den Schutz des Tatbestandes des Auffangens elektromagnetischer Abstrahlung für sein Computersystem in Anspruch nehmen will, müsste Geräte einer entsprechenden Abschirmklasse verwenden. Im rechtspolitischen Vergleich zur Strafbarkeit nach § 118a Abs 1 wäre nämlich nicht zu verstehen, warum der widerrechtliche Zugriff auf ein Computersystem, um sich Kenntnis von Daten zu verschaffen, lediglich unter der objektiven Strafbarkeitseinschränkung der »Überwindung einer spezifischen Sicherheitsvorkehrung« strafbar ist, während das bloße Auffangen von elektromagnetischer Abstrahlung, um Daten daraus zu rekonstruieren, bereits ohne das Vorhandensein einer solchen Vorkehrung den objektiven Tatbestand des § 119a Abs 1 zweiten DF bereits erfüllt. Obwohl lediglich für Art 2 CCC (umgesetzt in § 118a) ein Erfordernis der Überwindung von Sicherheitsvorkehrungen vorgesehen ist, wäre es mE angebracht, adäquate Tatbestandsvoraussetzungen auch in diesem speziellen Deliktsfall zu schaffen.[1046] Beide Delikte schützen faktisch die Vertraulichkeit von »gespeicherten« Daten.[1047] »Datenübertragungen« in Funknetzwerken fallen nämlich – wie *Reindl-Krauskopf* zutreffend anmerkt[1048] – nicht unter den Begriff »Abstrahlung« und werden von § 119 Abs 1 und § 119a Abs 1 Fall 1 abschließend erfasst. § 119a Abs 1 Fall 2 rückt daher näher an den »Widerrechtlichen Zugriff auf ein Computersystem« (§ 118a) als an die Bestimmungen über die Verletzung des Telekommunikations- (§ 119) bzw Übertragungsgeheimnisses (§ 119a Abs 1 Fall 1).

Aus diesem systematischen Verständnis heraus sollte aber, gerade um, wie vorgeschlagen[1049], eine Überkriminalisierung zu vermeiden, auf die Verwendung »technischer Mittel« abgestellt werden.

Allerdings darf bei diesen Betrachtungen nicht übersehen werden, dass der Strafgesetzgeber auch für den hier untersuchten Deliktsfall »übermittelte Daten« als Schutzobjekt vorsieht, was sich aus der Definition des erweiterten Vorsatzes des subjektiven Tatbestandes in § 119a Abs 1 ergibt, der für beide Deliktsfälle gleichermaßen maßgeblich ist.[1050] Daher sind wiederum nur solche Daten geschützt, die sich ge-

1046 Siehe ErlRV 1166 BlgNR XXI. GP, 26; weiters Art 2 CCC iVm ER (ETS 185) Pkt 50.
1047 Dazu auch *Hinterhofer,* Geheimnisschutz, 181.
1048 Vgl *Reindl-Krauskopf* in WK² § 119a Rz 10.
1049 Vgl ER (ETS 185) Pkt 53.
1050 Siehe dazu *Thiele* in SbgK § 119a Rz 34; auch *Reindl-Krauskopf* in WK² § 119a Rz 12; weiters *Seling,* Privatsphäre, 159.

rade am Transportweg befinden, was aber – wie oben bereits kritisiert – zu unangemessenen Ergebnissen führt. Deshalb wird in der Lit vorgeschlagen den »erweiterten Vorsatz in Bezug auf die zweite Tathandlung des § 119a so zu verstehen, dass der Täter beabsichtigt, Daten auszuspionieren, die zur Übertragung bestimmt sind oder die bereits übertragen wurden«.[1051] Dazu ist zu ergänzen, dass die Übertragungsform »im Wege eines Computersystems« indiziert, dass – wie oben bereits mehrfach ausgeführt – auch die Betrachtung oder die Bearbeitung von abgespeicherten oder zur Speicherung bestimmten Nachrichten umfasst sind, und darüber hinaus überhaupt auch alle anderen Daten[1052], die sich zur Zeit ihrer Verarbeitung auf internen Transportwegen (zB CPU, Arbeitsspeicher, Bussystem) befinden.

Beabsichtigt der Täter jedoch lediglich irgendein anderes gespeichertes Datum – das nicht Gegenstand einer Übertragung war oder zu einem solchen wird – durch das Abfangen von elektromagnetischen Wellen auszuspionieren, reicht das für eine Strafbarkeit nach § 119a Abs 1 Fall 2 nicht aus.[1053]

5. De lege ferenda-Empfehlung an den Gesetzgeber

Zur Vermeidung von Wertungswidersprüchen und Auslegungsproblemen wäre der Gesetzgeber gut beraten, den zweiten Deliktsfall als ein eigenständiges Delikt zu konzipieren. Man sollte folglich zB einen neuen Absatz bilden und dort durchaus für Daten und Nachrichten gleichermaßen das Auffangen der elektromagnetischen Emission mit dem Einleitungssatz »Wer außer in den Fällen der § 119 Abs 1 und § 119a Abs 1[1054] […]« unter Strafe stellen.

Bei einer Neufassung dieser Bestimmung könnten mehrere Unklarheiten und Unangemessenheiten beseitigt werden:

1051 Vgl *Reindl-Krauskopf* in WK² § 119a Rz 12; idS auch *Thiele* in SbgK § 119a Rz 34.

1052 Vgl ein Dokument eines Textverarbeitungsprogramms, das gerade bearbeitet wird, auch wenn es nicht zur Übertragung auf andere Computersysteme bestimmt ist. Der systeminterne (lokale) Transport reicht aus.

1053 Siehe auch *Reindl-Krauskopf* in WK² § 119a Rz 12.

1054 Nunmehr ohne den zweiten DF versteht sich.

1. Rekonstruierbare Daten und Nachrichten sollten ihrem unterschiedlichen Schutzniveau entsprechend kriminalpolitisch tatsächlich angemessen Berücksichtigung finden.
   Genau aus diesem Grund ist es nämlich nach der geltenden Fassung des § 119a Abs 1 nicht zu verstehen, warum der Gesetzgeber beim Abfangen der Abstrahlung nicht weiterhin dem Regime des unterschiedlichen Schutzniveaus im Bereich der Nachrichtenspionage (§ 119) und Datenspionage (§ 119a) treu bleibt. Warum soll der Inhalt einer Nachricht, von dem sich ein Unbefugter im Wege der Rekonstruktion aufgefangener elektromagnetischer Wellen Kenntnis verschaffen will, nicht dem Regelungsmodell des § 119 unterliegen?
2. Die in § 119 Abs 1 und § 119a Abs 1 Fall 1 verlangte, aber in § 119a Abs 1 Fall 2 nicht mehr tatbestandlich vorgesehene spezielle Vorrichtung sollte jedenfalls für dieses neue Delikt entfallen. Eine zu weitreichende Kriminalisierung müsste durch weitere (strafbarkeitseinschränkende) Merkmale verhindert werden.
3. Durch die Formulierung des geltenden Gesetzeswortlauts in § 119a Abs 1 Fall 2 iVm dem diesbezüglichen Telos der CCC[1055] ist klarzustellen, dass – wie oben bereits ausgeführt – elektromagnetische Emissionen selbst keine Daten im konventions- bzw StGB-terminologischen Verständnis sind und auch die Abstrahlung als ein Nebeneffekt elektronischer Geräte keine geschützte Übertragungsform nach § 119 bzw § 119a Abs 1 Fall 1 darstellt. Eine »Abstrahlung« ist daher keine Übertragung iSd Transmissionsmodells[1056] (Sender, Sendung, Empfänger), auf welchem aber der Schutz des Kommunikations- (§ 119) und Übertragungsgeheimnisses (§ 119a) grundsätzlich beruht.
   Aus diesem Grund ist auch offensichtlich, dass für den gegenständlichen Untersuchungsgegenstand (§ 119a Abs 1 Fall 2) ein vom Telekommunikations- bzw Übertragungsgeheimnis verschiedenes Rechtsgut geschützt sein muss. Zu denken wäre hier jedenfalls an die weitgefasste »Privatsphäre«.
4. Gerade für diesen DF wäre es daher angebracht, nicht auf »übermittelte« Daten abzustellen. Einerseits, weil sich in Anbetracht eines Rechtsguts »Privatsphäre« (und nicht »Übertragungsgeheimnis«) der Schutzbereich als viel zu eng darstellen würde. Andererseits

1055 Siehe ER (ETS 185) Pkt 57.
1056 Vgl etwa *Reisinger,* Rechtsinformatik, 126 f.

liefern weder die CCC[1057] samt Erl[1058] noch die GMat[1059] Anhaltspunkte dafür, dass es sich iZm dem Auffangen von elektromagnetischer Abstrahlung überhaupt um gerade am Transportweg befindliche Daten handeln muss. Vielmehr könnte daher auf »in einem Computersystem verarbeitete« bzw – in Anlehnung an § 126a Abs 1 – »von automationsunterstützt verarbeiteten, übermittelten oder überlassenen Daten« abgestellt werden.

Beide Tatbestandsalternativen stellen schlichte Tätigkeitsdelikte dar, da in beiden Fällen kein tatbestandlicher Erfolg verlangt wird. In § 119a Abs 1 Fall 1 liegt der Handlungsunwert im »Benützen einer Vorrichtung«, in § 119a Abs 1 Fall 2 im »Auffangen elektromagnetischer Abstrahlung«.

6. Subjektive Tatseite

In beiden Deliktsfällen des § 119a Abs 1 ist als strafbarkeitseinschränkender Ausgleich für den weiten objektiven Tatbestand auf der subjektiven Seite neben dem Tatbildvorsatz – im Gegensatz zu § 119 – eine mehrfache kumulativ vorliegende Absicht gefordert, wie sie bereits bei § 118a Abs 1[1060] formuliert wurde.

Der Täter muss daher im Zeitpunkt der Handlungsvornahme neben dem Tatbildvorsatz im Mindeststärkegrad eines dolus eventualis eine doppelte Absicht[1061] (hier: Datenspionageabsicht und Gewinn- bzw Schädigungsabsicht) iSd § 5 Abs 2 aufweisen, nämlich:

1057 Siehe etwa Art 3 CCC, indem zwar zum Ausdruck gebracht wird, dass die elektromagnetische Emission von nicht-öffentlichen Übertragungen von Computerdaten zu oder von einem Computersystem bzw innerhalb eines solchen als mitumfasst betrachtet wird, doch bezieht sich der diesbezügliche sprachliche Einschluss »including electromagnetic emissions from a computer system carrying such computer data«, generell auf Computerdaten und nicht nur auf solche, die gerade übermittelt werden.

1058 Siehe etwa ER (ETS 185) Pkt 57.

1059 Siehe ErlRV 1166 BlgNR XXI. GP, 27.

1060 Siehe oben.

1061 Siehe zur entsprechenden Begründung der hier vertretenen »doppelten Absicht« S 107; weiters – allerdings unbegründet – für eine doppelte Absicht: *Bertel/Schwaighofer,* BT I[12] § 119a Rz 3; *Köck,* Wirtschaftsstrafrecht[2], 114 f; wohl auch *Schmölzer,* ZStW 2011/123, 709 (729); *Eder-Rieder,* Wirtschaftsstrafrecht[3], 202; *Bergauer* in BMJ, 35. Ottensteiner Fortbildungsseminar, 27 (35); für eine dreifache Absicht (iS einer Datenspionageabsicht, einer Datenverwendungsabsicht und einer Gewinn- bzw Schädigungsabsicht): *Thiele* in SbgK § 119a Rz 32 ff; *Seling,* Privatsphäre, 158 f; *Reindl-Krauskopf,* Computerstrafrecht[2], 32; *Reindl-Krauskopf* in WK[2] § 119a Rz 8 f und 11.

- sich oder einem anderen Unbefugten Kenntnis von im Wege eines Computersystems übermittelten Daten zu verschaffen (= Datenspionageabsicht),
- sich oder einem anderen durch die Datenverwendung[1062] einen Vermögensvorteil zuzuwenden (= Gewinnabsicht) oder zumindest einem anderen einen Nachteil zuzufügen (= Schädigungsabsicht).

Die bloße Geheimnisverletzung ist somit kein Nachteil iSd erweiterten Vorsatzes des § 119a.[1063]

Wie auch § 118a Abs 1 ist § 119a Abs 1 in beiden Deliktsfällen unter Einbeziehung der überschießenden Innentendenzen ein verkümmert zweiaktiges Delikt mit zwei spezifischen, kupierten Enderfolgen.[1064] Ein Taterfolg im objektiven Tatbestand ist nicht gefordert.

Die Strafbestimmung des § 119a ist mit einer ausdrücklichen Subsidiaritätsklausel zu Gunsten des § 119 ausgestattet. Insofern dient sie als Auffangtatbestand, um einerseits Daten am Übertragungsweg zu erfassen und andererseits auch die elektromagnetische Abstrahlung von Daten, einschließlich Nachrichten, tatbestandlich zu umfassen.

7. Sonstiges

Aufgrund der Subsidiaritätsklausel in § 119a Abs 1, tritt – im Anwendungsfall des § 119 StGB – § 119a StGB zurück (sog »formelle Subsidiarität«).

In Abs 2 wird bestimmt, dass es sich bei § 119a Abs 1 um ein Ermächtigungsdelikt iSd § 92 StPO handelt. Die Ermächtigung ist von den jeweiligen Rechtsgutträgern zu erteilen. Das sind diejenigen, zu deren Kenntnisnahme die übermittelten Daten entweder bestimmt sind bzw von denen sie befugterweise stammen.[1065]

Sachlich ist das Bezirksgericht zuständig (§ 30 Abs 1 StPO).

1062 Im Sinne eines selbst benützen, einen anderen zugänglich machen oder veröffentlichen.
1063 Vgl *Reindl-Krauskopf* in WK² § 119a Rz 9.
1064 Siehe dazu bereits zu § 118a Abs 1.
1065 Siehe dazu auch *Thiele* in SbgK § 119a Rz 57.

E. Sonstige Verletzungen des Telekommunikationsgeheimnisses iSd § 120 Abs 2a

> § 120 [Auszug] (2a) Wer eine im Wege einer Telekommunikation übermittelte und nicht für ihn bestimmte Nachricht in der Absicht, sich oder einem anderen Unbefugten vom Inhalt dieser Nachricht Kenntnis zu verschaffen, aufzeichnet, einem anderen Unbefugten zugänglich macht oder veröffentlicht, ist, wenn die Tat nicht nach den vorstehenden Bestimmungen oder nach einer anderen Bestimmung mit strengerer Strafe bedroht ist, mit Freiheitsstrafe bis zu drei Monaten oder mit Geldstrafe bis zu 180 Tagessätzen zu bestrafen.
>
> (3) Der Täter ist nur mit Ermächtigung des Verletzten zu verfolgen.[1066]

Mit dem StRÄG 2002 wurde auch eine Änderung iZm dem vormals unter gerichtliche Strafe gestellten Geheimnismissbrauch nach § 102 TKG (1997)[1067] erforderlich. Da trotz Neufassung des § 119 – ebenfalls durch das StRÄG 2002 – § 102 TKG aF (1997) davon aber nicht vollständig umfasst war und eine ersatzlose Streichung dieser Strafbestimmung daher nicht in Frage kam, wurde eine diesbezügliche Abgrenzung zu § 119 nunmehr im Kernstrafrecht umgesetzt, welche wegen der Vergleichbarkeit der Tathandlungen[1068] allerdings bei § 120 unter einem neuen Absatz 2a Eingang gefunden hat.[1069] Die Eingliederung des Delikts unter die Deliktsbezeichnung »Missbrauch von Tonaufnahme- und Abhörgeräten« ist aber wohl verfehlt.[1070] »Die Geräte« zur Aufzeichnung von Nachrichten (wie eine Vorrichtung, ein Computer usw) werden nämlich gerade nicht – wie es etwa in den §§ 119f der Fall ist – tatbestandlich behandelt. Die Form des Empfangs von Nachrichten ist mit »im Wege einer Telekommunikation« iSd § 119 gleichzusetzen und auch bei dem für die Strafbarkeit verlangten Vorsatz im Stärkegrad der Absicht nach § 5 Abs 2 ist von einer korrespondierenden subjektiven Anforderung auszugehen.[1071] Die Tathandlung des »Aufzeichnens« wird nun aus dem § 102 TKG aF (1997) ins StGB übernommen und durch die an § 120 Abs 2 orientierten Handlungen des »Zugänglichmachens«

1066 BGBl 60/1974 idF I 56/2006.
1067 Aufgehoben durch BGBl I 134/2002.
1068 Im Sinne des Aufzeichnens und Mitteilens von Nachrichten.
1069 Siehe ErlRV 1166 BlgNR XXI. GP, 27.
1070 Vgl *Thiele* in SbgK § 120 Rz 27; weiters *Schmölzer,* ZStW 2011/123, 709 (729).
1071 Vgl ErlRV 1166 BlgNR XXI. GP, 27.

und »Veröffentlichens« ergänzt, um die vormals in § 102 TKG aF (1997) pönalisierten Handlungsweise des »Mitteilens« ebenfalls zu umfassen. Dadurch wurde der gesamte Regelungsinhalt des § 102 TKG aF (1997) ins StGB überstellt, sodass § 102 TKG aF (1997) als obsolet aufgehoben werden konnte.[1072] Auf Grundlage von systematischen Erwägungen ist jedoch verwunderlich, dass diese Regelung über den Schutz von Nachrichten in § 120 implementiert wurde, welcher bislang ausschließlich dem Schutz verbaler Äußerungen diente.[1073]

1. Tatobjekt und Schutzobjekt

Tatobjekt ist eine im Wege einer Telekommunikation übermittelte »Nachricht«[1074]. Das subjektive Unrechtselement des erweiterten Vorsatzes stellt aber – wie auch bei § 119 – als Bezugsobjekt auf den »Inhalt einer Nachricht« ab.[1075]

Wie bereits zu § 119 ausgeführt[1076], gibt es zwischen »Nachrichten« und »Inhaltsdaten« einen gravierenden Unterschied[1077], der sich unter anderem aus den Legaldefinitionen des § 92 Abs 3 Z 5 (Inhaltsdaten) und Z 7 (Nachrichten) TKG 2003 erkennen lässt. Die autonome Definition des Nachrichtenbegriffs im Strafrecht, die für § 119 getroffen wurde[1078], kann sich nun insoweit von § 120 Abs 2a unterscheiden, als die letztgenannte Bestimmung sowohl »Nachrichten« (hins objektivem Tatbestand und Tatbildvorsatz) an sich, als auch den »Inhalt von Nachrichten« (hins überschießender Innentendenz) im Tatbestand umfasst.[1079] Mit anderen Worten, es wird zwischen der technischen »Nachricht« einerseits, die im Wege einer Telekommunikation als eine in einen übertragungsfähigen Zustand gebrachte Mitteilung übertragen wird, und der »Mitteilung« andererseits, die das aus dem Geist Entsprungene darstellt, das dem Empfänger letztlich zur Kenntnis gebracht werden soll, unterschieden.[1080]

1072 Aufgehoben durch BGBl I 134/2002.
1073 Siehe *Reindl,* E-Commerce, 165.
1074 Vgl *Reindl,* E-Commerce, 167.
1075 Zu dieser Thematik siehe S 200 f.
1076 Siehe ebenfalls bereits S 164 ff.
1077 Nachricht = Inhalt einschließlich diverser Meta-Daten (wie etwa Bezug habende Namen, Nummern, Adressen); Inhaltsdaten = nur Inhalt einer Nachricht.
1078 Arg »die Vermittlung von Gedankeninhalten«.
1079 In einem anderen Zusammenhang stellen auch *Lewisch/Reindl-Krauskopf* in WK² § 120 Rz 31e die Gleichsetzung von Nachricht und deren Inhalt in Frage.
1080 Siehe dazu S 174 ff.

Daher vereint § 120 Abs 2a sowohl den bereits zu § 119 erörterten Begriff des »Inhalts einer Nachricht«[1081] in seiner überschießenden Innentendenz, mit dem Begriff der »Nachricht« in seinem objektiven Tatbestand.

Obwohl § 120 Abs 2a als Nachfolgebestimmung des § 102 TKG aF (1997) normiert wurde, müsste man wohl davon ausgehen, dass die darin angesprochene Begrifflichkeit auch nach dem bisherigen telekommunikationsgesetzlichen Verständnis zu bestimmen ist. Doch aus der nunmehrigen Einordnung im Kernstrafrecht (nach den Delikten §§ 119, 119a) und der damit verbundenen Aufgabe der speziellen Wertvorstellungen und Begrifflichkeiten des Sachgesetzes (TKG) kann darauf geschlossen werden, dass de lege lata ebenfalls die autonome Begriffsbestimmung idZ für »Nachricht« (aber daher indirekt auch für »Inhalt einer Nachricht«)[1082] für den hier angesprochenen 5. Abschnitt des StGB zu gelten hat. Daneben wird dies auch durch systematische Überlegungen indiziert, insb bezüglich der ausdrücklichen Subsidiarität des § 120 Abs 2a zu den vorstehenden Bestimmungen oder nach einer anderen Bestimmung mit strengerer Strafdrohung (gemeint §§ 119, 119a). Auch kann aus der Anmerkung in den GMat »Wie schon derzeit in § 102 TKG soll Schutzobjekt der Inhalt von »Nachrichten« sein«[1083] geschlossen werden, dass die Nachfolgeregelung des § 102 TKG aF (1997) dasselbe »Schutzobjekt« erfassen soll.[1084] Für die Zwecke der Zusammenfassung des Strafrechtsschutzes in Bezug auf Verletzungen des Telekommunikationsgeheimnisses im StGB kann folglich davon ausgegangen werden, dass die Begriffe »Nachrichten« und »Inhalt von Nachricht« in den §§ 119 und 120 Abs 2a weiter zu verstehen sind als im Verständnis des TKG 2003, weshalb aber davon jedenfalls auch die Inhalte von Nachrichten erfasst sind, die in den Anwendungsbereich des TKG 2003 fallen. Was § 120 Abs 2a betrifft, wäre ebenso die Verwendung einer weniger irreführenden Terminologie angebracht.

1081 Hier auch »Mitteilung« genannt.

1082 Obwohl bislang auch § 102 TKG iVm § 88 Abs 4 TKG aF (1997) auf die »Mitteilung« und somit auf die Vermittlung von Gedankeninhalten abgestellt hat, folgt ein »Inhalt einer Nachricht« freilich stets der Nachricht selbst, weshalb es auch für die Anwendbarkeit des § 102 TKG aF (1997) darauf ankam, ob die »Nachricht« selbst nach dem TKG zu beurteilen war.

1083 Vgl ErlRV 1166 BlgNR XXI. GP, 26.

1084 So auch zB *Thiele* in SbgK § 120 Rz 32; weiters *Seling,* Privatsphäre, 159.

Die begriffliche Unterscheidung ist jedenfalls dann relevant, wenn der Täter zwar das gegenständliche Tatobjekt, nämlich »Nachricht«[1085], zB aufgezeichnet, sich sein Vorsatz aber lediglich auf das Verschaffen äußerer Rahmendaten dieser Nachricht, wie zB der IP-Adresse des Absenders, und nicht auf den »Inhalt der Nachricht«[1086] bezieht. Der objektive Tatbestand und auch der allgemeine Tatbildvorsatz auf die objektiven Tatbestandsmerkmale ist zwar erfüllt, doch liegt der erweiterte Vorsatz (hier: Absicht sich vom Inhalt einer Nachricht Kenntnis zu verschaffen) nicht vor. Der Täter muss es daher auf den »Inhalt« einer Nachricht (den Gedankeninhalt) abgesehen haben.

Gleichwohl würde in unserem Beispielsfall auch § 119a Abs 1 Fall 1, der grundsätzlich jede Form und (jeden Inhalt) von Daten iSd § 74 Abs 2 schützt, nicht greifen, sofern der Täter keine Vorrichtung verwendet. Soweit § 119a Abs 1 Fall 1 nicht anzuwenden ist, gibt es folglich keinen strafrechtlichen Schutz für das Aufzeichnen, Zugänglichmachen oder Veröffentlichen einer Nachricht, wenn sich der erweiterte Vorsatz dabei lediglich auf dieser Nachricht anhaftende Verkehrsdaten bezieht. Man müsste daher genauer von einer »Inhaltsdatenspionageabsicht«[1087] (bezüglich einer Nachricht) sprechen. Dem Täter muss es auf den Informationswert des Nachrichteninhalts ankommen, und nicht auf Verarbeitungsdaten oder die technische Repräsentation.

2. Telekommunikation

§ 120 Abs 2a erfasst nur solche Nachrichten, die im Wege einer Telekommunikation übermittelt werden. Zur Übertragungsform »im Wege einer Telekommunikation« kann sinngemäß auf das oben zu § 119 Gesagte verwiesen werden. Wesentlich ist, dass eine »Telekommunikation als technischer Vorgang des Aussendens, Übermittelns und Empfangens von Nachrichten jeglicher Art in der Form von Zeichen,

1085 Damit ist die »technische Übertragungsform« der Mitteilung gemeint, die über die tatsächliche Mitteilung hinaus, noch weitere Daten beinhalten kann (wie Absender- und Empfängeradressen usw).

1086 Gemeint ist die Mitteilung selbst, die dem Empfänger zugehen soll.

1087 Insoweit ist auch die »Nachrichtenspionageabsicht« nicht ganz exakt bei *Hinterhofer,* Geheimnisschutz, 173 bzw die »Datenspionageabsicht« bei *Lewisch/Reindl-Krauskopf* in WK² § 120 Rz 31 f.

Sprache, Bildern oder Tönen mittels dazu dienender technischer Einrichtungen zu verstehen«[1088] ist.

Darunter würden audiovisuelle Videokonferenzen über das Internet ebenso fallen, wie bloße Bildübertragungen einer Kommunikation in Gebärdensprache.

Im Anwendungsbereich des § 120 Abs 2a liegen jedoch ausdrücklich nicht Nachrichten, die »im Wege eines Computersystems« übermittelt werden. Insoweit lässt sich festhalten, dass eine Abstufung des Schutzumfangs in den Strafbestimmungen, die das Kommunikations- bzw Übertragungsgeheimnis betreffen, zu erkennen ist:

- § 119 erfasst Nachrichten, die im Wege einer Telekommunikation oder im Wege eines Computersystems übertragen werden.
- § 119a stellt auf Daten ab, die im Wege eines Computersystems übertragen werden.
- § 120 Abs 2a erfasst Nachrichten, die im Wege einer Telekommunikation übertragen werden.

Anzumerken ist an dieser Stelle erneut, dass unter den Begriff der Telekommunikation neben der klassischen (auch analogen) Sprachtelefonie über Fest- oder Mobilfunknetze oder Nachrichten per Fernschreiber, Telegraf[1089] und Telefax[1090], auch die moderne IP-Telefonie[1091] sowie diverse Kommunikationen per (Computer-)Datenübertragungen (wie zB E-Mail, SMS, MMS)[1092] fallen.

Im Gegensatz zu den §§ 119, 119a wird bei den Tathandlungen nicht auf das bloße Benützen einer speziellen Vorrichtung abgestellt. Der Täter muss die Nachricht vielmehr entweder aufzeichnen oder sie einem anderen Unbefugten zugänglich machen oder veröffentlichen. Dies ist insofern auffällig, als das durch die Intensität dieser Tathandlungen bestehende Gefährdungspotential höher zu sein scheint, als beim blo-

1088 Vgl ErlRV 1166 BlgNR XXI. GP, 25 und ErlRV 1325 BlgNR XXII. GP, 6.
1089 Siehe *Thiele* in SbgK § 119 Rz 39 mit weiteren Beispielen.
1090 Vgl ER (ETS 185) Pkt 51.
1091 Auch Internet-Telefonie oder Voice-over-IP (VoIP) genannt; dabei wird ein Gespräch in digitalisierter Form in Echtzeit über ein paketvermittelndes Datennetz mittels des IP-Protokolls übertragen (siehe *Hein/Reisner,* TCP/IP², 499 f).
1092 Siehe dazu auch ErlRV 1316 BlgNR XXII. GP, 5; weiters *Schwaighofer* in WK² § 107a Rz 20.

ßen Benützen einer Vorrichtung (iSd §§ 119, 119a)[1093], und dass, obwohl § 120 Abs 2a die dazu subsidiäre Norm ist, die bezüglich ihrer Strafdrohung ein ungleich herabgesetztes Unrecht beschreibt.

§ 120 Abs 2a knüpft nämlich erst an Handlungen an, die über den bloßen Erhalt einer Nachricht hinausgehen, wie zB das bewusste Abspeichern, Weiterleiten oder Veröffentlichen.[1094]

Zwischen diesen drei Begehungsweisen muss jedoch streng unterschieden werden, denn sie sind nicht rechtlich gleichwertig. Das »bloße« Aufzeichnen der Nachricht, das zB nur eine abstrakte Gefährdung des Rechtsguts bedeutet, wird idR auch die Vorbereitungshandlung zum späteren Zugänglichmachen oder Veröffentlichen sein. Die beiden letzten Tathandlungen sollten daher mE auch strenger bestraft werden.[1095]

3. Aufzeichnen

Unter Aufzeichnen versteht die hM das nicht bloß flüchtige Festhalten einer Nachricht.[1096] Die Nachrichten können daher entweder auf einem digitalen elektronischen Datenträger (zB E-Mail, SMS, MMS, Telefax) oder aber auch auf analogen (Ton-)Trägern (zB bei Nachrichten mittels Funk- oder analogem Telefongerät) gespeichert werden. Es muss sich aber um ein vom Täter bewusstes (aktives) Speichern, iS eines dauerhaften Festhaltens, handeln.[1097] Das Erlangen einer Nachricht ohne Zutun des Täters ist nach dieser Tatmodalität nicht tatbildmäßig.[1098] Das bloße Öffnen eines E-Mails, das etwa fehlgeleitet wurde, stellt noch kein bewusstes Speichern iSd Aufzeichnens der Nachricht dar, und zwar auch dann nicht, wenn die Nachricht dadurch technisch bedingt – vom Nutzer unbeeinflusst – im Arbeitsspeicher vervielfältigt[1099] wird.[1100] Ebenso wird aus diesem Grund in der hL davon abgesehen, das automatische Speichern eines – wenn auch fehlgeleiteten –

1093 Siehe dazu auch *Schmölzer,* ZStW 2011/123, 709 (729).
1094 Siehe auch *Seling,* Privatsphäre, 159 f.
1095 Mehr dazu gleich im Anschluss.
1096 Siehe *Thiele* in SbgK § 120 Rz 57; weiters *Lewisch/Reindl-Krauskopf* in WK² § 120 Rz 31b.
1097 Vgl auch *Thiele* in SbgK § 120 Rz 58.
1098 Siehe auch *Seling,* Privatsphäre, 159 f.
1099 Sog »flüchtiges Speichern«.
1100 Siehe *Lewisch/Reindl-Krauskopf* in WK² § 120 Rz 31b.

E-Mails durch ein E-Mail-Programm ohne Zutun des Nutzers unter das tatbestandliche »Aufzeichnen« zu subsumieren.[1101] Wurde dem Empfänger ein E-Mail unaufgefordert (iS einer aufgedrängten oder fehlgeleiteten Nachricht) übermittelt, das von seinem E-Mail-Programm automatisch dauerhaft gespeichert wurde, so würden wohl grundsätzlich im (Tat-)Zeitpunkt der automatischen Speicherung der Tatbildvorsatz und die spezifischen überschießenden Innentendenzen fehlen. Treten Tatbildvorsatz und weitere innere Tendenzen erst nachträglich hinzu, stellt das lediglich die nachträgliche Billigung einer »unvorsätzlichen Tat« dar (dolus subsequens). Wird allerdings diese Nachricht in weiterer Folge mit entsprechendem Vorsatz einer anderen unbefugten Person zugänglich gemacht, so ist sowohl objektive als auch subjektive Tatbestandsmäßigkeit hergestellt.

Verwendet der Täter zB ein Sniffer-Programm, um sämtliche E-Mails, die an andere Personen des gemeinsamen Netzwerks adressiert sind, automatisch aufzuzeichnen[1102], so handelt der Täter tatbestandsmäßig. Wie der Täter die Nachrichten letztlich aufzeichnet, ist irrelevant, es muss sich aber um die ursprüngliche Form der im Wege einer Telekommunikation übermittelten Nachricht handeln und nicht etwa um eine Abschrift des Inhalts derselben.[1103] Einer speziellen Vorrichtung bedarf es – im Gegensatz zu § 119 und § 119a Abs 1 Fall 1 – nicht. Im Ergebnis findet durch das Aufzeichnen einer Nachricht eine von der Tathandlung abgetrennte Veränderung in der Außenwelt[1104] dadurch statt, dass nunmehr ein (auf einem Datenträger verkörpertes) Aufzeichnungsobjekt (bspw in Dateiform) existiert. § 120 Abs 2a stellt in Verwirklichung dieser Variante ein Erfolgsdelikt dar.

4. Zugänglichmachen

Der Täter macht die Nachricht einem anderen Unbefugten zugänglich, wenn er diesem die Nachricht weiterleitet.[1105] Expressis verbis verlangt

---

1101 Vgl *Lewisch/Reindl-Krauskopf* in WK² § 120 Rz 31b.

1102 Es spielt keine Rolle, ob der tatsächliche Empfänger die an ihn gerichtete Nachricht tatsächlich erhält.

1103 Vgl auch *Thiele* in SbgK § 120 Rz 62; auch *Lewisch/Reindl-Krauskopf* in WK² § 120 Rz 31b.

1104 Vgl generell zB *Fuchs,* AT I⁸ Rz 10/40; *Kienapfel/Höpfel/Kert,* AT¹⁴ Z 9 Rz 6 ff.

1105 Siehe *Lewisch/Reindl-Krauskopf* in WK² § 120 Rz 31d; weiters *Thiele* in SbgK § 120 Rz 54.

der Tatbestand, dass »die Nachricht« selbst jemandem zugänglich gemacht wird und nicht deren Inhalt. Daher muss es sich zB bei einem E-Mail um die ursprüngliche, im Wege der Telekommunikation übermittelte Nachricht handeln.[1106] Mit dem eröffneten Zugang zur Nachricht für einen anderen Unbefugten ist der tatbestandliche Erfolg[1107] eingetreten.[1108]

Um der Frage des Bedeutungsgehalts des »Zugänglichmachens« als Tathandlung näher nachzugehen, sollen zuerst die unterschiedlichen diesbezüglichen Ausdrucksformen der einzelnen Tatbestände dargestellt werden.

§ 120 Abs 2a, aber auch § 118a Abs 1, § 119a Abs 1 bzw § 120 Abs 2 sprechen – verkürzt dargestellt – vom »einem anderen zugänglich machen« bzw »einem Dritten zugänglich machen«, wohingegen ua § 126c Abs 1 und § 207a Abs 1 Z 2 vom »sonst zugänglich machen« ausgehen. Die beiden letzten Delikte beinhalten einen alternativen Mischtatbestand, sodass im Sinn eines umfassenden Rechtsgüterschutzes sämtliche denkbare Begehungsweisen erfasst werden sollen, was insb die Verbreitung im Wege aktueller Informationstechnologie[1109] betrifft.[1110]

Sinnvollerweise muss somit das »Sonst-Zugänglichmachen« jedenfalls bereits das »Veröffentlichen« iS eines »öffentlich Zugänglichmachen« mitumfassen, da das »Veröffentlichen«[1111] selbst keine der dort genannten Tathandlungen ist. Vom klaren Wortlaut der Formulierung »sonst zugänglich machen« wird auch das Veröffentlichen impliziert.[1112]

Wird nun aber die Tathandlung »einem anderen zugänglich machen« bzw »einem Dritten zugänglich machen« neben der des Veröffentlichens genannt, müssen sich wohl die beiden erstgenannten Alternativen (bezogen auf den Personenkreis der potentiellen Kenntnisnehmer) davon abgrenzen. Andernfalls könnte man von einer vermeidbaren Redundanz ausgehen.

1106 Siehe *Lewisch/Reindl-Krauskopf* in WK² § 120 Rz 31d; aA vormals noch *Reindl,* E-Commerce, 167.

1107 Tatsächlich geht aber dadurch jedenfalls nur eine konkrete Gefährdung des Rechtsguts einher, die allerdings für die Einordnung als Erfolgsdelikt ausreicht (siehe dazu oben § 51 DSG 2000).

1108 AA *Hinterhofer* in SbgK § 207a Rz 12.

1109 Siehe zB *Philipp* in WK² § 207a Rz 18 (Stand März 2014).

1110 Vgl etwa für § 207a Abs 1 Z 2 OGH 01.04.2008, 11 Os 21/08k.

1111 Zur »Veröffentlichung« siehe gleich im Anschluss.

1112 Vgl *Philipp* in WK² § 207a Rz 17 f.

Der Täter muss in den Fällen des einem anderen bzw einem Dritten Zugänglichmachens, die Nachricht[1113] einem »konkreten Dritten«[1114] – der selbst ein Unbefugter sein muss – aktiv weitergeben (iS einer »Individualkommunikation«[1115]). Darin indiziert »einem anderen«, dass es sich jedenfalls um einen anderen Menschen handeln muss, dem die Nachricht zugänglich gemacht wird. Nach den GMat wird darunter eine Handlung verstanden, die »einem anderen – auf welche Art auch immer – die Möglichkeit zur Kenntnisnahme verschafft«.[1116] Bemerkenswerterweise führt er dafür als Beispiel ein »Bild auf einer Internet-Homepage« an, was aufgrund des unbestimmten Adressatenkreises und der sukzessiven Wahrnehmbarkeit für eine unbestimmte Anzahl von Betrachtern[1117] wohl gerade ein Paradebeispiel einer Veröffentlichung darstellt.[1118]

Der sprachliche Ausdruck »einem« ist wiederum nicht als Zahlwort, sondern als (unbestimmter) Artikel zu verstehen und weist daraufhin, dass es sich um einen »konkreten« Empfänger handeln muss (empfängerorientiert). Ohne diesen Artikel käme man in den Konflikt mit dem Plural, der durch »anderen zugänglich machen« angezeigt wäre und die Einzelperson ausschließen würde.

Rechtspolitisch ließe sich argumentieren, dass wenn schon das Weiterleiten an einen Dritten strafbar sein soll, dann erst recht, wenn die Nachricht an mehrere konkrete Empfänger verbreitet wird.[1119] In einem solchen Fall liegt ein Zugänglichmachen in gleichartiger Idealkonkurrenz[1120] vor, das nach oben hin aber mit dem Richtwert für eine »öffentliche Begehung« nach § 69 begrenzt wird. Wird daher die Nachricht 5 Empfängern uno actu zugänglich gemacht, wird § 120 Abs 2a fünf Mal in echter gleichartiger Idealkonkurrenz verwirklicht. Wird

---

1113 Im hier interessierenden Zusammenhang iSd § 120 Abs 2a.

1114 Im Sinne von einer »bestimmten Person«.

1115 Zur Begrifflichkeit siehe auch *Gaderer* in Kucsko, urheber.recht § 18a Pkt 4.1 (Stand Dezember 2007).

1116 Vgl ErlME 82/ME XXIV. GP, 8.

1117 Und daher auch iSd § 69 für mehr als 10 Personen wahrnehmbar ist (anschließend gleich mehr dazu).

1118 Siehe ErlME 82/ME XXIV. GP, 8.

1119 Man beachte allerdings das Analogieverbot zu Lasten des Täters im Strafrecht, das auch jede Art der Lückenschließung, etwa durch Größenschluss, erfasst (vgl statt vieler *Fuchs,* AT I[8], Rz 4/26).

1120 Die ältere Lehre sprach von »verstärkter Tatbestandsmäßigkeit« vgl etwa *Ratz* in WK² Vorbem §§ 28–31 Rz 17 (Stand Oktober 2011).

die Personenanzahl für eine öffentliche Begehung jedoch überschritten, liegt ein (einfaches) Veröffentlichen vor und § 120 Abs 2a wird nur einmal verwirklicht, unabhängig davon, ob es sich dann noch um »bestimmte« Empfänger handelt oder nicht.[1121]

In vielen Fällen wird das Aufzeichnen einer Nachricht den weiteren verpönten Tathandlungen des Abs 2a vorgelagert sein. Doch ist der Tatbestand auch in den Fällen erfüllt, in denen die ursprüngliche Nachricht jemand anderem vorgeführt wird (wie zB durch das Öffnen des ursprünglichen E-Mails zu dessen Kenntnisnahme oder das für einen unbefugten Dritten hörbare Abspielen der auf einem Tonbandgerät aufgezeichneten Nachricht).[1122] Dass der Dritte die Nachricht aber auch tatsächlich liest, ist nicht erforderlich.

5. Veröffentlichen

Auch die Tathandlung des Veröffentlichens stellt in § 120 Abs 2a auf die ursprüngliche Nachricht ab, sodass eine Strafbarkeit erfordert, dass diese originale, im Wege der Telekommunikation übermittelte Nachricht veröffentlicht wird (zB durch das Weiterleiten einer Massen-E-Mail[1123] an mehr als 20 unberechtigte Empfänger). Mit dem eröffneten Zugang für die Öffentlichkeit ist der tatbestandliche Erfolg eingetreten (Erfolgsdelikt). Dafür reicht es nach hM aus, dass das Rechtsgut zumindest konkret gefährdet wird.[1124] Generell kann von einem »Veröffentlichen« dann gesprochen werden, wenn die Nachricht einem größeren unbestimmten Personenkreis zugänglich gemacht wird.[1125] Dies wird jedenfalls dann vorliegen, wenn die Nachricht einem völlig unbestimmten (größeren) Empfängerkreis zugänglich gemacht wird, wie die Zurverfügungstellung im Internet. In einem solchen Fall wird die Nachricht einem »bewusst« auf die Website zugreifenden unbestimmten Personenkreis zugänglich gemacht, was sich vom Zugänglichma-

---

1121 Siehe mehr dazu gleich im Anschluss.

1122 Vgl dazu auch *Lewisch/Reindl-Krauskopf* in WK² § 120 Rz 31d.

1123 Siehe OLG Wien 22.11.2002, 17 Bs 263/02 = MR 2003, 81; weiters und LG Klagenfurt 10.01.2008, 7 Bl 121/07y = jusIT 2008/44, 95 *(Bergauer);* nicht aber Einzel-E-Mails siehe OLG Wien 03.10.2002, 17 Bs 249/02 = MR 2002, 373.

1124 Denkbar wäre nämlich, dass der Täter die Nachricht im Internet zwar iSd Tatbestands veröffentlicht, aber niemand tatsächlich darauf zugreift (siehe dazu bereits die Überlegungen zu § 51 DSG 2000).

1125 Siehe etwa *Leukauf/Steininger,* StGB³ § 120 Rz 11; weiters *Lewisch/Reindl-Krauskopf* in WK² § 120 Rz 12; auch *Thiele* in SbgK § 120 Rz 51.

chen via E-Mail dadurch unterscheidet, dass letztere Übermittlungsart empfängerorientiert ist.[1126]

Die explizit genannte Tathandlung der Veröffentlichung ist als Ergänzung der zweiten Begehungsweise zu verstehen. Unklar ist, ob dabei die »Bestimmtheit« der Empfänger bzw des Empfängerkreises eine Subsumtion unter das »Veröffentlichen« verhindern würde.

Ist nämlich der Täter zB selbst berechtigter Nutzer eines firmeninternen Netzwerks (Intranet), das zB 300 namentlich bekannte bzw identifizierbare Mitarbeiter nutzen, so sind sowohl der Umfang des Personenkreises bestimmt als auch die Nutzer eindeutig individualisierbar.

In diesem Fall ist dem LG Klagenfurt zu folgen, das auch betriebsinterne Informationsvorgänge, wie etwa Rundschreiben an Mitarbeiter, als Informationen nach außen beurteilt hat und hierzu feststellte, dass es keinen Unterschied mache, ob es sich um einen vorausbestimmten Personenkreis handle oder nicht.[1127] In Anlehnung an den OGH[1128] wurde näher ausgeführt: »Auch ist die Öffentlichkeit eines Verhaltens immer dann anzunehmen, wenn keine Gewähr besteht, dass die Mitteilung nicht über einen relativ kleinen oder zumindest sehr geschlossenen und unter Geheimhaltungspflicht stehenden Kreis hinaus gelangt«.[1129]

Daraus folgt, dass es für die Beurteilung des »Öffentlichkeitswertes« nicht auf eine tatsächliche Identifizierbarkeit der im Gefahrenradius befindlichen Personen ankommt, sondern darauf, dass es sich lediglich um einen größeren Personenkreis handeln muss. Es ist daher anzunehmen, dass sich das im Schrifttum angetroffene Unbestimmtheitserfordernis jedenfalls auf die Anzahl der Personen bezieht. So versteht dies auch *Rauch,* wenn er ausführt: »Vom Zugänglichmachen unterscheidet es [Anm: das Veröffentlichen] sich nur durch das Wesensmerkmal der Mindestpublizität«.[1130]

Um festzustellen, ab welcher mengenmäßigen Anzahl von Personen die Schwelle zur Veröffentlichung überschritten wird, liegt es nahe, Interpretationsanleihe bei anderen Bestimmungen zu nehmen.

1126 Vgl OGH 01.04.2008, 11 Os 21/08k (11 Os 22/08g) mwN = jusIT 2008/82, 175 *(Bergauer)*.

1127 Vgl LG Klagenfurt 10.01.2008, 7 Bl 121/07y = jusIT 2008/44, 95 *(Bergauer)*.

1128 Vgl OGH 23.02.2006, 12 Os 119/05z.

1129 Vgl LG Klagenfurt 10.01.2008, 7 Bl 121/07y = jusIT 2008/44, 95 *(Bergauer)*.

1130 Vgl *Rauch,* »Happy-Slapping« und Paparazzi – Die strafrechtliche Erfassung zweier ungleicher Phänomene, in Mitgutsch/Wessely (Hrsg), Strafrecht Besonderer Teil. Jahrbuch 2010 (2010) 89 (95).

Nach § 69 wird eine Handlung nur dann öffentlich begangen, wenn sie unmittelbar von einem größeren Personenkreis wahrgenommen werden kann. Die einhellige Rsp geht dabei – wie auch bei der Umschreibung einer »größeren Zahl von Menschen« – ab einer Anzahl von zehn Personen aus, will aber keine starre kopfmäßige Mindestanzahl festschreiben.[1131]

Auch die GMat sehen eine Veröffentlichung (hier: iZm Bildaufnahmen) nicht erst bei einer massenmedialen Verbreitung als gegeben an, sondern – in Anlehnung an § 69 – schon dann, wenn »eine Bildaufnahme unmittelbar von einem größeren Personenkreis (Richtwert: ab etwa zehn Menschen) durch Zugänglichmachen (bloßes Bereitstellen durch z.B. Anbringen an öffentlichen Orten reicht aus) wahrgenommen werden kann«.[1132]

Eine »breite Öffentlichkeit«[1133] wird ab einem Richtwert von 150 Personen angenommen[1134], wobei dies bei einer Abrufmöglichkeit im Internet, wie zB von einer Website oder einer Statusmeldung einer sozialen Plattform[1135], die uneingeschränkt eingesehen werden können, jedenfalls anzunehmen sein wird.

Für eine klarere Abgrenzung von »einem anderen zugänglich machen« und »Veröffentlichen« (ebenso wie das – wie oben ausgeführt – dazu synonym verwendete »Sonst-Zugänglichmachen«) kann es aber zur Argumentationsunterstützung durchaus sinnvoll sein, einen Blick auf das Datenschutzgesetz zu werfen, soweit sich dieses mit sämtlichen Verwendungsformen von ua[1136] automationsunterstützt verarbeiteten (personenbezogenen) Daten auseinandersetzt. Dies nicht zuletzt, weil als Vorbild für die Formulierung der überschießenden Innentendenzen in § 118a Abs 1, § 119 Abs 1, § 119a Abs 1 und § 120 Abs 2a letztlich ua die historische Fassung der Strafbestimmung des § 51 DSG 2000 diente.[1137] Dazu wurde in den Erl ausgeführt, dass als Tathandlung die

---

1131 Siehe *Jerabek* in WK² § 69 Rz 2 (Stand Juli 2013) mwN; weiters *Fabrizy,* StGB¹¹ § 69 Rz 2; siehe auch *Rauch* in Mitgutsch/Wessely, Jahrbuch 2010, 89 (96).

1132 Siehe ErlME 82/ME XXIV. GP, 7 ff zum Entwurf eines neuen § 120a; siehe anstatt vieler auch iZm der Beleidigung *Rami* in WK² § 115 Rz 5 (Stand Dezember 2011).

1133 Wie sie etwa in § 111 Abs 2 verlangt wird.

1134 Vgl *Lambauer* in SbgK § 111 Rz 48 f mwN (Stand März 2009).

1135 Zur Begrifflichkeit von sozialen Netzwerken im Internet siehe *Thiele,* Persönlichkeitsschutz in Neuen Medien – Facebook, Google & Co, AnwBl 2013, 11.

1136 Hier sind »manuelle Dateien« angesprochen, die ebenfalls vom einfachgesetzlichen Teil des DSG 2000 erfasst werden.

1137 Siehe die krit Auseinandersetzung dazu bereits oben; siehe ErlRV 1166 BlgNR XXI. GP, 27.

»Benützung sowie die Weitergabe von Daten, insbesondere ihre Veröffentlichung« unter Strafe gestellt werden soll.[1138]

Siegwart sieht den Unterschied zwischen einer Veröffentlichung und Weitergabe von Daten nach datenschutzrechtlichem Verständnis im Empfängerkreis. Die Veröffentlichung sei demnach dadurch gekennzeichnet, dass sie sich an einen unbestimmten Kreis von Dritten wendet, für den die Möglichkeit bestünde, von den Daten Kenntnis zu erlangen.[1139] Er stellt klar, dass es dabei faktisch keinen konkreten Empfänger gibt. Ein zahlenmäßiges Mindesterfordernis gibt es dafür ebenfalls nicht. »So sind etwa Bekanntmachungen im Intranet (Closed User Groups) Weitergaben von Daten. Andererseits sind bspw Bekanntmachungen in einem Gemeindeblatt, auch mit einer geringen Auflage, Veröffentlichungen iSd Datenschutzgesetzes, denn schließlich haben Dritte die (theoretische) Möglichkeit, diese Daten in Erfahrung zu bringen.«[1140] Dieser Ansatz ist aus datenschutzrechtlicher Sicht schon deshalb nachvollziehbar, weil der (datenschutzrechtliche) Auftraggeber Daten nur iSd § 7 Abs 2 DSG 2000 übermitteln darf, wenn diese aus einer gem Abs 1 zulässigen Datenanwendung stammen (Z 1) und der Empfänger dem Übermittelnden seine ausreichende gesetzliche Zuständigkeit oder rechtliche Befugnis – soweit diese nicht außer Zweifel steht – im Hinblick auf den Übermittlungszweck glaubhaft gemacht hat (Z 2) und durch Zweck und Inhalt der Übermittlung die schutzwürdigen Geheimhaltungsinteressen des Betroffenen nicht verletzt werden (Z 3). Die Z 2 verlangt zunächst, dass es überhaupt einen Empfänger gibt, der seinerseits natürlich dem Regime des DSG 2000 unterworfen bleibt, was die Veröffentlichung als Datenübermittlung zu einem datenschutzrechtlichen Spezialfall der Datenübermittlung macht.[1141]

1138 Siehe ErlRV 1613 BlgNR XX. GP, 54.

1139 Siehe *Siegwart,* Das Veröffentlichen von Daten, in Jahnel/Siegwart/Fercher (Hrsg), Aktuelle Fragen des Datenschutzrechts (2007) 211 (223 f); siehe auch *Jahnel,* Handbuch, Rz 3/119 und Rz 4/126.

1140 Vgl *Siegwart* in Jahnel/Siegwart/Fercher, Aktuelle Fragen, 211 (224).

1141 Bei einer Veröffentlichung gibt es nämlich keinen (absehbaren) konkreten Empfänger, sondern werden die Daten der Allgemeinheit – also einem unbestimmten Empfängerkreis – zugänglich gemacht. Dies führt weiters zur Frage, wie man eine Befugnis zur Datenverwendung von »unbestimmten« Empfängern glaubhaft machen lassen kann. Mit anderen Worten, die Regelung des § 7 Abs 2 Z 2 DSG 2000 ist auf bestimmte Empfänger zugeschnitten und für die Handlungsweise der Veröffentlichung ihrem Wortlaut nach nicht sachgerecht formuliert. So sieht dies auch *Jahnel,* der aufgrund einer grammatikalischen Interpretation (arg »der Empfänger«) den Schluss zieht, dass in Fällen, in denen man § 7 Abs 2 Z 2 DSG 2000

Darüber hinaus genießen diese übermittelten Daten – auch nach ihrem Transfer – den vollständigen Geheimhaltungsschutz. Daraus folgt, dass es im Datenschutzrecht in Bezug auf die Datenweitergabe nicht auf eine mengenmäßig Anzahl von Empfängern ankommen kann, sondern nur, dass es sich dabei um konkrete Empfänger handeln muss, die die datenschutzrechtlichen Anforderungen erfüllen. Obwohl auch beim (datenschutzrechtlichen) Veröffentlichen die Daten rein faktisch Dritten weitergegeben werden, sind damit andere rechtliche Konsequenzen verbunden. Insoweit passt diese Handlung nicht unbedingt in die Systematik und Definition der Datenübermittlung (iSd § 4 Z 12 DSG 2000).[1142] Im Gegensatz zur Datenübermittlung im engeren Sinn gibt es bei der Veröffentlichung keinen konkreten Empfänger. Die Daten werden vielmehr der Allgemeinheit zugänglich gemacht. Sind sie zulässigerweise veröffentlicht worden, geht für diesen bestimmten[1143] Verwendungszweck der Anspruch auf Geheimhaltung verloren (siehe § 1 Abs 1 zweiter Satz DSG 2000).

Aus dem Gesagten kann abgeleitet werden, dass es im datenschutzrechtlichen Kontext sachlich unangebracht wäre, eine Veröffentlichung an einen kopfmäßigen Richtwert zu binden.[1144]

Im hier interessierenden strafrechtlichen Zusammenhang könnte man an einen Fall denken, in dem die Nachricht mehr als 10 namentlich bekannten Personen zugänglich gemacht wird (zB via E-Mail). Ein E-Mail ist dabei schon technisch bedingt stets an konkrete Empfänger(kreise) und nicht an die unbestimmte Allgemeinheit gerichtet. Orientiert man sich ausschließlich am zahlenmäßigen Empfängerkreis, würde iSd § 69 ein Veröffentlichen vorliegen (selbst wenn alle Empfänger Befugte wären). Hält man dagegen an der Bestimmtheit der (konkreten) Empfänger fest, könnte man auch von einem Zugänglichma-

---

auf eine unbestimmte Empfängeranzahl (man beachte aber, dass bei der Veröffentlichung auch »kein tatsächlicher Empfänger« denkbar ist) anwenden wollte, eine Überspannung des Wortsinns vorläge (vgl *Jahnel,* Handbuch, Rz 4/125 ff). Gleichwohl würde daher eine am Wortsinn haftende Interpretation zu einer rechtlichen Verunmöglichung einer jeden solchen Datenveröffentlichung führen. *Jahnel* schlägt daher im Ergebnis vor, § 7 Abs 2 Z 2 DSG 2000 teleologisch zu reduzieren und – anders als bei der reinen Datenweitergabe – gar nicht erst zur Anwendung gelangen zu lassen (siehe *Jahnel,* Handbuch, Rz 4/129).

1142 Vgl *Siegwart* in Jahnel/Siegwart/Fercher, Aktuelle Fragen, 211 (223).

1143 Durch die Entscheidung des EuGH 16.12.2008, C-73/07 wurde klargestellt, dass aber grundsätzlich auch »veröffentlichte personenbezogene Daten« in den Anwendungsbereich der Datenschutz-RL fallen.

1144 Zu den Tathandlungen der Strafbestimmung des § 51 DSG 2000 siehe S 145 ff.

chen ausgehen (wobei dann zu prüfen wäre, ob es sich wohl auch um Unbefugte handelt).

Zur Abgrenzung dieser beiden Sichtweise und Tathandlungen (sinnvollerweise auch im Fall einer Vermengung bestimmter und unbestimmter Adressaten) sollte mE ausschließlich das durch die Rsp konkretisierte quantitative Element einer öffentlichen Begehung als zahlenmäßiges Mindestmaß für eine »Veröffentlichung« herangezogen werden, was auch durch den Rechtsgüterschutz angezeigt ist. Die Weiterleitung einer Nachricht an bis zu 10 unbefugte Personen ist daher als Zugänglichmachen zu qualifizieren, darüber hinaus liegt ein Veröffentlichen vor, da gerade in Anbetracht moderner Informationstechnologien die »Multiplikationsgefahr« mit der Anzahl der (bestimmten oder unbestimmten) Empfänger – und unabhängig von einer etwaigen subjektiven Komponente des Täters – unkontrollierbar zunimmt. Dessen ungeachtet ist dies auch zur leichteren Klärung der Frage indiziert, welche der Tathandlungen vom Tatbildvorsatz des Täters erfasst waren.

Auch könnte untersucht werden, ob das urheberrechtliche Begriffsverständnis bezüglich des Zurverfügungstellungsrechts (§ 18a UrhG), das mit der UrhG-Novelle 2003[1145] eingeführt wurde, zu Interpretationszwecken berücksichtigt werden sollte.[1146] Dort wird jedoch darauf abgestellt, dass das Werk der Öffentlichkeit drahtgebunden oder drahtlos in einer Weise zur Verfügung gestellt wird, »dass es Mitgliedern der Öffentlichkeit von Orten und zu Zeiten ihrer Wahl zugänglich ist«. Es muss sich dabei also um einen »Pull-Dienst« handeln, bei dem es in der Entscheidung des (unbestimmten) Empfängers liegt, das geschützte Werk abzuholen oder nicht (iS eines interaktiven Abrufs). Wohingegen bei einem E-Mail-Versand, der nach der hM nicht § 18a UrhG, sondern – trotz Unkörperlichkeit des »elektronischen Werks« – dem Verbreitungsrecht (§ 16 UrhG) zugeordnet wird[1147], die Initiative vom Absender des E-Mails ausgeht (sog »Push-Dienst«).[1148] Im (kern-)strafrechtlichen

1145 BGBl I 32/2003.

1146 Siehe dazu auch *Schmölzer,* Die neue Rolle des Strafrechts im Internet, in Bergauer/Staudegger (Hrsg), Recht und IT. Zehn Studien (2009) 1 (23 ff), wobei das urheberrechtsakzessorische Erfordernis der Interaktivität des Abrufs (iS eines Pull-Dienstes) wegen der dort behandelten Thematik nicht näher ausgeführt wurde.

1147 Siehe *Walter,* Österreichisches Urheberrecht. Handbuch. I. Teil (2008) Rz 561.

1148 Siehe statt vieler *Jaksch-Ratajczek,* Urheberrechtliche Fragen zu im Internet bereitgestellten Lernmaterialien an Universitäten und Fachhochschulen, in Jaksch-Ratajczek (Hrsg), Aktuelle Rechtsfragen der Internetnutzung (2010) 99 (123).

Kontext übernehmen eine derartige Unterscheidung wohl die Tathandlungen des »Verschaffens« auf der einen Seite und des »Zugänglichmachens« (nun im übergeordneten, strafrechtlichen Sinn) auf der anderen. Aus der Perspektive des Täters entspräche ein »Sich-Verschaffen« dem Pull-Dienst, ein »einem anderen Zugänglichmachen« sowie »einem anderen Verschaffen« dem Push-Dienst. Eine derartige Unterscheidung spielt aber mE für das hier interessierende strafrechtliche Verständnis keine Rolle, geht es doch darum, die Gefährlichkeit der Tathandlung auf das Rechtsgut abzustimmen. Ob die Initiative zur tatsächlichen Wahrnehmung der online bereitgestellten Nachricht von einem Internet-Nutzer ausgeht, indem dieser den Inhalt dieser digitalen Quelle über eine Website betrachtet oder ob der »Täter« die Nachricht einem anderen (wenn von diesem auch ungewollt) übermittelt, spielt für den im deliktsspezifischen Zusammenhang stehenden Rechtsgüterschutz keine Rolle. Vielmehr kommt es auf eine quantitative Komponente an, da mit sukzessiver Zahl der potentiellen Betrachter (Nutzer) bzw Empfänger die Rechtsgutbeeinträchtigung zunimmt. Auf ein orts- oder zeitabhängiges bzw -unabhängiges Element sollte daher, wie auch auf das Erfordernis der Gleichzeitigkeit der Zugangsmöglichkeit, im Strafrecht verzichtet werden. In diesem Zusammenhang ist erneut indiziert, dass gerade spezifische Sachgesetze eigenständige Termini benötigen, um der jeweiligen ratio des Sachgesetzes Rechnung zu tragen. Um aber Verwirrungen und Vermengungen zu vermeiden, wäre bei abweichender Definition auch eine differenzierte Terminologie wünschenswert, um nicht mit dem Prinzip der Einheit der Rechtssprache in Konflikt zu geraten.[1149]

6. Mischdelikt

Aufgrund der Abgrenzung der beiden Termini erscheint die Normierung dieser Tathandlungen als gleichwertige Alternativen – wie oben bereits angesprochen – nicht sachgerecht.

So ist das Weiterleiten der Nachricht an eine einzelne Person – gerade was die Privatsphäre anlangt – keinesfalls so beeinträchtigend wie zB die Veröffentlichung im Internet. Noch deutlicher wird dieser Wer-

1149 Siehe für andere Beispiele terminologischer Unschärfen der Verbindung des Datenschutzrechts mit dem Strafrecht bei *Bergauer* in Jahnel, Jahrbuch 2010, 73 (78 ff).

tungsumstand, wenn man sich die Relation zwischen dem Veröffentlichen und dem »bloßen« Aufzeichnen (§ 120 Abs 2a Fall 1) der Nachricht ansieht, das lediglich eine abstrakte Gefährdung des Rechtsguts und keinen Taterfolg erkennen lässt. Das Aufzeichnen wird idR auch die Vorbereitungshandlung zum weiterführenden Zugänglichmachen oder Veröffentlichen sein. Darüber hinaus liegt im Vergleich zu den anderen Tathandlungen ein anderer – nämlich vorverlagerter – Vollendungszeitpunkt vor. Meiner Auffassung nach handelt sich insgesamt somit um ein kumulatives Mischdelikt.

In der Lit wird an dieser Stelle gerne das Veröffentlichen der Nachricht im Internet genannt.[1150]

Dabei muss aber darauf Bedacht genommen werden, dass es wieder auf die ursprüngliche Nachricht ankommt. Kopiert jemand lediglich den Inhalt eines E-Mails auf eine öffentlich zugängliche Webpage, dann hat er nicht die originäre Nachricht veröffentlicht, sondern nur deren Inhalt.

Nicht tatbestandsmäßig handelt daher, wer bloß den Inhalt nach- oder weitererzählt.[1151] *Thiele* lässt aber eine digitale 1:1-Kopie der Nachricht zur Realisierung dieser Tathandlungen genügen.[1152] Eine nur auszugsweise Kopie der originalen Nachricht, wie sie zB durch »Copy and Paste« erzielt werden könnte, mit anschließender Weiterleitung an einen unberechtigten Dritten oder Veröffentlichung auf einer Internetseite, ist nicht von § 120 Abs 2a erfasst.

7. Unbefugter

Die Nachricht darf nicht für denjenigen bestimmt sein, der sie aufzeichnet, einem anderen Unbefugten zugänglich macht oder veröffentlicht. Dadurch wird auch impliziert, dass der Täter ebenfalls ein Unbefugter sein muss.

Täter kann überhaupt nur jemand sein, für den die Nachricht nicht tatsächlich bestimmt ist.

1150 Siehe *Thiele* in SbgK § 120 Rz 55; wohl auch *Lewisch/Reindl-Krauskopf* in WK² § 120 Rz 31d.

1151 Siehe dazu *Lewisch/Reindl-Krauskopf* in WK² § 120 Rz 31d.

1152 Vgl *Thiele* in SbgK § 120 Rz 62.

Leitet daher ein berechtigter Empfänger die Nachricht einem Unbefugten weiter oder veröffentlicht er sie im Internet, so entfällt bereits der objektive Tatbestand.

Auch erfasst der Tatbestand nicht das Zugänglichmachen einer für den Täter nicht bestimmten Nachricht, sofern alle anderen Empfänger, denen er diese Nachricht weiterleitet, Personen sind, für die diese Nachricht ohnehin bestimmt ist.

Beispiel: A erhält irrtümlich ein E-Mail zugestellt, das nicht für ihn bestimmt ist. A leitet dieses E-Mail dem B weiter, an den jedoch – was A nicht wusste – die Nachricht tatsächlich adressiert war.

In diesem Fall ist B kein »anderer Unbefugter« iSd Tathandlung »einem anderen Unbefugten zugänglich machen«, weshalb der Tatbestand nicht erfüllt ist.

Interessant zeigt sich nun derselbe Fall, wenn es sich um eine Nachricht handelt, die nicht für den Täter bestimmt ist, aber von diesem »veröffentlicht« wird. In diesem Beispielsachverhalt kommt es somit auf eine größere – dem Öffentlichkeitsbegriff gerecht werdende – Anzahl von Personen an, denen die Nachricht zugänglich gemacht wird. Das tatbestandliche Erfordernis, dass es sich dabei um »Unbefugte« handeln müsse, gibt es bei dieser Alternative nicht. Dies ist aber nur schlüssig, solange man davon ausgeht, dass es sich beim Veröffentlichen eben um einen »unbestimmten« Personenkreis handelt. In anderen Fällen, in denen man ausschließlich auch auf das Erfordernis einer Mindestpublizität iSd § 69 abstellt, kann es für eine »öffentliche Begehung« unerwünschte Ergebnisse geben.

Beispiel: A erhält irrtümlich ein E-Mail von der Geschäftsführung eines Unternehmens zugestellt, das nicht für ihn bestimmt ist und eine Anleitung zu Vorgehensweisen für – seiner Meinung nach – dubiose Machenschaften enthält. A leitet dieses E-Mail uno actu an die 200 Mitarbeiter dieses Unternehmens weiter, um sie in Kenntnis dieser Unternehmenspolitik zu setzen. A wusste allerdings nicht, dass die Nachricht tatsächlich auch für die Mitarbeiter bestimmt ist bzw war.[1153]

1153 Man könnte an eine abgeschlossene Benutzergruppe mit etwa 1000 Personen als Empfänger denken, denen A die Nachricht zugänglich macht, wobei diese Nachricht tatsächlich auch – was A nicht weiß – für alle Teilnehmer dieser Benutzergruppe (ursprünglich) bestimmt ist bzw sie diese bereits ggf auch schon erhalten

In diesem Fall ist nach dem rein quantitativen Element (mehr als 10 Personen) iSd § 69 von einer öffentlichen Begehung und daher von der Tathandlung des Veröffentlichens auszugehen. Diese Tathandlung enthält aber tatbestandlich keine Einschränkung, welche die Unbefugtheit der Adressaten betrifft, sodass in concreto der Tatbestand erfüllt ist – obwohl die Empfänger in diesem Fallbeispiel alle befugte Rezipienten sind. Da der objektive Tatbestand erfüllt ist (die nicht für den Täter bestimmte deliktstaugliche Nachricht wurde von diesem veröffentlicht), stellen sich keine Tauglichkeitsfragen bezüglich eines Versuchs. Subjektive Tatbestandsmäßigkeit ist ebenfalls hergestellt, da der Täter – neben dem Tatbildvorsatz – auch in der Absicht handelte, einem anderen Unbefugten vom Inhalt dieser Nachricht Kenntnis zu verschaffen (dass tatsächlich kein Unbefugter als Empfänger dabei war, schadet nicht, handelt es sich doch dabei bloß um eine innere Einstellung des Täters, die im Tatzeitpunkt vorliegen muss). Doch auch mit einer fehlenden Sozialschädlichkeit der Handlung lässt sich mE nicht argumentieren, weil das »Veröffentlichen« einer deliktsgegenständlichen Nachricht mit entsprechendem Vorsatz gerade den strafrechtlichen Unwert der Tat herstellt.

Würde man in diesem Fall das Vorliegen der Tathandlung »einem anderen Unbefugten zugänglich machen« konstatieren, was vom Wortlaut gedeckt wäre, wäre das gesetzliche Tatbild mangels der Unbefugtheit der Empfänger gar nicht erfüllt, selbst wenn die innere Tatseite deliktsspezifisch vorliegen würde.

Die Erl zur Entstehung des § 120 Abs 2a verweisen für die Tathandlungen des »Zugänglichmachens« und »Veröffentlichens« auf § 120 Abs 2. Dort kommentieren *Lewisch/Reindl-Krauskopf,* dass der Täter eine Aufnahme veröffentlicht, »wenn er sie einem unbestimmten Personenkreis zugänglich macht«.[1154]

An anderer Stelle und in einem vergleichbaren Zusammenhang (nämlich zu einer in Erwägung gezogenen neuen Strafbestimmung bezüglich Verletzung schutzwürdiger Geheimhaltungsinteressen durch Bildaufnahmen)[1155] wird in den GMat hins der Tathandlung des Veröffentlichens unter Rückgriff auf *Lewisch – wie* bereits oben angemerkt –

---

haben (etwaige Irrtumsprobleme auf subjektiver Tatseite werden an dieser Stelle nicht näher untersucht).

1154 Vgl *Lewisch/Reindl-Krauskopf* in WK² § 120 Rz 12.

1155 Siehe ErlME 82/ME XXIV. GP, 8.

ausgeführt: »Von einer Veröffentlichung wird man nicht erst bei einer massenmedialen Verbreitung, sondern – in Anlehnung an § 69 (Öffentliche Begehung) – schon dann sprechen können, wenn eine Bildaufnahme unmittelbar von einem größeren Personenkreis (Richtwert: ab etwa zehn Menschen) durch Zugänglichmachen (bloßes Bereitstellen durch z.B. Anbringen an öffentlichen Orten reicht aus) wahrgenommen werden kann«.[1156]

Insgesamt sollte man mE durchaus am quantitativen Element zur Abgrenzung der beiden hier angesprochenen Tathandlungen festhalten. Im deliktsspezifischen Zusammenhang müsste allerdings neben einer tatbestandlichen Ergänzung durch den Gesetzgeber eine rechtsfortbildende teleologische Reduktion dieser Tatbegehungsvariante in der Praxis vorgenommen werden.

8. Subjektive Tatseite

Auf der inneren Tatseite[1157] ist neben dem (zumindest bedingten) Tatbildvorsatz noch ein erweiterter Vorsatz gefordert, der sich im Stärkegrad der Absichtlichkeit (iSd § 5 Abs 2) auf die Kenntnisverschaffung des Inhalts der Nachrichten richten muss (Nachrichteninhaltsspionageabsicht)[1158]. Insoweit wird durch diese Einschränkung der Strafbarkeit über die überschießende Innentendenz das Schutzobjekt der Bestimmung weiter konkretisiert. Demnach ist Schutzobjekt dieser Bestimmung nur der »Inhalt einer Nachricht« und nicht auch jene Teile einer Nachricht, die nicht den gedanklichen Inhalt (= Mitteilung, Botschaft udgl) betreffen (zB Meta-Daten, wie ggf Quell- und Zieladressen und technische Protokollinformationen).

Releviert man nun aber den »Inhalt einer Nachricht« als Schutzobjekt dieser Bestimmung, kommt man nicht an der Frage vorbei, warum das Weiterleiten von Teilinhalten der Nachricht, wie etwa in Form einer neuen – durch »Copy and Paste« von Inhaltsteilen erzeugten – Nachricht nicht vom Tatbestand erfasst sein soll. In diesem Fall würde

---

1156 Vgl ErlME 82/ME XXIV. GP, 8; Man beachte dabei den Hinweis auf *Lewisch* in WK², wo sich allerdings für die tatsächlich getroffene Aussage in den GMat kein Substrat findet.

1157 Siehe dazu auch bereits S 219.

1158 *Hinterhofer* spricht in diesem Zusammenhang unpräzise von »Nachrichtenspionageabsicht« (vgl *Hinterhofer,* Geheimnisschutz, 173; ebenfalls nicht exakt die »Datenspionageabsicht« bei *Lewisch/Reindl-Krauskopf* in WK² § 120 Rz 31 f.

zwar nicht die ursprüngliche Nachricht weitergeleitet werden, aber das Schutzobjekt der Außenwelt, nämlich der »Inhalt einer Nachricht«.[1159]

§ 120 Abs 2a verfügt über eine explizite doppelte Subsidiaritätsanweisung zu Gunsten der »vorstehenden Bestimmungen« (dh für § 120 Abs 1 und 2) oder einer anderen Bestimmung, die mit strengerer Strafe bedroht ist (wie zB § 119[1160]). Eine Notwendigkeit oder gar ein Mehrwert der ersten Subsidiaritätsklausel gegenüber der zweiten lässt sich aber nicht ausmachen, sehen doch auch die Rechtsfolgen des § 120 Abs 1 und § 120 Abs 2 bereits strengere Strafdrohungen als § 120 Abs 2a vor.[1161]

9. Sonstiges

Aufgrund des Strafsatzes (Freiheitsstrafe bis zu 3 Monaten oder Geldstrafe bis zu 180 Tagessätzen) fällt § 120 Abs 2a in die sachliche Zuständigkeit des Bezirksgerichts (§ 30 Abs 1 StPO).

Es handelt sich dabei gem § 120 Abs 3 um ein Ermächtigungsdelikt iSd § 92 StPO, wobei die Ermächtigung von den jeweiligen Rechtsgutträgern zu erteilen ist. Das sind diejenigen, zu deren Kenntnisnahme die übermittelten Daten entweder bestimmt sind bzw von denen sie befugterweise stammen.[1162]

II. Vermögensbezogene Computerdelikte

Die ersten echten Computerdelikte im Kernstrafrecht (§ 126a und § 148a) wurden mit dem StRÄG 1987[1163] eingeführt und sind überwiegend[1164] dem Vermögensstrafrecht zugeordnet.

Die im öStGB systematische Eingliederung dieser Delikte im sechsten Abschnitt bei den strafbaren Handlungen gegen fremdes Vermögen wurde allerdings durch die CCC bzw den EU-Rahmenbeschluss

---

1159 Offensichtlich finden sich aber *Lewisch/Reindl-Krauskopf* in WK² § 120 Rz 31d und 31e damit ab.

1160 Siehe auch *Birklbauer/Hilf/Tipold,* Strafrecht BT I² §§ 119, 119a, 120 Rz 18.

1161 Vgl auch *Bergauer/Schmölzer* in Jahnel/Mader/Staudegger, IT-Recht³, 635 (665).

1162 Siehe dazu auch *Thiele* in SbgK § 120 Rz 103 f.

1163 BGBl 605/1987.

1164 Welche Rechtsgüter darüber hinaus noch geschützt werden, wird in der Ausarbeitung dieser Delikte noch gesondert angeführt.

2005/222/JI über Angriffe auf Informationssysteme weitgehend relativiert. Der Rechtsgüterschutz dieser Delikte ist daher – spätestens wohl mit der formellen Ratifikation der CCC im Jahr 2012 – ausgedehnt worden und erfasst zB was § 126a anlangt nach den Erwägungen zu Art 4 CCC auch das Interesse an Datensicherheit (iSv Unversehrtheit sowie ungestörter Verwend- und Verfügbarkeit).[1165] Weitere echte Computerdelikte, wie § 126b und § 126c, die nun ihre Wurzeln in den europäischen Vorgaben haben, wurden allerdings der traditionellen Systematik folgend ebenfalls in den sechsten Abschnitt des StGB »Strafbare Handlungen gegen fremdes Vermögen« eingegliedert. Der Vermögensschutzcharakter dürfte daher – entgegen der hier vertretenen Meinung – in Ö nach wie vor dominieren.

A. Datenbeschädigung (§ 126a)

> § 126a (1) Wer einen anderen dadurch schädigt, daß er automationsunterstützt verarbeitete, übermittelte oder überlassene Daten, über die er nicht oder nicht allein verfügen darf, verändert, löscht oder sonst unbrauchbar macht oder unterdrückt, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.
>
> (2) Wer durch die Tat an den Daten einen Euro 3.000,– übersteigenden Schaden herbeiführt, ist mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bis zu 360 Tagessätzen, wer einen Euro 50.000,– übersteigenden Schaden herbeiführt oder die Tat als Mitglied einer kriminellen Vereinigung begeht, mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren zu bestrafen.[1166]

Vor dem StRÄG 1987 waren die Meinungen bezüglich der strafrechtlichen Einordnung des unbefugten Veränderns und Löschens von Computerdaten kontrovers. Es war zweifelhaft, ob Daten, die weder in sichtbarer noch unmittelbar lesbarer Form gespeichert werden, eine Sache iSd Sachbeschädigung darstellen.[1167] Richtig ist, dass die unbefugte Manipulation (zB Löschung) eines Programms bzw von Daten, solange dabei keine Datenträger (Hardware) mitbeschädigt werden, jedenfalls nicht als

1165 Vgl etwa ER (ETS 185) Pkt 60.
1166 BGBl 60/1974 idF I 109/2007.
1167 Vgl etwa JAB 359 BlgNR XVII. GP, 16.

»Sachbeschädigung durch Zerstören« iS einer Substanzverletzung qualifiziert werden kann, da Daten als reine (unkörperliche) Informationsträger keine »körperlichen Sachen« sind.[1168] Selbst wenn die Bedienbarkeit und Lauffähigkeit eines Computerprogramms oder die Bearbeitung und Betrachtung anderer elektronischen Dateien technisch bedingt zumindest eine gewisse[1169] physikalische Zuordnung zu einem Datenträger erfordern, ändert dies nichts an der grundsätzlichen Substanzlosigkeit von Computerdaten im Besonderen und Software im Allgemeinen.

Eine »gewisse« Verkörperung ist nämlich dort zu finden, wo sich solche Daten zB auf Datenträgern – wie zB Massenspeichern – durch die in einer für den Computer verarbeitbaren Form (Binärcodierung) über sog »Bitmuster«[1170] manifestieren. Es gibt magnetische Datenträger (zB Festplatten, Disketten- oder Bandlaufwerke), die auf einer magnetisierbaren Schicht die Bitmuster (iSv Anweisungen, ob Strom fließen soll oder nicht) mit gegensätzlicher Polarität darstellen[1171], oder auch optische Datenträger (CD[1172] bzw DVD[1173]), welche Bitmuster durch unterschiedlich stark reflektierende Einbohrungen (Pits und Lands) in Metalloberflächen abbilden, die in weiterer Folge mit einem Laserstrahl abgetastet werden können. Schließlich sind noch die weniger bedeutsamen magneto-optischen Speichermedien zu nennen, denen ein Mischverfahren aus magnetischen und optischen Schreib- und Lesevorgängen zugrunde liegt. Dabei wird die Oberfläche solcher Datenträger durch die Hitzeeinwirkung eines Laserstrahls magnetisch veränderbar.[1174]

Zusammenfassend ist festzustellen, dass bloße Anweisungen über (wenn auch physikalische) Spannungszustände keine für eine »Sachbeschädigung durch Zerstörung« notwendige Körperlichkeit (iS einer Sachsubstanz) besitzen.[1175]

1168 Siehe *Bergauer/Schmölzer* in Jahnel/Mader/Staudegger, IT-Recht[3], 635 (648); weiters *Birklbauer/Hilf/Tipold,* Strafrecht BT I[2] § 126a Rz 1; *Glaser,* Bitcoins aus strafrechtlicher Sicht, in Eberwein/Steiner (Hrsg), Bitcoins (2014) 127 (128); grundlegend bereits *Jaburek/Schmölzer,* Computer-Kriminalität, 53.

1169 Siehe dazu gleich im Anschluss.

1170 Bit = »Binary Digit« (vgl dazu *Tanenbaum,* Computerarchitektur[5], 87 f).

1171 Vgl etwa *Tanenbaum,* Computerarchitektur[5], 100 ff.

1172 Compact Disc.

1173 Digital Versatile Disc.

1174 Siehe zu diesen Massenspeicherverfahren eingehend *Kersken,* IT-Handbuch[5], 143 ff; weiters *Tanenbaum,* Computerarchitektur[5], 110 ff.

1175 Siehe dazu bereits *Schick/Schmölzer,* EDVuR 1992, 107; *Jaburek/Schmölzer,* Computer-Kriminalität, 53.

Eine »Sachbeschädigung am Computersystem« iS einer (bloßen) Substanzbeeinträchtigung bzw Funktionsstörung durch Unbrauchbarmachen wurde allerdings diskutiert.[1176] Nach gefestigter Rsp liegt eine Sachbeschädigung nämlich auch dann vor, wenn zwar keine Verletzung der Sachsubstanz vorliegt und die Sache an sich unbeschädigt bleibt, jedoch erst durch einen entsprechenden Aufwand an Zeit und Arbeit wieder der eigentlichen Zweckbestimmung zugeführt werden kann.[1177] Abgestellt wird in diesem Fall auf die konkrete Funktion der Sache. Um diese Auffassung auf die Informationstechnologie umzulegen, musste Hard- und Software als eine untrennbare Funktionseinheit angesehen werden, wobei die Schädigung nur eines dieser ungleichen Teile die gesamte Funktionseinheit unbrauchbar macht (vgl bspw Daten auf einer Festplatte).[1178] *Reindl* fasst diesbezüglich entsprechende Gegenmeinungen zusammen, die davon ausgehen, dass es geradezu die bestimmungsgemäße Aufgabe der (meisten[1179]) Datenträger sei, Daten zu speichern, aber auch wieder zu löschen, weshalb die bestimmungsgemäße Funktionalität trotz rechtswidriger Datenlöschung erhalten bleibe.[1180]

Die Diskussion über die Anwendbarkeit der Sachbeschädigung bei Datenbeschädigungen wurde durch die Einführung des – der Sachbeschädigung analogen[1181] – Spezialtatbestands der Datenbeschädigung (§ 126a) mit dem StRÄG 1987 weitgehend abgebrochen.[1182]

Aber auch Art 4 CCC sieht einen solchen Straftatbestand (»Data interference«) vor, den es für die Mitgliedstaaten des Europarats innerstaatlich umzusetzen gilt. In Österreich bestand allerdings zum Zeitpunkt der faktischen Teilumsetzung[1183] der CCC durch das StRÄG 2002 diesbezüglich kein Umsetzungsbedarf mehr, da nach den GMat die Vorgaben des Art 4 CCC bereits zur Gänze in § 126a idF StRÄG 1987

1176 Vgl *Schick/Schmölzer,* EDVuR 1992, 107; *Schmölzer* in FS Göppinger², 237 (255); weiters *Schmölzer,* EDVuR 1988, 20; siehe auch *Seiler,* JBl 1989, 746.

1177 Vgl bereits OGH 07.09.1978, 12 Os 94/78.

1178 Siehe zB als ein Vertreter dieser Ansicht *Seiler* in SbgK § 125 Rz 48.

1179 Ausgenommen müssen aber sachgemäß »Read-only-Speichermedien« sein.

1180 Vgl *Reindl,* E-Commerce, 129 f mwN; auch *Proske,* Hacking im Strafrecht, EDVuR 1990, 102.

1181 Siehe JAB 359 BlgNR XVII. GP, 16 und 17, wo die »verhältnismäßig weitgehende Ähnlichkeit sowohl in der äußeren Verhaltensweise als auch im Unwert« mehrfach angesprochen wird.

1182 Siehe dazu eingehend *Schick/Schmölzer,* EDVuR 1992, 107.

1183 Siehe dazu *Bergauer,* jusIT 2012/95, 205.

aufgingen.[1184] Obwohl der Tatbestand rein faktisch nicht mehr an Art 4 CCC angepasst werden musste, ist für dessen Auslegung die Konvention mitbestimmend.

Jedenfalls wurde von der Möglichkeit nach Art 4 Abs 2 CCC, dass nur ein solches Verhalten unter Strafe zu stellen ist, wenn die strafbare Handlung zu einem schweren Schaden führt, in Ö nicht Gebrauch gemacht, sodass de lege lata eine Strafbarkeit auch dann eintritt, wenn kein schwerer Schaden verursacht wird.[1185] Dass auch die Konventionsverfasser den Tatbestand der Datenbeschädigung analog zu dem der Sachbeschädigung vorgesehen haben und auch so verstanden wissen wollen, ergibt sich ausdrücklich aus ER (ETS 185) Pkt 60, wo festgehalten wurde: »The aim of this provision is to provide computer data and computer programs with protection similar to that enjoyed by corporeal objects against intentional infliction of damage«.

Der Vollständigkeit halber sein angemerkt, dass auch Art 4 EU-RB 2005/222/JI[1186] einen entsprechenden Tatbestand vorsieht. Hierbei wird ausdrücklich auf das »unbefugte vorsätzliche Löschen, Beschädigen, Verstümmeln, Verändern, Unterdrücken oder Unzugänglichmachen von Computerdaten eines Informationssystems« abgestellt.

Durch die systematische Einordnung der Datenbeschädigung im StGB unter den Abschnitt der Vermögensdelikte und das gesetzgeberische Analogon[1187] des § 126a zur Sachbeschädigung, liegt auch der primäre Schutz des Rechtsguts »Vermögen« auf der Hand. Mit der Normierung dieses neuen Straftatbestands erkannte der Gesetzgeber somit erstmals (automationsunterstützt verarbeitete) »Daten« als ein eigenständiges schützenswertes Vermögensobjekt an.[1188] Nach mittlerweile hM handelt es sich aber bei § 126a nicht um ein reines Vermögensdelikt, da auch das »Interesse am Fortbestand und der Verfügbarkeit von Daten« durch diese Strafbestimmung geschützt werde.[1189]

1184 Siehe ErlRV 1166 BlgNR XXI. GP, 27.

1185 Siehe ErlStV 1645 BlgNR XXIV. GP, 4.

1186 »Rechtswidriger Eingriff in Daten«.

1187 Siehe JAB 359 BlgNR XVII. GP, 16 f.

1188 Vgl *Reindl,* E-Commerce, 130; weiters *Fuchs/Reindl-Krauskopf,* BT I[4], 139.

1189 Vgl statt vieler *Triffterer* in SbgK § 126a Rz 21 (aF Stand Dezember 1992); weiters *Kienapfel,* BT II[3] § 126a Rz 5; weiters *Reindl-Krauskopf,* Computerstrafrecht[2], 20 f bzw *Reindl,* E-Commerce, 101 ff; weiters *Bergauer/Schmölzer* in Jahnel/Mader/Staudegger, IT-Recht[3], 635 (648); weiters *Birklbauer/Hilf/Tipold,* Strafrecht BT I[2] § 126a Rz 1.

In diesem Zusammenhang ist anzumerken, dass auf Konventionsebene überhaupt nur auf letztgenanntes Rechtsgut fokussiert wird, wenn klargestellt wird: »The protected legal interest here is the integrity and the proper functioning or use of stored computer data or computer programs«.[1190]

Nachdem auch Ö nicht von der Möglichkeit eines Vorbehalts nach Art 4 Abs 2 CCC – für die Strafbarkeit lediglich auf einen schweren Schaden abzustellen[1191] – Gebrauch gemacht hat, sollte nun auch aller Zweifel ausgeräumt sein, dass jede Betrachtung des Tatbestands neben vermögensrechtlichen Aspekten – zumindest auch (und spätestens seit formeller Ratifikation der CCC im Jahr 2012)[1192] – die Einbeziehung des »Interesses am Fortbestand und der Verfügbarkeit von Daten« erfordert.[1193]

Zudem kann damit insb auf Formen der Computerkriminalität reagiert werden, in denen der Täter mittels Malware[1194] Schäden an automationsunterstützt verarbeiteten Daten herbeiführt, wie zB durch »Computerviren« oder »Computerwürmern«.

1. Exkurs: Computerviren und Computerwürmer

Der Begriff »Computervirus« wurde 1984 von *Cohen* folgendermaßen definiert: »We define a computer virus as a program that can infect other programs by modifying them to include a possibly evolved copy of itself. With the infection property, a virus can spread throughout a computer system or network using the authorization of every user using it to infect their programs. Every program that gets infected may also act as a virus and thus the infection grows«.[1195]

1190 Vgl ER (ETS 185) Pkt 60.

1191 Siehe ErlStV 1645 BlgNR XXIV. GP, 4.

1192 Vgl *Bergauer,* jusIT 2012/95, 205.

1193 Was insb auch für die Anerkennung eines bloßen »Affektionsinteresses« bezüglich eines etwaigen (Vermögens-)Schadens an solchen Daten spricht (siehe dazu unten).

1194 Zusammengesetztes Kurzwort für »malicious software« und bezeichnet jegliche Arten von Schadprogrammen in informationstechnischen Systemen (siehe dazu auch *Slade,* Software Forensics, 95).

1195 Vgl *Cohen,* Computerviruses – Theory and Experiments, Computers and Security 1984, 22 (23).

Als Computervirus[1196] versteht man daher einen unselbstständigen Programmteil, der sich selbsttätig reproduzieren kann, indem er sich selbst in andere Programme hineinkopiert.[1197] Die Bezeichnung wurde in Analogie zur Reproduktionsfähigkeit des biologischen Virus gewählt.[1198] Computerviren verbreiten sich idR über ausführbare Computerprogramme, indem sie den Binärcode dieser Dateien manipulieren.[1199] Weit verbreitet sind auch sog »Virus-Construction-Kits«[1200], also »Virenbaukastensysteme«, die sehr einfach im Internet zu finden sind. Damit besteht für technisch nicht sonderlich Versierte die Möglichkeit, sich ganz ohne Programmierkenntnisse einen Computervirus »menügesteuert« zu generieren und ggf gleich zu verbreiten (sog »Kit-Virus«). Mit dem Virus infiziert ist eine Datei bzw ein Computersystem dann, wenn sich das Schadprogramm an diese Datei anhängt und in weiterer Folge im System tätig werden kann.[1201] Von Computerwürmern unterscheidet sich der Virus als bloßer Programmteil (bzw Programmroutine) grundsätzlich dadurch, dass er stets auf ein Träger- bzw Wirtsprogramm angewiesen ist und andernfalls gar nicht lauffähig wäre.

Viren entsprechen im Wesentlichen einer dreiteiligen Programm- bzw Funktionsstruktur: dem Infektions-, dem Payload- und dem Triggermechanismus.[1202]

Der Infektionsmechanismus sorgt für die Verbreitung des Schadprogramms und besteht grundsätzlich aus mehreren Teilen. Die erste Funktion deckt die Suche nach Objekten ab, die überhaupt – der Spezifikation zufolge – infiziert werden können. Im Zuge dessen wird aber idR auch überprüft, ob diese Datei bereits infiziert ist. Die zweite Funktion kümmert sich um das Einschleusen einer (Selbst-)Kopie des Virencodes in die gefundene Datei zB durch Schreiben eines neuen Codeabschnitts im Bootsektor oder Einfügen eines Codes in eine Pro-

1196 Es macht uU Sinn zur besseren Unterscheidung in der Informationstechnologie von »der Virus«, anstelle des medizinischen »das Virus« zu sprechen; in weiterer Folge ist mit dem Ausdruck »Virus« ausschließlich der Computervirus gemeint.

1197 Siehe *von Gravenreuth,* Computerviren, 2; weiters *Winterer,* Viren, 21; *Strauss,* Technische und organisatorische Maßnahmen zur Abwehr von Computerviren, EDVuR 1989, 130 ff.

1198 Siehe *Bergauer,* Malware, 156.

1199 Vgl *Kersken,* IT-Handbuch[5], 1058.

1200 auch »Virii-Creators« genannt; *Winterer,* Viren, 349.

1201 Vgl *Harley/Slade/Gattiker,* Anti-Viren-Buch, 36; vgl auch *Winterer,* Viren, 71 f.

1202 Siehe *Kersken,* IT-Handbuch[5], 1059; weiters *Harley/Slade/Gattiker,* Anti-Viren-Buch, 130 f.

grammdatei (sog »Infector«[1203]). Es gibt aber auch Varianten, die lediglich Sprungbefehle in Programmdateien implementieren, ohne eine Kopie des Virencodes in die konkrete Datei zu migrieren. Dabei referenziert dieser Sprungbefehl bloß auf den Viruscode einer bereits infizierten Datei. Der Befehlszähler (sog »Instruction Pointer«) wird während des Programmlaufs dadurch veranlasst, den Code der verwiesenen Speicheradressierung auszuführen.[1204]

Der Payload (Nutzlast) ist der Aktionscode eines Computervirus, der die eigentliche schädigende Funktionalität enthält. Ein solcher ist jedoch nicht zwingend notwendig, sodass oft schon die Infektion bzw ein Mehrfachbefall ausreicht, damit ein Programm nicht mehr bestimmungsgemäß ausgeführt werden kann.[1205]

Der Trigger (Auslöser) bestimmt, wann der Payload ausgeführt werden soll, sofern ein solcher vom Virenautor überhaupt definiert wurde. Dabei kann ein bestimmtes Datum oder ein anderes Kriterium vordefiniert werden, an dem sich der Payload aktivieren soll, zB wenn die Festplatte zu mehr als die Hälfte ausgelastet ist usw. Auch der Trigger ist optional und muss in einem solchen Schadprogramm nicht unbedingt vorhanden sein.[1206]

Computerviren werden nach unterschiedlichen Kriterien klassifiziert und kategorisiert[1207]:

a. Bootsektorviren

Auf jedem formatierten Datenträger befindet sich grundsätzlich ein Bootsektor bzw Master Boot Record (MBR), der im ersten physischen bzw logischen Sektor des Datenträgers angesiedelt sein kann. Beim Bootvorgang eines Computersystems wird nach dem Selbsttest der Stromversorgung und dem Abarbeiten des BIOS[1208]-Codes der Booteintrag der Partition im ersten Sektor des ersten Bootlaufwerks als

1203 Vgl *Solomon,* Computer Security, 81.
1204 Siehe *Harley/Slade/Gattiker,* Anti-Viren-Buch, 130 f.
1205 Siehe *Solomon,* Computer Security, 73 ff.
1206 Vgl *Harley/Slade/Gattiker,* Anti-Viren-Buch, 37 bzw 130 f; weiters *Solomon,* Computer Security, 81.
1207 Siehe nachfolgend eine Typenauswahl.
1208 Das »Basic Input/Output System« ist ein Programm, das in einem Festspeicher (ROM- bzw Flash-Speicher) auf der Hauptplatine (Mainboard) gespeichert ist. Es initialisiert die im System installierte Hardware und startet das eigentliche Betriebssystem (vgl etwa *Gumm/Sommer,* Informatik[10], 61 f).

Programm ausgeführt.[1209] Da prinzipiell jeder Bootsektor ein Bootprogramm enthält, das im normalen Betrieb nicht sichtbar ist, weil für dieses Programm kein Eintrag am Anfang der Dateiliste des Speichermediums (sog »Datenträgerindex«) existiert, werden Bootviren, die in diesen Sektor des Datenträgers implementiert wurden, unmittelbar nach dem BIOS-Code und noch vor dem Betriebssystem ausgeführt. Dabei wird der Virus beim Ausführen in den Arbeitsspeicher geladen und dort resident gehalten.[1210] Von dort aus können nun in weiterer Folge andere Datenträger und Programme infiziert bzw der Payload ausgeführt werden.[1211]

b. Dateiviren

Dateiviren nutzen verschiedene Methoden, um die Zieldatei zu befallen. Entweder sie überschreiben den Programmcode des ursprünglichen Programms (parasitäre Viren), fügen ihren Code am Anfang oder am Ende der Zieldatei hinzu oder sie schleusen den Virencode über Sprungbefehle in die Befehlskette ein, sodass er ausgeführt wird, wenn der Programmlauf der infizierten Datei über diese Sprungbefehle führt. In erster Linie werden ausführbare Programme bzw Skript-Dateien infiziert, wie etwa Files mit den Erweiterungen .EXE, .COM oder .VBS.[1212]

c. Polymorphe Viren

Diese Virengattung verschlüsselt sich durch die Verwendung von komplexen Verschlüsselungstechniken nach jeder Infektion komplett neu.[1213] Die Virussignatur wird dadurch völlig umgestaltet. Daher ist kein konstantes Muster zur Identifikation durch Virenschutzprogramme mehr vorhanden. Als Programmierhilfe für Virenautoren dienen sog »Mutation Engines«, die es erlauben, jeden Virus durch Selbstverschlüsselungsverfahren mutieren zu lassen. Es handelt sich hierbei nicht um einen eigenen Virus, sondern um einen Codegenerator, der durch Hinzufügen eines Codesegments den Virus polymorph macht.[1214]

1209 Vgl *Winterer,* Viren, 91 ff; vgl *Solomon,* Computer Security, 54 ff; auch *Harley/Slade/Gattiker,* Anti-Viren-Buch, 148 ff.
1210 Vgl etwa *Kersken,* IT-Handbuch[5], 1059.
1211 Vgl *Winterer,* Viren, 92 f.
1212 Vgl mit Beispielen *Bergauer,* Malware, 159.
1213 Siehe *Kersken,* IT-Handbuch[5], 1060.
1214 Vgl *Winterer,* Viren, 51 f; weiters *Harley/Slade/Gattiker,* Anti-Viren-Buch, 177 ff.

d. Stealth-Viren[1215]

Stealth-Viren werden konzipiert, um ihre Existenz auf einem Computersystem durch diverse Tarnmechanismen zu verschleiern. Sie sind allein schon deshalb schwer ausfindig zu machen, weil sie zB trotz Implementierung ihres eigenen Codes in das Wirtsprogramm eine unveränderte Dateigröße oder Prüfsumme dieser infizierten Datei vortäuschen[1216] oder aber auch Systembefehle bzw Virenschutzprogramme entsprechend manipulieren.[1217] Auch wenn der Virus selbst polymorpher Art wäre, müsste er sich grundsätzlich in das zu infizierende Trägerprogramm hineinkopieren, was zur Folge hätte, dass die Größe der Gesamtdatei zwangsläufig zunehmen würde. Der Virus liest jedoch zB die Dateiattribute des »Headers«[1218] des Trägerprogramms vor dessen Befall aus und stellt diese Werte gleich nach der Infektion wieder her. Die Stealth-Technologie im Bereich der Computerviren bezeichnet somit alle Mittel, die es einem Virus ermöglichen, versteckt und unerkannt zu operieren.[1219]

e. Hybridviren bzw multipartite Viren

Hybridviren vereinen unterschiedliche Vireneigenschaften in einem Virus. Beispielsweise wird nicht nur der Bootsektor eines Datenträgers infiziert, sondern es werden zusätzlich auch noch ausführbare Programme im Zielsystem befallen. Ein Hybridvirus stellt somit eine Kombination bspw aus einem Boot- und Dateivirus dar, weshalb sich die speziellen Eigenschaften dieser beiden Gattungen in einem Schadprogramm vereinen. Hybridviren sind in ihrem Design äußerst komplex und der Infektionsmechanismus nur schwer zu programmieren, sodass sie in der Praxis bislang kaum vorkommen.[1220]

1215 Auch Tarnkappenviren genannt.
1216 Siehe *Solomon,* Computer Security, 90 f; weiters *Harley/Slade/Gattiker,* Anti-Viren-Buch, 173 f; vgl auch *Winterer,* Viren, 94.
1217 Vgl *Kersken,* IT-Handbuch[5], 1060.
1218 Darunter versteht man äußere Zusatzinformationen (auch Meta-Daten oder Kopfdaten) einer Datei bzw eines Computerprogramms.
1219 Siehe *Solomon,* Computer Security, 90.
1220 Vgl *Solomon,* Computer Security, 63.

f. Makro- bzw Skriptviren[1221]

Als »Makro« bezeichnet man ein kleines Programm, das der Automatisierung von Routineaufgaben in diversen Programmen dienen soll.[1222] Dabei sind häufig die weitverbreiteten Programme der Firma Microsoft (vgl Word, Excel, Access, Powerpoint) betroffen, in denen für die Programmierung solcher Makros die Makrosprache »Visual Basic for Applications« (VBA) Verwendung findet. Damit können Befehle zur Steuerung von zB MS-Windows oder MS-Office verarbeitet werden. Makros sind allerdings nur in der Programmumgebung funktionstüchtig, von der sie unterstützt werden. Außerhalb einer solchen Umgebung ist ein VBA-Makro – und daher auch ein solcher Makrovirus – grundsätzlich nicht lauffähig. Die meisten Office-Makroviren befallen nicht selten sofort die Standard-Vorlagedateien und in weiterer Folge auch jedes neu erstellte Dokument.[1223]

Ein »Skript« ist eine Sammlung von Anweisungen – ähnlich einem Makro – die als Quelltext vorliegt und von einem geeigneten Interpreter in Echtzeit zeilenweise übersetzt und ausgeführt wird (zB VBS[1224]). Makro- und Skriptviren sind keine kompilierten (Binär-) Programme, sondern liegen als ein von einem Interpreter abzuarbeitender Quellcode vor, der von einem geeigneten Befehlsinterpreter prozessiert werden muss. Die schädigende Funktionalität dieser Viren unterscheidet sich kaum von anderen Virentypen, wobei Skriptviren sogar E-Mail-Attachments ohne Interaktion des Empfängers ausführen können.[1225]

g. Speicherresidente- bzw TSR-Viren

Das Akronym »TSR«[1226] stammt aus der Zeit der Microsoft »DOS«[1227]-Betriebssysteme. Durch diese Funktionalität konnten Programme ein Codesegment im Arbeitsspeicher hinterlassen, um ausführbar zu bleiben. Das Programm blieb daher im Arbeitsspeicher und konnte durch

---

1221 Vgl *Harley/Slade/Gattiker,* Anti-Viren-Buch, 167 ff; weiters *Solomon,* Computer Security, 63.
1222 Siehe *Solomon,* Computer Security, 52.
1223 Siehe *Kersken,* IT-Handbuch[5], 1060.
1224 Microsoft »Visual Basic Script«.
1225 Vgl *Winterer,* Viren, 89.
1226 »Terminate and stay resident«.
1227 »Disc Operating System«.

»Hardware-Interrupts«, wie zB den Keyboard-Handler bei der Verwendung von Hotkeys[1228], wieder ausgeführt werden. TSR-Viren verharren nach Aufruf des befallenen Programms im Arbeitsspeicher bis der Computer neu gestartet oder abschaltet wird. Einige derartiger Viren können auch während eines eingeschränkten Bootvorgangs (zB Warmstart) lauffähig im System verbleiben (zB sog »Joshi-Virus«[1229]). Die Problematik liegt bei speicherresidenten Viren darin, dass bei der Säuberung infizierter Dateien durch Virenschutzprogramme der im Arbeitsspeicher aktive Virusteil die bereinigte Datei sofort erneut befallen kann.

Grundsätzlich sind auch alle Bootsektorviren speicherresident konzipiert, da nach Abschluss des Bootvorgangs ein Bootsektor im normalen Betrieb nicht aufgerufen wird und der Virus sich nur entfalten kann, wenn er nach dem Booten im Arbeitsspeicher aktiv bleibt.[1230] Die Gefährlichkeit dieser Viren lässt sich auch daran erkennen, dass schädigende Operationen im System ausgeführt werden können, ohne dass der Benutzer überhaupt eine Aktion ausgelöst hat.[1231] Bei modernen Betriebssystemen können diese Techniken nicht mehr so einfach umgesetzt werden. Aktuell werden daher derartige speicherresidente Viren zB als virtuelle Gerätetreiber (VxD) oder als Windows-Dienste implementiert und ausgeführt.[1232]

h. Proof-of-Content-Viren

In den letzten Jahren sind immer mehr Viren aufgetaucht, die keinen schädigenden Payload besitzen und nur die Existenz von Schwachstellen eines Zielsystems aufzeigen sollen. Programmierer derartiger Viren werden meist von Neugier angetrieben und entstammen oft den Bereichen Wissenschaft oder Virenschutzindustrie. Einer der ersten Vertreter dieser Viren war »Concept«, der den »Beweis« dafür geliefert hat, dass »Word-Viren« (vgl Makroviren) möglich sind. »Concept« führte als Payload lediglich die Meldung »That's enough to prove a point« mit,

1228 Als Hotkeys werden Tastaturbefehle bezeichnet, die es ermöglichen sollen, Aktionen per Tastendruck schneller ausführen zulassen.
1229 Vgl *Securelist,* <www.securelist.com/en/descriptions/56696/Virus.Boot.Joshi.a> (01.04.2014).
1230 Siehe *Harley/Slade/Gattiker,* Anti-Viren-Buch, 134.
1231 Vgl *Bergauer,* Malware, 158 f.
1232 Vgl *Harley/Slade/Gattiker,* Anti-Viren-Buch, 134 f.

die bei gelungener Infektion eines Word-Dokuments dem Benutzer anzeigt wurde.[1233]

Prinzipiell können Computerviren jede Art von Schaden anrichten, der sich mit Software überhaupt realisieren lässt. In erster Linie beschränken sich typische Computerviren – im Gegensatz zu Computerwürmern – auf ein oder mehrere Dateien und einzelne Computersysteme. Doch auch technische Mischformen (vgl ein mit Wurm-Verbreitungstechniken ausgestatteter Makrovirus mit Spionagefunktionalität) kommen in der Praxis vor, sodass eine klare Unterscheidung der vielseitigen Schadprogramme kaum möglich erscheint.

i. Computerwürmer

Computerwürmer sind sich selbst reproduzierende Computerprogramme, die – im Unterschied zu Computerviren – keine Wirts- bzw Trägerprogramme benötigen und sich explosionsartig über Netzwerke verbreiten.[1234] Sie orientieren sich dabei nicht an einzelnen Dateien, sondern befallen komplette Systeme und Netzwerke.[1235]

Der einzelne Computer dient dabei lediglich als Mittel zum Zweck, nämlich ganze Computernetzwerke zu attackieren.[1236] Daher agiert ein Computerwurm grundsätzlich auf zwei Ebenen, der Computer- und der Netzwerkebene. Auf der Computerebene befällt der Computerwurm (in diesem Fall nur in Form eines »Wurmsegmets«) einzelne Computersysteme. In weiterer Folge führt die Vereinigung sämtlicher Wurmsegmente auf Netzwerkebene letztlich zur vollständigen Entfaltung der schädigenden Funktion (daher auch die Bezeichnung »Computerwurm«).[1237]

Computerwürmer gibt es bereits seit vielen Jahren. Einer der ersten Vertreter trat im Jahr 1971 unter der Bezeichnung »Creeper« auf und wurde von Entwicklern der Advanced Research Projects Agency (ARPA) im Rahmen einer Machbarkeitsstudie[1238] programmiert. Das

---

1233 Vgl *Winterer,* Viren, 87 f; vgl auch *Harley/Slade/Gattiker,* Anti-Viren-Buch, 74 f.
1234 Siehe *Harley/Slade/Gattiker,* Anti-Viren-Buch, 100.
1235 Vgl *Winterer,* Windows, 122.
1236 Siehe *Winterer,* Viren, 131; weiters *Winterer,* Windows, 122 ff.
1237 Vgl dazu auch *Gleißner/Grimm/Herda/Isselhorst,* Manipulation in Rechnern und Netzen. Risiken, Bedrohungen und Gegenmaßnahmen (1989) 23.
1238 Als Beweis dafür, dass sich Software selbstständig durch Netzwerke bewegen kann.

Programm stellt eine Verbindung mit Zielsystemen innerhalb des »ARPANET« her und replizierte sich in diese Systeme. Die Programmkopie ließ auf den infizierten Rechnern die Meldung »I'm the creeper, catch me if you can« erscheinen.[1239] Zur gezielten Entfernung dieses Computerwurms wurde »Reaper« programmiert, der sich ebenfalls im ARPANET selbstständig bewegen konnte, um Creeper-Programmkopien aufzusuchen und zu löschen. Ähnlichkeiten mit Creeper hatte auch der aus dem Jahr 1988 bekannt gewordene »Morris-Wurm«[1240], der von einem Studenten des MIT entwickelt wurde und öffentlich zugängliche Netzwerke durch Mehrfachbefall lahmgelegt hat. Der Morris-Wurm wurde daher auch als »Internetwurm« bezeichnet.

Wie auch Computerviren bestehen Computerwürmer im Wesentlichen aus dem »Infektionsmechanismus«, dem »Payload« und ggf einer »Trigger-Funktion«.

In vielen Fällen verbreiten sich Würmer selbsttätig über Sicherheitslücken in Betriebssystemen bzw Anwendungsprogrammen (sog »Netzwürmer« oder »Webwürmer«) oder E-Mail-Adressbücher (sog »E-Mail-Würmer«) der Angriffsobjekte.[1241] Einige Vertreter dieser Malware sind an die Mitwirkung der Opfer gebunden, die das E-Mail mit dem gefährlichen Wurm erst öffnen müssen, damit das Programm ausgeführt werden kann. Andere wiederum gehören zur Kategorie der »selbststartenden Computerwürmer«, bei denen das Opfer selbst keine Aktion mehr tätigen muss, um das Schadprogramm zu laden (zB der »Sasser-Wurm«[1242]).[1243] Eine aktive Internetverbindung reicht für die Infektion und die Schädigung bereits aus.[1244]

(Exkurs Ende)

1239 Siehe *Winterer,* Windows, 124; vgl auch *Chip Online,* Creeper: Der erste Computer-Wurm wird 40, <www.chip.de/news/Creeper-Der-erste-Computer-Wurm-wird-40_51912666.html> (01.04.2014).

1240 Der nach seinem Programmierer *Robert T. Morris* benannt wurde; vgl *Winterer,* Viren, 140 ff; siehe auch *Harley/Slade/Gattiker,* Anti-Viren-Buch, 405.

1241 Vgl *Winterer,* Windows, 130.

1242 Siehe mehr dazu auf S 539.

1243 Siehe *Harley/Slade/Gattiker,* Anti-Viren-Buch, 101.

1244 Auch die sog »Drive-by-Download«-Methode führt dazu, dass nach einem Download eines Programms von einer Website, das Programm (zB der Computerwurm) selbstständig ausführt wird.

2. Computerdaten

Tatobjekt des § 126a sind in erster Linie »automationsunterstützt verarbeitete, übermittelte oder überlassene Daten« (hier: Daten im engen Sinn bzw Computerdaten). Darüber hinaus muss der Täter »einen anderen« schädigen, weshalb als weiteres Tatobjekt ein anderer Mensch tatbildlich erfasst ist. Die Computerdaten, als Schädigungsobjekt des § 126a, sind Gegenstand der besonderen Verhaltensbeschreibung durch die, der andere Mensch geschädigt werden muss. Da nicht jede Schädigung eines anderen Menschen den Tatbestand erfüllt, sondern nur eine solche, die durch Datenbeschädigung herbeigeführt wird, handelt es sich bei § 126a um ein verhaltensgebundenes Erfolgsdelikt. Die tatbildlichen Daten müssen folglich den Rechtsgütern[1245] des anderen Menschen, als Rechtsgutträger, zugeordnet sein.

Der Datenbegriff wird seit dem StRÄG 2002 in § 74 Abs 2 für das gesamte Kernstrafrecht »inhaltlich konkretisiert«[1246] und umfasst – sehr weit gehalten – sowohl personenbezogene und nicht personenbezogene Daten als auch Programme. Die Klarstellung, dass in Abgrenzung zum Datenschutzgesetz 2000 jede Information vom Datenbegriff umfasst wird, führt zu dem Schluss, dass es auf den Inhalt der Daten faktisch nicht ankommt. So sind reine Systemdaten[1247] und Computerprogramme ebenso geschützt, wie sämtliche (pragmatische) Information, die mittels Daten repräsentiert wird (gedanklicher Inhalt). Selbst auf Systemebene als sinnlose Daten angesehene Zeichenfolgen werden geschützt, sofern ein (Vermögens-)Interesse des Nutzers daran besteht. Man denke bspw an verschlüsselte Dateien, die den Anschein von völlig zufälligen und sinnlosen Zeichenketten erwecken können.[1248]

Die tatbestandliche Einschränkung auf Daten, die automationsunterstützt verarbeitet, übermittelt oder überlassen werden, bildet aber die Brücke zu reinen Computerdaten (hier: Daten im engen Sinn).[1249]

1245 Entweder dem »Vermögen« oder dem »Interesse am Fortbestand und der Verfügbarkeit von Daten«.

1246 In Wahrheit stellt § 74 Abs 2 nämlich keine technische Begriffsdefinition von Daten dar, sondern eine auf den Inhalt abstellende Konkretisierung (siehe zum Datenbegriff des Kernstrafrechts bereits S 60 ff).

1247 Darunter auch Verkehrsdaten, Zugangsdaten, Standortdaten usw.

1248 Vgl auch *Schuhr,* Analogie und Verhaltensnorm im Computerstrafrecht, ZIS 2012, 441 (445).

1249 Siehe dazu auch ausdrücklich die Vorgabe aus Art 4 CCC und Art 4 des EU-RB 2005/222/JI.

Das Tatobjekt »Daten« wird daher einerseits im Tatbestand selbst auf die informationstechnische Verarbeitungsform (iSv Computerdaten[1250]) eingeschränkt und andererseits wird über die Begriffsbestimmung von Daten des § 74 Abs 2 bestimmt, sodass jede durch Computerdaten repräsentierte Information[1251] erfasst ist. Es gibt daher – außer was den Wiederherstellungsaufwand anlangt[1252] – auch keine Abstufung nach der Schutzwürdigkeit der durch die Daten verkörperten Information. Gegebenenfalls könnte, was insb die Schutzwürdigkeit von personenbezogenen Daten betrifft, § 51 DSG 2000 ins Treffen geführt werden.

Durch die Formulierung »automationsunterstützt verarbeitete, übermittelte oder überlassene Daten« werden konventionelle Daten – iSv manuellen Dateien, die nicht IT-mäßig verarbeitet werden bzw werden können – als Tatobjekte des § 126a ausgeschieden (zB Daten, die auf Papier geschrieben sind[1253]).

Alle Daten, die sich auf einem elektronischen Datenträger befinden, sind zwangsläufig verarbeitete oder übermittelte Daten.[1254] Die Trias des »Verarbeitens, Übermittelns und Überlassens« erinnert an die Terminologie des DSG. Dort wird nämlich aktuell unter dem »Verarbeiten von Daten« (§ 4 Z 9 DSG 2000) »das Ermitteln, Erfassen, Speichern, Aufbewahren, Ordnen, Vergleichen, Verändern, Verknüpfen, Vervielfältigen, Abfragen, Ausgeben, Benützen, Überlassen (Z 11), Sperren, Löschen, Vernichten oder jede andere Art der Handhabung von Daten mit Ausnahme des Übermittelns (Z 12) von Daten« verstanden. Unter »Übermitteln von Daten« ist gem § 4 Z 12 DSG 2000 »die Weitergabe von Daten an andere Empfänger als den Betroffenen, den Auftraggeber oder einen Dienstleister, insbesondere auch das Veröffentlichen von Daten; darüber hinaus auch die Verwendung von Daten für ein anderes Aufgabengebiet des Auftraggebers« erfasst und § 4 Z 11 DSG 2000

1250 In dieser Arbeit wird dafür auch der Begriff »Daten im engen Sinn« verwendet. Darunter versteht man in Anlehung an Art 1 lit b CCC: »[…] any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function.«

1251 In der hier verwendeten Terminologie auch als »Daten im weiten Sinn« bezeichnet.

1252 Dh es gibt zwar Wertqualifikationen in § 126a Abs 2 (»Wer durch die Tat an den Daten einen Euro 3,– 000 übersteigenden Schaden herbeiführt, ist mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bis zu 360 Tagessätzen, wer einen Euro 50,– 000 übersteigenden Schaden herbeiführt […], mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren zu bestrafen«, diese orientieren sich aber am Wiederbeschaffungs- bzw Rekonstruktionsaufwand.

1253 ZB auch Karteikärtchen, Briefe.

1254 Siehe auch *Bertel* in WK² § 126a Rz 1 (Stand Dezember 2008).

bestimmt das »Überlassen von Daten« als »die Weitergabe von Daten zwischen Auftraggeber und Dienstleister im Rahmen des Auftragsverhältnisses (Z 5)«.

Daraus lässt sich jedoch für das Strafrecht nicht viel gewinnen, da sämtliche Daten bereits mit ihrem »Input« in das System »verarbeitet« werden bzw sind. So werden Daten mit ihrer Eingabe über die Tastatur, mit dem Erfassen mittels anderer digitaler Eingabegeräte (wie Digitalkameras, Scanner usw) oder mit dem Einlesen über interne und externe Datenträger ins System bereits verarbeitet. Die ergänzende Nennung des Übermittelns oder Überlassens kann daher nur eine klarstellende Funktion haben, damit unstrittig zum Ausdruck gebracht wird, dass sämtliche Daten erfasst sein sollen, die in einer technischen Formatierung vorliegen, sodass sie elektronisch (mikroprozessorengestützt) verarbeitet werden (können).

Insgesamt kann gesagt werden, dass von der Strafnorm sämtliche Computerdaten, also »jede Darstellung von Tatsachen, Informationen oder Konzepten in einer für die Verarbeitung in einem Computersystem geeigneten Form einschließlich eines Programms, das die Ausführung einer Funktion durch ein Computersystem auslösen kann«[1255], erfasst sind.

Im Gegensatz dazu spielt diese Unterscheidung im Datenschutzrecht aber sehr wohl eine Rolle. Es werden diese Alternativen mit unterschiedlichen rechtlichen Datenverwendungskriterien verknüpft. Nicht hingegen darf mit dem Tatobjekt des § 126a der Begriff der »Datenanwendung« des § 4 Z 7 DSG 2000 in Verbindung gebracht werden. Darunter wird nämlich »die Summe der in ihrem Ablauf logisch verbundenen Verwendungsschritte (Z 8), die zur Erreichung eines inhaltlich bestimmten Ergebnisses (des Zweckes der Datenanwendung) geordnet sind und zur Gänze oder auch nur teilweise automationsunterstützt, also maschinell und programmgesteuert, erfolgen (automationsunterstützte Datenanwendung)« verstanden. Durch den Teilsatz »oder auch nur teilweise automationsunterstützt« werden selbst manuelle Datenverwendungsschritte, die ohne informationstechnologische Unterstützung verarbeitet werden, noch als automationsunterstützte Datenanwendung erachtet. Vielmehr noch legt § 58 DSG 2000 fest, dass auch manuelle Dateien, dh ohne Automationsunterstützung geführte

1255 Art 1 lit b CCC.

Dateien[1256], die in den Kompetenzbereich des Bundes fallen (iS einer Annexmaterie), als Datenanwendung zu verstehen sind.[1257] § 126a Abs 1 stellt dagegen ausschließlich auf Computerdaten ab, manuell geführte Daten werden – wie bereits erwähnt – nicht erfasst.

3. Verfügungsberechtigung

Der Täter darf über die Daten keine alleinige Verfügungsberechtigung besitzen. Dieses Tatbestandsmerkmal korrespondiert mit der geforderten »Fremdheit« der körperlichen Sache im Tatbestand der Sachbeschädigung. Eigentumsverhältnisse bezüglich des jeweiligen Datenträgers bzw des datenführenden Systems können im Bereich des § 126a lediglich Anhaltspunkte liefern. Aufgrund der Virtualität und Ubiquität von Daten geben sie keine verlässliche Auskunft über eine tatsächliche Verfügungsberechtigung des Täters über die konkreten Daten.[1258] Daher besteht auch aus Sachlichkeitsüberlegungen heraus überhaupt kein Anlass, einer Person eine »Inhaberstellung« zuweisen zu müssen[1259], vielmehr kommt es auf konkrete Zugriffs- bzw Verwendungsberechtigungen an. Werden einem Nutzer lediglich gewisse Berechtigungen (wie zB ein bloßes Leserecht) eingeräumt, um mit diversen Computerdaten zu verfahren, reicht eine Überschreitung dieser individuellen Berechtigung – zB im Fall der Löschung dieser Daten – für die Tatbestandsmäßigkeit grundsätzlich aus. Im Übrigen sind auch vom Inhalt solcher Daten betroffene Personen keine Berechtigten iSd § 126a. Ihnen kommt aber ggf ein Schutz nach den Regelungen des DSG 2000 zu.

4. Begehungsweisen

Die vier abschließend aufgezählten besonderen Handlungsmodalitäten erfassen das »Verändern«, »Löschen«, sonstige »Unbrauchbarmachen« und »Unterdrücken« von Daten. Eine Systematik lässt sich darin insoweit erkennen, als die Tathandlungen grundsätzlich zwei Kategorien der Beeinträchtigungen von Daten beschreiben, nämlich 1.) die

1256 Eine Datei ist gem § 4 Z 6 DSG 2000 eine »strukturierte Sammlung von Daten, die nach mindestens einem Suchkriterium zugänglich sind«.
1257 Vgl *Jahnel,* Handbuch, Rz 3/105.
1258 Siehe *Bergauer/Schmölzer* in Jahnel/Mader/Staudegger, IT-Recht[3], 635 (648).
1259 Siehe *Schuhr,* ZIS 2012, 441 (451).

Veränderung, Löschung (oder das Sonst-Unbrauchbarmachen) bestehender Daten[1260] durch Eingriff in deren Datensubstanz[1261] und 2.) die Unterdrückung von Daten[1262].[1263] Zu beachten ist aber, dass es sich beim »Sonst-Unbrauchbarmachen« nur um eine dem »Verändern« und »Löschen« subsidiäre (generalklauselartige) Auffangtathandlung handelt. Aus funktionaler Sicht kann eine Veränderung und Löschung von Daten nur automationsunterstützt – dh über IT-technische Maßnahmen – verursacht werden, wohingegen ein Sonst-Unbrauchbarmachen oder Unterdrücken von Daten auch durch konventionelle (manuelle) Handlungen abseits der Informationstechnik realisiert werden kann. Dass dem so ist, dafür sprechen schon die Begrifflichkeiten der Sachbeschädigung (§ 125), da dort die Tathandlungen »Zerstören«, »Beschädigen«, »Verunstalten« oder »Unbrauchbar machen« erfasst sind. Das »Verändern« ist ebenso wenig genannt, wie das »Löschen« oder »Unterdrücken«[1264]. Darüber hinaus fällt auf, dass die Tathandlungen des § 126a trotz grundsätzlicher Anlehnung des Tatbilds an die Sachbeschädigung[1265] nicht – wie in § 125 – hins ihrer gesteigerten Auswirkungen auf das Rechtsgut gereiht sind. Das weniger eingriffsintensive Verändern von Daten wird nämlich bereits vor der (unwiederbringlichen) Löschung genannt. Das Löschen sollte daher auch vor der Datenveränderung tatbestandlich positioniert werden. Der Begriff des Löschens stellt im konkreten Zusammenhang mit Computerdaten einen terminus technicus dar, der sich bei Umlegung auf den Tatbestand des § 125 im Ergebnis am ehesten mit dem »Zerstören« deckt, da die Daten nach

1260 Gemeint sind also Daten als digitale Repräsentation sämtlicher Information ebenso, wie inhaltliche Manipulationen den Informationsgehalt solcher Daten betreffend.

1261 Meines Erachtens indizieren diese drei Tathandlungen § 126a Abs 1 in diesen Begehungsweisen als ein Zustandsdelikt; aA für das »Sonst-Unbrauchbarmachen« *Triffterer* in SbgK § 126a Rz 108 (aF Stand Dezember 1992).

1262 Dabei handelt es sich idR um ein Dauerdelikt (vgl *Triffterer* in SbgK § 126a Rz 19 und 108 [aF Stand Dezember 1992]).

1263 Siehe auch *Reindl-Krauskopf,* Computerstrafrecht², 22.

1264 Das »Unterdrücken« ist aber deshalb nicht erfasst, da es hins der Unterdrückung körperlicher Gegenstände den eigenständigen Tatbestand der »Dauernden Sachentziehung« (§ 135) gibt.

1265 Siehe JAB 359 BlgNR XVII. GP, 17, wo die »verhältnismäßig weitgehende Ähnlichkeit sowohl in der äußeren Verhaltensweise als auch im Unwert« mehrfach angesprochen wird.

ihrer Löschung[1266] aufgehört haben zu existieren.[1267] So wird dies auch von den Verfassern der CCC erachtet, wenn sie ausführen: »›Deletion‹ of data is the equivalent of the destruction of a corporeal thing. It destroys them and makes them unrecognisable«.[1268]

Eine falsche Subsumtion unter die jeweilige Tathandlung des § 126a Abs 1 schadet aber strafprozessual nicht, da sämtliche Alternativen nach hM als rechtlich gleichwertig anzusehen sind[1269], was § 126a Abs 1 als alternatives Mischdelikt begreifen lässt.[1270] Eine genaue Feststellung welche Tathandlung im Einzelfall gesetzt wurde, muss daher wegen des alternativen Mischtatbestands grundsätzlich nicht erfolgen, eine Wahlfeststellung schadet – prozessual gesehen – nicht.

Nicht jede Veränderung des Datenbestands fällt unter § 126a. So ist etwa das Hinzufügen von Dateien – selbst wenn es sich dabei um ein Trojanisches Pferd (zB Keylogger) handeln sollte, das in ein fremdes Computersystem implementiert wird – dann keine Datenbeschädigung, wenn dadurch keine anderen im System vorhandenen Daten bezüglich ihrer bestimmungsgemäßen Verwendbarkeit für den Berechtigten beeinträchtigt werden. In einem solchen Fall nimmt das zusätzliche Programm neben den Daten am Zielsystem Platz, was zu keiner nachteiligen (vermögenswirksamen) Veränderung der bereits vorhandenen Daten führt, selbst wenn dadurch für den Berechtigten nicht wahrnehmbare Systemänderungen einhergehen, wie etwa die Erweiterung des Datenträgerindex um die Verweise der hinzugefügten Programme bzw Dateien.[1271] Die Grenze ist aber dort zu ziehen, wo durch das Hinzufügen von Daten zB die Oberflächengestaltung eines Programms beeinträchtigt wird. Man denke an das »Hacking von Websites«, bei dem einzelne Webseiten grafisch bzw inhaltlich so verändert wurden, dass der Zugriff des Hackers für alle Besucher dieses Internetauftritts erkenntlich ist (sog »Defacements«). Es kommt jedenfalls

1266 Siehe dazu gleich im Anschluss.

1267 Eine solche Interpretationsanleihe ist auch zulässig, denn man sollte in diesem Zusammenhang nicht übersehen, dass mit § 126a nicht eine von Grund auf neue Form der »Datenbeschädigungsdogmatik« indiziert ist, da der Gesetzgeber mit seiner Einführung, lediglich auf eine neue Form des Tatobjekts (arg »unkörperliche Sache«) – aber in Anlehnung an die klassische Sachbeschädigung – reagiert hat.

1268 Vgl ER (ETS 185) Pkt 61.

1269 Siehe aber krit dazu die Ausführungen unten (S 270 ff).

1270 Vgl *Triffterer* in SbgK § 126a Rz 65 (aF Stand Dezember 1992); *Komenda/Madl* in SbgK § 126a Rz 38; *Birklbauer/Hilf/Tipold,* Strafrecht BT I[2] § 126a Rz 8.

1271 Siehe auch *Bergauer,* Malware, 174; vgl auch *Komenda/Madl* in SbgK § 126a Rz 44.

darauf an, dass Daten (einschließlich Programme) bezüglich ihres Vermögenswertes (iS eines Tausch-, Gebrauchs- bzw aber auch Affektionswerts) nachteilig verändert werden müssen.[1272] Durch die Tathandlung muss grundsätzlich ein Schaden unmittelbar an den Daten selbst verursacht worden sein.[1273] Es reicht dabei aus, dass der Berechtigte seine Daten (zumindest über einen nicht ganz bedeutungslosen Zeitraum hinweg) nicht mehr bestimmungsgemäß verwenden kann.[1274] Mittelbare Schäden bleiben außer Betracht.[1275]

a. Verändern

Unter dem »Verändern« von Daten – wobei Daten im deliktsspezifischen Zusammenhang und nach dem weiten strafrechtlichen Verständnis sowohl Daten, Datensätze und Dateien sowie Computerprogramme sein können – versteht man einerseits das Hinzufügen von neuen Zeichen, Datensätzen bzw Inhalten[1276] oder technischen Elementen (zB interne Verweisungen[1277]) zu einer Datei, andererseits aber auch das Entfernen von Teilinhalten.[1278] In beiden Fällen sind Daten substanziell verändert worden, da ihr Informationswert nunmehr ein abgeänderter ist, was darauf hinweist, dass diese Tathandlung rein auf »inhaltliche Veränderungen« abstellt[1279], wie das Beispiel der sog »Website-Defacements« zeigt, bei denen Inhalte von Websites öffentlichkeitswirksam verändert werden.[1280] Eine solche Interpretation der Tathandlung des »Veränderns« bietet sich schon allein deshalb an, um den Begriff vom allgemeinen, sozial unschädlichen Bearbeiten von Daten abzugrenzen. In der Informationstechnologie führt jedes Ausführen von Programmen oder Bearbeiten von Dateien zwangsläufig zu »Veränderungen« des Datenbestands bzw der Datenintegrität.[1281] Der Tatbestand der Datenbe-

---

1272 Siehe *Fuchs/Reindl-Krauskopf,* BT I[4], 140; weiters *Birklbauer/Hilf/Tipold,* Strafrecht BT I[2] § 126a Rz 10 f; vgl weiters *Schmölzer,* ZStW 2011/123, 709 (723).

1273 Konkret betrifft dies aber bloß die Tathandlungen des Veränderns, Löschens und sonst Unbrauchbarmachens.

1274 Siehe etwa idS *Leukauf/Steininger,* StGB[3] § 126a Rz 13.

1275 Siehe anstatt vieler *Bertel* in WK[2] § 126a Rz 5.

1276 Nicht aber das Hinzufügen neuer Daten selbst, ohne auf bestehende Daten einzuwirken.

1277 Vgl auch *Birklbauer/Hilf/Tipold,* Strafrecht BT I[2] § 126a Rz 6.

1278 IdS *Triffterer* in SbgK § 126a Rz 66 (aF Stand Dezember 1992).

1279 So wohl auch *Kienapfel,* BT II[3] § 126a Rz 18.

1280 Vgl *Winterer,* Windows, 52 ff.

1281 Vgl auch *Schuhr,* ZIS 2012, 441 (448).

schädigung kann daher kein Verbot solcher sozial adäquater Verhaltensweisen normieren, sondern ausschließlich eines für nachteilige[1282] (negative[1283]) Manipulationen. Dies lässt sich aber für § 126a Abs 1 auch aus dem Erfordernis eines (unmittelbaren) Schadens ableiten, weshalb nur Verhaltensweisen mit schädigendem Charakter von den beschriebenen Tathandlungen erfasst sein können.

Nicht angebracht ist mE die von *Triffterer* idZ verwendete Wendung »also die Fälschung einer Datei bzw eines Programms«.[1284] Dies ist irreführend, da eine »Fälschung« prinzipiell das originäre Herstellen neuer Daten indiziert[1285], was in unserem Fall aber keine tatbestandsmäßige Handlung darstellt, solange durch das Hinzufügen neuer Daten keine bestehenden Datensätze beeinträchtigt werden. Von einem »Verfälschen« könnte hingegen schon gesprochen werden, da dabei der Inhalt von ursprünglich echten Daten nachträglich geändert wird.[1286]

Eine Veränderung von Daten iSd § 126a Abs 1 muss stets einen negativen (vermögenswerten) Charakter aufweisen und sich unmittelbar an bereits vorhandenen Daten auswirken. Sie kann nur in automationsunterstützter Form durchgeführt werden. Durch die Veränderung muss die Gebrauchsfähigkeit dieser Daten derart beeinträchtigt werden, dass sie für den Berechtigten faktisch unbrauchbar sind. Dies ergibt sich bereits aus der Wortinterpretation iZm der Auffangtathandlung des »Sonst«-Unbrauchbarmachens. Das Verändern und Löschen sind nämlich Beispielsfälle des Unbrauchbarmachens.[1287] Wobei das sonstige Unbrauchbarmachen von Daten – anders als das Verändern und Löschen – auch auf konventionellem Weg, zB durch Zerstörung des körperlichen Datenträgers, realisiert werden kann. Dass die beeinträchtigten Daten grundsätzlich einen Vermögenswert aufweisen müssen, ergibt sich zudem – neben der systematischen Einordnung des Delikts bei den Vermögensdelikten – aus der Formulierung »dadurch schädigt, daß«.[1288] Manipulationen zB des Betriebssystems[1289], die das

1282 Siehe auch *Reindl-Krauskopf,* Computerstrafrecht², 22.

1283 Siehe dazu ausdrücklich ER (ETS 185) Pkt 61, wo von »[…] a negative alteration of the integrity or of information content of data and programmes« gesprochen wird.

1284 Vgl *Triffterer* in SbgK § 126a Rz 66 (aF Stand Dezember 1992).

1285 Vgl OGH 23. 04. 2007, 15 Os 6/07g.

1286 Vgl OGH 23. 04. 2007, 15 Os 6/07g.

1287 Siehe *Bertel* in WK² § 126a Rz 3.

1288 Vgl etwa *Kienapfel,* BT II³ § 126a Rz 22 f.

1289 ZB sind das Aktivieren von zusätzlichen Funktionen des Betriebssystems oder das Verändern von Systemeinstellungen (Uhrzeit, Ansichten, Bildschirmschoner etc) – ohne Zustimmung des Nutzers bzw Verfügungsberechtigten – nicht erfasst.

Opfer nicht merklich schädigen bzw das Computersystem nicht nachteilig verändern, werden idR nicht erfasst.

b. Löschen

Das »Löschen« von Daten führt nach hM zu deren Zerstörung[1290] bzw Vernichtung[1291]. Das tatbestandliche Löschen erfordert aber mE einen automationsunterstützten Eingriff, da die Begrifflichkeit »löschen« einen informationstechnischen terminus technicus darstellt, der einen vordefinierten, technikgesteuerten Löschvorgang beschreibt. Man »löscht« auch nicht den Text aus einem Buch, indem man die Seiten verbrennt, sondern man vernichtet oder zerstört die Seite.[1292] Das Löschen elektronischer Daten ist daher – trotz seiner ergebnisbezogenen Ähnlichkeit – vom »Zerstören« oder »Vernichten« (körperlicher Sachen) zu unterscheiden. Das Zerstören eines (körperlichen) Datenträgers stellt kein programmspezifisches Löschen von Daten dar, selbst wenn der Datenbestand dadurch »unbrauchbar« gemacht wird. Folglich müssen solche Fälle unter die Auffangtathandlung des Sonst-Unbrauchbarmachens des § 126a Abs 1 subsumiert werden.

Im Zusammenhang mit dem Löschen ist prinzipiell zwischen dem physischen und logischen Löschen zu differenzieren. Während das physische Löschen die Daten physikalisch unwiederbringbar entfernt, wird beim logischen Löschen (vorerst) lediglich der Zugriff auf die Daten durch programmtechnische Maßnahmen verhindert.[1293] Genauer gesagt, werden nur die Daten(verweise) aus dem Datenträgerindex entfernt, was zur Folge hat, dass das Betriebssystem die konkreten Speicherbereiche am Datenträger wieder neu vergeben kann.[1294] Faktisch wird lediglich die Datenorganisation derart verändert, dass kein »gezielter Zugriff« mehr auf die betreffenden Daten möglich ist.[1295] Erst wenn diese – vom System freigegebenen – Speicherbereiche tatsächlich mit neuen Daten überschrieben werden, sind die – bis dahin nur als »ge-

---

1290 Vgl *Birklbauer/Hilf/Tipold,* Strafrecht BT I² § 126a Rz 7.

1291 Vgl *Triffterer* in SbgK § 126a Rz 66 (aF Stand Dezember 1992).

1292 Vgl dazu die Begrifflichkeiten und Überlegungen zur Sachbeschädigung bei körperlichen Sachen im einschlägigen Schrifttum.

1293 Siehe auch *Triffterer* in SbgK § 126a Rz 67 (aF Stand Dezember 1992).

1294 Dies gilt für eine einfache Datenträgerformatierung, bei der nur das – einfach ausgedrückt – »Inhaltsverzeichnis« gelöscht wird.

1295 Vgl dazu etwa RIS-Justiz RS0125838 mwN.

löscht markierten« – Daten prinzipiell physisch nicht mehr vorhanden. Solange die Speicherbereiche jedoch noch nicht überschrieben wurden, sind die entfernten Datenzuordnungen im Datenträgerverzeichnis hingegen grundsätzlich rekonstruierbar. Die Besonderheit der technischen Unterscheidung von logischem und physischem Löschen begründet sich in der Ubiquität und verlustfreien Reproduktionsmöglichkeit elektronischer Daten (Original und Kopie sind faktisch ident). Man beachte aber, dass das Verschieben von Daten in einen vom jeweiligen Betriebssystem unterstützten »Papierkorb« noch eine Vorstufe zum logischen Löschen darstellt, da die Speicherbereiche tatsächlich erst – im Gegensatz zum typischen logischen Löschvorgang – nach Ablauf einer definierbaren Frist zur Weiterverwendung für das Betriebssystem freigegeben werden. Mit anderen Worten, eine in den Papierkorb verschobene Datei wird erst nach Ablauf einer bestimmten bzw bestimmbaren Frist logisch gelöscht und erst bei tatsächlichem Überschreiben der entsprechenden Speicherbereiche physikalisch entfernt.[1296]

Das logische Löschen ist daher kein Löschen im eigentlichen Sinn[1297], da es sich dabei nur um ein Vorstadium zu einer physischen Löschung handelt. Die konkrete Tathandlung des »Löschens« stellt jedoch begrifflich sowie abgrenzungstechnisch sinnvoll und in Bezugnahme auf die korrespondierende Tathandlung des § 125 »Zerstören« auf die unwiderrufliche Vernichtung der Daten ab.[1298]

Darüber hinaus verlangt der Tatbestand, dass der Schaden unmittelbar durch die genannten Tathandlungen an den Daten eintritt, was sich bereits aus der Formulierung »[…] dadurch schädigt, daß er Daten […] löscht […]« ergibt.[1299] Durch den logischen Löschvorgang befinden sich die Daten aber physikalisch noch am Datenträger. Nur sind sie für

1296 Zur besseren Veranschaulichung des logischen Löschens in der virtuellen Welt des Computers könnte ein Beispiel aus der analogen Welt herangezogen werden, das vergleichbare Ergebnisse zur Schau stellt: Der Täter wirft ein fremdes Buch in den Altpapiercontainer, um es zu entsorgen. Zu diesem Zeitpunkt ist das Buch aber (noch) nicht beschädigt oder zerstört, sondern bloß unterdrückt bzw dauerhaft entzogen. Die vollständige Zerstörung wird erst später durch die Müllpresse udgl faktisch vollzogen, eine Sachbeschädigung iSd § 125 liegt daher zum Tatzeitpunkt nicht vor, ggf aber eine dauernde Sachentziehung (§ 136).

1297 Siehe dazu auch RIS-Justiz RS0125838 mwN.

1298 Siehe auch den ER (ETS 185) Pkt 61, wo iZm dem Löschen von Daten erklärt wird: »It destroys them and makes them unrecognisable«.

1299 Vgl zur Unmittelbarkeit auch *Triffterer* in SbgK § 126a Rz 84 (aF Stand Dezember 1992).

den Berechtigten im Rahmen der gewöhnlichen Systemnutzung nicht mehr verwendbar. Wohl aber sind sie unmittelbar durch die Tathandlung des »logischen Löschens« »unbrauchbar« bzw ggf auch »unterdrückt«.[1300] *Kienapfel* ordnet daher das »logische Vernichten« sachwidrig der Tathandlung des Löschens zu. Er erklärt aber gleich anschließend, dass die Daten dabei unwiederbringlich verloren sein müssen[1301], was gerade im Fall des logischen Löschens einen Widerspruch darstellt. Diese Aussage kann aus einer entsprechenden ergebnisorientierten ex post-Betrachtung heraus nur dann schlüssig sein, wenn man die Ergebnisse der logischen und physischen Datenlöschung erst ab dem Zeitpunkt miteinander vergleicht, zu dem die durch das logische Löschen freigegebenen Speicherplätze tatsächlich überschrieben wurden und somit die Daten auch physisch gelöscht sind. Die Ergebnisse sind wohl früher[1302] oder später[1303] ident, die (Tat-)Handlungen aber verschieden. Beim logischen Löschen hat der Täter durch seine Handlung die Daten nämlich weder unmittelbar noch unwiederbringlich vom Datenträger beseitigt, da sie dort faktisch weiterhin vorhanden sind. Daher gilt: Werden fremde Daten softwaregestützt – etwa über einen Löschbefehl des Betriebssystems – vom Täter »gelöscht«, liegt in Wahrheit gar keine Löschung vor, da sich die Daten auch nach Ausführung dieses Befehls (vorerst) weiterhin am Datenträger befinden und sich nur ihre Organisation geändert hat. Das tatbestandliche »Löschen« iSd § 126a Abs 1 stellt dagegen mE ausschließlich auf eine tatsächliche dauerhafte und unwiderrufliche Datenentfernung ab, die unmittelbar durch die Handlung realisiert werden muss. Das logische Löschen führt erst dann zu einer solchen, wenn die Speicherbereiche tatsächlich überschrieben wurden, womit es an der Unmittelbarkeit fehlt. Demzufolge beschreibt das logische Löschen nur ein Zwischenstadium vom computersystemspezifischen Löschbefehl (Entfernung des Verzeichniseintrags im Datenträgerindex) bis zum faktischen Überschreiben der Speicherbereiche durch neue Daten durch das Betriebssystem und daher unmittelbar nur eine Zugriffsverhinderung für den Berechtigten auf die Daten.[1304]

1300 AA *Birklbauer/Hilf/Tipold,* Strafrecht BT I² § 126a Rz 7; aA *Kienapfel,* BT II³ § 126a Rz 19.

1301 Vgl *Kienapfel,* BT II³ § 126a Rz 19.

1302 Vgl physische Löschung.

1303 Vgl logische Löschung.

1304 In diese Richtung wohl auch *Komenda/Madl* in SbgK § 126a Rz 45.

c. Unbrauchbarmachen

Ob nun aber für das logische Löschen ein Sonst-Unbrauchbarmachen, welches subsidiär zum Verändern und Löschen im Fall einer bloßen logischen Löschung in Betracht kommt oder ein tatbestandlicher »Hauptfall« des Unterdrückens, hängt davon ab, ob man die Dateiverweise im jeweiligen Datenträgerindex den Bezug habenden Daten zuordnet oder nicht. Aus technischer Sicht werden diese Verweisungen vom Betriebssystem angelegt und verwaltet. Die Einträge referenzieren lediglich auf die Speicherbereiche der jeweiligen Datei, weshalb man sie auch mit Hyperlinks[1305] vergleichen könnte, die inhaltlich zwar in keiner Weise mit den verwiesenen Daten in Verbindung stehen, aber für den Gebrauch dieser Daten unabdingbar sind, andernfalls die Daten vom System unter normalen Bedingungen nicht mehr bestimmungsgemäß verarbeitet werden können. Entfernt man daher die Verweisungen, können sie vom Nutzer bzw Berechtigten nicht mehr zweckbestimmt genutzt werden, obwohl die Daten physisch am Datenträger erhalten sind. Es kann daher iSd Dogmatik zur »Sachbeschädigung durch Unbrauchbarmachen« argumentiert werden, dass es für die Tatbestandsmäßigkeit ausreichend ist, »wenn allein die bestimmungsgemäße Brauchbarkeit einer Sache nicht unwesentlich eingeschränkt wurde«.[1306] Die Entfernung von Einträgen aus dem Datenträgerindex wirkt sich massiv auf die Verwendbarkeit der entsprechenden Daten aus, da die Verzeichniseinträge in einem engen »sachlichen« Zusammenhang mit der technischen Nutzbarkeit von Daten stehen.

Es liegt daher hins der relevanten Daten ein Unbrauchbarmachen vor, das subsidiär zum Verändern und Löschen als Auffangtathandlung zu sehen ist.[1307] Kommt man zum Ergebnis, dass in einem solchen Fall auch ein »Unterdrücken«[1308] vorliegt, da dem Berechtigten der Zugriff auf seine Daten mit deren logischer Löschung unmittelbar entzogen ist, so würde das Unbrauchbarmachen in Form einer Datenunterdrückung als konkrete »Spezialtathandlung« vorgehen. Dies ist damit zu

---

1305 Verweisungen auf Dokumente im Internet (siehe *Balzert,* Lehrbuch², 51 und 67).

1306 Vgl etwa *Seiler* in SbgK § 125 Rz 40.

1307 Dogmatisch betrachtet kann der Unterschied folgend verdeutlicht werden: In Anbetracht der Tathandlung des Löschens liegt zum Tatzeitpunkt des »logischen Löschens« bloß ein Versuch vor, die Tathandlung des Unbrauchbarmachens führt aber im Tatzeitpunkt bereits zur Vollendung.

1308 Zur Tathandlung der »Unterdrückung« siehe gleich im Anschluss.

begründen, dass das Sonst-Unbrauchbarmachen nur gegenüber den Tathandlungen des Veränderns und Löschens subsidiär ist, und daher im Fall der Anwendbarkeit im gleichen Rang wie die Datenunterdrückung steht.[1309] Die Tathandlung des Sonst-Unbrauchbarmachens ist allerdings im Fall des logischen Löschens der Datenunterdrückung vorzuziehen.

Das Sonst-Unbrauchbarmachen muss sich jedenfalls – wie das Verändern und Löschen – auf die Datensubstanz selbst beziehen.[1310] Dies muss zur Folge haben, dass diese »Daten in ihrer Gebrauchsfähigkeit so weit beeinträchtigt werden, dass sie ihren Zweck nicht mehr erfüllen können«.[1311] Insoweit könnte man beim Sonst-Unbrauchbarmachen – neben konventionellen Handlungen – auch von einer »technischen« Datenveränderung sprechen, im Gegensatz zur Tathandlung des Veränderns, wo es auf eine »inhaltliche Datenveränderung« ankommt. Eine technische Veränderung von Daten liegt vor, wenn zB Meta-Daten einer Datei manipuliert werden, sodass diese nicht mehr automationsunterstützt verwendet werden kann (zB das logische Löschen, die Änderung der Dateierweiterung[1312], Veränderung der »Header-Dateien«[1313] bzw »Datei-Header«[1314]), obwohl die Inhalte der Daten selbst unverändert bleiben. Dieses funktionale Kriterium kann daher auch zur Abgrenzung dieser beiden Tathandlungen herangezogen werden.[1315]

Dasselbe gilt im Übrigen ebenso für permanente (sog »Read-Only«) Speichermedien (CD-ROM, DVD-ROM[1316] etc), bei denen eine programmgesteuerte Veränderung des Dateninhalts (einschließlich der Löschung) technisch nicht möglich ist.[1317] Solche Datenträger müssten

---

1309 AA *Kienapfel,* BT II[3] § 126a Rz 20.

1310 Ein Tangieren der Datensubstanz bzw des Informationswertes bezüglich des bestimmungsgemäßen Gebrauchs reicht aber bereits aus.

1311 Vgl *Birklbauer/Hilf/Tipold,* Strafrecht BT I[2] § 126a Rz 8.

1312 Auch Dateiendung oder »Extension« genannt; es handelt sich um einen normalen Bestandteil des Dateinamens (siehe *Kersken,* IT-Handbuch[5], 311).

1313 Eine Header-Datei wird insbesondere bei der Programmiersprache »C« bzw »C++« verwendet. Darin werden die Schnittstellen von vordefinierten Bibliotheksdateien definiert, die in ein Programm eingebunden werden (vgl *Kersken,* IT-Handbuch[5], 479; weiters *Balzert,* Lehrbuch[2], 834).

1314 Darunter versteht man äußere Zusatzinformationen (auch Meta-Daten oder Kopfdaten) einer Datei.

1315 In diesem Sinne wohl auch *Triffterer* in SbgK § 126a Rz 70 (aF Stand Dezember 1992).

1316 Siehe *Kersken,* IT-Handbuch[5], 154.

1317 Vgl etwa *Korge,* Die Beschlagnahme elektronisch gespeicherter Daten bei privaten Trägern von Berufsgeheimnissen (2009) 14 f.

physisch zerstört werden, damit die darauf gespeicherten Daten beseitigt werden können. Doch beim Zerstören bzw Beschädigen des Datenträgers – zB durch Zerkratzen oder Zerschneiden des optischen Massenspeichers – werden die Daten ebenfalls nicht physisch gelöscht, sondern (sonst) unbrauchbar gemacht bzw unterdrückt. Nur jene Speicherbereiche des Datenträgers, die unmittelbar von der Beschädigung betroffen sind (iS etwa der Zerstörung der reflektierenden Einbohrungen in der Metalloberfläche, welche das Bitmuster der Daten abbilden), können prinzipiell vom Laserstrahl nicht mehr ordnungsgemäß abgetastet werden. Da nunmehr Datenteile für die programmtechnische Ausführung fehlen, sind die Daten an sich für den gewöhnlichen Nutzer »unbrauchbar«, weil zumindest Datenteile (physisch) mitzerstört wurden. Daher gilt: Wird ein Datenträger physisch beschädigt, muss das nicht auch für den Datenbestand gelten. Sind die relevanten Daten nicht von der Hardware-Schädigung[1318] betroffen, sind sie bloß »unterdrückt«, wohingegen sie bei einer teilweisen Beschädigung »sonst unbrauchbar gemacht« wurden.

d. Datenunterdrückung

Unter dem »Unterdrücken« von Daten versteht man generell die dauernde oder auch nur vorübergehende Zugriffsverhinderung.[1319] Erfasst ist daher primär nicht die Einwirkung auf das Tatobjekt selbst, sondern nur dessen Vorenthaltung. Die Datenunterdrückung wurde wohl als (ungleiches) Pendant zur »Dauernden Sachentziehung« (§ 135) in § 126a miterfasst, denn in der Sachbeschädigung (§§ 125 f) findet eine reine Unterdrückungsalternative keine Entsprechung. Gleichwohl ist eine »dauernde« Unterdrückung der Daten – anders als iSd § 135, wo verlangt wird, dass der Berechtigte nach objektiven Kriterien mit der Wiedererlangung nicht mehr rechnen kann[1320] bzw die Sache für immer verloren ist – nicht gefordert. Auch eine zeitweilige Verhinderung des Zugriffs auf die Daten, die für einen vernünftig denkenden Menschen ins Gewicht fällt, reicht für die Tatbestandsmäßigkeit nach hM aus.[1321]

1318 § 125 wäre hierfür anwendbar; siehe auch *Reindl,* E-Commerce, 130.

1319 Vgl *Kienapfel,* BT II³ § 126a Rz 21; weiters *Triffterer* in SbgK § 126a Rz 71 (aF Stand Dezember 1992).

1320 Vgl anstatt vieler *Birklbauer/Hilf/Tipold,* Strafrecht BT I² § 135 Rz 9.

1321 Vgl auch *Kienapfel,* BT II³ § 126a Rz 21; weiters *Triffterer* in SbgK § 126a Rz 71 (aF Stand Dezember 1992).

Das ist insofern interessant, als in den GMat bezüglich des § 135 noch angemerkt wurde, dass, abgesehen von eigens gesetzlich geregelten Spezialtatbeständen (zB der unbefugte Gebrauch von Fahrzeugen gem § 136), eine bloß vorübergehende Entziehung einer Sache keiner kriminellen Strafe bedürfe.[1322] Daher wird faktisch das temporäre Unterdrücken von Daten, nicht aber das temporäre Unterdrücken bzw Entziehen einer körperlichen Sache, als strafwürdig erachtet. Dieses Ergebnis erscheint allerdings mehr als fragwürdig, da das Tatobjekt »Computerdaten« (§ 126a) für den Gesetzgeber offenbar schutzwürdiger erscheint als ein Tatobjekt »körperlicher Konsistenz« (§§ 125 bzw 135). Dies ließe sich wohl am ehesten mit dem zusätzlichen hinter der Datenbeschädigung stehenden Rechtsgut des »Interesses am Fortbestand und der Verfügbarkeit von Daten« erklären, da sich dieses ideelle Schutzgut ausdrücklich auch auf die »Verfügbarkeit« von Daten erstreckt.

Doch auch für eine Datenunterdrückung nach § 126a Abs 1 wird die Grenze zur Strafbarkeit bei einem äußerst kurzfristigen Vorenthalten der Daten noch nicht überschritten sein, man denke etwa an bestimmte Formen des »Zeitdiebstahls«, bei denen jemand unbefugt einen fremden Computer nutzt, um zB die eigenen E-Mails über das Internet abzufragen.[1323] Wenn der Systeminhaber durch diesen unbefugten Nutzer nun daran gehindert wird, während dessen E-Mail-Abfrage auf seine Daten bzw das System selbst zuzugreifen, liegt noch keine tatbildliche Datenunterdrückung vor.

Im Schrifttum wird für diese Tathandlung überwiegend eine Interpretationsanleihe bei der Urkundenunterdrückung gem § 229 Abs 1 genommen[1324], wo unter dem Unterdrücken »jede (vorsätzliche) Handlung anzusehen [ist], die die Urkunde zwar unversehrt erhält, den Berechtigten jedoch um die Möglichkeit bringt, sich ihrer zu bedienen«.[1325] Wesentlich ist iZm der Urkundenunterdrückung (§ 229 Abs 1), dass ihr Tatobjekt nur eine Urkunde sein kann, deren bestehender Gedankeninhalt unversehrt ist.[1326] Dies ist aber freilich nur für den Fall der Urkundenunterdrückung unerlässlich, da zwangsläufig eine unverfälschte

1322 Vgl ErlRV 30 BlgNR XIII. GP, 283.
1323 Siehe idS auch *Triffterer* in SbgK § 126a Rz 72 (aF Stand Dezember 1992); vgl auch *Komenda/Madl* in SbgK § 126a Rz 47.
1324 Vgl etwa *Reindl,* E-Commerce, 104; *Kienapfel,* BT II³ § 126a Rz 21.
1325 Siehe statt vieler RIS-Justiz RS0095694.
1326 Siehe RIS-Justiz RS0095639.

Urkunde vorliegen muss, die in ihrer Beweisfunktion gerade nicht beeinträchtigt wurde.

Angesichts der Zielausrichtung des § 126a spielt aber eine solche Eigenschaft keine Rolle, ist doch der Datenbegriff – wie oben ausgeführt – sehr weitreichend und jedenfalls auch unabhängig von Gedankeninhalten und daher abstrakter zu verstehen. Darüber hinaus wurde in den GMat iZm der Einführung der Datenfälschung (§ 225a) durch das StRÄG 2002 ausdrücklich darauf hingewiesen, dass die Schaffung eines »§ 229a« (»Datenunterdrückung«) als Pendant zu § 229 (»Urkundenunterdrückung«) vorerst nicht geplant sei.[1327]

Für eine Datenunterdrückung iSd § 126a ist es daher grundsätzlich[1328] nicht erforderlich, auf (besondere) Inhalte – wie insb etwa Kriterien »urkundenähnlicher« Daten (iSd § 225a) – abzustellen. Auch in Anbetracht des technologischen Umfelds wäre es gar nicht sachgerecht, den Erhalt der absoluten Datenintegrität während deren Unterdrückung zu verlangen. Ein solches Erfordernis wäre nach hM wohl schon deshalb abzulehnen, da das Unterdrücken eine den übrigen Tathandlungen vollkommen gleichwertige Handlung sein soll.[1329]

Die Tathandlung des Unterdrückens in § 126a Abs 1 verlangt – im Gegensatz zu den anderen Alternativen – keinen Eingriff in die Datensubstanz, sondern beschränkt sich darauf, die Verwendungsmöglichkeit der Daten für den Berechtigten zu verhindern. Dies bedeutet aber nicht e contrario, dass kein Eingriff in die Datensubstanz vorliegen darf. Die Daten dürfen lediglich physisch nicht dauerhaft geschädigt oder gelöscht werden. Meines Erachtens ist es für ein Unterdrücken

---

1327 Vgl 1166 BlgNR XXI. GP, 31; dies gilt aber auch für die Beweismittelunterdrückung (§ 295): Werden Daten, die zur Verwendung in einem gerichtlichen oder verwaltungsbehördlichen Verfahren oder in einem Ermittlungsverfahren nach der StPO bestimmt sind und über die der Täter nicht oder nicht allein verfügungsberechtigt ist, »vernichtet, beschädigt oder unterdrückt«, so ist daher mangels eines eigenen Datenunterdrückungstatbestands, § 295 neben § 126a (in echter Konkurrenz) anzuwenden (vgl *Plöchl/Seidl* in WK² § 295 Rz 27 [Stand September 2010]).

1328 Man beachte allerdings, dass es im Bereich der virtuellen Kriminalität auch Erscheinungsformen einer Datenunterdrückung gibt, wo die Daten ieS beim Berechtigten verbleiben, diesem allerdings die Zugriffsmöglichkeit auf die Information (Daten iwS) durch zB »Ransomware« (siehe unten) entzogen wurde. Daher ist im deliktsspezifischen Zusammenhang der Datenbeschädigung auch von Daten iS eines höheren Abstraktionsgrad auszugehen. Es ist die technische Repräsentation der Information (Daten ieS), wie auch die technisch verarbeitete Information selbst (Daten iwS) als Tatobjekt des § 126a erfasst.

1329 Siehe aber krit dazu S 270 ff.

von elektronischen Daten nur erforderlich, dass der originäre Informationswert letztlich – nach Aufhebung der automationsunterstützten oder nicht automationsunterstützten Zugriffsblockade – wieder vollständig herstellbar sein muss. Andernfalls wären die Daten bereits »verändert« oder »sonst unbrauchbar«. Aufgrund der Ubiquität und Virtualität elektronischer Daten ist es wohl unbeachtlich, ob die Daten bzw ihre technische Verarbeitungsform während der Unterdrückung verändert werden oder nicht. Vielmehr sind alle Handlungen denkbar, die dazu geeignet sind den Berechtigten über einen kurz oder lang andauernden Zeitraum um die Möglichkeit der Datenverwendung zu bringen. Es spielt ebenfalls keine Rolle, ob der Berechtigte die Daten in dieser Zeit tatsächlich auch bestimmungsgemäß benützen wollte. Insbesondere ist dabei an die Beispiele des logischen Löschens, der Verschlüsselung von Dateien, das programmtechnische Verstecken von Dateien durch Dateiattribute oder die Zugriffsverhinderung durch Implementierung eines Passwortschutzes durch den Täter – zB mittels sog »Ransomware«[1330] – zu denken.[1331] Durch eine Verschlüsselung aber werden die in binärer Darstellungsform vorliegenden »Klartext«[1332]-Daten in Chiffre-Daten[1333] umgewandelt[1334], die nur mit dem entsprechenden Schlüssel wieder dechiffriert werden können, um den Informationswert der Daten wieder herzustellen. Der Inhalt der Daten wird dabei prinzipiell verändert, weshalb auch eine Datenveränderung vorliegen kann. Bei der Implementierung eines Passwortschutzes in eine Datei, muss dies jedoch nicht unbedingt der Fall sein. Aber auch hierbei werden zumindest Meta-Daten dieser Datei verändert.

Eine Datenunterdrückung ist nicht ausschließlich über eine IT-Manipulation – wie es gezwungener Maßen beim Verändern oder Löschen der Fall sein muss – realisierbar.[1335] Vielmehr führt auch das faktische

---

1330 Es handelt sich dabei um einen speziellen Unterfall der Malware, wodurch Daten des Opfers verschlüsselt werden und der Täter in weiterer Folge meist ein »Lösegeld« für die Freischaltung fordert (siehe dazu etwa *Borges/Schwenk/Stuckenberg/Wegener,* Identitätsdiebstahl, 100 f; weiters *Winterer,* Windows, 156 f).

1331 Vgl auch *Reindl-Krauskopf,* Computerstrafrecht², 22.

1332 Der technische Begriff des »Klartexts« bezieht sich hier auf die noch unverschlüsselte Darstellungsform. Er ist insoweit verwirrend, als freilich auch die Binärdarstellung selbst für den Menschen unverständlich ist.

1333 Auch »Geheimtext« genannt.

1334 Durch sog »Substitution« (Ersetzen von Zeichen) oder »Transposition« (Vertauschung von Zeichen) vgl *Wobst,* Kryptologie, 31 bzw 36.

1335 Wobei aber wie eingangs festgestellt solche Handlungen nicht unter die hier vertretene Auffassung von »Computerkriminalität« fallen.

Entziehen des körperlichen Datenträgers zu einer Unterdrückung der darauf gespeicherten Daten. Daher kann bei einer dauernden Entziehung des Datenträgers § 126a mit § 135 ebenso (echt) konkurrieren, wie mit § 125 im Falle einer Beschädigung des Datenträgers.[1336]

Wichtig ist aber mE anzumerken, dass insb ein Löschen oder Unbrauchbarmachen von Daten keine Datenunterdrückung im engeren Sinn impliziert, obwohl der Berechtige über gelöschte Daten ebenfalls nicht mehr verfügen kann. Daher gehen diese Handlungen ggf stets als die spezielleren Tathandlungen vor.[1337] Bei einer Unterdrückung ist nicht die Beschädigung oder Vernichtung der Daten intendiert, sondern es geht dem Täter darum, dem Berechtigten die Daten vorzuenthalten. Richtig ist, dass aus Sicht des Berechtigten die Daten im Zeitraum ihrer programmtechnischen Unterdrückung, bei der der Berechtigte weiterhin in Besitz bzw Verfügungsberechtigung[1338] derselben bleibt (zB beim logischen Löschen, der Verschlüsselung oder des Versehens mit einem Passwort), faktisch »unbrauchbar« sind, wobei im Fall einer Datenverschlüsselung oder eines Passwortschutzes bezüglich einzelner Dateien auch die Tathandlung des »Veränderns« prinzipiell in Betracht kommt. Das sonstige Unbrauchbarmachen ist hier lediglich gegenüber den Tathandlungen des Veränderns und Löschens subsidiär und tritt nicht auch hinter eine Datenunterdrückung zurück.[1339] Dies ergibt sich mE aus folgenden Überlegungen:

Zum einen wurde der Tatbestand der Datenbeschädigung (§ 126a) als Pendant zu dem der Sachbeschädigung (§ 125) eingeführt, wobei in Letzterem auf eine Unterdrückungstathandlung verzichtet wurde. In den einschlägigen GMat[1340] finden sich jedenfalls keine Erl zur Handlungsweise der Datenunterdrückung. Zum anderen lässt auch die Deliktsbezeichnung »Datenbeschädigung« darauf schließen, dass lediglich Schädigungen an den Daten erfasst sein sollen, dh die »Verletzung

1336 Vgl auch prinzipiell *Reindl,* E-Commerce, 104; weiters *Birklbauer/Hilf/Tipold,* Strafrecht BT I² § 126a Rz 16.

1337 Siehe zur Konsequenz gleich im Anschluss.

1338 Gemeint ist an dieser Stelle die faktische Verwendungsmöglichkeit der Daten als Repräsentation der Information, wobei über die Information selbst nicht verfügt bzw nicht darauf zugegriffen werden kann. Dem berechtigten Inhaber fehlt durch die Verschlüsselung die Bezug habende Interpretationskonvention zur Abstraktion der repräsentierten Information aus den verschlüsselten Daten.

1339 AA *Kienapfel,* BT II³ § 126a 20, der die Datenunterdrückung als dogmatisch vorrangig erachtet.

1340 Vgl IA 2/A XVII. GP, 77 ff; JAB 359 BlgNR XVII. GP, 17.

der Datenintegrität«. Die Namensgebung orientierte sich nämlich gerade an dem von der Sachbeschädigung her geläufigen Wort »Beschädigung«.[1341]

Diese Argumente zusammenfassend kann darauf geschlossen werden, dass zuerst geprüft werden muss, ob die Daten iSd Tathandlungen (Verändern, Löschen, Sonst-Unbrauchbarmachen) »beschädigt« wurden. Kann man aber in einem konkreten Sachverhalt nicht von einer derartigen Beeinträchtigung der Datensubstanz ausgehen, so reicht auch eine die Datensubstanz nicht zwangsläufig beeinträchtigende Datenunterdrückung aus, wenn sie ein ins Gewicht fallendes Maß an Intensität erreicht hat. Folglich ist die Datenunterdrückung eine den Datenbeschädigungshandlungen subsidiäre Tathandlung. Sie tritt hinter die Auffangtathandlung des Sonst-Unbrauchbarmachens zurück.

Dies ist auch sinnvoll, da für das Opfer im Fall einer (bloßen) zeitweisen Datenunterdrückung, im Gegensatz zu einer Veränderung, Löschung oder sonstigen Unbrauchbarmachung prinzipiell die Möglichkeit besteht, wieder an diese Daten bzw die Information zu gelangen; sie sind noch nicht ganz verloren. Dieses Argument ist insb für die österr Situation beachtlich, da es nach hM bei § 126a Abs 1 auf einen Vermögensschaden ankommt, und sohin auch[1342] dessen Ausmaß Beachtung findet. Fokussiert man hingegen ausschließlich auf die Rechtsgüter der »Datenintegrität« und »Datenverfügbarkeit«, kommt es auf den Aufwand zur Wiederherstellung oder Wiederbeschaffung gar nicht erst an, da die genannten Rechtsgüter bereits mit Beschädigung bzw Unterdrückung der Daten verletzt wären. Der Schaden liegt nach einer solchen Betrachtung lediglich in der beeinträchtigten Datenintegrität bzw -verfügbarkeit.[1343] *Triffterer* bezeichnete § 126a bereits als »eigenständiges Delikt gegen Individualinteressen«.[1344]

Die Datenunterdrückung ist idR ein Dauerdelikt[1345].[1346] Der Täter führt nicht nur den rechtswidrigen Zustand (hier: die Daten sind un-

1341 Vgl JAB 359 BlgNR XVII. GP, 17.

1342 Neben dem bloßen Affektionswert.

1343 Vgl etwa § 303a dStGB; siehe diese Richtung ebenfalls andeutend *Schmölzer,* ZStW 2011/123, 709 (722).

1344 Vgl *Triffterer* in SbgK § 126a Rz 21 (aF Stand Dezember 1992).

1345 Siehe zur Begrifflichkeit *Kienapfel/Höpfel/Kert,* AT[14] Z 9 Rz 28 ff.

1346 Vgl *Komenda/Madl* in SbgK § 126a Rz 13; weiters bereits *Triffterer* in SbgK § 126a Rz 19 und 108 (aF Stand Dezember 1992), der dies allerdings auch für das sonstige Unbrauchbarmachen für möglich erachtet; vgl auch die Rsp zur Urkundenunterdrückung RIS-Justiz RS0095588 mwN.

terdrückt) herbei[1347], sondern hält diesen Zustand anschließend durch ein (tatbestandsmäßiges) Verhalten weiter aufrecht[1348] (durch das Verhalten des Täters bleiben die Daten weiterhin unterdrückt). Das tatbestandsmäßige Verhalten kann entweder in einem fortdauernden Tun bestehen oder aber auch in einem einmaligen Tun mit anschließendem fortdauerndem Unterlassen.[1349] Beispielsweise nimmt A den USB-Stick von B an sich, auf welchem deliktsrelevante Daten bzw Programme gespeichert sind. A will dem B die Daten solange vorenthalten bis eine gewisse Frist verstrichen ist.

In diesem Fall ist § 126a Abs 1 mit dem Eintritt des Schadens (hier: Unterdrücken der Daten durch Wegnahme des USB-Sticks) rechtlich vollendet, aber erst mit Beendigung des tatbestandlichen Verhaltens (hier: Aushändigung des USB-Sticks samt Daten an den Betroffenen) materiell beendet. Das gilt auch für den Fall, in dem der Täter eine Datei mit einem Passwort schützt, damit der Berechtigte nicht mehr darauf zugreifen kann. Zu denken wäre hierbei an die Verwendung sog »Ransomware« als Tatmittel, wodurch die Daten verschlüsselt werden und der Täter in weiterer Folge meist ein »Lösegeld« vom Berechtigten fordert, um die Daten wieder zu entschlüsseln.[1350] Der Täter hat dabei durch ein einmaliges aktives tatbestandsgemäßes Tun die Daten bzw genauer die Dateninhalte durch Verschlüsselung unterdrückt und unterlässt es in weiterer Folge fortdauernd, durch Nichtnennung der entsprechenden Entschlüsselungsinformation (sprich durch Geheimhalten des Passworts) die Unterdrückung wieder aufzuheben. § 126a Abs 1 Fall 4 ist mit dem erstmaligen tatbestandsgemäßen Verhalten formell, aber erst mit Offenbarung des Entschlüsselungscodes materiell beendet. Es spielt dabei keine Rolle, dass der Berechtigte während des ge-

1347 Als Zustandsdelikt kann eine Datenunterdrückung begangen werden, wenn der Täter lediglich den rechtswidrigen »Zustand« herbeiführt, dass die Daten unterdrückt sind, aber im Anschluss kein (tatbestandsmäßiges) Verhalten mehr setzt, damit diese Unterdrückung aufrecht erhalten wird; zB wirft der Täter im Streit mit dem Berechtigten dessen Datenträger mit dringend benötigten Daten aus dem Fenster in eine dichtverwachsene Gartenanlage. Der Datenträger bleibt dabei unbeschädigt. Der Berechtige findet den Datenträger nach einer Stunde intensiver Suche.

1348 Siehe dazu allgemein *Kienapfel,* Dauerdelikt und Dauerstraftat am Beispiel der Begehungsformen der Hehlerei. Zugleich eine Besprechung der grundlegenden E eines verstärkten Senats OGH 16. 10. 1990, 15 Os 71/90, JBl 1991, 435.

1349 Man beachte dabei allerdings die Voraussetzungen des § 2; siehe *Schmoller* in SbgK § 99 Rz 15 (Stand August 1993).

1350 Vgl *Borges/Schwenk/Stuckenberg/Wegener,* Identitätsdiebstahl, 100 f.

samten Tatzeitraums faktisch selbst in Besitz und Verfügungsmacht der – wenn auch verschlüsselten – Daten[1351] blieb.[1352]

Eine Beteiligung an einem Dauerdelikt ist bis zur materiellen Vollbringung – dh Beendigung des rechtswidrigen Zustands – möglich.[1353]

Dies ist aber rechtspolitisch gesehen in Kombination mit einem alternativen Mischdelikt nicht unproblematisch, da eine Wahlfeststellung prozessual nicht schadet. Geht es daher um Fragen einer Beteiligung nach formeller Vollendung der Tat, könnte stets die Datenunterdrückung in einem solchen Fall ins Treffen geführt werden, um sämtliche Beitragstäter noch miterfassen zu können. Ist unklar, ob Daten gelöscht, sonst unbrauchbar oder unterdrückt wurden, wäre es – aus dem Blickwinkel der Strafverfolgungsbehörden – angesichts zB einer Ausschöpfung der Reichweite einer allfälligen Beteiligungsstrafbarkeit – hilfreich, als tatsächliches Geschehen eine Unterdrückung der Daten anzuklagen. Da eine Wahlfeststellung im Fall des § 126a Abs 1 als alternatives Mischdelikt grundsätzlich möglich ist, müssten sich auch die Gerichte nicht besonders um eine genaue Feststellung bemühen. Sie könnten schlicht begründen, dass der Berechtigte über physikalisch gelöschte Daten – wie eben bei einer anhaltenden Datenunterdrückung – nicht verfügen kann. Eine solche Vorgehensweise ist aber schon aus mehreren Gründen abzulehnen.

5. Mischdelikt

Eine Datenunterdrückung weist gegenüber den »Dateneinwirkungshandlungen« wohl einen anderen Sinngehalt auf, der die Frage aufwirft, ob diese beiden Handlungskategorien tatsächlich als rechtlich gleichwertig zu behandeln sind. Jedenfalls lässt sich darin eine unterschiedliche Intensität der Beeinträchtigung des Rechtsguts bzw des Tatobjekts erkennen. Die Tathandlungen des Veränderns, Löschens und Sonst-Unbrauchbarmachens erfordern nämlich, dass der Täter direkt auf die »Datensubstanz« einwirken muss. Im Fall einer Unterdrückung werden aber

1351 Das wäre mit dem Fall vergleichbar, in dem der Täter den Schlüssel einer fremden mit Geld befüllten Geldkassette wegnimmt und dadurch das Geld unterdrückt, wobei die Kassette weiterhin im Gewahrsam des Eigentümers verbleibt.

1352 Der Täter übt durch die Geheimhaltung des Passworts die Datenunterdrückung weiterhin aus. Insoweit liegt es in seinem Verhalten die Dateninhalte wieder frei zu geben.

1353 Siehe dazu auch *Triffterer* in SbgK § 126a Rz 108 (aF Stand Dezember 1992).

die Daten prinzipiell nicht in ihrer Substanz beeinträchtigt. Diese sind unbeschädigt weiterhin am Datenträger existent, nur ist dem Berechtigten der Zugriff darauf zeitweise oder dauerhaft entzogen. Dieses Ergebnis indiziert auch der Paralleltatbestand[1354] der Sachbeschädigung für körperliche Sachen (§ 125), da dort sämtliche Tathandlungen des Abs 1 (Zerstören, Beschädigen, Verunstalten, Unbrauchbar machen) ausschließlich eine Einwirkung auf die Sachsubstanz verlangen.[1355] Das gilt für das – mit § 126a vergleichbare und im Wesentlichen keine Beschädigung einer Sache erforderliche – Unbrauchbarmachen[1356] als bloße (idR straflose) Gebrauchsbehinderung ebenfalls, da auch hier die Substanz der Sache zumindest durch körperlichen Kontakt mit ihr tangiert werden muss.[1357] Daher genügt es für eine Sachbeschädigung auch nicht, zB ein Auto durch Versperren der Ausfahrt, am Wegfahren zu hindern.[1358] Das Vorenthalten des Zündschlüssels ist mangels Substanzeinwirkung am Kfz ebenfalls nicht erfasst.[1359] Warum sollte nun aber die Beeinträchtigung von unkörperlichen Daten gegenüber der Beeinträchtigung einer körperlichen Sache dadurch strenger geschützt werden, dass iSd § 126a Abs 1 bereits vorübergehende Datenunterdrückungen erfasst sind, wohingegen § 125 in Anbetracht einer körperlichen Sache überhaupt nicht darauf abstellt und der eigenständige Tatbestand des § 135 nur eine »dauernde« Entziehung[1360] einer solche Sache pönalisiert. Auch ist für eine (wenn auch nur vorübergehende Datenunterdrückung) im Gegensatz zu § 135 nach einem Teil der Lehre[1361] kein erweiterter Vorsatz erforderlich. Das Ergebnis einer dauerhaften Datenunterdrückung ist zwar grundsätzlich dem einer Datenveränderung, -lösch ung oder sonstigen Unbrauchbarmachung – was den deliktischen (vermögenseffektiven)

1354 Siehe idS auch JAB 359 BlgNR XVII. GP, 17.

1355 Vgl zB *Bertel* in WK² § 125 Rz 6.

1356 Daher liegt der Tatbestand der Sachbeschädigung auch dann vor, wenn allein die bestimmungsgemäße Brauchbarkeit einer Sache nicht unwesentlich eingeschränkt wurde (vgl *Seiler* in SbgK § 125 Rz 40 ff); siehe etwa das Ablassen von Luft aus einem Autoreifen, das Überkleben eines Plakates, das Zerlegen einer Uhr usw bei *Fabrizy,* StGB¹¹ § 125 Rz 2, *Kienapfel,* BT II³ § 125 Rz 37 und *Bertel* in WK² § 125 Rz 5 mwN.

1357 Siehe *Seiler* in SbgK § 125 Rz 16; auch *Kienapfel,* BT II³ § 125 Rz 37; weiters *Reindl,* E-Commerce, 129 f mwN.

1358 Vgl *Fuchs/Reindl-Krauskopf,* BT I⁴, 137; weiters *Seiler* in SbgK § 125 Rz 16.

1359 Siehe *Kienapfel,* BT II³ § 125 Rz 42.

1360 Vgl statt vieler *Fuchs/Reindl-Krauskopf,* BT I⁴, 176.

1361 Wie etwa *Wach* in SbgK § 135 Rz 8 und 28 mwN (Stand November 2009); weiters *Bertel/Schwaighofer,* BT I¹² § 135 Rz 7.

Erfolg anlangt – vergleichbar (in allen Fällen, sind die vermögenswerten Daten nicht bestimmungsgemäß verwendbar), doch liegt wohl ein Unterschied in der Wiederherstellung bzw Wiederbeschaffung, also was das Opferinteresse anlangt, insb dann vor, wenn den betroffenen Daten ausschließlich ein Affektionsinteresse anhaftet (zB Baby- bzw Urlaubsfotos). Wurden solche Daten nämlich unwiederbringlich entfernt, ist die Rechtsgutbeeinträchtigung (hier: »das Interesse am Fortbestand und der Verfügbarkeit der Daten«) bereits zu einer Rechtsgutverletzung intensiviert worden, da eine Schadensgutmachung bzw Restauration – im generellen Gegensatz zu Daten mit einem objektiv bestimmbaren Wert – überhaupt ausgeschlossen ist.[1362] Die Bilder sind faktisch nicht mehr beschaff- bzw herstellbar. Bei einer bloß vorübergehenden Datenunterdrückung ist hingegen die Möglichkeit, die Dateninhalte wieder zu erlangen, nicht von vornherein ausgeschlossen. Und selbst bei einer dauerhaften Datenunterdrückung, die dann angenommen wird, wenn das Opfer nicht mehr mit dem Zugriff darauf rechnen kann, bestünde zumindest noch die Möglichkeit, dass der Täter im Rahmen des Strafverfahrens diese Daten freigibt. Ob daher eine Unterdrückung die Erheblichkeitsschwelle einer unwiderruflichen (physischen) Datenlöschung bzw Unbrauchbarmachung erreicht, ist wohl mehr als fraglich. Der Grad der Verletzung könnte sich ggf iSd allgemeinen Grundsätze der Strafbemessung gem § 32 Abs 3 Fall 1 bei der Strafzumessung auswirken. Eine strengere Strafdrohung als die des Grunddelikts ist allerdings bei Daten mit bloßem Affektionswert – mangels einer diesbezüglich geeigneten Qualifikationsnorm – nicht möglich. Die Anerkennung des Rechtsguts des »Interesses am Fortbestand und der Verfügbarkeit von Daten« indiziert auch – die mE längst notwendige und sogar priorisierende Ausdehnung – der Schutzausrichtung des § 126a auf das Rechtsgut der »Privatsphäre«[1363] und den bloßen immateriellen »Informationswert«[1364] von Daten.

Abschließend ist festzuhalten, dass die Datenunterdrückung, jedenfalls in Form einer vorübergehenden Vorenthaltung, gegenüber den »Dateneinwirkungshandlungen« nicht nur ein aliud, sondern auf-

1362 Siehe zur Problematik iZm der Tätigen Reue (§ 167) weiter unten.

1363 Siehe in diese Richtung auch *Seling,* Privatsphäre, 82.

1364 Vgl auch die Intention der CCC diesbezüglich in ER (ETS 185) Pkt 60: »The protected legal interest here is the integrity and the proper functioning or use of stored computer data or computer programs.«

grund ihres differierenden sozialen Sinngehalts auch als ein eigenständiges Delikt betrachtet werden könnte.

6. Vermögensschaden

Den Deliktserfolg bildet idR der Eintritt des Vermögensschadens, der sich in der nachteiligen Beeinträchtigung der Daten oder Hinderung des Zugriffs auf die Daten manifestiert. Die gesetzlich definierten Handlungsmodalitäten müssen unmittelbar zu diesem Schaden bei einem anderen Menschen führen (arg »dadurch«).

Der Vermögensschaden orientiert sich am wirtschaftlichen Vermögensbegriff, dh aus der Differenz zwischen dem Vermögen vor und nach der Tat.[1365] Für die Bemessung und Feststellung des Schadens kommt es im Allgemeinen auf die Höhe des Aufwandes an, der zur Wiederherstellung des Datenbestandes im unbeschädigten Zustand erforderlich ist.[1366] Die Daten müssen daher grundsätzlich einen Tausch- oder Gebrauchswert aufweisen.

Aufgrund des von der hM eingeräumten weiteren Rechtsguts des »Interesses am Fortbestand und der Verfügbarkeit von Daten« ist auch das bloße Interesse an der Verfügbarkeit von Daten geschützt, denen ein bloß subjektiver (nicht ganz unerheblicher) Gebrauchswert für den Berechtigten anhaftet, der aber objektiv (wertmäßig) nicht feststellbar ist.[1367] Dies kann bspw bei digitalen Personen- oder Urlaubsfotos der Fall sein oder auch bei sonstigen persönlich relevanten Dateien (wie Haushaltstabellen, Einkaufslisten, Liebesbriefe, Geburtstagskalender usw), die nur den Wert der besonderen Vorliebe aufweisen (sog »Affektionsinteresse«[1368]).[1369] Ein solches Interesse, das für die Beurteilung eines Gebrauchswerts bedeutsam sein kann, muss prinzipiell für Dritte objektiv verständlich erscheinen.[1370] Eine deliktsspezifische Schadensqualifikation kann dadurch nicht verwirklicht werden.

1365 Siehe statt vieler *Triffterer* in SbgK § 126a Rz 82 (aF Stand Dezember 1992).

1366 Siehe *Birklbauer/Hilf/Tipold,* Strafrecht BT I² § 126a Rz 11 mwN.

1367 Siehe *Bergauer/Schmölzer* in Jahnel/Mader/Staudegger, IT-Recht³, 635 (649).

1368 Ein solches wurde auch bereits in der Rsp im Anwendungsbereich der Sachbeschädigung (§ 125) anerkannt; siehe OGH 21.11.1989, 15 Os 88/89.

1369 Siehe dazu auch *Reindl-Krauskopf,* Computerstrafrecht², 21; weiters *Fuchs/Reindl-Krauskopf,* BT I⁴, 139; siehe auch *Komenda/Madl* in SbgK § 126a Rz 25; weiters *Kmetic,* Grundzüge, 16.

1370 Siehe iZm § 125 *Seiler* in SbgK § 125 Rz 8.

Auch kann in einem derartigen Fall der Aufwand der Wiederherstellung oder Wiederbeschaffung der Daten mE nichts über die Intensität der Rechtsgutbeeinträchtigung aussagen, da in vielen Fällen der Affektionswert für den Berechtigten den reinen finanziellen Vermögenswert übersteigen dürfte. Demnach besteht wohl auch ein von der gesellschaftlichen Entwicklung und informationstechnischen Durchdringung getragenes Schutzbedürfnis für – nicht völlig unbedeutende – digitalisierte Information, selbst wenn kein objektiv bestimmbarer Vermögenswert damit verbunden sein mag. Trotz der strafrechtlich prinzipiell schwer zu fassenden Erscheinungsformen und Merkmale der Information selbst, die durch Ubiquität, verlustfreie Reproduzierbarkeit und Virtualität maßgeblich gekennzeichnet sind, wurde iZm § 126a neben dem Rechtsgut des »Vermögens« weitgehend auch das »Interesse am Fortbestand und der Verfügbarkeit der Daten« als grundsätzlich gleichwertiges[1371] Rechtsgut anerkannt.[1372] Treffenderweise ist mE als Sammelbegriff für »Schäden bezüglich Daten« der in einem anderen Zusammenhang bekannte Terminus des »Informationswerts« heranziehen. Dies lässt sich damit begründen, dass der Wortteil »Wert« auf eine für den Berechtigten bedeutende (iSv gewichtige) »Sache« verweist, sei es aus vermögensrechtlicher Sicht im engen Sinn (zB ein kommerzielles Computerprogramm; iSd Tauschwerts), aus vermögensrechtlicher Sicht im weiteren Sinn (zB Nutzung einer kostenlosen »Open Source«-Software; Gebrauchswert bzw objektives Gebrauchsinteresse) oder aus einer besonderen Vorliebe bezüglich des Informationsgehalts dieser Daten[1373] (zB digitale Personenfotos; Affektionswert bzw subjektives Gebrauchsinteresse). Resultiert aus den Daten nämlich keine für den Berechtigten relevante und zu bewahrende Information, so sind sie für den Berechtigten faktisch[1374] nutz- und bedeutungslos und fallen nicht unter den Schadensbegriff des § 126a. Man könnte daher das in Anbetracht des Rechtsgüterschutzes erforderliche Werterfordernis für einen Schaden iSd § 126a Abs 1 im »Informationswert« (im weiteren Sinn) zusammenfassen. Daraus folgt e contrario, dass die bloße »Information« an sich, an der also weder ein objekti-

1371 Wobei die dogmatische Realisierung dies nicht widerspiegelt (zB keine geeignete Qualifikationsnorm bei entsprechender Verletzung des subjektiven Gebrauchsinteresses).

1372 Vgl etwa jüngst *Komenda/Madl* in SbgK § 126a Rz 15 ff.

1373 Entspricht dem Informationswert der Daten im engeren Sinn.

1374 Selbst, wenn sie technisch gesehen eine Information bereithalten.

ves Vermögens- noch subjektives Affektionsinteresse besteht, kein von § 126a geschütztes Gut darstellt.

Nach der hM[1375] ist ein Vermögensschaden iSd § 126a in folgenden Fällen auszuschließen:

1. wenn das Opfer selbst kein Interesse mehr an den konkreten Daten hat.
   Das kann der Fall sein, wenn diese Daten bereits vom Berechtigten zur Löschung in den digitalen Papierkorb geschoben wurden. Werden nun ausschließlich diese Daten vom Täter gelöscht, liegt kein Vermögenschaden vor. Auch wäre an spezifische Computerprogrammdaten zu denken, die nach Deinstallation des Programms weiterhin – aber funktionslos – im System verbleiben. Denkbar wären auch (veraltete) temporär ausgelagerte Programmdateien oder Speicherabbildungen eines Systems, die nicht weiter verwendet oder benötigt werden.
2. wenn kein vernünftig denkender Mensch einen Aufwand tätigen würde, um diese Daten wiederherzustellen.
   Beispielsweise werden vom Täter Daten, völlig veraltete Computerprogramme oder Dateien gelöscht, die nicht mehr verwendet werden, aber im System noch vorhanden sind, wie eine veraltete Video- oder Musikkassettenauflistung udgl. Auch in dieser Variante des Entfalls eines Vermögensschadens wird auf den Informationsgehalt (hier: Daten im weiten Sinn) abgestellt.
3. wenn die Wiederherstellung der manipulierten Daten keinen spürbaren Aufwand bedeuten würde.
   Man denke etwa an vollständige, aktuelle Sicherungskopien wie Datenträgerkopien oder komplexere System- oder Festplattenspiegelungen, welche im Fall einer Löschung der Originaldaten die Daten im Grunde genommen weiterhin im Vermögen des Berechtigten halten.[1376]

Die letzte Ausschlussalternative ist jedoch bei genauer Betrachtung diskussionswürdig und nur unter der Prämisse zutreffend, dass man bei der Schadensbewertung von der Identität der konkret betroffenen Da-

1375 Siehe dazu statt vieler *Reindl-Krauskopf,* Computerstrafrecht², 21; weiters *Birklbauer/Hilf/Tipold,* Strafrecht BT I² § 126a Rz 10 mwN; auch *Bergauer/Schmölzer* in Jahnel/Mader/Staudegger, IT-Recht³, 635 (649).

1376 Siehe zu Sicherungskopien generell bereits *Reindl,* E-Commerce, 104.

ten abstrahiert. Denn die tatbildlichen Computerdaten (hier: Daten im engen Sinn) werden in einem derartigen Szenario tatsächlich auch gelöscht, nur die – durch die gelöschten Daten repräsentierte – Information (hier: Daten im weiten Sinn) bleibt durch den Datenbestand der Sicherungskopien erhalten. Der »Vermögensschaden« tritt daher nicht durch die Löschung der »in weiterer Folge tatsächlich auch gelöschten Daten« ein. Es stellt sich in concreto also die Frage, welches Identitätsverständnis bzw -erfordernis man bezüglich des Tatobjekts in Anbetracht des Rechtsgüterschutzes verlangen muss. Verbrennt der Täter ein fremdes wertvolles Buch, so ist das Tatobjekt eindeutig determiniert und die vermögenswerte Eigenschaft haftet diesem unverrückbar an. Löscht der Täter hingegen unkörperliche Daten, so sind lediglich die vom Löschvorgang betroffenen Daten eindeutig bestimmbar, der Wert bzw Informationswert muss aber nicht zwangsläufig (nur) diesen Daten zugeordnet sein bzw durch diese Daten repräsentiert werden.

Da es sich wie bereits angeführt bei § 126a nicht um ein reines Vermögensdelikt handelt[1377], sollte auch jedes berechtigte Interesse am Fortbestand und der Verfügbarkeit der Daten dadurch geschützt werden.

Fehlt es am entsprechenden Schaden, so kann eine Versuchsstrafbarkeit iSd §§ 15, 126a vorliegen.

7. Exkurs: Tauglichkeit des Versuchs

Gerade im Fall des Vorhandenseins einer vollständigen und aktuellen Sicherungskopie stellt sich die rechtspolitische Frage, warum der Täter, obwohl er die Daten zB mittels eines Schadprogramms tatsächlich physisch löscht, sich nur[1378] wegen eines Versuchs strafbar macht. Diese Privilegierung ergibt sich ausschließlich durch das Verhalten des Opfers. Besonders deutlich wird diese Problematik, wenn man sich analog dazu einen Sachverhalt vorstellt, in dem der Täter mit einer Pistole in Tötungsabsicht auf das Opfer schießt.

Vergleichbarkeit mit dem Datenlöschungsfall liegt aber nicht vor, wenn sich das Opfer im Zeitpunkt der Schussabgabe bspw zufällig aus der Schussbahn bewegt und dieses Opferverhalten nur zu einer Ver-

1377 Vgl auch weiters *Birklbauer/Hilf/Tipold,* Strafrecht BT I² § 126a Rz 1.

1378 Ein (bloßer) Versuch wirkt sich bei der Strafzumessung mildernd aus (vgl dazu § 34 Abs 1 Z 13).

suchsstrafbarkeit des Täters führt, da in einem solchen Fall das Opfer gerade nicht (tödlich) getroffen wird. Um die Sachverhalte vergleichen zu können, muss das menschliche Opfer durch den Schuss tödlich getroffen worden sein, aber dennoch in »gleicher Gestalt« und »seinem individuellen Wesen« unversehrt vorhanden sein. Dieses nur in der IKT mögliche »Paradoxon« entsteht aufgrund der Ubiquität und der Möglichkeit der verlustfreien Datenreproduktion, was bedeutet, dass das Original und seine Kopie faktisch ident sind.

Doch bei genauer Betrachtung muss nicht in jedem Fall ein solcher Versuch auch strafbar sein. Gem § 15 Abs 3 ist ein Versuch nämlich als »absolut untauglich« und daher straflos zu beurteilen, wenn die Vollendung der Tat aufgrund der Untauglichkeit des Subjekts, der Art der Handlung oder aufgrund des Tatobjekts unter keinen Umständen möglich war.[1379]

Überprüft man nun den Sachverhalt hins der Tauglichkeit der Tathandlung anhand der Eindruckstheorie[1380] auf der einen Seite und der objektiven ex ante[1381]-Betrachtung auf der anderen, so kommt man zu unterschiedlichen Ergebnissen.

Der den Täter im Handlungszeitpunkt fiktiv begleitende mit Durchschnittswissen und Tatplankenntnis ausgestattete Beobachter (iSd Eindruckstheorie) kann nicht wissen, dass die Sicherungskopie, die in der Schreibtischlade aufbewahrt wird, existiert, was – aufgrund des Eindrucks dieses Beobachters – zu einem nur relativ untauglichen und daher strafbaren Versuch führt.

Würde der Beobachter jedoch wissen, dass es sich beim Tatopfer um ein Unternehmen handelt, das stets vollständige und aktuelle Backups anlegt, welche auch einwandfrei funktionieren, dann könnte man ggf auch an einen absolut untauglichen Versuch denken.

Wird der Sachverhalt nun aus der Perspektive eines objektiven Beobachters beurteilt, der zum Handlungszeitpunkt die gänzlich wahre Sachlage kennt, also auch die Tatsache, dass eine entsprechende Sicherungskopie existiert, so weiß der Beobachter, dass der Computervirus

1379 Zur grundsätzlichen Problematik und den einzelnen Theorien siehe zusammenfassend statt vieler *Kienapfel/Höpfel/Kert,* AT[14], Z 24 Rz 10 ff.

1380 Der Eindruckstheorie schließt sich bei der Betrachtung der Untauglichkeit der Handlung neben dem überwiegenden Teil der Lehre (anstatt vieler *Kienapfel/Höpfel/Kert,* AT[14] Z 24 Rz 13 mwN) auch der OGH wieder an (vgl jüngst OGH 25.01.2012, 15 Os 165/11w; weiters RIS-Justiz RS0115363 mwN).

1381 Vgl etwa *Fuchs,* AT I[8], Rz 30/34 f.

nicht in der Lage ist, eine Sicherungskopie, die in der Schreibtischlage aufbewahrt wird, zu manipulieren, kann er doch die Datenverarbeitungsanlage – schlicht gesagt – nicht verlassen. Es steht daher bereits zum Tatzeitpunkt fest, dass der Täter mit diesem Tatmittel respektive mit der ausgeführten Tathandlung den Vermögensschaden nicht herbeiführen kann. Ungewisse zukünftige Geschehensabläufe spielen praktisch keine Rolle, denn zu jedem Zeitpunkt ist die Handlung bezüglich der Herbeiführung des Vermögensschadens ungefährlich. Es liegt nach dieser Ansicht ein absolut untauglicher (strafloser) Versuch vor, was jedoch in Anbetracht der oben dargestellten Problematik wohl ein kriminalpolitisch unerwünschtes Strafbarkeitsdefizit bedeutet.

Zumindest im hier untersuchten Beispielsfall ist der Eindruckstheorie daher auch der Vorzug zu geben.

(Exkurs Ende)

8. Subjektive Tatseite

In subjektiver Hinsicht muss der Täter bezüglich sämtlicher objektiver Tatbestandsmerkmale zumindest mit dolus eventualis handeln. Ist der Täter der Überzeugung, dass eine Sicherungskopie vorliegt, mangelt es am Schädigungsvorsatz. Geht der Täter irrtümlich davon aus, dass er allein über die Daten verfügen darf, schließt das den Vorsatz aus.[1382]

9. Deliktsqualifikationen

Anfangs wurde in § 126a Abs 2 idF BGBl 605/1987 noch selbst die Konkretisierung des tatbestandlichen Datenbegriffs vorgenommen. Mit dem StRÄG 2002 wurde dieser zu den Begriffsbestimmungen des § 74 transferiert und ist dort in Abs 2 nun für das gesamte StGB bedeutsam.

Reine Schadensqualifikationen befanden sich in der ursprünglichen Fassung des § 126a[1383] noch in dessen Abs 3, wo im ersten Fall ein ATS 25.000,- übersteigender Schaden verlangt wurde, der mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bis zu 360 Tagessätzen bedroht war. Die zweite Schadensqualifikation erfüllte, wer einen

1382 Siehe diese Beispiele bei *Triffterer* in SbgK § 126a Rz 92 und 109 (aF Stand Dezember 1992).

1383 BGBl 605/1987.

ATS 500.000,– übersteigenden Schaden herbeiführte, was mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren zu bestrafen war.

Bedingt durch die Einführung des Euro als Währung wurde mit BGBl I 130/2001 die erste Wertgrenze mit € 2.000,– und die zweite mit € 40.000,– bei gleichbleibenden Strafdrohungen festgesetzt.

Mit dem Budgetbegleitgesetz 2005[1384] wurden auf Grundlage der Geldwertentwicklung und dem Verhältnis von Vermögensdelikten zu anderen Deliktskategorien ua auch in der Qualifikationsnorm des § 126a Abs 2 die Beträge von € 2.000,– auf € 3.000,– und von € 40.000,– auf € 50.000,– erhöht.[1385]

Nunmehr enthält § 126a Abs 2 neben einer zweistufigen Schadensqualifikation (Fall 1 und 2) noch eine weitere Deliktsqualifikation (Fall 3).[1386] § 126a Abs 2 Fall 1 lehnt sich dabei im Wesentlichen an § 126 Abs 1 Z 7 an und stellt auf einen »durch die Tat an den Daten« herbeigeführten € 3.000,– übersteigenden Schaden ab. § 126a Abs 2 Fall 2 orientiert sich an § 126 Abs 2 und qualifiziert die Datenbeschädigung, wenn durch die Tat ein € 50.000,– übersteigender Schaden herbeigeführt wird. Ein derartiger Schaden muss bereits aus der Begehung des Grunddelikts resultieren (Deliktsqualifikation), wobei der qualifizierte Umstand (Wertgrenze) vom Vorsatz erfasst sein muss. Beide Schadensqualifikationen (wobei innerhalb der Schadensqualifikationen – bei Vorliegen sämtlicher Voraussetzungen – die höhere als lex specialis der niedrigeren vorgeht) können mit § 126a Abs 2 Fall 3 echt konkurrieren.

Nach § 126a Abs 2 Fall 3 wird strenger bestraft, wer die Tat als Mitglied einer kriminellen Vereinigung iSd § 278 Abs 2 begeht. Diese Qualifikationsnorm wurde mit dem StRÄG 2008[1387] in Umsetzung des Art 7 Abs 1 des EU-RB 2005/222/JI geschaffen.[1388]

Interessant sind die Qualifikationen des § 126a im Hinblick auf die eigentliche Parallele zur Sachbeschädigung, denn mit Ausnahme der schadensqualifizierenden Fälle des § 126 Abs 1 Z 7 und Abs 2 gibt es keine Qualifikationsfälle, die analog zu bspw § 126 Abs 1 Z 1[1389], 4,

1384 BGBl I 136/2004.
1385 Siehe ErlRV 649 BlgNR XXII. GP, 6.
1386 BGBl 60/1974 idF I 109/2007.
1387 BGBl I 109/2007.
1388 Siehe dazu auch ErlRV 285 BlgNR XXIII. GP, 8.
1389 Zu Religionen im Internet gibt es mittlerweile bereits einiges an Fachliteratur, in Zukunft könnte sich nicht nur – wie bereits aktuell – die Live-Übertragung von Gottesdiensten finden, sondern es könnte der Gottesdienst selbst mit interak-

5, 6[1390] wären. Dies ist inkonsequent, liegen doch elektronisch verarbeitete Daten wohl in bestimmten Fällen auch im Interesse der Allgemeinheit, was den Grund für die grundsätzliche Qualifizierung der Sachbeschädigung nach § 126 Abs 1 Z 1 bis 6 bildet.[1391]

Beispielsweise könnten – worauf nunmehr auch Art 9 Abs 4 lit c RL 2013/40/EG Bezug nimmt – die mittlerweile gänzlich oder teilweise computergesteuerten (intelligenten) Stromversorgungsanlagen, Kommunikationsinfrastrukturen, Verkehrsleitsysteme, Flugsteuerungsprogramme, Kraftwerke, Gaspipelines usw (iSd § 126 Abs 1 Z 5) durch Hacker-Angriffe oder terroristische Anschläge manipuliert werden. Man denke zB an die Verwendung eines Computerwurms[1392] (wie etwa »Stuxnet«) als Tatmittel. Der »Wurm-Trojaner« Stuxnet befiel programmierbare Speicherbausteine[1393] ua der Pumpen- und Ventilsteuerungssysteme des iranischen Atomkraftwerks in Buschehr, um die Geschwindigkeit der Zentrifugen zu beeinflussen und installierte darüber hinaus eine Fernzugriffsmöglichkeit für die Täter über das Internet (sog »Backdoor«).[1394] Auch andere oben angeführte »kritische Infrastrukturen«[1395] sind prinzipiell ebenfalls mit entsprechenden

---

tiven Elementen des Internet im weltumspannenden Netz abgehalten werden. Dann könnten auch »Daten« mit besonderem, religiösem Informationswert dem Gottesdienst gewidmet sein. Darüber hinaus können entsprechende Daten auf einer Website vorliegen, denen die Verehrung seitens einer Religionsgesellschaft entgegengebracht wird; siehe allgemein zu § 126 Abs 1 Z 1 zB *Bertel* in WK² § 126 Rz 1 ff mwN (Stand Dezember 2008); *Seiler* in SbgK § 126 Rz 2.

1390 Die Beschädigung von informationstechnischen Systemen, insb von Daten, die die Landesverteidigung, die Einsatzbereitschaft des Bundesheeres oder den Zivilschutz betreffen (sog »Cyberwar«), könnte analog zu diesem Qualifikationstatbestand genannt werden. Beispiele sind etwa Manipulationen von Flugsteuerungsprogrammen des Militärflugbetriebs oder von militärischen Kommunikationssystemen. Auch wäre die Beeinträchtigung der Software von militärisch oder für den Zivilschutz genutzten unbemannten Luftfahrzeugen (sog »Drohnen« bzw »Unmanned Aerial Vehicles« [UAV]) denkbar.

1391 Vgl OGH 06.10.2005, 12 Os 82/05h (12 Os 83/05 f); weiters OGH 08.03.1977, 9 Os 165/76.

1392 Siehe dazu und zum sog »Cyberterrorismus« iZm Gemeingefährdungsdelikten bei *Bergauer,* jusIT 2008/2, 2.

1393 Speicherbausteile und die Software »WinCC« der Firma Siemens waren betroffen.

1394 Siehe *Kröner,* Cyberterrorismus, 9 ff.

1395 In ErwG 4 RL 2013/40/EU wird vorgeschlagen unter kritischen Infrastrukturen Anlagen, Systeme oder deren Teile anzusehen, die von wesentlicher Bedeutung für die Aufrechterhaltung grundlegender gesellschaftlicher Funktionen, der Gesundheit, der Sicherheit und des wirtschaftlichen oder sozialen Wohlergehens der Bevölkerung sind – wie etwa Kraftwerke, Verkehrsnetze oder staatliche Netze – und deren Störung oder Zerstörung erhebliche Auswirkungen auf einen Mitgliedstaat

Speicherbauteilen ausgestattet, weshalb sie grundsätzlich als Ziele solcher Angriffe in Betracht kommen. In diesem konkreten Beispielsfall könnte man aber ggf von einer Sachbeschädigung durch Unbrauchbarmachen[1396] iSd § 125 vierter Fall ausgehen, die durch § 126 Abs 1 Z 5 qualifiziert ist.[1397] In anderen Fällen, wo es nicht um sehr hardwarenahe »Firmware« geht, sondern selbstständige Computerprogramme das Angriffsziel bilden, fehlt jedoch de lege lata ein vergleichbarer Qualifikationstatbestand. In der RV zum StRÄG 2015, mit dem auch der RL entsprochen werden soll, ist neben einer Begriffsbestimmung bezüglich »kritischer Infrastruktur« folgende Qualifikationsbestimmung in § 126a Abs 4 vorgesehen:

> »(4) Mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren ist zu bestrafen, wer […] 2. durch die Tat wesentliche Bestandteile der kritischen Infrastruktur (§ 74 Abs. 1 Z 11) beeinträchtigt, […].«[1398]

---

hätte, da diese Funktionen nicht aufrechterhalten werden könnten. Die Mehrheit der Arbeitsgruppe »StGB 2015« spricht sich für die Einführung folgender Definition in § 74 Abs 1 Z 11 aus: »Kritische Infrastruktur: Einrichtungen, Anlagen, Systeme oder Teile davon, die eine wesentliche Bedeutung für die Aufrechterhaltung der öffentlichen Sicherheit, die Funktionsfähigkeit öffentlicher Informations- und Kommunikationstechnologie, die Verhütung oder Bekämpfung von Katastrophen, den öffentlichen Gesundheitsdienst, die öffentliche Versorgung mit Wasser, Energie sowie lebenswichtigen Gütern oder den öffentlichen Verkehr haben.« (Bericht des Bundesministers für Justiz über die Fortschritte der Reformgruppe zum Strafgesetzbuch aufgrund der Entschließung des Nationalrates vom 29.04.2014, E 17-NR/XXV. GP; »StGB 2015« Bericht der Arbeitsgruppe, III-104 BlgNR XXV. GP, 11; <www.parlament.gv.at/PAKT/VHG/XXV/III/III_00104/imfname_366604.pdf> (03.03.2015). In der RV 689 BlgNR XXV. GP, 3 wird schließlich in § 74 Abs 1 Z 11 die kritische Infrastruktur wie folgt definiert: »Einrichtungen, Anlagen, Systeme oder Teile davon, die eine wesentliche Bedeutung für die Aufrechterhaltung der öffentlichen Sicherheit und der Landesverteidigung, die Funktionsfähigkeit öffentlicher Informations- und Kommunikationstechnologie, die Verhütung oder Bekämpfung von Katastrophen, den öffentlichen Gesundheitsdienst, die öffentliche Versorgung mit Wasser, Energie sowie lebenswichtigen Gütern, des öffentlichen Abfallentsorgungs- und Kanalwesens oder den öffentlichen Verkehr haben.«

1396 Siehe dazu iZm mit Computersystemen generell *Schmölzer* in BMJ, Strafrechtliche Probleme der Gegenwart 1989, 195 (208 ff).

1397 Siehe bereits oben bzw zur Diskussion darüber im Schrifttum zB *Seiler* in SbgK § 125 Rz 40 ff*; Reindl,* E-Commerce, 128 ff; bezüglich Firmware zB *Jaburek/Schmölzer,* Computer-Kriminalität, 12; auch *Triffterer* in SbgK § 126a Rz 29 (aF Stand Dezember 1992).

1398 RV 689 BlgNR XXV. GP, 7; vgl in diese Richtung bereits den Bericht des Bundesministers für Justiz über die Fortschritte der Reformgruppe zum Strafgesetzbuch aufgrund der Entschließung des Nationalrates vom 29.04.2014, E 17-NR/XXV. GP;

Darüber hinaus wäre aber auch daran zu denken, dass etwa wissenschaftliche oder künstlerische Werte, die in einer allgemein zugänglichen Sammlung im Internet veröffentlicht sind, durch einen Hackerangriff beeinträchtigt werden und nicht einfach ausgetauscht werden können (iSd § 126 Abs 1 Z 4). Denkbar wäre bspw ein Kunstprojekt, bei dem Künstler gemeinsam mit unbestimmten Internetnutzern durch Interaktion ein digitales Werk schaffen, das ständig weiter entwickelt wird und einmalig ist. Auch ein wissenschaftlich anerkanntes Werk, das ausschließlich im Internet zugänglich und nicht gehörig gesichert ist, könnte als Beispiel herangezogenen werden, wenn dadurch keine wirtschaftliche Austauschbarkeit mehr gegeben ist.[1399] In diesen beispielhaft aufgezählten Fällen wäre de lege lata – mangels eines speziellen Qualifikationstatbestands – bei einer »reinen« Datenbeschädigung lediglich das Grunddelikt nach § 126a Abs 1 erfüllt.

10. § 126a als terroristische Straftat

§ 126a Abs 2[1400] kann aber grundsätzlich auch eine »terroristische Straftat« gem § 278c Abs 1 Z 6 darstellen, sofern – entsprechenden Vorsatz vorausgesetzt – dabei eine Gefahr für das Leben eines anderen oder für fremdes Eigentum in großem Ausmaß entstehen kann. Voraussetzung dafür ist, dass die Tat geeignet ist, eine schwere oder längere Zeit anhaltende Störung des öffentlichen Lebens oder eine schwere Schädigung des Wirtschaftslebens herbeizuführen.[1401] In einem solchen Fall wird gem § 278c Abs 2 das Höchstmaß der Strafdrohung der entsprechenden Qualifikation des § 126a Abs 2 um die Hälfte hinaufgesetzt.

Zur Klarstellung, dass auch nur eine schadensqualifizierte Datenbeschädigung iSd § 126a Abs 2 gemeint ist, sollte der Klammerausdruck nach »Datenbeschädigung« in § 278c Abs 1 Z 6 von »(§ 126a)« auf »(§ 126a Abs 2 erster und zweiter Fall)« abgeändert werden. Dies ergibt sich zum einen aus den GMat[1402], wo klargestellt wird, dass es sich um eine »Beschädigung mit einem Schaden von mehr als Euro 2.000,–«

»StGB 2015« Bericht der Arbeitsgruppe, III-104 BlgNR XXV. GP, 25; <www.parlament.gv.at/PAKT/VHG/XXV/III/III_00104/imfname_366604.pdf> (03.03.2015).

1399 Im Sinne von OGH 06.10.2005, 12 Os 82/05h (12 Os 83/05 f).

1400 Aufgrund des nicht eindeutigen Wortlauts, aber hins historischer und teleologischer Erwägungen, ist ausschließlich eine schadensqualifizierte Datenbeschädigung iSd § 126a Abs 2 gemeint (siehe gleich im Anschluss).

1401 Siehe dazu *Bergauer,* jusIT 2008/2, 2.

1402 Vgl dazu ErlRV 1166 BlgNR XX1. GP, 40.

handeln müsse, was sich daher nur auf den ersten und zweiten Qualifikationsfall der Datenbeschädigung bezieht. Zum anderen liefert die korrespondierende Bestimmung der »schweren Sachbeschädigung« (§ 126) Anhaltspunkte dafür, wobei auch in diesem Fall lediglich § 126 Abs 1 Z 7 und § 126 Abs 2 als eine terroristische Straftat in Frage kommen dürfte.[1403]

11. Privilegierungen

Im Zusammenhang mit § 126a ist grundsätzlich eine analoge Anwendung der Privilegierung des § 141 (Entwendung) denkbar.[1404]

Dabei muss der Täter aus Not, Unbesonnenheit oder zur Befriedigung eines Gelüstes[1405] gehandelt haben und eine Sache geringen Wertes einem anderen entziehen oder sich oder einem anderen zueignen. Es muss sich bei der »Sache geringen Wertes«, um eine deliktsspezifische[1406] Sache mit einem objektiven Wert – nach hM – von höchstens € 100,– handeln.[1407] Man wird in Anbetracht einer Datenbeschädigung iSd § 126a Abs 1 wohl in erster Linie an eine Tatbegehung »aus Unbesonnenheit«, unter Umständen auch »zur Befriedigung eines Gelüsts« denken. Zur Befriedigung eines Gelüstes handelt, wer ein eigenes gegenwärtiges Bedürfnis in unmittelbarem zeitlichem Zusammenhang mit der Tathandlung stillen möchte.[1408] Es muss ein intensives, sachbezogenes Bedürfnis sein.[1409] Aus Unbesonnenheit begeht der Täter die Tat, wenn er spontan – ohne lange zu überlegen – einer augenblicklichen Eingebung folgt, die aus besonderen Gründen der Lenkung durch das ruhige Denken entzogen ist und nach der charakterlichen Beschaffen-

1403 Mehr zu § 126a als terroristische Straftat (S 538 ff).

1404 Vgl *Tipold* in SbgK § 141 Rz 11; weiters *Birklbauer/Hilf/Tipold,* Strafrecht BT I² § 126a Rz 14; auch *Komenda/Madl* in SbgK § 126a Rz 88.

1405 Dabei handelt es sich um »besondere Schuldmerkmale« siehe dazu *Wegscheider,* Strafrecht. Besonderer Teil. Eine multimediale Darstellung der Delikte des österreichischen Strafgesetzbuches⁴ (2012) 216; weiters *Birklbauer/Hilf/Tipold,* Strafrecht BT I² §§ 127, 128 Rz 63 mwN.

1406 Der Sachbegriff richtet sich nach den jeweiligen Delikten (siehe *Tipold* in SbgK § 141 Rz 14 [Stand April 2004]).

1407 Siehe RIS-Justiz RS0120079 mwN; wobei ein Abweichen nach unten aufgrund opferbedingter Faktoren ausnahmsweise anerkannt wird (vgl etwa *Fabrizy,* StGB¹¹ § 141 Rz 5; *Bertel* in WK² § 141 Rz 3a (Stand Dezember 2008); *Tipold* in SbgK § 141 Rz 20 f).

1408 *Tipold* in SbgK § 141 Rz 47; weiters *Bertel/Schwaighofer,* BT I¹² § 141 Rz 7; vgl auch OGH 21.06.1978, 10 Os 88/78 mwN.

1409 Vgl *Wegscheider,* BT⁴, 219.

heit des Täter idR unterdrückt worden wäre.[1410] Als Beispielsfall könnte etwa der Fall dienen, in dem eine schwangere Frau einer Freundin, die aber selbst aus medizinischen Gründen nicht schwanger werden kann, auf dem Computer digitale Ultraschallbilder ihres ungeborenen Kindes zeigt und jene ungeplant im Affekt diese Bilder löscht.[1411]

Im Beispielsfall wird aber sichtbar, dass in bestimmten Fällen eine analoge Anwendung des § 141 (iVm § 126a) kriminalpolitische Widersprüche aufzeigt. Einerseits kann gesagt werden, dass ein Ultraschallbild eines ungeborenen Kindes nur den Wert der besonderen Vorliebe (Affektionsinteresse) hat und objektiv wertmäßig nicht bestimmt werden kann. Geht man nun davon aus, dass eine solche Bilddatei unter der objektiven Wertgrenze der € 100,– einzuordnen ist, so wäre die Täterin in diesem Fall über § 141 privilegiert.[1412] Nach dem persönlichen Strafausschließungsgrund des § 141 Abs 3 ist überhaupt straffrei, wer die Tat zum Nachteil des Ehegatten, seines eingetragenen Partners, eines Verwandten in gerader Linie, seines Bruders, seiner Schwester oder zum Nachteil eines anderen Angehörigen, der mit dem Täter in Hausgemeinschaft lebt, begeht.

Auch ist iZm § 126a eine Privilegierung über § 166 Abs 1 möglich, wenn nämlich die Tat im Familienkreis[1413] begangen wird. In diesem Fall ist als Strafdrohung eine Freiheitsstrafe bis zu drei Monaten oder Geldstrafe bis zu 180 Tagessätzen heranzuziehen. Wenn die Tat jedoch sonst mit einer Freiheitsstrafe bedroht wäre, die drei Jahre erreicht oder übersteigt (wie zB im Fall des § 126a Abs 2 zweiter Fall), ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

Liegt eine Begehung im Familienkreis vor, so verwandelt sich zudem das Offizialdelikt gem § 166 Abs 3 in ein Privatanklagedelikt, was auch zu einer prozessualen Privilegierung führt.

1410 Vgl OGH 08.01.2004, 15 Os 118/03, zusammengefasst in RIS-Justiz RS0091000 mwN; weiters *Fabrizy,* StGB[11] § 141 Rz 3.

1411 Die Bilder sind der Berechtigten damit »entzogen«.

1412 Es handelt sich gem § 141 Abs 2 um ein Ermächtigungsdelikt.

1413 Ein solcher liegt gem § 166 Abs 1 vor, wenn der Täter die Tat zum Nachteil seines Ehegatten, seines eingetragenen Partners, eines Verwandten in gerader Linie, seines Bruders oder seiner Schwester oder zum Nachteil eines anderen Angehörigen begeht, sofern er mit diesem in Hausgemeinschaft lebt.

12. Tätige Reue

Schließlich kann grundsätzlich bei einer vollendeten Datenbeschädigung (samt Qualifikationen) eine Strafaufhebung durch Tätige Reue unter den Voraussetzungen des § 167 in Betracht kommen. Rechtspolitisch auffällig zeigt sich dieser Strafaufhebungsgrund dann, wenn Daten mit bloßem Affektionswert unwiederbringbar gelöscht wurden. In einem derartigen Fall können zB digitale Personenbildaufnahmen (wie auch die Ultraschallbilder im obigen Beispiel) des Verletzten nicht mehr hergestellt und auch mangels objektiver Bestimmbarkeit keine finanzielle Schadensgutmachung mehr unternommen werden.[1414] Die Schadensgutmachung nach § 167 Abs 2 erfordert aber entweder die Zurückversetzung in den vorigen Stand im Sinne einer Naturalrestitution oder den Ersatz des zugefügten Vermögensschadens auf Grundlage einer »objektiv-abstrakten Schadensberechnung«, wovon immaterielle Schäden ausgenommen sind.[1415] Dies mag überzogen klingen, doch wurde oben bereits ausgeführt, dass in vielen Fällen das Opferinteresse an nicht wiederbringbaren Dateien dem reinen finanziellen Interesse an rekonstruierbaren bzw wiederbeschaffbaren Daten oder Programmen vorgeht.[1416]

Der Strafanspruch des Staates wird somit auch nur bei Delikten, die als Rechtsgut das Vermögen schützen, durch Kompensation der Vermögensbeeinträchtigung durch vollständige Schadensgutmachung aufgehoben. In den GMat wurde iZm der Eingliederung der Datenbeschädigung in die »reuefähigen« Straftaten des § 167 erklärt, dass dies schon deshalb besonders wünschenswert erscheine, weil hier der Täter nicht selten der einzige sei, der in der Lage wäre, die Beeinträchtigung wieder »rückgängig zu machen«.[1417] Es fragt sich dabei allerdings unter Verweis auf die obigen Ausführungen zu den einzelnen Tathandlungen, wo und in welcher Form der Gesetzgeber diese Möglichkeit der

1414 Die »Tätige Reue« scheidet im Übrigen stets aus, wenn ein »Schaden« aus einer Tat (noch) gar nicht entstanden ist (vgl dazu OGH 28.01.1982, 12 Os 185/81), bzw wohl auch dann, wenn ein solcher nicht bestimmt werden kann.

1415 Siehe statt vieler *Kirchbacher* in WK² § 167 Rz 50 (Stand Juli 2013); weiters *Rainer* in SbgK § 167 Rz 14 (Stand Oktober 2003); vgl auch *Brandstetter,* Die Tätige Reue in der Judikatur des OGH, JBl 1987, 545.

1416 Man muss aber konzedieren, dass dies im Einzelfall wohl – wenn überhaupt – nur äußerst schwierig angemessen berücksichtigt werden kann.

1417 Vgl JAB 359 BlgNR XVII. GP, 19.

Rückgängigmachung der Beeinträchtigung – mit Ausnahme bei der oben dargestellten Freigabemöglichkeit der Daten im Fall der Datenunterdrückung – tatsächlich für realistisch erachtet hat.

Richtig ist, dass bei Mischdelikten, die mehrere Rechtsgüter schützen – wie auch § 126a – nur im Fall der Vermögensschädigung die Bestimmung über die »Tätige Reue« nach § 167 anwendbar ist.[1418] Dies führt jedoch zu einem rechtspolitischen Wertungswiderspruch. Ist ein vom Täter durch die Datenbeschädigung verursachter unmittelbarer Schaden objektiv bestimmbar, weil es sich etwa um eine wiederbeschaffbare Standard-Software oder eine neu programmierbare Individual-Software[1419] handelt, so kann die Strafbarkeit des Täters – auch bei einer qualifizierten Tat nach § 126a Abs 2 – grundsätzlich durch eine vollständige Schadensgutmachung iSd § 167 aufgehoben werden. Löscht der Täter aber auch nur eine einzige Datei, der ein objektiv nicht bestimmbarer Wert der besonderen Vorliebe des Verletzten anhaftet (das Rechtsgut bildet hier das »Interesse am Fortbestand und der Verfügbarkeit von Daten«), so ist eine Strafaufhebung durch Tätige Reue mangels Möglichkeit der Schadensgutmachung nicht möglich.[1420]

Im Ergebnis ist folglich festzuhalten, dass die Konzeption des Rechtsinstituts der Tätigen Reue trotz ausdrücklicher Erfassung der Datenbeschädigung als reuefähiges Delikt in Hinblick auf Computerdaten mit bloßem Affektionswert (dasselbe gilt im Übrigen analog zu § 126b in Bezug auf Computersysteme) versagt und in diesen Fällen keine strafaufhebende Wirkung entfalten kann.

13. Sonstiges

§ 126a fällt hins seines Grundtatbestands in Abs 1 gem § 30 Abs 1 StPO in die sachliche Zuständigkeit des Bezirksgerichts. Die qualifizierten Formen des Abs 2 fallen gem § 31 Abs 4 Z 1 StPO dem Einzelrichter des Landesgerichts zu.

1418 Siehe zu generellen Überlegungen zur Tätigen Reue iVm Delikten mit mehrfachem Rechtsgüterschutz *Schroll,* Zu den reuefähigen Delikten des Vermögensstrafrechts, ÖJZ 1985, 357.

1419 Der Schaden wird hier über die Herstellungskosten zu bemessen sein.

1420 So hat auch der OGH bereits festgestellt, dass die Tätige Reue ausscheidet, wenn ein »Schaden« aus einer Tat (noch) nicht entstanden ist. Lässt sich ein solcher objektiv nicht bestimmen bzw ein realer Schaden faktisch nicht beheben, ist eine Schadensgutmachung wohl auszuschließen.

B. Störung der Funktionsfähigkeit eines Computersystems (§ 126b)

> § 126b (1) Wer die Funktionsfähigkeit eines Computersystems, über das er nicht oder nicht allein verfügen darf, dadurch schwer stört, dass er Daten eingibt oder übermittelt, ist, wenn die Tat nicht nach § 126a mit Strafe bedroht ist, mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.
>
> (2) Wer durch die Tat eine längere Zeit andauernde Störung der Funktionsfähigkeit eines Computersystems herbeiführt, ist mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bis zu 360 Tagessätzen, wer die Tat als Mitglied einer kriminellen Vereinigung begeht, mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren zu bestrafen.[1421]

§ 126b ist das Ergebnis der Umsetzung des Art 5 CCC (System interference), der besagt:

> »Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data«.

Das teleologische Anliegen des Art 5 CCC, aber auch des aus dessen Umsetzung resultierenden § 126b, bilden sog »DoS-Attacken«.[1422]

1. Exkurs: DDoS-Angriffe

Das Akronym »DoS« steht für Denial-of-Service und beschreibt eine Handlung, die darauf abzielt, die Funktionsfähigkeit eines Computersystems oder einen bestimmten elektronischen Dienst zum Absturz zu bringen bzw schwer zu stören.[1423] Ein DoS-Angriff ist grundsätzlich rein destruktiv und beschränkt sich auf die Lahmlegung von Diensten oder ganzen Systemen.[1424] Im Zuge einer solchen Attacke werden wichtige Ressourcen des Zielsystems, wie Speicher, Prozessorzeit und/oder Netzwerkkomponenten, derart in Anspruch genommen, dass weitere

1421 BGBl 60/1974 idF I 109/2007.
1422 Vgl ErlRV zum StRÄG 2002, 1166 BlgNR XXI. GP, 29; siehe auch ER (ETS 185) Pkt 67.
1423 Siehe dazu auch *Kurose/Ross,* Computernetzwerke⁴, 80f; auch *Moore,* Cybercrime², 39.
1424 Siehe ganz allgemein dazu *Clough,* Cybercrime, 37.

Anfragen an den Server nicht mehr be- bzw verarbeitet werden können. Gehen die inkriminierten Datenübermittlungen von mehreren Computersystemen aus, spricht man von Distributed DoS-Angriffen (DDoS[1425]). Damit lassen sich bspw gefährliche Großangriffe auf (kritische) Informationssysteme ebenso durchführen[1426] wie politisch motivierte Maßnahmen im Rahmen des sog »Hacktivismus«[1427]. Dieses Phänomen beschreibt die Manipulation von Informationssystemen zur Durchsetzung bzw Verbreitung und Veröffentlichung von (idR politischen) Zielen, Meinungen, Informationen, Aufrufen zu Boykottierungen usw. Der Hacktivismus wird von seinen Vertretern als informationstechnisches Mittel der Demokratie erachtet und mit klassischen direkten Aktionen wie Demonstrationen, Streiks, Boykotts uÄ in Verbindung gebracht. DDoS-Angriffe, die für solche Zwecke von den Hacktivisten eingesetzt werden, überschreiten allerdings die Schwelle dieser tolerierten demokratischen Mittel bei weitem.[1428]

Doch gleichgültig, für welchen Zweck DDoS-Attacken Verwendung finden, sie lassen sich idR in zwei Phasen unterteilen. Zuerst sucht der Täter über port- bzw vulnerability-scans[1429] nach ungesicherten und für sein Vorhaben geeigneten Computersystemen in einem Netzwerk. In einem nächsten Schritt werden die als unsicher und für geeignet befundenen Systeme mit Schadprogrammen, wie zB »Trojanischen Pferden« oder Computerwürmen, infiltriert. Die Inhaber der als Tatwerkzeuge des Täters benutzten Systeme sind ahnungslos und in Unkenntnis darüber, dass ihre Computer Teil eines sog »Botnet«

1425 »Verteilter Angriff« auf ein gemeinsames Zielsystem (siehe dazu *Janowicz,* Sicherheit[3], 6; weiters *Kurose/Ross,* Computernetzwerke[4], 81).

1426 Vgl ErwG 5 f RL 2013/40/EU.

1427 Siehe zum Begriff ausf *Paget,* Hacktivismus, <www.mcafee.com/de/resources/white-papers/wp-hacktivism.pdf> (01.04.2014); weiters *Pfister,* Hacking, 85 f.

1428 Die ernstzunehmenden (schädigenden) Aktionen von Hacktivisten zusammenfassend *Paget,* Hacktivismus, <www.mcafee.com/de/resources/white-papers/wp-hacktivism.pdf> (01.04.2014).

1429 Siehe dazu *Rey/Thumann/Baier,* IT-Sicherheit, 25 ff und 33 ff; auch *Moore,* Cybercrime[2], 33.

wurden.[1430] Man nennt diese Computersysteme »Zombies«[1431], »Bots«[1432] oder »Drohnen«[1433]. Die Systeme vernetzen sich selbstständig untereinander und können über die geschaffene Hintertüre zentral oder dezentral vom Täter gesteuert werden.[1434] Je mehr Computersysteme Teil dieses Netzwerks sind, desto größer ist auch die Schlagkraft für die eigentlichen DDoS-Attacken.

a. Bot-Netzwerke

Je nach verwendeter Topologie können alle Zombiesysteme mit einem zentralen Master-Server (C&C[1435]-Server) verbunden sein.[1436] Bei dieser als Standard-Stern-Topologie erkennbaren Struktur werden dem Client-Server-Prinzip[1437] entsprechend die Zombiesysteme direkt[1438] mit dem C&C-Server verbunden. Diese Netzwerk-Architektur stellt jedoch eine einfache und auch unsichere Topologie dar. Werden zur Ausfallsicherung des Netzwerkes dem Master-Server weitere C&C-Server zentral zur Seite gestellt (sog »Multi-Server-Architektur«), kann die Aus-

1430 Siehe dazu allgemein *Wang/Aslam/Zou,* Peer-to-Peer Botnets, in Stavroulakis/Stamp (Eds), Handbook of Information and Communication Security (2010) 335 (338).

1431 Siehe dazu *Hoagland/Ramazan/Satish,* Bot Networks, in Jacobsson/Ramzan (Eds), Crimeware. Understanding New Attacks and Defenses (2008) 183 (183 ff).

1432 Als »bot« wird nun das einzelne Computerprogramm bzw Computersystem, das Teil eines sog »Bot-Netzwerks« ist, bezeichnet.

1433 Siehe die Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses zu der »Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen über den Schutz kritischer Informationsinfrastrukturen — ›Schutz Europas vor Cyber-Angriffen und Störungen großen Ausmaßes: Stärkung der Abwehrbereitschaft, Sicherheit und Stabilität‹« KOM (2009) 149 endg, ABl C 2010/255, 130.

1434 Siehe *Reindl-Krauskopf,* ÖJZ 2015/19.

1435 »Command and Control«.

1436 Siehe dazu auch den Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Angriffe auf Informationssysteme und zur Aufhebung des Rahmenbeschlusses 2005/222/JI des Rates, KOM (2010) 517 endg; *Stern.de,* <www.stern.de/digital/online/gefaehrliches-bot-netzwerk-tdl-4-es-ist-praktisch-unzerstoerbar-1701583.html> (01.04.2014).

1437 Siehe dazu *Kersken,* IT-Handbuch[5], 189.

1438 IdR wurde die IP-Adresse dieses Servers in den Trojanischen Pferden, die sich auf den Zombiesystemen befinden, »hardcodiert«, dh direkt im Source Code verankert. Diese Variante stellt zwar die einfachste Kommunikationsstruktur dar, doch besteht zumindest die Möglichkeit, die IP-Adresse des Master-Servers durch Überwachung der ausgehenden Verbindungen oder Decodierung der Schadsoftware auf den Clients zu eruieren.

fallssicherheit erhöht werden. In einem derartigen Fall verfügen die Zombies über die Adressinformationen aller C&C-Server, was ihnen bei Unerreichbarkeit oder Abschaltung einzelner dieser Server eine Ausweichmöglichkeit auf die weiteren arbeitsfähigen Kommandozentralen bietet. Für den Aufbau einer derartigen Netzwerk-Struktur ist aber ein wesentlich höherer Planungsaufwand erforderlich.[1439]

Damit nicht alle Zombiesysteme direkt mit dem Master-Server kommunizieren[1440] müssen und der Täter folglich nicht Gefahr läuft, durch die den Zombies bekannte IP-Adresse des C&C-Servers ausgeforscht zu werden, lässt sich auch eine hierarchische Topologie für DDoS-Angriffe nutzen. Der C&C-Server steuert in diesem Szenario lediglich höherrangige Zombiesysteme (sog »Handler«), welche dann in weiterer Folge die Befehle an die restlichen (niederrangigen) Zombiesysteme weiterleiten.[1441] Um die Identität des C&C-Servers noch weiter zu verschleiern, werden meist Proxy-Server[1442] dazwischengeschaltet, die als Stellvertreter agieren und die Anfragen der Zombiesysteme vorerst entgegennehmen.[1443] Ein Proxy übermittelt die Anfrage in weiterer Folge an den C&C-Server weiter. Dabei kommuniziert er nach außen hin mit einer eigenen IP-Adresse, weshalb die IP-Adresse des C&C-Servers den Zombies gegenüber verborgen bleibt. Als ein strukturbedingter Nachteil erweist sich in diesem Fall die anfallende Latenzzeit von der Befehlserteilung bis zu dessen Entgegennahme und Ausführung durch die Zombiesysteme.[1444]

Wesentlich besser abgesichert als zentral organisierte Bot-Netzwerke sind jene, die über dezentrale »Peer-to-Peer«[1445]-Strukturen miteinander verbunden sind. In solchen Netzwerken agieren die einzelnen teilnehmenden Systeme – im Gegensatz zu Client-Server-Architekturen – als gleichrangige Partner. Das bedeutet, dass alle Systeme

---

1439 Siehe dazu *Hoagland/Ramazan/Satish* in Jacobsson/Ramzan, Crimeware, 183 (188 f).

1440 Hierzu werden die unterschiedlichsten Kommunikationsprotokolle (wie zB IRC, HTTP) verwendet (siehe *Hoagland/Ramazan/Satish* in Jacobsson/Ramzan, Crimeware, 183 [193 ff]).

1441 Siehe dazu *Jia/Zhou,* Distributed Network Systems. From Concepts to Implementations (2005) 265 f; weiters *Hoagland/Ramazan/Satish* in Jacobsson/Ramzan, Crimeware, 183 (189).

1442 Engl für Stellvertreter.

1443 Siehe *Chantelau/Brothuhn,* Multimediale Client-Server-Systeme (2010) 52 f.

1444 Vgl *Hoagland/Ramazan/Satish* in Jacobsson/Ramzan, Crimeware, 183 (189).

1445 Auch als »P2P« bezeichnet; Peer (engl für Gleichgestellter, Kollege).

sowohl Server als auch Client-Aufgaben ausführen.[1446] Fallen einzelne Systeme aus, wird das gesamte P2P-Netzwerk nicht wesentlich beeinträchtigt. Der Täter, der mit seinem System ebenfalls als gleichrangiger Kommunikationspartner Teil dieses Netzwerks ist, sendet seine Befehle in verschlüsselter Form an die anderen Peers. Die verschlüsselte Befehlsanweisung ist notwendig, um ein Korrumpieren des Netzwerks zu verhindern, da andere »Teilnehmer«, die sich in Kenntnis der Existenz dieses Bot-Netzwerkes befinden, genauso Befehle innerhalb des P2P verteilen könnten.[1447]

In der zweiten Phase eines DDoS-Angriffs aktiviert der Täter durch Übermittlung von Befehlen die festgelegten Angriffsmodalitäten der »Zombiesysteme«, die in weiterer Folge annähernd gleichzeitig den eigentlichen Angriff auf das ausgewählte Zielsystem beginnen.

Ob der DoS-Angriff eine Überlastungssituation durch das gleichzeitige Absenden von zulässigen Datenpaketen schaffen soll, oder entsprechende Angriffs-Methoden durch manipulierte Datenpakete stattfinden, hängt von den in den Schadprogrammen der Zombiesystemen implementierten Funktionalitäten ab, die im Wesentlichen wiederum von den technischen Fähigkeiten des Täters und dessen Intention abhängen.

b. DoS-Methoden

In der Praxis sind unterschiedliche Methoden von DoS-Attacken bekannt, wobei laufend Modifikationen bzw Adaptierungen der technischen Vorgänge durchgeführt werden und auch eine Vielzahl von abgewandelten Bezeichnungen dieser Vorgänge existiert. Zur Veranschaulichung werden nachfolgend einige der bedeutenden Angriffskonzepte beispielhaft dargestellt.

1446 Siehe *Wang/Aslam/Zou* in Stavroulakis/Stamp, Handbook, 337.

1447 Als Beispiel für ein P2P-Bot-Netzwerk kann das »Conficker-Botnet« mit mehr als fünf Millionen Rechnern genannt werden (siehe dazu auch die Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses zu der »Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen über den Schutz kritischer Informationsinfrastrukturen — ›Schutz Europas vor Cyber-Angriffen und Störungen großen Ausmaßes: Stärkung der Abwehrbereitschaft, Sicherheit und Stabilität‹« KOM [2009] 149 endg, ABl C 2010/255, 130); zum Conficker-Wurm siehe auch *Wennig,* Cybercrime, in Landesgruppe Österreich der Internationalen Strafrechtsgesellschaft (AIDP) und Juristenverband (Hrsg), Cyber Crime – Zunehmende Bedrohung der Informationsgesellschaft (2012) 47 (47 ff).

(i.) Ping flooding bzw ICMP flooding

»Ping«[1448] ist ein Diagnose-Programm mit welchem die Erreichbarkeit von anderen Hosts im Netzwerk überprüft werden kann. Das entfernte System wird dabei über die IP-Adresse oder den Domainnamen mittels ICMP[1449] angesprochen.[1450] Dieses Protokoll baut auf dem IP[1451] auf, weshalb ICMP-Daten mit einem vollständigen IP-Header[1452] verschickt werden. Bei der Ausführung des Befehls wird ein ICMP-Paket vom Typ ICMP Echo Request an den adressierten Host gesendet (sog »Ping«). Der Empfänger sendet daraufhin alle im Datenpaket enthaltenen Daten mittels eines ICMP Echo Reply dem Sender zurück (sog »Pong«).[1453]

Beim sog »Ping flooding« werden nun möglichst viele Ping-Anfragen an das Zielsystem geschickt. Der attackierte Host versucht alle Requests spezifikationsgemäß zu beantworten, was jedoch aufgrund der hohen Anzahl der Anfragen zum Systemabsturz führen kann.[1454]

(ii.) Ping of Death bzw Large Packet Ping

Im Fall des »Ping of Death« wird abermals das Ping-Diagnoseprogramm verwendet, das zur Standard-Ausstattung vieler Betriebssysteme[1455] gehört. Ziel des Angriffs ist es, eine Ping-Anfrage mit einem nicht spezifikationsgemäßen IP-Paket[1456] an ein Zielsystem zu senden, um dieses zum Absturz zu bringen. Ein IP-Paket (= Datagramm[1457]) darf einschließlich des Headers und des Datenteils der höheren Protokolle höchstens 64 KB umfassen.[1458] Datenpakete dieser Größe können aber

1448 Packet Internet Groper.

1449 »Internet Control Message Protokoll« definiert in Request for Comments (RFC) 792; siehe dazu *Hein/Reisner,* TCP/IP², 41 ff.

1450 Beispiel über Eingabe im Kommandozeileninterpreter: »ping 192.168.1.12«.

1451 »Internet Protokoll« definiert in RFC 791; siehe *Hein/Reisner,* TCP/IP², 56 ff.

1452 Dh es wird ua die IP-Adresse des Senders, wie auch die IP-Adresse des Empfängers mitgeliefert; siehe dazu *Hein/Reisner,* TCP/IP², 58 und 63 f.

1453 Vgl *Hein/Reisner,* TCP/IP², 48; weiters *Studer,* Netzwerkmanagement und Netzwerksicherheit (2010) 114 f.

1454 Siehe *Studer,* Netzwerkmanagement 114 f.

1455 Überwiegend kam die Methode bei älteren Versionen der Microsoft-Betriebssysteme zum Einsatz.

1456 Nach IPv4; Für IPv6 wurde der Datagramm-Header deutlich vereinfacht (siehe *Kersken,* IT-Handbuch⁵, 232).

1457 Die Datenpakete der Schicht, auf der das Internet Protokoll (IP) arbeitet, werden Datagramme bezeichnet; siehe *Kersken,* IT-Handbuch⁵, 230.

1458 Siehe *Kersken,* IT-Handbuch⁵, 232.

von vielen Netzwerken nicht verarbeitet werden. Aus diesem Grund werden die Datagramme vorwiegend von Routern – die eine kleinere MTU[1459] benötigen – in kleinere Fragmente zerlegt, mit IP-Headern versehen und weitergeleitet.[1460] Beim Empfänger werden die Fragmente den Offset-Informationen im jeweiligen IP-Header entsprechend wieder zum richtigen und vollständigen Datagramm zusammengesetzt (Reassemblierung). Der Offset-Wert[1461] gibt dabei die konkrete Position des jeweiligen Fragments relativ zum Anfang des Datenblocks im ursprünglichen Datagramm an.[1462] Das erste Fragment und ein nicht fragmentiertes Paket haben im Fragment Offset des Headers den Wert Null eingetragen. Wird nun den Fragmenten über die Information ihrer Lage eine Größe bescheinigt, die das gesamte Datagramm über 64 KB werden lässt, so kann das Empfangssystem beim Zusammensetzen der Fragmente zum Absturz gebracht werden.[1463]

(iii.) Teardrop

Teardrop-Angriffe orientieren sich – ähnlich wie der »Ping of Death« – an Schwachstellen der IP-Fragmentierung. So wird eine Reihe von IP-Fragmenten mit sich überlappenden Offset-Werten versendet.[1464] Beim Versuch des Zielsystems, die Fragmente zum ursprünglichen Datagramm zusammenzufügen, kommt es zum Absturz des Systems.

1459 Dies rührt daher, dass verschiedene physikalische Netzarten existieren, die unterschiedliche Maximallängen für Datenpakete erlauben. Die Länge dieses Werts wird »Maximum Transmission Unit« (MTU) genannt und ist in manchen Netzwerken fix vorgegeben (siehe *Kersken,* IT-Handbuch[5], 232).

1460 Siehe auch *Olbrich,* Netze. Protokolle. Spezifikationen (2003) 98 f; weiters *Hunt,* TCP/IP[3], 18.

1461 IM IP-Header »Fragment Offset« genannt.

1462 Siehe *Hein/Reisner,* TCP/IP[2], 62.

1463 Beispiel über Eingabe im Kommandozeileninterpreter: »ping -l 65555 192.168.1.12«, wobei der Parameter »-l« die Paketgröße in Byte angibt.

1464 Siehe auch *Olbrich,* Netze, 100.

(iv.) Smurf[1465]

Ein Smurf-Angriff vereint das sog »IP-Spoofing«[1466] mit Broadcast[1467]- bzw Multicast[1468]-Adressierungen. Ein Router eines Netzwerks wird dabei mit »Ping«-Anfragen überflutet. Als Zieladresse der jeweiligen Anfragen wird für alle Pakete zB die Broadcast-Adresse des konkreten Netzwerks angegeben. Als Absenderadresse wird aber die tatsächliche IP-Adresse des auserwählten Opfers vorgetäuscht. Die mittels des Ping-Befehls initiierten ICMP Echo Request werden nun an alle mit dem entsprechenden Netzwerk verbundenen Hosts gesendet. Spezifikationsgemäß werden diese Anfragen von sämtlichen Systemen mit ICMP Echo Reply-Paketen (»Pong«) beantwortet. Da der Täter die Antwort-Pakete durch die Manipulation der Absenderadresse im Anfrage-Paket an ein konkretes Zielsystem geleitet hat, kann dieses durch die enorme Datenflut zum Absturz gebracht werden.[1469]

(v.) SYN-Flooding[1470]

Das Transmission Control Protokoll (TCP)[1471] ist ein verbindungsorientiertes Transportprotokoll[1472], das auf dem Internet Protokoll (IP) aufbaut. Der Verbindungsaufbau für eine konkrete Datenübertragung erfordert spezifikationsgemäß den sog »Three-Way-Handshake«.[1473]

1465 Engl für »Schlumpf«.

1466 Unter »Spoofing« versteht man generell das Vortäuschen einer Tatsache; siehe *Borges/Schwenk/Stuckenberg/Wegener,* Identitätsdiebstahl, 17 ff.

1467 Unter Broadcast (engl für Ausstrahlung, Rundfunk) versteht man eine an alle Hosts eines konkreten Netzwerks adressierte Meldung (siehe *Kersken,* IT-Handbuch[5], 222).

1468 Eine Multicast-Gruppe ist eine auf beliebige Netze verteilte Gruppe von Computersystemen, die sich dieselbe (Multicast-)IP-Adresse teilen (siehe *Kersken,* IT-Handbuch[5], 222).

1469 Siehe *Oppliger,* Internet and Intranet Security[2] (2002) 59 f; weiters *Studer,* Netzwerkmanagement, 112.

1470 Im Bereich des TCP-Flooding gibt es neben dem TCP SYN-Flooding noch eine Reihe weiterer ähnlich gelagerte Angriffsmethoden, die idR in eigenständigen Computerprogrammen abgebildet sind, wie etwa LOIC (Low Orbit Ion Cannon), das ua bei der »Operation Payback« von der Hackergruppe »Anonymous« eingesetzt wurde; siehe dazu *Janssen/Kuri/Schmidt,* Operation Payback: Proteste per Mausklick, <heise.de/-1150151> (01.04.2014).

1471 Definiert in RFC 793.

1472 Es baut eine virtuelle Punkt-zu-Punkt-Verbindung über sog »Ports« zwischen Sender und Empfänger auf (siehe *Kersken,* IT-Handbuch[5], 249).

1473 Siehe *Hunt,* TCP/IP[3], 22 f; weiters *Kersken,* IT-Handbuch[5], 249; vgl auch *Olbrich,* Netze, 143 ff; weiters *Janowicz,* Sicherheit[3], 24.

Dabei werden drei spezielle TCP-Datenpakete – lediglich mit entsprechenden Informationen im TCP-Header – ohne Nutzdaten ausgetauscht. Der Sender, der eine Verbindung herstellen will, sendet ein TCP-Paket mit einem gesetzten SYN-Bit[1474] (Synchronisierungs-Bit) im Header an einen konkreten TCP-Port[1475] des Zielsystems. Der Empfänger registriert diesen Synchronisierungswunsch, legt einen Eintrag in einem eigenen Pufferspeicher an und repliziert mit einem TCP-Paket mit gesetztem SYN- und ACK-Bit (Synchronisierungs-/Acknowledgement-Bit).

Der Sender bestätigt diese Sendung wiederum mit einem TCP-Paket mit gesetztem ACK-Bit. Sofern diese Kontaktaufnahme nun einwandfrei erfolgt ist, kann der eigentliche Nutzdatenaustausch beginnen.[1476]

Beim SYN-Flooding wird der TCP-Verbindungsaufbau dahingehend manipuliert, dass die Quell-IP-Adresse in der Synchronisierungsanfrage (SYN-Paket) geändert wird, um dem Empfänger eine völlig andere Absenderadresse (IP-Adresse und TCP-Port) vorzutäuschen.[1477] Der Empfänger des SYN-Pakets antwortet an die angegebene (aber falsche) Absenderadresse dem Three-Way-Handshake entsprechend mit einem SYN/ACK-Paket und wartet auf die endgültige Bestätigung (sog »Half-open Connection«).[1478] Die Bestätigung mit einem ACK-Paket bleibt aber zwangsläufig aus, da der Täter die Absenderadresse geändert hat und daher keine Antwort zu erwarten ist. Der Synchronisierungswunsch bleibt jedoch bis zum Ablauf des Time-out in einem speziellen Pufferspeicher (Backlog-Queue) am Empfängersystem gespeichert.[1479] Der Täter sendet nun permanent weitere solcher manipulierter Synchronisierungsrequests an das Zielsystem. Gibt es kein

1474 Auch als »Flag« bezeichnet; Im TCP-Header finden sich im »Control-Flag«-Feld »Ein-Bit-Indikatoren«, die zum Aufbau, Beenden und zur Aufrechterhaltung von Verbindungen dienen (siehe *Hein/Reisner,* TCP/IP², 215).

1475 Sog »Kommunikationsendpunkt«, der im Bereich zwischen 0 und 65.535 liegen muss und zusammen mit der IP-Adresse angegeben wird; TCP-Ports ermöglicht das gleichzeitige Kommunizieren auf mehreren Kommunikationskanälen mit einer IP-Adresse zB WWW (Port 80), FTP (Port 21), SMTP (Port 25); siehe dazu *Tanenbaum,* Computernetzwerke⁵ (2012) 630; weiters *Kersken,* IT-Handbuch⁵, 249 f; auch *Winterer,* Viren, 210.

1476 Siehe dazu *Kersken,* IT-Handbuch⁵, 249.

1477 Siehe *Russell/Cunningham,* Hacker-Buch, 497.

1478 Siehe dazu *Oppliger,* Internet², 60.

1479 Vgl *Oppliger,* Internet², 60.

Limit für halboffene Verbindungen auf der Empfängerseite, so können sämtliche Ressourcen des Zielsystems für die Verarbeitung dieser Verbindungsaufbauprozesse gebunden werden, was zu einer schweren Funktionsstörung des Systems führen kann. Doch selbst wenn das Zielsystem mit einem Limit (zB 10 Half-open Connections) für derartige Verbindungsanfragen ausgestattet ist, kann nach Erreichung dieses Limits keine weitere TCP-Verbindung mit diesem Zielsystem mehr aufgebaut werden, bis entweder halboffene Verbindungen aus dem Puffer durch ordnungsgemäße Abwicklung hergestellt und aus der Verbindungswarteschlange entfernt wurden, die »Half-open Connections« zurückgesetzt werden[1480] oder das jeweilige Time-out dieser TCP-Verbindungsanfragen eingetreten ist.[1481]

(vi.) Land-Attack

Land-Attacks funktionieren ähnlich wie das SYN-Flooding, wobei der Zielcomputer mit Synchronisierungsanfragen (SYN-Paketen) bombardiert wird, deren Quelladresse (IP-Adresse und TCP-Port) exakt der Adresse des Zielsystems entspricht.[1482] Für das Zielsystem entsteht daher der Eindruck, als müsse es sich die Pakete selbst senden. Darum versucht es permanent sich selbst auf die Synchronisierungsanfrage zu antworten. Dadurch wird die Systemperformance stark beeinträchtigt, was auch zum Systemabsturz führen kann.[1483]

(Exkurs Ende)

1480 Dies kann etwa dadurch eintreten, dass die vorgetäuschten Absenderadressen zufälligerweise im Internet im Zeitpunkt des Angriffs tatsächlich verwendet werden. In diesem Fall antwortet dieses unbedachte System auf das SYN/ACK-Paket mit einem RST-Paket (Reset), da es eben keine Verbindung eingehen will. Nach diesem RST-Paket wird der entsprechende Backlog-Eintrag im Zielsystem gelöscht und der Platz wieder freigegeben (siehe *Schmidt,* Dämme gegen die SYN-Flut, <heise.de/-270378> (01.04.2014).

1481 Siehe dazu ausf *Schmidt,* <heise.de/-270378> (01.04.2014); weiters *Oppliger,* Internet², 60.

1482 Siehe *Studer,* Netzwerkmanagement, 112 f.

1483 Siehe *Microsoft,* Land Attack, <support.microsoft.com/kb/165005/DE/> (01.04.2014).

2. Tatobjekt »Computersystem«

Tatobjekt des § 126b ist ein »Computersystem« iSd § 74 Abs 1 Z 8. Auf den ersten Blick mag das Tatobjekt verwundern, da es den Anschein erweckt, es müsse sich dabei tatsächlich um ein Gesamtsystem handeln, das zum Absturz gebracht oder schwer gestört wird. Dies drängt sich schon allein deshalb auf, da in anderen einschlägigen Computerdelikten von einem Computersystem oder von einem »Teil eines solchen« gesprochen wird[1484] und lediglich in § 126b ausschließlich das Computersystem selbst tatbildlich erfasst wird. Da es diese offensichtliche ungleiche Ausdehnung der Tatobjekte in unterschiedlichen speziellen Computerdelikten gibt, ist auch davon auszugehen, dass die Tatobjekte, die sowohl ein Computersystem als auch Teile eines solchen beschreiben (zB § 118a Abs 1), tatsächlich weiter zu verstehen sind als lediglich das Tatobjekt »Computersystem« ohne weiteren Zusatz in § 126b Abs 1.

Doch zielen gerade DoS-Attacken überwiegend auf die Lahmlegung von Diensten – iSv diversen Computerprogrammen, wie zB Webservices oder E-Mail-Diensten[1485] – ab, die auf einem Server ausgeführt werden. Der Server selbst ist in solchen Fällen nicht das eigentliche Angriffsziel. Wird nun zB bloß ein derartiger (Software-)Dienst angegriffen und daher lediglich dessen Funktion bzw ordnungsgemäßer Betrieb schwer gestört, nicht aber die Funktionsfähigkeit des Servers, stellt sich die Frage, ob der objektive Tatbestand des § 126b in einem derartigen Fall überhaupt erfüllt ist.

Unter Berücksichtigung der Legaldefinition des § 74 Abs 1 Z 8, die im Wesentlichen auf der Vorgabe des Art 1 lit a CCC beruht und ein Computersystem als sowohl einzelne als auch verbundene Vorrichtungen, die der automationsunterstützten Datenverarbeitung dienen, definiert, gelangt man jedoch zu dem Schluss, dass auch Computerprogramme als Vorrichtungen zur automationsunterstützten Datenverarbeitung in Betracht kommen und folglich als Computersysteme beurteilt werden können.[1486] Neben Hardware dienen auch Computer-

1484 Siehe etwa § 118a, § 126c Abs 1 Z 2.

1485 Man spricht hier auch von »Services«.

1486 Siehe ua auch Art 7 lit a des Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Angriffe auf Informationssysteme und zur Aufhebung des Rahmenbeschlusses 2005/222/JI des Rates, KOM (2010) 517 endg.

programme der elektronischen Datenverarbeitung, was zumindest zu einer Qualifikation als eine – mit Hardware – verbundene[1487] Vorrichtung führt. Das indiziert auch der Tatbestand des § 126c, der in Abs 1 Z 1 und Abs 2 von Computerprogrammen und vergleichbaren »solchen Vorrichtungen« spricht.[1488] Selbstständige datenverarbeitende »Teile eines Computersystems« sind somit, ohne sie im Tatbild explizit anzumerken, ohnehin bereits durch das Tatobjekt »Computersystem« tatbestandlich mitumfasst.

Diese sachgerechte Auslegung beruht aber zudem auf den GMat, in denen davon ausgegangen wird, dass eine DoS-Attacke einen Angriff darstellt, »der darauf abzielt, bestimmte Dienste[1489] oder auch einen gesamten Rechner zu blockieren, zB durch Herbeiführung einer Überlastungssituation von auf diesem Rechner implementierten Netzdiensten«.[1490] Auch der europäische Richtliniengeber will in diesem Zusammenhang mit Tatwerkzeugen Computerprogramme als »Vorrichtungen« verstanden wissen.[1491] Vom strafrechtlichen Begriff eines »Computersystems« nicht erfasst werden mE aber rein passive Daten wie zB nutzergenerierte Dateien bzw nicht selbstständig lauffähige und auch nicht mit (aktiven[1492]) Computerprogrammen verbundene unselbstständige Dateien. *Reindl-Krauskopf* erachtet Software, die in einem Computersystem abgespeichert wird, jedenfalls als »Teil« eines Computersystems, wenn sie verdeutlicht: »Was sich innerhalb des Systems befindet, installierte Hardware ebenso wie Daten, ist vielmehr als Teil des Systems anzusehen.«[1493] Darüber hinaus bescheinigt sie auch den »System- und Programmdateien« die Eignung als »Vorrichtung« iSd § 74 Abs 1 Z 8.[1494]

1487 Ohne einen entsprechenden Datenträger wäre keine Software lauffähig. Siehe zur wechselseitigen Abhängigkeit von Hard- und Software S 16.

1488 Siehe auch in der Lit zB *Nittel* in SbgK § 74 Rz 145.

1489 Bei Microsoft Betriebssystemen auch »Service« bezeichnet, im Unix-Umfeld gerne »Dämon« genannt.

1490 Vgl ErlRV 1166 BlgNR XXI. GP, 29.

1491 Siehe Art 7 lit a des Vorschlags für eine Richtlinie des Europäischen Parlaments und des Rates über Angriffe auf Informationssysteme und zur Aufhebung des Rahmenbeschlusses 2005/222/JI des Rates, KOM (2010) 517 endg, ABl C 2011/121, 25.

1492 »Aktiv« soll an dieser Stelle die Fähigkeit der programmgesteuerten, selbstständigen Abarbeitung von Handlungsanweisungen zur automationsunterstützten Datenverarbeitung beschreiben, die den »Computerprogrammen« innewohnt.

1493 Vgl *Reindl-Krauskopf* in WK²§ 118a Rz 8; weiters *Jerabek/Reindl-Krauskopf/Schroll* in WK² § 74 Rz 59.

1494 Vgl *Reindl-Krauskopf,* Computerstrafrecht², 12.

Eine schwere Funktionsstörung liegt daher auch dann vor, wenn lediglich Dritte (zB Internetnutzer) nicht auf veröffentlichte Daten zugreifen können, weil der Web-Dienst (iS eines Computersystems) eines Servers zum Absturz gebracht wurde, selbst wenn der Systeminhaber über die im System gespeicherten Daten weiterhin verfügen könnte. Die Möglichkeit des Systeminhabers, über die Daten zu verfügen, spielt für die Tatbestandsmäßigkeit des § 126b Abs 1 keine Rolle. Vielmehr kann diese aber für die Anwendbarkeit und den etwaigen Vorrang des § 126a ausschlaggebend sein. Dies mag zwar angesichts der grundsätzlich im Vermögensstrafrecht angesiedelten Strafbestimmung sonderbar anmuten, lässt sich aber aufgrund der Subsidiaritätsklausel des § 126b Abs 1 zu Gunsten des § 126a wohl letztlich doch schlüssig begründen.[1495]

Betrachtet man das Tatobjekt des § 126b Abs 1 genauer, so stellt man fest, dass nicht das Computersystem an sich gemeint ist, sondern dessen »Funktionsfähigkeit«. Die vom Gesetzgeber gewählte Terminologie ist diesbezüglich unpräzise, denn Art 5 CCC wie auch Art 4 Richtlinie 2013/40/EU stellen auf die »Funktionsweise« bzw den »Betrieb« eines Computersystems ab (arg »functioning«). Ein Computersystem, das durch einen DoS-Angriff derart lahmgelegt wird, dass das Antwortzeitverhalten dieses Systems (hins Netzwerkauslastung, Anfragendichte und Bearbeitungszeit des Servers) iS einer schweren Störung massiv verlängert wird, ist nämlich in seinem »Betrieb« bzw seiner »Funktionsweise« gestört, nicht aber in seiner generellen »Funktionsfähigkeit«. Unter der tatbildlichen »Funktionsfähigkeit eines Computersystems« ist daher konventions- und richtlinienkonform der »Betrieb« oder die »Funktionsweise« eines Computersystems zu verstehen.

3. Verfügungsberechtigter

Um den objektiven Tatbestand zu erfüllen, darf der Täter über das Tatobjekt nicht oder nicht allein verfügen dürfen. Ist der »Täter« alleiniger Verfügungsberechtigter über das Computersystem, dessen Betrieb er schwer stört, so entfällt der Tatbestand. Speichern mehrere Nutzer Daten, über die sie jeweils alleine verfügungsberechtigt sind, auf einem Computersystem, so impliziert dies nicht, dass diese Nutzer auch

1495 Siehe dazu gleich im Anschluss.

gleichzeitig Mitverfügungsberechtigte über das gesamte Computersystem sind. So können sich auch Computersysteme[1496] in Computersystemen befinden (zB in Form von unterschiedlichen Software-Diensten, die von einer gemeinsamen Hardware samt Systemsoftware gehostet werden), an denen jeweils andere (Verfügungs-)Berechtigungen haften. Freilich hängt die Feststellung einer Berechtigung an einem Computersystem auch stark davon ab, welchen konkreten Umfang die Berechtigungen des Nutzers aufweisen. Hat ein Nutzer lediglich Lese- bzw Ausführrechte und keinen Vollzugriff auf ein Computersystem in Form eines speziellen Software-Service (zB FTP-Dienst), so ist eine Verfügungsberechtigung iSd § 126b zu verneinen, sollte der Nutzer das serverseitige FTP-Programm löschen. In diesem Fall kann streng genommen auch nicht die »alleinige« Verfügungsberechtigung konstatiert werden, da der Täter hins der Löschung dieses Systems überhaupt keine Berechtigung besitzt.[1497]

4. Tathandlung

Tathandlung ist das schwere Stören der Funktionsfähigkeit bzw des Betriebs eines Computersystems, durch Eingabe oder Übermittlung von Daten. Daher erfüllt nicht jede Störung der Funktionsfähigkeit den Tatbestand und stellt strafrechtliches Unrecht dar, sondern nur eine solche, die durch Eingabe oder Übermittlung von Daten (iSd § 74 Abs 2) herbeigeführt wird. Diese Handlungsmodalitäten definieren die Art und Weise, wie die Funktionsfähigkeit des Computersystems schwer gestört werden muss. Es handelt sich daher bei § 126b um ein verhaltensgebundenes (Erfolgs-)Delikt.

a. Eingeben von Daten

Bei der Handlungsmodalität der Dateneingabe spielt es keine Rolle, wie die Daten ins Zielsystem eingegeben werden, also ob die Eingabe über Eingabegeräte des Zielsystems selbst oder durch einen Remote-Zugriff über ein Netzwerk erfolgt.[1498] Bei dieser Tathandlung müssen aber die – für die Funktionsstörung ursächlichen – Daten jedenfalls

1496 Zur Legaldefinition »Computersystem« siehe S 75 ff.
1497 Siehe ähnlich *Reindl-Krauskopf* § 126b Rz 7 (Stand Dezember 2008).
1498 Vgl auch *Reindl-Krauskopf* § 126b Rz 14.

im Zielsystem lokal »eingebracht« werden. So fällt auch das bloße Ausführen von Programmen, die zur schweren Funktionsstörung führen und im Zielsystem bereits vorhanden sind, unter die Tathandlung des Eingebens von Daten. Das Ausführen von Computerprogrammen erfordert grundsätzlich Anweisungen von außen. Derartige Anweisungen können sich in einem einfachen Mausklick wiederfinden oder aber aufwändige Timer- bzw bedingungsgesteuerte Trigger-Funktionalitäten darstellen, die ebenfalls innerhalb des Systems definiert werden müssen. Unbeachtlich ist allerdings, ob sich die letztlich für die Systemschädigung verwendeten Programme bereits vor Ort am System befinden (zB bei typischen Funktionalitäten eines Systems, wie etwa ein System durch einen Mausklick herunterzufahren) oder zuvor vom Täter ins System eingebracht wurden. Zur Realisierung der Tathandlung der Eingabe von Daten reicht es bereits aus, das System zwar – technisch betrachtet – ordnungsgemäß, aber unbefugterweise herunterzufahren.

Auch wäre etwa die Eingabe von bloßen Tastenkombinationen[1499], die zu einem Neustart[1500] eines Systems führen, unter diese Tathandlung zu subsumieren, sofern – wie später zu prüfen sein wird – daraus eine schwere Funktionsstörung des Systems resultiert.

Hier ist jedoch grundsätzlich zwischen den zwei Arten eines Neustarts zu unterscheiden, dem Warmstart und dem Kaltstart.[1501] Beim Warmstart wird das System durch eine entsprechende Programmanweisung des Betriebssystems über eine verkürzte Bootprozedur neu gestartet. Anders verhält es sich jedoch mit einem Kaltstart[1502], bei dem die Stromzufuhr des Systems durch die Betätigung eines I/O-Schalters[1503] oder durch Ziehen des Netzsteckers unterbrochen wird und erst durch erneutes Betätigen des Schalters die Stromversorgung wiederhergestellt wird. In diesem Fall werden keine Daten eingegeben, weshalb das Ziehen des Netzsteckers bzw jede manuelle Unterbrechung der Stromversorgung nicht unter die Tathandlungsbeschreibung des § 126b zu subsumieren ist. Ob eine derartige Handlung der Sachbe-

1499 Auch Shortcuts oder Hotkeys genannt.
1500 Vgl etwa unter MS-DOS das gleichzeitige Drücken der Tasten STRG, ALT und DELETE.
1501 Siehe dazu *Dembowski,* BIOS und Troubleshooting (2004) 482.
1502 Dieser führt zur vollständigen Neuinitialisierung des Systems.
1503 Ein-/Ausgabe bzw Input/Output-Schalter; vgl auch das Ziehen des Steckers der Stromversorgung des Netzteils eines Computersystems aus der Steckdose.

schädigung durch Unbrauchbarmachen nach § 125 unterzuordnen wäre, ist – mangels eines Angriffs auf die Sachsubstanz – wohl eher zweifelhaft.[1504] Lässt sich das Computersystem durch das bloße Einstecken des Netzsteckers in die Steckdose wieder starten und ordnungsgemäß benützen, wird wohl mangels eines ins Gewicht fallenden Aufwandes keine strafbare Sachbeschädigung, sondern noch eine bloße straflose Gebrauchsbehinderung vorliegen.[1505] Auch Schäden, die dadurch entstehen, dass das Computersystem eine bestimmte Zeit nicht verwendet werden konnte, sind keine Schäden an der Sache selbst und bleiben daher außer Betracht.[1506] Ist jedoch der Aufwand an Zeit und Mühe spürbar, da eventuell ein Techniker beauftragt werden oder das System durch den unvorhergesehenen Absturz ausschließlich manuell mit diverser Startparametrisierung in Betrieb genommen werden muss, so wäre eine Sachbeschädigung wieder denkbar. Nach gefestigter Rsp[1507] liegt eine Sachbeschädigung »nicht nur bei einer Verletzung der Sachsubstanz, sondern auch dann vor, wenn etwa ein wesentlicher Bestandteil entfernt wird, die Sache an sich aber unbeschädigt bleibt, jedoch erst durch einen entsprechenden Aufwand an Zeit und Arbeit wieder der eigentlichen Zweckbestimmung zugeführt werden kann«.

Differenzierter muss das Drücken der »Hardware-Reset«-Taste des Computersystems betrachtet werden, die meist neben dem I/O-Schalter am Gehäuse angebracht ist. Sie soll die Möglichkeit eines Neustarts dann bieten, wenn das Betriebssystem nicht mehr reagiert. Je nachdem, wie nun diese Taste konfiguriert ist[1508], ist jedoch bei modernen Systemen meist davon auszugehen, dass ein Neustart softwaregesteuert von der (sehr hardwarenahen) Firmware[1509], dem BIOS[1510], initiiert

---

1504 Siehe *Seiler* in SbgK § 125 Rz 48, der dies aus diesem Grund auch verneint; vgl auch *Schmölzer* in BMJ, Strafrechtliche Probleme der Gegenwart 1989, 195 (208 ff).

1505 Siehe dazu auch die Beispiele des Stromabschaltens bei einer Maschine in *Seiler* in SbgK § 125 Rz 48, der ausführt, dass mangels Angriffs auf die Substanz von einem Unbrauchbarmachen nicht gesprochen werden kann, und des Abschraubens eines Ventils von einer Dampfmaschine bei *Bertel* in WK² § 125 Rz 11; vgl auch *Schmölzer* in BMJ, Strafrechtliche Probleme der Gegenwart 1989, 195 (210).

1506 *Bertel* in WK² § 125 Rz 11 sowie *Bertel* in WK² § 126 Rz 27 mwN.

1507 Siehe idS OGH 07.09.1978, 12 Os 94/78; OGH 06.10.1983, 12 Os 120/83; OGH 23.06.1989, 16 Os 9/89; OGH 26.11.2009, 12 Os 79/09y.

1508 Bei neueren Systemen kann die Funktionalität dieser Taste im BIOS definiert werden.

1509 Vgl »in Hardware gegossene Software« bei *Schramm* in Jahnel/Schramm/Staudegger, Informatikrecht², 1 (5 f); weiters *Kersken,* IT-Handbuch⁵, 127.

1510 Siehe dazu *Kersken,* IT-Handbuch⁵, 127 ff; *Gumm/Sommer,* Informatik¹⁰, 61 f.

wird.[1511] Daher werden in diesem Fall durch das Drücken der Taste Daten eingegeben. Sollte die Taste hingegen lediglich die Stromversorgung des Systems unterbrechen, ohne dass durch die Betätigung der Reset-Taste eine Datenverarbeitung ausgelöst wird, so liegt wiederum keine Tathandlung iSd § 126b vor.[1512]

b. Übermitteln von Daten

Werden vom Täter keine Tätigkeiten innerhalb des Systems vorgenommen (wie zB bei der Eingabe eines »Shutdown-Befehls«), aber dennoch Daten an das Zielsystem gesendet[1513], die das System in seiner Funktionsweise schwer stören, so kann die Tathandlung der »Datenübermittlung« vorliegen. Dabei werden Daten(pakete) an das System gesendet, die entweder in der Lage sind Systemschwächen[1514] auszunutzen und dadurch Programmfehler zu erzeugen oder durch ihre massenhafte Übermittlung Überlastungssituationen schaffen, die sich auf die Funktionsfähigkeit des Systems auswirken. Allerdings weisen die GMat explizit darauf hin, dass nicht auch jedes »Spamming«[1515] von dieser Strafnorm erfasst sein soll.[1516] Es muss sich somit um »erhebliche« Fälle einer »schweren« Störung des Computersystems handeln. Solche schweren Fälle könnten jedoch iZm »Spamming« iVm sog »Mail-Bombs«[1517] vorliegen. Dabei werden vielfach E-Mails an einen Mail-Server versendet, um den E-Mail-Dienst lahmzulegen bzw zum Absturz zu bringen oder das E-Mail-Postfach des Nutzers zu blockieren. Das heißt, es sind auch Übermittlungen tatbildlich, die in ihrer Einzelform sozial adäquate und technisch übliche Anfragen an einen Server darstellen und ggf auch Systemprozesse auslösen und entspre-

---

1511 Siehe Warmstart.

1512 Siehe Kaltstart.

1513 Der Begriff »übertragen« wäre wohl an dieser Stelle nicht ganz zutreffend, da die Daten eben nicht ins System eingebracht werden müssen. Vielmehr reicht es aus, wenn Daten an das Zielsystem adressiert sind.

1514 Siehe dazu die beschriebenen DoS-Methoden wie zB »SYN-Flooding«, »Land-Attack« oder »Out-of-band« S 291 ff.

1515 Spamming soll daher weiterhin nur als Verwaltungsübertretung geahndet werden (vgl ErlRV 1166 BlgNR XXI. GP, 29).

1516 Siehe ErlRV 1166 BlgNR XXI. GP, 28 f.

1517 Dabei geht es nicht um die Verbreitung von unzulässiger Werbung, sondern gezielt um das Schaffen einer Überlastungssituation am Zielsystem oder das beharrliche Belästigen/Verfolgen eines Opfers im Wege des Cyber-Stalking (siehe dazu S 546 ff).

chende Ressourcen binden können (zB E-Mails und Ping-Requests[1518]). Dies auch dann, wenn entsprechende Datenpakete mehrfach mit sehr geringen zeitlichen Abständen versendet werden, um eine schwere Störung der Funktionsfähigkeit eines Computersystems herbeizuführen. Ob es am betroffenen Server hins der an ihn adressierten Datenpakete überhaupt zu einer systeminternen Datenverarbeitung kommt, ist irrelevant. Ebenso spielt der Inhalt der Daten, die für die Herbeiführung einer Funktionsstörung übermittelt werden, für die Deliktsverwirklichung keine Rolle.

Grundsätzlich muss die schwere Funktionsstörung unmittelbar durch die Dateneingabe oder -übermittlung verursacht werden. Das Unmittelbarkeitserfordernis darf aber idZ nicht allzu eng verstanden werden. Dies betrifft in erster Linie technische Zusammenhänge, wie bspw, dass eine Dateneingabe zunächst lediglich zu einer Datenveränderung im System führen kann, welche wiederum erst in weiterer Folge die Funktionsstörung bewirkt.[1519] Als Beispiel sei die Implementierung von »Computerviren«, »Computerwürmern« oder »logischen Bomben« genannt. Diese Schadprogramme bewirken je nach Konzeption zunächst Datenmanipulationen (wie zB Datenlöschungen oder -veränderungen) im Zielsystem. Erst die derartigen Beeinträchtigungen des Datenbestands führen schlussendlich zur schweren Funktionsstörung, was aber ebenfalls zur Verwirklichung des § 126b führt.

Nicht nur der Totalabsturz eines Computersystems oder eine massive Verlangsamung iS eines Quasi-Stillstands stellen eine schwere Funktionsstörung dar. So handelt es sich grundsätzlich ebenso um eine schwere Störung, wenn Programmabläufe manipuliert, Programme gelöscht oder Zugriffssperren unbefugterweise errichtet werden, sodass dadurch das Computersystem (bzw Programm) nicht mehr in der Lage ist, ordnungsgemäß zu funktionieren und ausgewählte Funktionen faktisch »stillstehen« oder überhaupt zum Absturz gebracht werden.

Gibt der Täter einen einmaligen »Befehl« zum Absturz des Computersystems ein (arg »Eingeben von Daten«), so ist mit Eintritt der schweren Funktionsstörung (zB des Systemabsturzes) das (einmalige) tatbestandliche Verhalten des Täters beendet und auch das Delikt formell vollendet. § 126b kann jedoch auch als (verhaltensgebundenes) Dauerdelikt begangen werden. Übermittelt der Täter etwa im Zuge eines

1518 Anfragen, ob ein Server im Netzwerk verfügbar, sprich »online«, ist.
1519 Siehe dazu auch die Bedenken von *Reindl-Krauskopf* in WK² § 126b Rz 16.

DDoS-Angriffs permanent Datenpakete an das Zielsystem, um die schwere Funktionsstörung aufrechtzuerhalten, so ist zwar das Delikt mit Beginn der Funktionsstörung formell vollendet, materiell beendet aber erst, wenn der Täter mit der Übersendung der Datenpakte aufhört und dadurch die Funktionsfähigkeit wieder hergestellt wird. Durch das anhaltende Übermitteln von das Zielsystem schwer störenden Datenpaketen wird ein rechtswidriger Zustand geschaffen, den der Täter in der Folge durch fortdauerndes Tun solange aufrecht hält – weshalb auch der Tatbestand ununterbrochen weiter verwirklicht wird – bis der Störvorgang tatsächlich seine Beendigung findet.[1520] Ebenso wäre § 126b Abs 1 bei DDoS-Attacken als Dauerdelikt verwirklicht, wenn der Täter es nach einem einmaligen Tun – zB dem Starten einer automatisierten DoS-Attacke[1521] – in weiterer Folge fortdauernd unterlässt, den Angriff, bspw durch Eingabe eines Beendigungsbefehls des DoS-Programms[1522] – zu stoppen.[1523] Dies hat zur Konsequenz, dass etwa eine strafbare Beteiligung iSd § 12 so lange möglich ist, bis der rechtswidrige Zustand – dh die schwere Funktionsstörung – beendet ist.

Dies gilt freilich auch für die Qualifikationsnorm des § 126b Abs 2 Fall 1. Sie wird solange verwirklicht, wie ein tatbildliches Verhalten gesetzt wird, wobei die Begehungsweisen des Grunddelikts in Anbetracht dieser Deliktsqualifikation erst dann formell vollendet sind, wenn die erforderliche »längere Zeit« der Störung der Funktionsfähigkeit abgelaufen ist. Es wird daher lediglich der Vollendungszeitpunkt zeitlich zurückverschoben. Solange dieser noch nicht erreicht ist, kommt grundsätzlich Versuch in Betracht. Unterlässt es der Täter darüber hinaus aber in weiterer Folge den Angriff zu beenden, obwohl er dies könnte, und hält er dadurch den rechtswidrigen Zustand aufrecht, verwirklicht er § 126b Abs 1 Fall 1 als Dauerdelikt. Das tatbestandsmäßige Verhalten dauert in diesem Fall ab erstmaliger formeller Vollendung (Überschreitung der qualifikationsbegründenden Zeitspanne) bis zur materiellen Beendigung (Ende der Funktionsstörung) kontinuierlich an.

1520 Siehe dazu auch den besonderen Erschwerungsgrund des § 33 Abs 1 Z 1 letzter Fall im Bereich der Strafzumessung.

1521 Siehe dazu oben.

1522 Vgl das DoS-Programm LOIC (Low Orbit Ion Cannon), mit dem man nach Eingabe der konkreten IP-Adresse des Zielsystems einen DoS-Angriff per Knopfdruck initiieren und auch wieder beenden kann (siehe *Wikipedia,* <de.wikipedia.org/wiki/Low_Orbit_Ion_Cannon> [01.04.2014]).

1523 Vgl dazu *Schmoller* in SbgK § 99 Rz 15.

5. Störung der Funktionsfähigkeit eines Computersystems und Schadensermittlung

Als geschütztes Rechtsgut wird – analog zur Datenbeschädigung (§ 126a) – die »ungestörte Verwendbarkeit des Computersystems« angesehen, die einen Vermögenswert darstellt.[1524] Insoweit kann im Verhältnis zur Datenbeschädigung (§ 126a) – trotz ausdrücklicher Subsidiarität des Grunddelikts (§ 126b Abs 1) – auf eine Vorverlagerung des Rechtsgüterschutzes geschlossen werden, da § 126a auf die Daten und § 126b auf das diese verarbeitende Computersystem fokussiert. Die Vermögensbeeinträchtigung (Taterfolg) liegt neben einem wirtschaftlichen Schaden am System vor allem aber im Gebrauchsinteresse. Aufgrund der Gleichwertigkeit, was das Schutzbedürfnis von Computersystemen anlangt, kann auch eine E des deutschen Bundesverfassungsgerichts – zwar iZm Online-Zugriffen – für eine Interpretationsanleihe im hier vertretenen Sinn herangezogen werden. Bemerkenswert ist nämlich, dass dort erstmals von einem aus dem allgemeinen Persönlichkeitsrecht (Art 2 Abs 1 iVm Art 1 Abs 1 GG) abgeleiteten Grundrecht auf »Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme« gesprochen wird.[1525] In eine solche Richtung bewegt sich aber wohl auch der österr (historische) Gesetzgeber, wenn in den GMat zu dieser Strafbestimmung erläutert wird, dass es nicht auf einen schweren Schaden ankomme, sondern auf eine schwere Störung der Funktionsfähigkeit.[1526] So auch *Maleczky,* der dazu ausführt, dass ein Schaden am Vermögen für die Vollendung im Gegensatz zu § 126a nicht einzutreten braucht, was die Einordnung dieses neuen Deliktes im Vermögensstrafrecht fragwürdig erscheinen lässt.[1527] Ein etwaiger (finanzieller) Aufwand, der zur Wiederherstellung eines ordnungsgemäß lauffähigen Computersystems erbracht werden muss, kann auch nach *Öhlbäck/Esztegar* bloß als ergänzendes Beurteilungskriterium für den Erfolgseintritt herangezogen werden.[1528]

1524 Siehe *Daxecker* in SbgK § 126b Rz 11 (Stand Mai 2012); *Reindl-Krauskopf* in WK² § 126b Rz 5.

1525 BVerfG 27.02.2008, 1 BvR 370/07.

1526 Vgl ErlRV 1166 BlgNR XXI. GP, 29.

1527 Vgl *Maleczky,* JAP 2002/2003, 115.

1528 Siehe *Öhlbäck/Esztegar,* Rechtliche Qualifikation von Denial of Service Attacken, JSt 2011, 126.

Einen wesentlichen Kritikpunkt stellt die ausdrückliche Subsidiarität iVm dem unterschiedlichen »Schadensbegriff« der beiden Bestimmungen dar. So bemisst sich der Vermögensschaden[1529] in § 126a am Wiederherstellungsaufwand bzw den Anschaffungs- oder Herstellungskosten der beeinträchtigten Daten, wohingegen § 126b prinzipiell nicht auf die Schwere des Schadens, sondern auf die Schwere der Störung der Funktionsfähigkeit des Computersystems abstellt.[1530]

Wie die »Schwere« einer derartigen Funktionsstörung bewertet wird, ist derzeit äußert strittig.

Nach *Reindl-Krauskopf* kann sich die »Schwere« der Störung durch den Aufwand ergeben, der notwendig ist, um die volle Funktionsfähigkeit des Systems wiederherzustellen.[1531] Sie konstatiert das Vorliegen einer schweren Störung jedenfalls bei einem Wiederherstellungsaufwand von mehr als € 1.000,–.[1532]

Meines Erachtens soll jedoch lediglich der faktische Zustand eines gestörten Computersystems als Anhaltspunkt herangezogenen werden, was auch in den GMat dadurch zum Ausdruck gebracht wird, dass es bei § 126b nicht auf die Schwere des Schadens, sondern auf die Schwere der Störung ankomme.[1533] Dadurch wird aber zudem der subjektive Gebrauchswert der Sache in den Vordergrund gerückt. In den Erl wird dazu klargestellt, dass es »auf die Schwere der tatsächlich beeinträchtigten (oder gefährdeten) Interessen des Opfers zur Herstellung der Tatbildlichkeit nicht ankommt, weil eben (nur) auf eine schwere Störung der Funktionsweise eines Computersystems, hingegen nicht auf einen schweren Schaden durch eine Störung der Funktionsweise eines Computersystems abgestellt wird.«[1534] Schwer ist eine Störung somit mE immer auch dann, wenn das System durch das Eingeben oder Übermitteln von Daten dermaßen gestört wird, dass der Betrieb einen Quasi-Stillstand erreicht. Auf den Aufwand zur Wiederherstellung eines störungsfreien Zustandes kommt es nicht an. So kann ein beeinträchtigtes Computersystem in vielen Fällen durch einen simplen Neustart wieder entstört und ordnungsgemäß in Betrieb genom-

1529 Siehe ausf S 273 ff.
1530 Siehe ErlRV 1166 BlgNR XXI. GP, 29.
1531 Vgl *Reindl-Krauskopf* in WK² § 126b Rz 12.
1532 Siehe *Reindl-Krauskopf,* Computerstrafrecht², 34; *Reindl-Krauskopf* in WK² § 126b Rz 12.
1533 Vgl erneut ErlRV 1166 BlgNR XXI. GP, 29.
1534 Siehe ErlRV 1166 BlgNR XXI. GP, 29.

men werden, was für einen vernünftig denkenden Menschen keinen bzw kaum[1535] einen ins Gewicht fallenden Aufwand darstellen würde. Der angesprochenen Argumentation[1536] *Reindl-Krauskopfs* folgend würden derartige Fälle mangels Erreichung der von ihr vorgeschlagenen Wertgrenze von mehr als € 1.000,– Wiederherstellungsaufwand überhaupt nicht von § 126b erfasst werden, was aber mE nicht der Intention dieser Regelung entspricht. Auch im Beispielsfall, in dem sich die Störung des Systems durch einen bloßen Neustart beheben ließe, könnte – unabhängig vom Wiederherstellungsaufwand – eine schwere Funktionsstörung vorliegen, wenn das System zB zum Absturz gebracht worden wäre oder nur mehr so langsam arbeiten würde, dass an eine ordnungsgemäße Verwendbarkeit nicht mehr zu denken ist. Die »Schwere« einer Störung ist daher nicht mit einer geldwerten Minderung des Vermögens festzumachen, sondern mit der faktischen Nicht-Verwendbarkeit des Systems.

Freilich muss eine solche anhand objektiver Kriterien ermittelt werden. Man wird dafür eine dynamische Beurteilung iSd eines »beweglichen Systems« heranziehen müssen, das die Ausgestaltung des konkreten Angriffs, das Ausmaß der Störung, der technische und zeitliche Behebungsaufwand usw berücksichtigt.

Das geschützte Rechtsgut ist in der Verwendbarkeit des Computersystems (»Gebrauchsinteresse«) und daher im Computersystem selbst auszumachen.[1537] In Anlehnung an ein »Informationsinteresse der Allgemeinheit (Internet) bzw der Nutzer (Intranet)«, wäre an dieser Stelle – neben einem etwaigen »Vermögensinteresse« des Systeminhabers – das Interesse von Dritten zu nennen, die auf zulässigerweise veröffentlichte Informationen auf einem Computersystem zugreifen wollen und in festgelegter Form auch dürfen. In Anbetracht eines solchen Universalrechtsguts sollte ein Qualifikationstatbestand in Erwägung gezogen werden, der – wie zB bei § 126a bereits angemerkt – iZm DoS-Attacken auf besonders schutzwürdige Systeme Bedacht nimmt, die »von wesentlicher Bedeutung für die Aufrechterhaltung grundlegender gesellschaftlicher Funktionen, der Gesundheit, der Sicherheit

1535 Man denke an einen Techniker, der ggf eine Stunde für eine derartige Tätigkeit in Rechnung stellen würde.

1536 Vgl *Reindl-Krauskopf,* Computerstrafrecht², 34; *Reindl-Krauskopf* in WK² § 126b Rz 12.

1537 Siehe *Reindl-Krauskopf* in WK² § 126b Rz 5.

und des wirtschaftlichen oder sozialen Wohlergehens der Bevölkerung sind«[1538], zB Stromversorgungsanlagen, Kommunikationsinfrastrukturen, Verkehrsleitsysteme, Flugsteuerungssysteme, Kraftwerke, medizinische Notversorgungsanlagen, Gaspipelines, diverse Systeme zur Landesverteidigung (Radarstationen, Waffensysteme usw) uÄ.

Hätte der Gesetzgeber tatsächlich ausschließlich auf einen Vermögensschaden iSd § 126a abstellen wollen, so wäre es nahegelegen, auf eine ähnliche Formulierung wie in § 126a Abs 1 zurückzugreifen, etwa »Wer einen anderen dadurch schädigt, …]«. In diesem Sinn betonen auch *Öhlbäck/Esztegar,* dass das Ausmaß des Schadens nur als ergänzendes Beurteilungskriterium herangezogen werden könne und eine Festlegung einer starren Wertgrenze für die Höhe des Schadens wenig hilfreich sei.[1539]

Einen weiteren Anhaltspunkt für diese Auslegung liefert die Deliktsqualifikation des § 126b Abs 2[1540], da dort keine – wie bei Vermögensdelikten überwiegend übliche – »Wert- bzw Schadensqualifikation«[1541] vorgenommen wurde, sondern in Abs 2 erster Fall die Herbeiführung einer schweren Störung dann schwerer bestraft wird, wenn diese »längere Zeit andauert«[1542]. Daraus folgt, dass die Formulierung der Qualifikationsnorm des Abs 2 erster Fall darauf schließen lässt, dass ein eigenständiges, über den reinen Vermögensaspekt hinausreichendes Rechtsgut[1543], nämlich das Interesse an der Verfüg- und Verwendbarkeit des Computersystems, zumindest auch geschützt werden soll.

1538 Vgl auch ErwG 4 RL 2013/40/EU.

1539 Vgl *Öhlbäck/Esztegar,* JSt 2011, 126.

1540 Zur genaueren Analyse des Abs 2 siehe gleich im Anschluss.

1541 Zu Wert- und Schadensqualifikationen im Vermögensstrafrecht siehe instruktiv *Hochmayer,* Wert- und Schadensqualifikationen versus Regelbeispiele, in Joerden/Scheffler/Sinn/Wolf (Hrsg), Vergleichende Strafrechtswissenschaft, FS Swarc (2009) 235 (235 ff).

1542 Im Gegensatz zu dieser vergleichbaren Begrifflichkeit bei § 107a Abs 2, wo sie Bezug auf die Tathandlung nimmt, ist sie bei § 126b Abs 2 erster Fall für den Erfolg maßgeblich.

1543 Dies betrifft sowohl Individual- als auch Kollektivrechtsgüter wie zB das Interesse der Allgemeinheit 1.) auf einen öffentlichen Server zuzugreifen bspw zur Abfrage der Edikts- und Insolvenzdatei (<www.edikte.justiz.gv.at/> [01.04.2014]) oder der authentischen Kundmachung von Normen im RIS, 2.) an der Funktionsfähigkeit von besonders schutzwürdigen Systemen (Stromversorgungsanlagen, Kommunikationsinfrastrukturen, Verkehrsleitsysteme, Flugsteuerungssysteme, Kraftwerke, medizinische Notversorgungsanlagen, Gaspipelines, Landesverteidigungssysteme usw).

Man könnte darin eine »Qualifikationsnorm hins der Beeinträchtigung des Affektionsinteresses« erblicken.

Wie bereits oben näher ausgearbeitet führt ein unbestimmter – äußerst interpretationsbedürftiger – Zeitfaktor zu einer qualifizierten schweren Störung der Funktionsfähigkeit eines Computersystems, nicht aber die Höhe des Schadens oder der Wert einer Sache. Ein fixes Zeitmaß ist nicht angegeben, was eine Konstatierung der Deliktsqualifikation in objektiver, aber vor allem auch in subjektiver Hinsicht erschwert. Dies rührt daher, dass nach den GMat bereits bei der »einfachen« schweren Störung im Grunddelikt die Dauer der Störung eine gewisse Relevanz besitze.[1544] *Öhlbäck/Esztegar* sind allerdings der Meinung, dass es im Grunddelikt nicht auf die Zeitdauer der Störungshandlung ankomme.[1545]

Für die Beurteilung einer längere Zeit andauernden Störung ist mE – wie bereits bezüglich des Grunddelikts – eine »dynamische Betrachtung« indiziert, die verschiedene Faktoren berücksichtigt. Dass die schwere Störung an einem Wochenende verursacht wurde, der Systemverantwortliche auf Urlaub ist oder ein vom Systemberechtigten beauftragter Techniker aufgrund seiner geschäftlichen Auslastung erst nach ein paar Tagen die Störung beheben kann, darf freilich nicht zur Erfüllung des Qualifikationstatbestandes führen.

Das umstrittene Verhältnis von § 126b und § 126a entsteht mE vor allem dadurch, dass einerseits beiden Delikten, aufgrund ihrer systematischen Positionierung und der zumindest ausdrücklich in § 126a Abs 1 verlangten tatbildlichen Schädigung[1546], das Rechtsgut »Vermögen« zu Grunde liegt. Andererseits wird aber auch mit § 126a das »Interesse am Fortbestand und an der Verfügbarkeit der Daten«[1547] bzw mit § 126b das Interesse an der Verwendbarkeit[1548] des Computersystems[1549] im Schrifttum genannt, weshalb sich der Schutzmantel dieser Bestimmungen über das Vermögen hinaus auch abstrakt über das Rechtsgut »Privatsphäre« ausbreitet.[1550]

1544 Vgl ErlRV 1166 BlgNR XXI. GP, 29; siehe auch ErlRV 285 BlgNR XXIII. GP, 8.
1545 Siehe *Öhlbäck/Esztegar,* JSt 2011, 126.
1546 Siehe dazu auch den Vergleich zur Sachbeschädigung in JAB 359 BlgNR XVII. GP, 17.
1547 *Triffterer* in SbgK § 126a Rz 21 (aF Stand Dezember 1992).
1548 Im Sinne einer uneingeschränkten Verwendbarkeit des Systems und seiner installierten Dienste (»Schutz der Systemintegrität«).
1549 Siehe dazu auch *Reindl-Krauskopf* in WK² § 126b Rz 5.
1550 Siehe ähnlich *Seling,* Privatsphäre, 82.

6. Subjektive Tatseite

Der Täter muss im Mindeststärkegrad eines dolus eventualis mit Tatbildvorsatz, der sich auf sämtliche objektiven Tatbestandsmerkmale bezieht, handeln. Er muss somit auch in seinen Vorsatz aufnehmen, dass sein Angriff das Computersystem schwer stört.

7. Problemfelder: Subsidiaritätsklausel und Deliktsqualifikation

Da § 126a bereits Datenbeschädigungshandlungen erfasst, wurden in § 126b lediglich die Tathandlungen des Eingebens und Übermittelns von Daten aufgenommen, die nicht zwingend zu einer Datenbeschädigung iSd § 126a führen.[1551] In der Praxis sind Anwendungsfälle – soweit überschaubar – nicht auszumachen, denn die schwere Störung der Funktionsfähigkeit eines Computersystems impliziert stets auch eine kurz oder lang andauernde Datenunterdrückung, die eben grundsätzlich (bei entsprechendem Vorsatz und auch schon im Versuchsstadium[1552]) von § 126a erfasst wird.[1553] Nach den GMat ist ein Computersystem nämlich dann schwer gestört, wenn es völlig lahmgelegt oder so verlangsamt wird, dass der verbleibende Gebrauchswert des Systems nicht wesentlich höher liegt als bei einem Stillstand[1554], was sich in beiden Fällen auch auf die Verfügbarkeit der gespeicherten Daten auswirkt. Die Auslagen, die zur Wiederherstellung bzw Verfügbarkeit der Daten aufgebracht werden müssen, stellen einen Schaden nach § 126a dar. Aufgrund der ausdrücklichen Subsidiarität des § 126b zu § 126a würde in derartigen Fällen stets § 126a zur Anwendung gelangen.[1555]

Die Qualifikationsbestimmung des § 126b Abs 2 StGB enthält in ihrem Wortlaut keine Subsidiaritätsklausel. Es fragt sich daher, ob und allenfalls wie sich die Subsidiaritätsklausel des Abs 1 auf das Konkurrenzverhältnis des § 126b Abs 2 mit § 126a auswirkt. Anhand zweier

---

1551 Vgl *Reindl-Krauskopf* in WK² § 126b Rz 4; vgl auch ErlRV 1166 BlgNR XXI. GP, 28; weiters ErlStV 1645 BlgNR XXIV. GP, 4.

1552 Insbesondere dann, wenn der Vermögensschaden zB durch das Vorliegen von aktuellen Sicherungskopien ausbleibt.

1553 Siehe auch *Bertel/Schwaighofer,* BT I¹² § 126b Rz 2.

1554 Vgl ErlRV 1166 BlgNR XXI. GP, 29.

1555 In diesem Sinne *Öhlbäck/Esztegar,* JSt 2011, 126.

durchaus praxisrelevanter Beispielsfälle soll diese Problemstellung erörtert werden:

Fall 1: Ein technisch versierter Täter löscht lediglich eine einzige Systemdatei des Zielsystems mit dem Vorsatz, dem Opfer durch diese Schädigungshandlung nur einen geringen Schaden zuzufügen. Ihm ist bekannt, dass sich der Aufwand der Systemwiederherstellung für einen Techniker (zB Reparatur bzw Neuinstallation des Betriebssystems) im finanziellen Rahmen unter € 3.000,– (vgl erste Wertqualifikation des § 126a Abs 2) hält.[1556] Durch die Eingabe des Löschbefehls wurden auch die Tatbestände des § 126b Abs 1 und Abs 2 verwirklicht, da die dadurch bewirkte Störung der Funktionsfähigkeit über eine »längere Zeit angedauert« hat, was auch im Vorsatz enthalten war (zB sogar beabsichtigt wurde). Trotz Einordnung dieser beiden Delikte bei den Vermögensdelikten und der Ähnlichkeit der weiteren von ihnen geschützten Rechtsgüter (wie das Interesse am Fortbestand und an der Verfügbarkeit der Daten bzw das Interesse an der Verfügbarkeit des Systems) liegen den Bestimmungen unterschiedliche Schadensbegriffe zugrunde. So bemisst sich der Vermögensschaden in § 126a – wie oben gezeigt – idR am Wiederherstellungsaufwand der beeinträchtigten Daten, wohingegen § 126b nicht auf die Schwere des Schadens, sondern auf die Schwere der (technischen) Störung abstellt.[1557]

Komenda/Madl lassen in diesem Fall die Subsidiaritätsklausel auch auf § 126b Abs 2 wirken, weshalb der Täter in diesem Beispielsfall nur nach § 126a Abs 1 zu bestrafen wäre.[1558]

Fall 2: Wie Fall 1, nur dass hier trotz Vornahme der Datenlöschung der Vermögensschaden ausbleibt, weil das Opfer die betroffenen Informationen, die auch noch von anderen Daten repräsentiert werden, an einem anderen Speicherort vorrätig hat (vollständige und aktuelle Sicherungskopien). Der Aufwand der Wiederherstellung fällt idR nach hM für einen vernünftig denkenden Menschen nicht ins Gewicht[1559], weshalb nur eine Versuchsstrafbarkeit bezüglich § 126a Abs 1 indiziert ist. Tatsächlich werden aber sowohl eine versuchte Datenbeschädi-

1556 Ähnliche Beispielsfälle, die in den hier angesprochenen Problembereich fallen, lassen sich etwa durch einfach konzipierte Ransomware (vgl »Polizei-Virus«), (DoS-)Angriffe mittels buffer-overflow im Zielsystem (zB Teardrop, SYN-Flooding, Ping-of-Death) udgl konstruieren.

1557 Vgl ErlRV 1166 BlgNR XXI. GP, 29; auch *Öhlbäck/Esztegar,* JSt 2011, 126.

1558 Siehe *Komenda/Madl* in SbgK § 126a Rz 90 f.

1559 Vgl richtungsweisend bereits *Reindl,* E-Commerce, 104.

gung (§§ 15, 126a Abs 1) als auch eine vollendete qualifizierte Störung der Funktionsfähigkeit eines Computersystems (§ 126b Abs 1, Abs 2 erster Fall) verwirklicht. Man stößt hier zudem auf einen auffälligen Aspekt der Figur des »qualifizierten Versuchs«[1560]. § 126b Abs 2 erster Fall würde – bei Ausdehnung der Subsidiaritätsklausel des § 126b Abs 1 auch auf Abs 2 – kraft gesetzlicher Anordnung hinter den »einfachen Versuch« der Datenbeschädigung zurücktreten. Tritt nun aber der Täter vom Versuch der Datenbeschädigung zB aufgrund des materiellrechtlichen Grunds der »Tätigen Reue« (§ 167) oder ggf des »Rücktritts vom Versuch« (§ 16) strafbefreiend zurück, entfällt die Sperrwirkung der Subsidiaritätsklausel und der strengere (gleichzeitig verwirklichte aber bislang verdrängte) Qualifikationstatbestand des § 126b Abs 2 erster Fall lebt auf.[1561]

Dies hat den kriminalpolitisch bizarren Effekt, dass der »verdienstlich« handelnde und sich quasi »selbstresozialisierende« Täter, der vom Versuch zurücktritt, strenger bestraft wird als derjenige, der an seinem Vorhaben festhält.

Unter Rückgriff auf den interpretativen Methodenkanon soll nunmehr die Reichweite der Subsidiaritätsklausel des § 126b Abs 1 verdeutlicht werden.

Streng nach dem Wortlaut interpretiert, bezieht sich die Subsidiaritätsklausel ausdrücklich auf die in § 126b Abs 1 umschriebene Tat. Bei der »Tat« handelt es sich um einen konkreten Lebenssachverhalt, der unter die gesetzliche Kategorie der in § 126b Abs 1 abstrakt formulierten strafbaren Handlung fällt, welche wiederum den sog »Unrechtstatbestand« bildet. Die Subsidiaritätsklausel, die nur das Konkurrenzverhältnis dieses zu einem anderen, verdrängenden Delikt (hier § 126a) zum Gegenstand hat, steht – ebenso wie die Rechtsfolgenseite des Abs 1 – außerhalb des Unrechtstatbestands, da sie in ihrer Formulierung selbst auf »die Tat« verweist und folglich auch nicht Teil der Tat bzw der normierten strafbaren Handlung sein kann. Sie ist lediglich der Tatbestandsperipherie und daher dem sog »Gesamttatbestand« zugehörig und dient dazu, bei einer (partiellen) Überlappung von »Typen« – zB § 126a Abs 1 und 2 sowie § 126b Abs 1 – die Konkurrenzsituation ausdrücklich aufzulösen. In § 126b Abs 2 findet sich nun keine

1560 Vgl allgemein *Kienapfel/Höpfel/Kert,* AT[14], Z 23 Rz 22; va *Burgstaller,* Die Scheinkonkurrenz im Strafrecht (I), JBl 1978, 459.

1561 Siehe anstatt vieler *Fuchs,* AT I[8], Rz 31/9; va *Burgstaller,* JBl 1978, 459.

Subsidiaritätsklausel. Auch existiert außerhalb des § 126b Abs 1 und Abs 2 keine positivierte Regel, die Anhaltspunkte für ein bestimmtes Rangverhältnis von § 126b und § 126a gibt.

Damit lässt sich im Rahmen (zumindest) einer sprachlichen Konvention klar aus dem Wortlaut ableiten, dass sich der Qualifikationstatbestand zB des § 126b Abs 2 erster Fall mit seiner zusätzlichen Unrechtsanforderung »längere Zeit andauernde Störung« expressis verbis bloß auf »die Tat« bezieht, die unter die Handlungsbeschreibung des Abs 1 fällt. Es besteht kein genereller Verweis auf Abs 1, der die dortige Subsidiaritätsklausel mitumfassen würde. Und damit schlagen die Rechtfolgenseiten des § 126b Abs 1 und die Subsidiaritätsanordnung, die nicht zum verwiesenen Unrechtstatbestand gehören, nicht auf den Qualifikationstatbestand durch. Dies ergibt sich methodologisch aus einer Interpretation und nicht aus einer teleologischen Reduktion[1562]. Die Strafdrohung der qualifizierten schweren Störung der Funktionsfähigkeit eines Computersystems nach § 126b Abs 2 erster Fall ersetzt bei dessen Tatbestandserfüllung die Rechtsfolgenseite des Grunddelikts (einschließlich der normierten Subsidiaritätsanordnung), weil nun durch eine zusätzliche, schwerer wiegende tatbestandliche Anforderung (längere Zeit andauernde Störung) auch eine speziellere Tat vorliegt, die strenger zu bestrafen ist. Anders als bei »absatzintegrierten Qualifikationen« (wie etwa § 126a Abs 2) hat sich der Gesetzgeber im Fall des § 126b für eine Aufgliederung in zwei getrennte Absätze entschieden, was nach dem Wortlaut klar gegen die Übernahme der Subsidiaritätsanordnung des Grunddelikts in § 126b Abs 2 spricht. Würde der Gesetzgeber die Subsidiaritätsklausel des Abs 1 auch auf den Qualifikationstatbestand anwendbar wissen wollen, ließe sich dies – unmissverständlich – in einem eigenen Absatz (zB Abs 3) bezüglich der Absätze 1 und 2 festlegen (vgl § 94 Abs 4, § 107b Abs 5, § 278d Abs 2, § 308 Abs 5). Erst dadurch würde die Reichweite der Subsidiaritätsklausel im Gesamttatbestand des Strafgesetzes – dem klaren Wortlaut nach – auch das Verhältnis der Qualifikationsbestimmung (§ 126b Abs 2) zu § 126a mitbestimmen.

Darüber hinaus ergibt sich dieser Anwendungsbereich der Subsidiaritätsklausel nicht nur aus dem Wortlaut und einer systematischen Interpretation, sondern auch aus teleologischen Erwägungen, da (die

1562 Insoweit im Ergebnis generell unrichtig und – die »teleologischen Erwägungen« betreffend – missverstanden von *Komenda/Madl* in SbgK § 126a Rz 91.

Ergebnisse von oben prägnant zusammengefasst) einerseits die beiden Delikte des § 126a und § 126b auf verschiedene Schutzobjekte fokussieren (Daten versus Systeme)[1563], unterschiedliche Stadien[1564] und Intensitäten[1565] der Rechtsgutsbeeinträchtigung behandeln sowie differierende Handlungsweisen[1566] erfassen (zB ausschließlich computerspezifische Tathandlungen in § 126b). Andererseits ergibt sich bereits aus der Strafdrohung des Qualifikationstatbestands des § 126b Abs 2 erster Fall im Vergleich zu der des mitverwirklichten § 126a Abs 1, dass der Unwert ein ungleich höherer sein muss.[1567] Gleichwohl muss konzediert werden, dass der OGH[1568] in einem anderen Fall zur Überzeugung gelangt ist, dass im Bereich einer ausdrücklichen Subsidiarität das strenger strafbedrohte Delikt grundsätzlich durchaus verdrängt werden kann.[1569] In den hier angesprochenen Fällen und generell für § 126b würde dies – sofern man überhaupt die Reichweite der Subsidiaritätsklausel des Abs 1 tatsächlich im interpretativen Weg auf Abs 2 zu erstrecken vermag – zu ausgesprochen unsachgerechten Ergebnissen führen. Man bedenke, dass in Fällen von DoS-Angriffen auf ein Computersystem (welche – wie oben angemerkt – das Zielanliegen der Bestimmung sind), bei denen schon zwangsläufig Daten durch die herbeigeführte schwere Systemstörung unterdrückt werden, § 126b überhaupt auch das gegenüber § 126a speziellere Delikt ist.

1563 Vgl § 126a (Vermögen, Interesse am Fortbestand und der Verfügbarkeit von »Daten«); § 126b (Vermögen, Interesse an der Verfüg- bzw Verwendbarkeit des »Computersystems«).

1564 Vorverlagerung des Rechtsgüterschutzes auf das datenverarbeitende Computersystem in § 126b. Die vermögenswerten Daten selbst, werden durch § 126a geschützt.

1565 § 126a verlangt den Eintritt eines Vermögensschadens bzw schützt das Interesse am Fortbestand und der Verfügbarkeit von Daten; § 126b stellt vorrangig auf die Verwendbarkeit des Systems iSd Gebrauchsinteresses ab, stellt aber nicht auf die Höhe eines damit verbundenen (Vermögens-)Schadens ab. Beide Delikte sind allerdings systematisch dem Vermögensstrafrecht zugeordnet. Schutz- bzw auch Tatobjekt des § 126a sind Computerdaten, § 126b fokussiert auf ein Computersystem.

1566 § 126a erfasst das »Verändern, Löschen oder sonst Unbrauchbarmachen oder Unterdrücken« von Daten; § 126b erfordert durch das »Eingeben oder Übermitteln« von Daten die Herbeiführung einer »schweren Funktionsstörung« eines Computersystems.

1567 Siehe dazu bereits *Bergauer,* jusIT 2012/93, 199; weiters *Bergauer/Schmölzer* in Jahnel/Mader/Staudegger, IT-Recht[3], 635 (650 ff).

1568 Vgl OGH 03.07.1980, 12 Os 72/80.

1569 Siehe dazu auch *Ratz* in WK[2] Vorbem §§ 28–31 Rz 40.

Im Ergebnis bleibt daher festzuhalten, dass sich die Subsidiaritätsklausel des § 126b Abs 1 aufgrund einer dogmatischen, insb auf rein interpretative Methoden gestützten Analyse nur auf die dort beschriebene Tat – nämlich die schwere Störung der Funktionsfähigkeit eines Computersystems, über das der Täter nicht oder nicht allein verfügen darf, durch Eingabe oder Übermittlung von Daten – bezieht und sich aufgrund des expliziten Verweises des Qualifikationstatbestands des § 126b Abs 2 lediglich auf »die Tat« des Grundtatbestands ihre Reichweite nicht auch auf die Qualifikationsnorm erstreckt. Darüber hinaus führt eine Ausdehnung des Anwendungsbereichs der Subsidiaritätsklausel auf Abs 2 auch zu kriminalpolitisch fragwürdigen Ergebnissen.

Eine ausdrückliche Subsidiarität ist wohl idR nur dann sinnvoll, wenn die verdrängte Norm gegenüber der verdrängenden Norm lediglich ein »tatbestandliches Weniger« erfasst und Kongruenz der Rechtsgüter und der Angriffsrichtung[1570], insb was den Unrechts- und Schuldgehalt betrifft, besteht.[1571]

Aus diesen Erwägungen ergibt sich aus meiner Sicht, dass die Subsidiaritätsklausel in § 126b Abs 1 generell unzweckmäßig und überflüssig ist und man sie – wenn überhaupt – de lege lata zumindest nur auf das dort definierte Grunddelikt anwenden darf.

Würde der Gesetzgeber die Subsidiaritätsklausel des Abs 1 auch auf den Qualifikationstatbestand anwendbar machen wollen, ließe sich dies – unmissverständlich – in einem eigenen Absatz bezüglich der Absätze 1 und 2 anordnen.[1572] Da § 126b Abs 2 erst mit dem StRÄG 2008 ergänzt wurde, wird allerdings in Betracht zu ziehen sein, dass der Anwendungsbereich bzw die Reichweite der Subsidiaritätsklausel nicht gehörig bedacht wurden.

Anzumerken ist, dass dieses Problem beim Qualifikationsfall des § 126b Abs 2 zweiter Fall (bezüglich der Begehung als Mitglied einer kriminellen Vereinigung, wofür eine Strafdrohung von 6 Monaten bis zu 5 Jahren Freiheitsstrafe vorgesehen ist[1573]) nicht auftritt.

1570 *Burgstaller,* Die Scheinkonkurrenz im Strafrecht (II), JBl 1978, 393.

1571 Ähnlich und allgemein zur Scheinkonkurrenz *Triffterer,* AT², 453.

1572 Beispielsweise iSd § 94 Abs 4.

1573 Ergänzt durch das StRÄG 2008 (BGBl I 109/2007), womit den entsprechenden Vorgaben aus Art 6 Abs 2 iVm Art 3 des EU-RB 2005/222/JI Rechnung getragen wurde. Art 3 (Rechtswidriger Systemeingriff): »Jeder Mitgliedstaat trifft die erforderlichen Maßnahmen, um sicherzustellen, dass die unbefugte vorsätzliche schwere Behinderung oder Störung des Betriebs eines Informationssystems, durch Ein-

8. Sonstiges

§ 126b ist ein Offizialdelikt. Entstammt der Täter dem Familienkreis des Opfers, ist er gem § 166 Abs 1 privilegiert. Darüber hinaus wird § 126b iVm § 166 Abs 3 zu einem Privatanklagedelikt. Eine Strafaufhebung durch Tätige Reue kommt prinzipiell unter den Voraussetzungen des § 167 in Betracht.[1574]

§ 126b Abs 1 fällt gem § 30 Abs 1 StPO in die sachliche Zuständigkeit des Bezirksgerichts. Die Deliktsqualifikationen in § 126b Abs 2 fallen gem § 31 Abs 4 Z 1 StPO in die sachliche Zuständigkeit des Einzelrichters am Landesgericht.

C. Missbrauch von Computerprogrammen oder Zugangsdaten (§ 126c)

§ 126c (1) Wer

1. ein Computerprogramm, das nach seiner besonderen Beschaffenheit ersichtlich zur Begehung eines widerrechtlichen Zugriffs auf ein Computersystem (§ 118a), einer Verletzung des Telekommunikationsgeheimnisses (§ 119), eines missbräuchlichen Abfangens von Daten (§ 119a), einer Datenbeschädigung (§ 126a), einer Störung der Funktionsfähigkeit eines Computersystems (§ 126b) oder eines betrügerischen Datenverarbeitungsmissbrauchs (§ 148a) geschaffen oder adaptiert worden ist, oder eine vergleichbare solche Vorrichtung oder

2. ein Computerpasswort, einen Zugangscode oder vergleichbare Daten, die den Zugriff auf ein Computersystem oder einen Teil davon ermöglichen,

---

geben, Übermitteln, Beschädigen, Löschen, Verstümmeln, Verändern, Unterdrücken oder Unzugänglichmachen von Computerdaten, zumindest dann unter Strafe gestellt wird, wenn kein leichter Fall vorliegt.«
Art 6 (Sanktionen): »1) Jeder Mitgliedstaat trifft die erforderlichen Maßnahmen, um sicherzustellen, dass die Straftaten nach den Artikeln 2, 3, 4 und 5 mit wirksamen, verhältnismäßigen und abschreckenden strafrechtlichen Sanktionen bedroht werden. (2) Jeder Mitgliedstaat trifft die erforderlichen Maßnahmen, um sicherzustellen, dass die Straftaten nach Artikel 3 und 4 mit einer Freiheitsstrafe im Höchstmaß von mindestens einem bis drei Jahren geahndet werden.«

1574 Siehe dazu aber auch die Bedenken iZm § 126a.

> mit dem Vorsatz herstellt, einführt, vertreibt, veräußert, sonst zugänglich macht, sich verschafft oder besitzt, dass sie zur Begehung einer der in Z 1 genannten strafbaren Handlungen gebraucht werden, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.
>
> (2) Nach Abs. 1 ist nicht zu bestrafen, wer freiwillig verhindert, dass das in Abs. 1 genannte Computerprogramm oder die damit vergleichbare Vorrichtung oder das Passwort, der Zugangscode oder die damit vergleichbaren Daten in der in den §§ 118a, 119, 119a, 126a, 126b oder 148a bezeichneten Weise gebraucht werden. Besteht die Gefahr eines solchen Gebrauches nicht oder ist sie ohne Zutun des Täters beseitigt worden, so ist er nicht zu bestrafen, wenn er sich in Unkenntnis dessen freiwillig und ernstlich bemüht, sie zu beseitigen.[1575]

In Umsetzung des Art 6 CCC wurde auch das spezielle Vorbereitungsdelikt des § 126c ins Strafgesetzbuch aufgenommen. Die Erl zu Art 6 CCC geben Aufschluss darüber, dass durch eine solche Strafbestimmung im Vorfeldbereich auch der Markt hins spezieller »Hackertools« eingedämmt werden soll.[1576] Bestimmte Vorbereitungshandlungen, die sich auf die Verwirklichung spezieller Computerdelikte richten und grundsätzlich mangels der deliktsspezifischen Ausführungsnähe zu den Computerdelikten noch in diesem frühen Stadium straflos wären, sollen von diesem Delikt nun ausdrücklich erfasst sein. Gleichwohl bestehen Zweifel, dass diese Norm tatsächlich ihren kriminalpolitischen Zweck hinreichend erfüllt.[1577]

Der objektive Tatbestand des § 126c Abs 1 erfasst das Herstellen, Einführen, Vertreiben, Veräußern oder sonst irgendwie Zugänglichmachen, das Sich-Verschaffen oder das Besitzen eines in § 126c Abs 1 Z 1 näher beschriebenen Computerprogramms bzw eines in § 126c Abs 1 Z 2 normierten Computerpasswortes, Zugangscodes oder vergleichbarer Daten, die den Zugriff auf ein Computersystem oder einen Teil davon

---

1575 BGBl I 60/1974 idF I 15/2004.

1576 ER (ETS 185) Pkt 71 in Anlehnung an die Europäische Konvention über Rechtsschutz für Dienstleistungen mit bedingtem Zugang und der Dienstleistungen zu bedingtem Zugang (ETS 178), <conventions.coe.int/Treaty/en/Treaties/Html/178.htm> (01.04.2014), die von Österreich allerdings nicht unterzeichnet wurde, und der Richtlinie 98/84/EG des Europäischen Parlaments und des Rates vom 20. November 1998 über den rechtlichen Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten, ABl L 1998/320, 54.

1577 Siehe hiezu und auch in weiterer Folge grundlegend bereits *Bergauer,* ÖJZ 2007/45, 532.

ermöglichen. Die Tathandlungen des »Sich-Verschaffens« und »Besitzens« wurden allerdings erst durch das StRÄG 2004[1578] aufgrund des EU-Rahmenbeschlusses 2001/413/JI[1579] ergänzt, wobei diese in Art 4 EU-Rahmenbeschluss ausschließlich Computerprogramme, nicht aber Zugangsdaten, betreffen.[1580] Eine Differenzierung wurde in der österr Umsetzung aber nicht gemacht, weshalb diese Tathandlungen in gleichem Maß auch für Zugangsdaten vorgesehen sind.

Ursprünglich – mit Einführung des § 126c durch das StRÄG 2002 – wurde noch von der Kriminalisierung des Besitzes und des Sich-Verschaffens der in § 126c genannten Computerprogramme und Zugangsdaten mit der Argumentation Abstand genommen, dass noch nicht die Schwelle erreicht sei, ab der eine Kriminalisierung gerechtfertigt erscheint.[1581]

Nach der CCC konnte ein Mitgliedstaat durch Erklärung eines Vorbehalts iSd Art 6 Abs 3 CCC gewisse Tathandlungen von der Strafbarkeit ausnehmen. Doch wurde Österreich durch Art 4 des EU-Rahmenbeschlusses zur Bekämpfung von Betrug und Fälschung iZm unbaren Zahlungsmitteln zwingend verpflichtet, auch den Besitz zu kriminalisieren.[1582] Darüber hinaus ist die Tathandlung des Sich-Verschaffens ebenfalls in Art 4 des EU-RB 2005/222/JI (Straftaten bezogen auf spezielle Tatmittel) vorgesehen und bedarf daher genauso einer zwingenden gesetzlichen Entsprechung – worauf jedoch in den GMat nicht hingewiesen wird. Nach den Erl wird die Ergänzung der Tathandlungen des § 126c Abs 1 jedoch ausschließlich auf eine Anregung im Begutachtungsverfahren gestützt, die auf eine den teilweise ähnlichen Tatbeständen (wie §§ 224a, 227, 241b, 241c und 241f) möglichst angeglichene Formulierung abstellt.[1583]

Vorbereitungshandlungen sind grundsätzlich noch so weit von einer konkreten Rechtsgutbeeinträchtigung entfernt, dass sie idR noch als straflos angesehen werden.

§ 126c stellt nun aber bereits Vorbereitungshandlungen zu den taxativ in Abs 1 Z 1 genannten speziellen Computerdelikten (diese sind

1578 Strafrechtsänderungsgesetz 2004, BGBl I 15/2004.
1579 Rahmenbeschluss 2001/413/JI zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln vom 28. 5. 2001, ABl L 2001/149, 1.
1580 Vgl *Reindl-Krauskopf* in WK² § 126c Rz 12 (Stand Dezember 2008).
1581 Siehe ErlRV 1166 BlgNR XXI. GP, 29.
1582 Vgl ErlRV 309 BlgNR XXII. GP, 7.
1583 Siehe dazu ErlRV 309 BlgNR XXII. GP, 7.

§§ 118a, 119, 119a, 126a, 126b, 148a)[1584] ausdrücklich unter Strafe. Gegenüber den genannten Computerdelikten ist § 126c daher ein klassisches Vorbereitungsdelikt, das vom Scheinkonkurrenztypus der stillschweigenden (materiellen) Subsidiarität geprägt ist und hinter den Versuch und umso mehr hinter die Vollendung eines dieser Hauptdelikte zurücktritt.[1585]

Trotz der systematischen Einordnung des Delikts im 6. Abschnitt des StGB (Strafbare Handlungen gegen fremdes Vermögen) ist das geschützte Rechtsgut nicht klar zu identifizieren. Angesichts der angeführten Hauptdelikte handelt es sich jedenfalls um individuelle Rechtsgüter und keine universellen. Weiters schützen die aufgezählten Hauptdelikte weitgehend verschiedene Rechtsgüter, so zB §§ 118a, 119, 119a Bereiche der Privatsphäre[1586], §§ 126a und 126b sowohl das Vermögen als auch (strittig) Bereiche der Privatsphäre, und § 148a das Vermögen.[1587] Es ist daher davon auszugehen, dass § 126c ebenfalls diese Rechtsgüter der Privatsphäre und des Vermögens schützt.[1588]

Zu den von § 126c Abs 1 erfassten Handlungen zählen ua das Herstellen, Verbreiten oder Besitzen von typischen »Hacker-Werkzeugen« oder aber auch das Sich-Verschaffen[1589] von Computerpasswörtern. Tatobjekt können iSd Z 1 Computerprogramme (oder auch vergleichbare »Vorrichtungen«) sein, die aufgrund ihrer besonderen Beschaffenheit geradezu zum Zweck der Begehung einer der genannten strafbaren Handlungen geschaffen oder adaptiert wurden, oder iSd Z 2 Computer-Zugangsdaten aller Art (Passwörter, Transaktionsnummern[1590], persönliche Identifikationsnummern[1591], Verfügernummern usw).

1584 § 148a wurde mit dem StRÄG 2004 in das Tatbild des § 126c aufgenommen.

1585 Siehe dazu allgemein zB *Kienapfel/Höpfel/Kert,* AT[14], Z 21 Rz 9.

1586 Genaueres siehe in der Auseinandersetzung mit dem jeweiligen Delikt in dieser Arbeit.

1587 Auch wurde § 126c nicht in die Privilegierung des § 166 Abs 1 aufgenommen, was darauf hinweist, dass das Vermögen jedenfalls kein Rechtsgut des § 126c sein dürfte.

1588 In diesem Sinne wohl auch *Hochmayr,* Strafbarer Besitz von Gegenständen (2005) 35 bzw 37.

1589 Siehe dazu auch das zu § 207a Abs 3 Gesagte.

1590 Kurz: TAN; dabei handelt es sich um sog »Einmalpasswörter«.

1591 Kurz: PIN.

1. Tatobjekt des § 126c Abs 1 Z 1

Nicht jedes Computerprogramm iSd § 126c Abs 1 Z 1, das zur Begehung derartiger Straftaten geeignet ist, soll Tatobjekt des § 126c sein.[1592] Es gibt freilich auch Software, die einen ganz legalen Zweck erfüllt, aber ebenso gut als Tatwerkzeug geeignet wäre, wie etwa typische Administratoren-Tools. Um nunmehr eine Unterscheidung zwischen diesen Programmen treffen zu können, wurde in den Tatbestand die Anforderung aufgenommen, dass es sich bei einem tatbildlichen Computerprogramm um ein Programm handeln muss, das nach »seiner besonderen Beschaffenheit« zur Begehung einer der in Z 1 genannten Straftaten geschaffen oder adaptiert wurde. Auch in den Erl[1593] zur CCC wird diese Problematik hins »Dual-use Devices« diskutiert.[1594] Im Ergebnis wurde ein Kompromiss gefunden, der den Anwendungsbereich der Konvention auf Fälle einschränkt, »where the devices are objectively designed, or adapted, primarily for the purpose of committing an offence«.[1595]

Zu bedenken ist dabei, dass die für solche Straftaten tauglichen Programme bzw technischen Grundlagen in sehr vielen Fällen von seriösen Programmierern für nützliche Zwecke geschaffen werden, wie zB Programme zur Fehleranalyse in Netzwerken (vgl Packet-Sniffer), Fernwartungssoftware (wie Remote-Access-Tools) oder Skript-Programme, die aufwendige Tippvorgänge ersparen und Routineaufgaben automatisieren sollen (zB das programmgesteuerte Löschen von temporären Dateien). Eine in weiterer Folge illegale Verwendung hängt daher lediglich vom Willen des Benutzers bzw Täters ab. In erster Linie lässt sich nämlich ex ante in objektiver Hinsicht lediglich aufgrund der Bezeichnung oder des Dateinamens der Programme erkennen, ob es sich dabei um tatbestandlich nicht erfasste nützliche Administratoren-Tools oder tatbestandlich erfasste Malware handelt.

Aus diesem Grund sollten die tatbildlichen Computerprogramme – in Anlehnung an § 239[1596] – eine für Computerstraftaten ausgerichtete

---

1592 Siehe *Reindl-Krauskopf* in WK² § 126c Rz 2 und 8.

1593 Siehe ER (ETS 185) Pkt 73.

1594 Siehe auch zur entsprechenden Umsetzung in Deutschland *Popp,* Computerstrafrecht in Europa Zur Umsetzung der »Convention on Cybercrime« in Deutschland und Österreich, MR-Int 2007, 84.

1595 Vgl *Bergauer,* ÖJZ 2007/45, 532; weiters *Bergauer* in BMJ, 35. Ottensteiner Fortbildungsseminar, 27 (30 ff).

1596 Siehe ErlRV 1166 BlgNR XXI. GP, 29.

spezifische Zweckbestimmung aufweisen, die schon aus der besonderen Beschaffenheit der Software objektiv ersichtlich sein muss; auf den Vorsatz des Täters kommt es dabei nicht an. Doch auch in derartigen Fällen ist mE eine objektivierbare Zweckbestimmung eines Programms, die »gute« von »böser« Software unterscheiden soll, in der Praxis nicht möglich.[1597]

Beispielsweise bezeichnet man ein »nützliches« Programm, das einen Zugang zu einem anderen Computersystem ermöglicht, als »Fernwartungssoftware«, wohingegen ein »unerwünschtes« Programm mit derselben Funktionalität zB »Trojanisches Pferd« bzw »Backdoor« genannt wird. Die wesentlichen zugrunde liegenden Programmabläufe von nützlichen Programmen unterscheiden sich grundsätzlich aber nicht von Malware, weshalb Trojanische Pferde (wie bspw Backdoors, Keylogger, Hijacker), Computerwürmer, Computerviren, Sniffer, DDoS-Tools, Brute Force-Programme usw prinzipiell dieselben technischen Eigenschaften wie zB Administratoren-Tools aufweisen können. Ob nunmehr ein spezielles Programm als Tatobjekt des § 126c zu qualifizieren ist, hänge den GMat zufolge davon ab, ob es nach seiner besonderen Beschaffenheit ersichtlich zur Begehung einer der in Z 1 genannten Straftaten *geschaffen* oder *adaptiert* wurde. Daraus folgt, dass zB ein »nützliches« Sniffer-Programm – das (ursprünglich) eben nicht für illegale Zwecke geschaffen wurde – per se kein Tatobjekt des § 126c Abs 1 Z 1 ist. Ein »bösartiges« Sniffer-Tool hingegen, das gerade zum Zweck der Begehung zumindest eines der genannten Delikte hergestellt wurde, wird jedoch sehr wohl von § 126c erfasst. In beiden Fällen können die Programme aber funktional ident und ausschließlich zum Zweck der Datenpaketaufzeichnung in einem Netzwerk geschaffen worden sein, nur, dass einmal damit ein Netzwerkadministrator Fehler analysieren und ein anderes Mal ein Täter sich damit Kenntnis von sensiblen Daten verschaffen will (»subjektive Zweckbestimmung«). Auch wird grundsätzlich in beiden Fällen anhand objektiver Merkmale nicht feststellbar sein, zu welchem Zweck diese Sniffer-Programme ursprünglich geschaffen oder adaptiert worden sind. Der Täter könnte bspw auch ein anfangs zur nützlichen Netzwerkanalyse entwickeltes Sniffer-Programm als Tatmittel zur Begehung eines Delikts gem § 119 bzw § 119a ohne jegliche Modifikation verwenden wol-

1597 Siehe dazu auch zur Situation in Deutschland *Ernst,* Das neue Computerstrafrecht, NJW 2007, 2661 (2663).

len, das auf der Website des Herstellers ausdrücklich als Administratorwerkzeug beworben und nur zu diesem Zweck geschaffen wurde. Absurderweise wäre dieses Programm dann, da es eben nicht zur Begehung eines der angeführten Delikte »geschaffen« wurde, nicht Tatobjekt des § 126c Abs 1, weshalb der objektive Tatbestand auch nicht erfüllt wäre. Noch restriktiver sehen es *Bertel/Schwaighofer*[1598], die nur solche Programme als Gegenstand des Delikts erfassen, die »keinem anderen legalen Zweck dienen können«.[1599] Dies führt dazu, dass ein »bösartiger« Sniffer, der lediglich zum Zweck der Begehung einer der aufgezählten Straftaten programmiert wurde, schon deshalb nicht von § 126c Abs 1 Z 1 erfasst ist, weil er grundsätzlich ebenfalls der legalen Netzwerkanalyse dienen könnte. Darüber hinaus könnten »Trojanische Pferde« als Fernwartungsprogramm Einsatz finden oder DoS-Tools für sog »Penetrationstests«[1600] herangezogen werden. Auf die spezielle Deliktstauglichkeit (iSd der in § 126c Abs 1 Z 1 genannten Hauptdelikte) eines Computerprogramms im Zeitpunkt seiner Herstellung bzw Modifikation sollte mE für die Einordnung des Programms als Tatobjekt des § 126c Abs 1 Z 1 nicht abgestellt werden.

Auch die Ansicht des BVerfG[1601] iZm mit der Situation in Deutschland überzeugt mE auch für die österreichische nicht, da sich – wie *Heghmanns* es auf den Punkt bringt – die Auslegung des Zweckbegriffs[1602] im objektiven Tatbestand des § 202c Abs 1 Z 2 dStGB inkonsequent wiederum auf rein subjektive Erwägungen stützt. Damit wird erneut ersichtlich, dass »Computerprogramme nur denjenigen Zweck haben können, der ihnen vom Menschen gegeben wird«.[1603]

Der Gesetzgeber sollte daher die Formulierung des objektiven Tatbestands dahingehend abändern, dass das gegenständliche Computerprogramm nach seiner besonderen Beschaffenheit ersichtlich zur Begehung eines der genannten Straftaten »geeignet« sein muss, ganz gleichgültig zu welchem Zweck es (ursprünglich) geschaffen oder

---

1598 Siehe *Bertel/Schwaighofer,* BT I[12] § 126c Rz 1.

1599 Siehe auch ER (ETS 185) Pkt 73.

1600 Siehe *Rey/Thumann/Baier,* IT-Sicherheit, 1 ff; zu den IT-Sicherheitsunternehmen siehe auch S 344 ff.

1601 Vgl BVerfG 18.05.2009, 2 BvR 2233/07 (2 BvR 1151/08, 2 BvR 1624/08).

1602 Anders als in § 126c Abs 1 Z 1 ist in § 202c Abs 1 Z 2 dStGB der Begriff »Zweck« ein ausdrückliches, objektives Tatbestandsmerkmal; vgl »[…] Computerprogramme, deren Zweck die Begehung einer solchen Tat ist […]«.

1603 Siehe dazu auch *Heghmanns,* Straftaten gegen die betriebliche Datenverarbeitung, in Achenbach/Ransiek (Hrsg), Handbuch Wirtschaftsstrafrecht[3] (2012) 741 (762).

ggf adaptiert wurde. Damit wäre zwar der objektive Tatbestand des § 126c Abs 1 Z 1 zumindest hins der Erfassung sämtlicher »Dual-use Devices« weiter gefasst, aber wohl auch sachgerechter. Die besondere objektive Gefährlichkeit solcher Programme ist eng mit der spezifisch rechtswidrigen Verwendung (in Form jeglichen Hantierens) verwoben, welche sich wiederum aus der subjektiven Zweckbestimmung bzw des Tatplans ergibt. Sollten »Dual-use Devices« nicht tatbestandlich erfasst werden, so liegt es wohl am Gesetzgeber einen Gesetzeswortlaut zu finden, der eine Abgrenzung von sozialschädlichen Computerprogrammen und sozialverträglichen Dual-Use Computerprogrammen eindeutig und rein in der objektiven Tatumschreibung manifestiert.

Was die technische Beschaffenheit eines Computerprogramms oder einer vergleichbaren solchen Vorrichtung anlangt, so ist ausschließlich die informationstechnische Darstellungs- bzw Verarbeitungsform eines Computerprogramms gemeint. Dies liegt nach einer teleologischen, wie auch rahmenbeschluss-[1604] bzw konventionskonformen[1605] Interpretation nahe, da ein Computerprogramm, das zur Begehung eines der nachgelagerten Hauptdelikte geeignet sein muss, zwangsläufig schon in einer unmittelbar computertechnisch ausführbaren Ausdrucksform vorliegen muss. Es muss sich dabei allerdings nicht ausschließlich um ein kompiliertes Maschinenprogramm handeln. Auch ein »Source Code«-basiertes, unmittelbar durch einen Interpreter ausführbares Computerprogramm fällt unter die Tatobjekte des § 126c Abs 1 Z 1. Nicht darunter fällt aber ein auf »Papier« verfasster Source Code einer Malware. Dies ist aus rechtspolitischer Sicht allerdings unterschiedlich zu bewerten, denn einerseits würde eine Ausdehnung auch auf analoge Trägermedien eine noch weiterreichende[1606] Vorverlagerung der Strafbarkeit bedeuten, auf der anderen Seite wäre nicht zu verstehen, warum ein auf Papier ausgedruckter Source Code eines (grundsätzlich inkriminierten) Schadprogramms, die Tatobjektstauglichkeit und daher – selbst die abstrakte – Gefährlichkeit verlieren sollte, kann der Besitzer dieses Blattes Papier diese doch jederzeit durch Übertragung in eine computertechnische Ausdrucksform reaktivieren bzw (straflos) verbreiten.[1607]

1604 Vgl Art 1 lit b letzter HS EU-RB 2005/222/JI.

1605 Vgl Art 1 lit b letzter HS CCC.

1606 Man bedenke, dass es sich bei § 126c bereits um ein Vorbereitungsdelikt handelt.

1607 Siehe mehr dazu bei den Tathandlungen bzw gleich im Anschluss zu den Tatenobjekten des Abs 1 Z 2.

Ob ein Tatobjekt des § 126c Abs 1 Z 1 nun in concreto vorliegt ist daher stets im Einzelfall zu beurteilen, denn ein in einer bloßen Textdatei gespeicherter Source Code eines Schadprogramms kann bei Verwendung eines entsprechenden Interpreters unmittelbar beim Nutzer ausgeführt werden (vgl zB Skript- oder Makroviren[1608]).

2. Tatobjekt des § 126c Abs 1 Z 2

§ 126c Abs 1 Z 2 umfasst prinzipiell Computerpasswörter, Zugangscodes oder vergleichbare Daten, die den Zugriff auf ein Computersystem oder einen Teil davon ermöglichen. Es sind darunter daher sämtliche Formen von Computerpasswörtern und Zugangsdaten, wie PIN, TAN, Verfügernummern, Benutzernamen, Hash-Werte[1609] usw zu verstehen, die einen Zugriff auf ein Computersystem oder einen Teil davon ermöglichen.[1610] Unter einem Teil eines Computersystems sind bspw auch verschlüsselte Dateien zu verstehen, die mit einem Passwort gesichert sind. Wesentlich ist, dass die Zugangsdaten gültig und aktiv sein müssen[1611], denn ein veralteter Zugangscode ermöglicht keinen Zugriff mehr. Auch ein Passwort, das sich jemand bereits vor der Einrichtung und der Inbetriebnahme der Zugangssicherung ausgedacht hat, ist bis zur tatsächlichen Aktivierung dieser Sicherheitsmaßnahme nicht schützenswert.

Durch den Passus »oder vergleichbare Daten« wird offensichtlich auf den umstrittenen[1612] Datenbegriff des § 74 Abs 2 verwiesen. Dort wird zum Ausdruck gebracht, dass man iSd StGB sowohl personenbezogene und nicht personenbezogene Daten als auch Programme darunter versteht. Programme scheiden jedoch für § 126c Abs 1 Z 2 schon grundsätzlich aus, werden diese doch von § 126c Abs 1 Z 1 erfasst. Auch die Einbeziehung von »personenbezogenen Daten«[1613] spielt deliktsspe-

1608 Siehe dazu oben.

1609 »Hash-Werte« (siehe gleich im Anschluss) eines Passworts können als Zugangscodes verwendet werden (vgl etwa »Pass-the-hash-Verfahren« uÄ) siehe *Kennedy/O'Gorman/Kearns/Aharoni,* Metasploit – Die Kunst des Penetration Testing (2012) 128 ff.

1610 Vgl auch *Daxecker* in SbgK § 126c Rz 21 (Stand Mai 2012); weiters *Reindl-Krauskopf* in WK² § 126c Rz 10.

1611 Vgl etwa *Heghmanns* in Achenbach/Ransiek, Handbuch Wirtschaftsstrafrecht³, 741 (761).

1612 Siehe dazu bereits ausf S 60 ff.

1613 Siehe genaueres zu personenbezogenen Daten auf S 138 bzw S 563 ff.

zifisch schon aus rein sachlichen Überlegungen keine Rolle. Mit dem einzig zutreffenden Element des § 74 Abs 2, dass Daten auch »nicht personenbezogen« sein können, lässt sich aber an dieser Stelle nicht viel gewinnen. Es ist wohl Wille des historischen Gesetzgebers gewesen, dass von einer Einschränkung auf »Daten« in einer rein technischen Verarbeitungsform – wie es die CCC oder der EU-RB 2005/222/JI über Angriffe auf Informationssysteme vorsehen – bewusst Abstand genommen wurde, da die bloße Abgrenzung des Datenbegriffs zu jenem des DSG 2000 an dieser Stelle ausreichend sei.[1614]

Dadurch ist grundsätzlich jede – daher auch analoge[1615] – Form eines Passworts, das Zugang zu einem Computersystem gewährt, als Tatobjekt iSd § 126c Abs 1 Z 2 zu betrachten. So sehen dies für das deutsche Recht auch *Gercke/Brunst,* wenn sie ausführen, dass zu Sicherungscodes jegliche – »auch nicht elektronisch gespeicherte« – Daten zählen, »die im Rahmen von Zugangskontrollsystemen oder Verschlüsselungen als Zugangs- und Aktionsberechtigung eingesetzt werden können«.[1616] Darüber hinaus hätte der Gesetzgeber durch einfaches Ergänzen des Tatbestands, das Tatobjekt in § 126c Abs 1 Z 2 – wie auch schon die »Daten« in § 126a Abs 1 – auf eine »automationsunterstützt verarbeitete, übermittelte oder überlassene« Darstellungsform einschränken können, wollte er tatsächlich nur solche tatbestandlich erfassen.

Gerade bei Zugangsdaten ist mE – im Vergleich zu Computerprogrammen – die Missbrauchsgefahr aber erhöht. Es sollte nach Sachlichkeitsüberlegungen wohl irrelevant sein, ob es sich um ein geheimes und gültiges Computerpasswort handelt, das auf einem Papier aufgeschrieben[1617] oder in einer Textdatei auf einem Datenträger in codierter Form gespeichert[1618] wurde. Selbst das Abfotografieren[1619] eines im Klartext eingegebenen Passworts von einem Computerbildschirm oder das Ausspionieren einer PIN-Eingabe durch das bildli-

1614 Vgl ErlRV 1166 XXI. GP, 23; weiters ErlStV 1645 BlgNR XXIV. GP, 3.

1615 ZB ein auf Papier geschriebenes Passwort eines Computersystems; vgl dazu *Bergauer/Schmölzer* in Jahnel/Mader/Staudegger, IT-Recht[3], 635 (654).

1616 Vgl *Gercke/Brunst,* Internetstrafrecht, 76; weiters *Ernst,* NJW 2007, 2661 (2663).

1617 ZB die PIN einer Bankomatkarte, die auf einen Zettel geschrieben wurde und in der Geldtasche verwahrt wird.

1618 ZB eine Passwortdatei, um sich die vielen unterschiedlichen Passwörter in Erinnerung rufen zu können.

1619 Man denke an eine extern angebrachte Minikamera oder an interne Screenshots eines Trojanischen Pferdes.

che Erfassen der Tastaturbetätigung oder von Paysafecards[1620] würden nicht die vollständigen Anforderung an das Tatobjekt des § 126c Abs 1 Z 2 erfüllen. Vielmehr könnten »Computerzugangsdaten« demnach – insb nach der Spezifikation von »Computerdaten« iSd CCC, des EU-RB 2005/222/JI bzw der RL 2013/40/EU – nur solche sein, deren Inhalte in einer unmittelbar von einem Computersystem ausführbaren Verarbeitungsform (hier: Daten im engen Sinn) vorliegen würden und inhaltlich den notwendigen Passwortcharakter aufweisen, um Zugang zu einem Computersystem oder Teil davon zu ermöglichen (hier: Daten im weiten Sinn). Faktisch müsste daher ein solches Zugangsdatum sowohl aus dem passenden Inhalt (zutreffende Zeichenfolge) und aus seiner computertechnischen Verarbeitungsform bestehen. Sogar wenn der Vorgang der Passworteingabe oder auch das Passwort im Klartext selbst in externer elektronischer oder analoger Form vom Täter aufgezeichnet würde, läge das Zugangsdatum nicht in seiner codierten Form vor, sondern nur in einer anderen codierten Form, die zwar auch die Information des Passworts enthielte, nicht aber dessen spezifische Codierung. In diesem Fall wäre nur ein Teil der Tatobjektsbeschaffenheit erfüllt, nämlich der semantische, nicht auch der technische, weshalb § 126c Abs 1 nicht anwendbar wäre. Einen sinnvollen Anwendungsbereich hätte § 126c Abs 1 Z 2 iSd hier untersuchten Erfordernisses nur dort, wo die Zugangsdaten im System, im Zuge ihrer Eingabe oder Übermittlung, also am Übertragungsweg, abgefangen werden.

In Anbetracht des Schutzcharakters dieser Bestimmung kann es doch wohl nur auf den Inhalt des Passworts und nicht auf dessen spezifische Codierung ankommen. Dies lässt sich aufgrund des weiten Datenbegriffs des § 74 Abs 2 auch durchaus schlüssig argumentieren. Dass die Tathandlungen des § 126c Abs 1 in ihrer Beschreibung nicht unbedingt gut auf seine Tatobjekte des § 126c Abs 1 Z 2 passen, wird sich gleich im Anschluss zeigen.

Als eine zusätzliche Besonderheit der Zugangsdaten iSd § 126c Abs 1 Z 2 führt *Daxecker* zutreffend aus, dass eine weitere Einschränkung auf eine spezifische Zweckbestimmung – wie sie noch in Z 1 expressis verbis verlangt ist – schon naturgemäß ausscheidet. Dies führe wegen des darin liegenden Wertungswiderspruchs »zur nicht sachgerechten, aber nicht vermeidbaren Konsequenz, dass ein Täter, der sich etwa ein le-

1620 Siehe dazu OLG Innsbruck 16.12.2014, 11 Bs 353/14w.

gales Administratoren-Tool, allerdings mit subjektiver Zweckbestimmung zur Tatbegehung eines in § 126c genannten Deliktes, verschafft, mangels geeigneten Tatobjekts keine strafbare Vorbereitungshandlung setzt, hingegen bei Verschaffen eines Zugangscodes mit gleicher subjektiver Zweckbestimmung schon.«[1621]

Damit wird augenscheinlich, dass zB ein Administrator, der sich vom zu betreuenden Nutzer das Passwort mitteilen lässt, bereits den objektiven Tatbestand erfüllt und nur mangels Erfüllung der subjektiven Anforderungen des § 126c straffrei bleibt.[1622]

Der objektive Tatbestand ist insoweit überschießend, da er grundsätzlich jede Art Computerpasswörter erfasst und daher auch solche, die jemand für den Zugriff auf sein eigenes Computersystem berechtigter Weise herstellt[1623], besitzt usw.

3. Herstellen

Unter dem Herstellen ist jede Art der Produktion eines inkriminierten Computerprogramms bzw »vergleichbarer solcher Vorrichtungen« (iSd § 126c Abs 1 Z 1) oder von Zugangsdaten (iSd § 126c Abs 1 Z 2) zu verstehen.[1624] Bezüglich Computerprogramme ist anzumerken, dass nur das Programmieren eines Computerprogramms in einer unmittelbar »computerablauffähigen« Form gemeint sein kann. Das Verfassen einer Spezifikation[1625] des Computerprogramms auf Papier (oder auch in einer Textdatei) wäre noch eine straflose Vorbereitungshandlung. Deliktsspezifisch muss daher entweder ein Computerprogramm im Object Code oder ein mittels Interpreter unmittelbar ausführbarer Source Code hergestellt werden. Dies erfordert aber nicht, dass ein solches Programm originär erzeugt werden muss. Vielmehr stellt auch das computertechnische Vervielfältigen (Kopieren) eines Schadprogramms ein tatbestandliches Herstellen dar.[1626]

1621 Vgl *Daxecker* in SbgK § 126c Rz 21.

1622 Zur Empfehlung an den Gesetzgeber bloß »unbefugte Handlungen« oder nur »Unbefugte« als Täter zu erfassen siehe gleich im Anschluss.

1623 Als Beispiel dafür können Computerprogramme genannt werden, mit welchen der Berechtigte sein vergessenes Passwort wiederherstellen kann.

1624 Siehe auch *Reindl-Krauskopf* in WK² § 126c Rz 11; *Daxecker* in SbgK § 126c Rz 23.

1625 Dabei handelt es sich um eine Art Bauplan der Software.

1626 Siehe dazu zB das Herstellen iZm § 207a Abs 1 bei *Philipp* in WK² § 207a Rz 16 mwN.

Der Begriff des »Herstellens« impliziert, dass ein »gebrauchsfertiges« Schadprogramm außenweltwirksam ursprünglich bzw zu einem schon existenten solchen Programm zusätzlich durch dessen Reproduktion neu entsteht (Erfolgsdelikt).[1627] Im Zuge des ggf mehraktigen Programmiervorgangs eines solchen Programms bewegt sich der Täter bereits im Versuchsstadium (§ 15). In diesem Zusammenhang kann von einem sehr unterschiedlich langen Versuchszeitraum (zB bei einem Programmierer als Einzeltäter mehrere Monate bzw Jahre[1628] bzw bei einem Täter, der schlicht ein existentes Schadprogramm via »Copy and Paste« herstellt, wenige Sekunden) ausgegangen werden. Mit Vorliegen des lauffähigen Schadprogramms ist die Malware tatbestandsgemäß hergestellt und § 126c Abs 1 verwirklicht. Dies ist auch dann der Fall, wenn ein unmittelbar ausführbarer Code des Schadprogramms bereits existiert, aber noch weitere Programmiertätigkeiten zB zur Optimierung geplant sind.[1629]

Was man unter der Tathandlung des »Herstellens« iZm Computerpasswörtern, Zugangscodes oder vergleichbaren Daten nun verstehen mag, ist unklar. In erster Linie könnte an »Brute Force«-Angriffe gedacht werden, bei denen der Täter Passwörter bzw Zugangsdaten durch bloßes Aus- bzw Durchprobieren von Zeichenfolgen durch Permutation aller möglicher Zeichenkombinationen eines vordefinierten Zeichensatzes eruiert.[1630] Weiters ist auch an sog »Wörterbuch-Angriffe« (Dictionary Attacks) zu denken, bei denen auf Sammlungen von potentiellen und häufig verwendeten Passwörtern bzw bei Passwort-Hash-Werten auf sog »Regenbogentabellen« zurückgegriffen wird, um das Passwort zu ermitteln.[1631] Dies ist auch in Zusammenschau des § 126c Abs 1 Z 2 mit einem vom Täter angestrebten widerrechtlichen Zugriff

1627 Siehe zB auch *Hinterhofer* in SbgK § 207a Rz 12.

1628 Je nach Umfang und Programmierfähigkeiten des Täters.

1629 Vgl »fortgesetztes Delikt«, wobei in jüngerer Rsp diese Rechtsfigur zugunsten der deliktsspezifisch angelegten tatbestandlichen Handlungseinheit aufgegeben wurde (siehe OGH 22.11.2005, 14 Os 116/05y = JSt 2006/19, 52 *(Huber)* = JSt 2006/23, 93 *(Huber)* = AnwBl 2006/8056, 478 *(Hollaender)*.

1630 Bei der Verwendung des entsprechenden umfangreichen Zeichensatzes muss das Passwort – mathematisch bedingt – ermittelt werden, doch ist die Zeitdauer eines solchen Angriffs zurzeit bei Verwendung eines umfangreichen Zeichensatzes unverhältnismäßig lang.

1631 Zwar wird dadurch die Geschwindigkeit der Passwortermittlung erhöht, jedoch ist die Trefferquote entsprechend gering.

auf ein Computersystem (§ 118a) schlüssig[1632], da der Täter ein gewisses Mindestmaß an krimineller Energie aufwenden muss[1633], um einen Zugangscode – der ihm nicht vom Berechtigten selbst mitgeteilt oder ohne einen ins Gewicht fallenden Aufwand zugänglich wurde – eruieren zu können.[1634] Der Berechnungsvorgang des Passworts (»Brute Force«-Attacke) stellt dabei bereits die Ausführungshandlung des »Herstellens« dar. Wird das Passwort durch diesen Angriff letztlich ermittelt, ist auch der deliktische Erfolg eingetreten und § 126c Abs 1 in dieser Begehungsweise vollendet. Das schlichte Ausprobieren eines (ausgedachten) Passworts – ohne für dessen Erforschung auf ein technisch unterstütztes »Herstellungsverfahren« (zB Programmieren eines Computerprogramms bzw eines entsprechenden Algorithmus oder spezieller Suchlogik zur Passwortermittlung) zurückzugreifen – ist aber nicht von der Tathandlung des Herstellens von Computerpasswörtern oder Zugangscodes erfasst.

Aus teleologischen Überlegungen muss das auch für ein Passwort gelten, das durch die Verwendung von Musterpassworttabellen, welche in konventioneller Art auf Papier gedruckt sind, errechnet wird. Man stelle sich vor, der Täter hat sich Regenbogentabellen auf Papier ausgedruckt und vergleicht den abgefangenen Hash-Wert des zu eruierenden Passworts mit den vorausberechneten Zuordnungen dieser Listen in analoger Form. Findet er den passenden Eintrag in diesen Tabellen durch mühevolle manuelle Auswertung, hat er das zutreffende Passwort wohl – trotz ungewöhnlicher Benennung der Tathandlung – »hergestellt«.

Auch das programmtechnische Kopieren eines Zugangscodes stellt – wie oben zum Tatobjekt des Abs 1 Z 1 bereits ausgeführt – ein tatbestandsmäßiges Herstellen dar. Diskussionswürdig erscheint an dieser Stelle erneut die Beurteilung eines solchen Vervielfältigungsvorganges unter Einbeziehung eines »System- bzw Medienbruchs« von digitaler zu analoger Darstellung, zB das bloße Abschreiben der Information eines automationsunterstützt verarbeitbaren Computerpassworts auf ein Blatt Papier. Das kriminalpolitische Bedürfnis auch diesen Vorgang zu pönalisieren liegt auf der Hand, geht doch auch hier eine vergleichbare Gefahr – bei nur unterschiedlicher technischer Darstel-

1632 Und wohl auch von der CCC intendiert, vgl ER (ETS 185) Pkt 74.
1633 Vgl dazu iZm § 118a auch ErlRV 285 BlgNR XXIII. GP, 7.
1634 Siehe dazu die Ausführungen zu § 118a.

lungsform – aus. In einigen Fällen ist ein Systembruch überhaupt erst notwendig, um mit einem Passwort eines der in § 126c Abs 1 genannten Delikte zu begehen, man denke etwa an das Eingeben einer PIN auf Terminalsystemen wie Bankomaten. Hier könnte man ein computergeneriertes Passwort in informationstechnisch codierter Form gar nicht direkt verwenden, denn an den meisten Terminals lassen sich nur manuelle Eingaben vor Ort vornehmen.

4. Einführen

Die Tathandlung des Einführens stellt auf den »Import«, also die Verbringung über die Staatsgrenze idR nach Österreich, ab und wirft iZm Software bzw Zugangsdaten ebenso Problemfälle auf. Grundsätzlich ist es unbeachtlich, ob diese Verbringung der Tatobjekte auf konventionellem (physischen) oder elektronischem Weg erfolgt.[1635] Daher werden inkriminierte Computerprogramme (§ 126c Abs 1 Z 1) oder generierte Zugangscodes (§ 126c Abs 1 Z 2) enthaltende Datenträger, die postalisch oder im Transitverkehr über die Grenze gebracht werden, ebenso tatbestandsgemäß eingeführt, wie solche Tatobjekte, die per E-Mail oder Filetransfer via Internet an eine in Österreich gelegene informationstechnische Infrastruktur übermittelt werden. Lädt sich ein Nutzer daher zB ein Schadprogramm von einem ausländischen Server auf sein Computersystem in Ö herunter oder speichert er es in einem Online-Speicher auf einem in Ö stationierten Server eines entsprechenden Diensteanbieters, hat er das Programm nach Ö eingeführt (aber auch »sich-verschafft« bzw durch Kopieren »hergestellt«). Es kommt insoweit aber nicht darauf an, ob der Täter dabei das Passieren sämtlicher Staatsgrenzen in seinen Tatplan aufgenommen hat. Das Vorhaben, ein inkriminiertes Computerprogramm von einem ausländischen Server nach Ö zu transferieren, schließt technisch bedingt die Überschreitung ggf zahlreicher Staatsgrenzen nicht aus[1636] und ist folglich auch ohne Rücksicht auf ein aktuelles technisches wie geographisches Bewusstsein des Täters von den einzelnen Staatsgebieten auf tatbildmäßige Einfuhr gerichtet, welche jeweils durch tatsächliches Verbrin-

1635 Vgl auch *Daxecker* in SbgK § 126c Rz 24.

1636 Gerade das IKT-spezifisch bedingte »Routing« der Datenpakete über unterschiedliche Verbindungswege im Internet erfolgt idR völlig unabhängig etwaiger Staatsgrenzen.

gen über die Grenze vollendet ist.[1637] Denkbar wäre daher, dass der Täter mittels »Brute Force«-Methoden aus einem über das Internet abgefangenen Hash-Wert[1638] auf einem ausländischen Server das zutreffende Passwort eines Computersystems ermittelt, dieses auf einen Datenträger speichert und mit dem Auto über die Grenze bringt. Interessant stellt sich an dieser Stelle erneut das Problem eines »Systembruchs« dar. Zum Beispiel könnte ein Täter auf einem ausländischen Computersystem viele Passwörter mittels »Brute Force«-Angriffs ermitteln, diese in Form einer Zuordnungstabelle (Benutzername samt dazugehörendem Passwort und Internetadresse des jeweiligen Bezug habenden Online-Diensts) auf Papier ausdrucken und mit dem Auto nach Ö transportieren. Er hat vor, diese Passwörter von Ö aus dann tatsächlich zur Begehung von in § 126c Abs 1 Z 1 genannten Computerdelikten zu gebrauchen. Von derselben kriminellen Energie geprägt wäre das Verhalten des Täters aber auch dann, wenn er sich die Zuordnungsliste in computercodierter Form an einen E-Mail-Server in Ö selbst zusenden würde und in weiterer Folge ohne dieser Passwortliste mit dem Auto nach Ö einreisen würde. Die Weiterverwendung dieser Zugangsdaten erfordert in jedem Fall einen weiteren physischen Zwischenschritt des Täters, um die jeweiligen Daten iZm dem entsprechenden Dienst gebrauchen zu können.

1637 Vgl dazu sinngemäß OGH 17. 12. 1998, 15 Os 175/98 und OGH 28. 01. 1993, 12 Os 135/92.

1638 Ein Hash-Wert ist ein kryptographischer Fingerabdruck eines beliebig langen Klartext-Dokuments (zB auch Passwort), der nicht den konkreten Inhalt des Dokuments, sondern lediglich eine eindeutige Prüfsumme mit einer bestimmten Länge erfasst. Verändert sich das Klartext-Dokument, ändert sich auch ihr Hash-Wert (man spricht von sog »Kollisionsfreiheit«, da ein konkreter Hash-Wert nur zu einem einzigen Klartext-Dokument passt bzw passen kann). Aus einem Hash-Wert, der über eine Einwegfunktion gebildet wird, kann grundsätzlich auch das Klartext-Dokument nicht geschlossen werden (vgl *Stein,* Rechnernetze und Internet[3] [2008] 181 ff). Mittels sog »Regenbogentabellen«, die Unmengen vorausberechneter Werte zur Umkehrung kryptographischer Hash-Funktionen enthalten, könnte die Eruierung eines Passworts aber gelingen; vgl *Kennedy/O'Gorman/Kearns/Aharoni,* Metasploit, 128; weiters *Street/Nabors/Baskin,* Forbidden Network. Anatomie eines Hacks (2011) 323 f.

5. Vertreiben, Veräußern und Sonst-Zugänglichmachen

Die Tathandlungen des Vertreibens, Veräußerns und Sonst-Zugänglichmachens bilden sämtliche Formen der »Distribution«[1639] der Tatobjekte ab.[1640] So wird durch das Sonst-Zugänglichmachen, das als Auffangtathandlung alle weiteren noch denkbaren Verteilungsmöglichkeiten erfassen soll, auch das »Veröffentlichen« der Tatobjekte im Internet pönalisiert[1641] oder das bloße Zugänglichmachen solcher Programme bzw Zugangsdaten über Hyperlinks auf einer Website oder per E-Mail (iSv Anbieten).[1642]

Die zeitlich erst später normierte Strafbarkeit des Sich-Verschaffens und des Besitzens inkriminierter Tatobjekte ist in mehrfacher Hinsicht umstritten. Dass Zugangsdaten keine objektiv erkennbare besondere Beschaffenheit zur Deliktsbegehung besitzen und eine solche auch gem § 126c Abs 1 Z 2 gar nicht gefordert ist, wurde bereits oben angemerkt. Der objektive Tatbestand ist somit zB bereits beim bloßen Besitz von Zugangsdaten (man stelle sich eine Liste mit unzähligen Zugangscodes vor, die für sich genommen keine nach objektiven Kriterien bestimmbare, rein kriminellen Zwecken dienende Eigenschaft besitzen) erfüllt.[1643]

6. Sich-Verschaffen

Für das Sich-Verschaffen von Computerprogrammen oder Zugangsdaten wird schon begrifflich ein aktives Tun des Täters verlangt, weshalb eine rein passive Haltung dafür nicht ausreicht (zB aufgedrängte Information eines Passworts oder eines Computerprogramms durch unaufgeforderte Zusendung desselben per E-Mail).

Betrachtet man die Tathandlung des Sich-Verschaffens iVm den Tatobjekten nach § 126c Abs 1 Z 2, so muss das Sich-Verschaffen von Zugangsdaten jedenfalls möglich sein. Dieses Vorbereitungsdelikt macht idZ nur dann Sinn, wenn etwa bereits das Ablesen eines (fremden) Passworts von einem Zettel als ein Sich-Verschaffen erachtet wird.[1644] Der

1639 ER (ETS 185) Pkt 72.
1640 Siehe *Reindl-Krauskopf* in WK² § 126c Rz 11; weiters *Daxecker* in SbgK § 126c Rz 25.
1641 Vgl auch *Reindl-Krauskopf* in WK² § 126c Rz 11.
1642 So intendiert dies auch Art 6 CCC; siehe ER (ETS 185) Pkt 72.
1643 Vgl *Reindl-Krauskopf* in WK² § 126c Rz 12.
1644 AA für die vergleichbare Situation in Deutschland *Heghmanns* in Achenbach/Ransiek, Wirtschaftsstrafrecht³, 741 (761).

Täter befindet sich nämlich dann bereits in Kenntnis dessen. Dass er auch den Zettel, als Träger der Schrift, an sich bringen muss, ist dabei wohl nicht erforderlich. Das wäre viel zu eng und kriminalpolitisch unbefriedigend. Die aktive Kenntnisverschaffung des Passworts als Vorbereitungshandlung zu entsprechenden Hauptdelikten ist daher Teil des von § 126c Abs 1 Z 2 erfassten Übels, denn mit der Kenntnis des Zugangscodes können diverse in § 126c Abs 1 Z 1 genannte Hauptdelikte verwirklicht werden. Eine solche Interpretation wird sinnvollerweise auch bei § 254 (»Ausspähung von Staatsgeheimnissen«) iZm der Tathandlung des Sich-Verschaffens vertreten, wenn *Bachner-Foregger* dazu erklärt, dass sich ein Staatsgeheimnis verschaffe, wer unbefugt Kenntnis von dem Geheimnis erwirbt. Unter anderem kann dies der Fall sein, »wenn jemand einen versehentlich unverschlossen gebliebenen Geheimakt studiert«.[1645] *Eder-Rieder* führt zu diesem Delikt darüber hinaus noch an, dass auch eine Kenntniserlangung durch Hören, Lesen etc in Betracht komme.[1646] Ergänzend kann aber zur Bekräftigung einer solchen Auslegung auf die GMat zu dieser Tathandlung des Sich-Verschaffens iZm § 241e zurückgegriffen werden[1647], wo festgehalten wurde, dass damit jede Form des »An-sich-Nehmens« gemeint sei und gerade im Gegensatz zu den Tathandlungen der Vermögensdelikte deshalb gewählt wurde, um nicht schon begrifflich eine Vermehrung des Tätervermögens durch diese Handlung zu verlangen.[1648] Die Geldwäscherei in § 165 Abs 2 Fall 1 enthält eine ähnliche Formulierung (arg »an sich bringt«) und stellt darüber hinaus auf – auch unkörperliche – »Vermögensbestandteile«[1649], wie zB Giralgeld, ab. Daher ist darauf zu schließen, dass wohl auch für den Gesetzgeber ein »Sich-Verschaffen« im Verständnis eines umfassenden »An-Sich-Nehmens bzw An-Sich-Bringens« die Erlangung[1650] unkörperlicher Sachen – ohne das Erfordernis einer Gewahrsamsbegründung an einem körperlichen Gegenstand – möglich sein muss.

1645 Siehe *Bachner-Foregger* in WK² § 254 Rz 7 (Stand November 2012).

1646 Vgl *Eder-Rieder* in SbgK § 254 Rz 14 mwN (Stand November 2010).

1647 Wobei die Erl ausdrücklich darauf hinweisen, dass eine – an die Tathandlungen der teilweise ähnlichen Tatbestände der §§ 224a, 227, 241b, 241c und 241f – möglichst angeglichene Formulierung als gerechtfertigt erschiene (vgl ErlRV 309 BlgNR XXII. GP, 8).

1648 ErlRV 309 BlgNR XXII. GP, 16.

1649 Siehe dazu statt vieler *Birklbauer/Hilf/Tipold,* Strafrecht BT I² § 165 Rz 4; *Fabrizy,* StGB¹¹ § 165 Rz 2; *Glaser* in Eberwein/Steiner, Bitcoins, 138.

1650 Besser wohl »Verfügungsmöglichkeit« über die unkörperliche Sache.

Mit dem Sich-Verschaffen von Zugangsdaten ist daher nicht notwendigerweise eine von der Tathandlung abtrennbare Wirkung in der Außenwelt verbunden[1651], weshalb sich daraus kein Erfolgsdelikt ableiten muss. Eine Gewahrsamsverschiebung ist dabei ebenso wenig zwingend erforderlich wie eine Gewahrsamserlangung an einem körperlichen Gegenstand[1652].[1653] Das eigene Zutun wird mE teleologisch auf den Normzweck bezogen bereits in der aktiven Kenntnisverschaffung der Information (Computerpasswort) liegen und nicht erst in einer entsprechenden körperlichen Gewahrsamsbegründung.

Um nicht über das Ziel hinauszuschießen, sollte man jedoch ein bestimmtes Mindestmaß an krimineller Energie bezüglich des Akts des Sich-Verschaffens verlangen. Die Kenntnisverschaffung bzw sonstige Erlangung des Zugangscodes muss mE zumindest rechtswidrig sein und dem Täter eine gewisse Anstrengung abverlangen, um das Passwort schließlich zu erhalten (zB durch Abnötigung, Herauslockung im Wege des Phishing, Errechung mittels »Brute Force«-Software, Wegnahme usw). Sofern daher etwa der Berechtigte den PIN-Code direkt auf seine Bankomatkarte geschrieben hat und die Karte in einer Weise aufbewahrt, dass sie für Dritte zugänglich ist (zB durch Ablegen auf einem Tisch mit sichtbarer PIN-Notiz), ist das Mindestmaß an kriminelle Energie wohl noch nicht erreicht, um den Tatbestand zu verwirklichen.[1654]

Was die Tathandlung des Sich-Verschaffens iZm inkriminierten Computerprogrammen iSd § 126c Abs 1 Z 1 anlangt, so reicht die bloße Kenntnisnahme – wie zB bei Passwörtern oder Geheimnissen – dafür nicht aus. An verschiedenen Stellen[1655] führt der JA dazu an, dass sich jemand ein Tatobjekt verschaffe, wer daran (durch eigenes Zutun) »Gewahrsam« erlangt. Die Tathandlung setze einen Bezug zu einem »körperlich fassbaren« Gegenstand voraus.[1656]

1651 Vgl generell zB *Fuchs,* AT I[8] Rz 10/40; *Kienapfel/Höpfel/Kert,* AT[14] Z 9 Rz 6 ff.

1652 Was allerdings in den GMat in vergleichbarem Zusammenhang vorgesehen ist (vgl ErlRV 674 BlgNR XXIV. GP, 6). Siehe zur Problematik des strafrechtlichen Gewahrsamsbegriffs iZm unkörperlichen Daten S 486 ff.

1653 Verschafft sich jemand einen USB-Stick auf dem das Passwort in einer Textdatei gespeichert wurde, so ist durch die Gewahrsamsverschiebung ein tatbestandlicher Erfolg eingetreten. Liest jemand ein Passwort lediglich vom Bildschirm oder durch Beobachtung der vom Berechtigten verwendeten Tastatureingaben ab, so beschreibt das diesbezügliche Sich-Verschaffen lediglich eine schlichte Tätigkeit.

1654 Vgl dazu auch die Zettel-Notiz eines Passworts, die unmittelbar an einem Monitor bzw der Tastatur angebracht wurde (siehe ähnlich oben zu § 118a).

1655 ZB zu § 207a Abs 3 oder zu § 278 f Abs 2.

1656 Vgl JAB 106 BlgNR XXIV. GP, 33; vgl JAB 1848 BlgNR XVIII. GP, 3.

Der strenge strafrechtliche Gewahrsamsbegriff, der als die »vom natürlichen Herrschaftswillen getragene tatsächliche Sachherrschaft«[1657] definiert wird, führt aber iZm unkörperlichen, ubiquitären Sachen zu nicht sachgerechten Ergebnissen. Stellt man sich etwa den Fall vor, wo sich der Täter ein Schadprogramm verschafft, indem er es in einem Online- bzw Cloud-Speicher (auf einem fremden – auch ausländischen – Server) im Internet abspeichert, so fehlt es an jeglicher faktischer Sachherrschaft des Täters über eine »körperliche Sache«. Bezüglich des konkreten (körperlichen) Massenspeichers des verwendeten Servers hat – und will[1658] – der Täter keine Sachherrschaft, er darf idR lediglich über ihm zugewiesene (dynamische[1659]) Speicherbereiche verfügen. Da das faktische Herrschaftselement einzelfallspezifisch nach der verständigen Verkehrsauffassung zu beurteilen ist, könnte auf die Rechtsfigur des »gelockerten Gewahrsams«[1660] bzw des »sozialen Gewahrsams« zurückgegriffen werden. Dabei wird das Kriterium der unmittelbaren Beherrschbarkeit bzw greifbaren, räumlichen Nähe des Gegenstands insoweit »gelockert«, als eine solche dann nicht vorliegen muss, wenn der Gegenstand kraft sozialer Zuschreibungsmomente der Person herrschaftsmäßig zugeordnet werden kann. Man vergleiche bspw die Sonntagszeitungen in den Zeitungsständern und die eingeworfenen Münzen, an denen der Aufsteller Gewahrsam hat.[1661]

Doch auch ein solches Verständnis hält letztlich an der Zuordnung einer körperlichen Sache zu einer Person fest. Um daher zu einem zutreffenden und wohl nach – wie *Lewisch* es noch zum gelockerten Gewahrsam ausdrückt[1662] – »gesundem Menschenverstand« auch sinnvol-

---

1657 Vgl statt vieler *Birklbauer/Hilf/Tipold,* Strafrecht BT I² § 127 Rz 19 mwN.

1658 Es kommt ihm auch subjektiv nicht auf den Datenträger, sondern auf die »Information« an.

1659 Welche Speicherbereiche der Täter tatsächlich verwenden darf und wo sich diese konkret befinden, hängt aber wieder von den freien Ressourcen und Kriterien des Speichermanagements am Server ab und ist einer Disposition des Nutzers vollständig entzogen.

1660 Vgl etwa *Kienapfel/Schmoller,* Studienbuch Strafrecht. Besonderer Teil II (2003) § 127 Rz 67; *Leukauf/Steininger,* StGB³ § 127 Rz 21; *Bertel* in WK² § 127 Rz 15; *Salimi* in SbgK § 127 Rz 84 (Stand November 2012); *Birklbauer/Hilf/Tipold,* Strafrecht BT I² § 127 Rz 20 f; *Schwaighofer,* Neue Ansichten des OGH zum Gewahrsamsbegriff – Bemerkungen zu 13 Os 69/11p, JSt 2012, 66; weiters auch jüngst OGH 28. 09. 2010, 14 Os 126/10a.

1661 Siehe OGH 20. 12. 1989, 14 Os 109/89 (14 Os 110/89); weitere Beispiele bei *Birklbauer/Hilf/Tipold,* Strafrecht BT I² § 127 Rz 21.

1662 Siehe *Lewisch,* Strafrecht. Besonderer Teil I. §§ 75 – 168e² (1999) 148.

len Resultat zu gelangen, sollte iZm (unkörperlichen) Daten, bei denen der Datenträger ausschließlich eine rein faktisch-notwendige Aufgabe erfüllt, eine Abstraktion von der körperlichen Substanz unternommen und rein auf die informationstechnische faktische Verfügungs- bzw Verwendungsmöglichkeit abgestellt werden, die jedenfalls – neben etwaigen anderen Handhabungsmöglichkeiten – den tatsächlichen Zugriff auf die Daten bedingen. Um nicht in begrifflichen Konflikt mit den genannten Rechtsfiguren zu treten, wird hier diese Form des Gewahrsams an unkörperlichen Sachen als »Quasi-Gewahrsam« iS eines »informationstechnischen Zugriffs« bezeichnet.[1663]

Zusammenfassend bedeutet dies, dass sich der Täter ein Computerprogramm iSd § 126c Abs 1 Z 1 dann verschafft hat, wenn er in der Lage ist, über dieses zu verfügen, unabhängig davon, auf welchem Datenträger[1664] es gespeichert ist und wo es sich räumlich befindet.

Besitz erfordert eigenen Gewahrsam an einem körperlichen Gegenstand.[1665] Eine Besitzstrafbarkeit kann es daher nur dort geben, wo jemand einen verbotenen Gegenstand (zB DVD oder Festplatte mit darauf gespeicherter Malware) innehat. Auch für die Tathandlung des Besitzens iZm Zugangsdaten (iSd § 126c Abs 1 Z 2) kann man auf einen körperlichen Träger (Festplatte, DVD, USB-Stick, Papier usw; ausgenommen Gehirn) wohl rein schon aus Beweisgründen nicht verzichten. Spioniert daher jemand ein Passwort eines anderen aus (arg »Sich-Verschaffen von Zugangsdaten«) und schreibt es auf ein Blatt Papier, ist dieser Täter – sofern der Nachweis des »Sich-Verschaffens« nicht gelingen mag – zumindest wegen des Besitzes strafbar. Technische Mittel sind für den Besitz von Zugangscodes ebenso wenig erforderlich wie das Abstellen auf ausschließlich digitale Ausdrucksformen derselben auf körperlichen Trägermedien.[1666]

1663 Siehe dazu ausf die Erwägungen zu § 207a Abs 3 (S 486 ff).
1664 Sowohl in technischer als auch in sachenrechtlicher Hinsicht.
1665 Vgl statt aller *Hochmayr,* Besitz, 6.
1666 Siehe mehr zum Besitz iZm § 207a Abs 3 auf S 489 ff.

7. Besitzen

In Verwirklichung der Besitztathandlung ist § 126c ein Dauerdelikt.[1667] Auf der einen Seite kann das Besitzen eine schlichte Tätigkeit durch Tun darstellen (schlichtes Tätigkeitsdelikt), wenn der Täter den Gewahrsam an der Sache aktiv aufrechterhält. Auf der anderen Seite kann ein Besitzen auch durch ein Unterlassen verwirklicht werden, indem es nämlich der Täter unterlässt, den Gewahrsam an der (ggf aufgedrängten) inkriminierten Sache aufzugeben (echtes Unterlassungsdelikt).[1668] Dadurch, dass die Gewahrsamserlangung an den inkriminierten Tatobjekten gesondert durch die Tathandlung des »Sich-Verschaffens« abgedeckt wird, erübrigt sich an dieser Stelle die Prüfung, ob auch die erstmalige »Besitzergreifung« vom Besitzen (in dieser Form als Zustand der Herbeiführung von Gewahrsam und tatbestandlichem Erfolg betrachtet) erfasst wird.

Anzumerken ist jedenfalls, dass aufgrund des tatbestandlichen unabdingbaren subjektiven Unrechtselements im erweiterten Vorsatz auch der Besitz mit der überschießenden Innentendenz erfolgen muss, dass das Schadprogramm – irgendwann und von wem auch immer – zur Begehung eines der genannten Computerdelikte gebraucht wird (kupiertes Erfolgsdelikt). Dass das Schadprogramm aber tatsächlich in weiterer Folge verwendet wird[1669], spielt für die formelle Deliktsvollendung keine Rolle. Es handelt sich dabei um einen rein subjektiv anvisierten Erfolg des Täters, der außerhalb des Tatbestands angesiedelt ist, aber zum Tatzeitpunkt vorliegen muss.

Die umfassenden Tathandlungen bringen zum Ausdruck, dass es wohl keinen – wie auch immer gelagerten – (illegalen) Markt für Malware oder inkriminierte Zugangscodes zum Schutz der Privatsphäre und des Vermögens geben soll. § 126c Abs 1 beinhaltet einen alternativen Mischtatbestand mit rechtlich gleichwertigen Tathandlungen[1670], weshalb eine Konstatierung einer in concreto falschen Tathandlung prozessual nicht schadet. Freilich ließe sich aber darüber diskutieren, ob nicht das Herstellen eines solchen Schadprogramms vom sozialen

1667 Vgl generell *Hochmayr,* Besitz, 63 ff; aA *Kienapfel/Höpfel/Kert,* AT[14], Z 9 Rz 30.
1668 Vgl etwa *Hochmayr,* Besitz, 53 ff bzw 147 f.
1669 Es reicht auch aus, dass der Täter den Gebrauch im Rechtsverkehr durch einen anderen in seinem Vorsatz aufgenommen hat.
1670 AA *Daxecker* in SbgK § 126c Rz 11.

Sinngehalt betrachtet weniger gefährlich erscheint, als ein Zugänglichmachen für einen unbestimmten Adressatenkreis im Internet.

8. Abstraktes Gefährdungsdelikt

Obwohl davon auszugehen ist, dass die meisten Tathandlungen des § 126c Abs 1 (wie das Herstellen, Einführen, Vertreiben, Veräußern, Sonst-Zugänglichmachen und idR Sich-Verschaffen) eine von der Tathandlung zumindest gedanklich abtrennbare Wirkung in der Außenwelt[1671] hervorrufen (Erfolgsdelikte), was sich allein aus der Tatbestandsauslegung ergibt, liegt aus dem Blickwinkel der Beziehung zum Zweck der Bestimmung mit § 126c auch ein »abstraktes Gefährdungsdelikt« bezüglich Malware vor. Denkt man va an die Gefährlichkeit von Schadsoftware iSd § 126c Abs 1 Z 1, wie zB Computerwürmer oder -viren, deren Schaden und Reichweite nicht einmal der Täter selbst abzuschätzen und zu kontrollieren vermag und die einzig und allein zum Zweck der Schädigung konzipiert werden, so erfasst § 126c Abs 1 bereits diese (abstrakte) Gefahr des Gebrauchs solcher Programme, indem jeglicher Umgang mit ihnen (einschließlich ihrer Herstellung) pönalisiert wird. Dabei werden die Tathandlungen, wie zB das Herstellen von Computerwürmern, als so gefährlich eingestuft, dass dieses Verhalten auch dann strafbar ist, wenn noch gar keine konkrete Gefährdung oder Verletzung eingetreten ist.[1672] Die Gefährlichkeit sämtlicher Handlungen bezüglich inkriminierter Schadprogramme wird daher vom Gesetzgeber (in abstracto) unwiderleglich vermutet und muss nicht erst (in concreto) eintreten oder gar bis zu einer Verletzung des Rechtsguts führen. Ob diese Einschätzung auch für Zugangscodes gilt, ist wohl mehr als fraglich, da solche idR – abgesehen vom Erlangungs-[1673] bzw Herstellungsakt[1674] – stets zumindest einen weiteren gezielten und sozialschädlichen Verwendungsakt erfordern, um eine

1671 Vgl generell zB *Fuchs,* AT I[8], Rz 10/40; *Kienapfel/Höpfel/Kert,* AT[14], Z 9 Rz 6 ff.

1672 Anzumerken ist an dieser Stelle, dass das Herstellen eines neuartigen Computerwurmprogramms als noch viel gefährlicher zu beurteilen ist als das Besitzen eines älteren – und somit den Virenschutzentwicklern und deren Antivirensoftware meist bekannten – Schadprogramms.

1673 Zum Beispiel durch das Abfangen von Zugangsdaten mittels Sniffer-Tools in einem Netzwerk.

1674 Man denke etwa an sog »Brute Force«-Programme, welche Zugangscodes errechnen.

Gefährdungslage zu schaffen. Unzweifelhaft wäre es daher als völlig verfehlt anzusehen, Zugangscodes per se als sozial inadäquat und derart gefährlich einzustufen, dass jeglicher Umgang damit (hier sogar bereits im Vorfeld) strafrechtlich erfasst werden sollte. Das führt zu einer unsachlichen Überkriminalisierung.

9. Subjektive Tatseite

Die Verwirklichung dieses Delikts hängt nicht nur von objektiven Kriterien ab, sondern erfordert vom Täter neben dem Tatbildvorsatz, der sich zumindest in Form des dolus eventualis auf sämtliche objektiven Tatbestandsmerkmale erstrecken muss, auch den erweiterten Vorsatz in diesem Stärkegrad, das Computerprogramm zur Begehung einer der in Z 1 angeführten strafbaren Handlungen verwenden zu wollen.

Dieser erweiterte Gebrauchsvorsatz muss sich auf die Verwendung des Tatobjekts des § 126c Abs 1 als Tatmittel zur Begehung eines der in Z 1 genannten Delikte richten, wobei der Täter sein Computerprogramm bzw das verschaffte Computerpasswort zur Verwirklichung eines dieser (Haupt-)Delikte (§§ 118a, 119, 119a, 126a, 126b, 148a) verwenden will. Auch die Verwirklichung dieser subjektiven Zielvorstellung muss er zumindest ernstlich für möglich halten und sich damit abfinden (dolus eventualis). Es kommt nicht darauf an, ob das Tatmittel in weiterer Folge auch tatsächlich gebraucht wird.[1675] Interessanterweise ist aber zB der Betrug (§ 146) keines der angeführten Delikte, weshalb ein Täter, der in seinen Tatplan lediglich den Vorsatz aufgenommen hat, die per Phishing[1676] verschafften Zugangsdaten ausschließlich gegenüber einer Person (zB Bankangestellten) zu verwenden, um Finanztransaktionen durchführen zu lassen, nicht von § 126c erfasst wird.

10. Exkurs: Technischer Hintergrund des »Skimming«

Auffällig zeigt sich dabei der Fall des Skimming, bei dem der Täter meist an Bankomaten unbemerkt ein Aufsatzlesegerät[1677] anbringt, um die Daten des auf der Bankomatkarte befindlichen Magnetstreifens zu ko-

1675 Siehe dazu *Reindl-Krauskopf* in WK² § 126c Rz 14.

1676 Siehe dazu *Bergauer,* Phishing im Internet – eine kernstrafrechtliche Betrachtung, RZ 2006, 82; weiters *Bergauer* in BMJ, 35. Ottensteiner Fortbildungsseminar, 27 (31).

1677 Auch als »Skimmer« bezeichnet (vgl auch *Seidl,* ZIS 2012, 415).

pieren und auf einen Plastikkartenrohling (sog »White Plastic Card«) zu übertragen. Magnetstreifen werden lediglich noch aus Kompatibilitätsgründen verwendet. Mikrochip-Karten besitzen eine wesentlich höhere Sicherheit und können zB – wie in Europa – den »EMV-Standard« (Europay, Mastercard und Visa) erfüllen. Diesem Standard müssen freilich auch die Geldausgabeautomaten Rechnung tragen, was außerhalb Europas nicht überall der Fall ist.[1678]

Beim Skimming können die ausgelesenen Datensätze prinzipiell auch bloß über das Internet ins Ausland weitergeleitet werden, wo sie in weiterer Folge auf Blankokarten kopiert und an nicht mit modernen Verfahren (zB EMV) ausgestatteten Geldausgabeautomaten verwendet werden. Der Einsatz im europäischen Ausland macht für die Täter deshalb Sinn, da die originalen Zahlungskarten idR mit dem »modulierten Merkmal« (MM) ausgestattet sind, das nicht auf dem Magnetstreifen gespeichert ist, sondern eine geheime maschinenlesbare Substanz (dielektrisch) am Kartenkörper darstellt und von einem Bankomaten über eine sog »MM-Box« überprüft werden kann. In vielen Ländern wird dieses Merkmal aber – mangels entsprechender Ausstattung der Geldausgabeautomaten – nicht überprüft.[1679] Zudem sind moderne Zahlungskarten – neben dem Magnetstreifen – mit der EMV-Chip-Technologie ausgestattet, was dazu führt, dass Geldausgabeautomaten innerhalb Europas stets den Chip überprüfen. Mittlerweile sind aber wiederum bereits »EMV-Skimmer« aufgetaucht, die das Kopieren von Chips ermöglichen. Die Kriminalitätsform des Skimming wird sich daher in Hinkunft wohl auf solche Chip-Technologien verlagern.[1680] Die Banken haben auf diese Kriminalitätsform reagiert, weshalb seit Jänner 2015 für alle Inhaber einer österreichischen Maestro Bankomatkarte die Funktion »GeoControl« automatisch aktiviert wurde. Dadurch können Bargeldbehebungen außerhalb Europas nur mehr auf eigenen Wunsch und individueller Freischaltung durchgeführt werden.[1681]

Daneben wird mit einer Miniaturkamera oder mit einem Tastatur-Aufsatzgerät[1682] die PIN-Eingabe des Berechtigten heimlich aufgezeich-

1678 Vgl *Rankl/Effing,* Handbuch[5], 384; Anzumerken ist noch, dass es weltweit unterschiedliche technische Normen und Industriestandards gibt.

1679 Siehe dazu *Rankl/Effing,* Handbuch[5], 52 f.

1680 Zur Vorgangsweise beim Skimming generell siehe *Seidl,* ZIS 2012, 415.

1681 Siehe *Payment Service Austria,* <www.psa.at/karteninhaber/sicherheitstipps/geocontrol/> (03.03.2015).

1682 Auch »Tastatur-Skimmer« genannt.

net. In weiterer Folge soll mit diesem Kartenfalsifikat samt dupliziertem Datensatz und PIN, Bargeld an einem Bankomaten (im Ausland) behoben werden. Skimming lässt sich aber ebenso durch das Duplizieren von Chip-Karten realisieren. Innerhalb Europas sind die Bankomaten technisch mit dem sog »EMV-Verfahren« ausgestattet, weshalb Kartenduplikate grundsätzlich erkannt werden. Lediglich im europäischen Ausland ist die Verwendung von reinen Magnetstreifenkarten zur Geldbehebung noch möglich.

(Exkurs Ende)

Sowohl das Sich-Verschaffen der PIN als auch das Auslesen der Kontozugangsinformationen des Magnetstreifens können grundsätzlich nur dann unter § 126c Abs 1 subsumiert werden, wenn der Täter diese Zugangscodes zur Verwirklichung eines Betrügerischen Datenverarbeitungsmissbrauchs (§ 148a) gebrauchen will, zB durch widerrechtliche Verwendung im Online-Banking-System des Opfers oder an einer Bankomatkassa (sog »POS[1683]-Terminal«) zur Bezahlung von Waren.

Aus kriminalpolitischen Gründen wäre es mE aber ebenso notwendig, den Straftatbestand des Diebstahls (§ 127) als eines der (Haupt-)Delikte in § 126c Abs 1 Z 1 aufzunehmen.[1684] Dies ist nämlich schon dadurch indiziert, dass zB das Sich-Verschaffen einer PIN oder das Auslesen der Kontozugangsdaten einer Zahlungskarte, um in weiterer Folge eine unbefugte Geldabhebung an einem Bankomaten vorzunehmen, nach Ansicht des OGH als Diebstahl iSd § 127 zu qualifizieren ist.[1685] Ausdrücklich stellte der OGH dabei auch auf unbefugt hergestellte Bankomatkarten-Duplikate ab.[1686]

Nach dieser Auffassung wäre in unserem Beispielsfall das Vorbereitungsdelikt des § 126c nicht anwendbar, was einen gravierenden kriminalpolitischen Widerspruch bedeutet.[1687] Man könnte hier wohl

1683 »Point of Sale«.

1684 Siehe dazu bereits grundlegend *Bergauer* in BMJ, 35. Ottensteiner Fortbildungsseminar, 27 (31).

1685 Siehe statt vieler RIS-Justiz RS0093560 mwN; ebenso *Schmölzer,* Die unbefugte Verwendung einer fremden Bankomatkarte – Strafrechtliche Aspekte, EDVuR 1990, 30; aA *Bertel/Schwaighofer,* BT I[12] § 148a Rz 2 mwN.

1686 Vgl OGH 30.10.1990, 15 Os 79/90.

1687 Vgl *Bergauer,* RZ 2006, 82; weiters *Bergauer* in BMJ, 35. Ottensteiner Fortbildungsseminar, 27 (31); zust auch *Reindl-Krauskopf,* Das Phänomen »Phishing«, SIAK-Journal 2007, 2 (11).

argumentieren, dass das Analogieverbot zu Lasten des Täters einer Gleichbehandlung dieser Fälle entgegensteht.[1688]

Schenkt man allerdings der Anmerkung des OGH zu 15 Os 127/89 Beachtung, so ist davon auszugehen, dass § 148a StGB, der zur Ausschaltung von Strafbarkeitslücken geschaffen wurde, ungeachtet der Frage, ob dieser ein derartiges Tatverhalten überhaupt erfasst, aufgrund materieller Subsidiarität hinter den hierfür anzuwendenden Diebstahl zurücktritt.

Das bedeutet, dass die Rsp die Anwendbarkeit des § 148a StGB für solche Handlungen wohl nicht per se ausschließt, sondern lediglich den Diebstahl diesbezüglich prävaliert. Sofern daher der Täter lediglich die Umstände hinter den Tatbestandsmerkmalen in ihrer rechtlich-sozialen Bedeutung erfasst, wobei eine juristisch korrekte Beurteilung hier nicht gefordert ist, spricht wohl auch nichts gegen eine Anwendbarkeit des § 126c im Fall der vom Täter anvisierten unbefugten Bargeldbehebung an einem Bankomaten. Tritt der Täter in das Versuchsstadium des Hautpdelikts (hier nach Meinung des OGH Diebstahl gem § 127) ein, wird in weiterer Folge § 148a, dessen Tatbestand dabei ebenfalls erfüllt zu seien scheint, aufgrund materieller Subsidiarität durch § 127 verdrängt. Die materielle Subsidiarität des § 148a umfasst aber auch das Vorbereitungsdelikt des § 126c, weshalb § 126c bei Verdrängung des Hauptdelikts nicht wieder auflebt.

Eine etwaige Strafbarkeit des Skimming könnte aber auch durch § 51 DSG 2000 realisierbar sein.[1689]

Wie *Reindl-Krauskopf*[1690] richtig anmerkt, impliziert der erweiterte Gebrauchsvorsatz auch den Tatbildvorsatz und ggf erweiterten Vorsatz jenes Delikts, das der Täter unter Zuhilfenahme seines zB Computerprogramms in weiterer Folge begehen will. Eine »Begehung« einer Straftat erfordert stets das Verwirklichenwollen eines gesetzlichen Tatbestands, weshalb die Prüfung der inneren Tatseite (Tatbildvorsatz und ggf erweiterter Vorsatz) des vom Täter angestrebten in § 126c Abs 1 Z 1 genannten Delikts vorgelagert erfolgen und die Vorsatzelemente im Tatplan des Täters nachgewiesen werden müssen.

1688 Vgl *Reindl-Krauskopf* in WK² § 126c Rz 7.

1689 Siehe dazu ua die Ausführungen zu § 51 DSG 2000 in seiner Variante als Allgemeindelikt (S 130 ff).

1690 Siehe *Reindl-Krauskopf* in WK² § 126c Rz 15.

Eine genaue Tatplankenntnis wird nicht verlangt werden können.[1691] Sollte in weiterer Folge eines der (Haupt-)Delikte versucht oder gar vollendet werden, tritt § 126c als Vorbereitungsdelikt aufgrund materieller Subsidiarität hinter dieses Delikt zurück.

11. Sonderproblem: IT-Sicherheitsexperten

Interessant wird die Beurteilung, wenn es sich um Unternehmen handelt, die sich darauf spezialisiert haben, gegen Bezahlung die Sicherheit von IT-Einrichtungen ihrer Kunden zu testen. Derartige Firmen, deren Bedeutung in der Praxis zunehmend größer wird, benützen ebenso Computerprogramme iSd § 126c Abs 1 Z 1, die jedenfalls zur Verwirklichung des Tatbildes der in Z 1 genannten Delikte geschaffen oder adaptiert werden, weshalb der objektive Tatbestand idR erfüllt sein wird. Der (Tat-)Vorsatz der Personen[1692], die Sicherheitstests durchführen, richtet sich jedenfalls auf sämtliche objektiven Tatbestandsmerkmale des § 126c Abs 1. Ob auch die geforderte überschießendende Innentendenz zum Tatzeitpunkt gegeben ist, müsste jedenfalls mühevoll geprüft werden. Richtig ist, dass hierbei ein Programm hergestellt oder besessen wird, das in weiterer Folge auch den Webdienst eines Servers des Kunden durch eine »DoS«-Attacke im Zuge von sog »Penetrationstests« lahmlegen und zum Absturz bringen soll.

In einer derartigen Fallkonstellation wird möglicherweise die strafrechtliche Prüfung aufgrund eines (tatbestandsausschließenden) Einverständnisses bereits auf Tatbestandsebene der (Haupt-)Delikte scheitern. Denn üblicherweise hat der Kunde (= Alleinverfügungsberechtigter über die Daten im Fall des § 126a bzw Alleinverfügungsberechtigter über das Computersystem bei § 126b) bereits vertraglich seine Zustimmung erklärt, sodass das IT-Sicherheitsunternehmen von vornherein »verfügungsberechtigt« iSd genannten Strafbestimmungen agiert.

Doch wie ist der Sachverhalt zu beurteilen, wenn (noch) kein Einverständnis bzw zivilrechtlicher Vertrag vorliegt?[1693] Das Sicherheitsun-

---

1691 Siehe *Reindl-Krauskopf* in WK² § 126c Rz 15.

1692 Auf eine nahe liegende Verantwortlichkeit des IT-Sicherheitsunternehmens im Lichte des Verbandsverantwortlichkeitsgesetzes (VbVG) wird hier nicht eingegangen.

1693 In diesem Zusammenhang könnte auch die umstrittene Form der Kundenakquirierung ein Thema werden, bei der ein User während des Surfens im Internet unbemerkt Sicherheitsüberprüfungen unterzogen wird und auch zB unaufgefordert

ternehmen wird diese bereits vorhandenen »tatbildlichen« Software-Werkzeuge weiterhin auf seinen Datenträgern gespeichert haben und ggf auch weitere dem technischen Stand angepasste Malware herstellen oder sich verschaffen. Auch ein Handwerker entledigt sich nicht nach jeder Geschäftsbesorgung seiner Werkzeuge.

Um nicht schon zu diesem Zeitpunkt der »Vorbereitungshandlung«, in dem eines der in Z 1 genannten Delikte weder vollendet noch versucht ist, gedanklich die Stufen der strafrechtlichen Falllösung – Tatbestandsmäßigkeit (objektive und subjektive Merkmale), Rechtfertigungsgründe (zB Einwilligung) usw – des vom Täter angestrengten (Haupt-) Delikts prüfen zu müssen, sollte der Gesetzgeber § 126c Abs 1 jedenfalls entsprechend konkretisieren. Dazu wäre es sinnvoll, auf den in Art 6 Abs 2 CCC genannten Entfall der Strafbarkeit im Falle des autorisierten Testens[1694] oder zum Schutz von Computersystemen abzustellen. Dennoch würde sich eine Straflosigkeit nur mangels Erfüllung der subjektiven Tatelemente realisieren lassen.

Man könnte nun auch daran denken, dass ein solches Handeln der IT-Sicherheitsunternehmen noch als von der Allgemeinheit gebilligtes und daher sozial adäquates Tun zu verstehen ist, das gar kein tatbestandsmäßiges Unrecht iSd in Betracht kommenden Vorbereitungsdelikts darstellt und dadurch bereits die Tatbestandsmäßigkeit nicht gegeben ist. Die mangelnde Rechtswidrigkeit könnte daher als (ungeschriebenes) allgemeines Deliktsmerkmal verstanden werden, weshalb der Tatbestand des § 126c Abs 1 bei »gerechtfertigten« IT-Sicherheitsexperten nicht erfüllt wird. Dies ließe sich damit begründen, dass ein Straftatbestand idR nur (strafrechtliches) Unrecht in Bezug auf das zu schützende Rechtsgut beschreibt und er es somit nicht vermag, sozial adäquate Verhaltensweisen zu determinieren. Aus diesem Grund ist der Tatbestand entsprechend einzuschränken. Allerdings ist dabei darauf zu achten, dass bei einigen weiteren Delikten (zB § 119, § 119a, § 148a) ebenfalls äußere Verhaltensweisen beschrieben sind, die per se keine soziale Unverträglichkeit darstellen und lediglich über die Innentendenzen des Täters ihre insgesamt soziale Inadäquanz erlangen. Das betrifft zB die Definitionen der objektiven Tatbestände in § 119, 119a (iSv Benützen einer Vorrichtung), § 148a (iSv Beeinflussen

»Pop-Up«-Fenster angezeigt bekommt, die ihn auf sein unsicheres bzw durch Malware infiziertes System aufmerksam machen.

1694 Siehe insb ER (ETS 185) Pkt 77.

eines Ergebnisses eines Datenverarbeitung zB durch das Eingeben von Daten), § 208a Abs 1 Z 1 (iSv zB Vorschlagen eines Treffens im Wege der IKT mit anschließender konkreter Vorbereitungshandlung zur Durchführung desselben) und § 208a Abs 1a (iSv Kontaktherstellung zur unmündigen Person im Wege der IKT). Die Annahme, eine grundsätzlich sozial adäquate Handlung lässt stets die Tatbestandlichkeit entfallen, ist daher ein Trugschluss und kein verlässlicher Indikator, um eine Tatbestandsmäßigkeit bereits vorab auszuschließen.

Meines Erachtens wäre in jedem Fall eine mit geringem Aufwand zu realisierende Konkretisierung des Tatbildes wünschenswert.

Es würde genügen, den Tatbestand des § 126c Abs 1 um das tatbestandsbegrenzende Merkmal »unbefugt« bzw »widerrechtlich« zu erweitern, sodass diese Bestimmung tatsächlich nur denjenigen erfasst, der derartige Programme oder Zugangscodes unzulässigerweise herstellt, einführt, vertreibt, veräußert, sonst irgendwie zugänglich macht, sich verschafft oder besitzt, um eine der in Z 1 genannten strafbaren Handlungen zu begehen.

Interessanterweise wird iZm der Einführung des § 107a in den GMat in ähnlicher Weise argumentiert und betont, dass eine ausdrückliche Verankerung des Begriffs »widerrechtlich« erforderlich erscheine, da es sich bei den in § 107a Abs 2 präzisierten Tathandlungen auch um an sich sozial adäquate Verhaltensweisen handeln kann. »Gerechtfertigtes Handeln von Personen, die sich auf eine rechtliche Befugnis, etwa eine gesetzliche Erlaubnisnorm, stützen können, ist vom Anwendungsbereich der Norm auszuscheiden.«[1695]

Würde man auch in § 126c Abs 1 ausdrücklich die Widerrechtlichkeit tatbestandlich betonen, wäre das IT-Sicherheitsunternehmen samt seinen Mitarbeitern – freilich nur in Ausübung der konkreten geschäftlichen Tätigkeiten – aufgrund seines Geschäftszwecks jedenfalls als rechtlich befugt anzusehen. Systematisch wäre die Ergänzung ebenfalls sinnvoll, da auch in den übrigen speziellen Computerdelikten bereits im gesetzlichen Tatbild expressis verbis die »mangelnde Befugnis« des Täters konkretisiert wurde, wie zB die mangelnde Verfügungsbefugnis des Täters über die Daten im Fall des § 126a, oder des Computersystems im Anwendungsbereich des § 126b. Selbst bei den

1695 Siehe ErlRV 1316 BlgNR XXII. GP, 4.

Straftatbeständen § 119, § 119a und § 120 Abs 2a wurde ausdrücklich festgehalten, dass der Täter ein »Unbefugter« sein muss.[1696]

12. Tätige Reue

Die Strafaufhebung nach § 126c Abs 2 orientiert sich an den für Vorbereitungsdelikte idR üblichen Bestimmungen über die »Tätige Reue«. Dies macht auch Sinn, da § 126c bereits im Vorfeldbereich von Hauptdelikten angesiedelt ist, bei welchen ihrerseits – im Fall von Vermögensdelikten (vgl §§ 126a, 126b, 148a) – die Anwendbarkeit der klassischen Tätigen Reue gem § 167 prinzipiell möglich ist.[1697] Die Bestimmung des § 126c Abs 2 reicht aber deutlich weiter, da ggf diese auch die Strafbarkeit bezüglich deliktsspezifischer Vorbereitungshandlungen zu Delikten gegen die Privatsphäre (zB §§ 118a, 119, 119a) aufheben kann. Obwohl es sich um eine Form der Tätigen Reue handelt, ist der persönliche Strafaufhebungsgrund den Regelungen des Rücktritts vom Versuch (§ 16) nachgebildet.[1698]

§ 126c Abs 2 erster Satz verlangt die freiwillige Verhinderung des Gebrauchs der Tatobjekte des § 126c Abs 1 Z 1 und 2 als Tatmittel der angeführten Computerdelikte. Dies wäre zB gegeben, würde der Täter ein inkriminiertes Schadprogramm freiwillig löschen, bevor es als Tatmittel zur Deliktsbegehung gebraucht werden kann.

§ 126c Abs 2 zweiter Satz behandelt eine sog »putative Tätige Reue«. Die Strafbarkeit wird aufgehoben, wenn die Gefahr eines Gebrauchs als Tatmittel der Begehung der genannten Hauptdelikte nicht besteht oder bereits ohne Zutun des Täters beseitigt wurde und sich der Täter in Unkenntnis dessen freiwillig und ernstlich bemüht, die vermeintliche Gefahr zu beseitigen.

13. Sonstiges

§ 126c Abs 1 ist – entgegen einiger seiner nachgelagerten Hauptdelikte[1699] – ein (reines) Offizialdelikt und fällt aufgrund seiner Strafdrohung gem § 30 Abs 1 StPO in die sachliche Zuständigkeit des Bezirksgerichts.

1696 Siehe auch ErlRV 1166 BlgNR XXI. GP, 25 f.
1697 Siehe dazu den Deliktskatalog des § 167 Abs 2.
1698 Siehe ErlRV 1166 BlgNR XXI. GP, 30.
1699 §§ 118a, 119, 119a sind Ermächtigungsdelikte.

Aufgrund der vielfach ähnlichen, aber nicht identen Tatbestandsmerkmale des § 10 ZuKG kann es mit diesem Vorbereitungsdelikt zu Subsumtions- und Abgrenzungsschwierigkeiten kommen. Offensichtlich ist jedoch, dass § 10 ZuKG auf die gewerbsmäßige Begehung abstellt und daher auch die speziellere Norm darstellt, weshalb sie § 126c vorgeht.[1700] Dieser Gewichtung entsprechen auch die deutlich unterschiedlichen Strafdrohungen. Es handelt sich allerdings bei § 10 ZuKG um ein Privatanklagedelikt.

14. § 10 Zugangskontrollgesetz

> § 10 (1) Wer gewerbsmäßig (§ 70 StGB) Umgehungsvorrichtungen vertreibt, verkauft, vermietet oder verpachtet, ist vom Gericht mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.
>
> (2) Ebenso ist zu bestrafen, wer gewerbsmäßig (§ 70 StGB) Umgehungsvorrichtungen herstellt, einführt oder mit dem Vorsatz erwirbt oder innehat, dass diese auf die im Abs. 1 beschriebene Art und Weise in Verkehr gebracht werden oder dass mit ihrer Hilfe anderen der Zugang zu einem geschützten Dienst ermöglicht wird.
>
> (3) Wer Umgehungsvorrichtungen ausschließlich zum privaten Gebrauch einführt, erwirbt oder sich sonst verschafft, ist nicht als Beteiligter (§ 12 StGB) zu bestrafen.
>
> (4) Ein Bediensteter oder Beauftragter des Inhabers oder Leiters eines Unternehmens (§ 5) ist nicht zu bestrafen, wenn er eine der in den Abs. 1 und 2 genannten Handlungen auf Anordnung des Dienst- oder Auftraggebers vorgenommen hat und ihm wegen seiner wirtschaftlichen Abhängigkeit nicht zugemutet werden konnte, die Vornahme der Tat zu unterlassen.
>
> (5) Der Täter ist nur auf Verlangen des in seinen Rechten verletzten Diensteanbieters zu verfolgen.[1701]

Das ZuKG regelt den rechtlichen Schutz von Diensteanbietern, die Fernsehsendungen, Radiosendungen oder Dienste der Informationsgesellschaft gegen Entgelt und unter einer Zugangskontrolle bereit-

1700 Vgl ErlRV 1166 BlgNR XXI. GP, 29; vgl auch ErlStV 1645 BlgNR XXIV. GP, 5.
1701 BGBl I 60/2000.

stellen (§ 1 ZuKG[1702]). Das ZuKG ist Ergebnis der Umsetzung der »Zugangskontroll-Richtlinie«[1703], die ihren Fokus auf den Schutz moderner Vertriebsmodelle (wie zB On-Demand-Pay-TV oder Online-Diensten) richtet. Solche Dienste sind nämlich ihrerseits nur dann rentabel, wenn sie durch Zugangskontrollen vor unbefugter Nutzung geschützt werden.[1704] Zugangskontrollen können technisch zB durch eine Verschlüsselung der Übertragungssignale, elektronische Sperren oder durch den Einsatz von Passworttechnologien bewerkstelligt werden.[1705] § 3 ZuKG formuliert das »Recht auf Zugangskontrolle« – was gleichsam das Rechtsgut hinter der Strafbestimmung darstellt[1706] – dahingehend, dass der Diensteanbieter das ausschließliche Recht hat, den Zugang zu einem von ihm bereitgestellten geschützten Dienst in verständlicher Form von seiner vorherigen individuellen Erlaubnis abhängig zu machen. Der »Eingriff in das Recht auf Zugangskontrolle« wird von der Strafbestimmung des § 10 ZuKG erfasst.

Strafbar macht sich gem § 10 Abs 1 ZuKG, wer gewerbsmäßig (iSd § 70) Umgehungsvorrichtungen vertreibt, verkauft, vermietet oder verpachtet. Eine Umgehungsvorrichtung ist ein Gerät oder Computerprogramm, das dazu bestimmt oder angepasst ist, den Zugang zu einem geschützten Dienst in verständlicher Form ohne Erlaubnis des Diensteanbieters zu ermöglichen (§ 2 Z 8 ZuKG).[1707] Beispielsweise fallen va Decoder, Smartcards, Software zum »Knacken« von Passwörtern (vgl auch »Brute Force«-Programme) oder Autorisierungscodes und sonstige Entschlüsselungstechniken darunter.[1708] Generell setzt Gewerbsmäßigkeit die Vorsatzform der Absicht (iSd § 5 Abs 2) voraus, da es dem gewerbsmäßig handelnden Täter gerade darauf ankommt, sich durch die Tatwiederholung eine fortlaufende Einnahmequelle zu verschaffen.[1709]

1702 Zugangskontrollgesetz, BGBl I 60/2000 idF I 32/2001.

1703 Richtlinie 98/84/EG des Europäischen Parlaments und des Rates vom 20. November 1998 über den rechtlichen Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten, ABl L 1998/320, 54.

1704 Vgl ErlRV 99 BlgNR XXI. GP, 6; weiters *Reindl,* E-Commerce, 174.

1705 Siehe ErlRV 99 BlgNR XXI. GP, 6.

1706 Vgl *Reindl,* E-Commerce, 189.

1707 Zur Auslegung des Begriffs der »illegalen Vorrichtung« des Art 2 lit e Zugangskontroll-RL auf europäischer Ebene siehe etwa EuGH 04.10.2011, C-403/08, C-429/08 (Football Association Premier League Ltd ua bzw Murphy) = jusIT 2012/20, 49 *(Staudegger*).

1708 Vgl ErlRV 99 BlgNR XXI. GP, 11.

1709 Vgl *Jerabek* in WK² § 70 Rz 2.

Anders als bei § 126c Abs 1 Z 1 des Kernstrafrechts und (§ 91 Abs 1 iVm) § 90b[1710] (aber strittig bei § 90c[1711]) UrhG[1712] – deren Tatobjekte ausschließlich für illegale Zwecke Verwendung finden können[1713] – sind als Umgehungsvorrichtungen des § 10 ZuKG nach den GMat unter Bezugnahme auf die RL auch multifunktionale »Geräte« (iSv Hard- und Software) erfasst: »Aus diesem Grund kann die Strafsanktion […] nicht auf Geräte oder Computerprogramme beschränkt werden, die ausschließlich dazu bestimmt sind, technische Zugangskontrollmechanismen zu umgehen«.[1714] Zur Abgrenzung des ZuKG zum UrhG ist noch anzumerken, dass es sich bei Erstgenanntem nicht um »Werke« geistiger Schöpfungen iSd UrhG handeln muss.

Als geschützter Dienst gem § 2 Z 2 ZuKG gelten: eine Fernsehsendung, eine Radiosendung oder ein Dienst der Informationsgesellschaft, die oder der gegen Entgelt und unter einer Zugangskontrolle erbracht wird, einschließlich der Zugangskontrolle für solche Dienste, soweit sie als eigenständiger Dienst anzusehen sind. In den Erl werden als Beispiele für zugangskontrollierte Dienste das Pay-TV[1715], geschützte Video-auf-Abruf-Dienste und passwortgesicherte Internetdienste angeführt.[1716] Darüber hinaus sind im Einklang mit Art 2 lit a RL 98/84/EG ebenfalls auch eigenständige Dienste der Zugangskontrolle, die selbst die eigentliche Zugangskontrolle gewährleisten, soweit sie als eigenständige Dienste anzusehen sind, mitumfasst. Zugangskontrolle bedeutet im Sinne dieses Gesetzes jede technische Maß-

1710 Mittel, die auch noch legale Verwendungszwecke haben, sind ausgenommen (vgl Art 7 Abs 1 lit c RL 2009/24/EG (kodifizierte Fassung); weiters ErlRV 40 BlgNR XXII. GP, 44).

1711 § 90c Abs 3 UrhG legt als ein Kriterium eines solchen Umgehungsmittels bzw einer Umgehungsdienstleistung fest, dass diese, »abgesehen von der Umgehung wirksamer technischer Maßnahmen, nur einen begrenzten wirtschaftlichen Zweck oder Nutzen haben« müssen. Einem Teil der Lehre folgend fallen »Dual-use Devices« nur unter die Bestimmung, sofern sie den Umgehungszweck als »Hauptzweck« haben (idS wohl *Wiebe,* Das neue »digitale« Urheberrecht – Eine erste Bewertung, MR 2003, 309; auch *Neubauer,* Technische Schutzmaßnahmen und Recht, in Wiebe [Hrsg], Internetrecht. Zivilrechtliche Rahmenbedingungen des elektronischen Geschäftsverkehrs [2004] 113 [121]); aA *Stockinger/Nemetz* in Kucsko [Hrsg], urheber.recht § 90c Pkt 6.2 [Stand Dezember 2007]).

1712 BGBl 1936/111 idF I 32/2003.

1713 Siehe dazu schon krit die Ausführungen zu den Tatobjekten des § 126c Abs 1 Z 1 (S 321 ff).

1714 Siehe ErlRV 99 BlgNR XXI. GP, 17 f.

1715 Siehe dazu *Engin-Deniz/Grünzweig,* P-TV-Piraterie im Strafrecht, ecolex 2001, 587.

1716 Vgl ErlRV 99 BlgNR XXI. GP, 9.

nahme oder Vorrichtung, die den Zugang zu einem geschützten Dienst in verständlicher Form von einer vorherigen individuellen Erlaubnis abhängig macht (§ 2 Z 6 ZuKG).

»Dienste der Informationsgesellschaft« werden in § 1 Abs 1 Z 2 NotifG 1999[1717] definiert. Danach muss die Dienstleistung als Dienst der Informationsgesellschaft drei wesentliche Merkmale erfüllen: ihre Erbringung muss 1. im Fernabsatz (lit a), 2. elektronisch (lit b) und 3. auf individuellen Abruf des Empfängers (lit c) erfolgen.[1718] In der Regel hat sie darüber hinaus gegen Entgelt zu erfolgen. Der EuGH stellt dazu klar, dass als »Entgelt« die wirtschaftliche Gegenleistung für die betreffende Leistung gemeint ist.[1719] Dadurch wird aber darüber hinaus angezeigt, dass die – ausschließlich wirtschaftlichen – Tätigkeiten auch Dienste erfassen, die nicht von demjenigen vergütet werden müssen, der sie empfängt.[1720]

Gem § 10 Abs 2 ZuKG ist ebenso zu bestrafen, wer gewerbsmäßig (§ 70) Umgehungsvorrichtungen herstellt, einführt oder mit dem Vorsatz erwirbt oder innehat, dass diese auf die im Abs 1 beschriebene Art und Weise in Verkehr gebracht werden oder dass mit ihrer Hilfe anderen der Zugang zu einem geschützten Dienst ermöglicht wird.

Sämtliche Fälle der strafrechtlichen Sanktionen des § 10 ZuKG treffen ausschließlich gewerblich handelnde Täter. Vielmehr noch stellt § 10 Abs 3 ZuKG ausdrücklich klar, dass private Nutzer von Umgehungsvorrichtungen nicht – auch nicht als Beteiligte (iSd § 12 zweiter und dritter Fall) – strafbar sind.

Wie in den GMat ausgeführt wird, soll der Inhaber eines Unternehmens nicht nur für eigenes Tun, sondern auch dafür einstehen, dass er »vorsätzlich« einen im Betrieb seines Unternehmens von einem Bediensteten oder Beauftragten begangenen gewerbsmäßigen Eingriff in das Recht der Zugangskontrolle nicht verhindert (vgl »Begehung durch Unterlassen« iSd § 2 bzw subsidiär auch § 286).[1721] Die Garantenstellung des Inhabers lässt sich wohl ex lege aus § 5 ZuKG begründen, da dort ua Folgendes normiert ist: »Der Inhaber eines Unternehmens kann we-

1717 NotifG 1999, BGBl I 183/1999.

1718 Vgl ErlRV 1898 BlgNR XX. GP, 12; Beispiele für keine solchen Dienste finden sich in Anlage 1 der RV 1898 BlgNR XX. GP, 7.

1719 Vgl EuGH 07.12.1993, C-109/92 (Wirth/Landeshauptstadt Hannover); vgl auch ErlRV 99 BlgNR XXI. GP, 8 f.

1720 Siehe ErlRV 99 BlgNR XXI. GP, 10.

1721 Vgl ErlRV 99 BlgNR XXI. GP, 18.

gen einer solchen unerlaubten Handlung auch dann auf Unterlassung belangt werden, wenn die Handlung im Betrieb seines Unternehmens von einem Bediensteten oder Beauftragten begangen worden ist oder von einer solchen Person droht«.[1722]

§ 10 Abs 4 ZuKG sieht einen besonderen Entschuldigungsgrund für Bedienstete oder Beauftragte eines Unternehmens vor, wenn sie sich gegen die Anordnungen des Dienst- oder Auftraggebers nicht zur Wehr setzen konnten. In diesem Fall sollen sie strafrechtlich nicht zur Verantwortung gezogen werden können.

§ 10 ZuKG ist – wie § 126c im StGB – ein Vorbereitungsdelikt, wobei es aufgrund ähnlicher Tatbestandsmerkmale zu Subsumtions- und Abgrenzungsschwierigkeiten kommen kann. Wesentliches Unterscheidungselement ist die ausschließlich gewerbsmäßige Begehung in allen Varianten des § 10 ZuKG, weshalb sie auch die speziellere Norm ist und § 126c ihr gegenüber zurücktritt.[1723] Auch spricht die unterschiedlich hohe Strafdrohung (§ 126c – Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen; § 10 ZuKG – Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bis zu 360 Tagessätzen) für eine materielle Subsidiarität des § 126c.

Im Gegensatz zu § 126c, bei dem es sich um ein Offizialdelikt handelt, ist § 10 ZuKG – in Anlehnung[1724] an § 91 Abs 3 UrhG – ein Privatanklagedelikt (§ 10 Abs 5 ZuKG). Als Verletzter ist ausschließlich der Diensteanbieter zu verstehen. Dieser kann – innerhalb der Verjährung prozessual unbefristet – einen Strafantrag (§ 210 Abs 1 StPO) oder einen selbstständigen Antrag auf Erlassung vermögensrechtlicher Anordnungen nach § 445 StPO beim zuständigen Gericht einbringen (§ 71 Abs 1 StPO). Sachlich zuständig ist gem § 31 Abs 4 Z 1 StPO der Einzelrichter des Landesgerichts. Ein Ermittlungsverfahren findet hierbei gem § 71 Abs 1 letzter Satz StPO nicht statt. Besondere prozessuale Bestimmungen finden sich in § 11 ZuKG (Einziehung) und § 12 ZuKG (Beschlagnahme).

1722 Vgl etwa *Bergauer/Schmölzer* in Jahnel/Mader/Staudegger, IT-Recht[3], 635 (676).
1723 Siehe ErlRV 1166 BlgNR XXI. GP, 29.
1724 Vgl ErlRV 99 BlgNR XXI. GP, 18.

D. Betrügerischer Datenverarbeitungsmissbrauch (§ 148a)

> § 148a (1) Wer mit dem Vorsatz, sich oder einen Dritten unrechtmäßig zu bereichern, einen anderen dadurch am Vermögen schädigt, daß er das Ergebnis einer automationsunterstützten Datenverarbeitung durch Gestaltung des Programms, durch Eingabe, Veränderung, Löschung oder Unterdrückung von Daten oder sonst durch Einwirkung auf den Ablauf des Verarbeitungsvorgangs beeinflußt, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.
>
> (2) Wer die Tat gewerbsmäßig begeht oder durch die Tat einen Euro 3,– 000 übersteigenden Schaden herbeiführt, ist mit Freiheitsstrafe bis zu drei Jahren, wer durch die Tat einen Euro 50,– 000 übersteigenden Schaden herbeiführt, mit Freiheitsstrafe von einem bis zu zehn Jahren zu bestrafen.[1725]

Zur Schließung einer echten Gesetzeslücke wurde mit dem StRÄG 1987 der »Betrügerische Datenverarbeitungsmissbrauch« in § 148a eingeführt, da es für die Unterordnung von Manipulationen einer Datenverarbeitung unter den Betrug (§ 146), an der Täuschung eines Menschen fehlt und es für eine etwaige Subsumtion unter die Untreue (§ 153), idR an einer dem Täter eingeräumten Rechtsmacht zur Verfügung über das betroffene Vermögen mangelt.[1726] Im Unterschied zum Betrug, bei dem der Getäuschte letztlich selbst die schädigende Vermögensverfügung tätigen muss (sog »Selbstschädigungsdelikt«[1727]), ist beim (vermeintlich betrugsähnlichen) Betrügerischen Datenverarbeitungsmissbrauch kein Mensch zwischengeschaltet, weshalb der Täter selbst durch die Manipulation der automationsunterstützten Datenverarbeitung unmittelbar den Vermögensschaden herbeiführen muss.[1728] Daher handelt es sich bei § 148a um ein Fremdschädigungsdelikt.[1729]

1725 BGBl 60/1974 idF I 136/2004.

1726 Vgl bereits JAB 359 BlgNR XVII. GP, 16 f; weiters *Schmölzer,* RZ 1986, 178.

1727 Siehe die Kritik zur Unschärfe dieses Begriffs iZm der Deliktsstruktur des Betrugs bei *Triffterer* in SbgK § 148a Rz 4 (aF Stand Dezember 1992).

1728 Siehe dazu auch unten.

1729 Siehe *Kienapfel,* BT II[3] § 148a Rz 5; weiters *Leukauf/Steininger,* StGB[3] § 148a Rz 5; *Lewisch,* BT I[2], 241.

1. Zum Tatobjekt »Ergebnis einer Datenverarbeitung«

Der objektive Tatbestand verlangt im Wesentlichen die Vermögensschädigung eines anderen durch die »Beeinflussung des Ergebnisses einer automationsunterstützten Datenverarbeitung«.

Tatobjekt ist – neben dem »anderen« Menschen – primär das »Ergebnis einer automationsunterstützten Datenverarbeitung«. Ein solches Datenverarbeitungsergebnis muss durch die tatbestandlich explizit genannten Begehungsweisen beeinflusst werden. Es spielt dem Wortlaut nach – entgegen der Ansicht *Wegscheiders*[1730] – keine Rolle, ob der Täter über die Datenverarbeitung verfügen darf oder nicht. Es muss sich daher nicht um eine fremde automationsunterstützte Datenverarbeitung handeln. Dies ergibt sich bereits aus den GMat, in denen auch an an Datenverarbeitungsanlagen tätige Personen gedacht wird, denen es technisch möglich ist, entsprechende Vorgänge zu beeinflussen.[1731] Zur Klärung, was man unter einer automationsunterstützten Datenverarbeitung iSd § 148a Abs 1 versteht, kann auf § 4 Z 7 DSG 2000 zurückgegriffen werden[1732], wobei es für § 148a – im Gegensatz zum DSG 2000 – nicht auf einen rein personenbezogenen Charakter der Datenverarbeitung ankommt.[1733] In § 3 Z 5 DSG 1978[1734] wurde noch ausdrücklich die »Datenverarbeitung« in den Begriffsbestimmungen genannt. Mit Einführung des DSG 2000[1735] wurde daraus – im Übrigen fast wortgleich – in § 4 Z 7 DSG 2000 die »Datenanwendung«.[1736] Darunter versteht man die Summe der in ihrem Ablauf logisch verbundenen Verwendungsschritte, die zur Erreichung eines inhaltlich bestimmten Ergebnisses (des Zweckes der Datenanwendung) geordnet sind und zur Gänze oder auch nur teilweise automationsunterstützt, also maschinell und programmgesteuert, erfolgen (automationsunterstützte Datenanwendung).

Im Wesentlichen könnte man aber auch die Definition des »Computersystems« nach § 74 Abs 1 Z 8 iVm Art 1 lit a CCC zur Auslegung

---

1730 Vgl *Wegscheider,* BT[4], 240.
1731 Siehe JAB 359 BlgNR XVII. GP, 15.
1732 Siehe zur diesbezüglichen »Annäherung der Ausdrucksweise an die des Datenschutzgesetzes« JAB 359 BlgNR XVII. GP, 18.
1733 Insofern siehe § 74 Abs 2.
1734 BGBl 565/1978 idF 370/1986.
1735 BGBl I 165/1999.
1736 Siehe dazu ErlRV 1613 BlgNR XX. GP, 38.

heranziehen. Der Strafgesetzgeber versteht unter einem »Computersystem« sowohl einzelne als auch verbundene Vorrichtungen, die der automationsunterstützten Datenverarbeitung dienen und verweist dabei einerseits in den GMat[1737] auf Art 1 lit a CCC[1738] und andererseits durch die ausdrückliche Bezugnahme auf eine automationsunterstützte »Datenverarbeitung« indirekt wiederum auf das Datenschutzgesetz.

In beiden Fällen muss eine Datenverarbeitung vorliegen, die ein »inhaltlich bestimmtes Ergebnis« hervorbringt und daher einem bestimmten Zweck dient. Ein bestimmter, »personenbezogene Daten« betreffender Zweck, wie im DSG 2000, ist aber aufgrund der Klarstellung bezüglich der Dateninhalte in § 74 Abs 2 für das strafrechtliche Datenverständnis nicht gefordert.

Die erschöpfend aufgezählten Handlungsmodalitäten (alternativer Mischtatbestand) umfassen die Gestaltung des Programms (= Programmmanipulation), die Eingabe, Veränderung oder Löschung oder Unterdrückung[1739] von Daten iSd § 74 Abs 2 (= Inputmanipulation) oder sonstige Einwirkungen auf den Ablauf des Verarbeitungsvorgangs. Es handelt sich dabei um ein verhaltensgebundenes Delikt, da das Ergebnis der Datenverarbeitung ausschließlich durch eine der vorgegebenen Begehungsweisen beeinflusst werden muss.

Im Wesentlichen entspricht § 148a nunmehr den Vorgaben des Art 8 CCC (Computer-related fraud), der Folgendes vorsieht:

> »Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: a any input, alteration, deletion or suppression of computer data; b any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.«

1737 Vgl ErlRV 1166 BlgNR XXI. GP, 23.

1738 Der gleichlautende Konventionsbegriff umfasst »eine Vorrichtung oder eine Gruppe miteinander verbundener oder zusammenhängender Vorrichtungen, die einzeln oder zu mehreren auf der Grundlage eines Programms automatische Datenverarbeitung durchführen«.

1739 Die Tathandlung der Unterdrückung wurde aber erst mit dem StRÄG 2002 in Umsetzung des Art 8 CCC ergänzt.

Das Ergebnis einer automationsunterstützten Datenverarbeitung muss durch die tatbestandlich genannten Begehungsweisen beeinflusst werden.

2. Gestaltung des Computerprogramms

Die erste Kategorie der Begehungsweisen des § 148a behandelt die »Gestaltung des Programms«. Sie erfasst grundsätzlich jegliche Veränderungen des konkreten ausführbaren Computerprogramms.[1740] Dabei wird das Programm selbst oder dessen vordefinierter Ablauf sachwidrig verändert.[1741] Vorstellbar sind Handlungen, bei denen der Täter das Programm selbst modifiziert, dh einzelne Verarbeitungsschritte (Algorithmen[1742]) abändert, umgeht oder hinzufügt.[1743] Aus dem Wortlaut geht jedoch auch hervor, dass es sich um Veränderungen »des« Programms handeln muss, also eines Programms, das bereits (zumindest[1744]) Teil der vom Täter anvisierten automationsunterstützten Datenverarbeitung ist. Daher ist das Hinzufügen eines neuen eigenen Programms, das von vornherein schon für die kriminellen Zwecke des Täters gestaltet wurde, von dieser Handlungsalternative nicht erfasst.[1745] Die Abgrenzung der Programmmanipulation zur Inputmanipulation verschwimmt, da für eine Gestaltung eines Programms ebenfalls Daten eingegeben werden müssen, um neue Handlungsanweisungen zu ergänzen und bestehende zu verändern oder zu löschen (zB Eingabe einer Löschanweisung).

1740 Gemeint ist daher ausschließlich die operative Ausdrucksform eines Computerprogramms im »Object Code« oder mittels Interpretersoftware unmittelbar ausführbarem »Source Code« (zB bei PHP, HTML, auch Java).

1741 Vgl auch JAB 359 BlgNR XVII. GP, 17; weiters *Leukauf/Steininger,* StGB[3] § 148a Rz 15.

1742 Rechenvorschrift oder Handlungsanweisung zur Lösung mathematischer Probleme (siehe zu Algorithmen allgemein *Kersken,* IT-Handbuch[5], 33 f bzw 91).

1743 Siehe zB *Triffterer* in SbgK § 148a Rz 15 (aF Stand Dezember 1992); nunmehr auch *Komenda/Madl* in SbgK § 148a (Stand Dezember 2013); weiters *Jaburek/Schmölzer,* Computer-Kriminalität, 58 f.

1744 Es reicht aber bereits aus, dass der Täter ein selbstständiges Teilprogramm der entsprechenden Datenverarbeitung gestaltet.

1745 AA *Triffterer* in SbgK § 148a Rz 15 (aF Stand Dezember 1992).

3. Manipulation mittels Computerdaten

Die zweite Kategorie der Begehungsweisen fokussiert auf die Beeinflussung eines Datenverarbeitungsergebnisses durch die Verwendung von Daten iSd § 74 Abs 2. Abgestellt wird im Wesentlichen aber wieder auf »Computerdaten« (hier: Daten im engen Sinn), weshalb der Datenbegriff in § 74 Abs 2 diesbezüglich nicht viel weiter hilft.[1746] Lediglich eine Aussage kann dazu getroffen werden, dass nämlich der Inhalt der Daten (hier: Daten im weiten Sinn bzw Information) für den Anwendungsbereich des § 148a unbeachtlich ist. Konkret wird das Eingeben, Verändern, Löschen oder Unterdrücken von Daten genannt. Die dafür verwendete Bezeichnung »Inputmanipulation« ist jedoch seit Ergänzung um die Datenunterdrückung nicht mehr ganz zutreffend, da dabei nicht unbedingt Daten über Eingabegeräte eingegeben werden müssen, wie es beim Eingeben, Verändern oder Löschen zwangsläufig der Fall sein muss. Anzumerken ist aber auch, dass bei der Eingabe selbst die Daten noch nicht in technischer Repräsentation (Codierung) vorliegen, da dies erst durch entsprechende Verarbeitungsprozesse bezüglich dieser »analogen Daten« geschieht. Zudem reicht es für eine Datenunterdrückung aus, dass verarbeitungsrelevante Daten durch das Handeln des Täters nicht für die konkrete Datenverarbeitung verwendet werden können. Unbeachtlich ist daher die Art und Weise der Datenunterdrückung, die nicht ausschließlich im Wege einer automationsunterstützten Datenverarbeitung realisiert werden muss, sofern sich eine solche Unterdrückung auf das Ergebnis der Datenverarbeitung auswirken kann. Man könnte hier daran denken, dass der Täter ein System durch schlichtes Abschalten von datenverarbeitenden Teilkomponenten (iS einer Datenunterdrückung) dieser Datenverarbeitungsanlage in seiner ordnungsgemäßen Datenverarbeitung beeinträchtigt und dadurch das Ergebnis derart beeinflusst, dass ein Vermögensschaden herbeigeführt wird.

4. Sonstige Einwirkungen

Die dritte Kategorie stellt – sehr weit gehalten – auf sonstige Einwirkungen auf den Ablauf des Datenverarbeitungsvorganges ab. Darunter

1746 Siehe dazu S 60 ff.

könnten die in den GMat angesprochenen Output- und Konsolenmanipulationen fallen, bei denen durch Einwirkungen auf den Ablauf des Ausdruckvorgangs unrichtige Daten ausgegeben oder der Ausdruck überhaupt unterbunden werden.[1747]

a. Outputmanipulation

Der Auffassung *Triffterers*[1748], dass der historische Gesetzgeber von einem sehr weiten Verständnis eines »Verarbeitungsvorgangs« ausgehen müsse, da sich nur in diesem Fall Output-Manipulationen darunter subsumieren ließen, weil sonst nicht einleuchten würde, warum sie noch zur »Verarbeitung« zählen, ist nicht zwangsläufig zu folgen. Dies ergibt sich bereits daraus, dass Datenverarbeitungsprozesse sinnvollerweise stets auch einen Output haben. Die per Datenverarbeitung erzielten Arbeitsergebnisse werden über das Ausgabewerk [1749] an eine Umweltschnittstelle[1750] ausgegeben.[1751] Der Output ist somit je nachdem, welche Ausgabefunktionalität programmgemäß definiert wurde, Gegenstand des Verarbeitungsvorgangs. Dies macht auch Sinn, da andernfalls zwar Eingaben vom System für den Nutzer berechnet, diesem aber die Ergebnisse nicht bekannt gegeben werden können. Aus diesem Grund muss man mE zwei Arten des Outputs unterscheiden: den »internen Berechnungs-Output« und den »externen Ausgabe-Output«.

Unter dem internen Output sind die bei der Datenverarbeitung mittels Prozessoren-gesteuerter Berechnung hervorgebrachten Ergebnisse zu verstehen, die dem Ausgabewerk[1752] übermittelt wurden und die noch nicht an die Umweltschnittstelle übergeben wurden. Der externe Output könnte in der tatsächlichen für den Nutzer bestimmten Kenntnisnahmemöglichkeit über diverse Ausgabegeräte gesehen werden. Beide dieser vordefinierten Programm-Outputs gehören zum Verarbeitungsvorgang.

1747 Vgl JAB 359 BlgNR XVII. GP, 17.

1748 Siehe aber dazu mit einem offensichtlich sehr engen Verständnis davon *Triffterer* in SbgK § 148a Rz 30 (aF Stand Dezember 1992).

1749 Die Bezeichnung »Ausgabewerk« beschreibt eine der fünf Funktionseinheiten des »Universalrechners« nach von Neumann.

1750 Darunter werden sämtliche Ausgabegeräte zusammengefasst, welche den Programm-Output dem Nutzer zur Kenntnis bringt (Grafikarten bzw Monitore, Drucker, Massenspeicher aber auch andere Computersysteme usw).

1751 Vgl *Schramm* in Jahnel/Schramm/Staudegger, Informatikrecht², 1 (3).

1752 Das Ausgabewerk als Funktionseinheit, im Unterschied zu »Ausgabegeräten«.

Aus diesem Grund lässt sich das tatbestandliche Ergebnis in zwei funktional verschiedenen Teilergebnissen zum Ausdruck bringen, die jeweils für sich beeinflusst werden können. Auf der einen Seite kann das (interne) »Berechnungsergebnis« manipuliert werden, auf der anderen der für die Kenntnisnahme des Nutzers bestimmte Ausgabe-Output. Um den Ausgabe-Output zu beeinflussen, könnte zB das eigentliche Berechnungsergebnis auf dem Weg zum Ausgabegerät verändert werden. Um das Tatobjekt des § 148a Abs 1 näher zu determinieren, kommt es darauf an, welche Ausgabeform in einem konkreten Sachverhalt programmgemäß vordefiniert wurde. Ein »Ausdruck« auf Papier ist nur dann Teil des Ergebnisses eines Datenverarbeitungsvorgangs, wenn er auch programmtechnisch vorgesehen ist und folglich für die Verursachung eines deliktsnotwendigen Vermögensschadens relevant ist. Wird ein Ausdruck für den gewöhnlichen Ablauf des Datenverarbeitungsvorgangs nicht benötigt und ist er nur zu Kontrollzwecken oder zur Archivierung von Programmabläufen programmimmanent, so handelt es sich bei einer Manipulation dieser Ausgabeform nicht um einen notwendigen und daher deliktsunbeachtlichen Output, der nach etwaigen anderen Strafbestimmungen zu beurteilen ist.[1753]

Geht es um die Manipulation einer Datenverarbeitungsanlage, welche eine Druckausgabe als einen wesentlichen Teil des Datenverarbeitungsvorgangs mitumfasst, und wird lediglich der Ausdruck – noch während der Verarbeitungsphase[1754] – manipuliert, liegt ein Beeinflussen des Ausgabe-Outputs vor.

Ist dagegen für einen entsprechenden Datenverarbeitungsvorgang kein Ausdruck gezwungener Maßen vorgesehen, wie etwa bei einer Giralgeldüberweisung im Zuge des Online-Bankings, kann ein solcher aber dennoch zB zu Beweiszwecken angefertigt werden, ist dieser Ausdruck nicht mehr zum Ergebnis des gegenständlichen Datenverarbeitungsprozesses der Online-Buchung zu werten und daher nicht von § 148a Abs 1 erfasst.

1753 In diesem Sinne auch *Kienapfel,* BT II³ § 148a Rz 32; auch *Kirchbacher/Presslauer* in WK² § 148a Rz 23.

1754 Wird der Ausdruck nach erfolgtem Druckvorgang manipuliert, werden die Bestimmungen des Urkundenstrafrechts zu prüfen sein.

b. Konsolenmanipulation

Unter Konsolenmanipulationen verstehen viele im juristischen Schrifttum das Einwirken auf den Datenverarbeitungsprozess während des Ablaufs – also in Echtzeit – von der Konsole aus, zB über die Tastatur.[1755]

Aus technischer Sicht stellt die »Konsole« (oder Kommandozeilenoberfläche[1756]) einen Spezialfall der Ein- und Ausgabensteuerung in der Bereitstellung der Benutzeroberfläche dar. Die Konsole ermöglicht das dialogbasierte Arbeiten, in dem der Nutzer zB per Tastatur[1757] eines Terminals Befehle eingibt und vom System auf einem Ausgabegerät Antworten erhält.[1758] Darunter könnte man sich zB auch Spielautomaten[1759] eines Casinos, Warenautomaten oder Geld- oder Parkscheinautomaten vorstellen. Wer sich durch missbräuchliches Einwirken auf einen Leistungsautomaten eine Leistung von diesem verschafft, ohne das Entgelt (vollständig) zu entrichten, erfüllt ggf auch den Tatbestand des § 149 Abs 2. Ein Missbrauch von Leistungsautomaten kommt aber nicht für Warenautomaten in Betracht. Ein wesentliches Kriterium für die Anwendbarkeit des § 149 Abs 2 ist darüber hinaus, dass die Automaten ihre Leistung erst gegen vorherige Entgeltzahlung erbringen. Warenautomaten sind nicht erfasst, diese werden vom Diebstahl (§§ 127 f) oder von der Entwendung (§ 141) berücksichtigt.[1760]

Man könnte sich vorstellen, dass der Täter in Echtzeit des Programmlaufs über manipulative Eingriffe mittels der Tastatur das Datenverarbeitungsergebnis beeinflusst. Zum Beispiel könnte die Datenverarbeitung durch das Betätigen diverser Tastenkombinationen oder die Mehrfacheingabe von Befehlen abgebrochen, überlastet oder Programmteile übersprungen werden.

1755 Vgl etwa *Wegscheider,* BT[4], 241; *Kirchbacher/Presslauer* in WK[2] § 148a Rz 21; *Kienapfel,* BT II[3] § 148a Rz 29; etwas differenzierter *Triffterer* in SbgK § 148a Rz 31 (aF Stand Dezember 1992); *Komenda/Madl* in SbgK § 148a Rz 53.

1756 In Betriebssystemen oft auch »Shell« genannt.

1757 Dabei muss es sich nicht um eine vollständige Tastatur handeln

1758 Siehe dazu *Kersken,* IT-Handbuch[5], 282 und 296 f.

1759 Für Spielautomaten iZm § 149 Abs 2 siehe *Schmölzer,* Geldspielautomaten im österreichischen Strafrecht, ÖJZ 1993, 507.

1760 Siehe dazu *Schallmoser* in SbgK § 149 Rz 44 (Stand November 2011); *Kirchbacher/Presslauer* in WK[2] § 149 Rz 14 ff (Stand November 2009); *Schmölzer,* Geldspielautomaten im österreichischen Strafrecht, ÖJZ 1993, 507; *Kienapfel,* BT II[3] § 149 Rz 32.

Im Wesentlichen werden aber Outputmanipulationen und Konsolenmanipulationen idR bereits von den Inputmanipulationsmöglichkeiten einschließlich der Datenunterdrückung oder der Programmmanipulation erfasst sein, da dabei regelmäßig auch Daten eingegeben und verarbeitet werden müssen.[1761]

5. »Beeinflussung« des Datenverarbeitungsergebnisses

»Beeinflusst« ist ein Ergebnis einer Datenverarbeitung nach hM dann, wenn ein von der materiellen Rechtslage abweichendes Resultat erzielt wird.[1762] Demnach ist es nach der überwiegenden Meinung auch unerheblich, ob das Arbeitsergebnis gegenüber einem programmgemäßen Ablauf verändert (verfälscht) ist, da es um die schlichte Benützung und nicht um eine Beeinträchtigung technischer Gegebenheiten geht.[1763] Das bloße Auslösen eines Datenverarbeitungsprozesses als Beeinflussung der Datenverarbeitung reicht daher aus.[1764]

Mit anderen Worten, auch die Eingabe von richtigen und vollständigen Daten, zB Überweisungsdaten für eine Online-Geldtransaktion (PIN, TAN, Verfügernummer usw), durch die das System schließlich (technisch völlig unbeeinflusst und) programmgemäß veranlasst wird, Geldüberweisungen eines Unberechtigten zu akzeptieren, ist von einer solchen Beeinflussung des Ergebnisses erfasst. Der Täter bringt dabei das datenverarbeitende System durch bloße Nutzung desselben dazu, einen lediglich formell (technisch) Berechtigten eine Transaktion durchführen zulassen, ohne dass aber tatsächlich das Ergebnis bzw der Ablauf der Datenverarbeitung technisch beeinträchtigt wird.[1765]

Demgegenüber hält es *Schmölzer,* neben einem weiteren Teil der Lehre[1766], nach dem Wortlaut des Tatbestands für erforderlich, dass durch eine der genannten Handlungsmodalitäten das Ergebnis der automationsunterstützten Datenverarbeitung derart beeinflusst sein

---

1761 In dieselbe Richtung auch *Kienapfel,* BT II³ § 148a Rz 31.

1762 Siehe *Kirchbacher/Presslauer* in WK² § 148a Rz 11 mwN; weiters OGH 14.12.1995, 15 Os 131/95.

1763 Siehe eine Aufarbeitung der Diskussion bei *Reindl,* E-Commerce, 32 ff; Vgl auch *Kirchbacher/Presslauer* in WK² § 148a Rz 11 und 1.

1764 Siehe statt vieler *Birklbauer/Hilf/Tipold,* Strafrecht BT I² § 148a Rz 8 mwN; weiters *Komenda/Madl* in SbgK § 148a Rz 68; aA *Schmölzer,* EDVuR 1990, 30; weiters *Leukauf/Steininger,* StGB³ § 148a Rz 21; auch *Lewisch,* BT I², 242.

1765 Siehe auch schon *Bergauer,* RZ 2006, 82.

1766 ZB *Leukauf/Steininger,* StGB³ § 148a Rz 12 und 18.

muss, dass auf den technischen Ablauf des Verarbeitungsvorgangs insofern eingewirkt wird, als ein iS der Datenverarbeitung formell falsches Resultat entsteht; ein bloß »materiell ungerechtes« Ergebnis reicht ihr zur Folge nicht aus.[1767]

Das Abstellen auf eine »unrichtige« Gestaltung eines Programms oder die Eingabe von »unrichtigen oder unvollständigen« Daten hat der Gesetzgeber bewusst vermieden, »weil sich das Unrechtmäßige der betreffenden Handlungen bereits aus dem auf eine unrechtmäßige Bereicherung gerichteten Vorsatz ergibt«.[1768] Der OGH stellt dazu unter Bezugnahme auf *Triffterer*[1769] ausdrücklich klar, dass Daten als gespeicherte Informationen für sich allein genommen weder richtig noch unrichtig sind. Erst wenn diese zur Realität in Beziehung gesetzt werden, lässt sich ihr Wahrheitsgehalt bestimmen. Dieser Argumentation folgend, sind daher Daten immer dann unrichtig, wenn sie den darzustellenden Lebenssachverhalt falsch wiedergeben.[1770] Der OGH stützt sich hier im Wesentlichen auf ein pragmatisches Verständnis des aus der Datenverarbeitung hervorgehenden Ergebnisses. Folglich interpretiert er die Beeinflussung eines Datenverarbeitungssystems subjektiv-zweckorientiert aus Sicht der Beteiligten und nicht nach einem objektiv-technischen Maßstab. *Lewisch* stellt allerdings iZm der widerrechtlichen Bargeldbehebung an einem Bankomaten zutreffend fest, dass zwar die bloße Verwendung einer fremden Bankomatkarte unautorisiert erfolge, aber diesfalls noch nicht das Ergebnis einer Datenverarbeitung »beeinflusst« werde.[1771] Wendet man die gerade angesprochene »Fiktion der Datenwahrheit« auf diesen Fall an, so liegen unrichtige Daten vor, weil der Verwender der fremden Bankomatkarte materiell nicht zur Geldbehebung berechtigt ist. Dabei spielt es offensichtlich für die Vertreter dieser Ansicht keine Rolle, dass das Ergebnis des Datenverarbeitungsprozesses in rein technischer Hinsicht unbeeinflusst bleibt.

1767 Vgl *Schmölzer,* EDVuR 1990, 30.
1768 Vgl JAB 359 BlgNR XVII. GP, 18.
1769 *Triffterer* in SbgK § 148a Rz 20 (aF Stand Dezember 1992).
1770 Siehe OGH 14.12.1995, 15 Os 131/95.
1771 Siehe *Lewisch,* BT I², 242.

a. Kritik an der Sozialadäquanz der äußeren Tatseite

Schmölzer kritisiert zurecht, dass es wohl nicht zulässig sei, in Ermangelung eines ausdrücklichen Tatbestandsmerkmals »unbefugt« (arg »unbefugte« Eingabe von Daten) »aus einer Zusammenschau und Verquickung objektiver und subjektiver Tatbestandsmerkmale diesen Mangel zu sanieren«, weshalb »die Aktivierung eines regulär ablaufenden elektronisch gesteuerten Prozesses durch die Eingabe vollständiger und richtiger Daten, die nur zufälligerweise unzulässig – weil mit dem Vorsatz, sich unrechtmäßig bereichern zu wollen – verwendet werden«, noch nicht dem Wortlaut des Gesetzes Genüge tun könne.[1772]

Aus diesem Grund reicht der Anwendungsbereich des § 148a auch viel weiter als der des Betrugs nach § 146, weil Letzterer nur durch die Behauptung unwahrer Tatsachen realisiert werden kann.[1773]

Schmölzer ist zuzustimmen, dass im Ergebnis jede bloß faktische Nutzung einer Datenverarbeitungsanlage bereits den objektiven Tatbestand erfüllt. Und zwar selbst dann, wenn es sich dabei um ein System handeln würde, über das der Nutzer selbst verfügen darf.[1774] Man müsste in einem solchen Fall – nicht unproblematisch[1775] – schon mit dem Fehlen einer sozial inadäquaten Handlung argumentieren, um die Rechtswidrigkeit auszuschließen und eine (objektive) Tatbestandsmäßigkeit zu verneinen. Eine ausdrückliche Verankerung eines Tatbestandsmerkmals wie zB »unbefugt« bzw »widerrechtlich«[1776] erscheint mE aber sehr deutlich angezeigt, weil gesetzliche Tatbilder generell sozial inadäquate Verhaltensweisen zum Ausdruck bringen sollen.

Man müsste somit (ähnlich wie bereits zu § 126c Abs 1 ausgeführt[1777]), um sinnvolle Ergebnisse zu erhalten, davon ausgehen, dass die mangelnde Rechtswidrigkeit – zumindest bezüglich der Benützung des Datenverarbeitungssystems – ein ungeschriebenes Tatbildmerkmal darstellt, das bei Vorhandensein im zu untersuchenden Lebenssachverhalt, die Tatbestandsmäßigkeit entfallen lässt.

1772 Vgl *Schmölzer,* EDVuR 1990, 30.
1773 Siehe *Kienapfel,* BT II[3] § 148a Rz 19.
1774 AA offenbar *Wegscheider,* BT[4], 240.
1775 Siehe dazu bereits die Auseinandersetzung iZm § 126c.
1776 Ein Handeln gegen den ausdrücklichen oder schlüssig erklärten Willen des Opfers wäre ebenfalls bereits ausreichend (vgl in einem anderen Zusammenhang ErlRV 1316 BlgNR XXII. GP, 4).
1777 Siehe dazu bereits oben zu § 126c.

Andernfalls gäbe es zwei Möglichkeiten eine Strafbarkeit in rein objektiver Hinsicht abzulehnen:

Zum einen muss es sich bei der »automationsunterstützten Datenverarbeitung« aus technischer Sicht überhaupt um ein System handeln, das faktisch in der Lage ist (iSd für § 148a entwickelten Dogmatik), einen »unmittelbaren« Vermögensschaden für einen anderen herbeizuführen. Eine automationsunterstützte Datenverarbeitung ist dann kein taugliches Tatobjekt, wenn damit überhaupt keine Vermögensverfügung technisch realisierbar wäre, weil es sich dabei zB um einen reinen Spielcomputer für Kinder handelt.[1778] Zudem muss es sich dem Wortlaut des § 148a zufolge, nicht um eine »fremde« Datenverarbeitung handeln.[1779] *Wegscheider* vertritt hingegen – ohne nähere Begründung – die Meinung, dass nur derjenige tatbestandsmäßig handeln könne, der keine Verfügungsbefugnis über die Datenverarbeitung hat.[1780] Dies ist aber weder dem Wortlaut zu entnehmen, noch aus den GMat ableitbar, geschweige denn rechtspolitisch erwünscht. Man denke dabei an Fälle, in denen ein Mitarbeiter über die Datenverarbeitungsanlage zwar formell verfügen darf, diese aber entgegen dem eigentlichen Bestimmungszweck für rechtswidrige Vermögensverschiebungen verwendet.[1781]

Zum anderen würde eine maßvolle, den Gesetzeswortlaut auf eine »unbefugte« Manipulation der Datenverarbeitung korrigierende teleologische Reduktion eine noch zulässige Rechtsfortbildung bedeuten.[1782]

Daneben würde als Korrektiv gegen eine Strafbarkeit ausschließlich der Entfall des erweiterten Vorsatzes (in Form der unrechtmäßigen Bereicherung) auf der subjektiven Tatseite wirken, wie es wohl auch dem Willen des historischen Gesetzgebers letztlich entsprechen dürfte, wenn in den GMat[1783] ausgeführt wird, dass sich das Unrechtmäßige der Handlungen aus dem erweiterten Vorsatz ergäbe. Dass einzig der erweiterte Vorsatz (hier: im Mindeststärkegrad eines dolus

1778 Der sog »Zeitdiebstahl« ist strafrechtlich gesehen unbeachtlich (siehe dazu auch bereits JAB 359 BlgNR XVII. GP, 16).

1779 AA *Wegscheider,* BT[4], 240.

1780 Siehe *Wegscheider,* BT[4], 240.

1781 Vgl auch JAB 359 BlgNR XVII. GP, 15.

1782 Vgl dazu jüngst die Zusammenfassung von Meinungen, die iZm dem zuweit gefassten Wortlaut des § 148a Abs 1 auf eine teleologische Reduktion abzielen *(Komenda/Madl* in SbgK § 148a Rz 40, 44, 48).

1783 Siehe JAB 359 BlgNR XVII. GP, 18.

eventualis) und daher lediglich eine »sozial inadäquate Intention« dafür ausschlaggebend sein soll, schießt mE über das Ziel hinaus. Daraus folgt, dass nicht vorrangig die Gefährlichkeit des objektiven Verhaltens bestraft wird, sondern die innere Einstellung und somit die Gesinnung des Täters, was ohnehin bedenklich erscheint.

Wo liegt die sozial inadäquate Gefährlichkeit der (objektiven) Tathandlungen des Betrügerischen Datenverarbeitungsmissbrauchs?

Es kann doch nicht die bloße Nutzung von tatbildlichen Datenverarbeitungen, ohne die Verarbeitungsvorgänge formell zu beeinträchtigen, bereits zu einer (zu weitreichenden) Kriminalisierung führen, die einzig durch das Vorhandensein eines subjektiven Elements (in concreto: Bereicherungsvorsatz) für eine Tatbestandsmäßigkeit ausschlaggebend ist. Jemand, der bspw berechtigterweise mit der Bankomatkarte seiner Ehefrau im Supermarkt Waren an einem POS-Terminal bzw Bankomatkassa bezahlt, würde bereits den objektiven Tatbestand erfüllen.

b. »Betrugsähnlichkeit«

Meines Erachtens fehlt es – was auch die hM mit ihrer Begründung einer »betrugsähnlichen« Konzeption[1784] des § 148a durch teleologisch-systematische Erwägungen indirekt fordern müsste – an einem dem Betrugstatbestand vergleichbaren objektiven Gefährlichkeitselement der Tathandlung.[1785]

Eine Betrugsähnlichkeit wird in der hM in mehreren Ausprägungen gesehen, so wurde § 148a zB als »Lückenschließer«[1786] in Bezug auf die fehlende Irrtumserregung bei einem Menschen normiert und auch systematisch unmittelbar bei den »Betrugsdelikten« eingegliedert. Darüber hinaus sei diese auch durch die Deliktsbezeichnung »Betrügerischer Datenverarbeitungsmissbrauch« indiziert.[1787] Dazu ist anzumerken, dass erst die Bezeichnung »Computerbetrug« im Gesetzwerdungsprozess diskutiert und nur aus dem Grund abgelehnt wurde, da man das Wort »Computer« vermeiden wollte.[1788]

1784 Zur Kritik an einer betrugsähnlichen Konzeption siehe gleich im Anschluss.
1785 Vgl auch jüngst *Komenda/Madl* in SbgK § 148a Rz 14 f.
1786 Vgl statt vieler RIS-Justiz RS0093560 mwN.
1787 Siehe dazu etwa *Reindl,* E-Commerce, 40 ff.
1788 Vgl JAB 359 BlgNR XVII. GP, 18.

Richtig ist auch, dass – nach den GMat – die Formulierung des erweiterten Vorsatzes ausdrücklich[1789] aus der Betrugsbestimmung übernommen und gleichzeitig darauf hingewiesen wurde, dass Manipulationen an Datenverarbeitungsanlagen einem Betrug gleichkommen.[1790]

Nicht zuletzt kann für die Betrugsähnlichkeit des § 148a noch ins Treffen geführt werden, dass ursprünglich an eine Einordnung der Tathandlung unmittelbar nach § 147 als Sonderform des schweren Betrugs gedacht war.[1791]

Reindl sieht es aus diesem Grund angebracht, die Tathandlungen des § 148a in einer »betrugsähnlichen Weise« auszulegen.[1792] Ihrem Ansatz folgend ist ein Sachverhalt einer »hypothetischen Mensch-anstelle-Maschine-Prüfung« zu unterziehen, und dabei zu fragen, ob auch der Tatbestand des Betrugs (§ 146) erfüllt wäre, wenn anstelle der Maschine ein Mensch gehandelt hätte.[1793] Ist eine Täuschungsähnlichkeit bei dieser inzidenten Prüfung anzunehmen, da der hinzugedachte Mensch aufgrund des Täterverhaltens getäuscht wurde, und wurde auch die Vermögensverfügung in betrugsähnlicher Weise verwirklicht, so sei § 148a anwendbar.[1794]

Eine inzidente fiktive Betrugsprüfung als Auslegungskriterium[1795] bei einem zwar ähnlichen, aber eigenständigen Delikt ist mE nicht angezeigt.

Obwohl konzediert werden muss, dass eine Betrugsähnlichkeit in den GMat an mehreren Stellen dargelegt wurde, ist mE davon auszugehen, dass die diesbezüglichen Argumente tatsächlich nicht ausschließlich auf eine lückenschließende Funktion und eine Betrugsähnlichkeit des § 148a abzielen. Der Gesetzgeber wollte nämlich wohl in erster Linie auf eine neue Bedrohung reagieren, wenn in den GMat ausgeführt wird: »Die Eigenart und der Einsatz dieser Anlagen [Anm: Datenverarbeitungsanlagen] lassen einen darauf bezogenen Ausbau des Justizstrafrechts [...] geboten erscheinen«.[1796] Daraus kann abgeleitet werden, dass

1789 Siehe JAB 359 BlgNR XVII. GP, 18.
1790 Vgl JAB 359 BlgNR XVII. GP, 16.
1791 Vgl JAB 359 BlgNR XVII. GP, 18.
1792 Siehe *Reindl,* E-Commerce, 46; *Reindl* in BMJ, Vorarlberger Tage 2003, 63 (72 f); weiters *Reindl-Krauskopf,* Computerstrafrecht², 78 f.
1793 Vgl *Reindl,* E-Commerce, 46.
1794 Für Überlegungen zum Analogieverbot siehe *Reindl,* E-Commerce, 46.
1795 Wohl gemerkt geht es dabei nicht darum, ob tatsächlich ein Betrug im klassischen Sinn vorliegt.
1796 Vgl JAB 359 BlgNR XVII. GP, 15.

Manipulationen an Datenverarbeitungsanlagen neue Kriminalitätsformen darstellen, auf die bislang legislativ nicht Bedacht genommen worden war. Man kann nun die diesbezüglichen Ausführungen in den GMat zum Betrug und zur Betrugsähnlichkeit auch schlicht als Begründung des Erfordernisses eines neuen Spezialtatbestandes (§ 148a) verstehen. Das Eingehen auf den Betrug respektive die Untreue kann in diesem Zusammenhang auch lediglich als Erklärung der Unzulänglichkeit dieser Tatbestände zur Erfassung dieser Phänomene erachtet werden.

Wenn in den GMat allerdings davon gesprochen wird, dass die Gefährlichkeit und der Schuld- und Unrechtsgehalt von Manipulationen an Datenverarbeitungsanlagen durchaus mit Betrugs- und Untreuehandlungen vergleichbar seien[1797], so kann das nicht heißen, dass hinter dem eigenständigen Spezialdelikt des § 148a stets die »klassischen« Bestimmungen des Betrugs oder der Untreue durch eine fiktive Umgestaltung des Sachverhalts zu prüfen sind. Außerdem müsste nach der von *Reindl* vorgeschlagenen »hypothetischen Mensch-anstelle-Maschine-Prüfung« schlüssigerweise auch eine solche analoge fiktive Prüfung für einen »untreueähnlichen« Sachverhalt in Erwägung gezogen werden, gibt es doch Praxisbeispiele, wie sie in den GMat selbst angedacht werden, die dabei sehr stark an die Untreue erinnern.[1798] Wie würden die Kriterien für eine solche Prüfung iSd § 153 aussehen?

Insgesamt ist daher aus meiner Sicht eine solche Prüfung, die als interpretative Grundlage einen Vergleich mit Kerninhalten anderer Bestimmungen hat, rechtspolitisch wie dogmatisch zweifelhaft.

Reindl ist aber zuzustimmen, dass – sofern man tatsächlich von einer Betrugsähnlichkeit des § 148a ausginge – diesem Kriterium eine entscheidende Bedeutung für den Unrechtsgehalt zukommen müsste und sich dieses daher auch im Tatbestand niederzuschlagen hätte. Im Zuge der Auseinandersetzung mit etwaigen Einwänden gegen ihre Interpretation präsentiert sie eine Gegenüberstellung der wesentlichen Merkmale des Betrugs auf der einen und der des Betrügerischen Datenverarbeitungsmissbrauchs auf der anderen Seite.[1799] Doch in diesem Vergleich betont *Reindl* als Äquivalent zur »Täuschung über Tatsachen« bei § 146 die »unbefugte« Dateneingabe seitens des § 148a. Nun ist aber, wie von *Schmölzer* – oben dargestellt – kritisiert wird, gerade

1797 JAB 359 BlgNR XVII. GP, 15.
1798 Siehe JAB 359 BlgNR XVII. GP, 15.
1799 Siehe *Reindl,* E-Commerce, 45; weiters *Reindl-Krauskopf,* Computerstrafrecht², 73.

das Merkmal »unbefugt« (oder auch »widerrechtlich«) kein ausdrückliches Tatbestandsmerkmal des Betrügerischen Datenverarbeitungsmissbrauchs. Die Unbefugtheit ergibt sich somit nur aus dem (rein subjektiven) erweiterten Vorsatz einer »unrechtmäßigen« Bereicherung (wie er aber expressis verbis ebenso in § 146 formuliert ist). Meines Erachtens liegt gerade hier das Missverhältnis begraben, das der normativen Betrugsähnlichkeit – mangels eines solchen Äquivalents (Gefährlichkeitselement) – entgegensteht. Beim Betrug handelt es sich um ein verhaltensgebundenes Delikt, das eine »Täuschung über Tatsachen« im äußeren Verhalten unverzichtbar erforderlich macht. Als Gegenstück dazu ist aus dem Wortlaut des § 148a lediglich die äußere Handlungsweise der Gestaltung eines Programms oder zB die Eingabe von Daten genannt, die zur Beeinflussung eines Ergebnisses führen muss. Zwischen der Täuschung eines Menschen (§ 146) und der (bloßen) Eingabe von (zB richtigen) Daten ist jedoch zumindest ein deutlicher Unterschied im tatbestandlichen Unrecht erkennbar. Immerhin erfordert die Täuschung eines Menschen jedenfalls einen anderen, in den Fällen, in denen ein § 148a ohne formelle Manipulation einer Datenverarbeitung (also zB durch die Eingabe richtiger Daten) begangen wird, auch zusätzlichen kriminellen Aufwand, nämlich »stets« eine Person in einen Irrtum zu führen und dadurch in ihrer Willensbildung zu beeinträchtigen. Demgegenüber kann ein automationsunterstützter Datenverarbeitungsvorgang auch vom Computer zuhause aus, mit ggf passenden – wenn auch widerrechtlich erlangten[1800] – Zugangsdaten verwirklicht werden, indem das Tatobjekt lediglich (technisch gesehen) ordnungsgemäß »bedient« wird, ohne dass sich das Handeln des Täters auf einen Menschen auswirken muss.

c. Kritik an der Betrugsähnlichkeit unter Berücksichtigung des § 108

Beide Delikte (§§ 146 und 148a) schützen grundsätzlich das Rechtsgut Vermögen[1801], wobei dem Tatbild des Betrugs (nunmehr in Relation zur Täuschung nach § 108 betrachtet) durch das Erfordernis der

1800 Wobei das Verschaffen von Zugangsdaten bereits eine strafbare Handlung sein kann (vgl etwa § 126c Abs 1 Z 2); siehe dazu zB *Bergauer,* RZ 2006, 82.

1801 Siehe statt vieler *Kirchbacher* in WK² § 146 Rz 4, *Kirchbacher/Presslauer* in WK² § 148a Rz 2.

Täuschung eines Menschen auch der Schutz des Rechtsguts der Willensbildungsfreiheit zukommt. Dieser Schluss liegt deshalb nahe, weil die Täuschung nach § 108 ein dem Betrug verwandtes Delikt ist, bei dem durch die Täuschungshandlung des Täters der Getäuschte selbst eine – ihn oder einen Dritten in seinen Rechten schädigende – Handlung, Duldung oder Unterlassung setzen muss (Selbstschädigungsdelikt). Das Tatbild des Betrugs ist dem der Täuschung nämlich angeglichen, weshalb die in beiden Delikten verwendeten gesetzlichen Begrifflichkeiten – wie zB das Täuschen über Tatsachen – auch gleich zu interpretieren sind.[1802] Lediglich für die Schadenszufügung wird für die Täuschung nach § 108 Absicht (iSd § 5 Abs 2) verlangt. Auf einen erweiterten Vorsatz (wie Bereicherungsvorsatz beim Betrug) wird aber verzichtet.

§ 108 schützt nun prinzipiell andere Rechtsgüter als das Vermögen, da nach überwiegenden Meinungen die Herbeiführung von täuschungsbedingten Vermögensschäden abschließend in § 146 geregelt wird.[1803] Doch kann vorrangig gerade daraus geschlossen werden, dass deshalb von § 146 auch das Rechtsgut der Willensbildungsfreiheit (neben dem Vermögen) mitgeschützt sein müsste. Andernfalls würde für eine absichtliche Täuschung um jemanden – ohne Bereicherungsvorsatz – im Vermögen (Vermögensrechten) zu schädigen, anders als bei anderen (Individual-)Rechten, eine Strafbarkeitslücke bestehen, selbst wenn es sich bei § 108 grundsätzlich lediglich um ein Auffangdelikt[1804] handelt.

Kontrovers wird im Schrifttum diskutiert, welche Rechte zur Verwirklichung des § 108 nun tatsächlich in Frage kommen können. Dabei wird § 108 »überhaupt als unanwendbar«[1805] gesehen bzw mangels

---

1802 Vgl *Fabrizy,* StGB[11] § 108 Rz 2.

1803 Siehe etwa *Bertel* in WK[2] § 108 Rz 4 und 14; *Bertel/Schwaighofer,* BT I[12] § 108 Rz 3; *Kienapfel/Schmoller,* StudB BT II § 146 Rz 25; *Schmoller* in SbgK § 108 Rz 20 (Stand Mai 1996); auch der Gesetzgeber dürfte sich dieser Argumentation anschließen, verweisen doch die GMat zur Einführung des § 107a (Beharrliche Verfolgung) iZm § 108 auf *Bertel* in WK[2] § 108 Rz 4 (Stand August 2000) (siehe ErlRV 1316 BlgNR XXII. GP, 5); aA auch *Fabrizy,* StGB[11] § 108 Rz 1 mwN, der das Vermögen ebenfalls als Rechtsgut hinter § 108 begreift, sofern kein Bereicherungsvorsatz vorliegt und daher Betrug unanwendbar bleibt; *Fuchs/Reindl-Krauskopf,* BT I[4], 98 f; *Kirchbacher* in WK[2] § 146 Rz 136; *Leukauf/Steininger,* StGB[3] § 108 Rz 9; wohl auch *Kert* in SbgK § 146 Rz 369 (Stand Mai 2012); ebenso OGH 12.06.1991, 13 Os 149/90.

1804 Siehe etwa OGH 19.11.1987, 13 Os 162/87; weiters OGH 02.09.1986, 11 Os 107/86 mwN.

1805 Vgl zB *Bertel* in WK[2] § 108 Rz 14.

gehöriger Bestimmtheit auch dessen Verfassungsmäßigkeit angezweifelt[1806]. *Kienapfel* bspw spricht sich in seinen »Vorschlägen zur Abänderung des Besonderen Teils« überhaupt für die ersatzlose Streichung dieser Bestimmung aus.[1807]

Der OGH hat keine Bedenken gegen die Verfassungsmäßigkeit dieser Strafbestimmung, da der Tatbestand hinreichend determiniert sei[1808] und spricht sich auch für eine weite Auslegung der tatbildlichen Rechte aus, wobei er grundsätzlich jedes konkrete Recht als darunter subsumierbar erachtet.[1809] Er spricht sogar expressis verbis von »irgendwelchen Rechten«.[1810]

In der Lit werden dagegen Konkretisierungen vorgeschlagen, wie zB, dass die Rechte »von Gesetzes wegen eingeräumt worden sind« und für ihren Träger eine »nicht unwesentliche Bedeutung« haben.[1811] Gleichwohl sind Hoheitsrechte gem § 108 Abs 2 ausdrücklich ausgeschlossen. Dies wohl mit der gesetzgeberischen Intention, dass für den Schutz von Hoheitsrechten dem Staat das (dafür ausreichende) Verwaltungsstrafrecht zur Verfügung steht. Das treffe aber im Allgemeinen nicht für Rechte von Privatpersonen zu. »Die Schädigung konkreter Rechte dieser Art soll daher von der Strafbestimmung weiterhin erfaßt werden«.[1812]

Da auch der Gesetzgeber die Diskussion und Rsp zu § 108 kennt und seit dem StRÄG 1987 nicht darauf reagiert hat, ist davon auszugehen, dass ihn die kritischen Lehrmeinungen zu § 108 nicht überzeugen. Im Übrigen ist mE das konkrete Individualrecht des »Grundrechts auf Geheimhaltung personenbezogener Daten« gem § 1 Abs 1 DSG 2000 jedenfalls als ein geeignetes Individualrecht der Täuschung anzuführen.[1813] Insbesondere unter dem Gesichtspunkt, dass nach den GMat

---

1806 Vgl *Kienapfel,* BT I[4] § 108 Rz 9 ff; *Weiß,* Kritische Betrachtung des Täuschungstatbestandes aus straf- und verfassungsrechtlicher Sicht – zugleich ein Beitrag zur Bestimmtheit von Strafnormen (Teil II), AnwBl 1989, 246; zusammenfassend *Kienapfel,* Grundriß des österreichischen Strafrechts. Besonderer Teil I[4] (1997) § 108 Rz 9 ff.

1807 Vgl *Kienapfel,* Vorschläge zur Abänderung des Besonderen Teils, RZ 1981, 117; vgl weiterhin *Kienapfel/Schroll,* Studienbuch. Besonderer Teil I[3] (2012) § 108.

1808 Siehe OGH 26.06.1986, 12 Os 69/86.

1809 Siehe OGH 22.05.1986, 12 Os 136/85.

1810 Vgl OGH 02.09.1986, 11 Os 107/86.

1811 Siehe zusammenfassend *Schmoller* in SbgK § 108 Rz 18 mwN.

1812 Siehe JAB 359 BlgNR XVII. GP, 15.

1813 Zu § 108 iVm § 1 Abs 1 DSG 2000 siehe S 404 ff.

im Allgemeinen die Schädigung sämtlicher konkreter Rechte einer Privatperson durch Täuschung von dieser Strafbestimmung erfasst werden soll.[1814]

Das vom Täuschungstatbestand geschützte Rechtsgut liegt nach den GMat[1815] in der »Freiheit der Willensbildung«, was auch die Einordnung unter die strafbaren Handlungen gegen die Freiheit erklären soll.[1816] Aufgrund dieser systematischen Einordnung und der Tatsache, dass jedes konkrete Recht relevant für § 108 sein kann, liegt mE sein Deliktsunwert primär in der Beeinträchtigung der Willensbildung[1817], die durch die tatbestandliche Täuschungshandlung repräsentiert wird[1818]; selbige wird aber ebenfalls vom Tatbestand des Betrugs verlangt. Dass der überwiegende Unrechtsgehalt des § 108 in der Täuschungshandlung liegt, legt aber auch schon der tatbestandsmäßige Erfolg des § 108 (Schädigung in einem Recht) nahe, bei dem sich aufgrund des weiten, inhaltlich unspezifizierten Rechteumfangs nicht auf ein spezielles Rechtsgut schließen lässt. Zudem wird der Unrechtsgehalt der Täuschung auch noch stärker bewertet als der des Betrugs, was sich grundsätzlich in den unterschiedlichen Strafdrohungen zeigt. Dagegen stellt aber § 108 gegenüber § 146 lediglich ein Ermächtigungsdelikt dar.[1819]

Somit kommt § 146 in Vertretung des § 108, der Vermögensschädigungen (jedenfalls mit Bereicherungsvorsatz) nicht erfasst, notwendigerweise auch die Funktion zu, das Rechtsgut der Willensbildungsfreiheit zu schützen. Dies nicht zuletzt, weil nicht zu verstehen wäre, warum die Willensbildungsfreiheit zwar in Bezug auf jedes konkrete (weitgehend unspezifizierte) Individualrecht, nicht aber in Zusammenhang mit dem Vermögen geschützt würde, nimmt doch gerade auch der Vermögensschutz im Strafrecht eine zentrale Rolle bei den Individual-

1814 Vgl JAB 359 BlgNR XVII. GP, 15.

1815 Siehe ErlRV 30 BlgNR XIII. GP, 239.

1816 Unterschiedliche Ansichten finden sich bei *Schmoller* in SbgK § 108 und *Bertel* in WK² § 108.

1817 Vgl sinngemäß auch *Schmoller,* Zum Tatbestand der Täuschung – § 108 StGB nach dem StrafrechtsänderungsG 1987, in BMJ (Hrsg), Strafrechtliche Probleme der Gegenwart. 16. Strafrechtliches Seminar 1988 (1989) 1 (42 f); aA OGH 03. 07. 1980, 12 Os 72/80.

1818 Siehe dazu *Bergauer* in BMJ, 35. Ottensteiner Fortbildungsseminar, 27 (33); ebenso *Bergauer,* Phishing und Geldkuriere im Strafrecht, in Bergauer/Staudegger (Hrsg), Recht und IT. Zehn Studien (2009) 109 (125 f).

1819 Vgl § 108 Abs 3.

rechtsgütern ein. Das aber selbst dann, wenn man – wie der OGH – davon ausginge, dass der Täuschungstatbestand nach § 108 Abs 1 grundsätzlich auch Vermögensrechte[1820] erfasse[1821], da andernfalls zumindest ein auf die Willensbeeinträchtigung ausgerichteter Auffangtatbestand im Bereich des Rechtsgüterschutzes des Vermögens (im Gegensatz zu grundsätzlich allen weiteren Rechtsgütern) fehlen würde.

Dies würde nun aber unter Bedachtnahme auf eine Betrugsähnlichkeit bedeuten, dass § 148a ebenfalls diese beiden Rechtsgüter zu schützen hätte und das Erfordernis eines der Täuschung beim Betrug adäquaten Gefährlichkeitselements enthalten müsste.

Da nun aber naturgemäß nicht auf eine Willensbildung einer Maschine bzw eines Computersystems eingewirkt werden kann, was schon mehrfach durch das Faktum der mangelnden Täuschungstauglichkeit von automationsunterstützten Datenverarbeitungsanlagen angesprochen wurde, und den GMat[1822] zufolge, der bloße »Zeitdiebstahl« ausdrücklich nicht erfasst sein soll[1823], ist davon auszugehen, dass der Betrügerische Datenverarbeitungsmissbrauch nicht auch willensbeeinträchtigenden Tathandlungen adäquate Manipulationen erfassen sollte, sondern lediglich auf das Vermögen als Ganzes fokussiert. Dies ergibt sich darüber hinaus mittelbar aus der herrschenden Interpretation des Tatbestandsmerkmals »beeinflussen«. Denn darunter werden Fälle erfasst, in denen der Täter richtige und vollständige Daten eingibt und nur der erweiterte Vorsatz auf unrechtmäßige Bereicherung gerichtet ist.[1824] Im Gegensatz dazu kann ein Betrug nur durch die Behauptung unwahrer Tatsachen begangen werden.[1825]

Was das Maß der kriminellen Energie anlangt, ist die Täuschung eines Menschen gegenüber der bloßen Eingabe von Daten (wenn auch mit dem Vorsatz der Bereicherung) höher zu bewerten und daher mit einem höheren Unrechtsgehalt verbunden.

1820 Erfolgt die Täuschung aber mit Bereicherungsvorsatz, liegt Betrug vor (vgl OGH 12.06.1991, 13 Os 149/90).

1821 Vgl OGH 12.06.1991, 13 Os 149/90; ebenso *Fabrizy,* StGB[11] § 108 Rz 1.

1822 Siehe JAB 359 BlgNR XVII. GP, 16.

1823 Dh eine Willensbeeinträchtigung des Berechtigten über die Datenverarbeitung, um diese – eben entgegen dem Willen – unbefugt zu nutzen, ist nicht gefordert.

1824 Vgl auch *Engin-Deniz/Grünzweig,* ecolex 2001, 587.

1825 Siehe *Kienapfel,* BT II[3] § 148a Rz 19.

Daneben stellt die angesprochene Konzeption des § 148a als Fremdschädigungsdelikt einer Betrugsähnlichkeit entgegen.[1826] Der Täter unternimmt nämlich – anders als beim Betrug – selbst die Vermögensverfügung, die das Opfer unmittelbar schädigt. Der Betrugstatbestand dagegen beschreibt eine – im Hacker-Jargon typischerweise als »Social Engineering«[1827] bezeichnete – Handlung, mit der der Täter mittels Täuschung über Tatsachen einen anderen dazu bringen muss, eine Vermögensverfügung zu tätigen, die diesen oder einen Dritten unmittelbar im Vermögen schädigt. Bei einer Manipulation einer Datenverarbeitung, bei der kein weiterer Mensch notwendigerweise für die Zwecke des Täters instrumentalisiert wird, dessen irrtumsveranlasste Handlung unmittelbar kausal für den Vermögensschaden ist, kann von einer Betrugsähnlichkeit nicht gesprochen werden. Dafür spricht erneut der – oben angesprochene – unterschiedliche Rechtsgüterschutz, was sich in der Struktur der Delikte des § 146 und § 148a augenscheinlich manifestiert. Das bloße Eingeben von Daten iSd § 148a ist einer Täuschung eines Menschen iSd § 146 somit nicht gleichwertig.[1828]

Als ein Indiz gegen eine tatsächliche Betrugsähnlichkeit kann auch die fehlende gänzliche Gleichstellung der Strafdrohungen der Deliktsqualifikationen herangezogen werden, denn die gewerbsmäßige Begehung wird nach § 148a Abs 2 Fall 1 wesentlich milder bestraft als der gewerbsmäßige Betrug (§ 148).

Darüber hinaus fällt auf, dass es kein dem »Notbetrug« (§ 150) vergleichbares Delikt im Bereich des Betrügerischen Datenverarbeitungsmissbrauchs gibt.[1829] Bei Annahme einer Betrugsähnlichkeit wäre doch eine adäquate Privilegierung auch für § 148a in den Fällen indiziert, in denen die Begehung aus Not mit einem nur geringen Schaden geschieht.

Zur Verwirklichung des § 150 muss der Täter alle Elemente der Strafbarkeit des Betruges erfüllen.[1830] In Not befindet sich nach § 150, wer objektiv infolge Mittellosigkeit einen Mangel an dem hat, was zum

1826 Der Betrug (§ 146) ist – wie oben erwähnt – ein Selbstschädigungsdelikt.

1827 Zur Begrifflichkeit siehe anstatt vieler *Borges/Schwenk/Stuckenberg/Wegener,* Identitätsdiebstahl, 96 ff.

1828 Siehe jüngst auch *Komenda/Madl* in SbgK § 148a Rz 15, die diesbezüglich § 148a gegenüber § 146 einen erweiterten Anwendungsbereich zuschreiben.

1829 Siehe auch *Tipold* in SbgK § 150 Rz 12 (Stand November 2004), der von einer planwidrigen Lücke spricht und daher eine Anwendung des § 150 per analogiam angezeigt sieht; siehe dazu auch *Reindl-Krauskopf,* Computerstrafrecht², 74; weiters *Komenda/Madl* in SbgK § 148a Rz 128 ff.

1830 Vgl *Tipold* in SbgK § 150 Rz 2 und 8.

Leben unbedingt erforderlich ist, wobei diese Notlage das Motiv zur Tat bilden muss.[1831] Man denke bspw an den (abgewandelten)[1832] Fall, in dem ein mittelloser Täter, der drei Tage hindurch seinen Ernährungsbedarf nicht befriedigen konnte, eine Bankomatkarte, auf der die zugehörige PIN handschriftlich notiert wurde, findet, und zur Bezahlung von Lebensmitteln an einer Bankomatkassa unbefugt verwendet.

Als gering werden nach hM prinzipiell nur Schäden angesehen, die – nach objektiven Gesichtspunkten – eine Grenze von ca € 100,– nicht überschreiten.[1833]

d. »Missbräuchliches Beeinflussen«

Auch wenn mE eine Betrugsähnlichkeit des § 148a in dogmatischer und rechtspolitischer Sicht unzutreffend erscheint, ändert dies – nach wie vor[1834] – nichts an der zu weit gefassten Formulierung des Tatbestands des § 148a.

Aus diesem Grund ist als Auslegungskriterium des »Beeinflussens« eine Verwendung einer Datenverarbeitungsanlage in »missbräuchlicher Hinsicht« zwingend angezeigt.[1835] Es handelt sich mE bezüglich des »Beeinflussens« um einen Begriff, der bereits eine emotionale Einstellung impliziert. Als Indiz dafür, dass ein technischer bzw formeller »Missbrauch« tatbildlich ist, kann auch die Deliktsbezeichnung »Betrügerischer Datenverarbeitungsmissbrauch« herangezogenen werden. Eine solche Interpretation schließt sich der Kritik *Schmölzers* an und macht es erforderlich, dass unter »Beeinflussen« nur Handlungen verstanden sein können, die sich auf vordefinierte ordnungsgemäße Programmläufe oder die Gestaltung eines Programms »negativ« auswirken. Das ist dann der Fall, wenn die Beeinflussung des Ergebnisses einer automationsunterstützten Datenverarbeitung unmittelbar aus der formellen Manipulation heraus selbstständig die schädigende Ver-

---

1831 Vgl *Kirchbacher/Presslauer* in WK² § 150 Rz 4; weiters *Tipold* in SbgK § 150 Rz 33; *Fabrizy,* StGB¹¹ § 150 Rz 1 mit Verweis auf § 141 Rz 2.

1832 Bei *Kirchbacher/Presslauer* in WK² § 150 Rz 4 (Stand November 2009).

1833 Vgl *Tipold* in SbgK § 150 Rz 18; weiters *Kirchbacher/Presslauer* in WK² § 150 Rz 4; *Komenda/Madl* in SbgK § 148a Rz 129

1834 Siehe oben, insb das Argument der fehlenden tatbestandlichen »Unbefugtheit« der Dateneingabe.

1835 AA etwa *Reindl-Krauskopf,* Computerstrafrecht², 72, die das »Beeinflussen« weiterhin als das bloß nachteilige Verändern versteht.

mögensverfügung bewirkt.[1836] Eine solche Auslegung scheint im Sinne einer strafbarkeitseinschränkenden Funktion geboten, um die überschießende Wirkung des objektiven Tatbestands einzuschränken. In diesem Sinn ist also das bloße Aktivieren bzw Auslösen – selbst wenn dabei etwa durch die unbefugte Verwendung einer fremden Bankomatkarte samt zutreffender PIN iSd »Fiktion der Datenwahrheit« »unrichtige Daten« eingegeben werden – mangels einer »Beeinflussung« einer Datenverarbeitung (noch) nicht tatbestandsmäßig.[1837]

Bei der widerrechtlichen Benutzung einer fremden Bankomatkarte geht der OGH aber trotz Einführung des § 148a weiterhin von einer Strafbarkeit nach § 127 aus.[1838] Dies, bei grundsätzlicher Anwendbarkeit des § 127 – in der E[1839], ohne überhaupt auf § 148a einzugehen – bereits deshalb, weil letztere Bestimmung zur Ausschaltung von Strafbarkeitslücken eingeführt wurde und daher aufgrund materieller Subsidiarität (dh Scheinkonkurrenz) zurücktrete.[1840] Der OGH hat aber an anderer Stelle in einem Fall des Bankomatkartenmissbrauchs[1841], in dem den Tätern die PIN bekannt war, festgehalten, dass nach gesicherter Rsp die Anwendbarkeit des Betrügerischen Datenverarbeitungsmissbrauchs (§ 148a) verneint wird, wobei zur Begründung ua auf *Leukauf/Steininger*[1842] verwiesen wurde.[1843] Diese Autoren stellen unter dieser Fundstelle sinngemäß fest, dass ein bloß unbefugtes Auslösen eines elektronischen Prozesses kein Beeinflussen eines Datenverarbeitungsergebnisses darstelle, weil dieses Resultat auch bei befugter Aktivierung dieses Prozesses erzielt werde. In jüngeren E hielt nun auch die Rsp, insb der OGH, die Eingabe richtiger Daten für tatbestandlich iSd § 148a.[1844]

1836 Siehe etwa OGH 14.07.2011, 13 Os 61/11m = jusIT 2011/103, 220 *(Bergauer)* = JSt 2011, 201 *(Schwaighofer)*.

1837 In diese Richtung wohl auch *Lewisch,* BT I², 242.

1838 Siehe statt vieler RIS-Justiz RS0093560 mwN; ebenso *Schmölzer,* EDVuR 1990, 30; aA *Bertel/Schwaighofer,* BT I¹² § 148a Rz 2 mwN.

1839 Vgl OGH 30.10.1990, 15 Os 79/90.

1840 Vgl auch statt vieler RIS-Justiz RS0093560 mwN; siehe auch die Zusammenfassung bei *Prunner,* Missbrauch der Bankomatkarte eines Angehörigen – kein § 166 StGB?, JAP 2014/2015/1; anders etwa das OLG Linz 08.06.1989, 8 Bs 129/89 = AnwBl 1990/3375 *(Fromherz)*.

1841 Vgl OGH 10.12.1996, 14 Os 71/96 (14 Os 78/96).

1842 Vgl *Leukauf/Steininger,* StGB³ § 148a Rz 20.

1843 In diesem Sinn die Rechtsmeinung des OGH zusammenfassend auch *Wegscheider,* BT⁴, 240f.

1844 Siehe OGH 01.06.2006, 12 Os 45/06v (12 Os 46/06s); weiters OGH 13.10.2005, 15 Os 99/05f, jedoch ohne darauf näher einzugehen; siehe auch OLG Innsbruck 16.12.2014, 11 Bs 353/14w iZm Paysafecards.

In diese Kerbe schlägt aber auch ein ME[1845], in dem eine entsprechende Klarstellung des § 148a vorgeschlagen wurde. Darin wurde eine Ergänzung in Erwägung gezogen, die im Anschluss an die Beschreibung der Begehungsweisen einer Inputmanipulation folgende Beifügung betraf: »mag dies auch unter Verwendung falscher, verfälschter oder entfremdeter unbarer Zahlungsmittel geschehen«. Obwohl dieser Entwurf in weiterer Folge nicht weiter legislativ behandelt wurde, war vom Entwurfsverfasser zweierlei intendiert, nämlich einerseits die eindeutige und klare Einordnung einer unbefugten Geldbehebung an einem Bankomaten mit der richtigen Karte und dem zugehörigen Code unter § 148a und auch die Hintanhaltung einer Aufweichung des Gewahrsamsbegriffs des Diebstahls (§ 127).[1846]

Dem entgegengesetzt ist zwar ursprünglich noch von *Kienapfel*[1847] gerade die unbefugte Verwendung einer fremden Bankomatkarte als ein klassisches Beispiel für den Betrügerischen Datenverarbeitungsmissbrauch (§ 148a) genannt worden, weshalb er auch im Verhältnis zu § 127 von einer tatbestandsausschließenden Exklusivität dieser Strafvorschrift ausging; mittlerweile stimmt aber auch er der diesbezüglichen Rsp zu.[1848]

e. Vergeistigung des Gewahrsamsbegriffs bei Geldbehebungen aus Bankomaten

Die Anwendbarkeit des Diebstahls nach § 127 auf Bankomatbehebungen unter Verwendung einer fremden Bankomatkarte (oder eines Kartenduplikats[1849]) mit zutreffender PIN mit dem Erfordernis eines »Gewahrsamsbruches« ergibt sich – nach der in der Lehre umstrittenen[1850] – höchstrichterlichen Rsp daraus, dass als Gewahrsam die tatsächliche Herrschaft über eine Sache verstanden wird, die mit dem Willen verbunden ist, diese

1845 Vgl 78/ME XXII. GP, wobei angemerkt sein muss, dass die vorgeschlagene Ergänzung des § 148a in der anschließenden RV 309 BlgNR XXII. GP nicht mehr weiter verfolgt wurde.

1846 ErlME 78/ME XXII. GP, 11.

1847 Vgl noch *Kienapfel,* BT II[3] § 148a Rz 39 und 21.

1848 Man beachte daher, dass *Kienapfel* seine Meinung dazu mittlerweile iSd OGH-Rsp revidiert hat; siehe *Kienapfel/Schmoller,* StudB BT II § 127 Rz 103; für Exklusivität *Triffterer* in SbgK § 148a Rz 22 (aF Stand Dezember 1992); weiters *Komenda/Madl* in SbgK § 148a Rz 134.

1849 Vgl OGH 24.10.1989, 15 Os 127/89.

1850 Siehe *Birklbauer/Hilf/Tipold,* Strafrecht BT I[2] § 148a Rz 9 mwN.

Herrschaft aufrecht zu erhalten. Diese beiden – objektiven und subjektiven – Komponenten sind nach den Anschauungen des täglichen Lebens zu interpretieren. Unter Beachtung dieses Auslegungskriteriums wird in der Rsp nicht so sehr die unmittelbare Einwirkungsmöglichkeit des Gewahrsamsträgers, sondern die soziale Zuordnung von Person und Sache in den Vordergrund gestellt. Demnach ist der Gewahrsam jene Zugehörigkeit einer Sache zu einer Person, die auch ein Außenstehender nicht nur als eine räumliche Beziehung, sondern als eine auf sozialen Gepflogenheiten beruhende Verbindung von Sache und Person zu erkennen vermag. Dieses Verhältnis erfordert keine greifbare Nähe zur Sache.[1851] Nur mit diesem äußerst weitgehaltenen »geistigen Vorbehalt«[1852], lässt sich eine Strafbarkeit nach § 127 überhaupt realisieren. Diese Auslegung wird jedoch indirekt auch in einem ME[1853] durch eine angedachte eindeutige und klarstellende Einordnung einer unbefugten Geldbehebung an einem Bankomat unter § 148a kritisiert, welche darüber hinaus auf die »Hintanhaltung einer Aufweichung des Gewahrsamsbegriffs des § 127« abzielen sollte.

»Bestohlener« iSd Diebstahls ist dabei nicht der (Konto-)Inhaber, sondern der Betreiber des Geldausgabeautomaten[1854] (hier: die für den konkreten Geldausgabeautomaten verantwortliche Bank).

Tatobjekt einer solchen Wegnahme ist Bargeld, also eine fremde bewegliche »körperliche«[1855] (und daher diebstahlsfähige) Sache, die sich der Täter unter Bruch der tatsächlichen Sachherrschaft zueignet. Anders ist es allerdings bei einem missbräuchlichen Transfer von unkörperlichem (und daher nicht diebstahlsfähigem) Giralgeld, obgleich die kriminelle (objektive und subjektive) Vorgehensweise, die technischen Umstände der Tat und die Vermögensschädigung in diesen Sachverhalten sehr vergleichbar sind und unter rein rechtspolitischen Aspekten eine Beurteilung nach unterschiedlichen Delikten nicht wirklich sachgerecht erscheint.

1851 Siehe dazu OGH 10.12.1996, 14 Os 71/96 (14 Os 78/96) mwN; auch OGH 28.09.2010, 14 Os 126/10a bzw RIS-Justiz RS0099100 mwN.

1852 Siehe auch jüngst die Zusammenfassung und die Kritik am »mentalen Vorbehalt« von *Komenda/Madl* in SbgK § 148a Rz 90 f.

1853 Siehe 78/ME XXII. GP, 11, wobei angemerkt sein muss, dass die vorgeschlagene Ergänzung des § 148a in der anschließenden RV 309 BlgNR XXII. GP nicht mehr weiter verfolgt wurde.

1854 Siehe zB OGH 30.08.2012, 13 Os 80/12 g = ÖJZ EvBl 2013/7, 42 *(Ratz)* = JAP 2014/2015/1, 4 *(Prunner);* OGH 10.12.1996, 14 Os 71/96 (14 Os 78/96); OGH 11.03.1993, 15 Os 156/92.

1855 Im Sinne des § 292 iVm § 285 ABGB.

Das widerrechtliche Aufladen eines Wertkartentelefons oder einer elektronischen Geldbörse (vgl Quick-Chip) unter Verwendung einer Bankomatkarte bzw das unbefugte Transferieren von Giralgeld über einen Überweisungsautomaten unter Verwendung einer entfremdeten Bankomatkarte wird vom OGH – mangels einer durch Gewahrsamsbruch erfolgten Sachwegnahme – nach § 148a beurteilt.[1856] Ebenso wird iZm widerrechtlichen Online-Ticketbuchungen § 148a – interessanterweise aber trotz etwaiger Vergleichbarkeit mit Geldbehebungen an einem Bankomaten nicht § 127 – vom OGH in Betracht gezogen.[1857] Auch das Bezahlen von Waren über die sog »PayPass«-Funktion einer Bankomatkarte, welche höchstens fünf durch NFC[1858]-Technik gewährleistete (kontaktlose) Bezahlvorgänge zu maximal je € 25,– (insgesamt daher nicht mehr als € 125,–) ohne PIN-Eingabe ermöglicht, ist wohl unter § 148a StGB zu subsumieren. Anders als beim Quick-Chip verbleiben diese Kleingeldbeträge bis zum konkreten Zahlungsvorgang in der tatsächlichen Höhe am Konto des PayPass-Berechtigten. Auf der Bankomatkarte selbst sind diese Werte nicht verkörpert, weshalb es sich bei einer Bankomatkarte mit aktivierter PayPass-Funktion um keinen selbstständigen Wertträger handelt.[1859]

6. Sonderproblem: Beendigung der Tat und strafbare Beteiligung

Zur Verwirklichung des § 148a wird bereits durch den Wortlaut vorausgesetzt, dass der tatbestandsmäßige Vermögensschaden als unmittelbare Folge einer auf die dort beschriebene Weise vorgenommene Beeinflussung des Ergebnisses einer automationsunterstützten Datenverarbeitung eintritt.[1860] Folglich muss die Beeinflussung eines solchen Ergebnisses selbsttätig und unmittelbar zum Schadenseintritt führen.[1861] Mit Einritt des Vermögensschadens ist das Erfolgsdelikt vollen-

1856 Vgl OGH 13.10.2005, 15 Os 99/05f; OGH 01.06.2006, 12 Os 45/06v.

1857 Siehe OGH 14.07.2011, 13 Os 61/11m = jusIT 2011/103, 220 *(Bergauer)* = JSt 2011, 201 *(Schwaighofer)*.

1858 Near Field Communikation.

1859 Siehe dazu *McAllister,* Strafrechtliche Auswirkungen der neuen »PayPass«-Funktion von Kredit- und Bankomatkarten, JBl 2014, 224; weiters *Prunner,* JAP 2014/2015/1.

1860 Siehe statt vieler RIS-Justiz RS0094395.

1861 Vgl OGH 14.07.2011, 13 Os 61/11m = jusIT 2011/103, 220 *(Bergauer)* = JSt 2011, 201 *(Schwaighofer)*.

det. § 148a Abs 1 verlangt in seinem Tatbild über diesen Erfolgseintritt hinaus keine weitere Aufrechterhaltung der Rechtsgutbeeinträchtigung. Aus diesem Grund handelt es sich um ein sog »Zustandsdelikt«, da die Rechtsgutbeeinträchtigung mit Herbeiführung des Schadens abgeschlossen ist. Bei Zustandsdelikten, die von einem unmittelbaren Täter begangen werden, ist prinzipiell eine strafbare Beteiligung (iSd § 12) an der Tat[1862] – im Gegensatz zu einem Dauerdelikt, bei dem eine solche bis zur materiellen Beendigung der Tat möglich ist – nur bis zur formellen Vollendung zulässig. Allein aus dieser Betrachtung heraus wäre bei § 148a Abs 1 eine Beteiligung grundsätzlich nur bis zum Eintritt des Vermögensschadens möglich, was auch dogmatisch plausibel ist, muss doch der Beitrag während der Tat (zB iSd § 12 dritter Fall) für die Vollendung vorsätzlich kausal geworden sein.

Denkbar wäre hier die Beiziehung eines Geldkuriers[1863] für eine Vermögensschädigung durch eine Phishing[1864]-Attacke.[1865] Sollte nämlich der Geldkurier zwar bis nach dem Eintritt des Vermögensschadens beim Opfer gutgläubig, dh ohne »bösen Vorsatz«, seine Leistung erbracht haben (zB durch argloses Bereitstellen seines inländischen Kontos)[1866], aber im Zeitpunkt der Barbehebung und anschließenden Weiterleitung des Geldes an den unmittelbaren Täter sich sehr wohl in Kenntnis der wahren Absicht und des bisherigen Tatverlaufs befinden, stellt sich die Frage, ob eine strafbare (sukzessive) Beteiligung an § 148a Abs 1 zu diesem Zeitpunkt noch möglich ist. Mit Eintritt des Vermögensschadens nach tatbestandlicher Beeinflussung des Ergebnisses einer automationsunterstützten Datenverarbeitung (hier: Transfer von Giralgeld auf das Konto des Geldkuriers) ist die Tat in rechtlicher Hinsicht (formell) vollendet. Der Eintritt der tatsächlichen Bereicherung, auf die sich der erweiterte Vorsatz richten muss, ist nicht mehr Tatbestandsvoraussetzung. Der tatbestandliche Erfolg liegt daher im Vermögensschaden (Erfolgsdelikt), der angestrebte Enderfolg der Tat in der Bereicherung des Täters.

1862 Ggf auch sukzessive Mittäterschaft.

1863 In der Praxis auch »Finanzagent« uÄ genannt.

1864 Zur Beurteilung der reinen Phishing-Phase siehe *Bergauer,* RZ 2006, 82.

1865 Siehe dazu ausf *Bergauer* in Bergauer/Staudegger, Recht und IT, 109 (109 ff).

1866 Vgl etwa die Sachverhalte in OGH 19.02.2009, 2 Ob 107/08 m = ecolex 2009, 577 *(Graf)* = ÖBA 2009/1551, 457 *(Bydlinski)* = jusIT 2009/69, 140 *(Mader)* und OGH 24.02.2009, 9 Ob 3/08v = ecolex 2009, 577 *(Graf)* = ÖBA 2009/1564, 595 *(Bydlinski)*.

a. Delikte mit überschießender Innentendenz

Bei Delikten mit überschießender Innentendenz, zB kupierten Erfolgsdelikten, ist strittig, wie lange eine strafbare Beteiligung möglich ist. Wie etwa die stRsp zum Betrug (§ 146) ausführt, tritt die materielle Beendigung (= Vollbringung) der Tat erst mit Eintritt der Bereicherung als Endziel ein.[1867] Bei § 148a Abs 1 handelt es sich (auch[1868]) um ein kupiertes Erfolgsdelikt, da der Täter im erweiterten Vorsatz einen über die (tatbildliche) Schädigung hinausreichenden weiteren Erfolg anstrebt, nämlich die unrechtmäßige Bereicherung. Das Delikt besteht somit aus zwei Unrechtsteilen, die Vermögensschädigung im objektiven Tatbestand auf der einen Seite und deren Korrelat im subjektiven Tatbestand, dem Bereicherungsvorsatz, auf der anderen. Bei strafbaren Handlungen mit überschießendem Vorsatz kann nach Rsp des OGH[1869] ein Tatbeitrag bis zu dem als materielle Vollendung bezeichneten Zeitpunkt, in dem das über die formale Vollendung hinaus Gewollte einzutreten beginnt, geleistet werden. Dies sei auch – nach Meinung des

---

1867 Siehe RIS-Justiz RS0103999 mwN; weiters zB *Kienapfel,* BT[3] § 146 Rz 254.

1868 Es handelt sich bei § 148a Abs 1 bezüglich des tatbestandlichen Erfolges (erster Erfolg bzw Zwischenerfolg) strukturell bereits um ein Erfolgsdelikt. In Anbetracht des finalen Enderfolgs der Bereicherung liegt auch ein kupiertes Erfolgsdelikt vor. Der Enderfolg ist tatbestandlich nicht gefordert, aber vom Täter als Endziel anvisiert. Die Strafbarkeit wird daher angesichts des zweiten Unrechtsteils vorverlagert.

1869 Vgl OGH 17.04.2002, 13 Os 179/01 = JBl 2003, 464 (krit *Schmoller);* jüngst bestätigt durch OGH 05.07.2012, 13 Os 36/12m; bereits auch OGH 09.09.1982, 12 Os 66/82; RIS-Justiz RS0090734 (T1); weiters *Fabrizy* in WK[2] § 12 Rz 94 mwN (Stand 01.05.2014) bzw *Fabrizy,* StGB[11] § 12 Rz 11; auch *Leukauf/Steininger,* StGB[3] § 12 Rz 48; weiters auch *Schick,* Rezension zu *Otto Triffterer,* Die österreichische Beteiligungslehre. Eine Regelung zwischen Einheitstäter- und Teilnahmesystemen?, ÖJZ 1984, 475; vgl auch *Schroll* in WK[2] § 241a Rz 21 (Stand Mai 2005) bzw § 232 Rz 28 (Stand August 2007) bzw § 233 Rz 15c (Stand August 2007); aA aber zB *Triffterer,* AT[2], 67 bzw *Triffterer,* Die österreichische Beteiligungslehre (1983) 22ff; aA auch *Fuchs,* AT I[8] Rz 28/7f bzw 33/61, der eine Beteiligung nur bis zur rechtlichen Vollendung für zulässig erachtet. Nach *Fuchs* würde in Anbetracht etwa des Betrugs (§ 146) bzw aller Delikte mit erweitertem Vorsatz (ausgenommen bei Dauerdelikten) die Vollendung und materielle Beendigung (zB mit dem Schaden des Opfers) stets zusammenfallen, weil der erweiterte Vorsatz nur eine bestimmte Innentendenz beschreibe, die für die Rechtsgutbeeinträchtigung bedeutungslos sei); aA auch *Schmoller,* der es ablehnt, für im Zeitpunkt des Hinzukommens des Beitragstäters bereits verwirklichte Unrechtsteile des unmittelbaren Täters, allein durch ein nachträgliches Einverständnis, dem »Beitragstäter« iSd § 12 zuzurechnen; siehe die Anmerkung von *Schmoller* zu OGH 17.04.2002, 13 Os 179/01 = JBl 2003, 464 (krit *Schmoller*).

zur Entscheidung berufenen Senats[1870] – iSd § 1 unbedenklich, da eine Wortinterpretation des § 12 dritter Fall, der auf einen Beitrag »zur Ausführung« abstellt, in die Richtung, dass auch, aber nicht nur eine Ausführungshandlung des unmittelbaren Täters vorliegen muss, noch innerhalb des äußersten Wortsinns der Vorschrift liege.[1871]

So sei dies auch beim Versandbetrug (§ 146), wenn etwa mit der Absendung der Ware die rechtliche Vollendung eintritt, die förderliche Entgegennahme der Ware aber noch einen strafbaren Beitrag zum Betrug darstelle.[1872]

Im Zusammenhang mit Computerdelikten könnte idZ an das Ermächtigungsdelikt des § 119 gedacht werden.[1873] Der unmittelbare Täter benützt eine tatbildliche Vorrichtung, um den Inhalt eines nicht für ihn bestimmten E-Mails in Erfahrung zu bringen. Nachdem aber der Inhalt der Nachricht in einer für ihn nicht verständlichen Form[1874] vorliegt, ersucht er einen damit vertrauten Bekannten – nach Offenbarung seiner Tat – ihm den Inhalt dieses E-Mails zur Kenntnis zu bringen. Die Tat ist mit dem Benützen der Vorrichtung in der Absicht, sich vom Inhalt der Nachricht Kenntnis zu verschaffen, formell vollendet, jedoch erst mit der tatsächlichen Kenntnisverschaffung des Nachrichteninhalts materiell beendet. In diesen Fällen darf freilich beim hinzutretenden Beitragstäter in subjektiver Hinsicht nichts fehlen, was insb auch den Inhalt des erweiterten Vorsatzes betrifft.[1875] Besonders Augenmerk ist im letzten Fall aber darauf zu richten, dass es sich nicht um ein Vermögensdelikt handelt, weshalb etwaige Anschlussdelikte wie Hehlerei (§ 164) oder Geldwäscherei (§ 165) naturgemäß von vornherein für eine Strafbarkeit des Hinzutretenden ausscheiden.

Zu Recht wirft *Schmoller* in diesem Zusammenhang die zentrale Frage auf, ob dem Hinzukommenden der bereits vor dem Zeitpunkt des Beitritts verwirklichte Unrechtsteil der Tat (hier: die Vermögens-

1870 Siehe OGH 17.04.2002, 13 Os 179/01 = JBl 2003, 464 (krit *Schmoller*).

1871 Vgl RIS-Justiz RS0116322 bzw OGH 17.04.2002, 13 Os 179/01 = JBl 2003, 464 (krit *Schmoller*).

1872 Vgl *Kirchbacher* in WK² § 146 Rz 134 mwN.

1873 Siehe S 154 ff.

1874 Denkbar wäre zB ein technisch verschlüsseltes E-Mail, dessen Inhalt nur von einem sehr versierten User entschlüsselt werden kann, auf dessen Hilfe der Täter – nach Aufklärung über den Tatplan – zurückgreift; ggf könnte auch der Inhalt in einer Fremdsprache verfasst sein und der Täter wird von einem eingeweihten Dolmetscher unterstützt udgl.

1875 Siehe gleich im Anschluss.

schädigung), an dem dieser aber in keiner Weise beteiligt war, angelastet werden darf, sodass das gesamte Unrecht des Delikts dem hinzustoßenden Beitragstäter zugerechnet wird.[1876] Nach *Schmoller* ist eine nachträgliche (sog »sukzessive«) Beteiligung in dem Sinn, dass einem Beteiligten auch vor seinem Hinzutreten bereits verwirklichte Unrechtsteile zugerechnet werden, überhaupt abzulehnen. Ein »nachträgliches Einverständnis« – wie *Schmoller* es nennt – kann seiner Meinung nach keine strafrechtliche Verantwortlichkeit begründen. »Gerecht erscheint, konsequent jeden Täter allein entsprechend dem von ihm (mit-)verwirklichten Unrecht zur Verantwortung zu ziehen.«[1877]

Die Thematik verlangt eine Berücksichtigung kriminalpolitischer und dogmatischer Aspekte. Aus kriminalpolitischer Sicht ist wohl nicht zu verstehen, warum ein geleisteter Beitrag zur Realisierung des vom Beitragstäter bzw unmittelbaren Täters Gewollten, auch nach dem Zeitpunkt, ab dem der unmittelbare Täter wegen der vollendeten Tat haftet, straflos bleiben soll, hat der Beitragstäter doch einen vorsätzlichen kausalen Beitrag (zumindest) zum Endziel geleistet. Der Endzweck verlangt in diesem Fall sowohl die Aufrechterhaltung des tatbestandlichen Schadens (erster Unrechtsteil) als auch dessen Intensivierung. Intensiviert wird der tatbestandsmäßige Vermögensschaden dabei dadurch, dass bis zur materiellen Beendigung das Korrelat zum Vermögensschaden noch nicht eingetreten ist und sich daraus eine das Endziel betreffende »schwebende Situation« insb auch für diverse Opferinteressen einstellt, die erst mit entsprechendem Eintritt der (stoffgleichen) unrechtmäßigen Bereicherung (zweiter Unrechtsteil) verfestigt wird. Es wäre unzutreffend zu glauben, dass das tatsächliche Unrecht einer unrechtmäßigen Bereicherung der bloße »Vorsatz« darauf ist. Richtig ist vielmehr, dass die unrechtmäßige Bereicherung das Übel des zweiten Unrechtsteils darstellt. Der Gesetzgeber hat idZ nur die Deliktsvollendung idZ vorverlegt. Das »Zeitfenster« für einen Tatbeitrag steht daher bis zur Erreichung des materiellen unrechten Endergebnisses offen. Es könnte zB daran gedacht werden, dass die Bank die rechtswidrige Abbuchung erkennt und die Überweisung umgehend storniert, denn »die Wirksamkeit der Gutschrift auf dem Konto des Überweisungsempfängers setzt einen rechtsgültigen Überweisungsauftrag voraus. Fehlt es an einem solchen Überweisungsauf-

1876 Vgl *Schmoller,* JBl 2003, 464.
1877 *Schmoller,* JBl 2003, 464.

trag, geht auch die Annahmeerklärung der Bank, also die Gutschrift, ins Leere und ist daher wirkungslos«.[1878] Solange somit der Geldkurier bzw Überweisungsempfänger noch nicht über den gutgeschriebenen Betrag verfügt hat, liegt – nach zivilrechtlicher Ansicht – noch gar keine »ungerechtfertigte Vermögensverschiebung« vor.[1879] Im Sinne des Strafrechts reicht aber eine bloß vorübergehende Vermögensminderung für einen wirtschaftlich nicht ganz bedeutungslosen Zeitraum aus, um von einem Vermögensschaden zu sprechen, sofern ein – wenn auch nur kurzzeitiger – effektiver Verlust an Vermögenssubstanz eingetreten ist.[1880]

Folglich muss festgestellt werden, dass in casu unzweifelhaft durch das (vorsätzliche) Handeln des Geldkuriers der Vermögensschaden durch die Realisierung der Bereicherung des unmittelbaren Täters intensiviert wurde.

Die Bejahung eines strafbaren Tatbeitrags in einem Stadium nach formeller Vollendung aber vor materieller Beendigung eines Zustandsdelikts orientiert sich mE – hier iZm Delikten mit überschießender Innentendenz – an den Überlegungen eines »allgemeinen Ingerenzprinzips«, das besagt, dass jeder, der eine Beeinträchtigung eines fremden Rechtsguts herbeigeführt hat, verpflichtet ist, den bevorstehenden Schaden oder einen bereits eingetretenen Erfolg wieder abzuwenden.[1881]

Durl stimmte einem solchen Ergebnis anfänglich[1882] zu, indem er zutreffend anführte, dass solange der Täter den angestrebten Endzweck nicht erreicht hat, grundsätzlich – trotz bereits eingetretenen Taterfolgs – noch erhöhte Chancen bestünden, das erlittene Unrecht wieder auszugleichen und die Interessen des Tatopfers zu wahren, noch bevor das Gesamtgeschehen seinen Abschluss findet.

1878 Vgl RIS-Justiz RS0124649 mwN.

1879 OGH 19. 02. 2009, 2 Ob 107/08 m = ecolex 2009, 577 *(Graf)* = ÖBA 2009/1551, 457 *(Bydlinski)* = jusIT 2009/69, 140 *(Mader)*.

1880 Vgl RIS-Justiz RS0094383 mwN.

1881 Vgl idS *Schmoller* in SbgK § 99 Rz 15 mwN; *Leukauf/Steininger,* StGB[3] § 99 Rz 10; *Triffterer* AT[2], 65.

1882 Siehe *Durl,* Die Pflicht zur Verhinderung von mit Strafe bedrohten Handlungen gemäß § 286 StGB (1999) 294 ff; In Anerkennung des dogmatischen Konzepts des Systems der Einheitstäterschaft revidierte *Durl* jedoch seinen ursprünglichen Ansatz; siehe *Durl,* Ausgewählte Aspekte des Normativs Zeit im StGB, in BMJ (Hrsg), 32. Ottensteiner Fortbildungsseminar aus Strafrecht und Kriminologie (2005) 55 (124 bzw 128).

Ein erweiterter Vorsatz beschreibt zwar – wie *Fuchs* richtig anmerkt[1883] – bloß eine Innentendenz, die aber in der Gesamtbetrachtung des Delikts insb hins seines Unwerts ein strafbares (Gesamt-)Verhalten determiniert, bei dem zwar die rechtliche Vollendung der Tat an objektiven Kriterien ausgerichtet ist (was die Haftung des unmittelbaren Täters wegen der vollendeten Tat betrifft), das tatsächliche verbotene Verhalten materiell aber darüber in Form einer – nicht mehr in der Beschreibung des Tatbestands ausdrücklich erfassten – finalen Zielausrichtung hinausreichen kann. Das durch das Gesetz beschriebene strafbare Gesamtverhalten beinhaltet zumindest bei Delikten mit überschießender Innentendenz noch einen weiteren Sachverhalt, der als Endziel nun (vom Täter) aber auch vom Beitragstäter tatsächlich angestrebt wird. Die kriminelle Energie des Täters reicht somit auch grundsätzlich bis zum Erreichen des eigentlichen Endziels. Die tatsächliche unrechtmäßige Bereicherung stellt im materiellen Ergebnis ein Übel dar, das typischer Weise zum Unrecht eines Betrügerischen Datenverarbeitungsmissbrauchs oder auch Betrugs gehört. Aus diesem Grund lässt sich argumentieren, dass sich das vom Gesetzgeber als Unrecht erachtete gesamte Tatgeschehen aus der Vermögensschädigung und der unrechtmäßigen Bereicherung zusammensetzt und dieses nicht durch den formellen Vollendungszeitpunkt begrenzt wird. Vielmehr verlagert der Gesetzgeber die (formelle) Vollendungsstrafbarkeit nach vorne und stellt dafür auf den Eintritt der Vermögensschädigung ab. So wird das als strafwürdig erkannte Gesamtgeschehen bereits mit Eintritt des ersten Unrechtsteiles rechtlich (vollständig) als strafbar erfasst, auf den Eintritt der Bereicherung kommt es (nur formell) nicht mehr an. Was die Rechtsgutbeeinträchtigung anlangt, ist festzuhalten, dass ein Tatbeitrag der erst nach formeller Vollendung eines Delikts, aber noch vor materieller Beendigung desselben geleistet wird, immer noch beachtliche Auswirkungen auf das Rechtsgut haben kann (hier: Intensivierung des Schadens durch Verwirklichung der Bereicherung und Aufrechterhaltung der Vermögensverschiebung). Der hinzutretende Beitragstäter manifestiert die Billigung des bisherige Tatgeschehens in Kenntnis des (nunmehr gemeinsamen) Tatplans durch seine konkrete Beitragshandlung zum von vornherein angestrebten finalen Ziel (hier: Bereicherung).

1883 Siehe *Fuchs,* AT I[8], Rz 28/7.

Der Wortlaut des § 12, dass nicht nur der unmittelbare Täter die strafbare Handlung begeht, sondern auch »jeder […] der sonst zu ihrer Ausführung beiträgt« (dritter Fall), lässt im Übrigen durchaus die Interpretation zu, dass eine »Ausführung« solange vorliegt, bis das rechtsgutverletzende Geschehen insgesamt seinen Abschluss gefunden hat. Weiters ist der Formulierung nicht zu entnehmen, dass es sich ausschließlich um einen Beitrag zur Ausführung der strafbaren Handlung durch den unmittelbaren Täter handeln muss.[1884] Jeder geleistete Beitrag zur Realisierung der Bereicherung bzw Erreichung des eigentlichen Endziels eines strafbaren Gesamtverhaltens kann daher einen Tatbeitrag darstellen. Nach einem solchen Verständnis kann grundsätzlich jede – auch noch so kleine – Förderung des strafbaren Gesamtverhaltens (dh bis zum Abschluss des sozialschädlichen Gesamtgeschehens) eine Tatbeteiligung durch einen sonstigen Beitrag iSd § 12 dritter Fall begründen.

Trotz Verständnisses für die aufgezeigten Gegenmeinungen, insb hins der diesbezüglichen Probleme iZm der dogmatischen Begründbarkeit und eines »unscharfen Verhältnisses« zum Bestimmtheitsgebot und Gesetzlichkeitsprinzip, ist es mE schon aus rechtspolitischen Gründen nicht adäquat, eine Beteiligung nicht bis zur tatsächlichen Beendigung einer Tat und der Erreichung des angestrebten Endziels für möglich zu erachten. Der Beitragstäter schließt sich nämlich der bisherigen Tatausführung – was das materielle Unrecht anlangt – iZm dem zweiten Unrechtsteil (erweiterter Vorsatz) objektiv durch die Realisierung des Endziels und subjektiv überhaupt in voller Hinsicht[1885] an, was die Sozialschädlichkeit seines Tatbeitrags darstellt. Die kriminelle Energie des unmittelbaren Täters endet idR[1886] stets erst mit Erreichung des Endziels.

Diese Erwägungen stützen sich auch auf das Argument, dass sich ein Tatbeitrag (im Gegensatz zu einer Mittäterschaft) lediglich in einer sehr untergeordneten Hilfestellung darstellen kann, die nicht einmal für die Tatausführung unabdingbar sein muss.[1887] Sogar ein psychischer oder intellektueller Beitrag, zB in Form eines Rats oder einer

1884 Vgl RIS-Justiz RS0116322.

1885 Selbst wenn er auch erst nach tatbestandlichen Erfolgseintritt hinzutritt.

1886 Er könnte die Verfolgung seines angestrebten Endziels allerdings vorzeitig – aber nach formeller Vollendung der Tat – aufgeben, oder es kann die Erreichung des Endziels aus anderen Gründen faktisch nicht mehr möglich sein.

1887 Vgl RIS-Justiz RS0108726 mwN; weiters *Fabrizy,* StGB[11] § 12 Rz 10a.

Bestärkung im Tatentschluss, ist nach stRsp ausreichend.[1888] Folglich genügt es im Sinn des § 12 dritter Fall bereits, dass das Verhalten des Beitragstäters der Vorbereitung einer (später zumindest versuchten) Straftat des unmittelbaren Täters dient, die zur Zeit des Tatbeitrages weder in allen Einzelheiten schon feststehen noch bereits in die Entwicklungsstufe des strafbaren Versuches getreten sein muss. Es kommt nicht einmal darauf an, dass die Tathandlung des Beitragstäters zur Unterstützung oder Förderung des Delikts eines anderen ausführungsnah sein muss.[1889]

Man könnte noch eine zusätzliche Komponente ins Spiel bringen, nämlich die »bewusste Disposition des unmittelbaren Täters bezüglich eines diversen Beitrags eines Hinzutretenden«. Veranschaulichen lässt sich dies mit folgendem Beispiel: Der technisch unbegabte A lädt sich ein Spionageprogramm (Keylogger, Sniffer etc) aus dem Internet auf seinen Computer herunter (§ 126c), um sich mit diesem Kenntnis von den E-Mails seiner Frau zu verschaffen, weil er eine Affäre seiner Frau mit einem anderen Mann vermutet. Da er aber nicht weiß, wie dieses Programm funktioniert bzw wie er es einsetzen muss, klärt er seinen technikaffinen Freund X über sein Vorhaben (Tatplan) vollständig auf und ersucht ihn, ihm die Funktionalität und die Verwendung dieses Programms zu erklären. X willigt ein und leistet die erbetene Hilfe. Bevor nun letztlich aber das Programm vom unmittelbaren Täter A tatsächlich am Laptop seiner Frau installiert bzw empfangsbereit gemacht werden kann, löscht A versehentlich das Programm.[1890]

Da bis zu diesem Zeitpunkt noch keine ausführungsnahe Handlung zB des § 119 gesetzt wurde, ist das Vorbereitungsdelikt des § 126c Abs 1 heranzuziehen. A verschafft sich bzw besitzt ein Computerprogramm iSd § 126c Abs 1 Z 1 mit dem Vorsatz, es zur Begehung eines inkriminierten Verhaltens nach zB § 119, zu gebrauchen. Die Tat ist mit dem Sich-Verschaffen bzw Besitzen formell vollendet. Nach Meinung des OGH iZm Delikten mit überschießender Innentendenz wäre eine Beteiligung des X aber darüber hinaus noch möglich, nämlich solange bis das Delikt materiell sein Ende gefunden hat.[1891] Anschlussdelikte

1888 Vgl RIS-Justiz RS0089549 mwN.
1889 Vgl RIS-Justiz RS0090516 mwN.
1890 § 119 wird daher noch nicht versucht, weshalb ausschließlich § 126c anwendbar ist.
1891 Vgl jüngst bestätigt durch OGH 05.07.2012, 13 Os 36/12m; OGH 17.04.2002, 13 Os 179/01 = JBl 2003, 464 (krit *Schmoller);* OGH 09.09.1982, 12 Os 66/82; RIS-Justiz RS0090734 (T1).

(wie §§ 164, 165) gibt es für solche Fälle nicht. Nach den oben angeführten Lehrmeinungen könnte sich X in diesem Fall gar nicht mehr an § 126c beteiligen. Beachtet man aber, dass es in concreto – aus Sicht der hL – nur vom Zeitpunkt der Befassung des X abhängt, ob der unmittelbare Täter diesen noch einer Strafbarkeit »aussetzt« oder nicht, so muss man sachwidrige Ergebnisse in Kauf nehmen. A geht auf X erst nach formeller Deliktsvollendung zu und ermöglicht es X somit auch erst ab diesem Zeitpunkt, einen sonstigen Beitrag vorsätzlich (aber straflos) zu leisten.

Würde hingegen A den X bereits vor dem Herunterladen des Programms einbeziehen und ihn nach Offenbarung seines Vorhabens ersuchen, ihm die Einsatzmöglichkeit des Spionageprogramms zu erklären, würde X unstrittig einen Tatbeitrag iSd § 12 dritter Fall leisten, da er den unmittelbaren Täter dadurch zumindest physisch in seinem Vorhaben bestärkt, das Programm tatsächlich herunterzuladen und zu verwenden. In beiden Fällen macht X aber stets dasselbe, er unterrichtet in hinreichender Tatplankenntnis den unmittelbaren Täter über die Einsatzmöglichkeit des Schadprogramms und weist ihn in dessen Benützung ein. X kennt den Tatplan und billigt den bisherigen Tatverlauf, in welchen er auch nachträglich einwilligt. Er hält die Verwendung des Tatobjekts als Tatmittel einer Verletzung des Telekommunikationsgeheimnisses (§ 119) durch A ernstlich für möglich und findet sich damit ab.[1892] Andere Ergebnisse wären hier nicht sachgerecht.

Aus all diesen Überlegungen stellt sich schließlich die Frage, warum nicht auch die – zwar nicht mehr tatbestandsmäßige – Realisierung des Inhalts des erweiterten Vorsatzes als »materieller Unwert« für einen strafbaren Tatbeitrag ausreichend sein sollte, wird doch das rechtsgutverletzende Verhalten dadurch sogar noch intensiviert. Eine »unrechtmäßige Bereicherung« – zurückkommend auf den Fall mit dem Geldkurier – ist auch ein typisches mit einem Betrug oder einem Betrügerischen Datenverarbeitungsmissbrauch festverbundenes (sozialschädliches) Unrecht. Man sollte mE im hier interessierenden Zusammenhang davon ausgehen, dass nicht nur die Herbeiführung des verpönten, im Tatbild umschriebenen Zustands strafbar sein soll, sondern auch die Aufrechterhaltung und Intensivierung desselben durch Realisierung der Bereicherung.

1892 Dh auch X handelt mit (erweitertem) Gebrauchsvorsatz.

Darüber hinaus ist es nämlich nach hM nicht einmal erforderlich, dass der Beitragstäter überhaupt Tatbestandsmerkmale erfüllt, da § 12 die Strafbarkeit eben auf einen bloßen Beitrag zur Tat ausdehnt.[1893]

Schließlich ist auch im hier angesprochenen Fall die Handlung des Geldkuriers im Tatplan des unmittelbaren Täters unabdingbar für seine tatsächliche Bereicherung, welche auch den – wenn auch bloß materiellen – Abschluss des gesamten Tatgeschehens bildet. Im Fall des § 126c könnte der unmittelbare Täter das Programm ohne Anleitung des Hinzutretenden gar nicht »gebrauchen«.

In subjektiver Hinsicht muss der Beitragstäter vollen Tatbildvorsatz auf Vollendung der »gesamten Tat« (durch den Ausführungstäter) haben[1894] und zumindest die Tat des unmittelbaren Täters ihrer Art nach und in groben Umrissen kennen.[1895] Bei Delikten mit erweitertem Vorsatz muss der Beitragstäter freilich auch selbst diese Innentendenz aufweisen[1896], wie zB den Bereicherungsvorsatz iZm § 148a Abs 1.

Handelt der Geldkurier – wie im angesprochenen Beispielsfall – bei der Behebung des Bargeldes mit »bösem Vorsatz« (einschließlich Bereicherungsvorsatz), ist zu diesem Zeitpunkt die Tat nach hM[1897] noch nicht materiell beendet, weshalb ein strafbarer Tatbeitrag iSd § 12 dritter Fall (hier: Realisierung der Bereicherung des unmittelbaren Täters) – nach Meinung des OGH – noch möglich ist. Die materielle Beendigung tritt nämlich erst mit tatsächlicher Bereicherung des unmittelbaren Täters ein. Beabsichtigte hingegen der unmittelbare Täter von Anfang an tatsächlich nur den Geldkurier zu bereichern – was doch sehr seltsam klingt –, wäre mit der Zubuchung des Giralgeldes am Konto des Geldkuriers das Delikt bereits materiell beendet.

Was den Bereicherungsvorsatz beim Geldkurier anlangt, so könnte ggf die Unmittelbarkeit der Bereicherung (Stoffgleichheit zwischen Schaden und Bereicherung) problematisch werden, da sich der Bereicherungsvorsatz des Geldkuriers auf die vom unmittelbaren Täter versprochene Provision für die Tätigkeit des Geldkuriers bezieht.[1898] Es ließe sich auf den ersten Blick darauf schließen, dass sich der Geld-

1893 Siehe zur Kritik an *Schmoller* auch *Fuchs,* AT I[8], Rz 33/63.
1894 Dh er muss hinreichend in Kenntnis des (gesamten) Tatplans sein und diesen billigen.
1895 Siehe RIS-Justiz RS0120600 mwN.
1896 Siehe etwa OGH 27.09.2007, 12 Os 101/07f.
1897 Siehe ausf oben.
1898 Vgl *Kienapfel,* BT[3] § 148a Rz 42.

kurier nicht aus dem Vermögen des »Überweisungsopfers« bereichern will, weshalb es an der Unmittelbarkeit der Bereicherung fehlt. Weiß nun der Geldkurier im Zeitpunkt der Geldbehebung, dass das Geld aus dem Vermögen des Überweisungsopfers stammt, ist ihm auch bewusst, dass die »Provision«, die er sich für seine »Arbeit« einbehalten kann, unmittelbar aus der durch § 148a verwirklichten Manipulation der Datenverarbeitung stammt. Anders wäre es freilich, wenn der Geldkurier dem unmittelbaren Täter den gesamten Betrag auszahlen müsste und erst danach seine Entlohnung aus dem Vermögen des unmittelbaren Täters ausgezahlt bekäme. Nur in einem solchen Fall mangelt es an der notwendigen Stoffgleichheit, was den Vorsatz ausschließt.

Folgt man idZ etwa den Meinungen von *Schmoller*[1899] oder auch *Fuchs*[1900] (der im Übrigen auf die »Lehre von der Beendigung der Straftat« überhaupt verzichten will), dass die formelle Vollendung mit der materiellen Beendigung – außer bei Dauerdelikten – generell zusammenfallen sollte, wäre eine (sukzessive) Beteiligung des Geldkuriers im hier angesprochenen Beispielsfall iZm § 148a nicht mehr möglich, was in concreto aber genau zu den angesprochenen unbilligen Ergebnissen führen würde.

b. Anschlussdelikte

Ggf könnte (bei Vermögensdelikten) dem Geldkurier – Wissentlichkeit (iSd § 5 Abs 3) und eine qualifizierte Begehung[1901] vorausgesetzt – Geldwäscherei nach § 165 Abs 2 vorgeworfen werden. Problematisch wäre dabei aber, dass es sich für die Anwendbarkeit von § 165 um einen Vermögensbestandteil handeln muss, der aus einer in Abs 1 genannten strafbaren Handlung herrührt. Darunter versteht § 165 Abs 5 einen Vermögensbestandteil, den der Vortäter durch die Vortat »erlangt« oder für ihre Begehung empfangen hat oder in dem sich der Wert des ursprünglich erlangten oder empfangenen Vermögenswertes verkörpert.[1902]

1899 Siehe oben.

1900 Siehe *Fuchs,* AT I[8], Rz 28/7 f bzw 33/61.

1901 Da als Anwendungsvoraussetzung für § 165 Abs 2 nach § 165 Abs 1 ua eine gegen fremdes Vermögen gerichtete Vortat verlangt wird, die mit mehr als einjähriger Freiheitsstrafe bedroht ist.

1902 Siehe dazu auch statt vieler *Kirchbacher* in WK² § 165 Rz 5 (Stand September 2011).

Im vorliegenden Beispielsfall hat der unmittelbare Täter aber gerade (noch) nicht diesen Vermögenswert erlangt. Aus diesem Grund war auch der Geldkurier Teil des Tatplans, der die Erlangung der »Beute« durch Barabhebung und Weiterleitung des Geldes erst realisieren sollte. Der ausdrückliche Wortlaut des § 165 Abs 5, dass der Täter den Vermögensbestandteil durch die Tat erlangt haben muss, steht einer Subsumtion in unserem Fall entgegen, da der Täter den Vermögenswert noch nicht in seiner Verfügungsmacht hatte. Doch selbst wenn man der Ansicht wäre, dass eine Verfügungsmöglichkeit über den Vermögenswert (hier: Giralgeld) ausreichend sei (da der unmittelbare Täter über den Vermögensbestandteil durch online-Transaktion effektiv disponierte), wäre dennoch nicht von einem »Erlangen« des Vermögenswertes zu sprechen.

Anders stellt sich die Situation aber iZm einem Ladendiebstahl dar, bei dem der Täter nach dem Verlassen des Geschäfts, die gestohlene Sache vorerst noch in einem Gebüsch versteckt, um sie später von einem Komplizen – der wiederum erst nachträglich in den Tatplan eingeweiht wurde – abholen und verwahren zu lassen. In diesem Fall hat nämlich der unmittelbare Täter die Beute – wenn auch nur vorübergehend – erhalten, da er sie in der Zeit vom Verlassen des Geschäfts bis zum Verstecken der Beute in seinem Gewahrsam hatte. Nun ist zwar für einen derartigen Sachverhalt der Tatbestand der Hehlerei (§ 164 Abs 2) zu prüfen (iSd Tathandlung »sonst an sich bringt«), doch stellt dieser auf eine »Sache«[1903] ab, die der Vortäter durch seine Tat erlangt hat (vgl § 164 Abs 1).[1904] Für die Beute des Ladendiebstahls ist dies in diesem Fallbeispiel unzweifelhaft zu bejahen.

Für andere (hier interessierende) Delikte mit überschießender Innentendenz, die nicht das Vermögen schützen, wie zB §§ 118a, 119, 119a, 120 (2a), kämen die genannten Anschlussdelikte aber a priori nicht in Betracht.

7. Subjektive Tatseite

Der Täter muss jeweils im Mindeststärkegrad eines dolus eventualis mit Tatbildvorsatz, bezogen auf sämtliche objektive Tatbestandsmerk-

1903 Im Sinne einer »körperlichen Sache«.

1904 Genauer gesagt ist (körperliche) »Sachidentität« bezüglich des vermögenswerten Gegenstands aus der Vortat und der Hehlerei gefordert.

male sowie mit einem erweiterten Vorsatz, sich oder einen Dritten unrechtmäßig zu bereichern, handeln. »Unrechtmäßig« bedeutet in diesem Zusammenhang, dass der Täter keinen Anspruch auf die Bereicherung haben darf.

8. Qualifikationen

§ 148a Abs 2 normiert drei Qualifikationsfälle: Die gewerbsmäßige Begehung wird in Abs 2 Fall 1 ebenso wie die Herbeiführung eines € 3.000,– übersteigenden Schadens (Fall 2) mit bis zu drei Jahren Freiheitsstrafe bedroht. Wer durch die Tat einen € 50.000,– übersteigenden Schaden herbeiführt (Fall 3), ist mit Freiheitsstrafe von einem bis zu zehn Jahren zu bestrafen.

9. Sonstiges

Das Offizialdelikt des § 148a wird gem § 166 Abs 1 privilegiert, wenn die Tat im Familienkreis begangen wird. Darüber hinaus wird es zu einem Privatanklagedelikt (§ 166 Abs 3). Eine Strafaufhebung durch Tätige Reue kommt unter den Voraussetzungen des § 167 in Betracht.

Was die sachliche Zuständigkeit anlangt, so fällt das Grunddelikt des Abs 1 gem § 30 Abs 1 StPO in die Kompetenz des Bezirksgerichts. Die Deliktsqualifikationen des Abs 2 Fall 1 und 2 fallen sachlich gem § 31 Abs 4 Z 1 StPO dem Einzelrichter am Landesgericht zu. Fall 3 fällt in die sachliche Zuständigkeit des Landesgerichts als Schöffengericht (§ 31 Abs 3 Z 1 StPO).

Anzumerken ist dabei, dass, soweit auf Grund bestimmter Tatsachen anzunehmen ist, dass ein iSd § 148a Abs 2 Fall 2 herbeigeführter Schaden € 5.000.000,– übersteigt, die »Wirtschafts- und Korruptionsstaatsanwaltschaft« (WKStA) gem § 20a Abs 1 Z 1 StPO zur Leitung des Ermittlungsverfahrens zuständig ist. Unpräzise wird jedoch vom Gesetzgeber im Klammerzitat auf § 148a Abs 2 »Fall 2« verwiesen, wobei nur (Qualifikation-)Fall 3 bzw der 2. HS gemeint sein kann.[1905]

1905 Siehe dazu bereits *Bergauer/Schmölzer* in Jahnel/Mader/Staudegger, IT-Recht[3], 635 (657).

III. Datenfälschung (§ 225a)

> § 225a Wer durch Eingabe, Veränderung, Löschung oder Unterdrückung von Daten falsche Daten mit dem Vorsatz herstellt oder echte Daten mit dem Vorsatz verfälscht, dass sie im Rechtsverkehr zum Beweis eines Rechtes, eines Rechtsverhältnisses oder einer Tatsache gebraucht werden, ist mit Freiheitsstrafe bis zu einem Jahr zu bestrafen.[1906]

Die Datenfälschung (§ 225a) wurde in Umsetzung des Art 7 CCC[1907] mit dem StRÄG 2002 ins Kernstrafrecht eingeführt. Systematisch ist diese Strafbestimmung bei den Urkundendelikten als Pendant zur Urkundenfälschung (§ 223) eingegliedert, da »Datenurkunden« nach hM keine Urkunden nach § 74 Abs 1 Z 7 sind. Eine Anpassung des Urkundenbegriffs hat der historische Gesetzgeber aber bewusst vermieden.[1908] Als Rechtsgut hinter dieser Bestimmung ist das allgemeine Interesse des »Vertrauens auf die Echtheit und Zuverlässigkeit elektronischer Dokumente« anzusehen.

Art 7 CCC besagt:

> »Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.«

Nach den GMat wurde dem Begriff »inauthentic data« sowohl bezüglich der Identität des Herstellers der Urkunde als auch bezüglich der Richtigkeit des Inhaltes der Urkunde Relevanz zuerkannt. Allerdings sei als Mindeststandard zumindest die Täuschung über die Identität des Herstellers der Urkunde zu erfassen.[1909]

1906 BGBl 60/1974 idF I 134/2002.
1907 »Computer-related forgery«.
1908 Siehe ErlRV 1166 BlgNR XXI. GP, 31.
1909 Siehe ErlRV 1166 BlgNR XXI. GP, 30.

A. Tatobjekt der Datenfälschung

Pönalisiert wird die Fälschung bzw Verfälschung von Daten iSd § 74 Abs 2. Tatobjekt sind demnach personenbezogene oder nicht personenbezogene Daten, aber auch Programme. Nach hM handelt es sich dabei um Daten, die mangels Schriftform keine »Urkunden« sind.[1910]

Der Wortlaut des § 225a ist aber in diesem Zusammenhang insoweit unscharf, als die »Eingabe, Veränderung, Löschung oder Unterdrückung von Daten« angesprochen ist und die Begriffsbestimmung von Daten in § 74 Abs 2 – anders als Art 7 CCC[1911] – gerade keine Aussage darüber trifft, in welcher Form die Daten verarbeitet werden müssen.[1912] § 74 Abs 2 stellt nämlich – abgesehen vom Einschluss der Computerprogramme – lediglich klar, welchen Informationsgehalt Daten iSd Strafrechts haben können, nämlich einen personenbezogenen oder nicht personenbezogenen. Mit dieser weitgefassten Absteckung bzw Konturierung des Anwendungsbereichs wären aber grundsätzlich auch konventionelle Daten zB auf Papier von § 225a mitumfasst. Würden daher solche Daten verändert oder unterdrückt, sodass zB falsche Daten hergestellt oder echte Daten verfälscht werden, würde § 225a in echte Konkurrenz mit der Urkundenfälschung (§ 223) treten. Dass dies nicht intendiert ist und unsachlich wäre, liegt auf der Hand. Die Problematik tritt daher wiederum nur deshalb in Erscheinung, weil der Gesetzgeber weder in der allgemeinen Begriffskonkretisierung des § 74 Abs 2 noch im konkreten Tatbestand des § 225a eine Einschränkung auf »automationsunterstützt verarbeitete, übermittelte oder überlassene Daten« (Computerdaten) vorgenommen hat, wie es auch in § 126a Abs 1 gemacht wurde. Da sich nicht alle Tathandlungen des § 225a ausschließlich über informationstechnische Manipulationen realisieren lassen (vgl zB die Eingabe von Daten) muss im deliktsspezifischen

1910 Siehe dazu *Thiele* in SbgK § 225a Rz 17 mwN; weiters *Reindl* in WK² § 225a Rz 3 (Stand Juli 2006).

1911 Hier sind ausschließlich und ausdrücklich »Computerdaten« gemeint.

1912 Selbst für die »Programme« ist nicht eindeutig erkennbar, von welcher Darstellungsform von Computerprogrammen der Gesetzgeber ausgeht (zB Object Code oder Source Code). Über eine rahmenbeschlusskonforme (bzw auch konventionsgerechte) Interpretation wird man wohl vom ausführbaren Maschinenprogramm (Object Code) und mittels Interpreterprogramm unmittelbar ausführbaren Source Code ausgehen müssen, da in beide internationalen Vorgaben von einem Programm die Rede ist, »das die Ausführung einer Funktion durch ein Informationssystem auslösen kann«.

Kontext der überschießende Gesetzeswortlaut teleologisch – im Sinne der ratio legis – auf »Computerdaten«[1913] reduziert werden.[1914]

Erneut deutet die Begriffsproblematik des § 74 Abs 2 darauf hin, dass die vorgenommene allgemeine inhaltliche Ausdehnung des Datenbegriffs – anders als es die GMat gerade in diesem Zusammenhang beabsichtigen[1915] – nicht ausreichend ist. § 225a bezieht sich daher in gleichem Maß – nach der hier verwendeten Terminologie – sowohl auf »Daten im engen Sinn«[1916] als auch auf »Daten im weiten Sinn«[1917].

Reindl-Krauskopf vertritt zum Tatobjekt der Datenfälschung die Meinung, dass »Programme allerdings bloß mathematische Beschreibungen der technischen Abläufe sind, die keinen Beweiswert im Rechtsverkehr haben und außerdem nicht zum Beweis gegenüber einem Menschen eingesetzt werden können […], weil sie über ihre mathematische Beschreibung hinaus nicht visualisiert werden können, kommen sie nicht als Fälschungsobjekte für § 225a in Frage«.[1918]

Neben der ausdrücklichen Klarstellung in den GMat[1919], dass neben personenbezogenen und nicht personenbezogenen Daten auch »Computerprogramme« erfasst sind, können aber mE unter Berücksichtigung des spezifischen Charakters von Computerprogrammen noch weitere Argumente gegen die Aussage *Reindl-Krauskopfs* ins Treffen geführt werden[1920]:

Menschen kommunizieren untereinander auf Grundlage einer gemeinsamen Sprache. Versteht einer der Gesprächspartner diese Sprache nicht, so ist eine Verständigung nicht oder nur schwer möglich. Schwieriger wird es noch, wenn darüber hinaus ein Gesprächspartner über einen nur eingeschränkten Sprachvorrat bzw -umfang verfügt. Ähnlich verhält es sich zwischen Mensch und Maschine. Natürlich-sprachliche Problemlösungen können von einem »automatischen Prozessor« nicht unmittelbar verarbeitet werden. Ein Prozessor bzw Automat ist nicht in der Lage, einen dem Menschen zur Verfügung ste-

---

1913 Vgl auch ErlRV 1166 BlgNR XXI. GP, 30 bzw den Regelungsinhalt des Art 7 CCC.
1914 In diesem Sinne auch der Datenbegriff des Datenbetrugs (§ 147 Abs 1 Z 1 dritter Fall).
1915 Siehe ErlRV 1166 BlgNR XXI. GP, 30.
1916 Was die technische Verarbeitungsform betrifft.
1917 Was die Information anlangt, da falsche oder verfälschte Daten über die Identität des Ausstellers täuschen müssen.
1918 *Reindl* in WK² § 225a Rz 3.
1919 Siehe ErlRV 1166 BlgNR XXI. GP, 30.
1920 Siehe bereits *Bergauer* in BMJ, 35. Ottensteiner Fortbildungsseminar, 27 (29).

henden umfangreichen Sprachvorrat zu bedienen, um Problemlösungen in verbaler oder formaler Art zu beschreiben.[1921] Auch besitzt nicht jeder Prozessor dieselben Fähigkeiten, was die Verständigung zudem erschwert. Es gibt grundsätzlich zwei Möglichkeiten, um Problemlösungen dem Prozessor verständlich zu machen:

Die erste Alternative bot in den Anfängen der Informatik die einzige Möglichkeit, um überhaupt Programme von einem Prozessor ausführen zulassen. Sie besteht darin, nur Sprachelemente in einem formalisierten Algorithmus[1922] zu verwenden, mit denen der jeweilige Prozessor auch umgehen kann (maschinennahe Programmierung mittels Assemblersprache).[1923]

Die zweite Alternative gestattet, einen Beschreibungsformalismus zu wählen, mit dem sich die Problemlösungsvorschriften ohne Rücksicht auf den jeweiligen Prozessor darstellen lassen. Dazu wird jedoch ein »Übersetzer« benötigt, der alle Sätze einer Quellsprache in gleichbedeutende Sätze einer Zielsprache transformiert (problemorientierte Programmierung).[1924] Ein derartiger Übersetzungsvorgang kann auf unterschiedliche Arten durchgeführt werden.

Beim »Kompilieren« übersetzt ein Compiler den Quellcode[1925] eines Programms einer problemorientierten Programmiersprache auf einmal in den Maschinencode[1926]. Wobei erst nach einer vollständigen Analyse des Programms und bei Fehlerfreiheit der strengen Syntax eine vom jeweiligen Prozessor eines entsprechenden Prozessortyps verarbeitbare Binärdatei entsteht (zB .exe-Datei). Das so entstandene Objekt-Programm kann dann beliebig oft ausgeführt werden, ohne dass eine erneute Analyse der Anweisungen durchgeführt wird.[1927]

Eine weitere Form der Übersetzung kann über sog »Interpreter« realisiert werden. Dabei wird der entsprechende Algorithmus eines Computerprogramms zeilenweise in Laufzeit analysiert und von einem eige-

---

1921 Siehe zu diesen Ausführungen *Balzert,* Lehrbuch², 72 ff.

1922 Rechenvorschrift oder Handlungsanweisung zur Lösung mathematischer Probleme (siehe zu Algorithmen allgemein *Kersken,* IT-Handbuch⁵, 33 f bzw 91).

1923 Die Assemblerprogrammierung kommt aber auch heute noch in den unterschiedlichsten Bereichen zum Einsatz.

1924 Siehe dazu ausf *Balzert,* Lehrbuch², 74.

1925 Darunter versteht man die formale Notation des Computerprogramms in einer Programmiersprache (Source Code).

1926 In den Befehlssatz des Prozessors übersetzter Object Code (sog »Maschinensprache«).

1927 Siehe *Balzert,* Lehrbuch², 84 ff.

nen Computerprogramm, dem Interpreter, übersetzt.[1928] Das Ergebnis wird dann unmittelbar am Bildschirm anzeigt. Als Echtzeit-Übersetzer fungiert dabei ein Interpreter-Programm, wie zB ein Internetbrowser, der den Quellcode einer Webpage interpretiert und visualisiert (zB HTML, Javascript, PHP).[1929] Mit dieser Übersetzer-Technologie erreicht man eine höhere »Abstraktionsschicht«, da die zur Problemlösung auszuführenden Programme nicht auf den jeweiligen Prozessortyp abgestimmt sein müssen.[1930] Ebenso gibt es in diesem Bereich Mischformen, wie zB Just-in-Time-Compiler, die aus Compiler- und Interpreterkomponenten (zB Java) bestehen.[1931]

Eine Website, als Summe sämtlicher »durch Interpreter ausführbarer Quelltexte«, kann nun aber durchaus auf die Willensbildung eines Menschen einwirken und wird auch im Rechtsleben relevant, wenn in ihrer Darstellung über die Identität des Herstellers/Gestalters getäuscht wird.[1932]

Ebenso können »kompilierte« Programme von seriösen Unternehmen als Service-Leistung für ihre Kunden eingesetzt werden, um gewisse Dienste vereinfacht abwickeln zu können, man denke etwa an Banking-Software (zB auch Apps für Smartphones oder Tablet-PCs). In diesem Sinn kann bspw das Herstellen eines »falschen« Computerprogramms durchaus geeignet sein, die Willensbildung des Users zu beeinträchtigen. »Falsch« sind nämlich Daten und eben auch Programme dann, wenn der Eindruck vermittelt wird, ein anderer Hersteller, Aussteller bzw Entwickler wäre für diese Software verantwortlich.[1933]

Als Beispiel kann an dieser Stelle ein Banking-Programm (als Client-Applikation) genannt werden, das von einem Programmierer derart entwickelt wurde, dass es in seiner Ausgabe bzw Oberfläche dem Erscheinungsbild eines seriösen Bankinstituts nachgebildet ist (Logo, Schrift, Farbgestaltung usw) und als Beweis im Rechtsverkehr gegenüber einem »Bankkunden« eingesetzt wird.

1928 Siehe *Kersken,* IT-Handbuch[5], 47.

1929 Vgl *Balzert,* Lehrbuch[2], 57 f.

1930 Vielmehr muss der Interpreter, als eigenständiges Computerprogramm, diesen Anforderungen Genüge tun.

1931 Derartige Programme werden erst als Ganzes in einen Zwischencode (Bytecode) übersetzt und in weiterer Folge von einem Interpreter ausgeführt; siehe *Balzert,* Lehrbuch[2], 84 f.

1932 Vgl ähnlich *Thiele* in SbgK § 225a Rz 30.

1933 Siehe dazu auch *Thiele* in SbgK § 225a Rz 28; weiters *Reindl* in WK[2] § 225a Rz 5.

Für die Verwirklichung des § 225a ist es wesentlich, dass die Daten längerfristig und nicht nur flüchtig gespeichert sein dürfen (Perpetuierungsfunktion). Daher kommen als Datenträger insgesamt nur permanente oder semi-permanente Speichermedien, nicht aber flüchtige, in Betracht.[1934]

Daran anknüpfend muss iSd Datenfälschung jedenfalls ein bestimmter Austeller bzw Hersteller erkennbar sein[1935], denn anonyme Daten und Programme fallen nicht unter § 225a.[1936] Der Täter nimmt in solchen Fällen im Sinne einer »Garantiefunktion« die Autorität einer bestimmten natürlichen oder juristischen Person, einer Behörde oder einer Firma in Anspruch.[1937] Es kommt nicht auf den konkreten Schreiber bzw Programmierer an, sondern auf den Erklärer.[1938]

Der Anschein, dass die konkreten Daten von einem bestimmten »Aussteller« stammen, kann sich aus den verschiedensten Merkmalen ergeben. Beispielsweise spricht *Reindl-Krauskopf* in diesem Zusammenhang die Verwendung einer bestimmten E-Mail-Adresse an.[1939]

Allerdings ist mE[1940] nicht nur der personenbezogene »local-part« einer E-Mail-Adresse geeignet, einen bestimmten Absender zu individualisieren, wie zB Herrn Max Muster über die E-Mail-Adresse »max.muster@xyz-bank.at«. Vielmehr weist in vielen Fällen der »domain-part« der E-Mail-Adresse auf einen ganz bestimmten Inhaber bzw einen »Erklärer« einer juristischen Person hin (zB »office@xyz-bank.at«). Die Überzeugungskraft eines (global registrierten) aussagekräftigen domain-parts stärkt den E-Mail-Empfänger noch vielmehr in seiner Annahme, die Nachricht stamme von der »XYZ Bank«. Der bloße Anschein bezüglich der Erkennbarkeit des Ausstellers reicht im Urkundenstrafrecht aus.[1941] Ein personifizierter local-part allein, ohne aussagekräftige Domänenangabe, wie zB »max.muster@network.com«, vermag es mE weniger, die »XYZ Bank« als Absender bzw Aussteller vorzutäuschen. Dem Empfänger eines solchen E-Mails werden sicher-

1934 Siehe zur technischen Unterscheidung etwa *Korge,* Beschlagnahme, 14 f.
1935 Siehe dazu auch OGH 23.04.2007, 15 Os 6/07g.
1936 Siehe *Thiele* in SbgK § 225a Rz 23; auch *Reindl-Krauskopf,* Computerstrafrecht², 66.
1937 Vgl dazu *Bertel/Schwaighofer,* Österreichisches Strafrecht. Besonderer Teil II (§§ 169 bis 321 StGB)¹¹ (2015) § 225a Rz 2.
1938 Siehe dazu *Thiele* in SbgK § 225a Rz 22 mwN; auch *Reindl* in WK² § 225a Rz 13.
1939 Siehe *Reindl-Krauskopf,* Computerstrafrecht², 66.
1940 Siehe dazu auch bereits *Bergauer,* RZ 2006, 82.
1941 Siehe dazu *Kienapfel/Schroll* in WK² § 223 Rz 56 (Stand Juli 2006).

lich nicht sämtliche Namen der MitarbeiterInnen der »XYZ Bank« bekannt sein, um aufgrund der Namensangabe festzustellen, ob und welches Unternehmen diesen ganz bestimmten Mitarbeiter beschäftigt, der das E-Mail als Verfasser unterzeichnet hat. Es kommt eben, wie oben angeführt, nicht auf den konkreten Schreiber an, sondern auf den Erklärenden (zB XYZ-Bank als Institution, anstelle eines Bankmitarbeiters, der das E-Mail angeblich verfasst hat).[1942] *Reindl-Krauskopf* ist aber insofern zuzustimmen, als tatsächlich weitgehend unbestimmte – wie sie es nennt – »Gruppenbezeichnungen« Verwendung finden (zB office@network.com). Man muss daher innerhalb dieser Gruppenbezeichnungen eines domain-part, zwischen »bestimmten« und »unbestimmten« generischen Bezeichnungen unterscheiden. Da kann sich die Bestimmbarkeit je nach Einzelfall unterschiedlich ergeben.

B. Falsche und verfälschte Daten

Die Tathandlungen sind das Herstellen falscher und das Verfälschen echter Computerdaten.

Doch erfasst § 225a nur solche Fälschungen bzw Verfälschungen von Daten, die auf die im Gesetz festgelegte Art und Weise, nämlich »durch Eingabe, Veränderung, Löschung oder Unterdrückung von Daten« herbeigeführt wird. Es liegt folglich ein verhaltensgebundenes (Erfolgs-)Delikt vor.

Als »falsche Daten« (oder »unechte« Daten) werden solche angesehen, die nicht von der Person stammen, die als Hersteller bzw Aussteller angegeben ist (siehe oben). Verfälschte Daten hingegen sind ursprünglich echte, die nachträglich durch Austausch der Angabe des Herstellers oder Ausstellers oder durch einen anderen gedanklichen Inhalt geändert wurden.[1943] Die Begriffsbestimmungen, die allerdings aus der Rsp stammen, wie falsche (= »unechte«) Daten bzw verfälschte Daten[1944], beziehen sich – anders als etwa im Kontext der Datenbeschädigung (§ 126a) – nicht auf einen technischen Datenbegriff, sondern

1942 Siehe zum weiten personalen Garantieelement der Garantiefunktion von Urkunden insb *Kienapfel/Schroll* in WK² § 223 Rz 54.

1943 Siehe OGH 10.10.2012, 12 Os 106/12y = JBl 2013, 536 *(Salimi);* OGH 23.04.2007, 15 Os 6/07g; weiters *Thiele* in SbgK § 225a Rz 28; *Reindl* in WK² § 225a Rz 4 ff.

1944 Vgl Siehe OGH 10.10.2012, 12 Os 106/12y = JBl 2013, 536 *(Salimi);* OGH 23.04.2007, 15 Os 6/07g.

auf die Information, also den für den Menschen relevanten, durch Daten repräsentierten Inhalt (hier: Daten im weiten Sinn). Es kommt darauf an, dass die Daten derart erzeugt oder manipuliert werden, dass der Anschein erweckt wird, das Dokument stamme von einem anderen Aussteller. Dieses Anscheinerwecken erfordert nun eine Fälschung bzw Verfälschung der diesbezüglichen (wenn auch nur begleitenden) Information. Für § 225a ist daher – wie bei § 223 – der rein ausstellerbezogene Echtheits- bzw Fälschungsbegriff maßgeblich.[1945] »Lugdaten«, welche die inhaltliche Richtigkeit der elektronischen Dokumente betreffen[1946], spielen keine Rolle.[1947]

Es ist somit festzuhalten, dass nicht jede Manipulation von Computerdaten eine Datenfälschung iSd § 225a impliziert.[1948] Der Datenbegriff des § 74 Abs 2 ist nämlich – wie bereits ausgeführt – unpräzise und wenig hilfreich. Er unterscheidet nicht zwischen technischer Repräsentation einer Information und der Information selbst.[1949] Eine Computerdatenfälschung liegt aber gerade dann nicht vor, wenn zB bloß syntaktische Änderungen in der Darstellungsweise elektronischer Daten vorgenommen werden[1950], ohne den Informationswert der Daten zu beeinträchtigen. Und selbst wenn der Informationsgehalt eines elektronischen Dokuments geändert wird, ist diese Handlungsweise nur dann vom Tatbestand erfasst, wenn dadurch über die Identität des Ausstellers getäuscht wird.[1951]

1945 Vgl *Kienapfel/Schmoller,* StudB BT III² § 225a Rz 4 bzw § 223 Rz 11 ff.

1946 Das heißt, wenn es sich um einen unwahren Inhalt des elektronischen Dokuments handelt. Ein E-Mail als elektronisches Dokument kann daher echt sein (wenn der tatsächliche Aussteller es selbst auch unter seiner Identität versendet), aber einen unwahren Inhalt haben (zB wenn er im E-Mail angibt der Geschäftsführer eines Unternehmens zu sein, obwohl er es nicht ist).

1947 Siehe dazu zB *Kienapfel/Schmoller,* StudB BT III² § 225a Rz 4; *Hinterhofer/Rosbaud,* Strafrecht. Besonderer Teil II⁵ §§ 169 – 321 StGB (2012) § 225a Rz 1.

1948 AA wohl *Thiele* in SbgK § 225a Rz 27, der bereits das Hinzufügen eines bloßen Leerzeichens in einen Speicherplatz als »falsches Datum« erfasst wissen will.

1949 Siehe dazu bereits S 60 ff.

1950 Als Beispiel könnte daran gedacht werden, dass jemand einem E-Mail lediglich ein neues Zeichen zB ein Leerzeichen an einer unbeachtlichen Stelle hinzufügt, ohne aber den Hinweis auf den konkreten Aussteller zu manipulieren; aA offensichtlich *Thiele* in SbgK § 225a Rz 27.

1951 Im Gegensatz dazu stellt etwa Art 7 CCC nicht auf eine solche Anforderung ab. In ER (ETS 185) Pkt 82 heißt es dazu: »It should be noted that national concepts of forgery vary greatly. One concept is based on the authenticity as to the author of the document, and others are based on the truthfulness of the statement contained in the document. However, it was agreed that the deception as to authenticity

Die Begehungsweise des »Eingebens« kann konventionskonform und teleologisch betrachtet nur in Bezug auf Computerdaten und in Form einer informationstechnischen »Input-Handlung« verstanden werden, selbst wenn die Daten, die zur Eingabe bestimmt sind, noch nicht in einer unmittelbar von einem Computersystem verarbeitbaren Form vorliegen. Wesentlich ist somit die Übertragung von Daten der »analogen Welt in die digitale« bzw die Weiterverwendung von bereits computertechnisch aufbereiteten Daten. So können neue Daten über spezielle Eingabegeräte, wie Tastatur, Maus, Scanner usw ebenso eingegeben werden, wie durch das Einlesen von Daten von internen und externen Datenträgern oder anderer Computersysteme zB über ein Netzwerk. Ein solcher deliktsspezifischer Dateninput muss allerdings dazu führen, dass auch die Information (Inhalt) eines zu schützenden »elektronischen Dokuments« verändert wird, dies entweder durch Fälschung oder Verfälschung im oben genannten Sinn. Scannt der Täter bspw einen gültigen Reisepass einer anderen Person ein und transformiert diesen dadurch in eine elektronische Kopie dieses Reisepasses, so handelt es sich selbst dann nicht um eine Computerdatenverfälschung, wenn er das Foto der digitalisierten Reisepasskopie durch ein digitales Passfoto, das seine Person zeigt, ersetzt. Es muss sich nämlich – wie auch bei § 223 – um die originäre Erklärung des Ausstellerwillens handeln, die nach ihrem Gegenstand und aufgrund der Erkennbarkeit des Ausstellers unmittelbare Rechtswirkungen entfaltet. Da es (derzeit) keinen amtlichen elektronischen Reisepass gibt, wird bei bloßer Manipulation einer eingescannten Kopie, kein elektronisches Dokument mit Quasi-Urkundencharakter hergestellt oder verfälscht.

Darüber hinaus ist auch ein davon angefertigter Ausdruck dieser manipulierten Kopie auf Papier, keine Urkunde iSd § 223[1952]. Es handelt sich lediglich um ein Objekt, das zwar prinzipiell mit beweiserheblichen Daten erzeugt wurde, selbst aber keine Urkundenqualität besitzt und daher nur eine Reproduktion der Erklärung ist. Bei Erklärungen in Form von Computerdaten liegt immer dann eine bloße Reproduktion der Erklärung vor, wenn sich aus der digitalen Kopie darauf schlie-

---

refers at minimum to the issuer of the data, regardless of the correctness or veracity of the contents of the data. Parties may go further and include under the term ›authentic‹ the genuineness of the data.«

1952 Nach hM kommt nur beglaubigten (Papier-)Kopien Urkundencharakter zu; vgl OGH 28.01.1993, 12 Os 128/92; *Kienapfel/Schroll* in WK² § 223 Rz 22; *Fabrizy,* StGB¹¹ § 74 Rz 16 mwN.

ßen lässt, dass es sich dabei nicht um die originäre Erklärung handeln kann (wie im Beispiel des eingescannten Reisepasses). Anders ist dies allerdings zu beurteilen, wenn die digitalen Daten selbst den Anschein erwecken, die Originalerklärung zu sein (zB ein manipuliertes E-Mail im Fall des Phishing).

Für die Begehungsweisen des Veränderns, Löschens oder Unterdrückens von Daten kann auf die Ausführungen zu §§ 126a bzw 148a verwiesen werden.[1953]

C. Subjektive Tatseite

Auf der subjektiven Seite muss der Täter neben dem Tatbildvorsatz mit dem erweiterten Vorsatz – jeweils im Mindeststärkegrad eines dolus eventualis – handeln, dass diese falschen bzw verfälschten Daten – von wem auch immer – im Rechtsverkehr zum Beweis eines Rechts, eines Rechtsverhältnisses oder einer Tatsache gebraucht werden.[1954]

Es liegt in Anbetracht der überschießenden Innentendenz ein kupiertes Erfolgsdelikt vor, da das Endziel des Täters, dass die Datenfälschungen im Rechtsverkehr tatsächlich gebraucht werden[1955], objektiv nicht (mehr) tatbestandlich ist.[1956] Es handelt sich somit um einen rein (subjektiv) anvisierten Erfolg des Täters, der außerhalb des Tatbildes liegt.

In concreto will der Täter durch das Imitieren eines anderen Herstellers bzw Versenders ein bestehendes Rechtsverhältnis mit dem Empfänger bzw Webnutzer vortäuschen. Das Opfer, das sich zB durch die falschen Daten im Glauben befindet, sein Bankinstitut benötige diverse Kontodaten zur ordnungsgemäßen Abwicklung des zugrunde liegenden Vertragsverhältnisses, wird veranlasst, die geforderten Daten preiszugeben. § 225a ist in diesem Fall anwendbar.

Ein wesentliches Kriterium für § 225a ist die Notwendigkeit, dass es dem Täter darum gehen muss, die falschen oder verfälschten Daten gegenüber einem Menschen – und nicht gegenüber einer Maschine –

1953 Siehe oben.
1954 Vgl dazu auch ErlStV 1645 BlgNR XXIV. GP, 5.
1955 Es reicht auch aus, dass der Täter den Gebrauch im Rechtsverkehr durch einen anderen in seinen Vorsatz aufgenommen hat.
1956 Eine solche Einordnung wirkt sich ua ggf auf eine strafbare Beteiligung aus.

verwenden zu wollen. Die bloße Verwendung der manipulierten Daten, um eine Maschine zu beeinträchtigen, reicht nicht aus.[1957]

Aus diesem Grund ist auch das Skimming nicht unter § 225a zu subsumieren. Beim Skimming wird vom Täter meist an Bankomaten unbemerkt ein Lesegerät angebracht, das die Daten auf dem Magnetstreifen der Zahlungskarte ausliest und speichert. Die Magnetstreifenkarte im ID-1-Format[1958] kann drei Spuren enthalten, die jeweils mit Datenformaten nach speziellen Zeichensätzen beschrieben werden können.[1959] Zumeist wird nur auf die ersten beiden Spuren fokussiert, die ua die Kontoinformation und Bankkennung zur Authentifizierung enthält.[1960] Diese Daten werden in weiterer Folge auf einen Plastikkartenrohling (auch »White Plastic Card« genannt) übertragen. Der Täter täuscht nicht über die Identität des Ausstellers, denn er will die Karte gerade nicht gegenüber einem Menschen einsetzen.[1961] Der Magnetstreifen der Plastikkarte dient dem Täter lediglich als Trägerkörper des Datensatzes. Behebungen mit »White Plastic Card-Fälschungen« können mittlerweile aber nur mehr im europäischen Ausland in dieser Form an Geldausgabeautomaten durchgeführt werden.[1962]

In diesen Fällen käme aber zB auch § 126c Abs 1 Z 2 und §§ 241a ff in Betracht.

Der Konzeption des § 225a fehlt eine dem § 223 Abs 2 analoge Bestimmung, mit der die vorsätzliche tatsächliche Verwendung falscher oder verfälschter Daten zu den genannten Zwecken unter Strafe gestellt wird. Dies insb, wenn in den GMat zum Ausdruck gebracht wird, dass § 225a »vor allem im Bereich der elektronischen Urkunde und der elektronischen Signatur« Bedeutung erlangen werde.[1963] Es wird nicht immer der »Datenfälscher« selbst sein, der seine Falsifikate zum Einsatz bringt bzw es wird sich dieser nicht immer nachweisbar mit sei-

---

1957 Vgl *Reindl-Krauskopf,* Computerstrafrecht², 67 f.

1958 Nach internationaler Norm »ISO 7810« für Identifikationskarten (vgl *Rankl/Effing,* Handbuch⁵, 32).

1959 Dazu auch *Rankl/Effing,* Handbuch⁵, 19.

1960 Die dritte Spur auf dem Magnetstreifen ist beschreibbar und für variable Daten vorgesehen, wie etwa für die Anzahl der Fehlversuche oder Kartenlimits (vgl generell zu Magnetstreifenkarten *Schmeh,* Elektronische Ausweisdokumente. Grundlagen und Praxisbeispiele [2009] 48).

1961 Vgl hins »White Plastic Card-Fälschungen« auch *Reindl-Krauskopf,* Computerstrafrecht², 68; weiters *Reindl,* E-Commerce, 123 f.

1962 Siehe oben S 340 ff.

1963 ErlRV 1166 BlgNR XXI. GP, 30 f.

nen Datenfalsifikaten in Verbindung bringen lassen.[1964] Deshalb wäre die Einführung eines »Abs 2« analog zu § 223 Abs 2 sinnvoll. Stellt man sich in diesem Zusammenhang den Fall vor, in dem der Fälscher die Daten einem in den Tatplan eingeweihten Dritten übermittelt, damit dieser die gefälschten Daten im Rechtsverkehr verwendet, was dieser schließlich auch tut, so tritt genau das ein was § 225a in einem Vorstadium verhindern will, nämlich die Verwendung solcher Fälschungen im Rechtsverkehr. Dennoch ist der tatsächliche unmittelbare Verwender grundsätzlich[1965] nicht nach § 225a zu bestrafen, selbst wenn er bereits von Beginn an als bloßer Mitwisser[1966] in das Vorhaben des Fälschers eingebunden war.

Der Strafaufhebungsgrund der Tätigen Reue nach § 226 Abs 1 und 2 kann expressis verbis auch für die Datenfälschung nach § 225a ins Treffen geführt werden.

§ 225a ist ein Offizialdelikt. Es fällt gem § 30 Abs 1 StPO in die sachliche Zuständigkeit des Bezirksgerichts.

Stellt der Täter bspw im Wege des Phishing oder Pharming ein E-Mail bzw eine Website her, die über die Identität des Versenders bzw Ausstellers täuscht, sodass der Anschein erweckt wird, sie stamme von einem anderen (zB seriösen oder vertrauten) Absender, ist der objektive Tatbestand erfüllt.

Beim Herstellen einer Phishing-E-Mail etwa, die die Empfänger dazu verleiten soll, Zugangsdaten preiszugeben, kann der Täter entweder durch die Herstellung neuer Daten Daten »fälschen« oder aber bereits bestehende Daten (zB E-Mail oder Website) durch diverse manipulative Datenverwendungshandlungen »verfälschen«.

1964 Siehe *Bergauer/Schmölzer* in Jahnel/Mader/Staudegger, IT-Recht[3], 635 (671).

1965 Ausgenommen man geht – wie auch der OGH – von einer strafbaren Beteiligung bis zur materiellen Beendigung der Tat aus (siehe oben). Selbst die Unterlassung der Verhinderung einer mit Strafe bedrohten Handlung gem § 286 Abs 1 würde für den Verwender nicht in Frage kommen, weil § 225a lediglich eine Strafdrohung von bis zu einem Jahr Freiheitsstrafe vorsieht, was aber ein Teil der objektiven Bedingung der Strafbarkeit im Tatbestand des § 286 Abs 1 zwingend vorsieht.

1966 Lässt sich dem Verwender allerdings ein kausaler – zumindest psychischer – Tatbeitrag zur Datenfälschung nachweisen, wäre in diesem Beispielsfall eine Strafbarkeit nach §§ 12 Fall 3, 225a möglich.

D. Vertiefte Untersuchung des Phänomens »Phishing« anhand § 108 StGB iVm dem Grundrecht auf Datenschutz

Das Kunstwort »Phishing« steht mittlerweile als abstrakter Überbegriff für Handlungen, mit denen versucht wird durch Selbstschädigung der Opfer an Zugangs- oder Kontodaten der Betroffenen zu gelangen.[1967]

1. Exkurs: »Phishing« und »Pharming«

Der Begriff »Phishing« setzt sich zusammen aus den Wörtern »Password« und »Fishing«, da die Täter schlicht und einfach über listige Aktionen nach »Passwörtern« von Internetnutzern »angeln«.[1968]

Auch das sog »Pharming« (»Password harvesting farming« bzw auch »Password harvesting fishing«) ist inhaltlich eng an das Phishing angelehnt. Die Opfer werden dabei durch DNS[1969]-Manipulation auf gefälschte Websites geleitet, die bspw dem Erscheinungsbild bekannter Bankinstitute entsprechen. Das Opfer wird in weiterer Folge dazu verleitet, seine Zugangs- und Kontodaten über ein Online-Formular bekannt zu geben.

So wie diese Kunstwörter aus dem Hacker-Jargon (deren Etymologie weitgehend ungeklärt und zum Teil strittig ist)[1970] selbst oft in Hacker-Kreisen mit unterschiedlichen Bedeutungen versehen werden, tauchen auch in der juristischen Fachliteratur differierende Bezeichnungen und Definitionen der zu Grunde liegenden modi operandi auf. Im Folgenden sollen die wesentlichsten Methoden kurz unter einer aussagekräftigen Bezeichnung dargestellt werden, um eine abgeklärte Grundlage für die weitere Befassung zu bieten.

1967 Vgl dazu auch den Begriff »Computer Based Social Engineering«.

1968 Siehe etwa *Schuh,* Computerstrafrecht, 230 ff; weiters *Malek/Popp,* Strafsachen im Internet² (2014) 67; etwas differenzierter *Gercke/Brunst,* Internetstrafrecht, 117 mwN; siehe zur Begrifflichkeit auch *Seifert,* Guide, 265.

1969 »Domain Name System«; DNS ist zuständig für die Auflösung von Internet-Adressen bzw Domains zu IP-Adressen. Bekannte Methoden sind das DNS-Cache-Poisoning oder das Manipulieren der lokalen »hosts«-Datei durch Trojanische Pferde.

1970 Vgl etwa *Gercke/Brunst,* Internetstrafrecht, 117; *Schuh,* Computerstrafrecht, 230; *Bergauer,* RZ 2006, 82; *Bergauer* in Bergauer/Staudegger, Recht und IT, 109 (110).

a. Phishing per E-Mail[1971]

Beim »klassischen« Phishing via E-Mail werden E-Mails zB in sog »HTML[1972]-Formatierung« verfasst, deren graphische Darstellung dem offiziellen Erscheinungsbild eines seriösen Unternehmens nachgeahmt sind. Dabei werden unter anderem Firmenlogo, Farben, charakteristische Schriftzüge, Grafiken und insb die E-Mail-Adresse dieses Unternehmens nachgebildet. Die Textierung soll dem (gezielt ausgewählten[1973]) Empfänger einen vertrauenserweckenden Eindruck vermitteln und diesen zu einer bestimmten Interaktion verleiten.[1974]

Als trivial angesehen und leicht zu bewerkstelligen gelten dabei E-Mails, deren Absender-Adresse gefälscht und deren Antwort-Funktionalität an eine funktionstüchtige E-Mail-Adresse des Täters adressiert ist, die jedoch dem Empfänger auf den ersten Blick verborgen bleibt. Die tatsächliche Antwort-Adresse findet sich nicht im Body-Teil eines E-Mails, der den eigentlichen Nachrichtentext enthält, sondern im Header, der die Meta-Informationen über die E-Mail-Übertragung beinhaltet (zB Absender- und Empfänger-Adresse). Ein etwas versierterer User könnte über das verwendete E-Mail-Programm Einsicht in die Header-Informationen nehmen und den angegebenen »Return-Path« herauslesen. Antwortet der Adressat auf die Nachricht über die im E-Mail-Client vorhandene Funktion, so wird die Antwort nicht an die angezeigte Absender-Adresse (ggf die echte E-Mail-Adresse eines Bankinstituts), sondern an die mitgelieferte Antwort-Adresse des Täters geschickt.

Tatsächlich leistet auch das Simple Mail Transfer Protocol (SMTP)[1975], das grundsätzlich nur für den E-Mail-Verkehr zwischen Mail-Servern konzipiert wurde, dem Täter hilfreiche Dienste, da es per se beim Verbindungsaufbau zwischen SMTP-Client und SMTP-Server keine Client-Authentifizierung vornimmt. Das bedeutet, dass prinzipiell auch keine Überprüfung der verwendeten und im E-Mail ausge-

---

1971 Siehe zur Darstellung der unterschiedlichen Methoden auch *Bergauer* in Bergauer/Staudegger, Recht und IT, 109 (111 ff); weiters auch *Mader,* Neues zum Online Banking, in Bergauer/Staudegger (Hrsg), Recht und IT. Zehn Studien (2009) 67 (73 f und 76 ff).

1972 Hypertext markup language.

1973 Auch »Spear-Phishing« genannt (vgl *Seifert,* Guide, 265).

1974 Siehe auch *Kersken,* IT-Handbuch[5], 1067 f.

1975 In diesem Zusammenhang ist auch das »Extended SMTP« (ESMTP) zu nennen, das eine erweiterte 8-Bit-Version des ursprünglichen SMTPs darstellt.

wiesenen Absenderinformationen erfolgt. Dadurch kann ein beliebiger Absender beim Versand eines E-Mails – zB um eine andere Identität vorzutäuschen (sog »Mail-Spoofing«) – angegeben werden. SMTP beruht auf der standardisierten »TCP/IP«[1976]-Kommunikation und regelt die Weitergabe eines E-Mails von einem Rechner im Internet zu einem anderen. Dabei muss auch für den E-Mail-Dienst – gemäß der Spezifikation des TCP – ein Kommunikationskanal, in concreto über den Port 25, bereitgestellt werden.[1977] TCP-Port 25 ist ein sog »Well-known«-Port, was bedeutet, dass gewisse Portnummern grundsätzlich für bestimmte Dienste reserviert sind. Dies ist jedoch nicht zwingend, sodass ein Administrator bzw Programmierer seinen Diensten bzw Programmen Portnummern zwischen 0 – 65.535 völlig frei zuweisen kann.[1978] Aufbauend auf den TCP/IP-Stack wird dann das in IP-Pakete zerlegte E-Mail über das Internet vom Mail-Ausgangsserver des Absenders zum Mail-Eingangsserver des Empfängers weitergeleitet. Der User, der die Nachricht verfasst, kommuniziert zuvor ebenso in einer eigenen TCP/IP-Session, jedoch als SMTP-Client mit zB dem Mail-Ausgangsserver (SMTP-Server) seines Internet Service Providers (ISP).

Die SMTP-Kommunikation selbst erfolgt prinzipiell über sog »Message Transfer Agents« (MTAs)[1979] im (ASCII[1980]-codierten) Klartext, weshalb man auch eine Nachricht »manuell« über ein simples Terminalprogramm (wie »Telnet«), das über die Eingabeaufforderung des Befehlsinterpreters in Windows-Betriebssystemen verfügbar ist, versenden kann.

In weiterer Folge wird nun die abgeschickte Nachricht vom Mail-Ausgangsserver des Urhebers über das Internet weitergeleitet, damit die Daten beim Mail-Eingangsserver des Empfängers (SMTP-Server) entgegengenommen werden können.

b. Phishing per »Abbruchtrojaner«

Trojanische Pferde sind Computerprogramme, die möglichst unbemerkt in fremde Computersysteme eingeschleust werden, um dort

1976 Transmission control protocol/internet protocol.
1977 Siehe *Kersken,* IT-Handbuch[5], 262; weiters *Gumm/Sommer,* Informatik[10], 655.
1978 Vgl *Gumm/Sommer,* Informatik[10], 640.
1979 Vgl *Halsall,* Computer Networking and the Internet[5] (2005) 527.
1980 »American Standard Code for Information Interchange«.

bestimmte Tätigkeiten zu verrichten.[1981] Ein Abbruchtrojaner ist eine Mischform aus »Keylogger«, der Tastaturanschläge des Opfers heimlich aufzeichnet und seinem Programmierer übermittelt, und »Browser-Hijacker«, der den vom Opfer verwendeten Internetbrowser auf fremde Websites »entführt«. Konkret wird eine aufrechte Online-Banking-Verbindung nach Eingabe der Zugangsdaten und einer Transaktionsnummer[1982] (TAN) durch den Trojaner abgebrochen und eine fingierte Fehlermeldung angezeigt, die das Opfer darauf hinweist, dass zB diese TAN bereits verwendet wurde und sämtliche Daten erneut eingegeben und mit einer neuen TAN bestätigt werden müssten. Inzwischen wurden die Daten der ersten Eingabe bereits über das Internet dem Täter übermittelt, der nunmehr sämtliche Zugangsdaten und eine noch funktionierende TAN des Opfers besitzt.

c. Pharming mittels Deep-linking bzw Framing

Bei dieser Methode werden in einem E-Mail »offizielle« Hyperlinks, die vermeintlich auf die tatsächliche Website des Unternehmens verweisen, angezeigt, um den offiziellen Charakter zu betonen. Hinter der vertrauenerweckenden Beschreibung dieses Links verbirgt sich jedoch ein Verweis auf eine ganz andere – vom Täter betriebene – Webpage, die per »Framing«-Technik zusammen mit originalen Webframes der Bank in eine gemeinsame Website eingebettet und dadurch in den Darstellungsaufbau des Internetbrowsers vollständig integriert wird.[1983] Selbst die Internetadresse der vom Täter betriebenen Website ähnelt in ihrer Notation sehr dem Original. Auch kann die Adressleiste des Browsers, um der Überzeugungskraft Nachdruck zu verleihen, gänzlich unterdrückt bzw durch technische Scripts (wie zB Java-Scripts) manipuliert werden. Der getäuschte User bekommt dann über ein Webformular die Aufforderung, bestimmte Daten einzutragen und abzusenden.

1981 Siehe oben S 89 ff.

1982 Es handelt sich dabei um sog »Einmalpasswörter«.

1983 Vgl auch OGH 17.12.2002, 4 Ob 248/02b = MR 2003, 33 *(Stomper)* = RdW 2003/298, 365 *(Handig)* = ecolex 2003/112, 254 *(Tonninger)* = MR 2003, 35 *(Krüger)*.

d. Pharming mittels Trojaner

Im Fall des Pharming können die Täter mit Hilfe von Trojanischen Pferden lokale Dateien manipulieren, um den Internetbrowser trotz Eingabe der tatsächlichen und exakten Internetadresse der Bank auf gefälschte Websites zu »entführen« (sog »Hijacker«). Das Opfer kann anhand der Adressleiste des Browsers nicht erkennen, dass er sich nicht auf dem offiziellen Server der Bank befindet. In den meisten dieser Fälle wird die lokale »hosts«-Datei in einfacher Weise verändert, sodass die IP-Adresse des Täter-Servers neben einer vertrauten Domainangabe in eine Textzeile geschrieben wird (zB 123.123.123.123 <www.xybank.at).> Die Kommunikation im Internet erfolgt prinzipiell ausschließlich auf Grundlage von IP-Adressen, weshalb Domainnamen stets in IP-Adressen übersetzt werden müssen. Der Browser sieht vor einem Verbindungsaufbau zuerst in dieser lokalen Datei nach, ob es dort eine bestimmte Zuordnung für die Namensauflösung der eingegebenen Adresse gibt, bevor weitere technische Protokolle die Übersetzungsnachfrage an vorgesehene DNS[1984]-Server weiterreichen.

e. Pharming mittels DNS-Cache-Poisoning[1985]

Auch DNS-Server können für Pharming-Angriffe sabotiert werden. Dazu führt der Täter einen Testaufruf einer Domain über den zu manipulierenden DNS-Server durch und beantwortet selbst die Anfrage des Servers an einen übergeordneten DNS-Server mit falschen DNS-Informationen. Der DNS-Server legt diese Informationen in einem Pufferspeicher ab. Gibt ein diesem DNS-Server zugeteilter Nutzer die Internetadresse ein, so teilt der Server seine im Puffer gespeicherte Namensauflösung dieser Anfrage mit. Das Opfer wird in weiterer Folge auf den Server des Täters geleitet. Bei dieser Methode ist kein Zugriff auf das Computersystem des eigentlichen Opfers notwendig.

Prinzipiell geht es bei allen einschlägigen Methoden um die Erlangung von Passwörtern oder Zugangsdaten über informationstechnische Systeme, wie dem Internet.

1984 Das DNS (Domain Name System) ist zuständig für die Namensauflösung von Internet-Adressen bzw Domains zu IP-Adressen (DNS-Resolution).

1985 Siehe dazu *Borges/Schwenk/Stuckenberg/Wegener,* Identitätsdiebstahl, 88 ff.

Die Opfer sollen durch das Vortäuschen von Tatsachen dazu gebracht werden, ihre Zugangsdaten dem Täter preiszugeben. Für die Realisierung dieses Zwecks werden zB – wie oben beschrieben – Websites gefälscht oder E-Mails an Empfänger versendet, deren Aussehen und Inhalt der offiziellen Aufmachung von seriösen und bekannten Bankinstituten, Behörden oder Ähnlichem nachgebildet sind. Im Vertrauen auf die Echtheit der Nachricht und des Absenders übermittelt der Getäuschte freiwillig Zugangsdaten an die vermeintliche Bank, wobei in Wirklichkeit diese Daten dem Täter zufließen.

Im Anschluss daran werden die Daten vom Täter benutzt, um unter der Identität des Phishing-Opfers, Online-Abbuchungen von dessen Konto bzw Online-Einkäufe mit der Kreditkarte des Getäuschten zu tätigen oder auch »Face-to-Face« Transaktionen mit einem Bankangestellten abzuwickeln. Um die geplanten Kontotransaktionen noch vor der Aufdeckung der Phishing-Aktionen und Einleitung von Gegenmaßnahmen durch ein Phishing-Opfer bzw in weiterer Folge durch die Bank durchführen zu können, ist eine rasche Verwertung der so erhaltenen Daten »notwendig«.

(Exkurs Ende)

2. Strafrechtliche Beurteilung der Phishing Phase

Der erste Sachverhaltsabschnitts (hier als Phishing-Phase bezeichnet) beruht im Wesentlichen auf einer Täuschung über Tatsachen, die das Opfer veranlassen soll, selbst seine Zugangsdaten gegenüber dem Täter preiszugeben. Der Betrug (§ 146) scheidet in der Phishing-Phase aus folgenden Gründen aus: 1.) die Daten sind keine selbstständigen Wertträger; 2.) es fehlt an der Unmittelbarkeit des Vermögensschadens; 3.) der Getäuschte schädigt sich nicht selbst, dies erfolgt vielmehr durch den Täter, indem er die Daten entsprechend verwertet.[1986] In den Fällen, in denen der Täter das Opfer dazu verleitet selbst unmittelbar eine Vermögensverfügung zu tätigen[1987], sind grundsätzlich die Bestimmungen bezüglich des Betrugs §§ 146 ff zu untersuchen.

1986 Vgl auch bereits grundlegend *Bergauer,* RZ 2006, 82; weiters *Bergauer* in BMJ, 35. Ottensteiner Fortbildungsseminar, 27 (28 ff).

1987 ZB könnte das Opfer mittels eines gefälschten E-Mails dazu verleitet werden, direkt Geld auf das Konto des Täters zu überweisen.

Vorauszuschicken ist, dass eines der massivsten Probleme der Strafrechtspraxis darin besteht, dass die Phishing-Täter überwiegend vom Ausland aus agieren und aufgrund der zahlreichen Verschleierungsmöglichkeiten im Internet kaum ausgeforscht werden können. Eine Strafverfolgung ist somit – wenn überhaupt – nur sehr schwer möglich. IdR werden Verfahren, welche sich gegen unbekannte, nicht ausforschbare Täter richten, von der StA gem § 197 StPO abgebrochen.

Zur Tatbestandsmäßigkeit des Fälschens bzw Verfälschens von Daten (hier: E-Mail, das über den Aussteller täuscht) gem § 225a ist auf die obigen Ausführungen[1988] bzw auf *Bergauer*[1989] zu verweisen. Auch was das Sich-Verschaffen von Zugangsdaten iSd Vorbereitungsdelikts nach § 126c Abs 1 Z 2 betrifft, kann im entsprechenden Kapitel nachgelesen werden.[1990] In beiden Fällen ist grundsätzlich die Tatbestandsmäßigkeit zu bejahen.[1991]

An dieser Stelle soll einer etwaigen Strafbarkeit nach § 108 (Täuschung) iVm dem Grundrecht auf Geheimhaltung personenbezogener Daten gem (§ 1 Abs 1 DSG 2000) besondere Beachtung geschenkt werden.

a. § 108 StGB iVm § 1 Abs 1 DSG 2000

Wie bereits ausf erörtert, ist die Strafbestimmung der Täuschung (§ 108 Abs 1) mit der des Betrugs (§ 146) verwandt.[1992] Anders als beim Betrug wird der Getäuschte durch die Täuschungshandlung des Täters nicht zu einer schädigenden Vermögensverfügung, sondern zu einer Handlung, Duldung oder Unterlassung verleitet, die einen Schaden in jemandes Recht herbeiführt. Auf der subjektiven Seite wird Tatbildvorsatz in der gesteigerten Form der Absicht iSd § 5 Abs 2 verlangt, eine überschießende Innentendenz ist nicht gefordert.

Sehr umstritten ist jedoch, welche Rechte als Tatobjekt des § 108 in Frage kommen.

1988 Siehe oben S 398 ff.
1989 Vgl *Bergauer,* RZ 2006, 82; weiters *Bergauer* in BMJ, 35. Ottensteiner Fortbildungsseminar, 27 (32 f).
1990 Siehe S 333 ff.
1991 Vgl *Bergauer,* RZ 2006, 82.
1992 Siehe dazu S 369 ff.

b. Die umstrittene Täuschungsbestimmung des § 108

Wie bereits ausgeführt, spricht sich – entgegen vieler Lehrmeinungen – der OGH für eine weite Auslegung der tatbildlichen »Rechte« aus, wobei er grundsätzlich jedes konkrete (Individual-)Recht als darunter subsumierbar erachtet.[1993] Bedenken gegen die Verfassungsmäßigkeit dieser Strafbestimmung hat der Gerichtshof nicht.[1994] Darüber hinaus ist dem Verbot, Rechtsvorschriften von vornherein ihren normativen Gehalt abzusprechen und dem Gesetzgeber zu unterstellen, überflüssige oder inhaltslose Normen zu schaffen, folgend, die Suche eines konkreten Anwendungsbereichs indiziert, welche mE im hier interessierenden Zusammenhang in § 1 Abs 1 DSG 2000 einen Erfolg verbuchen kann.[1995]

§ 108 Abs 1, dessen hauptsächlicher Zweck dem Schutz der Autonomie der Person und der Willensbildungsfreiheit[1996] dient, was ua aus der systematischen Einordnung dieser Bestimmung unter die Freiheitsdelikte hervorgeht, stellt – wie oben bereits ausgeführt – im Wesentlichen auf eine »Täuschungshandlung« zur Beeinträchtigung eines Individualrechts ab. Der historische Gesetzgeber wollte wohl mit dem Tatbild der Täuschung anstelle der Beeinträchtigung des Vermögens, die Schädigung an einem anderen Recht durch eine Täuschungshandlung erfasst wissen.[1997] Nicht zuletzt deshalb, weil in den Erl absichtliches Handeln (iSd § 5 Abs 2) für die Deliktsverwirklichung gefordert wird und ausdrücklich[1998] für verbleibende Fälle, die von speziellen Tatbildern typischer täuschungsbedingter Beeinträchtigungen wichtiger Rechtsgüter nicht erfasst werden, auf den Tatbestand der Täuschung verwiesen wird. Die täuschungsbedingte Beeinträchtigung der Willensbildungsfreiheit allein reicht aber für eine diesbezügliche Strafbarkeit noch nicht aus. Vielmehr muss aus ihr ein Schaden in jemandes Recht resultieren, weshalb das tatbestandliche Unrecht, neben dem

1993 Vgl OGH 22.05.1986, 12 Os 136/85.
1994 Siehe OGH 26.06.1986, 12 Os 69/86.
1995 Vgl in weiterer Folge auch *Bergauer* in BMJ, 35. Ottensteiner Fortbildungsseminar, 27 (32 f).
1996 Konkret ist in den ErlRV (1971) 30 BlgNR XIII. GP, 239 von der »Freiheit der Willensentscheidung« die Rede; vgl auch *Schmoller* in BMJ, Strafrechtliche Probleme der Gegenwart 1989, (1) 42.
1997 Vgl ErlRV 30 BlgNR XIII. GP, 239.
1998 Vgl ErlRV 30 BlgNR XIII. GP, 239.

überwiegenden Handlungsunwert, auch einen Erfolgsunwert verlangt. Der Erfolgsunwert spielt jedoch mE eine nur untergeordnete Rolle und dient lediglich der Grenzziehung von Täuschungshandlungen ohne konkrete rechtsrelevante Auswirkung für das Opfer (welche straflos bleiben sollen) auf der einen Seite und Täuschungshandlungen, mit einer solche rechteschädigenden Wirkung auf der anderen Seite. Darüber hinaus veranschaulicht dies generell auch die Versuchsstrafbarkeit bei Vorsatzdelikten (vgl § 15 Abs 1), die eben gerade bei Ausbleiben eines Erfolges einsetzen kann[1999] und quasi den (verbleibenden) »Handlungsunwert« der versuchten Tat für strafbar erklärt.[2000] Für den konkreten Schadenseintritt muss daher mE die bloße Feststellung einer (Individual-)Rechteverletzung genügen. Dies aber auch völlig unabhängig davon, ob weitere strafrechtliche Tatbestände oder (zivilrechtliche) Durchsetzungsmöglichkeiten diesbezüglich bestehen.

Eine andere Ansicht vertritt offenbar *Weiß,* der den Unrechtsgehalt durch die »unspezifizierte« und »nicht spezifizierbare« Täuschungshandlung nahezu ausschließlich am Schaden an irgendwelchen Rechten orientiert sieht.[2001] Doch diese Argumentation überzeugt schon deshalb nicht, weil in den GMat ausdrücklich von der Identität der Begehungsweisen bei den Delikten der Täuschung und des Betrugs gesprochen wird und gerade aus diesem Grund zur Vermeidung einer unterschiedlichen Auslegung der beiden Bestimmungen auch dieselbe Ausdrucksweise Verwendung findet. So zB expressis verbis »durch Täuschung über Tatsachen«.[2002] Zur »Täuschungshandlung« beim Betrug gibt es aber umfangreiche Konkretisierungen[2003], die in selber Art und Weise implizit auch für den Tatbestand des § 108 Abs 1 heranzuziehen sind. Von einer unspezifizierten oder gar unspezifizierbaren Täu-

1999 Ausgenommen ist hier der »absolut untaugliche Versuch« gem § 15 Abs 3.

2000 Dass bei einem Vorsatzdelikt mit Handlungs- und Erfolgsunwert tatsächlich bloß ein Versuch vorliegt, wirkt sich prinzipiell nur bei der Strafzumessung (mildernd) aus (vgl dazu § 34 Abs 1 Z 13). Dennoch rückt der Handlungsunwert in den Vordergrund, da es zwar einen Handlungsunwert ohne Erfolgsunwert gibt, nicht jedoch einen strafrechtlich relevanten Erfolgsunwert ohne Handlungsunwert (vgl *Fuchs,* AT I[8], Rz 10/15 f).

2001 Siehe *Weiß,* Kritische Betrachtung des Täuschungstatbestandes aus straf- und verfassungsrechtlicher Sicht – zugleich ein Beitrag zur Bestimmtheit von Strafnormen (Teil I), AnwBl 1989, 185.

2002 ErlRV 30 BlgNR XIII. GP, 239.

2003 Siehe stellvertretend für die umfangreiche Spezifikation der Täuschungshandlung beim Betrug bei *Kirchbacher* in WK² § 146 Rz 17 ff.

schungshandlung kann daher nicht bzw schon lange nicht mehr gesprochen werden.

Auch dass – wie *Weiß* hervorhebt – der Gesetzgeber die Beeinträchtigung der Willensbildungsfreiheit durch bloße Täuschung nicht genügen lassen wollte[2004], schadet der hier vertretenen Argumentation nicht.

Gerade in Anbetracht des Phishing bietet sich nämlich ein solches konkretes Individualrecht, das sich unproblematisch der Willensbildungsfreiheit und der »informationellen Selbstbestimmung« – also der Freiheit selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden[2005] – als »Freiheitsrechte« zuordnen lässt, als Tatobjekt der Täuschung geradezu an. Es handelt sich dabei um das »Grundrecht auf Datenschutz« iSd § 1 DSG 2000, das mit unmittelbarer Drittwirkung[2006] ausgestaltet ist. Genauer gesagt ist das zentrale »Grundrecht auf Geheimhaltung« personenbezogener Daten (§ 1 Abs 1 DSG 2000) als das relevante Individualrecht anzuführen.

c. Das Grundrecht auf Datenschutz nach § 1 Abs 1 DSG 2000

Es liegt auf der Hand, dass Verletzungen der Privatsphäre strafrechtlich nicht sonderlich umfassend und streng geschützt werden. Die Zurückhaltung des Gesetzgebers in dieser Angelegenheit manifestiert sich im Kernstrafrecht auch darin, dass die unter dem fünften Abschnitt mit »Verletzungen der Privatsphäre und bestimmter Berufsgeheimnisse« übertitelten Delikte (§§ 118 bis 124) überwiegend als Ermächtigungs- bzw Privatanklagedelikte ausgestaltet sind. Einzig die nebenstrafrechtliche Bestimmung des § 51 DSG 2000 wurde durch die DSG-Nov 2010[2007] durch Aufhebung des Abs 2 von einem Ermächtigungsdelikt[2008] zu einem reinen Offizialdelikt angehoben. Über die Konstellation des § 108

2004 Vgl *Weiß,* AnwBl 1989, 185.
2005 Vgl *Berka,* Datenschutz, 63.
2006 Siehe *Berka,* Verfassungsrecht[5], Rz 1265 und 1409; *Drobesch/Grosinger,* Das neue österreichische Datenschutzgesetz (2000) 102; *Jahnel* in FS Schäffer, 313 (337); *Jahnel,* Handbuch, Rz 2/70; *Duschanek/Rosenmayr-Klemenz,* Datenschutzgesetz 2000 (2000) 15; die Rsp zur Vorgängerbestimmung des § 1 Abs 6 DSG 1978 ua VfGH 12. 10. 1989, G 238/88.
2007 BGBl I 133/2009.
2008 Vgl noch die Fassung vor der DSG-Nov 2010.

iVm § 1 Abs 1 DSG 2000 lässt sich ein zusätzlicher (subsidiärer) Schutz der Privatsphäre in Hinblick auf täuschungsbedingte Schädigungen an schutzwürdigen personenbezogenen Daten erblicken.

Unter dem verfassungsgesetzlich gewährleisteten »Grundrecht auf Datenschutz« finden sich – wie oben angemerkt – tatsächlich vier subjektive Rechte, die in der Verfassungsbestimmung des § 1 DSG 2000[2009] normiert sind. Im Einzelnen handelt es sich dabei um das zentrale Grundrecht auf Geheimhaltung personenbezogener Daten (§ 1 Abs 1 DSG 2000), und die Rechte auf Auskunft (§ 1 Abs 3 Z 1 DSG 2000), Richtigstellung unrichtiger Daten (§ 1 Abs 3 Z 2 erster Fall DSG 2000) und auf Löschung unzulässiger Weise verarbeiteter Daten (§ 1 Abs 3 Z 2 zweiter Fall DSG 2000).[2010]

Das Grundrecht auf Datenschutz[2011] ist als bislang einziges Grundrecht mit »unmittelbarer Drittwirkung«[2012] ausgestaltet.[2013] Dies bedeutet, dass auch private Rechtssubjekte zur Geheimhaltung von personenbezogenen Daten verpflichtet sind.[2014] Diese unmittelbare Drittwirkung gilt freilich für alle unter der Überschrift »Grundrecht auf Datenschutz« in § 1 DSG 2000 normierten (Grund-)Rechte. Der Verfassungsgesetzgeber hat diese unmittelbare Drittwirkung ursprünglich durch die »Rechtswegklausel« des § 1 Abs 5 DSG 2000 verwirklicht.[2015] Mit der Verwaltungsgerichtsbarkeits-Nov 2012[2016] wurde allerdings § 1 Abs 5 DSG 2000 mit Wirkung zum 1.1.2014 aufgehoben und inhaltlich[2017] in § 5 Abs 4 DSG 2000 – im Rang eines einfachen Gesetzes – überstellt.

2009 BGBl I 165/1999.

2010 Die Rechte auf Auskunft, Richtigstellung und Löschung werden auch als »Begleitrechte«, »Betroffenenrechte« oder »Nebenrechte« bezeichnet (siehe *Jahnel,* Handbuch, Rz 2/3). *Duschanek* spricht von »Instrumenten zur besseren Verwirklichung der informationellen Selbstbestimmung« in *Duschanek,* Datenschutzrecht, in Holoubek/Potacs (Hrsg), Handbuch des öffentlichen Wirtschaftsrechts[2]. Bd 1 (2008) 299 (309).

2011 Mit dem abstrakten Begriff »Grundrecht auf Datenschutz« sind in weiterer Folge alle (Grund-)Rechte des § 1 DSG 2000 gemeint.

2012 Siehe bereits oben zum DSG 1978 S 42 f.

2013 Siehe ErlRV 2168 BlgNR XXIV. GP, 6; *Berka,* Verfassungsrecht[5], Rz 1265 und 1409; *Jahnel,* Handbuch, Rz 2/70; *Drobesch/Grosinger,* Datenschutzgesetz, 102; *Duschanek/Rosenmayr-Klemenz,* Datenschutzgesetz, 15; die Rsp zur Vorgängerbestimmung des § 1 Abs 6 DSG 1978 ua VfGH 12.10.1989, G 238/88.

2014 Vgl anstatt vieler *Berka,* Verfassungsrecht[5], Rz 1409.

2015 Vgl VfSlg 12.194/1989; siehe auch *Dohr/Pollirer/Weiss/Knyrim,* DSG[2] § 1 Anm 29.

2016 BGBl I 51/2012.

2017 BGBl I 51/2012; Lediglich der Begriff »Datenschutzkommission« wird durch den Begriff »Datenschutzbehörde« ersetzt.

Nach den Erl soll sich aber aus dieser Verschiebung hins des Inhalts und der Reichweite des Grundrechtes auf Datenschutz – insb was die unmittelbare Drittwirkung betrifft – nichts ändern, da sich diese aus § 1 Abs 1 DSG 2000 ergäbe.[2018] Leider wird aber in den GMat nicht klar genug begründet, wie sich tatsächlich diese unmittelbare Drittwirkung direkt aus § 1 Abs 1 DSG 2000 ableiten lässt.[2019]

Anzumerken ist, dass das Grundrecht auf Datenschutz bereits seit seiner Entstehung aufgrund seiner auffällig konkreten Formulierung kein Paradebeispiel für ein Grundrecht – mit hohem Abstraktionsgrad – darstellt. Die Begriffsinhalte sämtlicher Grundrechtstatbestandselemente des § 1 DSG 2000 erschließen sich aber auch hier nicht ausschließlich aus dem Wortlaut des Normtextes.

Grundrechtsträger der Verfassungsbestimmung in § 1 Abs 1 DSG 2000 ist »Jedermann«, weshalb das Grundrecht auf Datenschutz ein Menschenrecht darstellt, das unabhängig einer Staatsangehörigkeit, jedem Menschen zusteht.[2020] Neben dem Begriff »Jedermann« tritt in der Verfassungsbestimmung (§ 1 Abs 1 DSG 2000) auch der des »Betroffenen« auf, doch wird Letzterer erst in der einfachgesetzlichen Legaldefinition des § 4 Z 3 DSG 2000 näher determiniert. Beide Begriffe werden insgesamt synonym verwendet. § 4 Z 3 DSG 2000 bestimmt als Betroffenen jede vom Auftraggeber (§ 4 Z 4 DSG 2000) verschiedene natürliche oder juristische Person oder Personengemeinschaft, deren Daten verwendet (§ 4 Z 8 DSG 2000) werden. Die Definitionen des § 4 DSG 2000 beziehen sich aber expressis verbis auf die »folgenden Bestimmungen dieses Bundesgesetzes« und daher, dem Umkehrschluss folgend, nicht auf die Verfassungsbestimmung. Dies hat auch der VfGH[2021] in Bezug auf § 3 DSG 1978 idF DSG-Nov 1986[2022] festgestellt. Vor allem ist dabei anzumerken, dass in der Stammfassung des DSG 1978 der Einleitungssatz in § 3 ursprünglich noch »Im Sinne dieses Bundesgesetzes bedeuten:« lautete. Durch die Neufassung dieser Einleitung im Zuge der DSG-Nov 1986 in »Im Sinne der folgenden Bestimmungen dieses Bundesgesetzes bedeuten:«, hat der Novellierungsgesetzgeber geklärt, dass die einfachgesetzlichen Begriffsbestimmungen eben nicht auf

2018 Siehe ErlRV 2168 BlgNR XXIV. GP, 6.
2019 Siehe zu dieser Kritik auch *Jahnel,* Gesetzgebungsmonitor Datenschutz: Ministerialentwurf zu einer DSG-Novelle 2014, jusIT 2013/32, 58.
2020 Siehe *Jahnel* in FS Schäffer, 313 (315); weiters *Jahnel,* Handbuch, Rz 2/4.
2021 Siehe VfSlg 12.194/1989.
2022 BGBl 370/1986.

Art 1 und damit auch nicht auf § 1 DSG (zur Grundrechtsinterpretation) anzuwenden sind.

Somit stellt sich die Frage, ob für die Begriffsauslegung in Verfassungsbestimmungen ein Rückgriff auf einfachgesetzliche Definitionen überhaupt zulässig wäre. *Dohr/Pollirer/Weiss/Knyrim* vertreten dazu die Auffassung, dass die Legaldefinitionen des DSG für die Auslegung des Grundrechts nur bedingt tauglich seien. Sie begründen dies damit, dass es verfassungsdogmatisch bedenklich wäre, das Grundrecht durch einfachgesetzliche Vorschriften zu determinieren, sofern das Grundrecht keinen Ausführungsvorbehalt trifft. Dieser Ausführungsvorbehalt[2023] gelte zwar in concreto für die Grundrechte auf Auskunft, Richtigstellung und Löschung, nicht aber für das Recht auf Geheimhaltung.[2024]

Jahnel hingegen bejaht die Berücksichtigung der einfachgesetzlichen Legaldefinition zur Ermittlung des Inhalts des Grundrechts, indem er ausführt: »Wenn die Begriffsbestimmungen des § 4 über den Weg der Ausführungsbestimmungen zu § 1 Abs 3, nämlich § 26 (Auskunftsrecht) und § 27 (Recht auf Richtigstellung und Löschung) auf

---

2023 Besser wohl »Ausgestaltungsauftrag« (vgl *Jahnel,* Handbuch, Rz 2/32 mwN), denn dem einfachen Gesetzgeber obliegt es, die Betroffenenrechte bezüglich ihrer Reichweite und Durchsetzungsmodalitäten näher zu regeln. Diese Ausgestaltung muss § 1 Abs 4 DSG 2000 iVm § 1 Abs 2 DSG 2000 entsprechen.
Würde es sich tatsächlich – wie es der Wortlaut suggeriert – um einen Ausführungsvorbehalt, wie in Art 12 StGG (Versammlungs- und Vereinigungsfreiheit) handeln, wäre jeder Verstoß gegen das Ausführungsgesetz auch eine Grundrechtsverletzung. Die Konsequenz wäre, dass jede bescheidförmige Verletzung des einfachgesetzlichen Ausführungsgesetzes ausschließlich nach dem Bescheidbeschwerdeverfahren nach Art 144 B-VG vor dem VfGH geltend zu machen wäre (sog »Feinprüfungsgrundrecht«), es bestünde keine Zuständigkeit des VwGH (siehe etwa *Berka,* Verfassungsrecht[5], Rz 1060). Die einfachgesetzlichen Ausführungsregelungen zu den Betroffenenrechten fallen aber prinzipiell in die Prüfungskompetenz des VwGH, vgl auch § 40 Abs 2 DSG 2000. Eine auch vom VfGH zu prüfende Grundrechtsverletzung könnte aber etwa dann vorliegen, wenn einzelne Verfahrensregelungen zur Geltendmachung der Betroffenenrechte deren Ausübung einschränken würden (vgl *Lehner/Lachmayer,* Datenschutz im Verfassungsrecht, in Bauer/Reimer [Hrsg], Handbuch Datenschutzrecht [2009] 95 [109]). So sieht das auch der VfGH (VfSlg 12.194), wenn er ausführt: »Das Grundrecht auf Datenschutz wird zwar nicht durch jeden Fehler bei der Anwendung des DSG verletzt, doch können Verletzungen dieses Grundrechtes auch bei der Vollziehung dieses – das Grundrecht auf Datenschutz für den Bereich der automationsunterstützten Datenverarbeitung konkretisierenden – Gesetzes auftreten (vgl VfSlg. 11548/1987)«.

2024 Vgl *Dohr/Pollirer/Weiss/Knyrim,* DSG[2] § 1 Anm 6.

die verfassungsrechtliche Grundlage zurückwirken, so spricht bereits dies dafür, dass sie auch auf die Auslegung der – wortidenten – Begriffe des § 1 Abs 1, der nicht unter Ausführungsvorbehalt steht[2025], herangezogen werden können.«[2026] Andernfalls würde man – nach Ansicht *Jahnels* – dem Verfassungsgesetzgeber unterstellen, dass dieser dieselben Begriffe in verschiedenen Absätzen desselben Paragraphen nicht im selben Sinn verstanden wissen wollte.[2027] Als weiteres Indiz für die Orientierung des Verfassungsgesetzgebers an den einfachgesetzlichen Legaldefinitionen führt *Jahnel* schließlich an, dass der Gesetzgeber beide Teile des DSG 2000, also sowohl die Verfassungsbestimmungen als auch die einfachgesetzlichen Regelungen, gemeinsam beschlossen habe.[2028] In diesem Sinn sprechen sich bereits *Rill*[2029] und *Kotschy*[2030] für eine »gewisse Rückwirkung« der einfachgesetzlichen Bestimmungen auf das Grundrecht aufgrund der Gesetzgeberidentität aus. *Berka* hält fest, dass sich das Grundrecht auf Datenschutz und das einfachgesetzliche Datenschutzrecht wechselseitig bedingen und miteinander verknüpft seien. Das Grundrecht beziehe sich mit seiner Begrifflichkeit zum Teil auf das einfachgesetzliche Datenschutzrecht, sodass das einfache Recht für die Auslegung des Grundrechts mit herangezogenen werden müsse.[2031]

Gravierend erscheint hier jedenfalls, dass, würde man den Rückgriff auf einfachgesetzliche Vorschriften zur Interpretation von Verfassungsbestimmungen zulassen, dem (einfachen) Gesetzgeber im Wege der in seiner Verantwortung stehenden einfachen Gesetzgebung die Möglichkeit offen stünde, Grundrechte – die unter keinem Ausführungsvorbehalt stehen – inhaltlich dadurch mittelbar beliebig einzuschränken. Die das Grundrecht auf Datenschutz konstituierenden ver-

2025 § 1 Abs 1 DSG 2000 wird daher unmittelbar durch die Verfassung gewährleistet.
2026 Im Folgenden *Jahnel,* Handbuch, Rz 1/57 ff.
2027 Siehe *Jahnel,* Handbuch, Rz 1/58; vgl auch *Fercher,* Manuelle Dateien im Datenschutzgesetz 2000 in Jahnel/Siegwart/Fercher (Hrsg), Aktuelle Fragen des Datenschutzrechts (2007) 33 (41 f).
2028 Vgl *Jahnel,* Handbuch, Rz 1/58; vgl dazu auch *Lienbacher,* Datenschutzrecht und Staatsorganisation, in Österreichischer Juristentag (Hrsg), Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit. Referate und Diskussionsbeiträge (2012) 17 (23) unter Verweis auf die ständige Rsp des VfGH.
2029 Siehe *Rill,* Das Grundrecht auf Datenschutz, in Duschanek (Hrsg), Datenschutz in der Wirtschaft (1981) 15 (17).
2030 Siehe *Kotschy* in Matzka (Hrsg), Datenschutzrecht für die Praxis. Kommentar (3. Lfg 1988) § 3 K 1.
2031 Vgl *Berka,* Datenschutz, 29.

fassungsgesetzlich gewährleisteten Rechte – in concreto das Recht auf Geheimhaltung des § 1 Abs 1 DSG 2000, das eben nicht unter Ausführungsvorbehalt steht und von der Verfassung selbst wirksam garantiert wird, könnte dadurch durch den einfachen Gesetzgeber inhaltlich umorientiert werden.

Beispielsweise könnte eine Einschränkung der (einfachgesetzlichen) Legaldefinition des »Betroffenen« (§ 4 Z 3 DSG 2000) lediglich auf natürliche Personen (und nicht auch auf juristische) über den einfachen Gesetzgeber realisiert werden, wodurch sich das Geheimhaltungsrecht des § 1 Abs 1 DSG 2000 massiv einschränken ließe. Dies ist nicht ganz undenkbar, da die Grundrechtsberechtigung juristischer Personen ohnedies nicht selbstverständlich ist und sich auch sinnvollerweise nur auf all jene Grundrechte beschränkt, die »ihrem Wesen nach« juristischen Personen zustehen können, was in erster Linie bedeutet, dass es sich um Grundrechte handeln muss, in denen juristische Personen überhaupt verletzt werden können.[2032] Die Einschränkung des Grundrechts ausschließlich auf natürliche Personen wurde sogar im Ministerialentwurf der DSG-Nov 2008[2033] vorgeschlagen, wobei dort die Abänderung in Form der ausdrücklichen Normierung der Wortfolge »Jede natürliche Person hat Anspruch [...]« in der Verfassungsbestimmung des § 1 Abs 1 DSG 2000 selbst erfolgen sollte. Begründet wurde dies in erster Linie mit der Datenschutz-RL, die lediglich den Datenschutz natürlicher Personen regelt.[2034] Dabei ist anzumerken, dass in ErwG 24 ausgeführt wird, dass die Datenschutz-RL nicht die Rechtsvorschriften zum Schutz juristischer Personen bei der Verarbeitung von Daten, die sich auf sie beziehen, berührt. Daneben ergibt sich aus den ErwG 9 und 10, dass die Mitgliedstaaten nicht gehindert sind, einen bereits bestehenden, über den Anwendungsbereich der Datenschutz-RL hinausgehenden Rechtsschutz zu gewähren. Daher kann man davon ausgehen, dass für die Mitgliedstaaten zumindest die Möglichkeit offen bleibt, einen Schutz für juristische Personen einzuräumen. Weiters ließe sich wohl nur schwer argumentieren, dass Daten von juristischen Personen einer den natürlichen Personen vergleichbaren Schutzwürdigkeit unterliegen. Auch habe – laut GMat – die Praxis gezeigt, dass sich der Datenschutz juristischer Personen im

2032 Siehe *Berka,* Verfassungsrecht[5], Rz 1238 ff mwN.
2033 182/ME XXIII. GP.
2034 Siehe dazu auch Art 1 des Entwurfs einer Datenschutz-Grundverordnung.

Wesentlichen auf Daten, die einem Geschäfts- oder Betriebsgeheimnis unterliegen, reduziere. Das Geschäfts- und Betriebsgeheimnis sei aber in der österreichischen Rechtsordnung ohnehin durch andere Bestimmungen (zB des gewerblichen Rechtsschutzes oder des Urheberrechts) geschützt.[2035]

Mehr Erfolg für eine Auslegung der Verfassungsbestimmung durch Heranziehung einfachgesetzlicher Terminologie verspricht der von *Jahnel* zwar als eher ungewöhnlich bezeichnete aber dennoch vorgeschlagene Weg über die »richtlinienkonforme Interpretation«.[2036] Einerseits besteht zwar kein Gebot der richtlinienkonformen Interpretation soweit keine Umsetzungspflicht besteht, was auch im Fall der Datenschutz-RL gegeben ist, da diese die Mitgliedstaaten nicht zur Schaffung eines »Grundrechts« auf Datenschutz verpflichtet.[2037] Andererseits war selbstverständlich durch die Datenschutz-RL auch für Österreich eine Umsetzungspflicht insoweit gegeben, als einige inhaltliche Erfordernisse der Datenschutz-RL im (damals geltenden) DSG 1978 nicht vollständig oder in anderer Weise enthalten waren. Da der österr Gesetzgeber die Regelungsstrukturen des DSG 1978 grundsätzlich aufrecht erhalten wollte, blieb das Grundrecht auf Datenschutz weiterhin verankert, wurde aber durch umfangreiche einfachgesetzliche Bestimmungen (zB §§ 4 bis 64 DSG 2000) weiter ausgeführt.[2038] Dies kann nur bedeuteten, dass die auf Grundlage der Datenschutz-RL eingeführten einfachgesetzlichen Vorschriften aus dem autonomen, unionsrechtlichen Begriffsverständnis der Datenschutz-RL heraus entstanden[2039] und daher wie das Grundrecht auf Datenschutz ebenfalls richtlinienkonform zu interpretieren sind. Nachdem auch das Verfassungsrecht unionsrechtlichen Vorgaben zu entsprechen hat, ist es möglich bzw sogar geboten, die richtlinienkonform auszulegenden Legaldefinitionen der einfachgesetzlichen Vorschriften des DSG 2000 zur Grundrechtsinterpretation heranzuziehen. Dies nicht zuletzt, weil in den GMat iZm dem Grundrecht auf Datenschutz bereits eine richtlinienkonforme In-

2035 Vgl 182/ME XXIII. GP, 4; Die DSG-Novelle 2008 ist aber letztlich nicht beschlossen worden.
2036 Vgl *Jahnel,* Handbuch, Rz 1/51 ff.
2037 Vgl *Wiederin,* Privatsphäre, 58.
2038 Siehe ErlRV 1613 BlgNR XX. GP, 30.
2039 Zum Argument der »richtlinienkonformen Interpretation« siehe *Jahnel* in FS Schäffer, 313 (316 f).

terpretation eingeräumt werde.[2040] Die Erl zur DSG-Nov 2010 belegen weiter, dass das Grundrecht auf Datenschutz verständlicher hätte formuliert werden und die in § 1 Abs 1 DSG 2000 enthaltene Einschränkung »soweit ein schutzwürdiges Interesse daran besteht« aufgrund einer richtlinienkonformen Interpretation entfallen hätte sollen. Dies wird damit begründet, dass diese Formulierung aus dem »alten« DSG (1978) stammt und »seit Inkrafttreten des DSG 2000 richtlinienkonform dahingehend zu interpretieren [war], dass alle personenbezogene Daten als schutzwürdig zu betrachten waren, es sei denn, dass sie allgemein verfügbar waren«.[2041]

Es kann und darf jedoch keine – eine dem Stufenbau der Rechtsordnung widerstrebende –Vorschrift zur Heranziehung von einfachgesetzlichen Definitionen zur Auslegung von Grundrechtsterminologie geben. Denn auch der Weg über die »richtlinienkonforme Interpretation« hat seine Schwachstellen insb dann, wenn das Grundrecht mit seinen Gewährleistungen weiterreicht, als die Richtlinie. Als Beispiel kann erneut die (fiktive) bereits oben angeführte Änderung der Definition des »Betroffenen« strapaziert werden.[2042] Würde der einfache Gesetzgeber über die Legaldefinition des § 4 Z 3 DSG 2000 beschließen, den Grundrechtsschutz nur mehr »natürlichen Personen« zuzuerkennen, so wäre ein Rückgriff auf diese Definition zur Interpretation des Grundrechts ebenso richtlinienkonform, da die Datenschutz-RL – wie zudem aus dem Titel erkennbar – nur den Schutz von »natürlichen Personen« harmonisieren will.[2043] In einem derartigen Fall würde man bei der Interpretation des Grundrechts auf Datenschutz unter Heranziehung dieser einfachgesetzlichen eingeschränkten Konkretisierung zwar richtlinienkonform, aber jedenfalls verfassungswidrig handeln. Dass das Grundrecht auf Datenschutz in seiner derzeitigen Ausgestaltung nicht nur natürlichen, sondern auch juristischen Personen zukommt, zeigt ua auch der bereits mehrfach zitierte ME zur (nicht beschlossenen) DSG-Nov 2008[2044], da in der Verfassungsbestimmung selbst und in den Erl

2040 Vgl ErlRV 472 BlgNR XXIV. GP, 6.
2041 Siehe ErlRV 472 BlgNR XXIV. GP, 6.
2042 Siehe dazu den genannten und nicht beschlossenen ME (182/ME XXIII. GP).
2043 In ErwG 24 Datenschutz-RL wird darauf hingewiesen, dass die Richtlinie nicht die Rechtsvorschriften zum Schutz juristischer Personen bei der Verarbeitung von Daten, die sich auf sie beziehen, berührt.
2044 182/ME XXIII. GP.

begründet[2045] die Änderung der Grundrechtsträgerschaft auf »Jede natürliche Person hat Anspruch« vorgeschlagen war. Dadurch hat der Gesetzgeber wohl dargelegt, dass der Begriff »Jedermann« im bisherigen Verständnis dieses Grundrechts auch juristische Personen mitumfasst.

Das Grundrecht auf Datenschutz wirkt nicht absolut und kann durch bestimmte in § 1 Abs 2 DSG 2000 definierte Eingriffe beschränkt werden. Gemeint sind alle (Grund-)Rechte des § 1 DSG 2000, also sowohl das Recht auf Geheimhaltung als auch die Rechte auf Auskunft, Richtigstellung und Löschung, wobei für die Begleitrechte § 1 Abs 4 DSG 2000 ausdrücklich festhält, dass Beschränkungen nur unter den Voraussetzungen des § 1 Abs 2 DSG 2000 zulässig sind.

§ 1 Abs 2 DSG 2000 besitzt eine eigentümliche Vorbehaltsstruktur, da neben den überwiegenden reinen Interessenvorbehalten eine Eingriffsvariante auch einen materiellen Gesetzesvorbehalt vorsieht.

Es werden ausschließlich nachfolgende Eingriffsalternativen geregelt:

1. die Datenverwendung im lebenswichtigen Interesse des Betroffenen[2046]
2. die Datenverwendung mit Zustimmung des Betroffenen
3. die Datenverwendung zur Wahrung überwiegender berechtigter Interessen eines anderen und zwar
   a) bei Eingriffen einer staatlichen Behörde
      i. Gesetzesvorbehalt mit Notwendigkeit einer der Gründe in Art 8 Abs 2 EMRK
      ii. Interessenabwägung
   b) bei anderen Eingriffen
      i. Interessenabwägung

Mit dem letzten Satz des § 1 Abs 2 DSG 2000 wird das aus der Grundrechtsjudikatur und -dogmatik[2047] herausgearbeitete Verhältnismäßigkeitsgebot ausdrücklich im Datenschutzgrundrecht normiert.[2048] Das bedeutet, dass selbst im Fall einer grundsätzlich zulässigen Beschrän-

2045 Vgl ErlME 182/ME XXIII. GP, 4.

2046 Sofern eine Zustimmung nicht eingeholt werden kann. Dies ergibt sich aus § 1 Abs 2 letzter Satz DSG 2000, wonach zulässige Eingriffe jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden dürfen (vgl VfGH 11.10.2012, B 1369/11 = jusIT 2012/104, 225 *[Jahnel]*).

2047 Vgl für viele *Berka,* Verfassungsrecht[5], Rz 1300.

2048 Dazu vertiefend *Jahnel,* Handbuch, Rz 2/67.

kung nach den Eingriffstatbeständen des § 1 Abs 2 DSG 2000, der Eingriff in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden darf.[2049] Der Verfassungsgesetzgeber betont damit insb das »Gebot des gelindesten Mittels« (auch Verhältnismäßigkeit im engen Sinn genannt). Zur Frage, ob eine Datenverwendung auch tatsächlich das gelindeste Mittel darstellt, gelangt man aber erst, wenn die allgemeinen Voraussetzungen der Verhältnismäßigkeit – wie sie der VfGH konkretisiert hat (Öffentliches Interesse, Eignung, Erforderlichkeit, Adäquanz)[2050] – erfüllt sind.[2051] Ein massiver Grundrechtseingriff zur Beförderung eines sehr schwachen öffentlichen Interesses könnte nämlich das gelindeste Mittel und dennoch unverhältnismäßig sein.

Aber auch ein konkreter an sich gesetzlich zulässiger Eingriff in das Grundrecht wäre ebenfalls unzulässig, wenn er nicht in der jeweils gelindesten, zum Ziel führenden Art vorgenommen würde, was insb auch für Eingriffe einer staatlichen Behörde von Relevanz ist.[2052] Stellt sich nämlich heraus, dass eine Maßnahme nicht das schonendste Mittel zur Zweckerreichung ist, würde sich die Vornahme einer Interessenabwägung erübrigen.[2053]

Für Gesetze, welche die Verwendung von personenbezogenen Daten, die besonders schutzwürdig sind (vgl sensible Daten) vorsehen, werden die Anforderungen an die Verhältnismäßigkeit durch § 1 Abs 2 zweiten Satz DSG 2000 weiter angehoben. Solche Gesetze dürfen ausschließlich zur Wahrung *wichtiger* öffentlicher Interessen in Erwägung gezogen werden und müssen gleichzeitig angemessene Garantien für den Schutz der Geheimhaltungsinteressen der Betroffenen festlegen.

Alle »Teilgrundrechte« des Grundrechts auf Datenschutz beziehen sich auf personenbezogene Daten. In der Legaldefinition des § 3 Z 1 DSG 1978[2054] wurde der Begriff »Daten« noch mit »auf einem Datenträger gespeicherte Angaben« näher beschrieben, sodass es hieß:

2049 DSK 18.11.2009, K121.501/0016-DSK/2009.

2050 Siehe dazu bespw VfSlg 17.065/2003; VfSlg 17.940/2006.

2051 Vgl *Berka,* Verfassungsrecht[5], Rz 1299 f.

2052 Vgl dazu auch VfSlg 16.369/2001.

2053 Siehe OGH 19.12.2005, 8 Ob 108/05y = ÖJZ EvBl 2006/67, 376 *(Noll),* wobei dieses Ergebnis unter Bezugnahme auf § 16 ABGB iVm Art 8 EMRK erzielt wurde. Der explizite Hinweis auf das »Gebot des gelindesten Mittels« in § 1 Abs 2 DSG 2000 wäre jedoch ebenfalls ausreichend gewesen (siehe *Jahnel,* Handbuch, Rz 2/69).

2054 DSG 1978, BGBl 565/1978; Durch die DSG-Nov 1986 (BGBl 370/1986) wurde diese Formulierung in »auf einem Datenträger festgehaltene Angaben« geändert.

»1. Daten: auf einem Datenträger gespeicherte Angaben, die Informationen über eine bestimmte oder mit Wahrscheinlichkeit bestimmbare natürliche oder juristische Person oder handelsrechtliche Personengesellschaft darstellen (personenbezogene Daten)«.

Daher konnte man wegen des erweiterten Datenbegriffs des Grundrechts in § 1 Abs 1 DSG 1978[2055], der sämtliche personenbezogene Daten (auch manuelle Dateien) erfasste und dem eingeschränkten Datenbegriffs in der einfachgesetzlichen Legaldefinition des § 3 Z 1 DSG 1978, der lediglich auf einem Datenträger gespeicherte personenbezogene Daten einschloss, von einem unterschiedlichen Begriffsverständnis des Gesetzgebers ausgehen. Durch den Entfall dieser Einschränkung im Zuge der richtlinienkonformen Umsetzung der Datenschutz-RL findet sich nun kein Hinweis mehr darauf, dass der Verfassungsgesetzgeber den Datenbegriff im Grundrecht anders als in der einfachgesetzlichen Legaldefinition des § 4 Z 1 DSG 2000 verstanden wissen will.[2056]

Aber auch aktuell findet sich noch ein gravierender Unterschied im Anwendungsbereich der im Grundrecht auf Datenschutz verschränkten Rechte, der auf die Art der Verarbeitung Bezug nimmt. Das Grundrecht auf Geheimhaltung in § 1 Abs 1 DSG 2000 gewährt unabhängig davon, ob Daten überhaupt bzw auf welche Art Daten verarbeitet werden, einen umfassenden Geheimnisschutz. Bloße Kenntnis einer personenbezogenen Information fällt daher ebenso in diesen Schutzbereich, wie unstrukturierte Aktensammlungen, persönliche Notizen oder eben automationsunterstützt verarbeitbare Daten.[2057] Die Begleitrechte auf Auskunft, Richtigstellung und Löschung in § 1 Abs 3 DSG 2000, die der Durchsetzung des (Haupt-)Grundrechts auf Geheimhaltung dienen sollen, beziehen sich lediglich auf personenbezogene Daten, die zur automationsunterstützten Verarbeitung oder zur Verarbeitung in manuell, dh manuell-strukturierten ohne Automationsunterstützung geführten Dateien, bestimmt sind.[2058]

2055 DSG 1978, BGBl 565/1978.

2056 Siehe *Jahnel,* Handbuch, Rz 2/10.

2057 Vgl *Jahnel,* Handbuch, Rz 2/12.

2058 Siehe dazu *Rosenmayr-Klemenz,* Zum Schutz manuell verarbeiteter Daten durch das DSG 2000 – Gleichzeitig eine Bemerkung zum Beschluss des OGH vom 28.6.2000, 6 Ob 148/00h = ÖJZ 2001/1 (EvBl), ecolex 2001, 639; ebenso *Spenling,* Zivilverfahren und Datenschutz – Eine erste Orientierung zu den neuen §§ 83 bis 85 GOG, in BMJ (Hrsg), Vorarlberger Tage 2005. Bd 125 (2006) 135 (137 f).

Auf den Beispielsfall des Phishing zurückkommend, ist als ein konkretes Recht, welches für § 108 in Frage kommt, das Geheimhaltungsrecht personenbezogener Daten nach § 1 Abs 1 DSG 2000 zu nennen.

Personenbezogene Daten sind gem § 4 Z 1 DSG 2000 Angaben bzw Informationen über natürliche oder juristische Personen oder Personengemeinschaften, deren Identität bestimmt bzw bestimmbar ist (sog »direkt personenbezogene Daten«).[2059] »Indirekt personenbezogene Daten« sind Daten, die vom konkreten Verwender nur mit rechtlich unzulässigen Mitteln auf eine Person zurückgeführt werden können,[2060] zB wenn Daten einer Person nicht unter ihrem Namen, sondern unter einer Nummer gespeichert werden, die nur derjenige auf den Namen rückführen kann, der rechtmäßig im Besitz des Namens und der dazugehörenden Nummer ist. Zu beachten ist dabei, dass jede Form der rechtlichen Unzulässigkeit zum bloß indirekten Personenbezug führt. Ein bestimmter Schwierigkeitsgrad für den rechtswidrigen Zugang wird nicht verlangt.[2061] Die Einschränkung der Entschlüsselung indirekt personenbezogener Daten auf legale Mittel fand auch in die Erl[2062] Eingang, wobei auch in ErwG 26 Datenschutz-RL von einem vernünftigen Mittel, also einem, das weder seiner Art, noch seinem Aufwand nach vollkommen ungewöhnlich ist, gesprochen wird.

In erster Linie handelt es sich bei im Wege des Phishing erlangten Zugangscodes, um Zugangskennung und zugehöriges Passwort bzw den Geheimcode einer zugriffsberechtigten Person.[2063] Ein Benutzername wird idR vom Betreiber einer Datenanwendung nach verschiedenen Kriterien erstellt und vergeben. Nicht immer besteht dieser aus dem tatsächlichen Namen des Berechtigten, vielmehr werden Zeichen- oder Zahlenkombinationen (zB Verfügernummer), einer entsprechenden Logik folgend, dafür herangezogen. In vielen Fällen kann der Nutzer seinen Benutzernamen aber auch selbst festlegen, wobei zu beachten ist, dass ein Benutzername bzw Zugangskennung in der Daten-

2059 Siehe S 563 ff.

2060 Siehe zu dieser Datenkategorie krit *Bergauer,* Indirekt personenbezogene Daten – datenschutzrechtliche Kuriosa, in Jahnel (Hrsg), Datenschutzrecht. Jahrbuch 2011 (2011) 55 (55 ff); allgemein dazu *Drobesch/Grosinger,* Datenschutzgesetz, 117 bzw 140; auch *Dohr/Pollirer/Weiss/Knyrim,* DSG² § 4 Anm 2.

2061 Vgl *Löschnigg,* Datenermittlung, 143; *Löschnigg,* Datenschutz und Kontrolle im Arbeitsverhältnis, DRdA 2006, 459; vgl *Jahnel* in Jahnel, Jahrbuch 2008, 27 (36); *Jahnel,* Handbuch, Rz 3/78.

2062 Vgl ErlRV zum DSG 2000, 1613 BlgNR XX. GP, 37.

2063 Siehe zu den weiteren Ausführungen ausf *Bergauer,* RZ 2006, 82.

bank des Betreibers stets eindeutig sein muss und daher nur einmal vorkommen darf. Freilich können auch systemgenerierte Pseudonyme, die ein Identifizierungsmerkmal zB durch eine Buchstaben- und/oder Zahlenfolge ersetzen sollen, als personalisierte Zugangskennung herangezogen werden.[2064] In diesen Fällen lässt sich nur bei Kenntnis des verwendeten Algorithmus[2065] ein Personenbezug herstellen.

Gleichgültig, ob der Benutzername aus dem vollständigen Namen, aus Namensteilen des Berechtigten, Pseudonymen oder aus willkürlichen Zeichenketten besteht, er wird zumindest als »indirekt personenbezogenes Datum« iSd § 4 Z 1 letzter Satz DSG 2000 zu qualifizieren sein, da – abgesehen vom Inhaber des Benutzernamens selbst – lediglich für den Betreiber der Datenanwendung bzw datenschutzrechtlichen Auftraggeber die Identität dieser konkreten Person (seines Kunden) mit rechtlich zulässigen Mitteln bestimmbar ist. Somit liegen zweifelsohne personenbezogene Daten vor. Im Gegensatz zum Benutzernamen kann jedoch ein Passwort diese Datenqualität nicht erfüllen, da nicht einmal der Betreiber der Datenanwendung auf Grund der Kenntnis eines Passwortes – ohne Verbindung zum Benutzernamen – einen Personenbezug herstellen kann. Passwörter lassen idR nicht auf verlässliche (auch personenbezogene) Inhaltsdaten schließen, denn selbst wenn ein bestimmter Personenname als Passwort verwendet würde, hieße das nicht, dass es sich dabei auch um den Namen des Passwortinhabers handelt. Und selbst wenn doch, so verhindern prinzipiell Namensgleichheiten eine treffsichere Bestimmbarkeit. Darüber hinaus könnten viele Nutzer unabhängig und unwissend voneinander auch dasselbe Passwort verwenden, was ebenfalls ohne eine weitere Datenverknüpfung keine Individualisierung zulässt. Auch wären willkürliche Zahlenfolgen vermischt mit diversen Sonderzeichen als Passwörter denkbar, deren Zusammensetzung keine intendierte Semantik aufweist. Daher sind Passwörter im Allgemeinen keine codierten Identitätsdaten, wie zB Benutzernamen, Kontonummern oder Kreditkartennummern, die der berechtigte Inhaber mit dem entsprechenden Entschlüsselungscode auflösen kann. Passwörter teilen deshalb das (datenschutzrechtliche) Schicksal anonymer Daten und unterliegen daher in dieser Form – dh sofern sie nicht

2064 Vgl *Jahnel* in Jahnel, Jahrbuch 2008, 27 (37); *Dohr/Pollirer/Weiss/Knyrim,* DSG² § 4 Anm 2.

2065 Rechenvorschrift oder Handlungsanweisung (siehe zu Algorithmen allgemein *Kersken,* IT-Handbuch⁵, 33 f bzw 91).

durch weitere Datenverknüpfungen einer Person zugeordnet werden können – nicht dem Grundrecht auf Datenschutz.[2066]

Erst wenn der Benutzername[2067] bzw in einigen Fällen des Online-Banking auch eine Kontonummer und Bankleitzahl (bzw IBAN und BIC) mit dem entsprechenden Passwort in Verbindung gesetzt werden, fallen Passwörter durch den personifizierenden Konnex in den Schutzbereich des Datenschutzgesetzes. Dasselbe gilt auch für Transaktionsnummern[2068] (TAN), die ohne Verknüpfung mit weiteren geeigneten Daten keinen Bezug zu einer Person zulassen. Das Ergebnis entspricht der Tatsache, dass die bloße Kenntnis von Passwörtern bzw TAN allein für den Verwender (hier: Täter) völlig nutzlos wäre. Die konkrete Einstufung der Daten in datenschutzrechtlich relevante Kategorien muss stets einzelfallbezogen unter Berücksichtigung der konkreten Situation und der jeweiligen Perspektive des Verwenders zu einem bestimmten Zeitpunkt erfolgen.[2069]

Wie bereits erwähnt, erstreckt sich gem § 1 Abs 1 DSG 2000 das im Verfassungsrang abschließend geregelte Recht auf Geheimhaltung auf jede Form personenbezogener Daten, an denen ein schutzwürdiges Geheimhaltungsinteresse besteht. Ein solches Interesse ist lediglich dann ausgeschlossen, wenn Daten infolge ihrer allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind.[2070] Aber auch diese normative Ausklammerung ist europarechtskonform zu interpretieren, da der EuGH festgestellt hat, dass auch veröffentlichte Daten grundsätzlich weiterhin im Anwendungsbereich der Datenschutz-RL verbleiben.[2071]

2066 Verwirrend daher der erste Leitsatz zur E des OLG Wien 21.11.1989, 23 Bs 201/89, in dem festgehalten wurde: »Kennwörter (Passwörter) für elektronische Nachrichtensysteme sind personenbezogene Daten iSd § 3 Abs 1 DSG.« Im zugrunde liegenden Sachverhalt richtete nämlich der Täter, als Administrator, selbst das Kennwort für seinen Kunden für dessen private Mailbox ein. Folglich konnte der Täter den geforderten Personenbezug des Passwortes leicht durch Verknüpfung der Identität des Kunden mit dem Passwort herstellen; zu anonymen Daten siehe ua *Jahnel,* Datenschutzrecht, in Jahnel/Mader/Staudegger (Hrsg), IT-Recht[3] (2012) 415 (426).

2067 Auch ist an den tatsächlichen Namen des Inhabers der Zugangsdaten zu denken, der aus dem Antwort-E-Mail des Opfers oder aus den entsprechenden vom Opfer befüllten Datenfeldern einer (falschen) Formular-Webseite eruiert werden kann.

2068 TAN sind sog »Einmalpasswörter« (siehe allgemein dazu *Rankl,* Chipkarten-Anwendungen, 88 ff).

2069 Siehe *Bergauer* in Jahnel, Jahrbuch 2011, 55 (63 ff) mwN.

2070 § 1 Abs 1 zweiter Satz DSG 2000.

2071 Vgl EuGH 16.12.2008, C-73/07; weiters *Bergauer/Thiele,* jusIT 2012/74, 158.

Wie bereits releviert[2072], wäre das Grundrecht des § 1 Abs 1 DSG 2000 diesbezüglich seitens des Gesetzgebers zu modifizieren.[2073]

Für die hier interessierende Subsumtion eines Phishing-Angriffs unter § 108 StGB iVm § 1 Abs 1 DSG 2000 ist jedenfalls davon auszugehen, dass es sich stets um Daten handelt, die ihrem Wesen nach personenbezogen sind und der Geheimhaltung unterliegen.

Ein zulässiger Eingriff in das Geheimhaltungsrecht wird gem § 1 Abs 2 DSG 2000 ua über die Zustimmung (§ 4 Z 14 DSG 2000) des Betroffenen zur Verwendung der Daten eingeräumt. Eine solche muss aber in jedem Fall freiwillig, in Kenntnis der wahren Sachlage und ohne Zwang erfolgen.[2074] Handelt es sich bei den zu verwendenden Daten um nicht-sensible personenbezogene Daten, so ist prinzipiell iSd § 8 Abs 1 Z 2 DSG 2000 auch eine konkludente Zustimmung möglich. Bei sensiblen Daten (§ 4 Z 2 DSG 2000) ist jedoch ausschließlich eine ausdrückliche Zustimmung (§ 9 Z 6 DSG 2000) vorgesehen. Wesentlich für das Institut der datenschutzrechtlichen Zustimmung ist, dass eine gültige Zustimmung nicht die Schutzwürdigkeit des Geheimhaltungsinteresses ausschließt, sondern lediglich den konkreten Eingriff in das Grundrecht zulässig macht.[2075]

Im Übrigen ist bei jeder Zweckänderung der Datenverwendung – selbst wenn der Auftraggeber derselbe bleibt – stets neuerlich eine Zustimmung einzuholen, was sich aus dem strengen Zweckbindungsprinzip ergibt.[2076]

In unserem Phishing-Fall täuscht der Täter den E-Mail-Empfänger über die Identität des Versenders und nützt so eine geschäftliche Vertrauenssituation des Getäuschten mit dem seriösen Bankinstitut aus, um an die Zugangsdaten zu gelangen. Das Vorliegen einer wirksamen datenschutzrechtlichen Zustimmung bzw strafrechtlichen Einwilligung[2077]

2072 Siehe S 140 ff.

2073 Vgl daher auch das legistische Vorhaben in ErlRV 472 BlgNR XXIV. GP, 6.

2074 Siehe instruktiv *Jahnel,* Handbuch, Rz 3/130 ff mwN; jüngst auch DSK 13.07.2012, K212.766/0010-DSK/2012.

2075 Vgl *Wiederin,* Privatsphäre, 61; *Jahnel,* Handbuch, Rz 2/41.

2076 Vgl allgemein *Jahnel,* Handbuch, Rz 4/103.

2077 Siehe dazu OGH 18.06.2012, 17 Os 1/12v = jusIT 2012/64, 138 *(Bergauer)* = JBl 2013, 193 *(Hinterhofer),* der festhält, dass es sich beim Grundrecht auf Datenschutz um ein Recht handelt, das der Disposition des Einzelnen unterliegt, weshalb der Rechtfertigungsgrund der (tatsächlichen oder mutmaßlichen) Einwilligung in Betracht kommt.

in den Grundrechtseingriff ist in diesen Fällen wohl von vornherein auszuschließen.

Das Grundrecht selbst schützt nach hM[2078] aber auch vor der zwangsweisen Verpflichtung des Betroffenen oder eines Dritten zur Weitergabe oder Offenlegung der Daten sowie vor Versuchen, auf andere Weise – wie etwa durch Täuschung – die Daten in Erfahrung zu bringen. Daher gewährt das Grundrecht auf Datenschutz auch einen »Ermittlungsschutz«. *Wiederin* weist ausdrücklich darauf hin, dass ua auch die heimliche Erhebung der gewünschten Informationen beim Betroffenen als indirekter Informationserhebungseingriff am Grundrecht zu messen ist.[2079]

Verknüpft der Täter die bereits bekannten Identitätsdaten (zB Name des Empfängers) mit den durch Täuschung erhaltenen Zugangsdaten, der Konto- und Kreditkartennummer sowie Passwort, PIN, TAN, so kann er sich den »Entschlüsselungscode« zur Bestimmbarkeit, also die Zuordenbarkeit der erlangten indirekt personenbezogenen Daten zu einer konkreten Person, selbst erzeugen bzw erledigt diesen Schritt bereits der Getäuschte selbst durch die Preisgabe der Zugangsdaten mitsamt seinem Namen. Spätestens ab dem Zeitpunkt der Verknüpfung der indirekt personenbezogenen Daten mit den bereits vorhandenen direkt personenbezogenen Daten (zB Namen des Getäuschten), liegen unmittelbar folgend in ihrer Gesamtheit jedenfalls direkt personenbezogene Daten vor.

Weiters würde bereits die Ermittlung und Kombination dieser Daten unter den datenschutzrechtlichen Begriff des »Verwendens« bzw »Verarbeitens« von Daten (siehe § 4 Z 8 und 9 DSG 2000) fallen.

Aus (dem einfachgesetzlichen) § 7 Abs 1 DSG 2000 folgt bereits, dass schutzwürdige Daten nur verarbeitet werden dürfen, wenn der Auftraggeber dazu berechtigt ist und die schutzwürdigen Interessen des Betroffenen gewahrt bleiben. Unter der Bezeichnung »Auftraggeber« versteht man gem § 4 Z 4 DSG 2000 ua eine Person, die für sich die

---

2078 Siehe *Wiederin,* Privatsphäre, 62; auch findet sich bereits in den ErlRV zum DSG 1978 (72 BlgNR XIV. GP) der Hinweis, dass auch Daten, die ohne Mitwirkung des Betroffenen ermittelt wurden, dem DSG unterliegen; siehe weiters *Jahnel* in FS Schäffer, 313 (320); *Rill* in Duschanek, Datenschutz in der Wirtschaft, 26; *Drobesch/Grosinger,* Datenschutzgesetz, 98; insb auch VfSlg 12.228/1989, 12.880/1991, 16.369/2001; aA *Evers,* Der Schutz des Privatlebens und das Grundrecht auf Datenschutz in Österreich, EuGRZ 1984, 290.

2079 *Wiederin,* Privatsphäre, 62.

Entscheidung getroffen hat, Daten für einen bestimmten Zweck zu verwenden (§ 4 Z 8 DSG 2000) und zwar unabhängig davon, ob sie die Verwendung selbst durchführt oder einen Dienstleister (§ 4 Z 5 DSG 2000) hierzu heranzieht.

Auch der Phishing-Täter agiert demnach als Auftraggeber, da für eine derartige Qualifikation lediglich die faktischen Umstände (also die Entscheidung zur Datenverwendung) wesentlich sind und es hierfür nicht auf die rechtliche Zulässigkeit der Datenverwendung ankommt.[2080] So sieht dies wohl auch der Gesetzgeber, wenn in den GMat ausgeführt wird, dass »die Frage, wer Auftraggeber ist, von der Frage streng zu trennen ist, ob diese Funktion zu Recht ausgeübt wird«.[2081] Der faktische Umstand, dass sich jemand (in concreto auch der Täter) zur Verwendung von personenbezogenen Daten für einen bestimmten Zweck entschieden hat, genügt, auf eine Befugnis kommt es nicht an.[2082] Auftraggeber ist daher prinzipiell jeder, der personenbezogene Daten eigenverantwortlich verarbeitet.

Für das »Selbstschädigungsdelikt« des § 108 ist es – wie beim Betrug (§ 146) – erforderlich, dass sich der Getäuschte selbst und unmittelbar in einem konkreten Recht schädigt.

Bereits im Zuge des Ermittelns der Daten, als Handhabungsart des Verarbeitens (vgl § 4 Z 9 erster Fall DSG 2000), wird das Opfer durch den Täter täuschungsbedingt dazu gebracht, seine Daten zu übersenden. Mit der Weitergabe der schutzwürdigen Daten an einen Unberechtigten schädigt sich der Betroffene selbst in seinem Recht auf Geheimhaltung nach § 1 Abs 1 DSG 2000.[2083] Selbst wenn es sich dabei um Daten handeln würde, die nicht automationsunterstützt oder in Form einer manuellen Datei (§ 4 Z 6 DSG 2000) vorliegen, wäre der Betroffene in seinem Grundrecht nach § 1 Abs 1 DSG 2000 verletzt.

Was die datenschutzrechtliche Rollenverteilung anlangt, so ist diese stets im Einzelfall zu untersuchen und festzustellen. Die Verarbeitung eigener personenbezogener Daten durch den »Betroffenen«[2084]

2080 Vgl etwa *Drobesch/Grosinger,* Datenschutzgesetz, 120.

2081 Siehe ErlRV 554 BlgNR XVI. GP, 17.

2082 Siehe auch DSK 16.11.2004, K120.951/0009-DSK/2004.

2083 Insoweit kann die Selbstschädigung bereits im Zuge des unzulässigen Ermittelns von Daten durch das täuschungsbedingte Handeln des Opfers (Preisgabe der Daten) konstatiert werden, und nicht erst mit der datenschutzrechtlichen Übermittlung (anders noch, aber im Ergebnis unverändert *Bergauer,* RZ 2006, 82).

2084 Auf die Begrifflichkeit des Auftraggebers iSd § 4 Z 4 DSG 2000 wird bewusst verzichtet, da über die Definition des Betroffenen (§ 4 Z 3 DSG 2000) e contrario zum

ist solange datenschutzrechtlich irrelevant, solange kein Dritter hins dieser Datenverwendung in Erscheinung tritt.[2085] Im vorliegenden Beispielssachverhalt wird der Täter bereits durch seine Datenermittlungshandlung zum Auftraggeber iSd § 4 Z 4 DSG 2000, das Täuschungsopfer ist Betroffener (§ 4 Z 3 DSG 2000). Dies ergibt sich – wie gerade angemerkt – daraus, dass es nicht auf die rechtliche Zulässigkeit der Datenverwendung ankommt.

d. Zur Anwendbarkeit des § 108 StGB im Fall des Phishing

Reindl-Krauskopf zweifelt an der Eignung des § 1 Abs 1 DSG 2000 als Tatobjekt des § 108 Abs 1 StGB, da die Existenz eines solchen eigenständigen (strafrechtlich geschützten) Rechts auf Wahrung des »Geheimnisses an PIN und TAN« fraglich erscheint.[2086] Darauf ist jedoch Verschiedenes zu erwidern:

Erstens wurde oben bereits ausgeführt, dass es sich bei den in solchen Sachverhalten idR betroffenen Daten – um »personenbezogene Daten« handelt. Ein »Recht auf Wahrung des Geheimnisses an PIN und TAN«, wie es *Reindl-Krauskopf* nennt, besteht grundsätzlich nicht und ist auch hier nicht angezeigt. Passwörter, wie TAN und PIN[2087], sind für »sich genommen« keine Daten, die einem Datenschutz nach § 1 Abs 1 DSG 2000 zugänglich sind, da es sich idR um Daten handelt, die nicht auf den Betroffenen rückführbar und daher anonym sind. Richtiger Weise kann es sich bei der hier vertretenen Argumentation nur um das Recht auf Geheimhaltung »personenbezogener« Daten handeln. Durch die Verknüpfung bzw Verknüpfungsmöglichkeit von anonymen Daten mit personenbezogenen, liegen in ihrer Gesamtheit allerdings jedenfalls personenbezogene Daten vor, da sich dadurch die ursprünglich »anonymen« Daten

---

Ausdruck gebracht wird, dass es sich beim datenschutzrechtlichen Auftraggeber um eine vom Betroffenen verschiedene (natürliche oder juristische) Person handeln muss.

2085 Siehe dazu auch *Jahnel,* RdW 2005/244, 200; auf Grundlage unzutreffender Schlussfolgerung auch OGH 04.05.2004, 4 Ob 50/04p = RdW 2005/244, 200 *(Jahnel)* = ecolex 2004, 873 *(Knyrim)*.

2086 Vgl *Reindl-Krauskopf,* Computerstrafrecht², 85.

2087 Eine PIN (wie etwa eine vierstellige Ziffernfolge; zB 1234) – ohne zusätzliche Merkmale oder technische personifizierende Bezugspunkte, wie etwa die dazugehörige Bankomartkarte – vermag es nicht mit einer ganz bestimmten Person in Verbindung gebracht zu werden. Selbst wenn es sich der Bezeichnung nach um eine »Persönliche Identifikationsnummer« handelt, ist diese Nummer per se nicht Personen identifizierend.

auf eine Person rückführen lassen. Gegenständlich ist somit nicht von einem »Recht auf Wahrung des Geheimnisses an PIN und TAN«, sondern vom »Recht auf Geheimhaltung personenbezogener Daten« die Rede.

Zweitens überzeugt das Argument *Reindl-Krauskopfs* nicht, dass die bloße Verletzung des Rechts auf Wahrung der Geheimnissphäre nicht ausreichend sei, da selbst jene Delikte, die ausdrücklich die Verletzungen der Privat- und Geheimnissphäre unter Strafe stellen (§§ 118 ff sowie § 51 DSG 2000[2088]), zusätzliche, zumindest beabsichtigte Beeinträchtigungen verlangen würden.[2089] Gerade die ausdrücklich von *Reindl-Krauskopf* angeführte Bestimmung des § 51 DSG 2000, wurde durch die DSG-Nov 2010 in diese Richtung modifiziert, sodass als zweite subjektive Alternative der überschießenden Innentendenz die (bloße) Absicht, einen anderen durch die Datenverwendung in seinem von § 1 Abs 1 DSG 2000 gewährleisteten Geheimhaltungsanspruch personenbezogener Daten zu schädigen, nunmehr für die Erfüllung bereits ausreicht.[2090]

Darüber hinaus werden dabei auch die GMat außer Acht gelassen, wenn dort ausgeführt wird, dass die Schädigung »sämtlicher konkreter Rechte« einer Privatperson durch Täuschung von der Strafbestimmung des § 108 erfasst sein soll.[2091] Auch der OGH befindet – wie oben bereits ausgeführt – jedes konkrete Recht als Tatobjekt des § 108[2092] und spricht sogar expressis verbis von »irgendwelchen Rechten«.[2093] Deshalb ist auch das subjektive Recht auf Geheimhaltung personenbezogener Daten (§ 1 Abs 1 DSG 2000) bzw die »informationelle Selbstbestimmung« als Rechtsgut denkbar. Das ist schon in Anbetracht der Einordnung des § 108 unter den Freiheitsdelikten und dessen Zielanliegen der »Freiheit der Willensentscheidung« angezeigt. Zudem wird der Unrechtsgehalt der Täuschung auch noch stärker bewertet als der des Betrugs, was sich grundsätzlich in den unterschiedlichen Strafdrohungen zeigt. Dagegen stellt § 108 gegenüber § 146 wiederum nur ein Ermächtigungsdelikt dar.[2094]

2088 *Reindl-Krauskopf* bezog sich dabei noch auf die Fassung vor der DSG-Nov 2010.
2089 Vgl *Reindl-Krauskopf,* Computerstrafrecht², 85.
2090 Siehe dazu ausf oben zu § 51 DSG 2000 (S 117 ff).
2091 Vgl JAB 359 BlgNR XVII. GP, 15.
2092 Siehe OGH 22.05.1986, 12 Os 136/85.
2093 Vgl OGH 02.09.1986, 11 Os 107/86.
2094 Vgl § 108 Abs 3.

Insgesamt betrachtet ist damit entgegen *Reindl-Krauskopf* festzuhalten, dass die Täuschung über Tatsachen mit einem daraus resultierenden Schaden an »irgendwelchen Rechten« somit insb auch das Grundrecht auf Geheimhaltung personenbezogener Daten nach § 1 Abs 1 DSG 2000 betreffen kann. Im Zusammentreffen mit anderen anwendbaren Bestimmungen tritt § 108 aber aufgrund seiner Auffangfunktion, die jede täuschungsbedingte Schädigung eines konkreten Individualrechts betrifft, zurück (materielle Subsidiarität).[2095]

Bezüglich des subjektiven Tatbestands argumentiert *Reindl-Krauskopf* weiter, dass es dem Täter beim Phishing nicht darauf ankomme das Geheimhaltungsrecht an den für die Vermögenstransaktion erforderlichen Daten des Opfers (bzw datenschutzrechtlich Betroffenen) zu verletzen, denn nur so würde eine absichtliche Verletzung der Geheimsphäre durch die täuschungsbedingte Selbstschädigung des Opfers iSd § 108 realisiert werden können. Der Täter beabsichtigte aber die finale Vermögensschädigung.[2096]

Aus dieser Argumentation folgt, dass *Reindl-Krauskopf* das an sich sukzessive Geschehen der Phishing-Attacke einheitlich in einer Gesamtbetrachtung beurteilen muss. Dass eine Gesamtbetrachtung grundsätzlich eine zulässige und pragmatisch sachgerechte Lösung bieten kann, zeigen prinzipiell auch Beispiele aus der Rechtsprechung. Doch gerade aus dogmatischen Gründen bietet sich eine nach Sachverhaltsabschnitten gegliederte Untersuchung eines derartigen Sachverhalts – wie oben dargestellt – an.[2097] Unterteilt man das tatsächliche Geschehen in eine Phishing-Phase und eine Verwertungsphase, so zeigt sich deutlich, dass es dem Täter in der Phishing-Phase nun gerade darauf ankommt das Opfer in seinem Geheimhaltungsrecht nach § 1 Abs 1 DSG 2000 zu verletzen. Der Täter benötigt schließlich die personalisierten Zugangsdaten des Opfers, an denen dieses selbstverständlich ein berechtigtes Geheimhaltungsinteresse hat, für sein weiteres Vorhaben.[2098] Das Recht des Opfers auf Geheimhaltung dieser personenbezogenen Daten iSd § 1 Abs 1 DSG 2000 soll geradezu durch die Täuschungshandlung des Täters verletzt werden, um das Endziel über-

2095 Vgl idS ähnlich OGH 02.09.1986, 11 Os 107/86.

2096 Siehe *Reindl-Krauskopf,* Computerstrafrecht², 85 f; *Reindl-Krauskopf,* SIAK-Journal 2007, 2 (9).

2097 Siehe ausf *Bergauer,* RZ 2006, 82.

2098 Siehe dazu auch *Bergauer,* Aktuelles zum Computerstrafrecht – zugleich eine Buchbesprechung, jusIT 2010/58, 132.

haupt erreichen zu können. Dadurch, dass sich das Opfer über die vom Täter veranlasste Täuschung (zB gefälschtes E-Mail) durch die Übermittlung der Daten selbst in diesem Recht schädigt, ist der objektive und subjektive Tatbestand des § 108 erfüllt. Nur weil die Schädigung des Geheimhaltungsrechts nicht – wie es bei § 51 zweite subj Alt DSG 2000 gefordert ist – das Endziel des Täters ist, kann trotzdem, auch bei einer Gesamtbetrachtung des gesamten Phishing-Angriffs von einer absichtlichen Verletzung des Geheimhaltungsrechts, als Zwischenziel, ausgegangen werden. Dies selbst dann, wenn das tatsächliche Endziel in einer wie auch immer realisierten Bereicherung liegen mag. Unterstützt wird diese Argumentation von der stRsp zur »Absichtlichkeit« (§ 5 Abs 2), die in einem Rechtssatz zusammengefasst lautet: »Absichtliches Handeln liegt vor, wenn sich der Täter die Verwirklichung des tatbildmäßigen Unrechts, sei es auch nur als Mittel zur Herbeiführung eines weiteren erstrebten Erfolgs, direkt zum Ziele setzt«.[2099]

Das getäuschte Phishing-Opfer verletzt sich somit durch die vom Täter veranlasste Preisgabe datenschutzrelevanter Informationen selbst in seinem verfassungsgesetzlich gewährleisteten Recht auf Geheimhaltung personenbezogener Daten (§ 1 Abs 1 DSG 2000). Aus diesem Grund ist Tatbestandsmäßigkeit iSd § 108 Abs 1 StGB iVm § 1 Abs 1 DSG 2000 gegeben, wobei zu beachten ist, dass die Täuschung gem § 108 Abs 3 ein Ermächtigungsdelikt darstellt, weshalb der Täter nur mit der Ermächtigung des datenschutzrechtlich Betroffenen (= Verletzter) zu verfolgen ist.

3. Prüfung der »Verwertungsphase«

Der 2. Sachverhaltsabschnitt eines klassischen Phishing-Angriffs erstreckt sich auf den Zeitraum, in dem sich der Täter bereits über die tatplangemäße irrtumsbedingte Preisgabe der Zugangsdaten durch den Getäuschten in Kenntnis der entsprechenden Daten befindet. Sein Tatplan führt ihn unmittelbar zur Verwendung dieser Codes, um selbst Online-Abbuchungen vom Konto des Getäuschten vorzunehmen oder per Tele-Banking[2100] eine Geldtransaktion von einem Angestellten der Bank des Phishing-Opfers auf sein »tatsächliches« Konto durchführen zu lassen.

2099 RIS-Justiz RS0089333 mwN; vgl aber auch *Fuchs,* AT I[8], Rz 14/10; weiters *Kmetic,* Grundzüge, 32 bzw 69.

2100 Kurz für Telefon-Banking.

Für die Beurteilung dieser Handlungen kommen neben dem Widerrechtlichen Zugriff auf ein Computersystem (§ 118a) der Betrügerische Datenverarbeitungsmissbrauch (§ 148a) bzw der Betrug (§ 146) sowie die Datenverwendung in Gewinn- oder Schädigungsabsicht (§ 51 DSG 2000) in Betracht.

a. Zum Widerrechtlichen Zugriff auf ein Computersystem (§ 118a)

Tatobjekt des § 118a Abs 1 ist ein Computersystem iSd § 74 Abs 1 Z 8, oder ein Teil eines solchen. Bei einem Online-Banking-System handelt es sich unzweifelhaft um ein solches Computersystem. Der Cyberkriminelle wird idR auch nicht oder nicht allein über dieses System verfügen dürfen. Die Tathandlung besteht im Sich-Zugang zu einem Computersystem zu verschaffen, wobei der Täter eine spezifische Sicherheitsvorkehrung überwinden muss. Der Täter hat sich »Zugang« verschafft, wenn er in die Lage ist, innerhalb des Computersystems tätig zu werden. Dass er innerhalb des Systems auch tatsächlich tätig wird, ist nicht (mehr) gefordert.

Das Überwinden der Sicherheitsvorkehrung verlangt nun mE, dass sich der Täter durch Ausarbeitung eines Überwindungsplans mit der Sicherheitsvorkehrung befassen und auf diese aktiv reagieren muss. Das bloße Umgehen dieser technischen Hürde reicht daher mE nicht aus.[2101] Allerdings muss für das Überwinden der Sicherheitsvorkehrung ein gewisses Mindestmaß an krimineller Energie vorliegen, das nach den GMat dann als unzureichend einzustufen ist, wenn dem Täter die Zugangsdaten von der berechtigten Person selbst mitgeteilt wurden.[2102]

Will sich der Täter im Wege einer Phishing-Methode tatbildliche Zugangsdaten verschaffen, ist mE bereits von einem Überwindungsplan bezüglich der Authentifizierungsabfrage des Online-Banking-Systems auszugehen, weshalb die Mindestschwelle der geforderten kriminellen Energie durch diesen nicht unerheblichen Aufwand bereits überschritten wird. Des Weiteren hat der Täter durch die Eingabe der herausgelockten Zugangsdaten auf die im System angebrachte Sicherheitsvorkehrung direkt reagiert und diese folglich überwunden.

2101 Siehe dazu oben zu § 118a.
2102 Vgl ErlRV 285 BlgNR XXIII. GP, 7.

In subjektiver Hinsicht verlangt § 118a Abs 1 neben dem Tatbildvorsatz, der sich im Handlungszeitpunkt im Mindeststärkegrad eines dolus eventualis auf sämtliche Umstände des objektiven Tatbestands beziehen muss, auch das Vorhandensein eines (äußert komplizierten) – über den objektiven Tatbestand hinausreichenden – erweiterten Vorsatzes im Stärkegrad der Absicht (§ 5 Abs 2 StGB). Zum einen muss der Täter in der Absicht handeln, sich oder einem anderen Unbefugten von den im Computersystem gespeicherten Daten Kenntnis zu verschaffen. Zum anderen muss er sich oder einem anderen durch die Datenverwendung (iSd Selbst-Benützens, Einem-anderen-Zugänglichmachen oder Veröffentlichen) einen Vermögensvorteil zuwenden (= Gewinnabsicht) oder zumindest einem anderen einen Nachteil zufügen (= Schädigungsabsicht) wollen.

»Absichtliches Handeln« liegt bereits vor, wenn sich der Täter die Verwirklichung des tatbildmäßigen Unrechts, sei es auch nur als Mittel zur Herbeiführung eines weiteren erstrebten Erfolgs (wie hier die finale Vermögensschädigung bzw Bereicherung), direkt zum Ziel setzt.[2103]

b. Zum Betrügerischen Datenverarbeitungsmissbrauch (§ 148a)

Unstrittig ist, dass der Täter im Zuge des Online-Banking bzw des »vollautomatischen« Online-Shopping keine Person täuscht, sondern jedenfalls eine Maschine zum Objekt der Manipulation wird.

Bei der Prüfung des § 148a stellt sich in unserem Fall die strittige – oben[2104] bereits ausf behandelte – Problematik, ob die Beeinflussung des Ergebnisses eines automationsunterstützten Datenverarbeitungsprozesses durch die Eingabe von »richtigen« Daten (zB Zugangscodes) realisiert werden kann. Die Rsp[2105] und ein Teil der Lehre[2106] wählen den zwar kriminalpolitisch wünschenswerten, aber gegenüber dem strafrechtlichen Bestimmtheitsgebot bedenklichen Ansatz, dass das Ergebnis der Datenverarbeitung dann beeinflusst ist, wenn ein von der materiellen Rechtslage abweichendes Resultat erzielt wird. Eine Beeinflussung des Ergebnisses liegt nach hM dann vor, wenn die eingegebenen Daten mit der

2103 Vgl ua dazu RIS-Justiz RS0089333 mwN; vgl auch *Fuchs,* AT I[8], Rz 14/10, der neben dem angestrebten Endziel, zumindest eine notwendige Durchgangsstufe verlangt, ohne die das eigentliche Ziel nicht zu erreichen ist.

2104 Siehe etwa S 374 ff.

2105 Vgl etwa OGH 14.12.1995, 15 Os 131/95

2106 Vgl anstatt einiger *Kirchbacher/Presslauer* in WK[2] § 148a Rz 11 mwN.

Realität in Beziehung gesetzt werden und dadurch ein darzustellender Lebenssachverhalt falsch wiedergegeben wird.[2107] In concreto bedeutet das, dass, obwohl die unrechtmäßige Verwendung »passender« Zugangsdaten (zB Verfügernummer samt Passwort, PIN oder TAN) durch den Täter, die das System schließlich technisch völlig unbeeinflusst und programmgemäß veranlassen, den Zugang und die Abbuchung des rein technisch »berechtigten« Täters zu akzeptieren, eine täuschungsähnliche Beeinflussung des Ergebnisses der Autorisierungsprüfung und in weiterer Folge auch der durchführbaren Geldtransaktion durch den Täter vorliegt. Mit anderen Worten, der Täter bringt das System dazu, einen rechtlich Unbefugten als (technisch) Berechtigten zuzulassen, ohne aber tatsächlich das Ergebnis der technischen Datenverarbeitung zu beeinflussen.[2108] Als Indiz dafür, dass auch der Gesetzgeber die Eingabe von formell zutreffenden Daten als von § 148a mitumfasst sieht, kann die Aufnahme des § 148a in die taxative Liste der Hauptdelikte des § 126c Abs 1 Z 1 gedeutet werden.[2109] Vom Vorbereitungsdelikt des § 126c Abs 1 Z 2 wird ua das Sich-Verschaffen von Zugangscodes pönalisiert, sofern der Täter mit der überschießenden Innentendenz agiert, diese zur Begehung eines der in Z 1 genannten Delikte verwenden zu wollen. Da § 148a seit dem StRÄG 2004[2110] als eines dieser Hauptdelikte[2111] angeführt ist, muss auch mit unbefugt verschafften passenden Zugangscodes ein Betrügerischer Datenverarbeitungsmissbrauch verwirklichbar sein. Dabei ist zu bedenken, dass der objektive (vom äußeren Tatbestand geforderte) Erfolgsunwert der Tat iSd § 148a im Vermögensschaden liegt, der in der Geldüberweisung vom Konto des Phishing-Opfers auf das Konto des Täters (idR gemeinsam mit dem Eintritt der Bereicherung als rein subjektiv anvisiertes Endziel)[2112] realisiert wird, und nicht notwendigerweise in einer Manipulation oder bloßen Eingabe von Daten. In konsequenter Anwendung der Fiktion, dass Daten dann unrichtig sind, wenn ein dazustellender Lebenssachverhalt falsch wiedergegeben wird, müssen auch unbefugt ver-

2107 Siehe dazu etwa *Triffterer* in SbgK § 148a Rz 20 (aF Stand Dezember 1992); siehe auch *Kirchbacher/Presslauer* in WK² § 148a Rz 16.

2108 So auch *Lewisch,* BT I², 242.

2109 § 148a wurde (erst) mit dem StRÄG 2004 als eines der Hauptdelikte in den Katalog des § 126c Abs 1 Z 1aufgenommen.

2110 ErlRV 309 BlgNR XXII. GP, 7.

2111 Die Bezeichnung als Hauptdelikt wird deshalb verwendet, da § 126c lediglich Vorbereitungshandlungen zu diesen Delikten erfassen soll.

2112 Siehe oben zu § 148a.

wendetete, zutreffende Daten als »unrichtige Daten« qualifiziert werden (siehe oben).

Mit Eingabe der Zugangsdaten, um überhaupt erst ins Online-Banking-System zu gelangen, setzt der Täter idR noch keine tatbestandsmäßige Ausführungshandlung iSd § 148a Abs 1 StGB, weil er damit noch nicht das Ergebnis der Datenverarbeitung derart beeinflusst, dass dadurch ein Vermögensschaden eintreten kann. Diese Handlung wäre allerdings im Lichte des § 118a zu prüfen. Nicht jede Eingabe von Daten beeinflusst das Datenverarbeitungsergebnis im tatbestandlichen Sinn, sondern nur eine solche, die für den Vermögensschaden letztlich entscheidend ist. Wenn der Täter allerdings den Überweisungsauftrag durch Eingabe der herausgelockten TAN zur wirksamen Giralgeldtransaktion ausfüllt, tritt er in das Versuchsstadium ein. Nach hM kommt es für das Unmittelbarkeitserfordernis einer ausführungsnahen Handlung im Wesentlichen auf die zeitliche und örtliche Nähe sowie das Fehlen weiterer Zwischenakte an, was im Einzelfall deliktsspezifisch zu untersuchen ist.[2113]

Die innere Tatseite des § 148a erfordert vom Täter den (zumindest bedingten) Tatbildvorsatz, durch die Eingabe der erlangten Daten die Beeinflussung des Ergebnisses einer automationsunterstützten Datenverarbeitung zumindest ernstlich für möglich zu halten und sich auch damit abzufinden sowie dadurch einen anderen am Vermögen zu schädigen. Zudem muss auch noch ein erweiterter Vorsatz auf unrechtmäßige Bereicherung im Zeitpunkt der Handlungsvornahme vorliegen.

Sowohl der objektive als auch der subjektive Tatbestand des § 148a sind in unserem Fallbeispiel erfüllt.

c. Zum Betrug (§ 146)

Täuscht der Täter im Zuge des Tele-Banking durch die Verwendung der erlangten Daten einen Bankangestellten, der irrtumsbedingt die Vermögensverfügung zu Gunsten des Täters trifft, kommt Betrug gem §§ 146 ff in Betracht. Da die Prüfung des objektiven und subjektiven Tatbestands für diese menschenbezogene Täuschungsvariante des zweiten Sachverhaltsabschnitts keine größeren Probleme aufwirft, wird sie an dieser Stelle nicht weiter ausgeführt.

2113 Siehe dazu allgemein *Fuchs,* AT I[8], Rz 29/21 ff bzw 29/27 ff; auch *Kienapfel/Höpfel/Kert,* AT[14], Z 21 Rz 17.

d. Zur Datenverwendung in Gewinn- oder Schädigungsabsicht (§ 51 DSG 2000)

Als nebenstrafrechtliche Strafbestimmung wäre zur Beurteilung der Verwertungsphase auch § 51 DSG 2000 heranzuziehen, wobei das widerrechtliche Verschaffen der Daten selbst grundsätzlich noch nicht vom Unrechtstatbestand des § 51 DSG 2000 erfasst ist.[2114] Benützt der Täter vorsätzlich die insgesamt als personenbezogene Angaben zu qualifizierenden Daten jedoch in weiterer Folge selbst – indem er die Daten für eine Geldtransaktion via Online-Banking, mit dem erweiterten Vorsatz, sich dadurch unrechtmäßig zu bereichern, missbraucht – ist der objektive und subjektive Tatbestand des § 51 DSG 2000 erfüllt.

IV. Missbräuche im unbaren Zahlungsmittelverkehr

In Umsetzung des EU-RB 2001/413/JI[2115] zur Bekämpfung von Betrug und Fälschung iZm unbaren Zahlungsmitteln wurden mit dem StRÄG 2004[2116] eine Legaldefinition in § 74 Abs 1 Z 10 sowie spezifische Straftatbestände bezüglich »unbarer Zahlungsmittel« ins Kernstrafrecht eingeführt. Rechtsgut hinter diesen Bestimmungen ist das »Vertrauen in die Sicherheit und Zuverlässigkeit des Zahlungsverkehrs mit unbaren Zahlungsmitteln«, weshalb es auch grundsätzlich der Allgemeinheit und nicht dem Einzelnen als Rechtsgutträger zugeordnet wird.[2117] Der Fokus dieses Kapitels richtet sich auf Mikrochips als unbare Zahlungsmittel und »White Plastic Card-Fälschungen«, welche mit dem Phänomen des hier bereits mehrfach angesprochenen Skimming in Verbindung stehen.

2114 Siehe dazu bereits ausf oben zu § 51 DSG 2000.
2115 Rahmenbeschluss 2001/413/JI zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln vom 28. 5. 2001, ABl L 2001/149, 1.
2116 BGBl I 15/2004.
2117 Vgl ErlRV 309 BlgNR XXII. GP, 4 und 10.

A. Unbare Zahlungsmittel (§ 74 Abs 1 Z 10)

> § 74 (1) [Auszug] Im Sinn dieses Bundesgesetzes ist
>
> 10. unbares Zahlungsmittel: jedes personengebundene oder übertragbare körperliche Zahlungsmittel, das den Aussteller erkennen lässt, durch Codierung, Ausgestaltung oder Unterschrift gegen Fälschung oder missbräuchliche Verwendung geschützt ist und im Rechtsverkehr bargeldvertretende Funktion hat oder der Ausgabe von Bargeld dient.[2118]

§ 74 Abs 1 Z 10 soll in erster Linie Kreditkarten, Bankomatkarten mit und ohne Quick-Chip[2119] usw als unbare Zahlungsmittel erfassen. Die Rsp[2120] hat diese Begriffsbestimmung dahingehend konkretisiert, dass unbare Zahlungsmittel nur solche sind, die »im allgemeinen Zahlungsverkehr ubiquitär einsetzbar sind« und die breit gestreute, allgemeine Zahlungsfunktion von Geld ersetzen. Beispielsweise ist die »E-Card« somit kein solches Zahlungsmittel.[2121] Ebenso stellen etwa eine Kundenkarte mit Zahlungsfunktion oder eine das Sparbuch ersetzende Sparkarte, die nur gegenüber dem kartenausstellenden Kreditinstitut – und nicht ubiquitär – einsetzbar sind, keine unbaren Zahlungsmittel dar.[2122] Dasselbe gilt sinngemäß auch für Tankkarten[2123], Telefonwertkarten oder Kopierkarten[2124]. Solche Karten können in der Regel aber auf Grund einer besonderen Ausgestaltung – iS einer Ausstellererkennbarkeit und Beweisrelevanz – Urkundenqualität besitzen.[2125] Die in den §§ 241a bis 241g geschaffenen Strafbestimmungen stehen, da sie sich auf einen autonomen Gewährschaftsträger beziehen (unbare Zahlungsmittel), insb gegenüber den Urkundendelikten grundsätzlich

2118 BGBl 60/1974 idF I 61/2012.
2119 Entspricht der CEN-Norm EN 1546, lässt sich bis € 400,– vorab aufladen und erfordert keine PIN-Eingabe.
2120 Siehe RIS-Justiz RS0120525 mwN; aA offenbar noch in den ErlRV 309 BlgNR XXII. GP, 6.
2121 Vgl OGH 23.04.2007, 15 Os 6/07g.
2122 Siehe statt vieler OGH 18.10.2011, 12 Os 137/11f.
2123 Siehe jüngst OGH 07.03.2013, 12 Os 5/13x; OGH 14.12.2005, 13 Os 68/05g.
2124 Siehe *Bertel/Schwaighofer,* BT II[11] § 241a Rz 3 mwN.
2125 Vgl OGH 23.08.2007, 12 Os 88/07v.

im Verhältnis der Exklusivität.[2126] Der OGH beurteilt das Verhältnis des § 241e Abs 3 zu § 229 Abs 1 jedoch als stillschweigend subsidiär.[2127]

Was Bankomatkarten (iSv Debit-Karten) und Kreditkarten anlangt, so muss aufgrund der Eigenart und besonderen Funktionalität von personengebundenen Zahlungskarten, sowohl ein aussteller- als auch inhaberbezogener Echtheitsbegriff zugrunde gelegt werden.[2128] Eine Kreditkarte wird von einem bestimmten Aussteller[2129] idR nur für eine bestimmte Person ausgestellt. Eine Bankomatkarte wird von einer bestimmten Bank nur für eine bestimmte Person und ein bestimmtes Girokonto ausgestellt.

Nach den GMat kommen auch »Computerchips«[2130] (genauer wohl: Mikrocontroller) selbst in ihrer Funktion als »Cash-Chips« als unbare körperliche Zahlungsmittel in Betracht, die sich auf einer Bankomatkarte oder auch auf jeder anderen (neutralen)[2131] Plastikkarte befinden können.[2132] Bei derartigen Systemen muss aber grundsätzlich vorab ein Betrag auf den Cash-Chip aufgeladen werden (»pay before«), der in weiterer Folge an entsprechenden Terminals[2133] ohne PIN-Eingabe oder Unterschrift zur Bezahlung verwendet werden kann (zB Parkschein- bzw Fahrscheinautomaten, Getränke-, Snack- oder Zigarettenautomaten, Kopiersysteme oder SB-Waschmaschinen)[2134].[2135] Es spielt dabei allerdings keine Rolle, ob gerade ein Geldbetrag aufgebucht ist oder nicht. Vielmehr kommt es lediglich auf die grundsätzliche Eignung an, anstelle von Geld verwendet zu werden oder der Bargeldverschaffung zu dienen.[2136] Die geforderte Körperlichkeit eines unbaren Zahlungs-

---

2126 Vgl *Plöckinger,* Die neuen Tatbestände zum Schutz unbarer Zahlungsmittel und deren Verhältnis zu den Urkunden- und Vermögensdelikten, ÖJZ 2005/14, 256; *Hinterhofer/Rosbaud,* BT II[5] Kap 9 Vorbem Rz 3 mwN; *Schroll* in WK[2] Vorbem §§ 241a – 241g Rz 3 (Stand Mai 2005); vgl auch ErlRV 309 BlgNR XXII. GP, 7 und 10.

2127 Vgl OGH 11.01.2005, 11 Os 131/04, weiters OGH 21.10.2004, 15 Os 114/04.

2128 ErlRV 309 BlgNR XXII. GP, 11.

2129 ZB Visa oder MasterCard.

2130 Im Sinn einer »elektronischen Geldbörse« (»Cash-Chip« bzw in Ö auch »Quick-Chip«).

2131 Damit ist eine Plastikkarte ohne weitere Zahlungsfunktionen gemeint.

2132 Siehe dazu ErlRV 309 BlgNR XXII. GP, 6; weiters *Sautner,* Neue Straftatbestände zum Schutz unbarer Zahlungsmittel, RZ 2004, 26.

2133 ZB spezielle Automaten oder Bankomatkassen.

2134 *Quick,* <www.quick.at/pay/overview.php> (01.04.2014).

2135 Bei einer Kreditkarte gilt das »pay after«-, bei Bankomatkarten das »pay now«-Prinzip (vgl dazu auch *Rankl/Effing,* Handbuch[5], 810).

2136 Siehe etwa zu Bankomatkarten OGH 08.06.2006, 15 Os 35/06w.

mittels indiziert das Vorliegen einer speziellen Funktionseinheit, die dann gegeben ist, wenn die spezielle Software mit der entsprechenden Hardware (Chipmodul) explizit und ausschließlich für Zahlungszwecke hardwarenah verbunden ist (vgl Mikrocontroller, »Embedded Systems« oder Firmware). Das bedeutet, dass die Funktionseinheit als Ganzes (dh auch in den Hardware-Komponenten) mit den Kriterien eines unbaren Zahlungsmittels ausgestattet sein muss. Universell einsetzbare Geräte, die sich mit entsprechender Finanzsoftware (zB Paybox und andere mobile Payment-Verfahren) ausstatten lassen (zB Mobiltelefon, Computer), stellen selbst keine unbaren Zahlungsmittel iSd § 74 Abs 1 Z 10 dar.[2137] Dies lässt sich auch damit erklären, dass nur Gewährschaftsträger in Form besonderer Beglaubigungszeichen[2138] erfasst sein sollen, denen im Rechtsverkehr eine konkrete Garantiefunktion zukommt.[2139] Es liegt in diesen mobilen Zahlungsmodellen ein lediglich per Software »aufgesetztes[2140] Zahlungssystem« vor, bei dem der Schutz gegen missbräuchliche Verwendung nicht im körperlichen Zahlungsmittel (zB Handy) selbst verankert ist, weshalb auch kein Gewährschaftsträger im beschriebenen Sinn vorliegt.[2141]

Wesentlich ist, dass unbare Zahlungsmittel den Aussteller erkennen lassen müssen. Dies kann dann der Fall sein, wenn durch die Gestaltung der Plastikkarte (wie zB bei Kredit- oder Bankomatkarte) der Aussteller mit freiem Auge erkennbar ist. Was den erwähnten Mikrocontroller anlangt, so reicht aber nach den GMat bereits die bloße »elektronische Erkennbarkeit« des Ausstellers aus.[2142]

Darüber hinaus wird in den Erl lapidar und unbegründet angemerkt, dass die »elektronische Geldbörse« lediglich durch ihre Ausgestaltung als elektronischer Datenträger grundsätzlich schon gegen

2137 Siehe statt vieler *Nittel* in SbgK § 74 Rz 169; aA *Wach,* »Unbare Zahlungsmittel« iS des § 74 Abs 1 Z 10 StGB – droht eine Ausuferung der Strafbarkeit?, RZ 2005, 130.

2138 Zu den geschützten Gewährschaftsträgern im StGB zählen Urkunden und Beweismittel sowie Geld, Wertpapiere, Wertzeichen und unbare Zahlungsmittel.

2139 Vgl *Plöckinger,* Die neuen Tatbestände zum Schutz unbarer Zahlungsmittel, in BMJ (Hrsg), 33. Ottensteiner Fortbildungsseminar aus Strafrecht und Kriminologie (2005) 103 (105); weiters *Jerabek/Reindl-Krauskopf/Schroll* in WK² § 74 Rz 60e.

2140 Die Zahlungsfunktionalität wird auf das universell einsetzbare Computersystem eingespielt, es stellt bezüglich eines Zahlungsmittels insgesamt keine solche Funktionseinheit dar.

2141 Siehe dazu *Jerabek/Reindl-Krauskopf/Schroll* in WK² § 74 Rz 60p.

2142 Vgl ErlRV 309 BlgNR XXII. GP, 6; siehe auch *Bertel/Schwaighofer,* BT II¹¹ § 241a Rz 2.

Fälschung geschützt sei.[2143] Auch *Kienapfel/Schmoller* sind der Meinung, dass als Codierung bereits jede elektromagnetische Speicherung von Information auf einem Magnetstreifen oder einem integrierten Chip genügt.[2144] Doch wie in den GMat an anderer Stelle betont wird[2145], kann eine falsche Zahlungskarte auch durch das bloße Kopieren des Datensatzes eines Magnetstreifens oder Computerchips auf eine »White Plastic Card« hergestellt werden (vgl Skimming). Die bloße Ausgestaltung eines unbaren Zahlungsmittels als elektronischer Datenträger samt – mit menschlichem Auge nicht unmittelbar wahrnehmbaren – Daten allein gewährt daher keinen (tauglichen) Fälschungsschutz. Welchen Sinn würde es auch machen auf »Schutzvorkehrungen« als ein Kriterium eines unbaren Zahlungsmittels abzustellen, die technisch gesehen, gar keinen Schutz bieten können. Dass man binärcodierte (Computer-)Daten bloß mit dem freien Auge nicht sehen kann, ist wohl kein ausreichender Schutzmechanismus. Vielmehr werden doch spezifikationsgemäße[2146] kryptographische Algorithmen gemeint sein, die dafür verantwortlich sind, dass die Informationen vor Manipulationen geschützt werden.[2147] Es stehen dafür verschiedene Verschlüsselungsstandards[2148] zur Verfügung. Die Legaldefinition des § 74 Abs 1 Z 10 sieht zwar vor, dass das Zahlungsmittel – alternativ neben Ausgestaltung[2149] oder Unterschrift – auch durch »Codierung« gegen Fälschung geschützt sein kann. Dies erfordert aber eine dafür spezielle Codierung iS einer technischen Verschlüsselung oder einer Passwortsicherung. Unter »Codierung« versteht man im Allgemeinen die eindeutige Zuordenbarkeit eines Zeichens aus einem definierten Zeichenvorrat zu einem eindeutigen Zeichen eines anderen festgelegten Zeichenvorrats.[2150] Werden lediglich die Aussteller-Informationen im »Klartext« auf dem Chip oder dem Magnetstreifen eines »unbaren Zahlungsmit-

2143 Siehe ErlRV 309 BlgNR XXII. GP, 6; siehe auch *Bertel/Schwaighofer,* BT II[11] § 241a Rz 2; *Jerabek/Reindl-Krauskopf/Schroll* in WK[2] § 74 Rz 60s; *Nittel* in SbgK § 74 Rz 171; *Schroll* in WK[2] Vorbem §§ 241a – 241g Rz 9; *Oshidari* in SbgK § 241a Rz 7; *Kienapfel/Schmoller,* StudB BT III[2] Vorbem §§ 241a ff Rz 30; *Fabrizy,* StGB[11] § 74 Rz 20.

2144 Vgl *Kienapfel/Schmoller,* StudB BT III[2] Vorbem §§ 241a ff Rz 25.

2145 Siehe ErlRV 309 BlgNR XXII. GP, 11.

2146 Vgl ISO/IEC 7816–4.

2147 Vgl zB *Rankl/Effing,* Handbuch[5], 831.

2148 ZB der symmetrische DES-Algorithmus oder das asymmetrische RAS- oder DSS-Verfahren (siehe dazu *Rankl/Effing,* Handbuch[5], 831).

2149 ZB mittels Hologrammen (vgl *Wach,* RZ 2005, 130).

2150 Vgl zB *Freyer,* Nachrichten-Übertragungstechnik[6], 211.

tels« in erforderlicher standardisierter Binärcodierung gespeichert, so sind die Daten zwar codiert, aber die Lesbarkeit und insb die Integrität der Informationen können dadurch keineswegs vor Fälschung geschützt werden. Mit einer »Codierung« iSd § 74 Abs 1 Z 10 – die aus diesem Grund notwendigerweise einen Fälschungsschutz implizieren muss – kann daher nur eine »kryptographische Codierung« samt Kopierschutz gemeint sein.[2151] Bei Bankomatkarten stellt wohl in erster Linie die auf der Karte verschlüsselt gespeicherte PIN ein Sicherheitsmerkmal dar, welche jedoch bei der Bezahlung mittels elektronischer Geldbörse (auch Quick-Chip) gerade nicht verwendet werden muss. Mangels Erfüllung dieser Kriterien ist wohl entgegen der hM – aber mit *Birklbauer/Hilf/Tipold*[2152] – davon auszugehen, dass die elektronische Geldbörse gerade kein unbares Zahlungsmittel darstellt.

Die Deliktsgruppe um unbare Zahlungsmittel lässt sich in zwei Kategorien einteilen. Auf der einen Seite (§§ 241a bis 241c; § 241d) sind Bestimmungen vorgesehen, die die Fälschung und Verfälschung bzw den Umgang mit solchen Falsifikaten pönalisieren, auf der anderen Seite (§§ 241e und 241f; § 241g) wird auf echte (unverfälschte) unbare Zahlungsmittel fokussiert und die Entfremdung bzw der Umgang mit (entfremdeten) unbaren Zahlungsmitteln unter Strafe gestellt.

B. Fälschung unbarer Zahlungsmittel (§ 241a)

> § 241a (1) Wer ein falsches unbares Zahlungsmittel mit dem Vorsatz herstellt oder ein echtes unbares Zahlungsmittel mit dem Vorsatz verfälscht, dass es im Rechtsverkehr wie ein echtes verwendet werde, ist mit Freiheitsstrafe bis zu drei Jahren zu bestrafen.
>
> (2) Wer die Tat gewerbsmäßig oder als Mitglied einer kriminellen Vereinigung begeht, ist mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren zu bestrafen.[2153]

2151 Siehe ähnlich *Sikora,* Der strafrechtliche Schutz des bargeldlosen Zahlungsverkehrs (2008) 21 f.

2152 Siehe *Birklbauer/Hilf/Tipold,* Strafrecht BT I² §§ 127, 128 Rz 15.

2153 BGBl 60/1974 idF I 15/2004.

Das Vorbereitungsdelikt des § 241a pönalisiert in Abs 1 das Herstellen eines falschen unbaren Zahlungsmittels oder das Verfälschen eines echten unbaren Zahlungsmittels, wenn es mit dem Vorsatz geschieht, dass ein solches falsches oder verfälschtes unbares Zahlungsmittel im Rechtsverkehr wie ein echtes verwendet werden soll. In diesem Fall ist der Täter mit Freiheitsstrafe bis zu drei Jahren zu bestrafen.

1. Fälschen oder Verfälschen

Ein falsches unbares Zahlungsmittel wird hergestellt, wenn ein echtes mit anderen Aussteller- und/oder Inhaberinformationen (zB bei Bankomat- oder Kreditkarten) nachgemacht wird. Das Erscheinungsbild eines solchen Falsifikats weckt den Anschein, als läge ein echtes unbares Zahlungsmittel vor. Mit dem bloßen Abschreiben der Kreditkartennummer samt Kartenprüfzeichen wird kein falsches unbares Zahlungsmittel hergestellt.

Zahlungskarten können auf verschiedene Art und Weise verwendet werden, wie zB für Zahlungen, bei deren Abwicklung Menschen eingebunden sind (vgl Kreditkartenzahlung), bei Bargeldbehebungen an Bankomaten oder für die Bezahlung von Waren an Bankomatkassen, bei welchen keine Überprüfungspflichten für anwesende Personen hins der Echtheit der Karte bestehen. Für eine Fälschung reicht es bereits aus, wenn lediglich der Anschein der Echtheit durch den ausschließlich maschinell lesbaren Datensatz, der auf dem Magnetstreifen oder Chip gespeichert wurde, erweckt wird (vgl zB das Kopieren der Daten eines echten unbaren Zahlungsmittels auf einen Plastikkarten-Rohling im Fall des Skimming[2154]). Das äußere Erscheinungsbild einer White Plastic Card erweckt dabei nicht den Anschein der Echtheit, wohl aber der kopierte Datensatz am Magnetstreifen oder am Mikrocontroller (für das jeweilige Terminal).[2155]

Eine echte Zahlungskarte wird verfälscht, wenn bspw die lesbaren Schriftzeichen (zB Name des Karteninhabers oder des Ausstellers) oder die auf dem Magnetstreifen oder auf dem Chip einer Zahlungskarte gespeicherten Daten (zB Kontonummer, PIN-Code, Kartenlimit, Gül-

2154 Siehe dazu zB auch den Sachverhalt zu OGH 10.08.2000, 15 Os 64/00.

2155 Vgl ErlRV 309 BlgNR XXII. GP, 11; weiters *Oshidari* in SbgK § 241a Rz 9 (Stand April 2007).

tigkeitsdauer) nachträglich verändert werden.[2156] Für das Verfälschen eines unmittelbaren Zahlungsmittels ist es daher erforderlich, dass eine Veränderung eines ursprünglich echten unbaren Zahlungsmittels erfolgt.

Maßgeblich ist in beiden Fällen die Verwechslungstauglichkeit des falschen oder verfälschten Zahlungsmittels, wenn es gegenüber einer Person eingesetzt oder in automationsunterstützter Form (ohne menschliche Kontrollmöglichkeit) verwendet wird.[2157] Für die Herstellung oder Verfälschung ist – im Gegensatz zu § 225a, wo die Eingabe, Veränderung, Löschung oder Unterdrückung von Daten zur Datenfälschung oder -verfälschung verlangt wird[2158] – jede Modalität möglich und von § 241a Abs 1 erfasst. Das rechtlich gleichwertige Herstellen und Verfälschen beschreiben einen alternativen Mischtatbestand.[2159] Das Herstellen oder Verfälschen eines solchen inkriminierten unbaren Zahlungsmittels ist aber an sich – was die Gefahr für das Rechtsgut der Sicherheit und Zuverlässigkeit des Rechtsverkehrs mit unbaren Zahlungsmitteln anlangt – noch weitgehend (konkret) ungefährlich. Dies gilt auch für entsprechende Besitzdelikte iSd § 241b. Erst wenn es tatsächlich in den (Zahlungs-)Verkehr gebracht wird, könnte es zu einer Gefährdung des Rechtsverkehrs und zur Beeinträchtigung des Vertrauens in das Institut der unbaren Zahlungsmittel kommen.[2160] Daher stellt die Pönalisierung des Herstellens und Verfälschens noch eine Vorstufe der Rechtsgutgefährdung im Vergleich zu den Besitzdelikten dar, die wiederum für sich selbst bereits eine Vorverlagerung der Strafbarkeit beanspruchen. Es handelt sich – was die Beziehung zum Rechtsgut anlangt – um ein abstraktes Gefährdungsdelikt. Darüber hinaus ist mit § 241c eine (noch) weitere Vorverlagerung des Rechtsgüterschutzes eingerichtet, der die Vorbereitungshandlungen bezüglich Fälschungsmittel bzw Werkzeuge zur Fälschung unbarer Zahlungsmittel (§ 241a) bereits unter Strafe stellt.

2156 Siehe ErlRV 309 BlgNR XXII. GP, 11; weiters *Sikora,* Zahlungsverkehr, 70.

2157 Siehe *Schroll* in WK² § 241a Rz 5 f und 11; weiters *Oshidari* in SbgK § 241a Rz 13 ff.

2158 § 225a »Wer durch Eingabe, Veränderung, Löschung oder Unterdrückung von Daten falsche Daten mit dem Vorsatz herstellt oder echte Daten mit dem Vorsatz verfälscht, dass sie im Rechtsverkehr zum Beweis eines Rechtes, eines Rechtsverhältnisses oder einer Tatsache gebraucht werden, ist mit Freiheitsstrafe bis zu einem Jahr zu bestrafen.«

2159 Siehe *Oshidari* in SbgK § 241a Rz 3; *Schroll* in WK² § 241a Rz 1.

2160 Vgl dazu auch *Hochmayr,* Besitz, 38.

2. Schlichtes Tätigkeits- oder Erfolgsdelikt?

Ein Teil der Lehre erachtet § 241a als ein schlichtes Tätigkeitsdelikt.[2161] Verfolgt man aber die hM zur Definition eines Erfolgsdelikts, so liegt immer dann ein solches vor, wenn der Tatbestand einen Erfolg – iSd »Eintritts einer von der Tathandlung zumindest gedanklich abtrennbaren Wirkung in der Außenwelt« – erfordert.[2162] Stellt jemand daher ein falsches Zahlungsmittel her, so liegt im Ergebnis eine Veränderung der Außenwelt insoweit vor, als nunmehr ein falsches Zahlungsmittel physisch existiert und wahrgenommen werden kann. Die Herstellung beschreibt den Prozess der Erzeugung mit dem Erfolg, dass ein Falsifikat entsteht. Dasselbe gilt für das Verfälschen, bei dem im Ergebnis in der Außenwelt ein nunmehr verfälschtes Zahlungsmittel vorliegt.[2163] Von einer zumindest »konkreten« Rechtsgutbeeinträchtigung, die als ein Gefährdungserfolg angesehen werden könnte, kann aber dabei noch nicht gesprochen werden. Im Ergebnis liegt daher im Verhältnis zum Rechtsgut ein abstraktes Gefährdungsdelikt, bezüglich der tatbestandlichen Struktur – unter exakter Anwendung der vorherrschenden Definition – ein Erfolgsdelikt vor.[2164]

Darüber hinaus wird, über den objektiven Tatbestand hinaus, im subjektiven Tatbestand – neben dem (zumindest bedingten) Tatbildvorsatz – verlangt, dass die Tathandlungen mit dem (ebenfalls zumindest bedingten) erweiterten Vorsatz verübt werden, dass das falsche oder verfälschte Zahlungsmittel im Rechtsverkehr wie ein echtes verwendet wird.[2165] Diese überschießende Innentendenz beschränkt sich auf das rechtserhebliche Verwenden, ohne dass es auf eine Erfolgsintention ankommt. So lässt sich dabei von einem verkümmert zweiaktigen Delikt sprechen.

2161 Vgl *Schroll* in WK² § 241a Rz 1; *Oshidari* in SbgK § 241a Rz 3; aA *Kienapfel/Schmoller,* StudB BT III² § 241a Rz 18.

2162 Vgl zB *Fuchs,* AT I⁸, Rz 10/40; *Kienapfel/Höpfel/Kert,* AT¹⁴, Z 9 Rz 6 ff.

2163 Siehe in ähnlichem Zusammenhang das Beispiel mit dem Briefgeheimnis und dem schlichten Öffnen des Briefes bei *Fuchs,* AT I⁸, Rz 10/47.

2164 Siehe auch *Bergauer,* jusIT 2012/26, 60.

2165 Es reicht dh eine allgemeine Zweckbestimmung für den erweiterten Vorsatz aus (vgl ErlRV 309 BlgNR XXII. GP, 12); siehe dazu auch *Fabrizy,* StGB¹¹ § 241a Rz 7; siehe krit dazu *Sautner,* RZ 2004, 26.

3. Subjektive Tatseite

Neben dem zumindest bedingten Tatbildvorsatz, der sich auf die gesamte äußere Tatseite erstrecken muss, wird im selben Stärkegrad ein überschießender Verwendungsvorsatz verlangt. Dieser erweiterte Verwendungsvorsatz, das falsche oder verfälschte Zahlungsmittel im Rechtsverkehr wie ein echtes zu gebrauchen, muss sich aber im Gegensatz zu § 225a nicht ausschließlich auf die Verwendung gegenüber einer Person beziehen. Die größere Reichweite des erweiterten Vorsatzes überzeugt, da das Delikt nicht verwirklicht wäre, würde sich der erweiterte Vorsatz des Täters lediglich auf die Verwendung eines falschen oder manipulierten unbaren Zahlungsmittels gegenüber Maschinen erstrecken.[2166]

§ 241a Abs 1 ist daher eine geeignete Bestimmung, zB um beim Skimming (zumindest) das Herstellen von »White Plastic Card-Fälschungen« zu erfassen. Das Kopieren des Datensatzes des Magnetstreifens oder des Mikrochips kann unter das Herstellen eines falschen unbaren Zahlungsmittels subsumiert werden. Handelt der Täter dabei mit dem bedingten Vorsatz, dieses Falsifikat zur widerrechtlichen Behebung von Bargeld an einem Bankomaten einzusetzen, ist auch der subjektive Tatbestand erfüllt.

4. Deliktsqualifikationen

§ 241a Abs 2 qualifiziert den Grundtatbestand des Abs 1, sofern die Tat gewerbsmäßig (Fall 1) oder als Mitglied einer kriminellen Vereinigung (Fall 2) begangen wird. In diesem Fall ist der Täter mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren zu bestrafen.

Die gewerbsmäßige Verwirklichung orientiert sich an § 70 und erfordert die Absicht, sich durch wiederkehrende Begehung – einer Fälschung oder Verfälschung von unbaren Zahlungsmitteln – eine fortlaufende Einnahme zu verschaffen. Dem gewerbsmäßig handelnden Täter muss es daher darauf ankommen (§ 5 Abs 2), sich durch die Wiederholung von Straftaten desselben Deliktstyps eine zumindest für einen längeren Zeitraum wirksame Einkommensquelle zu erschließen.

2166 Vgl auch *Reindl-Krauskopf,* Computerstrafrecht², 59.

Unter einem »längeren Zeitraum« sind zumindest einige Wochen zu verstehen.[2167]

Anzumerken ist jedoch, dass eine Qualifikationsnorm bezüglich einer gewerbsmäßigen Begehung des § 241a Abs 1 (auch § 241e Abs 1)[2168] im gesamten zwölften[2169] und dreizehnten[2170] Abschnitt ein systemwidriges Novum darstellt. Für keinen der in diesen Abschnitten des StGB erfassten Gewährschaftsträger – mit Ausnahme der »unbaren Zahlungsmittel« – ist eine Qualifikation bei gewerbsmäßiger Begehung vorgesehen. Auch der mit diesen Regelungen umzusetzende EU-RB 2001/413/JI[2171] berücksichtigt eine solche nicht.

C. Annahme, Weitergabe oder Besitz falscher oder verfälschter Zahlungsmittel (§ 241b)

> § 241b Wer ein falsches oder verfälschtes unbares Zahlungsmittel mit dem Vorsatz, dass es im Rechtsverkehr wie ein echtes verwendet werde, von einem anderen übernimmt, sich oder einem anderen verschafft, befördert, einem anderen überlässt oder sonst besitzt, ist mit Freiheitsstrafe bis zu einem Jahr zu bestrafen.[2172]

An § 241a anknüpfend und um eine lückenlose Kette zeitlich aufeinanderfolgender strafbarer Verhaltensweisen bis zur missbräuchlichen Verwendung falscher oder verfälschter unbarer Zahlungsmittel zu schaffen[2173], pönalisiert § 241b auch denjenigen, der ein falsches oder verfälschtes unbares Zahlungsmittel iSd § 74 Abs 1 Z 10 von einem anderen übernimmt, sich oder einem anderen verschafft, befördert, einem anderen überlässt oder sonst besitzt. Darüber hinaus muss der Täter mit dem erweiterten Vorsatz handeln, dass ein solches Zahlungs-

2167 Siehe OGH 08.06.2006, 15 Os 35/06w; vgl *Jerabek* in WK² § 70 Rz 7 (Stand Juli 2013); vgl *Rainer* in SbgK § 70 Rz 19 (Stand Mai 1996) mwN.

2168 Vgl § 241e Abs 2.

2169 Strafbare Handlungen gegen die Zuverlässigkeit von Urkunden und Beweiszeichen.

2170 Strafbare Handlungen gegen die Sicherheit des Verkehrs mit Geld, Wertpapieren, Wertzeichen und unbaren Zahlungsmitteln.

2171 Rahmenbeschluss 2001/413/JI zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln vom 28.5.2001, ABl L 2001/149, 1.

2172 BGBl 60/1974 idF I 15/2004.

2173 Vgl ErlRV 309 BlgNR XXII. GP, 12.

mittel im Rechtsverkehr wie ein echtes verwendet wird.[2174] Die Strafdrohung beläuft sich auf Freiheitsstrafe bis zu einem Jahr.

Nach den GMat soll § 241b Ähnlichkeiten mit dem »Hehlereitatbestand« (§ 164) bezüglich ge- oder verfälschter unbarer Zahlungsmittel aufweisen.[2175] Dies ist jedoch ungenau, weil der Unrechtsgehalt der Vortat (§ 241a) wohl selbst erst in der Verbreitung und Verwendung des Zahlungsmittels liegt.[2176] Darüber hinaus geht es dem Täter nicht um das Falsifikat selbst, sondern um dessen Gebrauch.

1. Vorbereitungsdelikt unterschiedlicher Intensität

Bei diesen im Vorfeldbereich angesiedelten Delikten bezüglich unbarer Zahlungsmittel, handelt es sich um »Vorbereitungsdelikte verschiedener Intensität«. Darüber hinaus indiziert der Tatbestand des § 241b in Relation zum Rechtsgut ein abstraktes Gefährdungsdelikt. Durch die Annahme, Weitergabe oder den Besitz falscher oder verfälschter Zahlungsmittel mit dem erweiterten Vorsatz, dieses im Rechtsverkehr wie ein echtes verwenden zu wollen, wird die abstrakte Gefährdung des Vertrauens in die Sicherheit und Zuverlässigkeit des (unbaren) Zahlungsverkehrs prolongiert.[2177] Dennoch ist das Delikt gleichzeitig als Nachtat der eigentlichen Fälschungshandlung nach § 241a zu sehen.[2178] Für den unmittelbaren Täter oder sonstigen Tatbeteiligten einer Fälschung oder Verfälschung eines unbaren Zahlungsmittels iSd § 241a stellt die Erfüllung des § 241b daher bloß eine straflose Nachtat dar. Der Unwert der Tat nach § 241b wird in diesem Fall bereits vollständig von der Haupttat erfasst.[2179]

2. Übernehmen eines Falsifikats

Der Täter übernimmt (§ 241b Fall 1) das Falsifikat, wenn er es sich einvernehmlich mit dem Übergeber aneignet (dh jegliche Form des derivativen Erwerbs).[2180] Er verschafft es sich (Fall 2), wenn er es faktisch an

---

2174 Vgl dazu auch die Ausführungen zu § 241a.
2175 Vgl ErlRV 309 BlgNR XXII. GP, 12; weiters *Sautner,* RZ 2004, 26.
2176 Siehe dazu iVm § 241 f *Hochmayr,* Besitz, 37.
2177 Siehe auch *Sautner,* RZ 2004, 26.
2178 Siehe ErlRV 309 BlgNR XXII. GP, 12.
2179 Siehe ErlRV 309 BlgNR XXII. GP, 12.
2180 Vgl *Bertel/Schwaighofer,* BT II[11] § 241b Rz 1; *Schroll* in WK[2] § 241b Rz 4 (Stand Mai 2005); *Oshidari* in SbgK § 241b Rz 10 f (Stand April 2007).

sich nimmt. Mit der Gewahrsamserlangung sind diese Handlungsvarianten formell vollendet. Nach den GMat zu § 241e[2181] soll ein »Sich-Verschaffen« vorliegen, »gleichgültig ob der Täter das unbare Zahlungsmittel durch Bruch des Gewahrsams des berechtigten Karteninhabers, durch Behalten eines gefundenen, eines ihm sonst zugekommenen oder eines anvertrauten Zahlungsmittels oder durch Verleitung des berechtigten Karteninhabers zur Herausgabe durch Täuschung über Tatsachen erlangt hat«.[2182] Eine Rechtswidrigkeit im Erlangungsakt ist gerade durch die klarstellende Nennung dieser Beispiele nicht ableitbar. Die Lehrmeinung[2183], dass es sich dabei um einen Akt handle, der ein An-sich-Nehmen ohne oder gegen den Willen des früheren Inhabers – also rechtswidrig – beschreibe, spiegelt sich nicht im Wortlaut des Gesetzestexts wider. Die Tathandlung des Sich-Verschaffens iZm dem »Übernehmen« wurde und wird – von §§ 224a, 227, 239 abgesehen – überwiegend in einer Auffangfunktion verwendet, wie dies etwa aus den Formulierungen »von einem anderen übernimmt oder sich auf andere Weise verschafft«[2184], oder »von einem anderen übernimmt, sich sonst verschafft«[2185] hervorgeht.[2186] Daraus kann geschlossen werden, dass die Handlung des Von-einem-anderen-Übernehmens prinzipiell auch von der abstrakteren Handlungsbeschreibung des Sich-Verschaffens mitumfasst ist. Daher ist mit dem »Von-einem-anderen-Übernehmen«, wohl eher der speziellere Akt gemeint, bei dem ein Vorbesitzer bekannt ist und dieser das Falsifikat seinem »Nachfolger« in dessen Gewahrsam übergibt. Die Initiative geht vom Inhaber aus, der Nachfolger als Übernehmer muss nur noch aktiv zugreifen. Strafbar macht sich in diesem Fall der Übernehmer.

2181 Es ist aber wohl davon auszugehen, dass der Gesetzgeber – zumindest – innerhalb derselben Regelungsmaterie (wie dem 13. Abschnitt des StGB) von derselben Begrifflichkeit ausgeht.

2182 Siehe ErlRV 309 BlgNR XXII. GP, 16.

2183 Vgl *Bertel/Schwaighofer,* BT II[11] § 241b Rz 1; *Schroll* in WK[2] § 241b Rz 4; *Hinterhofer/Rosbaud,* BT II[5] § 241b Rz 4; *Oshidari* in SbgK § 241b Rz 13 f.

2184 Vgl § 234 Abs 2 Z 1; § 238 Abs 2 Z 1.

2185 Vgl § 233 Abs 1 Z 1.

2186 Interessanterweise sucht man in anderen Tatbeständen außerhalb des 12. und 13. Abschnitts des StGB, wo ebenfalls das Sich-Verschaffen als Tathandlung aufgenommen wurde (wie zB § 126c Abs 1, § 207a Abs 3), die Formulierung »von einem anderen übernimmt« vergeblich. Das ist mE auch ausreichend, da das Sich-Verschaffen gerade sämtliche Formen des faktischen An-sich-Nehmens erfassen soll (vgl ErlRV 309 BlgNR XXII. GP, 16).

3. Sich- oder Einem-anderen-Verschaffen

Beim Sich-Verschaffen hingegen geht einzig die Initiative vom Täter selbst aus. Ein Vorbesitzer muss gar nicht bekannt sein, und es spielt auch keine Rolle, ob der Sich-Verschaffende mit bzw ohne Einverständnis oder gar gegen den ausdrücklichen Willen des vorherigen Inhabers an die Sache gelangt. Jede Form der Gewahrsamserlangung ist denkbar. Auch der Fund eines inkriminierten Zahlungsmittels – selbst wenn der Vorbesitzer den Gewahrsam daran schon aufgegeben hat – fällt unter das Sich-Verschaffen, da der Täter selbst aktiv werden muss, um das Fundstück in seinen Gewahrsam zu überführen.[2187] Im Anschluss daran besitzt er es.

Einem anderen verschafft (§ 241b Fall 3) es der Täter, wenn aufgrund seines Tätigwerdens das Tatobjekt in die Verfügungsmacht des Empfangenden gelangt.[2188] Würde man hier – aufgrund der in den GMat unterstellten Ähnlichkeit mit der Hehlerei – nun eine Interpretationsanleihe bei der Tathandlung des § 164 Abs 2 dritter Fall (arg »einem Dritten verschafft«) nehmen, so wäre derjenige erfasst, der eine solche Sache – ohne dabei selbst Verfügungsmacht erlangt zu haben, einem Dritten vermittelt.[2189] Dies wäre nicht sachgerecht. Meines Erachtens soll die Tathandlung des § 241b »Einem-anderen-Verschaffen« jede vom Täter aktive Tätigkeit zur Gewahrsamsverschaffung für einen anderen erfassen. Die Grenze zur Tathandlung »Einem-anderen-Überlassen« lässt sich erneut mit der Betrachtung des jeweiligen Initiators ziehen. Denn letztere Handlung wird vom Übernehmer angeregt, der das Tatobjekt erlangen will. Der Überlassende willigt ein und übergibt. Tatsächlich aber sind die Handlungsbeschreibungen der Gruppe des »An-sich-Bringens« gleichwertig, eine genaue Unterscheidung muss im Einzelfall nicht durchgeführt werden. Dies betrifft die Fälle des § 241b Fall 1 und 2.

2187 AA *Bertel/Schwaighofer,* BT II[11] § 241b Rz 1.
2188 Siehe *Hinterhofer/Rosbaud,* BT II[5] § 241b Rz 4.
2189 Siehe *Kirchbacher* in WK[2] § 164 Rz 2 (Stand September 2011); auch *Fabrizy,* StGB[11] § 164 Rz 9.

4. Befördern eines Falsifikats

Der Täter befördert (Fall 4) das ge- oder verfälschte unbare Zahlungsmittel, wenn er es von einem Ort zu einem anderen Ort bringt.[2190] Die Beförderung beginnt mit dem Abtransport und endet mit der Ankunft am Zielort. Sinnvollerweise verlangt sie aber eine gewisse ins Gewicht fallende räumliche Reichweite. Zumindest wird man davon ausgehen müssen, dass der Täter seinen räumlichen Herrschaftsbereich zur Beförderung verlassen muss. Trägt der Täter das Falsifikat von seinem Wohnzimmer ins Schlafzimmer, liegt wohl kein tatbestandliches Befördern vor. Nicht erforderlich ist es, dass der Täter das corpus delicti einem anderen überbringt oder zustellt. Analog dazu ist die Tat mit dem Abtransport bereits formell vollendet, mit Beendigung der Ortsveränderung ist sie es auch in materieller Hinsicht.[2191] § 241b ist daher hins des Beförderns ein Dauerdelikt.[2192] Durch das Transportieren des unbaren Zahlungsmittels wird ein rechtswidriger Zustand geschaffen, den der Täter in der Folge solange aufrecht erhält (und durch dessen Fortdauer der Straftatbestand ununterbrochen weiter verwirklicht wird) bis der Transportvorgang tatsächlich beendet wurde. Jede Beförderung impliziert aber in den meisten Fällen auch den Besitz.[2193]

5. Einem-anderen-Überlassen

Einem anderen wird das Falsifikat überlassen (§ 241b Fall 5), wenn der Täter die Verfügungsgewalt darüber willentlich einem anderen überträgt.[2194] Mit der Gewahrsamsaufgabe ist diese Handlungsvariante vollendet. Strafbar ist daher der Übergeber, auch wenn die Initiative vom (späteren) Übernehmenden ausgeht. Diese Handlung ist das »spiegelverkehrte« Ebenbild des »Von-einem-anderen-Übernehmens«. Die Initiative geht beim Überlassen zwar vom Übernehmer aus, die Tathandlung wird aber vom Übergeber gesetzt. Beim Übernehmen geht

2190 Vgl ErlRV 294 BlgNR XXII. GP, 11; *Oshidari* in SbgK § 241b Rz 15 f.
2191 Vgl *Schroll* in WK² § 241b Rz 6.
2192 Siehe etwa *Kienapfel/Schroll* in WK² § 224a Rz 6 (Stand Juli 2006); *Schroll* in WK² § 233 Rz 13; sowie *Schroll* in WK² § 241b Rz 6; *Nimmervoll* in SbgK § 104a Rz 5 und 100 (Stand Mai 2010).
2193 Zur Tathandlung des »sonst Besitzens« siehe im Anschluss.
2194 Vgl *Schroll* in WK² § 241b Rz 7; weiters *Oshidari* in SbgK § 241b Rz 17.

die Initiative vom Übergeber aus, strafbar macht sich bei dieser Handlungsalternative aber der Übernehmer.

In den Handlungsalternativen der Fälle 1 bis 5 stellt § 241b ein Erfolgsdelikt dar.[2195] Nach der Tatbestandsauslegung verlangt jede dieser Tathandlungen eine von ihr zumindest gedanklich abtrennbare Wirkung in der Außenwelt. Übernimmt jemand oder verschafft dieser sich oder einem anderen ein entsprechendes Falsifikat, überlässt er es einem anderen oder befördert er es, so finden jeweils von der einzelnen Handlung abtrennbare Veränderungen in der Außenwelt statt. Die Weitergabe oder Annahme bzw Verschaffung erfordert einen Inhaberwechsel bezüglich der Fälschung. Im deliktsspezifischen Zusammenhang indiziert die Tathandlung des »Sich-Verschaffens« einen tatbildlichen Erfolg, da unbare Zahlungsmittel – ergo auch ihre Fälschungen – per definitionem nur körperliche Sachen sein können und mit dem Verschaffungsakt daher ein Gewahrsamswechsel stattfindet.[2196] Die Beförderung verlangt die außenweltwirksame Ortsveränderung von Standort A, über mehr oder weniger viele Zwischenstandorte während des Transportes, zum Endstandort B.[2197] Mit dem Wegbewegen der Sache wird die Außenwelt dadurch verändert, dass sich das Falsifikat nun während und nach Abschluss der Beförderung an einem anderen Ort als dem Ausgangsort befindet.

Von der Tathandlung des Sonst-Besitzens unterscheidet sich das Befördern durch das Erfordernis in der Außenwelt bewegt zu werden, was mE – wie oben dargelegt – anders als beim Besitzen auch den tatbestandlichen Erfolg indiziert.

6. Besitz des Falsifikats

Die Auffangtathandlung des Besitzens wird bereits im Zuge der meisten anderen Haupthandlungsweisen des § 241b mitverwirklicht (vgl zB das Überlassen, Übernehmen, Sich-Verschaffen, Befördern). Sie hat daher nur Aushilfscharakter und tritt bei Vorliegen einer der anderen Handlungen hinter diese zurück (Subsidiarität). Der bloße Gewahr-

2195 Nach *Oshidari* gilt das nur für die Fälle 1 bis 4 (vgl *Oshidari* in SbgK § 241b Rz 4).
2196 Siehe im Gegensatz dazu aber zum Sich-Verschaffen von Zugangsdaten (S 335).
2197 Siehe zum Befördern, als Tathandlung, die einen Erfolg indiziert iZm § 1 Abs 1 lit b PornG OGH 30.10.1986, 12 Os 93/86.

sam[2198] an der inkriminierten Sache, dh die Ausübung der faktischen Herrschaftsgewalt darüber, reicht für das Besitzen bereits aus.[2199] In Verwirklichung der Besitztathandlung ist § 241b ebenfalls ein Dauerdelikt.[2200] Auf der einen Seite kann das Besitzen eine schlichte Tätigkeit durch Tun darstellen (schlichtes Tätigkeitsdelikt), wenn der Täter das Gewahrsam an der Sache aktiv aufrechterhält, zB indem er das Falsifikat bei sich versteckt. Auf der anderen Seite kann ein Besitzen auch durch ein Unterlassen verwirklicht werden, indem es nämlich der Täter unterlässt das Gewahrsam an der inkriminierten Sache aufzugeben (echtes Unterlassungsdelikt).[2201] Aufgrund des tatbestandsnotwendigen subjektiven Unrechtselements im erweiterten Vorsatz liegt aber insb auch in § 241b sechster Fall ein kupiertes Erfolgsdelikt vor.[2202] Denn auch der Besitz muss in der subjektiven Innentendenz erfolgen, dass das Falsifikat im Rechtsverkehr – irgendwann und von wem auch immer – wie ein echtes verwendet wird.

7. Mischdelikt

Schroll erachtet § 241b als kumulatives Mischdelikt, dessen Tathandlungen selbstständige, untereinander nicht austauschbare Tatmodalitäten darstellen.[2203]

Meines Erachtens ist dem aber nicht zu folgen. Denn wie bereits angemerkt geht idR das Befördern, wie auch das Sich-Verschaffen und Von-einem-anderen-Übernehmen mit dem (anschließenden) Besitz des Falsifikats einher.[2204] Dies ergibt sich schon aus dem Verständnis, dass der strafbare Besitz als jede »Herbeiführung oder Aufrechterhaltung von Gewahrsam« gedeutet wird.[2205] Diese Handlungen, durch denselben Täter verwirklicht, bilden demnach ein und dieselbe strafbare Handlung mit gleichem Sinn- und Wertgehalt. Es wäre auch nicht zu verstehen, warum zB das Sich-Verschaffen eines Falsifikats anders zu beurteilen wäre, als das von einem anderen Übernehmen oder das Be-

2198 Auch Mitgewahrsam reicht schon aus.
2199 Siehe zur Tathandlung des Besitzens bei § 207a Abs 3.
2200 Vgl generell *Hochmayr,* Besitz, 63 ff; aA *Kienapfel/Höpfel/Kert,* AT[14], Z 9 Rz 30.
2201 Siehe *Oshidari* in SbgK § 241b Rz 4; weiters *Hochmayr,* Besitz, 53 ff bzw 147 f.
2202 Eine solche Einordnung wirkt sich ua ggf auf eine strafbare Beteiligung aus.
2203 Vgl *Schroll* in WK[2] § 241b Rz 3; dem zustimmend *Oshidari* in SbgK § 241b Rz 9.
2204 Vgl idS zu § 27 Abs 1 SMG RIS-Justiz RS0114037.
2205 Vgl ausf *Hochmayr,* Besitz, 56 ff, 85 ff, 145 ff.

fördern anders als das Besitzen. In diesen Fällen liegt jedenfalls ein gleicher Sinn- und Wertgehalt vor. Daher sind die Tathandlungen des (sinngemäß) »An-sich-Nehmens« und Besitzens, also § 241b erster, zweiter, vierter, sechster Fall, alternativer Natur. Die Subsumtion unter die falsche Variante begründet angesichts der Gleichwertigkeit dieser Formen des verbotenen Umgangs keine Urteilsnichtigkeit (gem § 281 Abs 1 Z 10 StPO).

Demgegenüber bilden § 241b dritter (arg »einem anderen verschaffen«) und fünfter Fall (arg »einem anderen überlassen«)[2206], die wiederum selbst untereinander gleichwertige Handlungsalternativen beschreiben (= alternativer Mischtatbestand), ein kumulatives Mischdelikt. Das Gesetz fasst dabei unter derselben Bezeichnung Handlungsweisen mit unterschiedlichem Sinn- und Wertgehalt zusammen und unterwirft sie der gleichen Rechtsfolge.

Die Handlungsgruppe des »An-sich-Nehmens« und Besitzens geht idR der Gruppe der »Verbreitung« vor. Verschafft sich der Täter daher ein Falsifikat und überlässt es anschließend einem anderen, liegen zwei strafbare Handlungen vor. Verschafft es sich der Täter und hält den Gewahrsam daran aufrecht, so liegt trotz des anschließenden Besitzes nur eine strafbare Handlung vor.[2207]

D. Vorbereitung der Fälschung unbarer Zahlungsmittel (§ 241c)

> § 241c Wer mit dem Vorsatz, sich oder einem anderen eine Fälschung eines unbaren Zahlungsmittels zu ermöglichen, ein Mittel oder Werkzeug, das nach seiner besonderen Beschaffenheit ersichtlich zu einem solchen Zweck bestimmt ist, anfertigt, von einem anderen übernimmt, sich oder einem anderen verschafft, einem anderen überlässt oder sonst besitzt, ist mit Freiheitsstrafe bis zu einem Jahr zu bestrafen.[2208]

Als »Vorbereitungsdelikt zu den Vorbereitungsdelikten (§§ 241a f)« pönalisiert § 241c bereits denjenigen, der spezifische Fälscherwerkzeuge oder -mittel anfertigt, von einem anderen übernimmt, sich oder einem

2206 Man könnte sie als Handlungsgruppe der »Verbreitung« zusammenfassen.
2207 Jeweils mit entsprechender deliktsspezifischen (überschießender) Innentendenz.
2208 BGBl 60/1974 idF I 15/2004.

anderen verschafft, einem anderen überlässt oder sonst besitzt, wenn er dies mit dem Vorsatz macht, sich oder einem anderen eine Fälschung eines unbaren Zahlungsmittels zu ermöglichen.

1. Deliktsspezifische Fälschungswerkzeuge

§ 241c verlagert die Strafbarkeit noch weiter ins Vorbereitungsstadium. In objektiver Hinsicht hat dabei nur die spezielle Zweckbestimmung der Fälschungswerkzeuge eine strafbarkeitseinschränkende Funktion.[2209] Derartige Mittel müssen daher eine spezifische Eignung aufweisen. Vorrichtungen, die für legale Zwecke eingesetzt werden können (sog »Dual-use Devices«) scheiden daher als Tatobjekte aus. Spezifische fälschungstaugliche Computerprogramme können aber grundsätzlich als solche Fälschungsmittel angesehen werden.[2210] Bei der Anfertigung, also Herstellung, eines solchen Werkzeugs, stellen die einzelnen handelsüblichen Bauteile selbst noch keine inkriminierten Mittel- oder Werkzeuge dar. Erst mit dem entsprechenden Zusammenbau bzw mit der Programmierung[2211] ergibt sich für die letztlich gebrauchsfähige Vorrichtung oder das einsatzfähige Computersystem diese Deliktstauglichkeit.

Was Lesegeräte für Magnetstreifen oder Mikrochips iZm Skimming anlangt, so ist fraglich, ob die an den Bankomaten eingesetzten entsprechend adaptierten Skimmer (zB Aufsatzlesegeräte), die die Datensätze des Magnetstreifens oder Mikrochips auslesen und aufzeichnen, als solche Fälschungswerkzeuge angesehen werden können.

Da es sich um ein Mittel oder Werkzeug handeln muss, das nach seiner besonderen Beschaffenheit objektiv ersichtlich zum Zweck der Fälschung bestimmt ist, kann – dem Wortlaut entsprechend – nur ein solches Werkzeug gemeint sein, das selbst unmittelbar zur Herstellung eines Falsifikats verwendet werden kann. Selbst wenn ein gewöhnliches Kartenlesegerät zu einem »Aufsatzskimmer« umfunktioniert bzw baulich adaptiert wird, handelt es sich nicht um ein spezifisches Fälscherwerkzeug, da es nicht zur Fälschung eines unbaren Zahlungsmittel verwendet werden kann, sondern nur zum Beschaffen der Datensätze

2209 Vgl *Sautner,* RZ 2004, 26.
2210 Vgl ErlRV 309 BlgNR XXII. GP, 13.
2211 Sofern es sich um typische Fälschungscomputersysteme handelt.

eines Magnetstreifens oder eines Mikrochips.[2212] Für die Einordnung als Fälschungsmittels bzw -werkzeug fehlt es solchen Geräten an unmittelbarer Fälschungstauglichkeit. Diese besondere Eigenschaft bildet aber auch ein strafbarkeitsbegrenzendes Korrektiv, was die weitreichende Vorverlagerung der Strafbarkeit insgesamt betrifft. Würde man sämtliche Mittel und Werkzeuge, die zwar zu Fälschungen beitragen können, selbst aber nicht unmittelbar die Fälschungen erzeugen, erfassen, würde das zwar auch die gegenständlichen Lesegeräte (vgl Skimmer) einschließen, aber in Anbetracht der massiven Vorverlagerung der Strafbarkeit im Verhältnis einer Beeinträchtigung des geschützten Rechtsguts über das Ziel hinausschießen. Für das Beschreiben eines Magnetstreifens bzw Mikrochips einer »White Plastic Card« und daher auch das unmittelbare Fälschen oder Verfälschen eines unbaren Zahlungsmittels bedarf es eines geeigneten Codiergeräts. Solche Codiergeräte, die grundsätzlich beim Skimming nicht vor Ort am Bankomaten eingesetzt[2213] und daher auch nicht entsprechend manipuliert werden, sind idR handelsüblich und daher ebenfalls nicht erfasst. Dasselbe gilt für White Plastic Card-Rohlinge, die per se legal im Handel gekauft werden und auch legale Zwecke erfüllen können. Es handelt sich dabei um sog »Dual-use Devices«[2214].

Zu den Beschreibungen der einzelnen Tathandlungen kann weitgehend auf § 241b verwiesen werden. Die Tatmodalität des Anfertigens (Fall 1) beschreibt jede Form der Herstellung eines spezifischen Fälscherwerkzeugs oder -mittels. Darunter fällt zB auch das Programmieren von speziellen Fälschungsprogrammen.[2215]

2. Mischdelikt

Was das Verhältnis der Tathandlungen untereinander anlangt, so ist entgegen *Schroll*[2216] nicht bei sämtlichen Tatmodalitäten von kumulativen, dh selbstständigen, nicht austauschbaren, Varianten auszugehen. Richtig ist, dass das Anfertigen gegenüber den weiteren Tathandlungen eine selbstständige Handlung ist, die sich durch ihren Wert- und

2212 AA offensichtlich *Schroll* in WK² § 241c Rz 4 (Stand Mai 2005).
2213 Es gibt jedoch grundsätzlich auch kombinierte Geräte, die sowohl für Lese- als auch für Codierzwecke verwendet werden können.
2214 Siehe dazu bereits S 321 ff.
2215 Vgl *Reindl-Krauskopf,* Computerstrafrecht², 60; weiters *Schroll* in WK² § 241c Rz 6.
2216 Vgl *Schroll* in WK² § 241c Rz 5.

sozialen Sinngehalt von den anderen Tathandlungen unterscheidet. Wie auch bei § 241b handelt es sich aber bei den Tatmodalitäten, die ein An-sich-Nehmen und Besitzen beschreiben, also § 241c zweiter (arg »von einem anderen Übernehmen«), dritter (arg »Sich-Verschaffen«), sechster Fall (arg »Sonst-Besitzen«), um alternative, dh nicht selbstständige, austauschbare Tathandlungen. Insoweit stellt § 241c daher ein alternatives Mischdelikt dar. Die Subsumtion unter die falsche Variante begründet angesichts der Gleichwertigkeit dieser Formen des verbotenen Umgangs keine Urteilsnichtigkeit gem § 281 Abs 1 Z 10 StPO.

Die Gruppe der »Verbreitungshandlungen«, § 241c vierter (arg »einem anderen Verschaffen«) und fünfter (arg »einem anderen Überlassen«) Fall, beinhaltet im Innenverhältnis wiederum selbst gleichwertige Handlungsalternativen, die einen alternativen Mischtatbestand darstellen.

In Gesamtbetrachtung stellt sich daher folgende Struktur dar:

Die jeweiligen Begehungsweisen der Gruppe des Anfertigens (§ 241c Fall 1), der Gruppe des »An-sich-Nehmens/Besitzens« (Fälle 2, 3, 6) und der Gruppe der »Verbreitung« (Fälle 4, 5) stellen kumulative Handlungen dar. Innerhalb der Gruppen liegen jedoch alternative Tatmodalitäten vor.

3. Subjektive Tatseite

§ 241c ist ein Delikt mit überschießender Innentendenz. Neben dem (zumindest bedingten) Tatbildvorsatz ist ein (ebenfalls zumindest bedingter) erweiterter Vorsatz, »sich oder einem anderen eine Fälschung eines unbaren Zahlungsmittels zu ermöglichen«, erforderlich. Es handelt sich unter Einbeziehung der überschießenden Innentendenz deshalb um ein kupiertes Erfolgsdelikt, da das Endziel des Täters – »eine Fälschung zu ermöglichen« – objektiv tatbestandlich nicht (mehr) eintreten muss, um das Tatbild zu verwirklichen.[2217] Mit der Ausübung einer Tathandlung ist das Delikt bereits formell vollendet. Materiell ist die Tat erst beendet, wenn mit dem speziellen Werkzeug oder Fälschungsmittel die Fälschung oder Verfälschung eines unbaren Zahlungsmittels »möglich« wird. Verlangt wird aber in dieser überschießenden Innentendenz nicht, dass der Täter (oder ein anderer) ein

2217 Eine solche Einordnung wirkt sich ua ggf auf eine strafbare Beteiligung aus.

Falsifikat tatsächlich herstellen will. Enderfolg ist daher, dass der Täter selbst oder ein anderer durch das spezielle Mittel bloß in die Lage versetzt wird, eine Fälschung durchzuführen. Daraus folgt, dass dieses kupierte Erfolgsdelikt als (gewünschten) Enderfolg einen Gefährdungserfolg in Beziehung zum Tatobjekt des § 241a verlangt, da auch die überschießende (rein subjektive) Anforderung der inneren Tatseite nur vorsieht, dass es jemandem mit dem deliktsgegenständlichen Mittel oder Werkzeug möglich sein muss, ein Falsifikat herzustellen. Dass dies tatsächlich jemand tut, muss nicht vom Täter intendiert sein.

§ 241c tritt bei (versuchter) Verwirklichung des § 241a, zB durch das tatsächliche Herstellen eines Falsifikates, als »echtes« technisches Vorbereitungsdelikt kraft materieller Subsidiarität zurück.

Für die Gruppe der Bestimmungen gegen die Fälschung und Verfälschung bzw den Umgang mit Falsifikaten sieht § 241d – wie für Vorbereitungsdelikte grundsätzlich und iZm den Bestimmungen anderer Gewährschaftsträger (vgl insb § 226) üblich – einen persönlichen Strafaufhebungsgrund (»Tätige Reue«) vor.

Nach den Erl bedarf es dann nicht der Bestrafung des Täters, wenn dieser rechtzeitig und freiwillig die Gefahr des Gebrauchs des Falsifikats im Rechtsverkehr bzw die Gefahr der Verwendung der Falsifikate oder der Fälschungsmittel beseitigt. Darüber hinaus knüpfe dieser besondere Strafaufhebungsgrund daran an, dass die Pönalisierung des Vorbereitungsstadiums eine weitgehende Strafbarkeitsvorverlagerung bedeutet und es daher eines entsprechenden »Ventils« bedürfe.[2218]

E. Die Tätige Reue-Bestimmung des § 241d

> § 241d (1) Wegen einer der in den §§ 241a bis 241c mit Strafe bedrohten Handlungen ist nicht zu bestrafen, wer freiwillig, bevor das falsche oder verfälschte unbare Zahlungsmittel im Rechtsverkehr verwendet worden ist, durch Vernichtung des unbaren Zahlungsmittels, oder, bevor das Mittel oder Werkzeug zur Fälschung eines unbaren Zahlungsmittels verwendet worden ist, durch Vernichtung des Mittels oder Werkzeuges, oder auf andere Art die Gefahr einer solchen Verwendung beseitigt.

2218 Vgl ErlRV 309 BlgNR XXII. GP, 14.

> (2) Besteht die Gefahr einer solchen Verwendung nicht oder ist sie ohne Zutun des Täters beseitigt worden, so ist er nicht zu bestrafen, wenn er sich in Unkenntnis dessen freiwillig und ernstlich bemüht, sie zu beseitigen.[2219]

§ 241d Abs 1 gewährt die Tätige Reue demjenigen Täter, der freiwillig, bevor das falsche oder verfälschte unbare Zahlungsmittel im Rechtsverkehr verwendet worden ist, durch Vernichtung des unbaren Zahlungsmittels oder, bevor das Mittel oder Werkzeug zur Fälschung eines unbaren Zahlungsmittels verwendet worden ist, durch Vernichtung des Mittels oder Werkzeuges, oder auf andere Art die Gefahr einer solchen Verwendung beseitigt.

Abs 2 behandelt die »putative Tätige Reue«, bei der der Täter zumindest glaubt, eine noch bestehende Gefahr der Fälschungsverwendung, die allerdings objektiv gar nicht (mehr) besteht, zu beseitigen. Er muss in Bezug auf die tatsächliche Ungefährlichkeit aber in Unkenntnis, freiwillig und ernsthaft bemüht handeln. Die Formulierung entspricht im Wesentlichen dem Rücktritt vom Versuch nach § 16 Abs 2.

F. Entfremdung unbarer Zahlungsmittel (§ 241e)

> § 241e (1) Wer sich ein unbares Zahlungsmittel, über das er nicht oder nicht allein verfügen darf, mit dem Vorsatz verschafft, dass er oder ein Dritter durch dessen Verwendung im Rechtsverkehr unrechtmäßig bereichert werde, ist mit Freiheitsstrafe bis zu zwei Jahren zu bestrafen. Ebenso ist zu bestrafen, wer sich ein unbares Zahlungsmittel, über das er nicht oder nicht allein verfügen darf, mit dem Vorsatz verschafft, sich oder einem anderen eine Fälschung unbarer Zahlungsmittel (§ 241a) zu ermöglichen.
>
> (2) Wer die Tat gewerbsmäßig oder als Mitglied einer kriminellen Vereinigung begeht, ist mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren zu bestrafen.
>
> (3) Wer ein unbares Zahlungsmittel, über das er nicht oder nicht allein verfügen darf, mit dem Vorsatz, dessen Verwendung im Rechtsverkehr zu verhindern, vernichtet, beschädigt oder unterdrückt, ist mit Freiheitsstrafe bis zu einem Jahr zu bestrafen.[2220]

2219 BGBl 60/1974 idF I 15/2004.
2220 BGBl 60/1974 idF I 15/2004.

Mit § 241e wird Art 2 lit a des EU-RB 2001/413/JI zur Bekämpfung von Betrug und Fälschung iZm unbaren Zahlungsmitteln umgesetzt.[2221] Es handelt sich dabei um die »Entfremdung«[2222] in Bezug auf unbare Zahlungsmittel. § 241e Abs 1 erfasst zwei vorbereitende Verhaltensweisen.

1. Bereicherungsentfremdung und Fälschungsentfremdung

Zum einen stellt § 241e Abs 1 erster Satz die Entfremdung eines unbaren Zahlungsmittels zum Missbrauch desselben für unrechtmäßige Bereicherungszwecke unter Strafe. Zum anderen erfasst § 241e Abs 1 zweiter Satz das Sich-Verschaffen eines unbaren Zahlungsmittels zu Fälschungszwecken iSd § 241a.[2223]

In beiden Fällen muss es sich beim Tatobjekt um ein echtes unbares Zahlungsmittel handeln, das sich der Täter zu diesen Zwecken verschafft. Er darf über das unbare Zahlungsmittel keine (alleinige) Verfügungsbefugnis haben. Nicht kommt es dabei aber auf konkrete Eigentumsverhältnisse an, was sich insb dort auswirkt, wo der Aussteller (zB Bank) weiterhin zivilrechtlicher Eigentümer bleibt.[2224]

Auch ist zB die »eigene« Kreditkarte, die der Täter durch Täuschung des Ausstellers erlangt hat (arg »Sich-Verschaffen«), ein entfremdetes unbares Zahlungsmittel und daher auch Tatobjekt des § 241e.[2225] Die Tathandlung des Sich-Verschaffens[2226] indiziert in Bezug auf körperliche Gegenstände[2227] einen tatbestandsmäßigen Erfolg, da das unbare Zahlungsmittel seinen Inhaber wechselt bzw geänderte Sachherr-

---

2221 Rahmenbeschluss 2001/413/JI zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln vom 28. 5. 2001, ABl L 2001/149, 1.

2222 Der Begriff wurde deshalb gewählt, um nicht mit dogmatisch bereits besetzten Begriffen, wie etwa der Wegnahme iZm körperlichen Sachen des Diebstahls, welche Sachen mit Wertträgereigenschaft erfordert, Problemfelder zu eröffnen, können doch unbare Zahlungsmittel selbst entweder Wertträger (zB aufgeladener Cash-Chip) sein oder nicht (zB Bankomatkarte ohne aufgeladenen Cash-Chip); vgl ErlRV 309 BlgNR XXII. GP, 14.

2223 Siehe auch ErlRV 309 BlgNR XXII. GP, 14.

2224 Vgl ErlRV 309 BlgNR XXII. GP, 16; weiters *Bertel/Schwaighofer,* BT II[11] § 241e Rz 2; weiters *Reindl-Krauskopf,* Computerstrafrecht[2], 62.

2225 Siehe OGH 08. 11. 2006, 13 Os 103/06f; weiters *Schroll* in WK[2] § 241e Rz 7; aA *Bertel/Schwaighofer,* BT II[11] § 241e Rz 3.

2226 Vgl oben zu § 241b und § 126c.

2227 Anders bei der Tathandlung des Sich-Verschaffens bezüglich unkörperlicher Daten bzw Informationen (wie etwa Geheimnisse oder Zugangsdaten). Die bloße Kenntnisverschaffung von Zugangsdaten oder Geheimnissen – zB durch Lesen eines Schriftstücks oder eines Bildschirms – stellt eine schlichte Tätigkeit dar.

schaftsverhältnisse vorliegen. Insoweit stellt § 241e Abs 1 in beiden Sätzen bezüglich seiner tatbestandlichen Struktur ein Erfolgsdelikt dar.[2228] Die Strafbarkeit beider objektiv beschriebener Deliktsfälle gründet sich auf zwei verschiedenartig konzipierte überschießende Innentendenzen.[2229] Diesbezüglich kann bei § 241e Abs 1 von einem »subjektiven Mischtatbestand« gesprochen werden.

Die Tathandlung muss daher vom Täter – neben dem (zumindest bedingten) Tatbildvorsatz – entweder mit dem erweiterten (zumindest bedingten) Vorsatz gesetzt werden, dass er oder ein Dritter durch die Verwendung des entfremdeten unbaren Zahlungsmittels im Rechtsverkehr unrechtmäßig bereichert (erste subj Alt bzw § 241e Abs 1 erster Satz) oder dass ihm oder einem anderen eine Fälschung unbarer Zahlungsmittel (§ 241a) ermöglicht werde (zweiter subj Alt bzw § 241e Abs 1 zweiter Satz). Beide Deliktsfälle beschreiben daher auch kupierte Erfolgsdelikte, da das jeweilige Endziel (Bereicherung durch Verwendung des Tatobjekts bzw Fälschungsermöglichung) ein über den objektiven Tatbestand hinausreichender, vom Täter bloß angestrebter Erfolg ist, der nicht (mehr) tatbestandsmäßig ist.[2230] Mit einer solchen Konzeption wird der formelle Vollendungszeitpunkt auf die Tathandlung vorverlagert. Materiell ist die Entfremdung aber erst beendet, wenn die eine oder andere subjektive Zielvorstellung des Täters auch tatsächlich eintritt. Strafgrund ist daher eigentlich nicht das tatbestandsmäßige Verhalten des Täters samt Tatbildvorsatz, sondern der Inhalt des erweiterten Vorsatzes, nämlich das angestrebte Ziel als Enderfolg der Tat. Das Sich-Verschaffen eines unbaren Zahlungsmittels, über das man nicht oder nicht allein verfügen darf, ist daher an sich nicht strafbar, sondern wird es erst, wenn der Täter dadurch eines der (gewünschten) Ziele – entweder Bereicherung durch Verwendung des Tatobjekts oder Fälschungsermöglichung – erreichen will. Die Tathandlung muss aber objektiv für solche Zwecke geeignet sein. Es handelt sich daher iVm den Vorsatzinhalten um Quasi-Erfolgsdelikte, deren Vollendungszeitpunkt vorverlagert ist.[2231]

2228 Vgl *Oshidari* in SbgK § 241e Rz 2 (Stand April 2007).
2229 Siehe dazu auch OGH 18.10.2011, 12 Os 137/11f.
2230 Eine solche Einordnung wirkt sich ua ggf auf eine strafbare Beteiligung aus.
2231 Vgl dazu sinngemäß auch *Medigovic,* Unterlassung der Anzeige nach § 84 StPO – Amtsmißbrauch?, JBl 1992, 420.

Bei der subj Alternative der künftigen Bereicherung durch Verwendung (§ 241e Abs 1 erster Satz) des unbaren Zahlungsmittels kann der Zeitpunkt der formellen Vollendung mit dem der materiellen Beendigung zusammenfallen. Dies ist etwa bei der Entfremdung unbarer Zahlungsmittel der Fall, die gleichsam selbstständige (kombinierte) Wertträger sind (zB Bankomatkarte mit aufgeladenem Quick-Chip).[2232]

2. Vorbereitungshandlungen

Was die Beziehung des § 241e Abs 1 zu anschließenden Vermögensdelikten anlangt, stellen beide Deliktsfälle des Abs 1 strafbare Vorbereitungshandlungen dar, deren eigenständiger Deliktsunwert auch im Fall einer der Entfremdung zeitlich nachfolgenden Begehung eines Vermögensdeliktes durch denselben Täter mittels Verwendung des unbaren Zahlungsmittels oder Falsifikats nach § 241a fortdauert. Es liegt daher echte ungleichartige[2233] Konkurrenz vor, die sich auch aus der Unterschiedlichkeit der geschützten Rechtsgüter begründet, weil die Entfremdung eines unbaren Zahlungsmittels einen Angriff auf die Sicherheit des Rechts- und Zahlungsverkehrs mit unbaren Zahlungsmitteln darstellt, während sich die spätere missbräuchliche Verwendung dieses Zahlungsmittels gegen fremdes Vermögen richtet.[2234]

Ist ein kombinierter Wertträger (zB Bankomatkarte mit aufgeladenem Quick-Chip) Gegenstand einer Entfremdung, wobei es dem Täter nicht nur auf den etwaigen Wert auf dem Cash-Chip, sondern auch auf die Ausnützung sonstiger Funktionen der Bankomatkarte im unbaren Zahlungsverkehr zu einem späteren Zeitpunkt ankommt, liegt echte Idealkonkurrenz des § 241e Abs 1 mit zB §§ 127f vor.[2235]

Verschafft sich der Täter jedoch einen aufgeladenen Cash-Chip, der selbst ein unbares Zahlungsmittel darstellt, aber nicht auf einem anderen unbaren Zahlungsmittel wie zB einer Bankomatkarte oder Kredit-

2232 Siehe dazu auch *Schroll* in WK² § 241e Rz 10.

2233 Dh mehrere Delikte unterschiedlicher Art.

2234 Siehe dazu RIS-Justiz RS0119780 mwN; weiters *Sautner,* RZ 2004, 26.

2235 Vgl ErlRV 309 BlgNR XXII. GP, 14; weiters *Fabrizy,* StGB¹¹ § 241e Rz 4f; aA *Bertel/Schwaighofer,* BT II¹¹ § 241e Rz 2 und 7 sowie *Kienapfel/Schmoller,* StudB BT III² § 241e Rz 23 und 40: Strafbarkeit nur nach § 241e Abs 1 und nicht auch nach dem Vermögensdelikt, da dieser Vermögensaspekt nicht ins Gewicht fällt; *Plöckinger,* ÖJZ 2005/14, 256: Exklusivität; *Schroll* in WK² § 241e Rz 24 (Stand Mai 2005): Konsumtion.

karte angebracht ist, so ist das Konkurrenzverhältnis äußerst umstritten. Die GMat[2236], *Kienapfel/Schmoller*[2237] und *Bertel/Schwaighofer*[2238] geben in einem solchen Fall einzig dem Vermögensdelikt den Vorrang. *Plöckinger*[2239] und *Schroll*[2240] lassen wiederum das Vermögensdelikt zurücktreten. *Sautner*[2241] spricht von echter Idealkonkurrenz, für *Reindl-Krauskopf*[2242] sind beide letztgenannten Relationen denkbar. Solche massive Unklarheiten bezüglich des Konkurrenzverhältnisses sollten auf gesetzgeberische Ebene eindeutig geklärt werden.

3. Deliktsqualifikationen

§ 241e Abs 2 sieht bei einem gewerbsmäßig (iSd § 70) agierenden Täter oder bei Verwirklichung durch ein Mitglied einer kriminellen Vereinigung (iSd § 278 Abs 2) einen höhere Strafsatz (sechs Monate bis zu fünf Jahre Freiheitsstrafe) vor.

Eine gewerbsmäßige Verwirklichung erfordert die Absicht, sich durch wiederkehrende Begehung eine fortlaufende Einnahme zu verschaffen. Dem gewerbsmäßig handelnden Täter muss es daher darauf ankommen (§ 5 Abs 2), sich durch die Wiederholung von Straftaten desselben Deliktstyps eine zumindest für einen längeren Zeitraum wirksame Einkommensquelle zu erschließen, ohne dass diese regelmäßig und dauernd fließen muss. Unter einem »längeren Zeitraum« sind zumindest einige Wochen zu verstehen.[2243]

Diese Qualifikationsnorm bezüglich einer gewerbsmäßigen Begehung des § 241e Abs 1 ist – wie schon bei § 241a Abs 1[2244] angemerkt – im gesamten zwölften[2245] und dreizehnten[2246] Abschnitt des StGB ein systemwidriges Novum. Für keinen der in diesen Abschnitten des StGB

2236 Vgl ErlRV 309 BlgNR XXII. GP, 15.
2237 Vgl *Kienapfel/Schmoller,* StudB BT III² § 241e Rz 23 und 39.
2238 Siehe *Bertel/Schwaighofer,* BT II¹¹ § 241e Rz 2 und 7.
2239 Vgl *Plöckinger,* ÖJZ 2005/14, 256.
2240 Siehe *Schroll* in WK² § 241e Rz 24.
2241 Vgl *Sautner,* RZ 2004, 26.
2242 Vgl *Reindl-Krauskopf,* Computerstrafrecht², 64.
2243 Siehe OGH 08.06.2006, 15 Os 35/06w; vgl *Jerabek* in WK² § 70 Rz 7; vgl *Rainer* in SbgK § 70 Rz 19 mwN.
2244 Vgl § 241a Abs 2.
2245 Strafbare Handlungen gegen die Zuverlässigkeit von Urkunden und Beweiszeichen.
2246 Strafbare Handlungen gegen die Sicherheit des Verkehrs mit Geld, Wertpapieren, Wertzeichen und unbaren Zahlungsmitteln.

erfassten Gewährschaftsträger – mit Ausnahme der hier gegenständlichen unbaren Zahlungsmittel – ist eine Strafsatzerhöhung bei gewerbsmäßiger Begehung vorgesehen. Für eine kriminelle Vereinigung setzt § 278 Abs 2 voraus, dass der Zusammenschluss von mehr als zwei Personen (mit der in jener Bestimmung bezeichneten Ausrichtung) auf längere Zeit angelegt ist, einige Stunden oder Tage reichen daher dafür nicht aus.[2247] Ebenso genügt es bereits, dass sich diese Personengruppe zur Begehung auch nur einer einzigen entsprechend angeführten Straftat zusammengeschlossen hat.[2248]

4. Unterdrückung des unbaren Zahlungsmittels

Die Unterdrückung des (echten) unbaren Zahlungsmittels wird durch § 241e Abs 3 erfasst. Damit lehnte sich der Gesetzgeber an § 229 Abs 1 an.[2249] Strafbar macht sich derjenige, der ohne alleinige Verfügungsberechtigung ein unbares Zahlungsmittel iSd § 74 Abs 1 Z 10 mit dem Vorsatz, dessen Verwendung im Rechtsverkehr zu verhindern, vernichtet, beschädigt oder unterdrückt.

Von diesem Deliktsfall werden auch jene Fälle erfasst, in denen der Vorsatz des Täters zwar nicht die besonderen Zweckbestimmungen des Abs 1 umfasst, aber darauf ausgerichtet ist, die Verwendung des unbaren Zahlungsmittels durch den berechtigten Inhaber im Rechtsverkehr zu verhindern.[2250]

Da es sich bei unbaren Zahlungsmitteln per definitionem des § 74 Abs 1 Z 10 um körperliche Gegenstände handeln muss, erfordert ein Vernichten oder Beschädigen derselben die Einwirkung auf ihre Sachsubstanz. Es muss also das unbare Zahlungsmittel im Fall des Vernichtens überhaupt aufhören als solches zu existieren (zB durch Verbrennen).[2251] Wird aber lediglich die (unkörperliche) Software des Mikrochips eines entfremdeten Zahlungsmittels gelöscht oder verändert, ohne dass in die physische Integrität des Chips eingegriffen wird, ist daher in erster Linie[2252] an § 126a Abs 1 zu denken. Eine Beschädi-

2247 Vgl RIS-Justiz RS0125232 mwN.
2248 Siehe ErlRV 1166 BlgNR XXI. GP, 35.
2249 Vgl ErlRV 309 BlgNR XXII. GP, 17.
2250 Siehe dazu auch ErlRV 309 BlgNR XXII. GP, 17.
2251 Siehe dazu etwa *Kienapfel/Schroll* in WK² § 229 Rz 14 (Stand Juli 2006).
2252 § 225a wird idR nicht anwendbar sein, da der Täter hierbei die Verwendung der verfälschten Daten als Beweis gegenüber einem Menschen vor Augen haben muss.

gung eines unbaren Zahlungsmittels iSd § 241e Abs 3 Fall 3 liegt vor, wenn sein bestimmungsgemäßer Gebrauch durch eine Beeinträchtigung der Substanz oder des Inhalts eingeschränkt wird.[2253] Wesentliches Kriterium ist, dass das unbare (körperliche) Zahlungsmittel selbst unmittelbar beschädigt wird.

Im Zusammenhang mit einem Cash-Chip (zB elektronische Geldbörse), der nach hM ein unbares Zahlungsmittel darstellt[2254], bedeutet das aber, dass es darauf ankommt, den Mikrochip zu schädigen und nicht dessen Träger (zB Zerschneiden einer Plastikkarte, ohne dabei den aufgebrachten Mikrocontroller als Zahlungschip zu zerstören). In einem solchen Fall wäre das unbare Zahlungsmittel (Mikrochip) weder vernichtet noch beschädigt, wohl aber faktisch unbrauchbar gemacht, da durch die Zerstörung des Chip-Trägers die Verwendungsmöglichkeit des unbaren Zahlungsmittels in technischer Hinsicht idR nicht mehr gegeben ist. Der berechtigte Inhaber kann in weiterer Folge mangels Verwendbarkeit des Chips – aufgrund der Deformierung seines prinzipiell standardisierten Trägers in Ansehung der darauf abgestimmten Lesegeräte – keine elektronischen Datenverarbeitungsprozesse mehr auslösen. Ein »Sonst-Unbrauchbarmachen« – wie es bspw in § 126a Abs 1 Eingang gefunden hat – ist aber tatbestandlich nicht erfasst. Ebenso liegt auch keine »Unterdrückung« des unbaren Zahlungsmittels (§ 241e Abs 3 Fall 3) vor, da der berechtigte Inhaber weiterhin über den Mikrochip und daher das unbare Zahlungsmittel verfügen kann. Unter einem »Unterdrücken« versteht man generell die dauernde oder auch nur vorübergehende Zugriffsverhinderung, wobei sich das unbare Zahlungsmittel dabei in der tatsächlichen Verfügungsmacht des Täters befinden muss.[2255] Wer eine Plastikkarte mit Zahlungschip nur kurz an sich nimmt, um die Karte – ohne den Chip zu zerstören – zu zerschneiden, unterdrückt das unbare Zahlungsmittel (zB elektronische Geldbörse) nicht.[2256]

Trotz Hinweis in den GMat, dass durch die Normierung dieses Deliktsfalls allfällige Strafbarkeitslücken vermieden werden sollen, liegt eine solche vor.[2257]

2253 Vgl *Sikora,* Zahlungsverkehr, 126.

2254 Vgl dazu allerdings die bereits oben angeführte Kritik bzw *Birklbauer/Hilf/Tipold,* Strafrecht BT I² §§ 127, 128 Rz 15.

2255 Siehe etwa *Kienapfel/Schroll* in WK² § 229 Rz 23.

2256 Siehe sinngemäß *Kienapfel/Schroll* in WK² § 229 Rz 23.

2257 Siehe dazu auch ErlRV 309 BlgNR XXII. GP, 17.

Auch § 125 wäre in einem solchen Fall mangels eines objektiv bestimmbaren Werts der Plastikkarte selbst prinzipiell nicht anwendbar.[2258]

Alle drei Tathandlungen des § 241e Abs 3 indizieren tatbestandsmäßige Erfolge (Erfolgsdelikt) und sind rechtlich gleichwertig.[2259] Dass es sich in diesem deliktsspezifischen Zusammenhang – gerade was auch die Tathandlung des Unterdrückens betrifft – um ein alternatives Mischdelikt handelt, ergibt sich daraus, dass sich – im Gegensatz zu § 126a Abs 1[2260] – das jeweilige Ergebnis im Bezug habenden Sinngehalt stets gleich auf das hier gegenständliche Rechtsgut auswirkt. Wird ein unbares Zahlungsmittel vernichtet, beschädigt oder unterdrückt, so wirkt sich das gleichermaßen auf die Allgemeinheit und das Vertrauen in die Sicherheit und Zuverlässigkeit eines solchen Zahlungsverkehrs aus. Es geht in diesem Kontext nicht um individuelle Opferinteressen, sondern um die Institution der unbaren Zahlungsmittel selbst und deren Bestandsschutz.

In der Begehungsweise der Unterdrückung ist § 241e Abs 3 Fall 3 ein Dauerdelikt. Die Aufrechterhaltung der Zugriffsverhinderung gehört daher noch zum Tatbild. Das Delikt ist mit der nicht bloß geringfügigen Entziehung des unbaren Zahlungsmittels formell vollendet, aber erst dann materiell beendet, wenn der berechtigte Inhaber die Verfügungsmacht über das unbare Zahlungsmittel wieder erlangt hat.[2261]

Auf der subjektiven Tatseite wird – neben dem (zumindest bedingten) Tatbildvorsatz – eine überschießende Innentendenz des Täters (ebenfalls zumindest im Stärkegrad eines bedingten Vorsatzes) zum Tatzeitpunkt verlangt, durch eine der angeführten Tathandlungen die Verwendung des unbaren Zahlungsmittels im Rechtsverkehr zu verhindern. Es handelt sich daher bei § 241e Abs 3 unter Einbeziehung des erweiterten Vorsatzes (auch[2262]) um ein kupiertes Erfolgsdelikt. Der vom Täter bloß anvisierte Enderfolg besteht daher in der tatsächlichen Verhinderung des Gebrauchs des unbaren Zahlungsmittels seitens des Berechtigten.

2258 Vgl zB *Bertel/Schwaighofer,* BT I[12] § 125 Rz 7.
2259 Siehe anstatt vieler *Sikora,* Zahlungsverkehr, 126.
2260 Siehe S 270 ff.
2261 Vgl auch *Oshidari* in SbgK § 241e Rz 38.
2262 Dh neben dem durch Tatbestandsauslegung ermittelten Erfolg, welcher sich durch die Tathandlungen ergibt.

G. Die Tätige Reue-Bestimmung des § 241g

> § 241g (1) Nach den §§ 241e und 241f ist nicht zu bestrafen, wer freiwillig, bevor das entfremdete unbare Zahlungsmittel im Rechtsverkehr oder zur Fälschung eines unbaren Zahlungsmittels verwendet worden ist, durch Übergabe an die Behörde (§ 151 Abs. 3) oder auf andere Art die Gefahr einer solchen Verwendung beseitigt.
>
> (2) Besteht die Gefahr einer solchen Verwendung nicht oder ist sie ohne Zutun des Täters beseitigt worden, so ist er nicht zu bestrafen, wenn er sich in Unkenntnis dessen freiwillig und ernstlich bemüht, sie zu beseitigen.[2263]

Im Sinne des § 241g Abs 1 nicht zu bestrafen ist nur jener Täter, der freiwillig, bevor das entfremdete unbare Zahlungsmittel im Rechtsverkehr oder zur Fälschung eines unbaren Zahlungsmittels verwendet worden ist, durch Übergabe an die Behörde bzw auf andere Art (zB durch Übergabe an den Berechtigten) die Gefahr einer solchen Verwendung beseitigt. Obwohl unter der zur in § 241g formulierten Generalklausel nach den GMat auch die Rückgabe des entfremdeten unbaren Zahlungsmittels an den berechtigten Karteninhaber verstanden werden könne, weil dadurch die Gefahr einer missbräuchlichen Verwendung oder einer Verwendung zur Fälschung ebenfalls endgültig hintangehalten wäre[2264], ist eine Anwendung dieser Bestimmung lediglich auf § 241e Abs 3 Fall 3 (Unterdrückung) – analog zu § 229 Abs 2 – möglich.

Nach § 241e Abs 3 kommt es dem Täter nicht auf eine Verwendung des unbaren Zahlungsmittels, sondern um die Verhinderung der Verwendung durch den Berechtigten an. Ein Täter, der im Zeitpunkt der Entfremdung bereits mit eigenem Gebrauchsvorsatz handelt, ist gar nicht nach § 241e Abs 3, sondern nach § 241e Abs 1 zu bestrafen.[2265]

2263 BGBl 60/1974 idF I 15/2004.

2264 Vgl ErlRV 309 BlgNR XXII. GP, 18.

2265 Zum Verhältnis dieser beiden Bestimmungen führt der OGH aus: »Die gesetzlichen Tatbestände nach § 241e Abs 1 erster Fall StGB und nach Abs 3 leg cit stehen zueinander im Verhältnis der Exklusivität. Denn auf Grund der in beiden Tatbeständen enthaltenen widerstreitenden Merkmale in Bezug auf die subjektive Tatseite ist begrifflich unmöglich, dass ein Täter in Bezug auf ein entfremdetes unbares Zahlungsmittel zur selben Zeit die in diesen Bestimmungen enthaltenen unterschiedlichen Vorsatzrichtungen entwickelt. Begrifflich möglich ist jedoch eine Fallgestaltung, bei der vom Täter in einem Zugriff mehrere unbare Zahlungsmittel entfremdet werden und sein Vorsatz von vorne herein in Ansehung einzel-

Daher macht es auch keinen Sinn, dass – wie *Reindl-Krauskopf* es beschreibt[2266] – sich ein Täter, der in Unkenntnis einer solchen Verwendungsgefahr ist, § 241g Abs 2 entsprechend, um die Vernichtung des unbaren Zahlungsmittels freiwillig und ernstlich bemüht, da er in diesem Fall § 241e Abs 3 verwirklichen würde. § 241g Abs 2 (wie auch § 241g Abs 1) stellt ausdrücklich nicht auf die »Vernichtung« des unbaren Zahlungsmittels ab[2267], sondern beschreibt abstrakt die »Beseitigung der Verwendungsgefahr« (iS einer »putativen Tätigen Reue«).[2268] Da eine Vernichtung den Tatbestand des § 241e Abs 3 erfüllen würde, ist sie auch keine geeignete Reuehandlung iSd § 241g.[2269]

Insgesamt ist die Bestimmung über die Tätige Reue in § 241g iZm der Tathandlung der Unterdrückung (§ 241e Abs 3 Fall 3) systematisch – in Bezug auf § 229 Abs 2 – und auch teleologisch sinnvoll.

Hinsichtlich der Begehungsweisen der Vernichtung (§ 241e Abs 3 Fall 1) und Beschädigung (§ 241e Abs 3 Fall 2) trifft zwar der Wortlaut des § 241g Abs 1 und 2 grundsätzlich zu, da in beiden Fällen keine bzw kaum mehr[2270] Gefahr besteht, das unbare Zahlungsmittel im Rechtsverkehr zu verwenden. In den GMat wird aber selbst eine Vernichtung[2271] (und nur diese) des entfremdeten unbaren Zahlungsmittels als Reuehandlung des § 241g ausgeschlossen.[2272] Sinnvollerweise wäre doch wohl auch die Beschädigung (iSd § 241e Abs 3 Fall 2) eines solchen unbaren Zahlungsmittels als Reuehandlung auszunehmen. Man stelle sich zB vor, der Täter würde ein beschädigtes[2273] entfremdetes unbares Zahlungsmittel dem Berechtigten in »Tätiger Reue« (§ 241g)

---

ner dieser Zahlungsmittel auf die Zweckbestimmung des § 241e Abs 1 erster und zweiter Fall StGB und in Ansehung der restlichen Zahlungsmittel auf die Zweckbestimmung des Abs 3 leg cit gerichtet ist« (siehe OGH 02.03.2005, 13 Os 145/04 = JSt 2005/42, 201 *[Mitgutsch]*).

2266 Siehe *Reindl-Krauskopf,* Computerstrafrecht², 65.

2267 Siehe ErlRV 309 BlgNR XXII. GP, 18; weiters *Fabrizy,* StGB¹¹ § 241g Rz 1.

2268 Die Formulierung entspricht sinngemäß dem Rücktritt vom Versuch nach § 16 Abs 2.

2269 Vgl auch *Bertel/Schwaighofer,* BT II¹¹ § 241g Rz 1.

2270 Je nach Art der Beschädigung.

2271 Wie sie in § 241d ausdrücklich als Reuehandlung normiert ist.

2272 Vgl ErlRV 309 BlgNR XXII. GP, 18.

2273 Beispielsweise ein mit einem Hammer zerklopfter Mikrochip auf einer Plastikkarte.

zurückgeben[2274] und wäre wegen der Entfremdung (§ 241e Abs 1) und der Beschädigung (§ 241e Abs 3 Fall 3) nicht zu bestrafen.

Die Bestimmung über die Tätige Reue des § 241g ist daher mE in Bezug auf § 241e Abs 3 aus mehreren Gründen unschlüssig:

1. Der Täter nach § 241e Abs 3 strebt – ebenso wie bei »Inanspruchnahme« des § 241g Abs 1 und 2 – gar nicht an, das unbare Zahlungsmittel im Rechtsverkehr zu verwenden. Vielmehr noch will er dessen Verwendung bewusst verhindern.
2. § 241e Abs 3 erfasst keine Vorbereitungshandlungen zum Gebrauch entfremdeter unbarer Zahlungsmittel. Solche sind aber in der Systematik des StGB iZm Delikten der Urkunden-, Daten- und Geldfälschung (nun auch unbaren Zahlungsmitteln) sowie den Vermögensdelikten gerade der typische Grund für Tätige Reue-Bestimmungen.[2275]
3. Gerade wenn der Gesetzgeber davon ausgeht, dass für § 241g wesentlich sei, dass »die aus der Entfremdung eines unbaren Zahlungsmittels entstandene Gefahr für die Sicherheit des Rechts- und Zahlungsverkehrs mit unbaren Zahlungsmitteln, die in einer künftigen missbräuchlichen Verwendung oder Fälschung eines unbaren Zahlungsmittels liegt, (endgültig) beseitigt wird«, stellt sich die Frage, warum nicht gleich auch eine Beschädigung (iSd § 241e Abs 3 Fall 2) desselben, die idR[2276] ebenfalls zu einer endgültigen Beseitigung der Gefahr einer allfälligen missbräuchlichen Verwendung führt, nicht ausdrücklich – wie die Vernichtung – ausgeschlossen wurde. Eine solche wäre zwar iZm dem Universalrechtsgut der »Gefahr für die Sicherheit des Rechts- und Zahlungsverkehrs mit unbaren Zahlungsmitteln« – anders als bei den Bestimmungen über die Tätige Reue im Vermögensstrafrecht, wegen der dort verlangten vollständigen Schadensgutmachung – prinzipiell denkbar, würde aber genauso den Tatbestand des § 241e Abs 3 erfüllen, was sie als Reuehandlung ungeeignet erscheinen lässt.

2274 Im Fall eines entfremdeten unbaren Zahlungsmittels kann nach den GMat auch die Rückgabe desselben an den berechtigten Karteninhaber verstanden werden, wodurch die Gefahr einer missbräuchlichen Verwendung oder einer Verwendung zur Fälschung ebenfalls endgültig hintangehalten werden könne (vgl ErlRV 309 BlgNR XXII. GP, 18).

2275 Siehe ErlRV 309 BlgNR XXII. GP, 14 und 17.

2276 Gegebenenfalls vermag eine nur leichte Beschädigung eines unbaren Zahlungsmittels eine weitere missbräuchliche Verwendung nicht endgültig auszuschließen.

Meines Erachtens sind daher die Bestimmungen über die Tätige Reue nach § 241g Abs 1 und 2 jedenfalls nicht auf § 241e Abs 3 Fall 1 und 2 anwendbar. Für § 241e Abs 3 Fall 3 (arg »unterdrückt«) ergeben sie aber dennoch grundsätzlich Sinn.

H. Annahme, Weitergabe oder Besitz entfremdeter unbarer Zahlungsmittel (§ 241f)

> § 241f Wer ein entfremdetes unbares Zahlungsmittel mit dem Vorsatz, dass er oder ein Dritter durch dessen Verwendung unrechtmäßig bereichert werde, oder mit dem Vorsatz, sich oder einem anderen eine Fälschung unbarer Zahlungsmittel (§ 241a) zu ermöglichen, von einem anderen übernimmt, sich oder einem anderen verschafft, befördert, einem anderen überlässt oder sonst besitzt, ist mit Freiheitsstrafe bis zu einem Jahr zu bestrafen.[2277]

§ 241f entspricht in seinem Aufbau dem Deliktstypus des § 241b[2278], wobei deliktsspezifisch (echte) »entfremdete unbare Zahlungsmittel« als Tatobjekte intendiert sind und ergänzt § 241e als Anschlussdelikt, weil er alle einer Entfremdung nachfolgende Handlungen kriminalisiert.[2279] Damit wird ebenfalls – wie schon § 241b – der Umsetzung des Art 2 lit c des EU-RB 2001/413/JI Rechnung getragen.

Insbesondere ist daher auch der fortdauernde Besitz eines entfremdeten unbaren Zahlungsmittels strafbar.[2280] Dies gilt nicht nur für das im Anschluss an das Sich-Verschaffen iSd § 241e verwirklichte Besitzen durch den unmittelbaren Täter der Entfremdung, sondern grundsätzlich auch für den – vom entsprechenden Vorsatz getragenen – aufgedrängten Besitz, sofern der Besitzer diesen nicht umgehend aufgibt. Anders als § 241b verlangt aber der subjektive Tatbestand des § 241f, dass der Täter die Tathandlungen[2281] – neben dem (zumindest bedingten) Tatbildvorsatz entweder mit dem erweiterten Vorsatz begeht, dass er oder ein Dritter durch die Verwendung des Tatobjekts unrechtmä-

2277 BGBl 60/1974 idF I 15/2004.
2278 Hier werden »falsche oder verfälschte unbare Zahlungsmittel« thematisiert.
2279 Vgl *Schroll* in WK² § 241f Rz 1 mwN (Stand Mai 2005).
2280 Vgl *Kienapfel/Schmoller,* StudB BT III² §§ 241f–241g.
2281 Siehe dazu die Ausführungen zu § 241b.

ßig bereichert werde, oder alternativ mit dem erweiterten Vorsatz, sich oder einem anderen eine Fälschung unbarer Zahlungsmittel (iSd § 241a) zu ermöglichen.[2282] § 241f impliziert daher unter Berücksichtigung dieser beiden überschießenden Innentendenzen zwei alternative kupierte Erfolgsdelikte.[2283]

Wird sowohl § 241e als auch § 241f verwirklicht, tritt Letzterer als mitbestrafte Nachtat zurück.[2284] Der Unwert der Tat nach § 241f wird in diesem Fall bereits vollständig von der Haupttat erfasst.

V. Sexualbezogene Delikte mit IKT-Bezug

Die in diesem Abschnitt untersuchten Delikte dienen überwiegend dem Schutz der sexuellen Integrität und ungestörten sexuellen Entwicklung von Minderjährigen sowie der Bekämpfung der sexuellen Ausbeutung und der Kinderpornografie.

Die Informations- und Kommunikationstechnologie nimmt in diesem Deliktsbereich eine besondere Rolle ein, da sie technologiebedingt die Verbreitung und den Zugang zu multimedialem kinderpornographischem Material – wie insb Standbilder, Videos oder Liveübertragungen – erleichtert. Durch die IKT haben sich neue Verbreitungswege etabliert, die es den Strafverfolgungsbehörden aufgrund technischer Anonymisierungs- und Verschlüsselungsverfahren zunehmend erschweren, Straftaten aufzuklären und Täter zu verfolgen.

A. Pornographische Darstellungen Minderjähriger (§ 207a)

§ 207a (1) Wer eine pornographische Darstellung einer minderjährigen Person (Abs. 4)

1. herstellt oder

2. einem anderen anbietet, verschafft, überlässt, vorführt oder sonst zugänglich macht,

ist mit Freiheitsstrafe bis zu drei Jahren zu bestrafen.

2282 Das entspricht den überschießenden Innentendenzen des § 241e Abs 1 und 2.
2283 Siehe dazu die Ausführungen zu § 241e Abs 1.
2284 Siehe ErlRV 309 BlgNR XXII. GP, 17; *Kienapfel/Schmoller,* StudB BT III² §§ 241f–241g.

(2) Mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren ist zu bestrafen, wer eine pornographische Darstellung einer minderjährigen Person (Abs. 4) zum Zweck der Verbreitung herstellt, einführt, befördert oder ausführt oder eine Tat nach Abs. 1 gewerbsmäßig begeht. Mit Freiheitsstrafe von einem bis zu zehn Jahren ist zu bestrafen, wer die Tat als Mitglied einer kriminellen Vereinigung oder so begeht, dass sie einen besonders schweren Nachteil der minderjährigen Person zur Folge hat; ebenso ist zu bestrafen, wer eine pornographische Darstellung einer minderjährigen Person (Abs. 4) unter Anwendung schwerer Gewalt herstellt oder bei der Herstellung das Leben der dargestellten minderjährigen Person vorsätzlich oder grob fahrlässig gefährdet.

(3) Wer sich eine pornographische Darstellung einer mündigen minderjährigen Person (Abs. 4 Z 3 und 4) verschafft oder eine solche besitzt, ist mit Freiheitsstrafe bis zu einem Jahr zu bestrafen. Mit Freiheitsstrafe bis zu zwei Jahren ist zu bestrafen, wer sich eine pornographische Darstellung einer unmündigen Person (Abs. 4) verschafft oder eine solche besitzt.

(3a) Nach Abs. 3 wird auch bestraft, wer im Internet wissentlich auf eine pornographische Darstellung Minderjähriger zugreift.

(4) Pornographische Darstellungen Minderjähriger sind

1. wirklichkeitsnahe Abbildungen einer geschlechtlichen Handlung an einer unmündigen Person oder einer unmündigen Person an sich selbst, an einer anderen Person oder mit einem Tier,

2. wirklichkeitsnahe Abbildungen eines Geschehens mit einer unmündigen Person, dessen Betrachtung nach den Umständen den Eindruck vermittelt, dass es sich dabei um eine geschlechtliche Handlung an der unmündigen Person oder der unmündigen Person an sich selbst, an einer anderen Person oder mit einem Tier handelt,

3. wirklichkeitsnahe Abbildungen

a) einer geschlechtlichen Handlung im Sinne der Z 1 oder eines Geschehens im Sinne der Z 2, jedoch mit mündigen Minderjährigen, oder

b) der Genitalien oder der Schamgegend Minderjähriger,

soweit es sich um reißerisch verzerrte, auf sich selbst reduzierte und von anderen Lebensäußerungen losgelöste Abbildungen handelt, die der sexuellen Erregung des Betrachters dienen;

4. bildliche Darstellungen, deren Betrachtung – zufolge Veränderung einer Abbildung oder ohne Verwendung einer solchen – nach den Umständen den Eindruck vermittelt, es handle sich um eine Abbildung nach den Z 1 bis 3.

> (5) Nach Abs. 1 Z 1 und Abs. 3 ist nicht zu bestrafen, wer
>
> 1. eine pornographische Darstellung einer mündigen minderjährigen Person mit deren Einwilligung und zu deren eigenem Gebrauch herstellt oder besitzt oder
>
> 2. eine pornographische Darstellung einer mündigen minderjährigen Person nach Abs. 4 Z 4 zu seinem eigenen Gebrauch herstellt oder besitzt, sofern mit der Tat keine Gefahr der Verbreitung der Darstellung verbunden ist.[2285]

Die Strafbestimmung des § 207a ist mit Ausnahme von Abs 3a technik- bzw medienneutral formuliert.[2286] Das bedeutet, dass eigentlich nur § 207a Abs 3a – nach der hier vertretenen Auffassung – dem Computerstrafrecht im engen Sinn zugehörig ist, da dort expressis verbis auf eine Begehung im Internet abgestellt wird. Die übrigen Bestimmungen über pornographische Darstellungen Minderjähriger können aber bei entsprechendem Sachverhalt dem Computerstrafrecht iwS unterfallen.[2287] In welcher Form pornographische Darstellungen Minderjähriger nämlich vorliegen, ist unbeachtlich.[2288] Es kommen Fotos, Dias, Videofilme, aber auch sonstige Bild- oder Datenträger, wie CD-ROMs, DVDs, Computerspiele udgl in Betracht.[2289] Mangels Wirklichkeitsnähe können zB Schriften, Tonaufnahmen, Zeichnungen, Gemälde oder Plastiken nicht erfasst werden.[2290] Wobei es bspw bei Schriften oder Tonaufnahmen schon an den entsprechenden »Abbildungen« (»bildliche« Darstellung) scheitert.[2291] Es handelt sich um visuell wahrnehmbare Darstellungen. Somit ist die österr Strafbestimmung – wie auch die RL 2011/93/EU – weiter, als die Vorgabe aus der CCC, die in Art 9 bei sämtlichen zu krimina-

---

2285 BGBl 60/1974 idF I 40/2009.

2286 Daher reicht die Umsetzung des Art 9 CCC (»Offences related to child pornography«) auch weiter als die Vorgabe (vgl ErlStV 1645 BlgNR XXIV. GP, 5).

2287 Insbesondere wäre auch an die Generierung »virtueller Pornographie« iSd § 207a Abs 4 Z 4 zu denken; ebenfalls an die Weitergabe von inkriminierten Dateien an Dritte über das Internet zB per E-Mail, Website bzw Filesharing-Systeme oder Chatrooms.

2288 Siehe *Schmölzer* in Bergauer/Staudegger, Recht und IT, 1 (21 f) mwN; weiters *Reindl-Krauskopf,* Computerstrafrecht², 41.

2289 Vgl ErlRV 294 BlgNR XXII. GP, 21; weiters JAB 1848 BlgNR XVIII. GP, 1 und 3; ausf *Schmölzer,* Internet und Strafrecht, in BMJ (Hrsg), Strafrechtliche Probleme der Gegenwart. 26. Strafrechtliches Seminar 1998 (1998) 129 (169 ff); weiters *Hinterhofer* in SbgK § 207a Rz 27.

2290 Siehe *Hinterhofer* in SbgK § 207a Rz 27 mwN; weiters *Bertel/Schwaighofer,* BT II¹¹ § 207a Rz 2.

2291 Vgl JAB 1848 BlgNR XVIII. GP, 1; weiters *Philipp* in WK² § 207a Rz 8.

lisierenden Tathandlungen auf die Begehung über ein Computersystem abstellt. Es werden daher nachfolgend lediglich hier interessierende technikbezogene Aspekte dieser Bestimmung behandelt.

§ 207a Abs 1 beinhaltet in der durch das Zweite Gewaltschutzgesetz[2292] geänderten Fassung das Verbot der Herstellung (Z 1), des einem anderen Anbietens, Verschaffens, Überlassens, Vorführens oder Sonst-Zugänglichmachens (Z 2) von pornographischen Darstellungen einer minderjährigen Person.

Abs 1 umfasst daher sämtliche minderjährigen Personen iSd § 74 Abs 1 Z 3, nämlich Personen, die das achtzehnte Lebensjahr noch nicht vollendet haben. Das sind sowohl mündige als auch unmündige Personen (iSd § 74 Abs 1 Z 1).

1. Pornographische Darstellungen

Pornographische Darstellungen Minderjähriger[2293] werden in § 207a Abs 4 definiert und sind – mit Ausnahme der sog »virtuellen Pornographie«[2294] des Abs 4 Z 4, wo es nur um den Anschein solcher Abbildungen geht, »wirklichkeitsnahe Abbildungen«. Dass solche Darstellungen auch informationstechnisch verarbeitbare Dateien sein können, wurde bereits an anderer Stelle nachgewiesen.[2295] All diesen Abbildungen wesentlich ist deren Wirklichkeitsnähe. Die Abbildungen müssen daher von einer derartigen Qualität sein, dass der Betrachter den Eindruck hat, er sei Augenzeuge gewesen.[2296]

§ 207a Abs 4 Z 1 beschreibt die sog »Realpornographie«, dh wirklichkeitsnahe Abbildungen einer geschlechtlichen Handlung mit unmündigen bzw mündig minderjährigen Personen[2297] (§ 207a Abs 4 Z 3 lit a erster Fall), die tatsächlich stattgefunden hat.[2298]

2292 BGBl I 40/2009.

2293 Es handelt sich um ein normatives Tatbestandsmerkmal, das zwecks rechtsrichtiger Subsumtion der Wertausfüllung bedarf (vgl OGH 04.10.2011, 14 Os 107/11h; OGH 15.01.2009, 12 Os 151/08k).

2294 Zum Begriff siehe ErlRV 294 BlgNR XXII. GP, 22.

2295 Näheres dazu bei *Schmölzer* in Bergauer/Staudegger, Recht und IT, 1 (21f); vgl ErlRV 294 BlgNR XXII. GP, 21.

2296 Vgl ErlRV 294 BlgNR XXII. GP, 21; weiters *Philipp* in WK² § 207a Rz 8; *Bertel/Schwaighofer,* BT II¹¹ § 207a Rz 2; auch *Hinterhofer* in SbgK § 207a Rz 27.

2297 Personen, die bereits das vierzehnte, aber noch nicht das achtzehnte Lebensjahr vollendet haben (siehe ErlRV 294 BlgNR XXII. GP, 20).

2298 Siehe weiterführend *Philipp* in WK² § 207a Rz 9f.

§ 207a Abs 4 Z 2 behandelt die sog »Anscheinspornographie«, dh wirklichkeitsnahe Abbildungen eines Geschehens mit unmündigen bzw mündig minderjährigen Personen (§ 207a Abs 4 Z 3 lit a zweiter Fall), deren Betrachtung den Eindruck vermittelt, als handle es sich um eine geschlechtliche Handlung iSd Z 1. Eine solche geschlechtliche Handlung muss aber nicht tatsächlich stattgefunden haben.

§ 207a Abs 4 Z 3 lit b befasst sich mit wirklichkeitsnahen Abbildungen der Genitalien oder der Schamgegend Minderjähriger, wenn sie reißerisch verzerrt, auf sich selbst reduziert und von anderen Lebensäußerungen losgelöst sind und der sexuellen Erregung des Betrachters dienen.[2299]

§ 207a Abs 4 Z 4 pönalisiert bildliche Darstellungen, deren Betrachtung nach den Umständen den Eindruck vermittelt, es handle sich um eine Abbildung eines tatsächlichen Geschehens nach den Z 1 bis 3. Dabei muss eine bestehende Abbildung (computertechnisch) manipuliert oder eine Darstellung vollkommen künstlich, aber täuschend realistisch geschaffen worden sein, ohne dass eine echte Abbildung verwendet wurde (zB rein computergenerierte [auch -animierte], real wirkende Bilder).[2300]

Die Tathandlungen des § 207a Abs 1 Z 2[2301] indizieren prinzipiell ein alternatives Mischdelikt, weil im Sinne eines umfassenden Rechtsgutschutzes alle Handlungen umfasst werden, durch die die inkriminierten Darstellungen zur Kenntnis Dritter gelangen können; vor allem die Verbreitung im Wege aktueller Informationstechnologie.[2302]

2. Mischdelikt

Was die Tathandlung des »Anbietens« betrifft, handelt es sich um keine vollständig gleichwertige Tathandlung, da sie noch eine die tatsächliche Weitergabe der Abbildung (zeitlich) vorgelagerte Tätigkeit[2303] (iSd

2299 Siehe ausf *Hinterhofer* in SbgK § 207a Rz 38 ff.

2300 Vgl ErlRV 294 BlgNR XXII. GP, 22; weiters *Bertel/Schwaighofer,* BT II[11] § 207a Rz 7; vgl auch *Reindl-Krauskopf,* Computerstrafrecht[2], 41.

2301 Nicht aber das »Herstellen« von pornographischen Darstellungen Minderjähriger in Z 1.

2302 Vgl OGH 01.04.2008, 11 Os 21/08k (11 Os 22/08g) mwN = jusIT 2008/82, 175 *(Bergauer)*.

2303 Es handelt sich bei § 207a Abs 1 Z 2 erster Fall auch um ein schlichtes Tätigkeitsdelikt (vgl *Hinterhofer* in SbgK § 207a Rz 12).

Anbahnung einer Weitergabe) beschreibt. Alle weiteren Handlungen betreffen tatsächliche Weitergaben bzw Zugänglichmachungen.[2304] Ein »Anbieten« impliziert nicht den sofortigen Zugang (bzw die Zugriffsmöglichkeit) zu den tatbildlichen Darstellungen, sondern die Anbahnung, in einem nächsten Schritt erst den Zugang ggf gegen Entgelt zu gewähren, wie zB durch die Aufforderung zur Kontaktaufnahme mit dem Anbieter in einem Zeitungs- bzw Internetinserat, oder aber in geschlossenen Chatrooms oder anderen (zugangsbeschränkten) Internetseiten, wobei erst nach etwaiger Aushandlung der Gegenleistung[2305] die einschlägigen Bilder zugänglich gemacht werden.[2306] In diesem Sinn wäre das Versenden eines Hyperlinks via E-Mail, der lediglich auf eine Internetseite mit dem verbotenen Material referenziert, als ein Anbieten iSd § 207a Abs 1 Z 2 erster Fall zu verstehen (denn der Täter weist dabei auf das über ihn beschaffbare Material hin). Dabei genügt mE die Erstellung des Angebots (zB via Inserat im Internet), die Annahme desselben ist nicht ausschlaggebend. Das Veröffentlichen der verpönten pornographischen Darstellungen auf einer einschränkungslos erreichbaren Internetseite ohne expliziten Hinweis des Täters auf die verpönten Inhalte und ohne weitere Zugriffsschranke, wäre dann als subsidiäres »Sonst-Zugänglichmachen« iSd § 207a Abs 1 Z 2 fünfter Fall zu beurteilen. In diesem Deliktsfall wird aber auf das faktische Zugänglichsein des verbotenen Inhalts und nicht schon auf die Erklärung des Täters zur Bereitstellung (= anbieten) abgestellt werden müssen.[2307]

Es ist daher davon auszugehen, dass das »Anbieten« eine kumulative Tatbestandsalternative zu den anderen Tathandlungen des § 207a Abs 1 Z 2 ist. Das Anbieten stellt nämlich eine Vorbereitungshandlung des anschließenden »Verschaffens, Überlassens, Vorführens oder Sonst-Zugänglichmachens« dar, weshalb es auch bei Vorliegen einer der tatsächlichen Handlungen des Zugänglichmachens hinter diese zurücktritt (materielle Subsidiarität). Es wäre nicht adäquat, jemanden wegen des Anbietens von inkriminierten Darstellungen, die

2304 Vgl *Bergauer,* Verbreitung von Kinderpornografie und verbotene Veröffentlichung über das Internet, jusIT 2008/82, 175; weiters *Schmölzer* in Bergauer/Staudegger, Recht und IT, 1 (24).

2305 Dabei muss es sich nicht um eine finanzielle Gegenleistung handeln.

2306 In diesem Sinn wohl auch *Kienapfel/Schmoller,* Grundriss des österreichischen Strafrechts. Besonderer Teil III (1999) § 207a Rz 18.

2307 Vgl *Bergauer,* jusIT 2008/82, 175; weiters *Schmölzer* in Bergauer/Staudegger, Recht und IT, 1 (24).

er selbst zu diesem Zeitpunkt noch gar nicht besitzt, aber beschaffen könnte, gleich zu bestrafen wie jemanden, der tatsächlich das Bildmaterial einem anderen zugänglich macht.

Sämtliche Fälle des § 207a Abs 1, die im Wesentlichen auf Produzenten und Distributoren abzielen, werden mit Freiheitsstrafe bis zu drei Jahren sanktioniert.

§ 207a Abs 2 sieht lediglich für Handlungen, die unter Abs 1 zu subsumieren sind, Qualifikationen vor. Solche gibt es für die »Konsumentenstrafbarkeit« nach § 207a Abs 3 und 3a nicht.[2308]

3. Qualifikation des Abs 1

Nach § 207a Abs 2 Satz 1 sind das Herstellen zum Zweck der Verbreitung, das Einführen, Befördern und Ausführen sowie die gewerbsmäßige Begehung des Abs 1 mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren bedroht.

Ein Herstellen zum Zweck der Verbreitung könnte etwa vorliegen, wenn ein Dritter eine geschlechtliche Handlung, an der ein Minderjähriger mitwirkt, fotografiert oder filmt, um das Produkt im Internet oder per Handy zu verbreiten. Ein derartiger Fall fällt unter das Phänomen »Happy Slapping«, das im Wesentlichen darin besteht, dass meist jugendliche Personen andere misshandeln, erniedrigen, verletzen, vergewaltigen usw, wobei diese Handlungen mit Kameras oder Mobiltelefonen aufgezeichnet werden, um diese Aufnahmen anderen per E-Mail, MMS oder über das Internet zugänglich zu machen.[2309]

Auch fällt darunter das heimliche Aufzeichnen von sexuellen Handlungen, die von den Beteiligten freiwillig vorgenommen werden, um das Bildmaterial zB über soziale Netzwerke wie Facebook, Mobiltelefonen, Internetsites usw anderen zugänglich zu machen.[2310]

Wird eine pornographische Darstellung zum Zweck der Verbreitung hergestellt, wird die Tat gem § 207a Abs 2 Satz 1 Fall 1 qualifiziert begangen und strenger bestraft.

2308 Siehe auch *Hinterhofer* in SbgK § 207a Rz 63.

2309 Vgl 82/ME XXIV. GP, 7.

2310 In 82/ME XXIV. GP wurde ein eigener »Happy Slapping«- bzw »Paparazzi«-Tatbestand in § 120a unter der Bezeichnung »Verletzung schutzwürdiger Geheimhaltungsinteressen durch Bildaufnahmen« angedacht. Nach einer kontroversen Diskussion im Begutachtungsverfahren wurde allerdings noch kein neuer Entwurf vorgelegt.

Die Verbreitung verlangt idZ keine »Massenverbreitung«. Das Produkt muss lediglich einem anderen zugänglich gemacht werden.[2311] Auf der inneren Tatseite indiziert die Wendung »zum Zweck«, dass der Täter mit einem erweiterten Vorsatz im Stärkegrad der Absicht (iSd § 5 Abs 2) handeln muss, die Darstellungen zu verbreiten.[2312]

Auch die gewerbsmäßige Begehung der Tat nach Abs 1 wird durch § 207a Abs 2 Satz 1 Fall 4 qualifiziert. Der Täter muss die Tat in der Absicht begehen, sich durch die wiederkehrende Begehung eine fortlaufende Einnahme zu verschaffen (§ 70).

Darüber hinaus sehen § 207a Abs 2 Satz 2 und Satz 3 weitere strafsatzerhöhende Umstände vor.[2313]

4. Sich-Verschaffen und Besitzen inkriminierter Bilder

§ 207a Abs 3 behandelt – neben § 207a Abs 3a – die Konsumentenstrafbarkeit, in dem die Bestimmung auf das Sich-Verschaffen bzw Besitzen einer pornographischen Darstellung einer mündigen (Satz 1) bzw unmündigen (Satz 2) minderjährigen Person abzielt. Dafür ist in Satz 1 eine Strafdrohung mit bis zu einem Jahr bzw in Satz 2 bis zu zwei Jahren Freiheitsstrafe vorgesehen. Der Täter muss dabei im Tatzeitpunkt wenigstens mit dolus eventualis handeln. Strafbar soll in diesem Zusammenhang nur der Besitz oder eine auf einen solchen ausgerichtete Verschaffungshandlung sein, nicht aber das bloße Betrachten.[2314] Beide Handlungen verlangen Unmittelbarkeit, dh ein Link (Verweis) zu inkriminierten Bildern, der im Browser unter den Favoriten bzw Lesezeichen abgespeichert ist, stellt keinen Besitz derselben dar. In diesem Sinn verschafft sich auch niemand ein solches Material, wenn er sich bloß den Link darauf abspeichert, ohne sich die Darstellungen selbst herunterzuladen.

2311 Siehe *Philipp* in WK² § 207a Rz 19 mwN.

2312 Vgl *Hinterhofer* in SbgK § 207a Rz 52.

2313 Zu Überlegungen bezüglich weiterer Qualifikationstatbestände insb zur »Beförderung« von Computerdateien iSd (Abs 2 Satz 1 Fall 3) siehe *Reindl-Krauskopf,* Computerstrafrecht², 43.

2314 Vgl JAB 1848 BlgNR XVIII. GP, 3.

a. Gewahrsamserlangung und Körperlichkeit

Gleichwohl verschafft sich aber pornographische Darstellungen Minderjähriger, wer sich derartiges Material aus dem Internet (aktiv) herunterlädt und auf der Festplatte speichert.[2315] Der Täter muss sich daher die inkriminierten Abbildungen durch eigenes Aktivwerden in sein Gewahrsam zuführen. Nach dem JA verschafft sich jemand ein Tatobjekt, wer daran (durch eigenes) Zutun »Gewahrsam« erlangt. Die Tathandlung setzt einen Bezug zu einem »körperlich fassbaren« Gegenstand voraus[2316], weshalb man auch von einem ungeschriebenen Tatbildmerkmal »Gewahrsam« bzw »Gewahrsamsbegründung« ausgehen muss.

Dieser Bezug wird in praxi idR durch das Abspeichern auf einen (eigenen) Datenträger hergestellt. Die bloße technisch bedingte – vom Nutzer unbeeinflusste – Vervielfältigung der Abbildung im Arbeitsspeicher[2317] oder die automatische Zwischenspeicherung im Internet-Cache sind grundsätzlich nicht der Tathandlung des Sich-Verschaffens unterzuordnen, da der Täter die inkriminierten Dateien nicht bewusst abspeichert, um sie sich zu verschaffen.[2318] Wüsste der Täter aber, dass durch das Aufrufen der Webseite mit den inkriminierten Darstellungen, diese Bilddateien automatisch auf seiner Festplatte im (temporären) Internet-Cache-Ordner abgespeichert würden, und strebt er an, in weiterer Folge über diese Dateien zu disponieren, dann wäre der Aufruf der Internetseite mit einer aktiven Abspeicherung gleichzusetzen.[2319] Selbst wenn der Täter wüsste, dass die Daten dabei lediglich flüchtig im Arbeitsspeicher abgelegt würden und er sie nur kurzzeitig (nämlich bis zum Beenden der entsprechenden Anwendung, die ihm eine Betrachtung der Bilder ermöglicht) verwenden könnte, wäre das Sich-Verschaffen durch die bloße Gewahrsamserlangung vollendet. Auf eine Dauerhaftigkeit und die Kriterien eines etwaigen anschließenden Besitzes kommt es hier nicht an. Betrachtet man das Tatobjekt (§ 207a Abs 4) genauer, fällt auf, dass die technische Aufbereitung der pornographischen Darstellungen Minderjähriger – wie oben bereits

2315 Siehe etwa *Hinterhofer* in SbgK § 207a Rz 58.
2316 Vgl JAB 106 BlgNR XXIV. GP, 33; vgl JAB 1848 BlgNR XVIII. GP, 3.
2317 Siehe JAB 1848 BlgNR XVIII. GP, 3.
2318 Zum reinen Betrachten beachte aber § 207a Abs 3a.
2319 In diesem Sinne, aber auf die Tathandlung des »Besitzes« bezogen, auch *Reindl-Krauskopf,* Computerstrafrecht², 42.

angeführt – unbeachtlich ist. Daher sind auch sämtliche (technische) Darstellungsformen von der Strafbestimmung erfasst.

Der »Bezug zu einem körperlich fassbaren Gegenstand«[2320] ist jedenfalls dann unproblematisch gegeben, wenn die inkriminierten Darstellungen unverrückbar mit ihrem Trägerkörper verbunden sind (zB konventionelle Fotos, [einmal beschreibbare] CD-ROMs, DVD-ROM). In diesem Fall verschafft sich der Täter körperliche Gegenstände, die er vorher noch nicht in seinem Gewahrsam hatte, weshalb er auch neuen Gewahrsam an diesen Materialien begründet. In diesem Sinn kann sich jemand auch einen USB-Stick oder eine externe Festplatte mit den gegenständlichen Bildern verschaffen, wenn er diese Medien nicht selbst für die Verkörperung der Kopien bereitgestellt hat.

Speichert der Täter aber inkriminierte Bilddaten – wie es in den GMat idZ selbst als Beispiel genannt wird[2321] – aus dem Internet auf seiner Festplatte ab oder kopiert er sich die Dateien auf seinen USB-Stick, so wird nicht der ursprüngliche Träger (samt Daten) in das Gewahrsam des Täters überführt, sondern die Computerdaten selbst. Diese befinden sich nach dem Sich-Verschaffen auf einem anderen Datenträger, der vom Täter selbst bereitgestellt wurde und bereits in seinem Gewahrsam ist. Für eine Datenübertragung von A nach B, wobei es gleichgültig ist, ob diese über Netzwerke oder lokale Laufwerke erfolgt, geht die bisherige auf einem Datenträger fixierte Verkörperung der Kopie der Datenvorlage für den Übertragungsvorgang verloren, da sie in mehrere Datenpakete aufgeteilt und zum Zielort transportiert wird, wobei stets – technisch und physikalisch bedingt – eine dynamische Verkörperung der übertragenen Datenpakete zu jedem Zeitpunkt notwendig ist. Am Zielort wird die Datei durch Reassemblierung der Datenpakete wieder zusammengesetzt. Am körperlichen »ursprünglichen«[2322] Datenträger (aber auch an den dynamischen Trägerkörpern) samt Daten (zB Festplatte des Servers im Internet) wird kein Gewahrsam begründet. Nachdem Gewahrsam nach hM aber nur an körperlichen Sachen begründet werden kann, stellen sich mehrere Fragen:

Kann man an einem bereits in seinem Gewahrsam befindlichen Gegenstand überhaupt erneut Gewahrsam begründen? Akzeptiert der

2320 Vgl JAB 1848 BlgNR XVIII. GP, 3.
2321 Siehe JAB 106 BlgNR XXIV. GP, 33; vgl JAB 1848 BlgNR XVIII. GP, 3.
2322 Der klarerweise nicht der tatsächliche originäre Datenträger sein muss und daher nur für diese Datenübertragung als der ursprüngliche Datenträger angesehen wird.

Gesetzgeber durch die Formulierung in den GMat »Bezug zu einem körperlich fassbaren Gegenstand«[2323] – da er nicht vom körperlichen Gegenstand selbst spricht – jeden Datenträger als eine Art »technischen Gewahrsamsdiener« oder »Gewahrsamsmittler«? Wäre es nicht angezeigt, in Anbetracht der Virtualität und Ubiquität von elektronischen Daten neue angepasste Wege im Strafrecht zu beschreiten und im gegenständlichen Zusammenhang einzig – anstelle des Erfordernisses des Gewahrsams an körperlichen Sachen – von der uneingeschränkten Verfügungsgewalt bzw -möglichkeit über die Daten auszugehen?

Stellt man sich vorab die Frage, was eigentlich durch § 207a Abs 3 erfasst werden soll, so klären die GMat, dass dadurch der Besitz oder eine auf einen solchen ausgerichtete Verschaffungshandlung pönalisiert sein soll, nicht aber das bloße Betrachten.[2324]

Daraus folgt im Wesentlichen nur, dass der Täter durch diese Handlung die tatsächliche und unmittelbare Herrschaft über die Sache ausüben können muss. Er reicht nicht aus, dass das Tatobjekt nur in seinen Wahrnehmungsbereich gelangt. Dass der ratio dieser Bestimmung nur durch die Erlangung einer körperlichen Sache Rechnung getragen werden kann, ist – gerade im hier interessierenden Zusammenhang mit Computerdaten – unzutreffend. Dies folgt auch schon daraus, dass der Täter für die Tathandlung des Sonst-Zugänglichmachens (Abs 1 Z 2 Fall 5) das Tatobjekt auf solche Weise in den »Wahrnehmungsbereich« oder Herrschaftsbereich eines anderen gelangen lassen muss, dass dieser die unmittelbare Zugriffsmöglichkeit (iSd faktischen Gewahrsamsbegriffs[2325]) auf die Sache selbst und damit auch die Möglichkeit der Kenntnisnahme ihres Inhalts erlangt (zB die Übergabe einer unverschlossenen Fotosammlung an einen anderen zum Transport oder zur Aufbewahrung).[2326]

Wenn schon für die Tathandlung des Zugänglichmachens keine Gewahrsamsverschaffung im klassischen Sinn notwendig ist, sollte wohl auch bei der des Sich-Verschaffens die »unmittelbare Zugriffsmöglichkeit« auf das Tatobjekt selbst ausschlaggebend sein. Damit wäre jedenfalls das Problem der Gewahrsamsbegründung an der eigenen Sache

2323 Vgl JAB 1848 BlgNR XVIII. GP, 3.
2324 Vgl JAB 1848 BlgNR XVIII. GP, 3.
2325 Siehe dazu zB *Hochmayr,* Besitz, 65 ff.
2326 Vgl JAB 1848 BlgNR XVIII. GP, 2.

beseitigt und die Tathandlung auch hins moderner informationstechnischer Darstellungsformen der Tatobjekte angemessen. Das Sich-Verschaffen sollte daher lediglich auf den Vorgang des »An-sich-Bringens« der Inhalte abstellen, gleichgültig wodurch sie letztlich verkörpert werden. Wenn der Täter die umfassende Verfügungsmöglichkeit über die Dateien erlangt hat, hat er sie sich tatbildlich verschafft. Der Wortlaut deckt jedenfalls auch eine solche Auffassung ab. Zudem geht die Gefährlichkeit nicht vom Datenträger, sondern von den Daten (genauer gesagt der Information) aus. In der modernen IKT spielen nämlich die Trägermedien stets eine untergeordnete Rolle, viel bedeutender ist die faktische Verfügungsgewalt über die Daten, die anderes als bei körperlichen Gegenständen nicht (nur) durch die unmittelbare Herrschaft über den Datenträger gegeben ist.

Ist man hingegen – wie offenbar der historische Gesetzgeber – der Meinung, dass es auf die Erlangung eines körperlichen Datenträgers ankomme, so muss geprüft werden, ob bei Bereitstellung des Datenträgers durch den Täter selbst überhaupt »neuer Gewahrsam« daran begründet werden kann.

Damit sich dies schlüssig begründen lässt, müsste man wohl auf die Eigenschaft des Datenträgers vor und nach der Tat abstellen. Vor der Tat handelt es sich bei diesem bereitgestellten Datenträger zB um eine sozial adäquate Festplatte mit einem sozial adäquaten Inhalt. Nach der Tat bleibt zwar die Festplatte an sich in ihrer Funktionalität und physischen Beschaffenheit weiterhin (sozial adäquat) unverändert, bezüglich ihres Inhalts trägt sie nun aber einen neuen (sozial inadäquaten) Informationswert, der sie insgesamt – solange diese Daten dort vorhanden sind – zu einem anderen, gefährlichen Datenträger konvertieren lässt. Die GMat weisen ebenfalls in eine solche Richtung, wenn davon gesprochen wird, dass wer eine bildliche Darstellung auf die Festplatte abspeichert, »damit ein mögliches Objekt für unerlaubten Besitz oder unerlaubte Weitergabe schafft«.[2327]

Man müsste daher argumentieren, dass durch diese vom Täter veranlasste Adaption durch Hinzufügen unrechtsbeladener Tatobjekte ein quasi »neuer Datenträger« mit anderer Eigenschaft geschaffen wurde, der nunmehr originär »gewahrsamserlangungsfähig« wird. Dies erscheint iZm der Tathandlung des Sich-Verschaffens nicht sachgerecht,

2327 Siehe JAB 106 BlgNR XXIV. GP, 34.

da der Täter den Gewahrsam an der Festplatte in keiner Sekunde aufgegeben hat (diese hat weder ihren räumlichen Aufstellungsort verlassen noch wurde sie jemandem übergeben bzw Rechte daran anderen übertragen) und daher eine Neubegründung schlicht nicht möglich ist. Ein solches Ergebnis ist deshalb an dieser Stelle unzutreffend, weil es beim Vorgang des Sich-Verschaffens – nach den oben angesprochenen (aber widersprüchlichen[2328]) Erl – nur um das Sich-Zuführen einer neuen körperlichen Sache handelt, an der der Täter nunmehr Gewahrsam begründen kann. Damit sind aber schlüssigerweise alle Verschaffungsvorgänge rein unkörperlicher Computerdaten, wie der Download von inkriminiertem Bildmaterial aus dem Internet oder das Übertragen dieser Daten von einem Datenträger auf einen vom Täter selbst beigestellten Datenträger nicht vom Sich-Verschaffen des § 207a Abs 3 erfasst. Eventuell käme man aber in Anbetracht der Tathandlung des Besitzens zu einem anderen Ergebnis.

Bezüglich der Tathandlung des Sich-Verschaffens hins § 241e erklären die GMat, dass diese jede Form des »An-sich-Nehmens« zum Ausdruck bringe und gerade im Gegensatz zu den Tathandlungen der Vermögensdelikte deshalb gewählt wurde, um nicht schon begrifflich eine Vermehrung des Tätervermögens durch diese Handlung zu verlangen.[2329] Lediglich bei den Zueignungsdelikten hat das Dogma der tatsächlichen (körperlichen) Sachherrschaft daher notwendigerweise noch bedeutenden Charakter.

Eine solche Abgrenzungsanleihe – was die Zueignungsdelikte betrifft – macht aber mE auch iZm § 207a Abs 3 Sinn, da der Gesetzgeber dadurch erklärt, dass diese Tathandlung eine neutrale Beschreibung des bloßen An-sich-Bringens von Tatobjekten sei. Warum sollte es aber bei § 207a Abs 3 (der nebenbei angemerkt auch keinen Vermögenstatbestand beschreibt) auf das strenge Verständnis des Gewahrsams ankommen? Begrifflich wird ein Gewahrsamserfordernis wohl nicht indiziert. Sachgerecht wäre es, wie oben ausgeführt, auf das Verschaffen der unmittelbaren Verfügungsmöglichkeit abzustellen, die im Übrigen bei diversen Computerdelikten – mangels Körperlichkeit der Tat-

2328 Da er das Abspeichern von Bildern aus dem Internet durch das ausdrückliche Anführen als einen Beispielsachverhalt, trotz anfänglicher Bezugnahme auf einen körperlichen Gegenstand, dann doch als erfasst erachtet (Siehe JAB 106 BlgNR XXIV. GP, 33 und JAB 1848 BlgNR XVIII. GP, 3).

2329 ErlRV 309 BlgNR XXII. GP, 16.

objekte – das »Gewahrsamserfordernis« ersetzt.[2330] Wenn man schon auf ein Gewahrsam nicht verzichten möchte, sollte der Begriff des Gewahrsams idZ[2331] weiter und jedenfalls in einer der Informationstechnik gerecht werdenden Weise verstanden werden. Wird daher vom »Bezug zu einem fassbaren Gegenstand« gesprochen, so muss das nicht heißen, dass die pornographischen Darstellungen selbst einen körperlichen Gegenstand darstellen müssen. Vielmehr kann damit auch nur gemeint sein, dass im Ergebnis eine (wenn auch nur technisch notwendige) Verkörperung der inkriminierten Darstellungen auf einem Trägerkörper vorliegen muss. Begreift man nun das Gewahrsam als (soziale) Zuordnung einer Sache zu einer Person[2332] nach allgemeiner Verkehrsauffassung, dann wird Gewahrsam in diesem Fall auch dann begründet, wenn eine neue solche Zuordnung geschaffen wird.

Durch das Herunterladen der Bilder auf einen bereitgestellten Datenträger, wird daher nicht am Datenträger Gewahrsam begründet, sondern an der neuen Zuordnung des nunmehrigen Informationswerts des Datenträgers zur Person.

Zum Ergebnis, dass jede »dynamische, rein technische Verkörperung« bereits ausreichend sein muss und das Herunterladen von inkriminierten Bildern aus dem Internet von der Tathandlung des Sich-Verschaffens des § 207a Abs 3 erfasst ist, kommt man auch über eine Interpretationsanleihe bei § 126c Abs 1, wo genauso das Sich-Verschaffen als Tathandlung iZm (unkörperlichen) Computerprogrammen (Z 1) oder Zugangsdaten (Z 2) genannt ist. Betrachtet man nun diese Tathandlung iVm den Tatobjekten nach Z 2, so muss das Sich-Verschaffen von Computerpasswörtern, Zugangscodes uÄ jedenfalls möglich sein. Dieses Vorbereitungsdelikt macht idZ nur dann Sinn, wenn zB bereits das Ablesen eines (fremden) Passworts von einem Zettel als ein Sich-Verschaffen erachtet wird.[2333] Der Täter befindet sich nämlich dann in Kenntnis dessen. Dass er auch den Zettel, als Träger der Schrift, an sich bringen muss, ist dabei wohl nicht erforderlich. Andernfalls wäre diese Auslegung viel zu eng. Die Kenntnisnahme des Passworts als Vorbereitungshandlung zu entspre-

2330 Siehe etwa § 126a Abs 1, wo Täter nur sein kann, wer nicht oder nicht allein über die Daten verfügen darf, als Pendant zur »fremden Sache« bei § 125. Es geht nicht darum, wer die Daten in seinem Gewahrsam hat, sondern wer darüber verfügen darf.

2331 Vgl JAB 106 BlgNR XXIV. GP, 33; JAB 1848 BlgNR XVIII. GP, 3.

2332 Siehe dazu ausf unten zum Besitz.

2333 AA für die vergleichbare Situation in Deutschland *Heghmanns* in Achenbach/Ransiek, Wirtschaftsstrafrecht[3], 741 (761).

chenden Hauptdelikten, ist somit das vom Vorbereitungsdelikt erfasste Übel, denn mit Kenntnis des Zugangscodes können diverse in § 126c Abs 1 Z 1 genannte Hauptdelikte verwirklicht werden. Es kann folglich auf eine Körperlichkeit der zu verschaffenden Tatobjekte nicht ankommen.

In diesem Sinn wird sinnvollerweise auch § 254 (»Ausspähung von Staatsgeheimnissen«) iZm der Tathandlung des Sich-Verschaffens interpretiert, wenn *Bachner-Foregger* dazu erklärt, dass sich ein Staatsgeheimnis verschafft, wer sich unbefugt Kenntnis von dem Geheimnis erwirbt. Unter anderem kann dies der Fall sein, »wenn jemand einen versehentlich unverschlossen gebliebenen Geheimakt studiert«.[2334] *Eder-Rieder* führt dazu an, dass auch die Kenntniserlangung durch Hören, Lesen etc in Betracht kommt.[2335]

Auch ist mE iZm § 278f Abs 2[2336] den GMat nicht zu folgen, wenn in diesen bezüglich der Tathandlung des Sich-Verschaffens von Informationen aus dem Internet ein Abspeichern auf einem Speichermedium vorausgesetzt wird. Dies wird damit begründet, dass der Täter beim Sich-Verschaffen ein eigenes Zutun zur Gewahrsamserlangung setzen müsse.[2337] Das eigene Zutun liegt aber mE – dem Normzweck entsprechend – wohl bereits in der aktiven Kenntnisverschaffung der Information und nicht erst in einer entsprechenden körperlichen Gewahrsamsbegründung.[2338]

b. »Quasi-Gewahrsam«

Der Rückgriff auf andere Bestimmungen zeigt deutlich auf, dass ein Sich-Verschaffen nicht per se an eine Gewahrsamserlangung anknüpft bzw sinnvollerweise auch gar nicht anknüpfen sollte. Mit einer solchen Einengung wären informationstechnologische Sachverhalte nur schwer bis gar nicht erfassbar. Denkt man bspw an den Fall, dass sich jemand Bilddateien nicht auf seinen lokalen Computer herunterspeichert, sondern lediglich in einem »Online-Speicher« im Internet ablegt, hat er sich die volle Verfügungsmöglichkeit (dh »Quasi-Gewahrsam[2339]«) verschafft und dennoch keinen faktischen Gewahrsam an

2334 Siehe *Bachner-Foregger* in WK² § 254 Rz 7.
2335 Vgl *Eder-Rieder* in SbgK § 254 Rz 14 mwN.
2336 Eingeführt durch BGBl I 103/2011.
2337 Vgl ErlRV 674 BlgNR XXIV. GP, 6.
2338 Vgl auch § 126c Abs 1 Z 2.
2339 In Erweiterung der Rechtsfigur des »gelockerten Gewahrsams«.

einer körperlichen Sache begründet.[2340] In diesem Fall wird nicht einmal ein im Gewahrsam des Täters befindlicher Datenträger verwendet. Gerade durch einen solchen Fall lassen sich die gegenständlich untersuchten Probleme gut darstellen, denn der Täter würde beim Herunterladen von inkriminierten Bildern aus dem Internet auf einen Online-Speicher gar nicht tatbestandlich iSd Sich-Verschaffens handeln, da er dabei keinen Gewahrsam an körperlichen inkriminierten Sachen erlangt. Aber selbst die Besitzstrafbarkeit wäre in diesem Fall in Bezug auf den unmittelbaren Täter fraglich, weil dieser keinen »Gewahrsam« am körperlichen Gegenstand hat, der diese unkörperlichen Bilder verkörpert. Hinsichtlich einer etwaigen Besitzstrafbarkeit könnte man auf die Rechtsfigur des »gelockerten Gewahrsams«[2341] iSd »sozialen Gewahrsamsbegriffs«[2342] zurückgreifen. Beim »gelockerten Gewahrsam« »behält den Gewahrsam auch, wer die Sachherrschaft zwar durch einen Dritten, aber entsprechend seinen Weisungen und unter seiner zumindest potentiell gegebenen Aufsicht ausüben lässt«.[2343] Man müsste dabei aber einräumen, dass der faktische Gewahrsamsdiener bzw -mittler, der in solchen Fällen bloß Mitgewahrsam begründet, nicht »in Gegenwart« des Obergewahrsamsträgers agiert, weshalb man gerade nicht – was jedoch zumindest diese eben zitierte E indiziert – von »kurzfristen Überlassungen zum unmittelbaren Gebrauch« sprechen kann.

Der »soziale Gewahrsamsbegriff« erfordert nun keine greifbare (dh räumliche) Nähe zur Sache. Vielmehr reicht eine soziale Zuordnung eines Gegenstands zu einer Person aus.[2344] Die Sache wird daher auch bei fehlender körperlicher Anwesenheit des Gewahrsamsträgers diesem kraft sozialer Zuschreibungsmomente zugeordnet. Als ein wesentliches Kriterium spielt dabei die Überwachungsmöglichkeit durch den übergeordneten Gewahrsamsträger eine Rolle.[2345] Dieses Kriterium ist nach dem OGH eng zu fassen und darf sich für den unmittelbaren Sachinhaber nicht bloß als »abstrakt-theoretische« Variante darstellen.

2340 Ähnlich bei Dateien im E-Mail-Postfach auf einem (fremden) Server im Internet.

2341 Siehe zur Begrifflichkeit ua etwa *Kienapfel/Schmoller,* StudB BT II § 127 Rz 67; *Leukauf/Steininger,* StGB³ § 127 Rz 21; *Bertel* in WK² § 127 Rz 15; *Salimi* in SbgK § 127 Rz 84; *Schwaighofer,* JSt 2012, 66; *Birklbauer/Hilf/Tipold,* Strafrecht BT I² § 127 Rz 20 f.

2342 Siehe dazu *Kienapfel/Schmoller,* StudB BT II § 127 Rz 64 ff.

2343 Vgl OGH 03.06.2003, 14 Os 51/03; vgl weiters RIS-Justiz RS0093841 mwN.

2344 Siehe OGH 13.11.2007, 14 Os 123/07 f; weiters *Kienapfel/Schmoller,* StudB BT II § 127 Rz 64 ff.

2345 Vgl *Kienapfel/Schmoller,* StudB BT II § 127 Rz 90; Siehe auch OGH 03.06.2003, 14 Os 51/03.

Eine permanente Kontrolle wird aber nicht verlangt, insoweit genügt eine rasch realisierbare Nachschau durch den Träger des übergeordneten (Mit-)Gewahrsams.[2346]

Im hier interessierenden informationstechnischen Kontext, insb was ubiquitäre unkörperliche Daten anlangt, ist aber auch dieses soziale bzw gelockerte Verständnis von Gewahrsam unzureichend. Dies ergibt sich aus der eben erwähnten Tatsache, dass beim gelockerten Gewahrsam die Zuordnung eines »Gegenstands« zu einer Person maßgeblich ist. Mit anderen Worten, in den hier untersuchten Fällen muss der jeweils verwendete Datenträger bzw dessen konkrete Speicherbereiche dem Verfügungsberechtigten über die darin gespeicherten Daten zugeordnet werden.

In Zusammenhang mit unkörperlichen Daten(-inhalten), bei denen der Datenträger ausschließlich eine rein faktisch-notwendige Aufgabe erfüllt, ist es höchst an der Zeit, eine zweckmäßige Adaptierung der spezifischen Dogmatik vorzunehmen und dabei iZm unkörperlichen Sachen endlich eine Abstraktion von der körperlichen Substanz sinnvoll einzubeziehen. Insbesondere sind selbstverständlich auch dynamische Weiterentwicklungsprozesse zu berücksichtigen. Die herkömmlichen informationstechnischen Datenträger, wie CDs und DVDs, werden zunehmend durch moderne abstrakte Modelle, wie »Cloud Computing«[2347], verdrängt. Im Wesentlichen befinden sich dann das systemführende IT-System, die verwendete Software und der individuelle Datenspeicherplatz, nicht mehr beim Nutzer selbst, sondern werden ihm virtuell über ein Netzwerk als Dienstleistung zur Verfügung gestellt.[2348] Der Verfügungsberechtigte über die Daten hat in solchen Systemen keine Kenntnis davon, wo sich der jeweilige Datenträger befindet, auf dem seine Daten verkörpert werden. Auf den »körperlichen Datenträger« bezogen fehlt dem Verfügungsberechtigten über die dort gespeicherten Daten jegliches subjektive Gewahrsamselement.

Da ohnehin grundsätzlich auch der Besitz von pornographischen Darstellungen Minderjähriger eigenständig strafbar ist, sollte man mE in diesem Zusammenhang zunächst die Frage nach dem Gewahrsam stellen. Für das Sich-Verschaffen darf mE nur der Vorgang der Erlangung der vollständigen Verfügungs- bzw Kenntnisnahmemög-

2346 Siehe OGH 03.06.2003, 14 Os 51/03.
2347 Siehe zur Begrifflichkeit zB *Sonntag* in Jahnel/Mader/Staudegger, IT-Recht[3], (1) 17.
2348 Vgl *Popp,* JSt 2012, 30; weiters *Kersken,* IT-Handbuch[5], 989.

lichkeit[2349] ausschlaggebend sein. Die Abgrenzung zum bloßen wissentlichen Zugreifen (Abs 3a) liegt dabei in der Tatsache, dass man über Bilder, die man im Internet bloß betrachtet, nicht auch vollständig und umfassend verfügen kann. Man hat lediglich Zugriff auf den Inhalt. Es ist also in diesem Fall die uneingeschränkte Verfügungsmöglichkeit iS einer tatsächlichen Herrschaft über die Tatobjekte samt Bezug habender vollständiger Einwirkungsmöglichkeit auf die Daten (noch) nicht gegeben, wohl aber die Kenntnisnahmemöglichkeit. Die Computerdaten müssen im Sinne einer umfassenden Verfügungsmöglichkeit für den Täter technisch uneingeschränkt verarbeitbar und wahrnehmbar sein. Das bedeutet, dass sie in seine Verfügungsmacht gelangt sein müssen, wo er die Dateien löschen, verändern, verschieben, kopieren[2350] oder betrachten kann. Dass auch andere Personen mit denselben Verfügungsmöglichkeiten über diese Daten ausgestattet sein können, schadet nicht. Um über Dateien auf Websites im Internet umfassend verfügen zu können, müssen die Daten grundsätzlich erst reproduziert und abgespeichert werden. Diese Handlungen, insb die dazu notwendige Verfügungsberechtigung über die Daten, grenzen aber das bloße Zugreifen im Internet vom Sich-Verschaffen klar ab.

Der bloße Aufruf einer Website im Internet, auf der sich kinderpornographische Bilder befinden, stellt mE aber bereits dann ein Sich-Verschaffen iSd § 207a Abs 3 dar, wenn der Täter weiß, dass sich diese mit dem Laden der Daten auch in den Arbeitsspeicher bzw Internet-Cache seines Computers übertragen. Eine Besitzstrafbarkeit muss hierbei noch gar nicht eingetreten sein. Eine Aufrechterhaltung iS einer gewissen Dauerhaftigkeit der Speicherung (auf einem permanenten bzw semi-permanenten Datenträger) spielt in weiterer Folge lediglich für eine Einordnung unter die Besitz-Tathandlung eine Rolle, nicht für die Handlungsweise des Sich-Verschaffens.

c. Besitzverbot

Besitz ist prinzipiell jede Form des Gewahrsams an den Darstellungen, selbst wenn dieser ohne das Zutun des Täters begründet wurde.[2351]

2349 Je nach Delikt zB Verfügungsmöglichkeit (§ 207a Abs 3) bzw Kenntnisnahmemöglichkeit (§ 126c Abs 1, § 254).

2350 Im Sinne von »automationsunterstützt verarbeiten«.

2351 Vgl *Bertel/Schwaighofer,* BT II[11] § 207a Rz 10; vgl *Hinterhofer* in SbgK § 207a Rz 59; weiters *Philipp* in WK[2] § 207a Rz 20.

Nach den GMat besitzt ein Tatobjekt, wer daran allein oder gemeinsam mit anderen Gewahrsam hat, also die tatsächliche und unmittelbare Herrschaft über den Gegenstand ausüben kann. Auch diese Tathandlung setzt einen Bezug zu einem körperlich fassbaren Gegenstand voraus.[2352]

Es kommt daher nach hM in erster Linie auf die tatsächliche vom Herrschaftswillen getragene unmittelbare Sachherrschaft an, die die konkrete Einwirkungsmöglichkeit auf die Sache impliziert.[2353] Ob ein faktisches Herrschaftsverhältnis vorliegt, ist dabei einzelfallbezogen nach der verständigen Verkehrsauffassung zu beurteilen.[2354] Die faktische Innehabung von solchen Darstellungen im temporären Internet-Cache[2355] auf der Festplatte, reicht für einen (objektiven) Besitz aber bereits aus, selbst wenn der Täter davon nichts weiß.[2356] Dies ergibt sich zB aus einem – nach der Verkehrsauffassung zu beurteilenden – »generellen Herrschaftswillen«, der sich auf einen bestimmten »Herrschaftsbereich« richtet (zB Wohnung, Briefkasten, Computer, Handtasche, Auto) und nicht auf eine konkrete Sache innerhalb desselben.[2357] *Hochmayr* sieht einen solchen Herrschafts- oder Besitzwillen für den Gewahrsam an Sachen innerhalb der (räumlichen) Privatsphäre für entbehrlich an.[2358] Entscheidend sei lediglich die Tatsache, dass sich die Sache in der Privatsphäre befindet. Die Begrifflichkeit »Privatsphäre« ist mE an dieser Stelle und in diesem Zusammenhang ungeeignet, da sich diese nicht nur auf Bereiche der »räumlichen Nähe« bezieht. Man denke etwa an private E-Mails, die im Postfach auf einem räumlich entfernten Mail-Server liegen und dennoch zur (informationellen) Privatsphäre des Postfachinhabers gehören. Es wäre wohl die Bezeichnung »Bereich der räumlichen Nähe« bei *Hochmayr* treffsicherer.

Daher verhindert im Fall des Besitzes von inkriminierten Bildern im Internet-Cache lediglich die Nichterfüllung des subjektiven Tatbestands die Tatbestandsmäßigkeit des Besitzdelikts. Anders als bei der

---

2352 Vgl JAB 1848 BlgNR XVIII. GP, 3, darauf verweisend auch JAB 106 BlgNR XXIV. GP, 33.

2353 Siehe dazu ausf *Hochmayr,* Besitz, 10 mwN; weiters *Kienapfel,* BT II[3] § 127 Rz 54 ff; weiters *Leukauf/Steininger,* StGB[3] § 127 Rz 21 ff; vgl auch OGH 28.09.2010, 14 Os 126/10a.

2354 Siehe OGH 10.04.1996, 13 Os 17/96 mwN.

2355 Technisch bedingte Zwischenspeicherung von Elementen von Websites.

2356 Vgl *Hinterhofer* in SbgK § 207a Rz 61; vgl auch JAB 106 BlgNR XXIV. GP, 35.

2357 Vgl auch *Kienapfel,* BT II[3] § 127 Rz 72 ff; weiters *Leukauf/Steininger,* StGB[3] § 127 Rz 24 ff;

2358 Vgl *Hochmayr,* Besitz, 74 ff und 81.

bloßen Vervielfältigung der Bilddateien im flüchtigen Arbeitsspeicher, sind die Dateien, selbst wenn sie in einem grundsätzlich[2359] temporär angelegten Verzeichnis gespeichert sind, längerfristig verfügbar und jederzeit abrufbar.[2360]

Das bloße Erreichen des Besitzzustands iSd faktischen umfassenden Verfügungs- und Wahrnehmungsmöglichkeit, wird im Fall des § 207a Abs 3 auch bereits vom Sich-Verschaffen miterfasst. Das Besitzen, als eigenständige Tathandlung neben dem Sich-Verschaffen, ist aber als ein Verhalten des Täters zu verstehen[2361], das über die faktische Besitzerlangung hinausgeht, weshalb die Erlangung der Verfügungsmöglichkeit über digitale Darstellungen bzw Gewahrsamsverschaffung bei körperlichem Bildmaterial vollendet und die Verfügungs- bzw Gewahrsamsausübung auf eine gewisse Aufrechterhaltung ausgelegt sein muss. Das verbotene Bildmaterial befindet sich daher bei der nunmehrigen Auseinandersetzung mit dem Besitz – unabhängig wie auch immer es in den Gewahrsam gelangt ist – auf einem körperlichen Datenträger, der dem Gewahrsam des Täters zugerechnet wird.

Die Tathandlung des Besitzens bezieht sich – anders als bspw das Zugreifen im Internet (Abs 3a) – nach hM auf rein körperliche Gegenstände, denen eine inkriminierte Darstellung anhaftet.[2362] Erst wenn daher die Bilddateien zB auf der Festplatte gespeichert sind, können sie strafbar besessen werden.[2363] Mit anderen Worten, nach hM ist an Computerdaten selbst, dh in einer vom Datenträger losgelösten Form, kein Gewahrsam und daher auch kein Besitz (im strafrechtlichen Verständnis) möglich. Der Datenträger ist aber in diesem Fall nur der Trägerkörper des tatbestandlichen unrechtsbehafteten Tatobjekts. Der (neutrale) Datenträger stellt nicht das eigentliche Tatobjekt der Bestimmung dar, deliktsspezifisches Tatobjekt ist nur dessen (nunmehriger) inkriminierter Inhalt (hier: eine »pornographische Darstellung Minderjähriger«). Es kann daher vorkommen, dass im Zuge des Sich-Verschaffens von kinderpornographischen Dateien diese auf einem bereits im (rechtmäßigen) Besitz des Täters befindlichen Datenträger gespeichert

2359 Über die temporären Internetdateien und eine etwaige Abspeicherung dieser kann der Nutzer selbst über entsprechende Browser-Einstellungen disponieren.
2360 Siehe dazu auch Vgl *Hinterhofer* in SbgK § 207a Rz 61.
2361 Vgl *Hochmayr,* Besitz, 85.
2362 Siehe *Hochmayr,* Besitz, 6; weiters *Reindl-Krauskopf,* Computerstrafrecht², 88.
2363 Vgl *Hochmayr,* Besitz, 6 mwN.

werden, weshalb für die Verwirklichung des anschließenden Besitzes die zuerst unauffällige – im Gewahrsam des Täters befindliche – Festplatte zu einem wesentlichen Teil des Besitzdelikts wird. Ein »neuer Besitz« wird aber dadurch – wie oben ausgeführt – nicht begründet.

Im Zusammenhang mit dem Besitz und der »faktischen Eigenschaft der Gesamtsache« – nicht aber was die Gewahrsamserlangung betrifft – könnte sich daher mE eine andere Situation ergeben, als die oben zum Sich-Verschaffen dargestellte. Als Vergleich kann ein gewöhnliches (strafrechtlich unbeachtliches) Eisenstück betrachtet werden, das sich im Besitz des Täters befindet. Verändert der Täter dieses Eisenstück so, dass daraus ein verbotener Schlagring entsteht, so darf das Eisenstück in dieser Eigenschaft (weil verbotene Waffe) nicht mehr besessen werden.[2364] Diese Transformation hat folglich nichts mit der Begründung eines neuen Gewahrsams zu tun, sondern mit der Veränderung der Eigenschaft einer bereits vorhandenen Sache, sodass daraus ein verbotener Gegenstand wird, an dem ein Besitzverbot besteht. Eine solche Eigenschaftsveränderung kann aber mE nur in Anbetracht eines Besitzdelikts eine Rolle spielen und nicht für den Vorgang des Sich-Verschaffens, weil sich Letzterer – nach offensichtlicher, aber widersprüchlich formulierter Ansicht des Gesetzgebers – auf das Verschaffen eines körperlichen Gegenstandes beziehen muss, währenddessen sich bei der Prüfung einer Besitzstrafbarkeit schon naturgemäß die Sache im Besitz des Täters befinden muss.[2365]

Nur im Fall des Besitzens wäre daher ein solcher Ansatz, dass nun ein Objekt eines unerlaubten Besitzes vorläge, denkbar.[2366]

Der verbotene Informationswert, der nunmehr auf der Festplatte gespeichert ist, macht aber den Datenträger selbst nicht zum gefährlichen Gegenstand, da es sich – anders als beim Schlagring – dabei nicht um eine unveränderbare Eigenschaft handelt. Vielmehr ist die Festplatte als sozial adäquates Trägermedium[2367] nur vorübergehend, aber faktisch, zum Tatmittel des Besitzes von Tatobjekten avanciert (»technischer Besitzdiener«).

2364 Vgl § 17 Abs 1 Z 6 WaffG 1996, BGBl I 12/1997 idgF.

2365 Daher auch in Form der Verkörperung auf einem Datenträger, unabhängig davon, wie er an die verbotenen Bilddateien gekommen ist.

2366 AA JAB 106 BlgNR XXIV. GP, 34.

2367 Es ist gerade die Bestimmung einer Festplatte, dass sie willkürliches Beschreiben, Lesen und Löschen von den unterschiedlichsten Daten ermöglicht.

Die als eine Funktionseinheit zu betrachtende Verbindung von Trägerkörper und Inhalt ist gerade bei ubiquitären und gleichwertigen, ohne Qualitätsverlust reproduzierbaren[2368] bzw verschiebbaren[2369], unkörperlichen Computerdaten (bestimmungsgemäß) auflösbar. Dies ist gerade bei der Datenübertragung über Netzwerke ein entscheidendes Element für den paketvermittelnden Transport. »Neuer« Gewahrsam wird daher bei Datenübertragungen über informationstechnische Netzwerke nie am Datenträger begründet. Der jeweilige Bezug habende Datenträger ist allenfalls rein faktischer, weil technisch notwendiger, (deliktisch bedeutungsloser) »technischer Gewahrsamsdiener« für sämtliche unkörperliche Computerdaten. Die Gewahrsamsbegründung kann daher – wie oben ausgeführt – an den Datenträgern nicht sinnvoll festgemacht werden. Das gilt insb für einen Datenträger, der bereits vor der Tathandlung – also ohne die inkriminierten Abbildungen – im Besitz des Täters war.

Dass jede Form des Besitzens den Gewahrsam der Sache durch körperliche Manifestation benötigt, ist auch in Anbetracht des § 126c Abs 1 Z 2 unklar. Strapaziert man nämlich erneut den Vergleich mit § 126c Abs 1, so stellt man auch iZm der Tathandlung des Besitzens fest, dass der »Besitz« von Zugangsdaten (Z 2) strafbar ist und daher auch faktisch möglich sein muss. Kriminalpolitisch auffällig ist die Tatsache, dass Täter iSd Besitzens nur derjenige ist, der in Besitz eines Passworts auf einem körperlichen (Daten-)Träger ist. Ein solcher Träger könnte eine Festplatte, ein USB-Stick oder aber ein Blatt Papier[2370] sein, dem das entsprechende Passwort als Informationswert und Inhalt anhaftet. Merkt sich der Täter ein Passwort eines anderen bloß, so wäre dies kein Besitz. Natürlich stellt sich in so einem Fall die Frage nach der Beweisbarkeit eines solchen »Besitzes« bzw einer solchen Kenntnis, weshalb eine materielle Verkörperung auch sinnvollerweise verlangt wird. In Anbetracht des Zielanliegens der Bestimmung wäre die Verneinung einer Strafbarkeit in diesem Fall aber im Vergleich zu einem Sachverhalt, in dem sich der Täter das Passwort selbst auf einen Zettel aufschreibt,

2368 Im Sinne von »vervielfältigbar« (Kopie und Original sind weiterhin vorhanden).

2369 Im Sinne von kopierbar und gleichzeitig am ursprünglichen Ort aber gelöscht (nur mehr die – nicht differenzierbare – Kopie ist vorhanden).

2370 Konventionelle analoge Medien kommen nur dann in Betracht, wenn man akzeptiert, dass sich die Tathandlungen des § 126c Abs 1 nicht nur durch rein automationsunterstützte Vorgehensweisen realisieren lassen (siehe dazu die obigen Ausführungen zu § 126c).

kriminalpolitisch nicht sachgerecht. Im letzteren Beispiel liegt ein strafbarer Besitz des Computerpassworts seitens des Täters vor, da er den Zettel (als körperlichen Gegenstand) in seinem Gewahrsam hat. Und dennoch spielt der Zettel selbst zwar eine buchstäblich »tragende«, aber keine deliktische Rolle. Hätte sich der Täter das Passwort bloß gemerkt, wäre er hins des Besitzens straflos.[2371] Liest jemand ein Passwort von einem Zettel ab, so macht er sich grundsätzlich – sofern man auf eine Körperlichkeit der Zugangsdaten bei dieser Tathandlung verzichtet – bezüglich des Sich-Verschaffens strafbar. Für das Sich-Verschaffen darf es folglich nicht (auch) auf die Körperlichkeit ankommen.

Man sollte darüber hinaus bei Sachverhalten, in denen 1.) nicht ausschließlich originale Datenträger samt Bildmaterial und 2.) keine schreibgeschützten (dh nicht mehr beschreibbaren) körperlichen Trägermedien (CD-ROM, DVD-ROM) verwendet werden, von der unmittelbaren, grundsätzlich auch fortgesetzten Verfügungsmöglichkeit über die Daten als einem »besitzähnlichen« Zustand ausgehen. Der Gewahrsamsbegriff könnte iZm unkörperlichen Computerdaten sachgerecht gelockert werden. Faktisch Verfügungsberechtigter ist nämlich dabei nicht bloß derjenige, der den entsprechenden Datenträger in seiner Herrschaft hat, sondern auch derjenige, der die tatsächliche Verfügungsmacht über den Datenbestand ausüben kann.

Damit könnte auch im hier untersuchten Zusammenhang die Frage leichter beantwortert werden, wer als Besitzer iSd § 207a Abs 3 in Frage kommt, wenn inkriminierte Bilddateien in einem »Online-Speicher« auf einem Server im Internet abgespeichert sind, über den ein bzw eine bestimmte Anzahl konkreter (pädophiler) Nutzer virtuell verfügungsberechtigt[2372] ist.[2373] Gerade bei Daten wird deshalb in sehr vielen Fällen Mitgewahrsam vorliegen, wobei nur einer der Gewahrsamsträger den Datenträger selbst faktisch innehat. Unstrittig ist, dass in diesem Fall der tatsächliche Inhaber des konkreten Datenträgers (dem aber vermutlich wiederum der Herrschafts- bzw Verfügungswille über die

2371 Was wohl eine problematische Beweisfrage darstellt.

2372 Zum leichteren Verständnis wird hier von einer uneingeschränkten Verfügungsberechtigung über den zugewiesenen Speicherplatz ausgegangen.

2373 Es wäre auch denkbar, dass ein Einzeltäter die Bilddateien auf einem Server im Internet versteckt, um sie nicht auf seinem Computer oder anderen Datenträgern zuhause aufzubewahren.

Daten seiner Kunden fehlen dürfte), nach dem faktisch-normativen Gewahrsamsbegriff die Abbildungen in seinem Besitz hat (Provider).[2374]

Keiner der Nutzer dieses Online-Speichers hat den körperlichen Gegenstand »Festplatte mit den inkriminierten Darstellungen« in seiner tatsächlichen Herrschaftsgewalt. Das heißt, dass die Nutzer über die (körperliche) Festplatte selbst weder frei verfügen können, noch auf sie unmittelbar physisch einwirken oder etwa Kontroll- oder Überwachungsmöglichkeiten[2375] ausüben.[2376] Sie können lediglich über ihre Funktionalität der Datenverwaltung in einem sehr kleinen Ausschnitt mittels eines virtuellen Zugangs verfügen (iSd Abs 3a). Nicht aber können eigenverantwortlich Veränderungen am Datenträger selbst per Weisung oder Auftrag wirksam dem unmittelbaren Sachinhaber (hier: Provider) erteilt werden. Insoweit ist jeder Nutzer nur ein Mitverfügungsberechtigter. Man wird aber sinnvollerweise und nach allgemeiner Verkehrsanschauung in diesem Fall von einem Besitz an den auf dem (fremden) Datenträger verkörperten Darstellungen auszugehen haben, selbst wenn die Nutzer keine unmittelbare tatsächliche Nähe oder soziale Zuordnung zum körperlichen Datenträger haben (»Quasi-Gewahrsam«[2377]).

Nach der Rsp ist nämlich nicht nur die strenge unmittelbare Einwirkungsmöglichkeit des Gewahrsamsträgers auf die Sache selbst maßgebend, sondern vielmehr die soziale Zuordnung von Person und Sache.[2378] Demnach ist der Gewahrsam jene Zugehörigkeit einer Sache zu einer Person, die auch ein Außenstehender nicht nur als eine räumliche Beziehung, sondern als eine auf sozialen Gepflogenheiten beruhende Verbindung von Sache und Person zu erkennen vermag. Daher erfordert dieses Verhältnis auch keine greifbare Nähe zur Sache.[2379]

2374 Auf eine etwaige Strafbarkeit des Host-Providers unter Bedachtnahme der Providerhaftung gem §§ 13 ff ECG wird hier nicht näher eingegangen.

2375 Siehe *Kienapfel/Schmoller,* StudB BT II § 127 Rz 90; weiters OGH 03.06.2003, 14 Os 51/03, wobei dieses Kriterium als »wesentlich« für einen gelockerten bzw sozialen Gewahrsam erachtet wird.

2376 Abgesehen von der mittelbaren (bestimmungsgemäßen) Möglichkeit durch das Hinzufügen oder Löschen von Daten technisch bedingte physikalische Eigenschaften der Festplatte zu verändern.

2377 Siehe oben.

2378 Siehe dazu auch die Ausführungen zur widerrechtlichen Geldbehebung an einem Bankomaten S 376 ff.

2379 Siehe dazu OGH 10.12.1996, 14 Os 71/96 (14 Os 78/96) mwN; auch OGH 28.09.2010, 14 Os 126/10a bzw RIS-Justiz RS0099100 mwN.

Hochmayr erklärt dies bei Sachen, die sich außerhalb der Privatsphäre[2380] befinden, damit, dass sich der Gewahrsam an einer solchen Sache aus dem funktionalen Zusammenhang zwischen der Art der Sache und ihrem Standort erschließt, wenn nämlich aus dieser Zusammenschau resultiert, dass über die Sache möglicherweise noch verfügt werden wird.[2381] Für die objektive Beurteilung, ob Gewahrsam an Sachen außerhalb der Privatsphäre vorliegt, sind subjektive Elemente erforderlich. Dem Gewahrsamsinhaber muss der Standort der Sache zumindest mitbewusst sein und er muss den Willen haben, die Sache haben zu wollen.[2382] Das faktische Herrschaftsverhältnis ist in diesem Fall abgeschwächt, aber nicht beseitigt.[2383]

Gewahrsam könnte daher prinzipiell vorliegen, wobei aber auf die Körperlichkeit der konkreten Sache (in der Herrschaftsgewalt der jeweiligen Nutzer) weitgehend verzichtet werden müsste (was außerhalb des Vermögensstrafrechts auch nicht wirklich problematisch erscheint). Was die Körperlichkeit der Sache anlangt, so käme man nämlich erneut in Erklärungsnotstand, da zwar die entsprechenden Bilddateien über Speicherbereiche der im fremden Gewahrsam befindlichen Festplatte verkörpert werden, diese aber nicht vom Herrschaftswillen des Täters umfasst sind, der sich nur auf die Inhalte der Speicherplätze bezieht. Der Online-Speicher ist wiederum nur »technischer Gewahrsams- bzw Besitzdiener«, da die Dateien in ihrer funktionellen Form[2384] sonst gar nicht existieren könnten.[2385]

2380 Wobei »Privatsphäre« von ihr iSv räumlicher Nähe ausgelegt wird. Diese ist aber bekanntermaßen weiter zu verstehen, da auch ein E-Mail auf einem entfernten Mail-Server oder eine Datei im Internet der Privatsphäre einer Person zuzurechnen sein wird.

2381 Siehe *Hochmayr,* Besitz, 82 und 146.

2382 Subjektive Elemente für den objektiven Tatbestand wirken sich nicht auf den subjektiven Tatbestand aus. Es sind lediglich Teile des Tatbildvorsatzes sowohl für den objektiven als auch für den subjektiven Tatbestand relevant (siehe dazu *Hochmayr,* Besitz, 83).

2383 Zum »gelockerten Gewahrsam« siehe *Kienapfel,* BT II³ § 127 Rz 59; *Kienapfel/Schmoller,* StudB BT II § 127 Rz 67, *Leukauf/Steininger,* StGB³ § 127 Rz 21; *Bertel* in WK² § 127 Rz 15; *Salimi* in SbgK § 127 Rz 84; *Birklbauer/Hilf/Tipold,* Strafrecht BT I² § 127 Rz 20 f; *Schwaighofer,* JSt 2012, 66; weiters auch jüngst OGH 28. 09. 2010, 14 Os 126/10a.

2384 Man könnte den Binärcode der Bilddatei auf Papier ausdrucken, was faktisch sinnlos wäre.

2385 Siehe dazu oben.

Würde man auch in diesen Fällen eine Besitzstrafbarkeit ablehnen, entstünden Strafbarkeitslücken, wenn der Täter die inkriminierten Darstellungen auf Online-Speichermedien fremder Server aufbewahren würde, aber umfassende Verfügungsbefugnis – iSd »Quasi-Gewahrsams« – darüber hätte. In diesem Fall wäre trotz »besitzähnlicher« Konstellation und Indikation des § 207a Abs 3 dennoch »nur« § 207a Abs 3a, wo dem Täter aber Wissentlichkeit nachgewiesen werden muss, anwendbar. In Zukunft wird sich die Informationstechnologie wohl noch weiter von einer physischen Zuordenbarkeit von Informationen zu einem konkreten Datenträger entfernen. Bei modernen Modellen der informationstechnischen Datenorganisation, die durch die Weiterentwicklung der technischen Grundpfeiler Flüchtigkeit, Virtualisierung, Automatisierung und Ubiquität gekennzeichnet sind (zB Cloud Computing), wird dann in einem solchen strafrechtlichen Zusammenhang lediglich die Frage nach dem »Access« (Zugang) – iSd oben ausgeführten »Quasi-Gewahrsams« – adäquate Ergebnisse hervorbringen können.

Mit anderen Worten, die Information erfüllt unabhängig vom Träger ihren Zweck, welcher grundsätzlich auch durch Reproduktion und Transmission in seiner abstrakten Erscheinungsform nicht verändert wird.

d. Aufgedrängter Besitz

Gelangt jemand ungewollt – zB durch Zustellung einer inkriminierten Darstellung per E-Mail, MMS oder durch Überlassen einer DVD – in den Besitz von pornographischen Darstellungen Minderjähriger, so ist er, um straflos zu bleiben, verpflichtet, diesen (faktischen) Besitz umgehend[2386] aufzugeben.[2387] Eines ROM[2388]-Datenträgers kann man sich durch dessen Zerstörung oder Entsorgung entledigen, ein E-Mail bzw andere Dateien, die solche Inhalte haben, lassen sich programmtechnisch löschen. Dabei ist aber nicht ausnahmslos eine physische (iSv dauerhafte) Löschung notwendig.[2389] Eine solche ist lediglich dann an-

2386 Nach Ablauf einer Überlegungsfrist (vgl *Hochmayr,* Besitz, 101 ff).

2387 Siehe *Hochmayr,* Besitz, 100, die Besitzdelikte als echte Unterlassungsdelikte begreift; weiters *Hochmayr* in BMJ, 33. Ottensteiner Fortbildungsseminar, 87 (96 ff); auch zB *Bertel/Schwaighofer,* BT II[11] § 207a Rz 10; vgl dazu weiters OGH 13.10.1998, 14 Os 129/98 = JBl 2000, 554 *(Medigovic*).

2388 »Read-Only-Memory«.

2389 AA *Hinterhofer* in SbgK § 207a Abs 3 Rz 60 mwN.

gezeigt, wenn der Inhaber weiß, dass die Daten durch das Verschieben in den Papierkorb (»logisches Löschen«[2390]) nicht gelöscht werden.

Gelangt inkriminiertes Bildmaterial zunächst zwar ungewollt in den Besitz des Täters, bildet dieser aber danach den Vorsatz aus, diese Bilder behalten zu wollen, so hat auch ein »dolus subsequens« in der Tathandlung des Besitzens strafbarkeitsbegründende Wirkung.

In allen Fällen des § 207a Abs 3 reicht dolus eventualis aus.

Hat der Täter zuvor selbst hergestellte pornografische Darstellungen mit Minderjährigen weiterhin in seinem Besitz, so stellt das Besitzen gegenüber dem Herstellen (§ 207a Abs 1 Z 1) nach hM eine vorbestrafte Nachtat dar.[2391] Innerhalb der einzelnen Sätze des § 207a Abs 3 geht stets das Sich-Verschaffen dem (anschließenden) Besitzen vor.[2392] Aus diesem Grund steht das Besitzen zum Sich-Verschaffen im Scheinkonkurrenzverhältnis der Subsidiarität. Was das Verhältnis der Sätze innerhalb des § 207a Abs 3 anlangt, könnte auf den ersten Blick der zweite Satz eine (auf das Alter der mit dem Tatobjekt verknüpften Personen bezogene) Deliktsqualifikation zum Grunddelikt des ersten Satzes sein, da sich eine Abwandlung eines Tatbestandsmerkmals – nämlich eine besondere Eigenschaft des Tatobjekts[2393] im weiten Sinn – qualifizierend ändert. Der Unrechtsgehalt des 1. Satzes wird durch die Abänderung eines Tatbestandsmerkmals (vom mündigen zum unmündigen Minderjährigen) gesteigert. Das geschützte Rechtsgut, »die ungestörte sexuelle Entwicklung von Minderjährigen«[2394], ist dasselbe. Dass dabei Satz 1 das Grunddelikt darstellt, wird durch die Anordnung innerhalb des Absatzes indiziert. Andererseits könnte auch – aufgrund der historischen Entwicklung dieser Strafbestimmung[2395] und der höheren Schutzwürdigkeit Unmündiger[2396] – Satz 2 das Grunddelikt und Satz 1 dessen Privilegierung darstellen.

2390 Siehe oben zu § 126a.

2391 Vgl OGH 12.12.2011, 11 Os 152/11d.

2392 Vgl auch *Hinterhofer* in SbgK § 207a Abs 3 Rz 90.

2393 Tatobjekt im engeren Sinn ist die pornographische Darstellung (iSd § 207a Abs 4); Tatobjekt im weiten Sinn ist zudem die Eigenschaft (also das Alter) der Personen die darin mitwirken.

2394 Vgl *Hinterhofer* in SbgK § 207a Rz 9; weiters *Philipp* in WK² § 207a Rz 5.

2395 Siehe dazu § 207a idF BGBl 622/1994, 762/1996, I 134/2002.

2396 Vgl dazu die strengere Strafdrohung; man beachte auch *Schick* in WK² § 207a Rz 12 (aF Stand Mai 2007), der die Erweiterung des Tatbestands auf mündige Minderjährige überhaupt kritisch betrachtet.

Die ausdrückliche Verwendung der Phrasen »mündige minderjährige Person«[2397] bzw »unmündige Person« – lässt den Schluss zu, dass keine Qualifikation oder Privilegierung vorliegt, da bereits a priori – aufgrund der Umschreibung der betroffenen Altersgruppen – eine exakte Zuordenbarkeit gegeben ist, die tatbestandliche Exklusivität der beiden Sätze vorgibt. Es handelt sich daher jeweils um selbstständige Delikte mit exklusiven Voraussetzungen.

5. Der »Zugriff« auf pornographische Darstellungen Minderjähriger im Internet

§ 207a Abs 3a wurde mit dem 2. GeSchG 2009[2398] eingeführt und soll ausdrücklich das wissentliche Zugreifen auf pornographische Darstellungen Minderjähriger im Internet pönalisieren. Zum Zeitpunkt des Zugreifens auf das inkriminierte Material muss der Täter wissentlich iSd § 5 Abs 3 handeln. Er muss es daher für gewiss halten, dass auf der Website, die er gerade aufruft, pornographische Darstellungen mit Minderjährigen enthalten sind.

Die Tathandlung des »Zugreifens« auf pornographische Darstellungen Minderjähriger umfasst aber mehr als das bloße Betrachten[2399], weshalb nicht nur die rein visuelle Wahrnehmung, sondern jegliches wissentliche »Verarbeiten« solcher inkriminierten Dateien erfasst ist. Zu denken wäre etwa an einen Fall, in dem der Täter (zB als Administrator bzw Moderator eines einschlägigen Pädophilenforums) solche Abbildungen von Server A auf Server B kopiert bzw überhaupt mit solchen Darstellungen hantiert, ohne sie dabei aber selbst zu betrachten oder herunterzuladen. Hingegen wäre ein wissentliches (heimliches) »Über-die-Schulter-schauen«, während ausschließlich der unmittelbare Täter auf die Bilddateien zugreift, nicht erfasst, da der mittelbare Zuschauer die Materialien lediglich passiv betrachtet, nicht aber auf diese zugreift.[2400]

2397 Wobei der Begriff »mündige Minderjährige« im Kernstrafrecht nicht ausdrücklich definiert ist, aber in den GMat von Personen, die bereits das vierzehnte, aber noch nicht das achtzehnte Lebensjahr vollendet haben, gesprochen wird (siehe ErlRV 294 BlgNR XXII. GP, 20).

2398 BGBl I 40/2009.

2399 Vgl dazu aber § 215a Abs 2a.

2400 Zur weiteren Abgrenzung des »Zugreifens« gegenüber des »Betrachtens« siehe zu § 215a Abs 2a.

Der Zugriff erfordert ein aktives Tun des Täters, um – ebenfalls wie zu den Handlungen nach Abs 3 bereits ausgeführt – einen unmittelbaren bzw direkten Kontakt zu den Darstellungen zu erlangen. Das Öffnen einer Website auf der sich lediglich Links zu den pornographischen Darstellungen Minderjähriger befinden, stellt noch keinen Zugriff auf die Abbildungen selbst dar. Gegebenenfalls könnte ein Versuch vorliegen.

Die Tathandlung des Zugreifens nach § 207a Abs 3a tritt stillschweigend hinter das Sich-Verschaffen des Abs 3 zurück. Zugriff auf eine Darstellung, die ohne Zutun des Täters in seinen Gewahrsam gelangt ist, wird wiederum vom Besitz nach Abs 3 konsumiert.[2401]

Durch den Verweis in Abs 3a »Nach Abs 3 wird auch bestraft« wird die geteilte Strafdrohung für mündige bzw unmündige minderjährige Personen des Abs 3 übernommen.[2402]

Erstmals hat der Strafgesetzgeber mit dieser Bestimmung – neben § 278f[2403] – expressis verbis das »Internet« als Tatbestandsmerkmal und somit als Legalterminus erfasst. Es fragt sich allerdings, ob der lapidare Hinweis des JA tatsächlich ausreicht, um dieses Merkmal zu präzisieren bzw definieren, wenn er erklärt, dass sämtliche Internetdienste gemeint seien.[2404] Das bedeutet aber nur, dass sämtliche Dienste des »Internet« – wie zB WWW[2405], E-Mail, Newsgroups, Chat[2406], FTP[2407], Telnet[2408] erfasst sind, nicht aber andere technische Umgebungen, die nicht (mehr) Teil des Internet sind.

a. Internet vs Intranet

Deliktsspezifisch könnte in diesem Zusammenhang die Frage aufgeworfen werden, ob der Zugriff auf pornographische Bilddateien Minderjähriger in einem privaten Netzwerk ebenfalls von § 207a Abs 3a erfasst ist (zB Intranet[2409] eines Studentenwohnheims oder eines Unternehmens). In der Informatik wird ua dann vom Internet gespro-

2401 Siehe dazu JAB 106 BlgNR XXIV. GP, 35 mwN.
2402 JAB 106 BlgNR XXIV. GP, 35.
2403 Siehe dazu S 532 ff.
2404 JAB 106 BlgNR XXIV. GP, 35.
2405 World Wide Web.
2406 Im Sinne von »Instant Messaging« über diverse Protokolle.
2407 »File Transfer Protocol«.
2408 Siehe ua *Balzert,* Lehrbuch², 40 f.
2409 Es handelt sich dabei zB um einen Zusammenschluss von Computersystemen, die nicht öffentlich erreichbar sind (zB auch militärische Netzwerke).

chen, wenn es sich um ein öffentlich zugängliches Netzwerk handelt, in dem alle kommunizierenden Systeme dieselbe »Sprache« sprechen, dh auf derselben Übertragungsprotokollfamilie, nämlich TCP/IP[2410], aufbauen.[2411] Das Intranet ist hingegen gerade kein öffentliches Netzwerk, sondern ein geschlossener Computerverbund für interne Kommunikation, dem nur berechtigte Systeme angehören. Freilich kann, muss aber nicht, bei Intranetlösungen das TCP/IP und darauf aufbauende Dienste zum Einsatz gelangen, es könnte aber auch ein anderer Netzwerkübertragungsstandard – wie zB IPX/SPX[2412], AppleTalk, NetBIOS bzw NetBEUI – die technische Grundlage eines Intranet bilden. In diesem Fall würden bereits zwei wesentliche Kriterien, die das Internet aus technischer Sicht definieren, entfallen. Vieles deutet daher daraufhin, dass der Begriff »Internet« als Tatbestandsmerkmal im materiellen Strafrecht mit seiner umgangssprachlichen Bedeutung Eingang gefunden hat. Meiner Auffassung nach sollte dafür allerdings eine Legaldefinition geschaffen werden, um Auslegungsschwierigkeiten zu vermeiden und dem Rechtsanwender dadurch klare Begriffsinhalte zu vermitteln. De lege lata wird wohl – diesem allgemeinem Sprachgebrauch folgend – das »Intranet« und Netzwerke mit anderen Protokollgrundlagen ebenfalls darunter zu verstehen sein.

b. Die »Stand-Alone PC«-Ausnahme

Als ein weiterer Fall, der aufgrund des eindeutigen Wortlauts des § 207a Abs 3a nicht erfasst ist, kann die bloße Betrachtung von pornographischen Darstellungen auf einem Einzel-Computersystem (PC) genannt werden. Täter A besitzt (iSd § 207a Abs 3) inkriminiertes Bildmaterial auf seinem ungesicherten Notebook, das er während des Besuchs des Speisewagons im Zugabteil eingeschaltet liegen lässt. Der neugierige B, ein weiterer Fahrgast, klickt auf einen Ordner, in dem sich Kinderpornos befinden, welche er trotz anfänglicher Skrupel betrachtet.

2410 Lediglich im DoD (Department of Defense)-Modell wird bei den vier Schichten von TCP/IP-Netzwerken von einer »Internetschicht« gesprochen, in der die logische Adressierung der jeweiligen Rechner im Netzwerk über die sog »IP-Adresse« sichergestellt wird.

2411 Siehe auch *Balzert,* Lehrbuch², 36 ff.

2412 IPX/SPX (Internetworking Packet Exchange/Sequence Packet Exchange) ist ähnlich wie das TCP/IP eine Protokoll-Familie für lokale Netzwerke.

Obwohl B in diesem Fall auf die pornographischen Darstellungen »zugreift«, mangelt es für eine Strafbarkeit nach Abs 3a an der erforderlichen Begehungsweise »im Internet«. Eine Besitzstrafbarkeit nach Abs 3 scheidet ebenfalls aus.[2413]

Es ist nicht eruierbar, wie der (nationale) Gesetzgeber auf die ausdrückliche Nennung des Begriffs »Internet« als Tatbestandsmerkmal gekommen ist, zumal die internationalen wie europäischen Vorgaben idZ jeweils auf »Informations- und Kommunikationstechnologien« Bezug nehmen. Wesentlich sachgerechter erscheint es daher, im Sinne dieser Vorgaben (Art 20 Abs 1 lit f des Übereinkommens des Europarates zum Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch [CETS 201][2414] bzw Art 5 Abs 3 RL 2011/93/EU) auch umfassend auf »Informations- und Kommunikationstechnologien« abzustellen. Der Zugriff auf inkriminiertes Bildmaterial über ein privates Netzwerk wäre dann ebenso erfasst, wie der über einen Stand-Alone Computer.

§ 207a Abs 5 sieht spezielle Strafausschließungsgründe vor, wie zB die hier interessierende Z 2 bezüglich der Herstellung (§ 207a Abs 1 Z 1) und des Besitzes (§ 207a Abs 3) zum eigenen Gebrauch einer virtuellen pornographischen Darstellung (iSd § 207a Abs 4 Z 4) einer mündigen minderjährigen Person, sofern mit der Tat keine Gefahr der Verbreitung der Darstellung verbunden ist. Es darf daher kein tatsächliches Geschehen bzw keine tatsächliche Handlung vorliegen und keine unmündige Person auf der Darstellung abgebildet sein.[2415]

§ 207a ist ein Offizialdelikt und fällt (sofern die Strafdrohungen in einzelnen Varianten nicht über fünf Jahren Freiheitsstrafe liegen und gem § 31 Abs 3 Z 1 StPO Schöffengerichtszuständigkeit begründen) jedenfalls (zT gem § 31 Abs 4 Z 2 iVm § 30 Abs 1 Z 9 StPO ausnahmsweise) in die Zuständigkeit des Einzelrichters am Landesgericht. Insbesondere ist gem § 30 Abs 1 Z 9 StPO iZm § 207a Abs 3 »Fall 1« (besser[2416] wohl »Satz 1«, der die mündigen Minderjährigen betrifft) und Abs 3a (ebenfalls bezogen auf Satz 1 der gesplitteten Strafdrohung des Abs 3)

2413 Zum Umfang des »Gewahrsamsbegriffs« siehe ausf *Hochmayr,* Besitz, 65 ff.

2414 Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201) <conventions.coe.int/Treaty/en/Treaties/Html/201.htm> (01.04.2014); BGBl III 96/2011.

2415 Siehe *Hinterhofer* in SbgK § 207a Rz 78 mwN.

2416 Da eine weiterreichende Differenzierung der Tathandlungen üblicherweise durch Fallbestimmungen realisiert wird und nicht durch die Sätze (zB § 207a Abs 3 Satz 1 Fall 1).

Eigenzuständigkeit des Einzelrichters des Landesgerichts gegeben. § 207a Abs 3 Satz 2 sowie der darauf bezugnehmende Abs 3a, sofern es unmündige Personen betrifft, fallen aufgrund der Strafdrohung von »bis zu zwei Jahren« Freiheitsstrafe ohnehin in die Zuständigkeit des Einzelrichters am Landesgericht (§ 31 Abs 4 Z 1 StPO).

6. Wissentliche Betrachtung pornographischer Darbietungen Minderjähriger (§ 215a Abs 2a)[2417]

> § 215a [Auszug] (2a) Wer wissentlich eine pornographische Darbietung, an der eine mündige minderjährige Person mitwirkt, betrachtet, ist mit Freiheitsstrafe bis zu einem Jahr zu bestrafen. Mit Freiheitsstrafe bis zu zwei Jahren ist zu bestrafen, wer wissentlich eine pornographische Darbietung, an der eine unmündige Person mitwirkt, betrachtet.[2418]

Mit Einführung des § 215a Abs 2a durch die Strafgesetznovelle 2011[2419] wurde der Umsetzung von Art 21 Abs 1 lit c des Übereinkommens des Europarates zum Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch[2420] Rechnung getragen.

Art 21 Abs 1 lit c der Konvention sieht vor, den wissentlichen Konsum einer pornographischen Darbietung, an der Kinder mitwirken, unter Strafe zu stellen. Unter Kindern im Sinn dieser Vorgabe versteht der Konventionsgeber nach Art 3 lit a Personen unter 18 Jahren. Geschützt werden – also nach österr Rechtsterminologie – die Minderjährigen ua vor sexueller Ausbeutung.[2421]

Als Tathandlung ist das wissentliche Betrachten einer pornographischen Darbietung, an der ein mündiger Minderjähriger (Satz 1) bzw ein Unmündiger (Satz 2) mitwirkt, normiert. Unmündig ist eine Person gem § 74 Abs 1 Z 1, wenn sie das 14. Lebensjahr noch nicht vollen-

2417 Es wird nachfolgend lediglich die hier interessierende Bestimmung des § 215a Abs 2a behandelt. Die übrigen Delikte des § 215a werden mangels relevanter Computerstrafrechtsbezogenheit ausgeklammert.

2418 BGBl 60/1974 idF I 116/2013.

2419 BGBl I 130/2011.

2420 Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201), <conventions.coe.int/Treaty/en/Treaties/Html/201.htm> (01.04.2014); BGBl III 96/2011.

2421 Vgl *List* in SbgK § 215a Rz 4 (Stand November 2009).

det hat. Um einen mündigen Minderjährigen handelt es sich gem § 74 Abs 1 Z 3 (iZm § 74 Abs 1 Z 1), wenn die Person zwar das vierzehnte, jedoch nicht das achtzehnte Lebensjahr vollendet hat. Nach der jeweiligen Eigenschaft des Tatobjekts richten sich auch die unterschiedlich hohen (gesplitteten) Strafdrohungen.[2422]

§ 215a Abs 2a stellt ein schlichtes Tätigkeitsdelikt dar, da es auf keinen tatbestandlichen Erfolg ankommt und mit dem Betrachten der inkriminierten Darbietung das Delikt vollendet ist.

7. Pornographische Darbietung

Im Unterschied zu einer pornographischen Darstellung nach § 207a Abs 4 handelt es sich bei einer pornographischen Darbietung um ein aktuelles (»Live«-)Geschehen.[2423] Das Europaratsübereinkommen unternimmt keine Begriffsbestimmung und überlässt die Definition den Vertragsstaaten, was zB die Berücksichtigung des öffentlichen, privaten, kommerziellen oder nicht kommerziellen Charakters für eine Begriffsbestimmung anlangt. Wesentlich ist allerdings der Zweck des Art 21 des Übereinkommens, den die Konventionsverfasser darin sehen, dass »the provision is intended to deal essentially with organised live performances of children engaged in sexually explicit conduct«.[2424]

Art 2 lit e RL 2011/93/EU versteht hingegen unter Darbietung die »Live-Zurschaustellung für ein Publikum, einschließlich mittels Informations- und Kommunikationstechnologie«.

§ 215a Abs 2a erfasst daher als Darbietung entsprechende Handlungen, die »in Echtzeit« stattfinden, wie dies etwa beim Besuch einer Live-Aufführung oder bei Direktübertragungen (sog »Live-Streaming«) über das Internet mittels Web-Cam der Fall sein kann.

Film- oder Bildmaterial, das von einem solchen Geschehen angefertigt wurde, aber erst zu einem späteren Zeitpunkt – zB im Internet – zugänglich gemacht wird, stellt folglich keine »Darbietung«, sondern – bei entsprechender Mitwirkung von Minderjährigen – eine pornographische »Darstellung« iSd § 207a Abs 4 dar. Abgespeicherte

2422 Diese Aufsplittung wurde aus dem Vorschlag der RL 2011/93/EU übernommen; siehe aber die Überlegungen zu § 207a Abs 3 oben.

2423 Vgl *Philipp* in WK² § 215a Rz 10a (Stand März 2014).

2424 ER (CETS 201) Pkt 147, <conventions.coe.int/Treaty/EN/Reports/Html/201.htm> (01.04.2014).

Bilder und Videos sind daher grundsätzlich nicht mehr vom Begriff der Darbietung umfasst. Die Strafbestimmung des § 215a Abs 2a geht daher als lex specialis dem Zugreifen auf pornographische Darstellungen iSd § 207a Abs 3a vor.

Bei technischer Aufbereitung einer pornographischen Darbietung kann dies nur beim »Live-Streaming« bzw »Real-Time-Streaming«, wie bspw über Websites oder Live-Video-Chats (zB Skype), der Fall sein. Beim Live-Streaming werden die Inhalte während der Übertragung (in Echtzeit) aufgezeichnet, wohingegen beim sog »File-Streaming« die Inhalte vor der Übertragung aufgenommen werden bzw schon vorliegen und in weiterer Folge lediglich die Datei progressiv übertragen wird.[2425]

Wird über eine geeignete Web- oder Phone-Cam inkriminiertes Bildmaterial in Echtzeit (der tatsächlichen geschlechtlichen Handlungen) ins Internet übertragen, liegt begrifflich solange eine »Darbietung« vor, als die geschlechtliche Handlung tatsächlich noch andauert und eingespeist wird, selbst wenn – wie jede Live-Übertragung ins Internet – technisch bedingt eine Zwischenspeicherung zu einer geringfügig zeitversetzten[2426] Übertragung führt. Während des Zugriffs auf den Live-Stream wird auf dem Endgerät (Computer, Smartphone etc) des Betrachters jedenfalls eine technisch notwendige flüchtige Kopie im Arbeitsspeicher erzeugt, die letztlich das Datenmaterial der Betrachtung darstellt. Aber auch aufgrund von kürzeren oder längeren Übertragungswegen und der jeweiligen Auslastungen und Verarbeitungsgeschwindigkeiten der beteiligten Server entstehen Übertragungsverzögerungen. Solche Zwischenspeicherungen und Verzögerungen sind – wie bereits angemerkt – für das Unmittelbarkeitserfordernis der Wahrnehmung der Darbietungen weitgehend unbeachtlich.

Im Unterschied zum klassischen Download, wo eine Datei als Ganze vollständig und uno actu übertragen wird, findet beim Real-Time-Streaming die Übermittlung der Inhalte über einen andauernden »Datenstrom« in Form von Datenpaketen statt, die annähernd in Echtzeit übertragen und nach Erhalt sofort ausgeführt werden. Während ein Teil bereits abgespielt wird, werden die weiteren Datenpakete fortlaufend übertragen und nachgeladen (sog »Pufferung«).[2427]

2425 Vgl *Dickreiter/Dittel/Hoeg/Wöhr,* Handbuch der Tonstudiotechnik. Bd I[8] (2014) 1158.

2426 IdR handelt es sich dabei von einigen Millisekunden bis zu wenigen Sekunden.

2427 Vgl dazu *Kurose/Ross,* Computernetzwerke[4], 632 ff; weiters *Longolius,* Web-TV. AV-Streaming im Internet (2011) 43 ff; auch *Dickreiter/Dittel/Hoeg/Wöhr,* Tonstudiotechnik[8], 1152 ff.

Hat die tatsächliche Handlung bereits aufgehört, so stellt das Bildmaterial, das ab dem Zeitpunkt der Beendigung aufgrund der temporären Zwischenspeicherung zeitversetzt ins Internet übertragen wird, nunmehr eine pornographische Darstellung dar. Dies ergibt sich daraus, dass es sich nunmehr um ein historisches Geschehen handelt und nicht aus der notwendigen Zwischenspeicherung, wie es der Gesetzgeber begründet.[2428] Denn selbst wenn im umgekehrten Fall ein Live-Geschehen zeitversetzt übertragen wird, liegt solange eine Darbietung iSd § 215a Abs 2a vor, bis das tatsächliche Geschehen aufhört. Ab diesem Zeitpunkt wird die Darbietung zur Darstellung iSd § 207a.

Eine tatbildliche Darbietung kann in Form eines Live-Videos oder von (Live-)Einzelbildern vorliegen, die noch während einer gerade stattfindenden pornographischen Handlung (an der eine minderjährige Person mitwirkt) ins Internet gestellt werden. Werden Einzelbilder von einer Handlung vorerst aufgezeichnet und zeitlich erst nach der tatsächlichen geschlechtlichen Handlung ins Internet gestellt, ist für ein wissentliches Betrachten dieser Darstellungen wiederum § 207a Abs 3a anzuwenden. Selbst das Aufzeichnen einer Live-Übertragung (zB durch eine zeitgesteuerte Aufnahme[2429]) – ohne dass währenddessen der Aufnehmende die Darbietung selbst betrachtet – führt dazu, dass nach Beendigung der realen Handlung insgesamt eine pornographische Darstellung iSd § 207a Abs 3 in Form eines Videoclips besessen wird.

Gem § 215a Abs 3 wirkt an einer pornographischen Darbietung mit, wer dabei eine auf sich selbst reduzierte, von anderen Lebensäußerungen losgelöste und der sexuellen Erregung eines Betrachters dienende geschlechtliche Handlung an sich selbst, an einer anderen Person oder mit einem Tier vornimmt, eine solche geschlechtliche Handlung an sich vornehmen lässt oder auf solche Weise seine Genitalien oder seine Schamgegend zur Schau stellt.

8. Tathandlung »Betrachten«

Unter »Betrachten« einer solchen Darbietung ist jede Form der visuellen Wahrnehmung (zB Live-Aufführung vor Ort oder Live-Übertragung im

2428 Siehe ErlRV 1505 BlgNR XXIV. GP, 8.
2429 Vergleichbar mit einem Videorekorder.

Internet) zu verstehen.[2430] Wobei zu ergänzen ist, dass es naturgemäß eine »unmittelbare« Wahrnehmung sein muss, handelt es sich doch um ein gerade stattfindendes Geschehen. Zeichnet der Täter einen Internet-Live-Stream auf, in dem er diesen auf seiner Festplatte abspeichert, um das Video später anzusehen, ist nach § 207a Abs 3 vorzugehen.

Die Tathandlung des Betrachtens von Darbietungen weist – im Vergleich zur korrespondierenden Bestimmung bezüglich Darstellungen des § 207a Abs 3a, wo als Tathandlung das weiterreichende »Zugreifen« gewählt wurde[2431] – auf ein auf das »bloße« Ansehen beschränktes Verhalten hin. Ein Betrachten verlangt – im Gegensatz etwa zum bloßen »Sehen« – eine gewisse Zeitdauer.[2432] Die Darbietungen müssen daher bewusst wahrgenommen werden. Ein – sofern dies überhaupt der Realität entspricht – zufälliger Klick auf eine inkriminierte Live-Übertragung im Internet, bei dem der Nutzer »im Augenwinkel« Darbietungen zwar erkennen konnte, er diese aber nicht gezielt visuell konsumiert, da er es eben auf ein solches Material nicht abgesehen hat, stellt kein tatbestandliches »Betrachten« dar.

Das Betrachten wurde vom Gesetzgeber offenbar deshalb gewählt, weil im englischen Originaltext des Europaratsübereinkommens und der Richtlinie des Europäischen Parlamentes und des Rates zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornographie und zur Ersetzung des Rahmenbeschlusses 2004/68/JI[2433] die Tathandlung in »attending pornographic performances« besteht und die Übersetzungen uneinheitlich sind.[2434] In der deutschen Übersetzung des Art 21 Abs 1 lit c des Übereinkommens des Europarates findet sich als Tathandlung der »Besuch einer pornographischen Darbietung«. Hingegen wird Art 4 Abs 4 RL 2011/93/EU in der deutschen Übersetzung mit »an pornographi-

2430 Vgl ErlRV 1505 BlgNR XXIV. GP, 8; weiters *Hinterhofer/Rosbaud,* BT II[5] § 215a Rz 6.

2431 Weil hier bereits das Zugreifen auf das Bildmaterial im Internet, ohne die Inhalte aber tatsächlich betrachten zu müssen, schon erfasst ist (siehe dazu bereits S 499 ff). Beim Betrachten iSd § 215a Abs 2a reicht aber das bloße Zugreifen auf eine Streaming-Datei für eine Verwirklichung noch nicht aus. Es könnte aber eine ausführungsnahe Handlung vorliegen, die zu einer Versuchsstrafbarkeit führt.

2432 Vgl etwa *Philipp* in WK[2] § 215a Rz 10a.

2433 Richtlinie 2011/93/EU des Europäischen Parlaments und des Rates vom 13. Dezember 2011 zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie sowie zur Ersetzung des Rahmenbeschlusses 2004/68/JI des Rates, ABl L 2011/335, 1 idF L 2012/18.

2434 Vgl Art 21 Abs 1 lit c Europaratsübereinkommen bzw Art 4 Abs 4 RL 2011/93/EU.

schen Darbietungen teilnehmen« umschrieben. In jedem dieser Fälle wird aber auf die strafrechtliche Verantwortung des wissentlichen Zuschauers fokussiert, weshalb in den GMat die Tathandlung des »Betrachtens« am treffendsten erachtet wird.[2435] Ein Betrachten verlangt hingegen, sowohl nach dem Wortlaut interpretiert als auch wie es in den GMat umschrieben wird, eine »visuelle Wahrnehmung«[2436]. Streng genommen scheidet daher eine blinde Person als Tatsubjekt a priori aus. Darbietungen im Sinne eines tatsächlichen Live-Geschehens sind audiovisueller Natur. Sie bedienen daher sowohl den visuellen als auch den auditiven Sinn eines Menschen. Ein derartiger Live-Stream im Internet, würde prinzipiell ebenfalls eine AV-Medienübertragung in Bild und Ton darstellen. Aus diesem Grund könnte man sich gerade bei pornographischen Darbietungen, die – anders als bloße Fotografien – die Eigenschaft der auditiven Wahrnehmbarkeit besitzen, vorstellen, dass sich eine sehbehinderte Person ihre sexuelle Erregung an den geschlechtlichen Handlungen, an denen Minderjährige mitwirken, allein dadurch verschafft, dass sie die dabei gesprochenen Stimmen, Laute bzw einstudierten Dialoge anhört, die offensichtlich von einer minderjährigen Person stammen. Insoweit ist die Tathandlung des Betrachtens gegenüber einer Tathandlung »Teilnehmen«[2437] bzw »Besuchen«[2438], insb was eine Live-Aufführung anlangt, eingeengt. An einer anderen Stelle – nämlich zu § 207a – setzte der JA dem »bloßen Betrachten« den Klammerausdruck »(der ›Konsum‹)« nach, was wohl zum Ausdruck bringen soll, dass hier das Betrachten iSd Konsumierens zu pönalisieren sei, und (noch) nicht der Besitz oder eine auf einen solchen ausgerichtete Verschaffungshandlung.[2439] (Der Verschaffungsakt selbst ist kein Konsum, sondern er geht einem solchen idR voran.) Eine genaue Begründung fehlt. Auch findet sich keinerlei Information darüber, warum im Fall des § 207a Abs 3a nun aber das »Zugreifen« (und daher nicht bloß der Konsum) und nicht das »Betrachten« als Tathandlung gewählt wurde. Wollte der Gesetzgeber das »Betrachten« tatsächlich iSd umfassenderen Begriffs des »Konsumierens« verstanden wissen,

2435 Siehe ErlRV 1505 BlgNR XXIV. GP, 8.
2436 Vgl ErlRV 1505 BlgNR XXIV. GP, 8; weiters *Hinterhofer/Rosbaud,* BT II[5] § 215a Rz 6.
2437 Vgl die deutsche Übersetzung des Art 4 Abs 4 RL 2011/93/EU, wo es mit »an pornographischen Darbietungen teilnehmen« umschrieben wird.
2438 Vgl die deutsche Übersetzung des Art 21 Abs 1 lit c des Europaratsübereinkommens, wo es »Besuch einer pornographischen Darbietung« heißt.
2439 Siehe JAB 106 BlgNR XXIV. GP, 34.

hätte er es wohl auch in beiden Bestimmungen verwenden können bzw müssen.[2440] Wesentlich ist, dass in keiner Bestimmung eine Entgeltlichkeit des Konsums der Tatobjekte eine Rolle spielt. Mein Vorschlag wäre, die Tathandlungen sprachlich dem § 207a Abs 3a anzugleichen und die Strafbarkeit iSd § 215a Abs 2a ebenfalls auf den Verschaffungsakt vorzuverlegen. Was die Wahrnehmung der Darbietung im Wege einer Direktübertragung zB im Internet anlangt, so könnte ebenfalls – wie das »Zugreifen« in § 207a Abs 3a – auf eine Audio-Video neutrale Begrifflichkeit abgestellt werden, wie zB »wahrnimmt«[2441], »zugreift«[2442] bzw »sich zugänglich macht« oder ggf »benützt«. Um daher sämtliche als strafwürdig erachtete Sachverhaltsvarianten zu erfassen, sollten mehrere Handlungsalternativen auch gesetzlich angeführt werden. Dabei könnte zumindest an eine generalklauselartige Auffangtathandlung wie »oder sich sonst zugänglich macht« gedacht werden. Andernfalls wäre zwar das Zugreifen auf eine kinderpornographische Abbildung im Internet (auch) für einen Blinden als Täter strafbar (§ 207a Abs 3a), nicht aber das Betrachten eines audiovisuellen Live-Streams einer kinderpornographischen Darbietung.

Mag § 215a Abs 2a hins des Betrachtens gegenüber dem Zugreifen in § 207a Abs 3a enger sein, so ist § 215a Abs 2a, was die weiteren Tatmodalitäten anlangt, dennoch weiter gefasst. Wie oben ausgeführt, macht sich gem § 207a Abs 3a nur strafbar, wer auf pornographische Darstellungen (wissentlich) im »Internet« zugreift. § 215a Abs 2a kennt so eine Einschränkung nicht. § 207a Abs 3a ist daher – anders als § 215a Abs 2a – medien- bzw technikgebunden.[2443]

9. Subjektive Tatseite

Auf der subjektiven Tatseite muss der Täter in seinem Tatbildvorsatz wissentlich iSd § 5 Abs 3 handeln. Demzufolge muss er es für gewiss halten, dass ein Minderjähriger (§ 215a Abs 2a erster Satz) bzw ein Unmündiger (§ 215a Abs 2a zweiter Satz) an der pornographischen Darbietung mitwirkt.

2440 Siehe dazu JAB 106 BlgNR XXIV. GP, 34; etwa in die Richtung *Hinterhofer* in SbgK § 207a Rz 61.

2441 Was sämtliche menschliche Sinne mitumfassen würde.

2442 Siehe § 207a Abs 3a.

2443 Mehr dazu oben S 499 ff.

10. Sonstiges

Das Offizialdelikt des § 215a Abs 2a erster Satz fällt aufgrund der Strafdrohung in die sachliche Zuständigkeit des Bezirksgerichts, was wohl auf ein Redaktionsversehen schließen lässt, da für die vergleichbare Bestimmung des § 207a Abs 3a (auch hins mündiger Minderjähriger) – wie für die des § 207a Abs 3 (auch Satz 1) – die (teils ausnahmsweise) Zuständigkeit des Einzelrichters am Landesgericht gem § 31 Abs 4 Z 2 StPO iVm § 30 Abs 1 Z 9 StPO besteht.[2444] Dies sollte wohl auch für § 215a Abs 2a Satz 1 nachgebessert werden.

§ 215a Abs 2a zweiter Satz fällt gem § 31 Abs 4 Z 1 StPO in die Zuständigkeit des Einzelrichters am Landesgericht.

B. Exkurs: Pornographiegesetz

§ 1 (1) Eines Verbrechens macht sich schuldig, wer in gewinnsüchtiger Absicht

a) unzüchtige Schriften, Abbildungen, Laufbilder oder andere unzüchtige Gegenstände herstellt, verlegt oder zum Zwecke der Verbreitung vorrätig hält,

b) solche Gegenstände einführt, befördert oder ausführt,

c) solche Gegenstände anderen anbietet oder überläßt, sie öffentlich ausstellt, aushängt, anschlägt oder sonst verbreitet oder solche Laufbilder anderen vorführt,

d) sich öffentlich oder vor mehreren Leuten oder in Druckwerken oder verbreiteten Schriften zu einer der in den lit. a bis c bezeichneten Handlungen erbietet,

e) auf die in lit. d bezeichnete Weise bekanntgibt, wie von wem oder durch wen unzüchtige Gegenstände erworben oder ausgeliehen oder wo solche Gegenstände besichtigt werden können.

(2) Die Tat wird mit Freiheitsstrafe bis zu einem Jahr bestraft. Neben der Freiheitsstrafe kann eine Geldstrafe bis zu 360 Tagessätzen verhängt werden.

2444 Siehe *Bergauer/Schmölzer* in Jahnel/Mader/Staudegger, IT-Recht[3], 635 (680).

> (3) Wurde die Tat mit Beziehung auf ein Druckwerk verübt, so sind die für das Vergehen nach § 516 StG. geltenden Bestimmungen des Preßgesetzes über den Verfall des Druckwerkes, die Unbrauchbarmachung der zu seiner Herstellung dienenden Platten und Formen, die vorläufige Beschlagnahme und das Strafverfahren in Preßsachen überhaupt dem Sinne nach anzuwenden.[2445]

Neben den angesprochenen Delikten des Kernstrafrechts könnte sich auch die Anwendbarkeit des § 1 Pornographiegesetz[2446] in solchen Fällen ergeben, wobei das PornG technik- und medienneutrale Tatbestände enthält. Wesentlich ist jedoch, dass sich die Strafbestimmung des § 1 PornG ausschließlich an Produzenten und Distributoren richtet.[2447] Die verschiedenen Erscheinungsformen der erfassten Handlungen sind lediglich dann strafbar, wenn sie in »gewinnsüchtiger Absicht« begangen worden sind. Gewinnsucht liegt idS immer dann vor, »wenn durch die Verwendung des Tatobjektes im wirtschaftlichen Sinn ein Vermögensvorteil entsteht bzw. entstehen soll«.[2448] Sie kann auch in der Verwendung eines unzüchtigen Werkes als Werbemittel begründet sein. Entscheidend ist, dass der Vermögensvorteil unter Verwendung des Tatobjektes im wirtschaftlichen Sinn gezogen werden soll, und zwar entweder unmittelbar aus diesem Tatobjekt oder mit Hilfe desselben.[2449]

Tatobjekte des § 1 PornG sind im Wesentlichen »unzüchtige Schriften, Abbildungen, Laufbilder oder andere unzüchtige Gegenstände«. Daraus folgt, dass die Tatobjekte des § 1 PornG in einer in der Außenwelt verkörperten Form existieren müssen.[2450] Im Zusammenhang mit unkörperlichen Daten bedeutet dies, dass die inkriminierten Dateien auf Datenträgern abgespeichert sein müssen.[2451] Eine »dynamische Verkörperung«[2452] während eines Übertragungsvorgangs, reicht dazu nicht aus. Die Tathandlung des § 1 Abs 1 lit a dritter Fall PornG »zum Zwecke der Verbreitung vorrätig halten« beschreibt den strafbaren Besitz, wenn dieser in der Absicht erfolgt, diese Gegenstände anderen zu-

2445 BGBl 97/1950 idF 422/1974.
2446 Pornographiegesetz, BGBl 97/1950 idF 422/1974.
2447 Vgl *Reindl-Krauskopf,* Computerstrafrecht², 46.
2448 Siehe OGH 24.11.1978, 13 Os 102/78.
2449 Vgl RIS-Justiz RS0087997 mwN.
2450 So auch *Schmölzer* in FS Posch, 321 (334); *Reindl-Krauskopf,* Computerstrafrecht², 45.
2451 Vgl *Reindl-Krauskopf,* Computerstrafrecht², 45.
2452 Siehe zu dieser hier verwendeten Begrifflichkeit auch S 481 ff.

gänglich zu machen.[2453] Der bloße Besitz durch einen Konsumenten ist von dieser Strafnorm daher nicht erfasst.

Ob nun die Darstellung einer Schrift durch programmtechnische Abläufe auf einem visuellen Ausgabegerät (zB Monitor) oder die Anweisungen einer Schriftendarstellung in einer (Binär-)Datei selbst, als Schriften iSd § 1 PornG anzusehen sind, ist strittig.

Der Begriff der Schrift ist im PornG gar nicht, im StGB nicht ausdrücklich definiert. Lediglich im Legalbegriff der »Urkunde« in § 74 Abs 1 Z 7[2454] findet sich der nicht näher bestimmte Terminus der Schrift. Für das Urkundenstrafrecht kann daher das Schrifterfordernis wie folgt zusammengefasst werden:

»Schrift sind nach hM alle Zeichen, die dazu bestimmt sind, einen beliebigen Gedankeninhalt für andere lesbar zu machen. Schrift setzt somit grundsätzlich die Verwendung von Buchstaben und/oder Zahlen voraus. […] Im Regelfall wird die schriftliche Erklärung auf Papier, Karton, Pergament oder ähnlichem angebracht sein; als Unterlage kommen aber auch andere Materialien in Betracht, wie Stoffe, Holz oder Metall. Ohne Bedeutung ist schließlich auch das verwendete Schreibmaterial; allerdings muss die Verkörperung des Gedankeninhalts von einiger Dauerhaftigkeit sein«.[2455] Ergänzend wird ua von *Reindl-Krauskopf* ausgeführt, dass eine Schrift nur sein könne, was der Mensch mit freiem Auge unmittelbar, also ohne technische Hilfsmittel[2456], wahrnehmen kann.[2457] Bezieht sich *Reindl-Krauskopf* dabei auf die Rsp, so muss aber angemerkt werden, dass in concreto der Magnetstreifen einer Bankomatkarte angesprochen war, der als solcher für das menschliche Auge nicht lesbar ist und deshalb keine Schrift in der Bedeutung des § 74 Abs 1 Z 7 darstellt.[2458] Vielmehr ging es in dieser E[2459] aber nur um die Frage der Urkundenqualität einer Bankomatkarte. Für den hier interessierenden Gegenstand besitzt sie somit nur begrenzt Relevanz.

2453 Vgl *Hochmayr,* Besitz, 18.

2454 § 74 Abs 1 Z 7 StGB »Urkunde: eine Schrift, die errichtet worden ist, um ein Recht oder ein Rechtsverhältnis zu begründen, abzuändern oder aufzuheben oder eine Tatsache von rechtlicher Bedeutung zu beweisen.«

2455 Vgl *Schmölzer* in FS Posch, 321 (334); weiters *Bergauer/Schmölzer* in Jahnel/Mader/Staudegger, IT-Recht[3], 635 (684).

2456 Abgesehen von Hilfsmitteln, die die Wahrnehmungsfähigkeit des Auges unterstützen, wie Brille oder Lupe.

2457 Vgl *Reindl-Krauskopf,* Computerstrafrecht[2], 45; siehe auch ErlRV 309 BlgNR XXII. GP, 5.

2458 Vgl RIS-Justiz RS0093167 mwN.

2459 OGH 19.12.1984, 11 Os 184/84.

Gerade was nämlich die Grundintention des PornG – im Gegensatz zu den teleologischen Zielen des Urkundenstrafrechts – anlangt, ist nicht zu verstehen, warum auf das strenge Schriftverständnis des »Urkundenstrafrechts« abgestellt werden sollte. Es muss doch wohl aus in der hier interessierenden Thematik die formale Umschreibung, dass eine Schrift alle Zeichen erfasst, »die dazu dienen, einen Gedanken zu verkörpern und für andere lesbar zu machen« ausreichend sein.[2460]

Es ist daher *Schmölzer* beizupflichten, wenn sie argumentiert, dass in diesem Zusammenhang auch der Text auf einem Bildschirm eine solche Schrift darstellen sollte, da auch in diesem Fall ein Gedankeninhalt für jemanden über eine gewisse Zeit lesbar ist und es ohnehin weder auf die verwendete Schriftart oder Sprache, noch auf das Schreibmaterial ankommt.[2461]

Auch *Reindl-Krauskopf* schließt eine Interpretation der Schrift iZm dem PornG, die sich nicht am Urkundenstrafrecht orientiert, nicht aus, meint aber dann doch, dass man iSd Einheit der Rechtsordnung vom selben Begriff ausgehen sollte.[2462] Dies ist mE jedoch keine ausreichende Begründung, weil es doch nicht um die Vergleichbarkeit von Begriffen, sondern um kriminalpolitische Zwecke geht. Das Pornographiegesetz als spezielles Sachgesetz – wie auch in anderem Zusammenhang das DSG 2000 – regelt eine Materie, die ihre eigenen Wertvorstellungen und Begrifflichkeiten besitzt. Der Gesetzgeber sollte daher zur Klarstellung eine – gegenüber dem Urkundenstrafrecht neutrale – materienübergreifende Legaldefinition der »Schrift« schaffen, auf die das strenge Schriftlichkeitserfordernis des Urkundenstrafrechts in weiterer Folge bloß aufbaut.

Indiziert der Gegenstandsbegriff auch eine gewisse Dauerhaftigkeit der körperlichen Fixierung[2463], so ist diese mE ebenso in der Form einer fortgesetzten Reproduzierbarkeit der Darstellung gegeben. Eine solche wäre dabei auch bei einer Text- bzw Binärdatei in einem gewöhnlichen Dateiformat[2464] gegeben, die zwar ubiquitär verwend-

2460 Zu dieser Aussage grundlegend *Kienapfel/Schroll* in WK² § 223 Rz 28.

2461 Siehe *Schmölzer* in Jahnel/Schramm/Staudegger, Informatikrecht², 335 (362 f).

2462 Vgl *Reindl-Krauskopf,* Computerstrafrecht², 45.

2463 Keine Dauerhaftigkeit besitzen daher zB Zeichen in den Sand, in den Schnee oder auf eine beschlagene Fensterscheibe geschrieben (vgl *Kienapfel/Schroll* in WK² § 223 Rz 36).

2464 Dateiformate ermöglichen den jeweils durch ein spezielles Format (zB Musik- bzw Videodatei, Bild- oder Textdatei) festgelegten Zugriff auf die Inhalte der Da-

bar, aber doch nachhaltig einsehbar konzipiert ist. Der Gedankeninhalt (Information) einer solchen Datei kann prinzipiell so lange eingesehen werden, bis die Datei gelöscht oder der Zugriff auf diese oder auf den Datenträger verhindert wird.[2465] Die technische Aufbereitung der Inhalte zur visuellen Darstellung ändert schließlich auch nichts an den inkriminierten Inhalten. Auf das Kriterium, dass der Mensch die Datei in ihrer computertechnischen Konzeption selbst nicht lesen kann, kommt es bei einem solchen Ansatz schon aus Sachlichkeitserwägungen nicht an, sofern die Datei überhaupt funktionsbereit und verarbeitbar ist.[2466]

Was die »Unzüchtigkeit« der inkriminierten Gegenstände anlangt, so ergibt sich eine solche iZm Datenträgern klarerweise[2467] aus dem Inhalt der darauf gespeicherten Daten.[2468] Dem Täter muss die Unzüchtigkeit der Gegenstände aber nicht bewusst sein. Es genügt, dass er die Tatsachen kennt, die im konkreten Fall das rechtliche Merkmal der Unzüchtigkeit des Deliktsobjektes verwirklichen, also sich jener Tatsachen bewusst ist, aus denen das Gericht auf die Unzüchtigkeit, Schriften, Abwicklungen usw schließt.[2469] Dabei ist der normative Gehalt des Tatbildmerkmales »unzüchtig« an der herrschenden Wertvorstellung der Gesellschaft im Sinne einer »opinio communis« orientiert, die über längere Zeiträume hin einem gewissen Wandel unterliegt.[2470]

Wird § 1 PornG in einer seiner Begehungsweisen durch den Inhalt eines Mediums verwirklicht, liegt ein Medieninhaltsdelikt (§ 1 Abs 1 Z 12 MedienG[2471]) vor. Als Medium kann gem § 1 Abs 1 Z 1 MedienG jedes Mittel zur Verbreitung von Mitteilungen oder Darbietungen mit gedanklichem Inhalt in Wort, Schrift, Ton oder Bild an einen größeren Personenkreis im Wege der Massenherstellung oder der Massen-

---

ten. Spezielle Dateiformate werden idR auch mit spezifischen Programmen verknüpft.

2465 Dies ist wohl den Textinhalten aus Büchern sehr ähnlich.

2466 Vgl auch das analoge Problem in § 3d VerbotsG (StGBl 13/1945 idF BGBl 148/1992); siehe *Bergauer/Schmölzer* in Jahnel/Mader/Staudegger, IT-Recht[3], 635 (686); weiters *Schmölzer,* Strafrechtliche Aspekte zum Thema Rassismus, Neonazismus und Rechtsextremismus im Internet, in Stiftung Dokumentationsarchiv des österreichischen Widerstandes (Hrsg), Das Netz des Hasses (1997) 246 (258 f); weiters *Schmölzer* in FS Posch, 321 (334).

2467 Die Festplatte selbst wird daher nicht als »unzüchtig« angesehen.

2468 Siehe *Reindl-Krauskopf,* Computerstrafrecht[2], 45; idS auch OGH 03.05.1973, 10 Os 46/73, bezüglich einer Langspielplatte.

2469 Siehe OGH 01.02.1972, 10 Os 256/71.

2470 Vgl OGH 05.03.1974, 10 Os 168/73.

2471 Mediengesetz, BGBl 314/1981 idF I 101/2014.

verbreitung in Frage kommen. Das können bspw Websites, Internet-Tauschbörsen, Chat-Rooms oder Massen-E-Mails[2472] sein.

Wird allerdings die Tathandlung nicht durch, sondern lediglich mit Beziehung auf Druckwerke begangen, liegt wiederum kein Medieninhaltsdelikt vor.[2473]

Aufgrund der Strafdrohung fällt § 1 PornG grundsätzlich in die sachliche Zuständigkeit des Bezirksgerichts (§ 30 Abs 1 StPO). Im Fall der Begehung als Medieninhaltsdelikt ist gem § 41 Abs 2 und 3 MedienG die Sonderzuständigkeit des Einzelrichters des Landesgerichts für Strafsachen gegeben.

(Exkurs Ende)

C. Anbahnung von Sexualkontakten zu Unmündigen (§ 208a) – »Cyber-Grooming«

§ 208a (1) Wer einer unmündigen Person in der Absicht, an ihr eine strafbare Handlung nach den §§ 201 bis 207a Abs. 1 Z 1 zu begehen,

1. im Wege einer Telekommunikation, unter Verwendung eines Computersystems oder

2. auf sonstige Art unter Täuschung über seine Absicht ein persönliches Treffen vorschlägt oder ein solches mit ihr vereinbart und eine konkrete Vorbereitungshandlung zur Durchführung des persönlichen Treffens mit dieser Person setzt, ist mit Freiheitsstrafe bis zu zwei Jahren zu bestrafen.

(1a) Wer zu einer unmündigen Person in der Absicht, eine strafbare Handlung nach § 207a Abs. 3 oder 3a in Bezug auf eine pornographische Darstellung (§ 207a Abs. 4) dieser Person zu begehen, im Wege einer Telekommunikation oder unter Verwendung eines Computersystems Kontakt herstellt, ist mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

(2) Nach Abs. 1 und 1a ist nicht zu bestrafen, wer freiwillig und bevor die Behörde (§ 151 Abs. 3) von seinem Verschulden erfahren hat, sein Vorhaben aufgibt und der Behörde sein Verschulden offenbart.

2472 Vgl dazu LG Klagenfurt 10.01.2008, 7 Bl 121/07y = jusIT 2008/44, 95 *(Bergauer);* vgl auch *Wittmann/Zöchbauer* in Röggla/Wittmann/Zöchbauer (Hrsg), Medienrecht. Praxiskommentar (2012) MedienG § 1 Rz 10.

2473 Siehe OGH 13.02.1997, 12 Os 183/96.

> (2) Nach Abs. 1 ist nicht zu bestrafen, wer freiwillig und bevor die Behörde (§ 151 Abs. 3) von seinem Verschulden erfahren hat, sein Vorhaben aufgibt und der Behörde sein Verschulden offenbart.[2474]

Durch die Strafgesetznovelle 2011[2475] trat mit 01.01.2012 unter der Deliktsbezeichnung »Anbahnung von Sexualkontakten zu Unmündigen« § 208a in Kraft. Vorlage seiner Normierung war Art 23 des Übereinkommens des Europarates zum Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch[2476], der das sog »Grooming« behandelt.[2477] Darunter wird die Kontaktanbahnung bzw Anwerbung eines Kindes für sexuelle Zwecke verstanden.[2478] Das Übereinkommen sieht aber – anders als die österr Umsetzung – ausschließlich Maßnahmen gegen das »Cyber-Grooming«, dh in Begehung über Informations- und Kommunikationstechnologie, vor.[2479]

> »Article 23 – Solicitation of children for sexual purposes
>
> Each Party shall take the necessary legislative or other measures to criminalise the intentional proposal, through information and communication technologies, of an adult to meet a child who has not reached the age set in application of Article 18, paragraph 2, for the purpose of committing any of the offences established in accordance with Article 18, paragraph 1.a, or Article 20, paragraph 1.a, against him or her, where this proposal has been followed by material acts leading to such a meeting.«

Unter »Kind« wird in diesem Konventionszusammenhang[2480] des Art 23 iVm Art 18 Abs 2 eine Person verstanden, die nach den einschlägigen Bestimmungen des innerstaatlichen Rechts noch nicht das gesetzliche Alter für sexuelle Handlungen erreicht hat. In Österreich kann dieses Alter der sexuellen Mündigkeit den Bestimmungen des §§ 206 und 207 entnommen werden. Dort muss es sich um »unmündige« Personen iSd § 74 Abs 1 Z 1 handeln.[2481]

2474 BGBl 60/1974 idF I 116/2013.
2475 BGBl I 130/2011.
2476 Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201), <conventions.coe.int/Treaty/en/Treaties/Html/201.htm> (01.04.2014); BGBl III 96/2011.
2477 Zur Begrifflichkeit siehe *Messner,* Anbahnung von Sexualkontakten zu Unmündigen. Der neue Grooming-Paragraf in § 208a StGB, JAP 2011/2012/12.
2478 ER (CETS 201) Pkt 156; weiters ErlStV 881 BlgNR XXIV. GP, 2 und 14.
2479 Siehe auch ErlStV 881 BlgNR XXIV. GP, 14; weiters ER (CETS 201) Pkt 159.
2480 Generell wird nach Art 3 lit a des Übereinkommens als »Kind« eine Person unter achtzehn Jahren verstanden.
2481 Vgl ErlStV 881 BlgNR XXIV. GP, 12.

Eine Anbahnung von Sexualkontakten zu Unmündigen kann in der Praxis so aussehen, dass etwa der Täter in Chat-Foren udgl vorgibt, selbst ein Kind zu sein, und so versucht, unmündige Personen dazu zu bringen, intime Dinge zu besprechen oder eindeutiges sexuelles Bildmaterial zu zeigen, um die Hemmschwelle zu senken.[2482] Wird eine unmündige Person zB dazu überredet, eigene sexualisierte Bilder anzufertigen und dem Täter zu übermitteln, könnte dieser damit einen Druck auf das Kind ausüben und dieses zu einem Treffen nötigen. Kommt es zu einem realen Treffen, könnte das Opfer sexuell missbraucht werden.[2483]

Gem § 208a Abs 1 macht sich strafbar, wer einer unmündigen Person in der Absicht, an ihr eine strafbare Handlung nach den §§ 201 bis 207a Abs 1 Z 1 zu begehen,

1. im Wege einer Telekommunikation, unter Verwendung eines Computersystems (online-Kontakt) oder
2. auf sonstige Art unter Täuschung über seine Absicht (offline-Kontakt)

ein persönliches Treffen vorschlägt oder ein solches mit ihr vereinbart und eine konkrete Vorbereitungshandlung zur Durchführung des persönlichen Treffens mit dieser Person setzt. Der Täter ist in diesem Fall mit Freiheitsstrafe bis zu zwei Jahren zu bestrafen.

1. § 208a Abs 1

§ 208a Abs 1 ist als mehraktiges Delikt aufgebaut, da neben den Begehungsweisen des Vorschlagens oder Vereinbarens eines persönlichen Treffens als erste Tathandlung zudem noch eine konkrete Vorbereitungshandlung für ein solches Treffen als zweite Tathandlung verlangt wird. Zwischen den beiden Tathandlungen kann prinzipiell eine sehr lange wie auch äußerst kurze Zeitdauer liegen, was iZm der Nachweisbarkeit des subjektiven Tatbestands, der im Zeitpunkt der Handlungsvornahme erfüllt sein muss, problematisch erscheint. Zudem ist auch bereits der Versuch strafbar.[2484]

2482 Siehe ua *Mahler,* »Grooming«: Anbahnung von Sexualkontakten zu Unmündigen, JSt 2012, 22.

2483 Vgl ErlRV 1505 BlgNR XXIV. GP, 5.

2484 Siehe bereits in *Bergauer/Schmölzer* in Jahnel/Mader/Staudegger, IT-Recht[3], 635 (681).

Der objektive Tatbestand umfasst das Vorschlagen oder Vereinbaren eines persönlichen Treffens mit einer unmündigen Person (iSd § 74 Abs 1 Z 1) über eine der angeführten Kommunikationsarten (sog »Cyber-Grooming«) oder unter Täuschung über die Absichten des Täters und darüber hinaus eine konkrete Vorbereitungshandlung zur Durchführung eines solchen Treffens. Die beiden Tathandlungen sind rechtlich gleichwertig.[2485]

Die erste Tathandlung ist hins beider Begehungsweisen verhaltensgebunden, da sie nur entweder online »im Wege einer Telekomunikation« oder »unter Verwendung eines Computersystems« (§ 208a Abs 1 Z 1), oder offline »unter Täuschung« über die wahren Absichten des Täters (§ 208a Abs 1 Z 2) begangen werden kann. Für die zweite Tathandlung kommt grundsätzlich jede Vorbereitungshandlung in Betracht, solange es sich dabei bereits um ein konkretes Verhalten zu einem tatsächlichen Treffen handelt.

a. IKT-Begehungsweisen

Unter Telekommunikation versteht man – wie auch in den §§ 119, 120 Abs 2a – den technischen Vorgang des Aussendens, Übermittelns und Empfangens von Nachrichten jeglicher Art in der Form von Zeichen, Sprache, Bildern oder Tönen mittels dazu dienender technischer Einrichtungen.[2486] Die Formulierung »unter Verwendung eines Computersystems« ist dagegen in dieser Form ungewöhnlich, wurde doch bisher in Ergänzung zur Telekommunikation überwiegend[2487] der Wortlaut »im Wege eines Computersystems« verwendet.[2488] Daraus könnte methodengerecht geschlossen werden, dass der Gesetzgeber durch die Verwendung unterschiedlicher Formulierungen auch Unterschiedliches meint. Er weist jedoch lediglich darauf hin, dass der Begriff »Computersystem« in § 74 Abs 1 Z 8 definiert ist.[2489] Man könnte daher davon ausgehen, dass eine Strafbarkeit auch dann vorliegt, wenn der Täter das Kind zu einem Treffen dadurch überreden will, dass er diesem ein Computersystem (vgl Notebook, Smartphone usw) als Geschenk

2485 Vgl *Philipp* in WK² § 208a Rz 6 (Stand März 2014).
2486 Vgl ErlRV 1505 BlgNR XXIV. GP, 6; siehe auch *Philipp* in WK² § 208a Rz 7.
2487 Vgl § 119 Abs 1 und § 119a Abs 1.
2488 In § 107a Abs 2 Z 2 Fall 2 wird von »unter Verwendung eines sonstigen Kommunikationsmittels« gesprochen.
2489 Siehe ErlRV 1505 BlgNR XXIV. GP, 6.

in Aussicht stellt, was auch in der Praxis nicht selten vorkommen dürfte. In einem derartigen Fall würde – auch bei einem persönlichen Ansprechen auf der Straße, in einem Brief usw – die erste Alternative des § 208a Abs 1 Z 1 erfüllt sein und nicht die eigentlich dafür intendierte zweite, bei der es – anders als bei den IKT-Kontaktformen der Z 1 – zu einer Täuschung des Opfers kommen müsste. Die Formulierung sollte daher auf einen spezifischeren und treffsicheren Wortlaut wie etwa »im Wege eines Computersystems« bzw »unter informationstechnischer Verwendung eines Computersystems« abgeändert werden. Ein Täuschungselement ist bei dieser IKT-Begehungsweise konventionsgemäß ohnedies nicht verlangt.[2490] Auch ist zu hinterfragen, warum überhaupt beide IKT-Varianten in Abs 1 Z 1 normiert wurden.[2491] Im konkreten deliktischen Zusammenhang kann es sich nur um Kommunikationsfälle handeln. An anderer Stelle[2492] wurde bereits ausgeführt, dass das Abstellen auf Telekommunikation einerseits und auf Computersysteme andererseits dem Umstand Rechnung tragen sollte, dass der Begriff des Computersystems in der CCC sehr weit definiert ist.[2493] Die damit angesprochen weiterführenden Erfassungsbereiche des Art 3 CCC betreffen aber jene Fälle, in denen Computerkommunikationen innerhalb eines Computersystems (zB vom Prozessor zur Grafikkarte)[2494] stattfinden und daher nicht unter das Telekommunikationsgesetz[2495] fallen. Für die hier deliktsgegenständliche Anforderung spielt dieses umfassendere Verständnis – wegen der bloß internen Übertragungsform ohne Außenwirkung – wohl keine Rolle.

b. Konventionelle Kontaktaufnahme

Über die Vorgaben der Konvention hinaus wurde – Stellungnahmen im Begutachtungsverfahren folgend – in § 208a Abs 1 Z 2 eine weitere Begehungsweise ohne IKT pönalisiert.[2496] Der Täter muss in diesem Fall der sonstigen Kontaktaufnahmen (zB persönliches Gespräch, Brief)

2490 Siehe bereits in *Bergauer/Schmölzer* in Jahnel/Mader/Staudegger, IT-Recht[3], 635 (682).
2491 Siehe *Mahler,* JSt 2012, 22.
2492 Zu § 119 und Begrifflichkeit des Computersystems nach der CCC.
2493 Vgl ErlRV 1166 BlgNR XXI. GP, 25.
2494 Vgl ER (ETS 185) Pkt 55.
2495 Vgl ErlRV 1166 BlgNR XXI. GP, 25.
2496 Vgl krit dazu *Messner,* JAP 2011/2012/12, 132.

die unmündige Person über seine Absicht – an ihr eine strafbare Handlung nach §§ 201 bis 207a Abs 1 Z 1 zu begehen[2497] – täuschen. Diese Begehungsweise hat Auffangcharakter und kommt auch nur zur Anwendung, wenn keine online-Kontaktierung (mit oder ohne Täuschung) stattgefunden hat. In der Begehungsweise des § 208a Abs 1 Z 2 liegt – nach Meinung des Gesetzgebers – die besondere Gefährlichkeit in der »Täuschung der unmündigen Person«.[2498] Wenn der Gesetzgeber nun allerdings darin die besondere Gefährlichkeit dieser Begehungsweise sieht, so impliziert dies für die Begehungsweise des § 208a Abs 1 Z 1, dass hier die »besondere Gefährlichkeit« bereits in der bloßen »Nutzung« informations- und telekommunikationstechnischer Systeme liegen muss.

Vermutlich hat dies der Gesetzgeber aus den Materialien des Europaratsübereinkommens abgeleitet, wo deshalb von einer besonderen Gefahr gesprochen wird, weil sich eine Überwachung der Kommunikationen im Internet und über Mobiltelefone als schwierig erweist.[2499] Eine solche Begründung ist aber in Anbetracht der bloßen sozial adäquaten Nutzung informations- und kommunikationstechnischer Systeme bzw des bloßen Betriebs solcher Systeme strikt abzulehnen. Andernfalls müsste zumindest auch die vorherrschende Ablehnung des Ingerenzprinzips zur Begründung einer Garantenstellung für Host-Provider überdacht werden.[2500] Aufgrund der offensichtlichen Verlagerung des spezifischen Unrechts auf die subjektive Tatseite fragt sich, ob die Sozialschädlichkeit des Täterverhaltens nicht hauptsächlich am Plan des Täters und daher an dessen Gesinnung ansetzt.[2501] Bejaht man eine solche Nähe zum Gesinnungsstrafrecht, fragt sich allerdings umso mehr, ob in diesem Fall tatsächlich die Tatbestandsumschreibung den strengen Erfordernissen des verfassungsrechtlichen Bestimmtheitsgebots entspricht.[2502]

Wie eine Täuschung iSd § 208a Abs 1 Z 2 erfolgen kann, richtet sich im Wesentlichen nach § 108 und § 146. Dazu können falsche Tatsachen

---

2497 Durch die Formulierung »strafbare Handlung nach den §§ 201 bis 207a Abs 1 Z 1« kann auch die Alterstoleranzklausel nach § 206 Abs 4 und § 207 Abs 4 als persönlicher Strafausschließungsgrund grundsätzlich (dh bezüglich §§ 206 und 207) zur Anwendung gelangen (ErlRV 1505 BlgNR XXIV. GP, 7).

2498 Siehe ErlRV 1505 BlgNR XXIV. GP, 6.

2499 ER (CETS 201) Pkt 159.

2500 Siehe dazu statt vieler etwa *Reindl-Krauskopf,* Computerstrafrecht[2], 122; weiters *Bergauer/Schmölzer* in Jahnel/Mader/Staudegger, IT-Recht[3], 635 (682 und 705).

2501 Siehe zu dieser Kritik *Mahler,* JSt 2012, 22.

2502 In diesem Sinne *Mahler,* JSt 2012, 22.

vorgespiegelt oder auch richtige Tatsachen entstellt oder unterdrückt werden. Auch zur Irreführung des Opfers unternommene schlüssige Handlungsweisen genügen.[2503] Täuscht der Täter eine unmündige Person allerdings nicht über seine Absichten – spricht er diese ggf sogar explizit an – und schlägt er ein Treffen vor, oder vereinbaren Täter und Opfer ein solches außerhalb der IKT-Kommunikationsformen, macht sich der Täter nicht nach § 208a strafbar. Gerade aus dieser Überlegung und in Anbetracht der besonderen Eigenschaft des Tatobjekts sowie des intendierten Rechtsgüterschutzes liegt die »besondere Gefährlichkeit« dieser Begehungsweise doch wohl nicht in der Täuschung, sondern in jeder konkreten Handlung, die eine unmündige Person zu einem Treffen für sexuelle Übergriffe bewegt, ob nun mittels Täuschung oder nicht.[2504]

Die zweite Tathandlung des mehraktigen Delikts erfordert eine konkrete Vorbereitungshandlung zur Durchführung des persönlichen Treffens mit dem Opfer. Sie wurde bewusst weit gefasst, um den verschiedenen Konstellationen in der Praxis ausreichend Rechnung zu tragen.[2505] Der Täter muss seine erste Tathandlung daher durch eine weitere Handlung bekräftigen. In den GMat werden dazu die Beispiele des Kaufs einer Fahrkarte zum Treffpunkt, aber auch bereits die Übermittlung einer Weg- oder Personenbeschreibung an das Opfer oder das Eintreffen des Täters am Tatort angeführt.[2506] »Konkret« meint, dass der Täter eine dem Treffen dienende Handlung setzen muss, die seinen Entschluss – das Zusammentreffen tatsächlich durchzuführen – in der Außenwelt manifestiert.[2507]

c. Subjektive Tatseite

In subjektiver Hinsicht muss der Täter über den bedingten Tatbildvorsatz bezogen auf sämtliche objektiven Tatbestandsmerkmale – insb auch die Unmündigkeit des Opfers[2508] betreffend – hinaus mit dem erweiterten Vorsatz in Form der Absicht (§ 5 Abs 2) handeln, an der un-

2503 Vgl ErlRV 1505 BlgNR XXIV. GP, 6 f.
2504 Siehe dazu schon *Bergauer/Schmölzer* in Jahnel/Mader/Staudegger, IT-Recht[3], 635 (682).
2505 Siehe ErlRV 1505 BlgNR XXIV. GP, 7.
2506 Siehe ErlRV 1505 BlgNR XXIV. GP, 7.
2507 Vgl *Bergauer/Schmölzer* in Jahnel/Mader/Staudegger, IT-Recht[3], 635 (683).
2508 Siehe *Hinterhofer/Rosbaud,* BT II[5] § 208a Rz 7.

mündigen Person eine strafbare Handlung nach §§ 201 bis 207a Abs 1 Z 1 zu begehen. Dem in einem Vorbereitungsdelikt grundsätzlich ungewöhnlichen Stärkegrad des erweiterten Vorsatzes der Absicht kommt, als Ausgleich zur weiten Vorverlagerung der Strafbarkeit, eine strafbarkeitseinschränkende Funktion zu. Anhaltspunkte für eine solche Intention des Täters können sich zu diesem frühen Zeitpunkt daraus ergeben, dass der Täter dem Kind pornographisches Material zeigt oder er sich mit ihm über intime Dinge, die nicht dem Alter der unmündigen Person entsprechen, unterhält.[2509] Es handelt sich bei § 208a Abs 1 um ein Absichtsdelikt ieS, wobei diese überschießende Innentendenz wohl auch als Korrektiv für die teils unbestimmt gefassten Tathandlungen fungiert.[2510]

2. § 208a Abs 1a

Erst jüngst wurde § 208a durch das Sexualstrafrechtsänderungsgesetz 2013[2511] bereits wieder modifiziert und in materiell-rechtlicher Umsetzung von Art 6 Abs 2 Richtlinie 2011/93/EU[2512] um einen neuen Tatbestand (Abs 1a) erweitert, welcher am 01.08.2013 in Kraft trat. Nach Art 6 Abs 2 Richtlinie 2011/93/EU haben die Mitgliedstaaten sicherzustellen, dass der Versuch eines Erwachsenen, mit Mitteln der IKT Straftaten gem Art 5 Abs 2 und 3 zu begehen (hierbei handelt es sich um die Konsumierungsverbote von Kinderpornographie betreffend den Erwerb, Besitz oder bewussten Zugriff)[2513], indem er Kontakt zu einer unmündigen Person aufnimmt, um kinderpornografische Darstellungen dieser Person zu erhalten, strafbar ist. Ein solcher Tatbestand war bislang in keiner internationalen oder unionsrechtlichen Vorgabe enthalten, weshalb insoweit ein Umsetzungsbedarf gegeben ist.

Der Gesetzgeber interpretiert die missverständliche Diktion »Versuch einer Straftat nach den Art. 5 Abs. 2 und 3« dahingehend, dass »diese Vorgabe mit Blick auf den Titel der Bestimmung ›Kontaktauf-

2509 Vgl ErlRV 1505 BlgNR XXIV. GP, 7.
2510 Siehe *Philipp* in WK² § 208a Rz 3.
2511 Sexualstrafrechtsänderungsgesetz 2013, BGBl I 116/2013.
2512 Richtlinie 2011/93/EU des Europäischen Parlaments und des Rates vom 13. Dezember 2011 zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie sowie zur Ersetzung des Rahmenbeschlusses 2004/68/JI des Rates, ABl L 2011/335, 1 idF L 2012/18.
2513 Vgl § 207a Abs 3 und 3a.

nahme zu Kindern für sexuelle Zwecke‹ nur so verstanden werden [kann], dass ein spezielles Vorbereitungsdelikt vorzusehen ist«[2514]. Dieses selbstständige Delikt soll jene Fälle des Grooming erfassen, in denen Täter versuchen, das Vertrauen von Kindern zu gewinnen, um von ihnen kinderpornografisches Material zu erhalten. Zum Teil geht es den Tätern nur darum, sich an den Bildern sexuell zu erregen oder zu befriedigen, zum Teil setzen die Täter übermittelte Bilder aber auch als Druckmittel zur Erzwingung weiterer (sexueller) Handlungen ein, indem sie bspw mit der Veröffentlichung des Materials drohen.[2515] Vor Einführung dieser Bestimmung gab es in diesem Bereich kein spezielles Vorbereitungsdelikt, weshalb gegen den Täter nur vorgegangen werden konnte, wenn dieser mit seiner Tat zumindest ins Versuchsstadium des § 207a StGB gelangt war.

a. IKT-gebundene Verhaltensweise

Wie auch § 208a Abs 1 ist § 208a Abs 1a ein verhaltensgebundenes Delikt, wobei Letzteres überhaupt nur mittels IKT verwirklicht werden kann. Eine konventionelle Kontaktaufnahme zu Unmündigen – wie sie in § 208a Abs 1 Z 2 berücksichtigt wurde (zB durch Ansprechen vor der Schule oder durch klassischen Briefverkehr) – ist für § 208 Abs 1a nicht vorgesehen. Daraus folgt, dass die persönliche Kontaktaufnahme außerhalb der IKT und das Überreden der unmündigen Person, pornographische Darstellungen von sich an den Täter – wenn auch mittels IKT – zu übersenden, nicht vom Tatbestand erfasst sind. In ErwG 19 RL 2011/93/EU führt der Richtliniengeber allerdings an, dass die Mitgliedstaaten die Bedeutung der Bekämpfung der Kontaktaufnahme zu einem Kind außerhalb der IKT anerkennen und somit den Mitgliedstaaten empfohlen werde, die Kontaktaufnahme zu einem Kind für ein Treffen mit dem Täter unter Strafe zu stellen. Unabhängig davon, welche rechtliche Lösung dazu gewählt werde, um eine »offline« begangene Kontaktaufnahme unter Strafe zu stellen, sollten die Mitgliedstaaten gewährleisten, dass sie die Täter solcher Straftaten in der einen oder anderen

2514 Siehe ErlRV 2319 BlgNR XXIV. GP, 17 f; in den GMat wird ausgeführt, dass durch diese Diktion auch der Eindruck hätte entstehen können, dass man im österreichischen Recht mit der Strafbarkeit des Versuchs gem §§ 15, 207a Abs 3 oder 3a dem Richtlinienziel bereits de lege lata Rechnung trägt.

2515 ErlRV 2319 BlgNR XXIV. GP, 18.

Weise verfolgen.[2516] Österreich ist einer solchen »offline«-Variante in Bezug auf § 208a Abs 1a – im Gegensatz zu Abs 1 – allerdings nicht gefolgt.

Die Tathandlung des § 208a Abs 1a besteht im Herstellen des Kontakts zu einer unmündigen Person (§ 74 Abs 1 Z 1) im Wege einer Telekommunikation oder »unter Verwendung eines Computersystems«[2517].

In Anbetracht des neu geschaffenen Delikts fällt erneut[2518] auf, dass der Gesetzgeber ein gesetzliches Tatbild normiert hat, dem eine sozial inadäquate Verhaltensweise fehlt. So handelt jeder, der mit Unmündigen über das Internet kommuniziert, bereits (objektiv) tatbestandsgemäß. Selbst wenn eine Kontaktaufnahme im Internet zu Unmündigen erfolgt, muss der Inhalt der Kommunikation nicht einmal etwas mit dem Inhalt der überschießenden Innentendenz (dh der Absicht eine strafbare Handlung nach § 207a Abs 3 oder 3a an diesem Unmündigen zu begehen) zu tun haben. Das Unrecht der Tat ergibt sich ausschließlich aus dieser überschießenden Innentendenz.[2519]

Tatobjekt kann – trotz des allgemeinen Verweises des Bezugsobjekts des erweiterten Vorsatzes auf § 207a Abs 3 und 3a – nur eine unmündige Person (§ 74 Abs 1 Z 1) sein. § 208a Abs 1a reicht daher nur soweit, als Unmündige vom Täter kontaktiert werden, nicht auch wenn dieser es auf pornographische Darstellungen einer zB 15-jährigen Person abgesehen hat und mit dieser dazu den Kontakt herstellt. Warum solche Vorbereitungshandlungen lediglich iZm Unmündigen und nicht auch mündigen Minderjährigen – wie es § 207a Abs 3 und 3a vorsehen – strafbar sein sollen, ergibt sich wohl in erster Line aus der Richtlinie 2011/93/EU selbst, wenn in Art 6 Abs 1 und 2 von Kindern gesprochen wird, die das Alter der sexuellen Mündigkeit noch nicht erreicht haben. Darunter versteht Art 2 lit b RL 2011/93/EU »das Alter, unterhalb dessen die Vornahme sexueller Handlungen mit einem Kind nach dem nationalen Recht verboten ist«. In Österreich wurde dieses Alter mit 14 Jahren festgesetzt, was sich aus den Bestimmungen des §§ 206 und 207 ergibt, wonach die Personen »unmündig« iSd § 74 Abs 1 Z 1 sein müssen.[2520]

2516 Vgl ErwG 19 RL 2011/93/EU.

2517 Zur missverständlichen Diktion »unter Verwendung eines Computersystems« sowie zu den IKT-Mittel im deliktspezifischen Zusammenhang siehe bereits oben das zu § 208a Abs 1 Z 1 zweiter Fall Gesagte.

2518 Wie zB auch schon § 208a Abs 1.

2519 Siehe dazu kritisch gleich im Anschluss zur subjektiven Tatseite.

2520 Vgl auch ErlStV 881 BlgNR XXIV. GP, 12.

b. Zur Strafbarkeitslücke bezüglich pornographischer Darbietungen

Streng der Richtlinienvorgabe entsprechend wurde § 208a Abs 1a nur als Vorbereitungsdelikt konzipiert, das im erweiterten Vorsatz lediglich auf die Absicht des Täters abstellt, eine strafbare Handlung bezüglich »pornographischer Darstellungen« iSd § 207a Abs 3 und 3a iVm § 207a Abs 4 hins der unmündigen Person zu begehen. Diese nicht gerade weitsichtige Umsetzung eröffnet im Bereich der »pornographischen Darbietungen« iSd § 215a Abs 2a eine Lücke. Demnach wird die IKT-Kontaktaufnahme zu einer unmündigen minderjährigen Person, zB um diese zu pornographischen Live-Darbietungen über eine Webcam zu bewegen, nicht schon im Vorfeldbereich erfasst. Daraus folgt, dass eine strafrechtliche Verfolgbarkeit in diesem Fall zumindest den Eintritt des Täters in das Versuchsstadium (= Vorliegen wenigstens einer ausführungsnahen Handlung iSd § 15 Abs 2) verlangt.

Der Gesetzgeber sollte diese Lücke durch Ausweitung des Bezugsobjekts der überschießenden Innentendenz in § 208a Abs 1a um die strafbare Handlung nach »§ 215a Abs 2a« erweitern, sodass diese lauten könnte:

»[…] in der Absicht, eine strafbare Handlung nach § 207a Abs. 3 oder 3a in Bezug auf eine pornographische Darstellung (§ 207a Abs. 4) oder nach § 215a Abs. 2a in Bezug auf eine pornographische Darbietung (§ 215a Abs. 3) dieser Person zu begehen […]«.

c. Kontaktherstellung zur unmündigen Person

Im deliktsspezifischen Kontext ist keine Kommunikation iS einer Unterhaltung erforderlich, vielmehr reicht diesfalls bereits die »Kontaktaufnahme« zu einer unmündigen Person über IKT aus. Ein Kontakt ist bspw dann hergestellt, wenn der Täter diese Person als Facebook-Freund hinzufügt oder ihr ein (nicht empfangsbedürftiges) E-Mail oder eine SMS zusendet. In ErwG 12 RL 2011/93/EU führt der Unionsgesetzgeber beispielhaft die Kontaktaufnahme zu Kindern über die Websites sozialer Netzwerke und Chatrooms an. Das Anschreiben der unmündigen Person via Chat-Forum, bei dem beide Kommunikatoren angemeldet sind, stellt somit ebenfalls den Kontakt her. Insgesamt kann mE gesagt werden, dass ein Kontakt immer dann hergestellt ist, wenn die Handlungen des Täters über die IKT in die Sphäre des Opfers reichen

und das Opfer mit der Kontaktaufnahme durch den Täter derart konfrontiert ist, dass dieses den Kontakt zum Täter erwidern könnte. Das Opfer muss mE dadurch in die Lage versetzt werden, in die Kommunikation mit dem Täter eintreten zu können. Entweder, weil dem Opfer diverse Kontaktmöglichkeiten vom Täter ausdrücklich mitgeteilt bzw durch das jeweilige IKT-Mittel faktisch schon technikbedingt bekannt wurden (zB Nickname, E-Mail-Adresse), oder – mangels Offenlegung von Kontaktdaten durch den Täter – weil das Opfer zB das Telefongespräch bei unterdrückter Rufnummer angenommen hat.

Daraus ergibt sich ein (Zwischen-)Erfolg für den Täter, der durch die erfolgte Kontaktaufnahme den Gefahrenbereich für eine Rechtsgutbeeinträchtigung bei der konkreten unmündigen Person eröffnet. Meines Erachtens muss das Opfer die Kontaktaufnahme des Täters jedenfalls wahrgenommen haben[2521], und es muss sich für dieses ein (potentieller) Kommunikationskanal zum Täter ergeben. Wie dieser Kommunikationskanal aussieht, ist nebensächlich. So könnte dies eine E-Mail-Adresse, eine Telefonnummer (für Anrufe oder SMS) oder ein gemeinsamer Chatroom sein, die dem Opfer den Zugang zur Kommunikation mit dem Täter ermöglichen. Der Kontakt ist aber auch hergestellt, wenn die unmündige Person die per IKT eingegangenen Nachrichten bzw Anrufe – bei prinzipieller Bekanntheit von Kontaktdaten des Täters – ignoriert oder einfach nur nicht darauf antwortet, »obwohl sie könnte«. Versucht der Täter bloß – entsprechender Vorsatz vorausgesetzt – mit unterdrückter Telefonnummer einen Kontakt zur unmündigen Person herzustellen, nimmt diese jedoch das Gespräch nicht an, wurde auch kein Kontakt hergestellt und § 208a Abs 1a nicht vollendet.[2522]

Identifiziert man – wie hier – § 208a Abs 1a (technisch gesehen) als Erfolgsdelikt, verhindert dies schließlich eine noch weitere (bzw zu weite) Vorverlagerung der Vollendungsstrafbarkeit.

Welche gedanklichen Inhalte der Täter mit der unmündigen Person tatsächlich kommuniziert, ist genauso unbeachtlich wie die Frage, ob die unmündige Person die wahre Identität des Täters oder lediglich dessen Nicknamen aus einem Chatroom kennt. Selbst eine ano-

2521 Wird ein kontakteinleitendes E-Mail direkt in den Spam-Ordner des E-Mail-Programms verschoben, auf den der Empfänger nicht zugreift, kann – mangels Kenntnis eines Kontaktversuches beim Empfänger – mE nicht von einer »Kontaktherstellung« gesprochen werden.

2522 Eine Versuchsstrafbarkeit gem §§ 15, 208a Abs 1a wäre in diesem Fall grundsätzlich denkbar.

nyme Kontaktaufnahme ist tatbildlich. Darüber hinaus spielt es keine Rolle, ob das Opfer bei der Kontaktaufnahme durch den Täter, dessen verwerfliche Intention vernimmt. Auch ist für eine Strafbarkeit nach § 208a Abs 1a nicht nur die »erstmalige« Kontaktaufnahme zum Opfer maßgeblich. Befindet sich der Täter bereits seit längerer Zeit im Kontakt mit einer unmündigen Person und bildet er zu diesem Zeitpunkt seinen »bösen Vorsatz« iSd subjektiven Tatseite des § 208a Abs 1a aus, wirkt die von dieser Innentendenz getragene nächstfolgende Kontaktherstellung mit der unmündigen Person für den Täter strafbarkeitsbegründet. Werden mehrere Nachrichten vom Täter an die unmündige Person gerichtet, um sein inkriminiertes Ziel zu erreichen, so liegt eine tatbestandliche Handlungseinheit bezüglich einer zusammenhängenden Abfolge tatbestandsmäßiger Handlungen (hier: mehrere Kontaktherstellungen mittels IKT) vor, die eine einzige Verletzung der Strafvorschrift – folglich »eine« Tat – darstellt.[2523]

Vom Wortlaut des § 208a Abs 1a ist auch die Kontaktherstellung über Dritte umfasst. Man denke an Mittelspersonen (»Kommunikationsvermittler«), die den Kontakt für den Täter herstellen. Man stelle sich vor, der Täter fordert (ggf ebenfalls unmündige) Geschwister der konkreten unmündigen Person auf, diese zu ermutigen, pornographische Abbildungen zu übermitteln.

Das Herstellen eines Kontakts verlangt ein aktives Tun des Täters, der sich um den Kontakt zu Unmündigen bemühen muss. Eine rein passive Haltung einer Person, dh wenn ein Unmündiger dieser Person – von dieser völlig unmotiviert (iSd »aufgedrängten Besitzes«) – pornographisches Bildmaterial von sich übermittelt, stellt kein Kontaktherstellen iSd § 208a Abs 1a dar. Der Empfänger dieser Bilder hat sich allerdings dieser kinderpornographischen Darstellungen umgehend zu entledigen.[2524]

Mit der Herstellung des Kontakts zu einer unmündigen Person ist das Zustandsdelikt des § 208a Abs 1a formell verwirklicht. Die einmalige Kontaktaufnahme für den inkriminierten Zweck genügt dazu bereits.

Die Gefährlichkeit dieser Tat liegt nicht überwiegend in der konkreten Handlung der Kontaktaufnahme, sondern in der Schaffung

2523 Vgl zur tatbestandlichen Handlungseinheit allgemein *Kienapfel/Höpfel/Kert,* AT[14], E 8 Rz 62.

2524 Siehe zum »aufgedrängten Besitz« auch bereits oben zu § 207a Abs 3 (S 497 ff).

einer gefährlichen Situation für das Opfer bezüglich pornographischer Darstellungen der unmündigen Person. § 208a Abs 1a ist daher ein Vorbereitungsdelikt, das diese Vorbereitungshandlung ausdrücklich unter Strafe stellt. Im Verhältnis zum Rechtsgut (hier: Schutz der Kinder vor sexuellem Missbrauch, sexueller Ausbeutung bzw Kinderpornographie) ist diese Bestimmung somit ein abstraktes Gefährdungsdelikt, da das Verhalten des Täters ohne Rücksicht auf eine tatsächlich eingetretene Rechtsgutgefährdung oder -verletzung für strafbar erklärt wird.[2525] Die Gefahr für das Rechtsgut ist dabei hoch, jene für ein konkretes Tatobjekt gering. Tatbestandlich betrachtet verlangt eine Kontaktherstellung aber eine von dieser in der Außenwelt zumindest gedanklich abtrennbare Wirkung. Die gefährliche Handlung führt über die Kontaktherstellung zu einem tatbestandlichen (Zwischen-)Erfolg, der allerdings noch keine konkrete Rechtsgutgefährdung bedeutet. Folglich ist § 208a Abs 1a gleichermaßen ein abstraktes Gefährdungsdelikt wie Erfolgsdelikt. Der von der Tathandlung abtrennbare (tatbestandliche) Erfolg liegt nun darin, dass das Opfer nach Kontaktherstellung durch den Täter jederzeit über die IKT mit diesem kommunizieren kann. Die Tathandlung der »Kontaktherstellung« ist vergleichbar mit der des »Zugänglichmachens«[2526]. Das Opfer kann nach der Kontaktaufnahme durch den Täter idR über eine bekanntgegebene E-Mail-Adresse, Telefonnummer oder einen Nicknamen eines Chat-Forums bzw durch die Annahme eines Telefonanrufs (auch bei unterdrückter Rufnummer) mit dem Täter in Kontakt treten. Es wurde ihm durch die Handlung des Täters ein informations- bzw kommunikationstechnischer »Zugang« zu diesem eröffnet.

d. Subjektive Tatseite

Der Unrechtsgehalt der Tat erschließt sich ausschließlich aus der inneren Einstellung des Täters, nämlich aus seinem Vorsatz. § 208a Abs 1a ist ein Absichtsdelikt ieS[2527], da es der Täter in seinem Vorhaben auf ein besonderes Endziel abgesehen haben muss, nämlich eine strafbare

2525 Siehe dazu generell *Fuchs,* AT I[8], Rz 10/43.
2526 Vgl etwa § 120 Abs 2a, § 126c Abs 1, § 207a Abs 1 Z 2, § 278f Abs 1 sowie § 51 DSG 2000.
2527 Da in diesem Zusammenhang auch tatsächlich »Absicht« iSd § 5 Abs 2 in Bezug auf den angestrebten Erfolg vorliegen muss.

Handlung nach § 207a Abs 3 oder 3a in Bezug auf eine pornographische Darstellung (§ 207a Abs 4) dieser Person zu begehen.

Aus der gänzlichen Verlagerung des spezifischen Unrechts in den subjektiven Tatbestand, liegt der Schluss nahe, dass die Sozialschädlichkeit des Täterverhaltens hauptsächlich an dessen innerer Einstellung ansetzt. Eine solche Subjektivierung des Unrechts ist jedenfalls verfassungsmäßig bedenklich, insb was die Bestimmtheit der konkret verpönten Tatbeschreibung anlangt.[2528] Es fragt sich, ob sich aus der Formulierung des Tatbestands überhaupt verpönte, dem Bestimmtheitsgebot hinreichend entsprechende Ausführungs- bzw ausführungsnahe Handlungen[2529] ableiten lassen.

§ 208a Abs 1a ist ein Delikt mit überschießender Innentendenz. Neben dem zumindest bedingten Tatbildvorsatz, der sich auf die Kontaktherstellung mit einer unmündigen Person im Wege der IKT beziehen muss, wird somit vom Täter im Handlungszeitpunkt ein erweiterter Vorsatz im Stärkegrad der Absicht (§ 5 Abs 2) verlangt, mit dieser unmündigen Person eine strafbare Handlung nach § 207a Abs 3 oder 3a bezüglich einer pornographischen Darstellung zu begehen. Dass diese strafbaren Handlungen bezüglich der pornographischen Darstellungen aber tatsächlich begangen werden, spielt für die formelle Deliktsvollendung keine Rolle. Vielmehr muss es dem Täter im Tatzeitpunkt der Kontaktherstellung nur darauf ankommen (iSd § 5 Abs 2), diesen Absichtsinhalt (später einmal) zu realisieren.

Der Täter muss eine pornographische Darstellung iSd § 207a Abs 4 jener Person anvisieren, zu der er den Kontakt hergestellt hat. Dadurch werden nach Meinung des Gesetzgebers jene Fälle ausgeschieden, »in denen sich ein Täter der Computerkenntnisse einer unmündigen Person bedienen will, weil er selbst mit der modernen Technik nicht so gut umgehen kann, und die Person daher anspricht, für ihn einschlägiges Material im Internet zu suchen«.[2530]

Beide Vorbereitungsdelikte des § 208a treten aufgrund materieller Subsidiarität zurück, sobald eine zumindest ausführungsnahe Hand-

---

2528 Siehe idS zu § 208a Abs 1 bereits *Mahler,* JSt, 2012, 22.

2529 Dies betrifft auch die Problematik einer Versuchsstrafbarkeit; siehe zur Diskussion eines Versuch bei Vorbereitungsdelikten allgemein *Kienapfel/Höpfel/Kert,* AT[14], Z 21 Rz 7; *Wieser,* Der Versuch beim Vorbereitungsdelikt (Teil I), JBl 1987, 497; weiters *Hager/Massauer* in WK[2] §§ 15, 16 Rz 12; aA *Fabrizy,* StGB[11] § 15 Rz 2; differenzierend *Fuchs,* AT I[8], Rz 28/31 f.

2530 ErlRV 2319 BlgNR XXIV. GP, 18.

lung zu §§ 201 bis 207a Abs 1 Z 1 (§ 208a Abs 1) bzw § 207a Abs 3 oder Abs 3a (§ 208a Abs 1a) gesetzt wurde und die jeweiligen Hauptdelikte somit ins strafbare Versuchsstadium vorgedrungen sind.[2531]

3. Tätige Reue

Der Systematik von Vorbereitungsdelikten entsprechend ermöglicht § 208a Abs 2 die strafbefreiende »Tätige Reue«. Nicht nach Abs 1 und Abs 1a zu bestrafen ist demnach, wer freiwillig und bevor die Behörde von seinem Verschulden erfahren hat, sein Vorhaben aufgibt und der Behörde sein Verschulden offenbart. Es handelt sich dabei um einen persönlichen Strafaufhebungsgrund. Unter einer Behörde iSd § 151 Abs 3 ist eine zur Strafverfolgung berufene Behörde in dieser ihrer Eigenschaft zu verstehen. Ihr stehen in dieser Eigenschaft zur Strafverfolgung berufene öffentliche Sicherheitsorgane gleich. Für den Gesetzgeber erscheint die Offenbarung des Verschuldens an die Behörde als nach außen tretende Reuehandlung vor allem deshalb sachgerecht, weil die Behörde den Täter auf Beratungsstellen aufmerksam machen könne, die sog »Täterarbeit« anbieten.[2532] Gleichwohl spiegelt dieses Offenbarungserfordernis der Tätigen Reue kein realistisches Szenario wider[2533] und wird in der Praxis wohl eher selten Anwendung finden.

4. Sonstiges

§ 208a ist insgesamt ein Offizialdelikt. § 208a Abs 1 fällt wegen seiner Freiheitsstrafdrohung mit »bis zu zwei Jahren« in die sachliche Zuständigkeit des Einzelrichters am Landesgericht (§ 31 Abs 4 Z 1 StPO). § 208a Abs 1a sieht dagegen als Sanktion der Verwirklichung des Tatbestandes eine Freiheitsstrafe »bis zu einem Jahr« oder eine Geldstrafe »bis zu 360 Tagessätzen« vor, weshalb gem § 30 Abs 1 StPO die sachliche Zuständigkeit des Bezirksgerichts gegeben ist.

2531 Vgl sinngemäß dazu die ErlRV 2319 BlgNR XXIV. GP, 18, wo allerdings fälschlicherweise von Abs 2 (anstatt von Abs 1a) gesprochen wird, wenn es heißt: »Die Strafbarkeit nach § 208a Abs. 2 StGB entfällt, wenn der Täter die beabsichtigte Tat nach § 207a StGB tatsächlich begangen oder zumindest versucht hat«.

2532 Siehe ErlRV 1505 BlgNR XXIV. GP, 7.

2533 Vgl auch krit *Mahler,* JSt 2012, 22; weiters *Messner,* JAP 2011/2012/12, 132; auch *Bertel/Schwaighofer,* BT II[11] § 208a Rz 5.

Wie auch schon zu § 215a Abs 2a erster Satz kritisch angemerkt, sollte mE auch § 208a Abs 1a – durch Ergänzung des § 30 Abs 1 Z 9 StPO – in Hinkunft gem § 31 Abs 4 Z 2 StPO iVm § 30 Abs 1 Z 9 StPO in die Sonderzuständigkeit des Einzelrichters am Landesgericht fallen.

VI. Sonstige Delikte mit IKT-Begehungsweisen

A. Anleitung zur Begehung einer terroristischen Straftat (§ 278f)

> § 278f (1) Wer ein Medienwerk, das nach seinem Inhalt dazu bestimmt ist, zur Begehung einer terroristischen Straftat (§ 278c Abs. 1 Z 1 bis 9 oder 10) mit den im § 278e genannten Mitteln anzuleiten, oder solche Informationen im Internet in einer Art anbietet oder einer anderen Person zugänglich macht, um zur Begehung einer terroristischen Straftat aufzureizen, ist mit Freiheitsstrafe bis zu zwei Jahren zu bestrafen.
>
> (2) Ebenso ist zu bestrafen, wer sich ein Medienwerk im Sinne des Abs. 1 oder solche Informationen aus dem Internet verschafft, um eine terroristische Straftat (§ 278c Abs. 1 Z 1 bis 9 oder 10) zu begehen.[2534]

§ 278f Abs 1 zielt auf Situationen der Zurverfügungstellung von Informationen als Anleitung zur Begehung terroristischer Straftaten mit den in § 278e angeführten Mitteln[2535] bzw das Selbststudium von Medienwerken oder von Informationen aus dem Internet ab.[2536] § 278f gehört zu den Friedensdelikten ieS[2537], die auf die Bewahrung des öffentlichen Friedens im Inland abzielen.

Die Strafnorm erfasst als technisches Vorbereitungsdelikt die Vorbereitungsphase zu einer terroristischen Straftat. Bezogen auf das Rechtsgut stellt § 278f Abs 1 ein abstraktes Gefährdungsdelikt dar,

2534 BGBl 60/1974 idF I 103/2011.

2535 Dabei handelt es sich um »Sprengstoff, Schuss- oder sonstigen Waffen oder schädlichen oder gefährlichen Stoffen oder in einer anderen ebenso schädlichen oder gefährlichen spezifisch zur Begehung einer terroristischen Straftat nach § 278c Abs. 1 Z 1 bis 9 oder 10 geeigneten Methode oder einem solchen Verfahren«.

2536 Siehe ErlRV 674 BlgNR XXIV. GP, 6.

2537 Vgl etwa *Plöchl* in WK² Vorbem §§ 274 Rz 1 ff (Stand Jänner 2014).

wobei die Tathandlung des Anbietens aus tatbestandlicher Sicht ein schlichtes Tätigkeitsdelikt beschreibt, die Handlung des Einer-anderen-Person-Zugänglichmachens allerdings ein Erfolgsdelikt.

1. Medienwerk

Der Begriff des Medienwerks entspricht dem Willen des Gesetzgebers nach jenem des § 1 Abs 1 Z 3 MedienG. Danach ist ein Medienwerk »ein zur Verbreitung an einen größeren Personenkreis bestimmter, in einem Massenherstellungsverfahren in Medienstücken vervielfältigter Träger von Mitteilungen oder Darbietungen mit gedanklichem Inhalt«. Es handelt sich dabei um einen Unterbegriff des »Mediums« (§ 1 Abs 1 Z 1 MedienG), wobei als wesentliches Merkmal ein körperlicher Träger für die publizistischen Inhalte dienen muss. Zu den Medienwerken zählen insb Druckwerke[2538] wie Bücher, Zeitschriften, Zeitungen, Rundschreiben, Postwurfsendungen usw, aber auch Bild- und Tonträger, zB mit Filmaufnahmen, Vorträgen oder Musik.[2539] Zu den Medienwerken gehören gem § 1 Abs 2 MedienG auch die in Medienstücken vervielfältigten Mitteilungen der Mediendienste. Unkörperliche Medien – wie Rundfunksendungen oder Websites – sind keine Medienwerke.[2540] Die vervielfältigten einzelnen Exemplare eines Medienwerks werden »Medienstücke« genannt.[2541]

2. Tatbestandsmerkmal »Internet«

Was der Gesetzgeber unter dem Tatbestandsmerkmal »Internet« versteht, ist auch in dieser Strafbestimmung unklar.[2542] Zu § 207a Abs 3a hat der JA lapidar angemerkt, dass »sämtliche Internetdienste« gemeint seien.[2543] Stellt jedoch der Gesetzgeber gerade den Bezug des Tatbestands auf das »Internet« deshalb her, um »virtuelle Trainings-

2538 Ein Druckwerk (§ 1 Abs 1 Z 4 MedienG) ist wiederum ein Unterfall des Medienwerks.

2539 Siehe dazu *Wittmann/Zöchbauer* in Röggla/Wittmann/Zöchbauer, MedienG § 1 Rz 14.

2540 Siehe ErlRV 784 BlgNR XXII. GP, 4; weiters; vgl auch *Rami* in WK² MedienG § 1 Rz 18 (Stand Juli 2011).

2541 Vgl etwa JAB 743 BlgNR XV. GP, 3; siehe auch *Wittmann/Zöchbauer* in Röggla/Wittmann/Zöchbauer, MedienG § 1 Rz 14.

2542 Siehe dazu bereits oben zu § 207a Abs 3a.

2543 JAB 106 BlgNR XXIV. GP, 35.

camps« für Terroristen in dieser Umgebung dadurch zu erfassen[2544], sollte mE der Begriff des Internet – analog meiner Empfehlung zu § 207a Abs 3a – entweder durch eine Legaldefinition hinreichend determiniert oder einfach durch Informations- und Kommunikationstechnologie ersetzt werden.

Dies wird wohl auch über die Erl zum »Übereinkommen des Europarates zur Verhütung des Terrorismus«[2545] indiziert, da in Pkt 104 von »mass media or electronic facilities, in particular the Internet« gesprochen wird.[2546] Das Internet wird dort nur bspw angeführt, genauso wie in ER (ETS 196) Pkt 172, wo ausdrücklich auf die CCC Bezug genommen wird und von der »Begehung durch Computersysteme oder über das Internet« gesprochen wird.[2547] So wird das wohl auch in ErwG 3 EU-RB 2008/919/JI[2548] gesehen, wo von Terrorzellen gesprochen wird, die Verbindungen zwischen internationalen Netzen herstellen und zunehmend von neuen Technologien, »insbesondere dem Internet«, Gebrauch brauchen.[2549]

Diese über informationstechnische Systeme realisierbaren Begehungsweisen bilden im Übrigen auch die Grundlage der Aufnahme dieser Strafbestimmung in den § 64 Abs 1 Z 9[2550], da die Ausbildung in »Terrorcamps« in der Regel nicht in Österreich und die Einspeisung von Informationen zur Anleitung zur Begehung von terroristischen Straftaten in das Internet auch im Ausland erfolgen werden.[2551]

Andererseits verweist der Gesetzgeber in diesem Tatbestand nicht generell auf Medien iSd § 1 Abs 1 Z 1 MedienG – wovon auch Websites

2544 Vgl ErlRV 674 BlgNR XXIV. GP, 2; vgl auch ErwG 4 des Rahmenbeschlusses 2008/919/JI des Rates vom 28. November 2008 zur Änderung des Rahmenbeschlusses 2002/475/JI zur Terrorismusbekämpfung, ABl L 2008/330, 21.

2545 Convention on the Prevention of Terrorism (ETS 196), <conventions.coe.int/Treaty/en/Treaties/Html/196.htm> (01.04.2014); BGBl III 34/2010.

2546 Vgl ER (ETS 196) Pkt 104.

2547 Siehe ER (ETS 196) Pkt 172: »[…] In the case of crimes committed by use of computer systems or through the Internet, for instance public provocation to commit a terrorist offence, there will be occasions in which more than one Party has jurisdiction over some or all of the participants in the crime. […]«.

2548 Rahmenbeschluss 2008/919/JI des Rates vom 28. November 2008 zur Änderung des Rahmenbeschlusses 2002/475/JI zur Terrorismusbekämpfung, ABl L 2008/330, 21.

2549 Hervorhebung nicht im Original.

2550 Eingeführt mit BGBl I 103/2011.

2551 Vgl ErlRV 674 BlgNR XXIV. GP, 4.

im Internet, Massen-E-Mails[2552] usw erfasst werden –, was eigentlich schon deshalb naheliegen würde[2553], da in Anbetracht körperlicher Publikationen (Medienwerke) sehr wohl in den Erl der Bezug zur Terminologie des MedienG hergestellt wird. Der Begriff des Mediums nach § 1 Abs 1 Z 1 MedienG verlangt aber ua, dass Mitteilungen oder Darbietungen zur Verbreitung für einen »größeren Personenkreis« bestimmt sein müssen. Ein individuelles E-Mail an einen einzigen Empfänger, wäre daher kein solches Medium und vom Tatbestand nicht erfasst. Dasselbe würde im Übrigen auch für Webinhalte gelten, die nur einem begrenzten Teilnehmerkreis zugänglich sind (Intranet).[2554] Aus diesem Grund kann davon ausgegangen werden, dass der Gesetzgeber mit der Formulierung »Informationen im Internet« die Strafbarkeit gerade nicht – wie es bei § 282a[2555] der Fall ist – auf eine Verbreitung für einen größeren Personenkreis einschränken will. Vielmehr noch bringt die Tathandlung »einer anderen Person zugänglich machen« zum Ausdruck, dass der Gesetzgeber bewusst (auch) die Individualkommunikation über Dienste (zB E-Mail) des Internet für einen inkriminierten Informationsaustausch erfassen will. Und dennoch verhindert mE die Verwendung des Begriffs »Internet« eine vollständige Erfassung solcher Individualkommunikationen; dies bspw dann, wenn Informationen über ein privates Firmennetzwerk oder auch über andere Kommunikationsformen außerhalb des Internet (wie zB SMS, MMS, FAX) angeboten oder zugänglich gemacht werden. Geht man allerdings davon aus, dass der Gesetzgeber lediglich von einem umgangssprachlichen Begriffsverständnis ausgegangen ist, so könnte man auch ein Intranet oder ein Netzwerk mit anderen Protokollgrundlagen als TCP/IP vom Wortlaut dieses Tatbestandsmerkmals erfasst sehen.[2556]

2552 Siehe etwa *Rami* in WK² MedienG § 1 Rz 13 mit vielen Beispielen und Nachweisen; auch *Wittmann/Zöchbauer* in Röggla/Wittmann/Zöchbauer, MedienG § 1 Rz 10 und 17.

2553 Vgl auch § 282a; eingeführt mit BGBl I 103/2011.

2554 Siehe dazu auch *Wittmann/Zöchbauer* in Röggla/Wittmann/Zöchbauer, MedienG § 1 Rz 10 und 17.

2555 Wobei auch hier keine breite Öffentlichkeit (ab ca 150 Personen) wie in § 282 gefordert ist, sondern etwa 30 Personen genügen sollen (vgl ErlRV 674 BlgNR XXIV. GP, 6).

2556 Siehe dazu bereits die Ausführungen zu § 207a Abs 3a.

3. Tatbestandsmerkmal »Information«

Zum Begriff der »Informationen« ist erneut[2557] anzumerken, dass dieser wohl im hier interessierenden Verständnis der Sache nach den für den Menschen relevanten Bedeutungsinhalt von Daten (hier: Daten im weiten Sinn) betrifft. Sie fallen daher in das »semantisch/pragmatische« Verständnis von Daten[2558]. Die »Information« ist ein weitläufig verwendeter und nur schwer abzugrenzender Begriff, der auch in unterschiedlichen Wissenschaftsdisziplinen keine identischen Bedeutungen hat. Es erscheint mE daher nicht gerechtfertigt, den Begriff der »Information« als Legalterminus ohne explizite Definition für das Strafrecht einfach zu übernehmen.

Auf die »Verarbeitungsform der Informationen« (hier: Daten im engen Sinn) kommt es aber bei § 278 – im Gegensatz zu § 278f Abs 1 und 2[2559] – nicht an. Gerade deshalb, weil innerhalb von systematisch ähnlich gelagerten Delikten auf unterschiedliche (technische) Darstellungsformen abgestellt wird, der Relevanzzusammenhang des Bedeutungsgehalts der Daten aber vergleichbar ist, erscheint es unverständlich, weshalb nicht auch in diesen Bestimmungen auf den (inhaltlich abgegrenzten) Datenbegriff des § 74 Abs 2 zurückgegriffen wurde. Vielmehr noch wird durch die zusätzliche – dem StGB ohnehin neue – Begrifflichkeit der »Information« der Eindruck verstärkt, als handle es sich dabei im Hinblick auf »Daten« auf der einen und »Informationen« auf der anderen Seite um Verschiedenes. Wie jedoch mehrfach bereits betont, ist in beiden Fällen der Informationsgehalt angesprochen und nicht (ausdrücklich, aber ggf mittelbar) die (technische) Verarbeitungsform.

An dieser Strafbestimmung ist bemerkenswert, dass der Gesetzgeber in den einzelnen Wendungen »Informationen im Internet« (Abs 1) bzw »Informationen aus dem Internet« (Abs 2) jeweils zwei weitverbreitete, polysemische Begriffe als Legaltermini miteinander in einem Unrechtstatbestand kombiniert, ohne sie für das strafrechtliche Verständnis zu definieren.

2557 Vgl bereits oben S 60 ff.

2558 Dh »Daten im weiten Sinn« bzw »Information«.

2559 Durch den tatbestandlichen Hinweis, dass es sich um Information im (Abs 1) bzw aus (Abs 2) dem Internet handeln muss, wird die Verarbeitungsform dieser »Informationen« auf informationstechnische Darstellungen (Computerdaten) eingeschränkt.

Das Medienwerk und die Informationen (arg »solche«) müssen nach ihren Inhalten objektiv geeignet sein, als Anleitung zu einer terroristischen Straftat iSd § 278c Abs 1 Z 1 bis 9 oder 10 zu dienen.

Die Tathandlungen umfassen das »Anbieten« und das »Einer-anderen-Person-Zugänglichmachen« des Medienwerks oder der Informationen im Internet.

Es ist aber nicht erforderlich, dass der Täter nach Abs 1 die Informationen selbst zB ins Internet gestellt hat.

4. Anbieten

Beim Anbieten handelt es sich noch nicht um eine Weitergabe-Handlung, sondern um eine der tatsächlichen Weitergabe des Medienstücks oder der einschlägigen Information vorgelagerte Tätigkeit (iSd Anbahnung einer Weitergabe).[2560] Es ist eine einseitige, nicht empfangsbedürftige Erklärung, die inkriminierten Informationen zugänglich machen zu können. Dadurch wird aber noch nicht der sofortige Zugang zu den Inhalten ermöglicht, sondern handelt es sich zeitlich betrachtet erst um das Angebot, in einem weiteren Schritt den Zugang (ggf erst gegen Erbringung einer Gegenleistung) zu gewähren.[2561] Nach diesem Verständnis wäre etwa das Versenden eines Hyperlinks via E-Mail, der lediglich auf eine Webseite mit den entsprechenden aufreizenden Informationen referenziert, ohne diese selbst zu beinhalten, bereits als ein Anbieten iSd § 278f Abs 1 Fall 1 zu verstehen (denn der Täter weist dabei auf die von ihm beschaffbare Information hin). Die Informationen hat der Empfänger dabei aber (noch) nicht erhalten. Die bloße Stellung des Angebots reicht bereits aus, um diese Begehungsweise zu erfüllen. Auf die Annahme des Angebots durch den Empfänger des E-Mails (zB per tatsächlichem Aufruf der verlinkten Seite) kommt es – anders als bei § 278f Abs 2 – hier nicht mehr an. Auch könnte man an ein Inserat im Internet denken, das an einen unbestimmten Adressatenkreis gerichtet ist und bei Interesse in weiterer Folge zur Zugänglichkeit der entsprechenden Informationen führen könnte. Würde der Täter die Informationen unmittelbar als Inhalt des E-Mails dem Empfänger übermitteln, so wäre § 278f Abs 1 Fall 2 hergestellt, da die Informationen einer anderen Per-

2560 Vgl *Bergauer,* jusIT 2008/82, 175; weiters *Schmölzer* in Bergauer/Staudegger, Recht und IT, 1 (24).

2561 Siehe dazu bereits oben zum Anbieten iSd § 207a Abs 1 (insb S 477).

son zugänglich gemacht wurden. Das Anbieten stellt im Gegensatz zur zweiten Handlungsalternative (einer anderen Person Zugänglichmachen) aufgrund seines einseitigen, nicht empfangsbedürftigen Charakters eine schlichte Tätigkeit dar (schlichtes Tätigkeitsdelikt).

5. »Einer-anderen-Person-Zugänglichmachen«

Die besondere Formulierung des Tatbestands was Weitergabehandlungen zB im Internet anlangt, ist untypisch, gerade weil die für das Internet grundsätzlich zutreffendste Handlung des »Veröffentlichens« nicht gesondert genannt wird. Es wird daher in diesem Delikt nicht – wie in anderen Bestimmungen[2562] – zwischen einem Zugänglichmachen für einen bestimmten Empfänger und dem Zugänglichmachen für einen unbestimmten Empfängerkreis unterschieden. Das Publizieren von Informationen auf einer einschränkungslos erreichbaren Internetseite ist aber auch kein Anbieten (mehr), sondern bereits ein Zugänglichmachen für einen unbestimmten Adressatenkreis bzw ein Veröffentlichen.

Da der sprachliche Ausdruck »einem« nicht als Zahlwort, sondern als ein unbestimmter Artikel zu verstehen sein wird, ist wohl davon auszugehen, dass im deliktsspezifischen Kontext nicht nur das Zugänglichmachen für eine »konkrete« Person als Empfänger (iS einer Individualkommunikation) strafbar ist, sondern auch das Zugänglichmachen an unbestimmte Empfänger wie es bei vergleichbaren Tatbestandsdefinitionen iZm Übermittlungshandlungen über die IKT bereits üblich ist.[2563] In Zusammenhang mit ähnlichen Formulierungen für Weitergabehandlungen hat *Salimi* zu § 51 DSG 2000 kommentiert, dass die Übermittlung an einen unbestimmten Adressatenkreis von der Tathandlung des »Einem-anderen-Zugänglichmachen« ausgenommen ist, da in einem solchen Fall ein Veröffentlichen vorliege.[2564]

Der konventionelle Sprachgebrauch die Tatbestandsformulierung betreffend erfasst aber offensichtlich nicht nur das Zugänglichmachen für *eine* andere Person, sondern auch das Zugänglichmachen für *mehrere* (andere) – wenn auch unbestimmte – Personen (Veröffentlichen).

2562 Vgl etwa § 118a Abs 1, § 119a Abs 1, § 120 Abs 2, § 120 Abs 2a bzw § 51 DSG 2000.

2563 Siehe zB § 118a Abs 1, § 119a Abs 1 bzw § 120 Abs 2, § 120 Abs 2a, sprechen – verkürzt dargestellt – vom »Einem-anderen-Zugänglichmachen« bzw »Einem-Dritten-Zugänglichmachen«, wohingegen etwa § 126c Abs 1 und § 207a Abs 1 Z 2 ein »Sonst-Zugänglichmachen« vorsehen.

2564 Vgl *Salimi* in WK² DSG § 51 Rz 51.

Obwohl im deliktsspezifischen Zusammenhang der Wortlaut und auch teleologische Erwägungen dazu führen, dass auch das Veröffentlichen an einen unbestimmten Empfängerkreis[2565] von § 278f Abs 1 erfasst ist, sollte der Tatbestand in Anbetracht einer sprachlichen Vereinheitlichung von auf vergleichbare Verhaltensweisen bezogenen Formulierungen um die Tathandlung des »Veröffentlichens« ergänzt werden.[2566] Eine auf singulärer Ebene vorgenommene deliktsspezifische Auslegung der Tathandlung, die allerdings von der Begriffsverwendung in anderen vergleichbaren Tathandlungen abweicht, kann auf diese anderen Delikte ausstrahlen und daher unerwünschte Ergebnisse liefern.

Das Unrecht der Tat sollte sich daher bezüglich der inkriminierten Informationen auf das »Anbieten, Einer-anderen-Person-Zugänglichmachen und Veröffentlichen« erstrecken.

Jedenfalls sind – nach der hier vertretenen Auffassung – das »Anbieten« und das tatsächliche »Zugänglichmachen«, keine gleichwertigen Tathandlungen, weder bezüglich ihres sozialen Sinngehalts, noch was die Intensität der Rechtsgutbeeinträchtigung anlangt. Es handelt sich somit in § 278f Abs 1 um jeweils selbstständige Delikte, die ein kumulatives Mischdelikt indizieren. Das Anbieten stellt eine Vorbereitungshandlung zum anschließenden Zugänglichmachen dar, weshalb es auch bei Vorliegen eines tatsächlichen Zugänglichmachens zurücktritt (materielle Subsidiarität). Aus Sicht der Begehungsweise des Einer-anderen-Person-Zugänglichmachens ist § 278f Abs 1 ein Erfolgsdelikt.[2567]

6. Die Datenbeschädigung als terroristische Straftat

§ 278c Abs 1 Z 6 Fall 2 erfasst als terroristische Straftat – neben der schweren Sachbeschädigung (§ 126) – die »Datenbeschädigung (§ 126a)«, sofern dadurch eine Gefahr für das Leben eines anderen oder für fremdes Eigentum in großem Ausmaß entstehen kann. Darüber hinaus muss die Tat die Eignung und Zielsetzung einer terroristischen Straftat auf-

2565 Denkbar wäre allerdings auch eine »Veröffentlichung« der Informationen in einem privaten Netzwerk für einen bestimmten Empfängerkreis, zu dem mehr als 10 (iSd § 69) bestimmbare Personen Zugang haben (zB Firmen-Intranet).

2566 Siehe zur Auseinandersetzung mit den angesprochenen Tathandlungen bereits mehrfach oben.

2567 Siehe zu den diversen ähnlich formulierten Tathandlungen bezüglich des Zugänglichmachens oben.

weisen, weshalb sie geeignet sein muss, eine schwere oder längere Zeit anhaltende Störung des öffentlichen Lebens oder eine schwere Schädigung des Wirtschaftslebens herbeizuführen.

Auf der subjektiven Seite wird neben dem Tatbildvorsatz auch ein erweiterter (überschießender) Vorsatz verlangt, die Bevölkerung auf schwerwiegende Weise einzuschüchtern, öffentliche Stellen oder eine internationale Organisation zu einer Handlung, Duldung oder Unterlassung zu nötigen oder die politischen, verfassungsrechtlichen, wirtschaftlichen und sozialen Grundstrukturen eines Staates oder einer internationalen Organisation ernsthaft zu erschüttern oder zu zerstören. Für diesen Fall wird gem § 278c Abs 2 das Höchstmaß der Strafdrohung des § 126a um die Hälfte hinaufgesetzt.

Die Eignung eines Computerwurms[2568] zur Begehung einer Gemeingefährdung (§ 176) oder einer Datenbeschädigung als terroristische Straftat wurde bereits an anderer Stelle untersucht und grundsätzlich bejaht.[2569] Dass durch Computerwürmer eine Gefährdung für Leib oder Leben mittelbar realisiert werden kann, hat auch ein deutsches Gericht im Fall des »Sasser-Wurms« bestätigt. Der Angeklagte habe nämlich durch die Verbreitung seines Internetwurms Notrufanlagen und ähnliche Einrichtungen vorübergehend funktionsunfähig gemacht und dadurch eine Gefahr für Leib und Leben anderer herbeigeführt.[2570]

Das Ausmaß der Schäden, die durch Computerwürmer zu erwarten sind, ist beträchtlich. Der »Loveletter«-Wurm richtete im Jahr 2000 einen auf 10 Milliarden Euro geschätzten Schaden an[2571], und auch im Fall »Sasser-Wurm« hat die ermittelnde Staatsanwaltschaft einen Schaden iHv € 130.000,– festgestellt, wobei davon ausgegangen werden kann, dass der Schaden weltweit mehr als eine Million Euro betragen hat.[2572]

Im Zusammenhang mit § 278c Abs 1 Z 6 und der Datenbeschädigung nach § 126a fällt auf, dass der Gesetzgeber alternativ neben

---

2568 Freilich wäre auch an »logische Bomben« oder »DDoS-Angriffe« zu denken.

2569 Siehe *Bergauer,* jusIT 2008/2, 2.

2570 Pressemitteilung des Landgerichts Verden, Urteil im Sasser-Prozess, <www.landgericht-verden.niedersachsen.de/portal/live.php?navigation_id=13888&article_id=58136&_psmand=57> (01.04.2014).

2571 *Reischl,* Gefährliche Netze (2001) 32.

2572 *Heise online,* Entwickler des Wurms Sasser steht vor Gericht, <www.heise.de/newsticker/meldung/61392> (01.04.2014).

der Gefahr für Leib und Leben auch auf die Gefahr für »fremdes Eigentum in großem Ausmaß« abstellt. Er räumt dadurch indirekt ein, dass es durch eine »Datenbeschädigung« möglich sein muss, Eigentum (im strafrechtlichen Sinn) zu gefährden bzw zu verletzen. Bislang ist jedoch unbestritten, dass die Datenbeschädigung nach § 126a ein Delikt darstellt, welches als Rechtsgut zumindest[2573] das »Vermögen« schützt. Prüft man nunmehr das Tatbestandsmerkmal »Eigentum«, so muss man sich erst die Frage stellen, von welchem Eigentumsbegriff das Strafrecht ausgeht. In der Lehre wird jedenfalls weitgehend die Auffassung vertreten, dass sich der strafrechtliche Eigentumsbegriff grundsätzlich an dem des Zivilrechts (Eigentum im engeren Sinn) orientiere.[2574] Expressis verbis ist in der Definition des Tatbestandes der vorsätzlichen Gemeingefährdung von »Eigentum« die Rede, was indiziert, dass das bloße Vermögen (zivilrechtliches Eigentum im weiteren Sinn[2575]) nicht von diesem Delikt erfasst ist. Daraus folgt, dass es sich bei der Gemeingefährdung lediglich um die Gefährdung körperlicher Gegenstände handeln kann.[2576]

Daher ist es für eine solche Datenbeschädigung notwendig, dass die als Tatmittel eingesetzte Malware überhaupt in der Lage ist, »Hardware« zu beschädigen. Man denke zB an Würmer, die Überlastungsroutinen für Festplatten-Schreib-/Leseköpfe als Payload mitführen, wodurch idR ein »Headcrash« verursacht werden kann.[2577] Die explosionsartige, unkontrollierbare Ausbreitung eines noch unbekannten Computerwurms und die damit verbundene konkrete Gefährdung unzähliger Festplatten der mit dem Internet verbundenen Computersysteme können durchaus eine Gefährdung von Eigentum in großem Ausmaß darstellen. Die »konkrete« Gefährdung ist dabei jeweils im

---

2573 Neben dem »Interesse am Fortbestand und der Verfügbarkeit« von Daten (siehe dazu oben zu § 126a).

2574 Vgl etwa *Seiler* in SbgK § 125 Rz 5; ebenso *Bertel* in WK² § 125 Rz 3.

2575 Siehe etwa *Holzner* in Kletečka/Schauer (Hrsg), ABGB-ON § 353 Rz 1 (Stand September 2014); *Eccer* in KBB³ § 354 Rz 1 (Stand Juli 2010); *Klicka* in Schwimann/Kodek (Hrsg), ABGB Praxiskommentar⁴ § 354 Rz 1 (Stand Mai 2012); ebenso *Spielbüchler* in Rummel (Hrsg), ABGB I³ § 354 Rz 1 (Stand Jänner 2000); aA *Staudegger,* Zur Qualifikation von Verträgen, die der Überlassung von Computersoftware dienen, JBl 1998, 604; *Staudegger,* Das Computerprogramm als Rechtsobjekt – zugleich ein Beitrag zum Sachbegriff im Informationszeitalter (Habilitationsschrift 2009) 530 f.

2576 Vgl etwa den Hinweis auf §§ 125, 126 in *Bertel/Schwaighofer,* BT II¹¹ § 177 Rz 3.

2577 Vgl *Bergauer,* jusIT 2008/2, 2.

Einzelfall zu prüfen und hängt stark vom Infektionsmechanismus und Payload des Computerwurms ab.

Wichtig für den Anwendungsbereich von § 126a ist jedoch die Angriffsadressierung auf Computerdaten[2578], denn würde der Täter ausschließlich Hardware schädigen wollen, wäre ohnehin die Sachbeschädigung heranzuziehen. Ist ein Schadprogramm lediglich in der Lage, unkörperliche Software zu löschen bzw zu gefährden, kann auch das »Eigentum« nicht gefährdet werden. Im Zivilrecht geht die hL[2579] davon aus, dass die sachenrechtlichen Bestimmungen des ABGB grundsätzlich nur auf körperliche Sachen abzielen, weshalb durch die Unkörperlichkeit und Ubiquität von Software kein Eigentum (ieS) daran begründet werden kann. Auch das Auslegungsprinzip der Einheit der Rechtssprache stärkt diese Betrachtung, da im Allgemeinen davon auszugehen ist, dass in der Rechtssprache geprägte Begriffe eine konstante Bedeutung haben. Die Zivilrechtsakzessorietät des strafrechtlichen Eigentumsbegriffs iVm dem Analogieverbot verhindern de lege lata, dass die Gefährdung von Software durch einen Computerwurm, auch wenn der wirtschaftliche Wert von Software idR über dem der Hardware steht, eine Gefährdung von »Eigentum in großem Ausmaß« darstellen kann.[2580]

Als Vorgabe der Bestimmung des § 278c diente der EU-RB 2002/475/JI zur Terrorbekämpfung[2581], in dem idZ von »Zerstörungen an Privateigentum« gesprochen wird, die »zu erheblichen wirtschaftlichen Verlusten führen können«. Darin lässt sich mE jedoch eine Vermischung der Begrifflichkeiten »Eigentum« (»Privateigentum«) und »Vermögen« (»wirtschaftliche Verluste«) erblicken. Zudem zählt § 278a Z 1[2582] strafbare Handlungen auf, die eine »kriminelle Organisation« näher beschreiben. Demnach ist eine kriminelle Zielsetzung der Organisation ua die Bedrohung von »Vermögen«, nicht aber »Eigentum«. Aus den GMat[2583] lässt sich diesbezüglich kein Anhaltspunkt gewinnen, warum in § 278a das »Vermögen« und in der detaillierten taxativen Aufzählung

2578 Siehe oben zu § 126a (S 250 ff).
2579 Vgl *Holzner* in Kletečka/Schauer, ABGB-ON § 353 Rz 1; *Eccer* in KBB[3] § 354 Rz 1; *Klicka* in Schwimann/Kodek, ABGB Praxiskommentar[4] § 354 Rz 1; ebenso *Spielbüchler* in Rummel, ABGB I[3] § 354 Rz 1; aA *Staudegger,* JBl 1998, 604; *Staudegger,* Computerprogramm, 530 f.
2580 Siehe dazu auch *Bergauer,* jusIT 2008/2, 2.
2581 Rahmenbeschluss 2002/475/JI des Rates vom 13. Juni 2002 zur Terrorismusbekämpfung, ABl L 2002/164, 4.
2582 Der die Gründung bzw Beteiligung an einer kriminellen Organisation pönalisiert.
2583 Vgl ErlRV 1166 BlgNR XXI.GP, 37.

der terroristischen Straftaten in § 278c Abs 1 Z 6 die Gefährdung fremden »Eigentums« genannt ist.

Man könnte daher entweder auf ein Redaktionsversehen schließen oder an die unbedachte Übernahme der gegenständlichen Wortfolge aus den Formulierungen der bestehenden Gemeingefährdungsdelikte (iSd §§ 169 ff) denken. Sollte nämlich tatsächlich nur eine Datenbeschädigung iSd § 126a gemeint sein, die durch die Manipulation von Daten zusätzlich auch körperliche Gegenstände (Hardware) »gefährdet«, an denen (zivilrechtlich) Eigentum bestehen kann, wäre freilich die Nennung der Datenbeschädigung in § 278c Abs 1 Z 6 überflüssig, weil – wie bereits angemerkt – die (schwere) Sachbeschädigung an körperlichen Sachen ohnedies von § 126 erfasst wäre. Der Gesetzgeber ist daher insoweit gefordert, die angesprochenen Unstimmigkeiten zu beseitigen und eine Vermengung der herkömmlichen strafrechtlichen Verwendung der Begriffe »Eigentum« und »Vermögen« tunlichst zu vermeiden.[2584] Umso unverständlicher ist es mE, dass etwa § 126b, der auf die Störung der Funktionsfähigkeit eines Computersystems abstellt, nicht in den Katalog der terroristischen Straftaten aufgenommen wurde. Der JA begründet dies kurzerhand damit, dass er sich nicht vorstellen könne, dass »ein (nur) diesem Tatbestand zu subsumierender Sachverhalt (dh eine Störung der Funktionsfähigkeit eines Computersystems insbesondere ohne Sachbeschädigungs-, Datenbeschädigungs- oder Gemeingefährdungsvorsatz) zugleich den Charakter einer terroristischen Straftat aufweist«.[2585]

Ergänzend ist zu § 278c Abs 1 Z 6 anzumerken, dass die Formulierung unpräzise ist, da die schwere Sachbeschädigung (§ 126) und Datenbeschädigung (§ 126a) genannt sind. Man könnte daher einerseits darauf schließen, dass für eine terroristische Straftat nach Z 6 nur eine Sachbeschädigung in qualifizierter Form iSd § 126 in Frage kommt, wohingegen bereits eine »einfache« Datenbeschädigung nach § 126a ausreicht, da sich der Klammerverweis nach der Datenbeschädigung nur auf »§ 126a« bezieht und nicht ausschließlich auf die Qualifikationsfälle des Abs 2 Fall 1 und 2. Andererseits könnte man den Wortlaut dahingehend verstehen, dass sich das Attribut »schwere« vor dem Wort »Sachbeschädigung« durch das anschließend verwendete Bindewort »und« auch auf das Wort »Datenbeschädigung« bezieht. In den GMat

2584 Siehe dazu bereits *Bergauer,* jusIT 2008/2, 2.
2585 Vgl JAB 1213 BlgNR XXI. GP, 1.

wird allerdings darauf hingewiesen, dass man in diesem deliktsspezifischen Verständnis eine »schwere Sachbeschädigung oder Datenbeschädigung, dh eine solche Beschädigung mit einem Schaden von mehr als Euro 2.000,–, wobei darüber hinaus durch diese Beschädigung eine Gefahr für das Leben eines anderen oder für fremdes Eigentum in großem Ausmaß entstehen können muss«, vor Augen hatte.[2586] Damit ist klargestellt, dass iZm der Datenbeschädigung aber nur § 126a Abs 2 (genauer erster und zweiter Fall) gemeint sein kann, was auch durch Ergänzung des Klammerausdrucks zum Ausdruck gebracht werden sollte.

7. Zur Begehung einer terroristischen Straftat »aufreizen«

Interessanterweise erklären die GMat iZm dem »Aufreizen« – das nunmehr im Vergleich zu ähnlich formulierten Delikten (§§ 282 f) erstmals nicht in der Definition des objektiven, sondern in der des subjektiven Tatbestands verlangt wird –, dass die Strafbarkeit nach Abs 1 zusätzlich voraussetze, »dass die Umstände der Verbreitung, also des Anbietens oder des Zugänglichmachens dazu geeignet sein müssen, den Entschluss zur Verübung einer terroristischen Straftat emotionell besonders nahe zu legen.«[2587] Es fragt sich allerdings, warum dafür auf die Art der Verbreitung und nicht auf die konkreten Informationen abgestellt wird. Mit anderen Worten, die Veröffentlichung solcher Informationen im Internet selbst muss in einer solchen Weise geschehen, dass die Bereitschaft zur Begehung von terroristischen Straftaten erhöht wird. Es geht daher nicht um die Gefährlichkeit der verbreiteten Information (zB Bombenbauplänen) selbst, sondern darum, dass die Information derart aufbereitet ist, dass dem Betrachter durch deren Lektüre die Verübung einer terroristischen Straftat »emotional besonders nahegelegt«[2588] wird. Eine Bauanleitung für einen Sprengsatz ließe sich vermutlich auch in einem Handbuch für Chemiker finden.[2589] Eine solche Information ist aber, ihrem Kontext nach zu urteilen, nicht als Anleitung zur Begehung einer terroristischen Straftat bestimmt. Um in den Anwendungsbereich der Strafbestimmung des § 278f Abs 1

2586 Vgl ErlRV 1166 BlgNR XXI.GP, 40.
2587 Vgl ErlRV 674 BlgNR XXIV. GP, 6.
2588 Siehe zu Begrifflichkeit des »Aufreizens« etwa ErlStV 95 BlgNR XXIV. GP, 5; anstatt vieler *Hinterhofer* in SbgK § 283 Rz 19 mwN (Stand Februar 2001).
2589 Vgl das Beispiel aus *Bertel/Schwaighofer,* BT II[11] § 278 f Rz 1.

zu gelangen, muss daher die gefährliche Information zusätzlich mit weiteren »aufreizenden« Meta-Informationen versehen sein, weshalb es auf den Kontext und die pragmatische Relevanz für den Betrachter ankommt. Die Aufforderung muss geradezu dazu bestimmt sein, zur Begehung einer terroristischen Straftat anzuleiten, weshalb auch auf der inneren Tatseite die Absicht[2590] bestehen muss, dass zur Begehung einer solchen Tat aufgereizt wird.[2591] Es handelt sich dabei um eine überschießende Innentendenz. In tatsächlicher (objektiver) Hinsicht muss der Täter die Anleitung zur Begehung einer terroristischen Straftat (§ 278c) mit den in § 278e angeführten Mitteln lediglich anbieten oder einer anderen Person zugänglich machen. Strafbar ist diese Handlung aber erst, wenn der Täter darüber hinaus zum Tatzeitpunkt auch noch die Absicht hat, zur Begehung einer terroristischen Straftat aufzureizen. Es liegt daher ein Absichtsdelikt ieS vor.

8. Sonstiges

Die Strafdrohung des Abs 1 sieht eine Freiheitsstrafe von bis zu zwei Jahren vor und so fällt § 278f somit gem § 31 Abs 4 Z 1 StPO in die sachliche Zuständigkeit des Einzelrichters des Landesgerichts.

9. Sich-Verschaffen von inkriminierten Informationen

Ebenso ist nach § 278f Abs 2 zu bestrafen, wer sich ein Medienwerk iSd Abs 1 oder solche Informationen aus dem Internet verschafft, um eine terroristische Straftat (iSd § 278c Abs 1 Z 1 bis 9 oder 10) zu begehen.

Die Tathandlung des Sich-Verschaffens – bezogen auf Informationen aus dem Internet – setzt nach den Erl »das Abspeichern auf einem Speichermedium voraus, da der Täter beim Sich-Verschaffen ein eigenes Zutun zur Gewahrsamserlangung setzen muss«.[2592] Abgesehen davon, dass bereits beim Öffnen bzw Laden solcher Informationen durch das Klicken auf entsprechende Dateiverlinkungen auf einer Website ein aktives Tun des Täters vorliegt und daher bereits das grundsätzli-

2590 Im Sinne des § 5 Abs 2.

2591 Vgl auch JAB 1422 BlgNR XXIV. GP, 5.

2592 Vgl ErlRV 674 BlgNR XXIV. GP, 6; idS wohl auch *Brandstetter,* Neues aus dem Besonderen Teil des StGB, in Mitgutsch/Wessely (Hrsg), Strafrecht Besonderer Teil. Jahrbuch 2012 (2012) 13 (20).

che Erfordernis des Tätigwerdens für ein »Sich-Verschaffen« gegeben ist, darf mE iZm inkriminierten Inhalten von ubiquitären Daten nicht auf eine Gewahrsamsbegründung im strengen strafrechtlichen Verständnis abgestellt werden.[2593] Vielmehr geht es im deliktsspezifischen Kontext um das Sich-Kenntnisverschaffen der konkreten tatbildlichen Informationen (Informationsverschaffung). Das Unrecht des definierten objektiven Verhaltens liegt wohl im aktiven Bemühen des Täters, an solche deliktischen Informationen zu gelangen. Dass sich der Täter die Dateien, welche die Informationen repräsentieren, daher – nach den Erl – erst noch auf einen Datenträger herunterladen müsse, um das gesetzliche Tatbild zu erfüllen, verfehlt das teleologische Zielanliegen dieser Bestimmung. Selbst wenn der Täter zB eine spezielle Anleitung für terroristische Anschläge samt Bombenbauplan zwar im Internet aufrufen, lesen und ggf unmittelbar befolgen würde, wäre er nach den GMat offensichtlich – aber auch unsachlich – nicht strafbar, da er die Information nicht auf einem körperlichen Speichermedium abgespeichert hat. Der Gesetzgeber hätte in Anlehnung an § 207a[2594] Abs 3a auch das Sich-Verschaffen von Medienwerken auf der einen und das wissentliche »Zugreifen« auf solche Informationen im Internet auf der anderen Seite als Tathandlungen definieren können. Auch aus dem Faktum, dass der »Besitz« solcher Informationen oder Medienwerke kein tatbestandliches Unrecht darstellt, lässt sich ableiten, dass es gerade nicht auf die körperliche Innehabung solcher Informationen (aber auch Medienstücke) ankommt. Gelangt daher jemand in den Besitz einschlägiger Medienwerke oder Informationen, ohne sich aktiv den Gewahrsam daran zu verschaffen, so liegt diesbezügliche keine strafbare Handlung vor. Daher gilt: Es gibt kein grundsätzliches Besitzverbot für solche Informationen.

Gerade aber weil in den GMat iZm § 278f mehrfach auf § 207a Abs 3 verwiesen wird und insb auch die Strafdrohung des § 278f dem Sich-Verschaffen oder Besitzen einer pornographischen Darstellung einer unmündigen[2595] Person nach § 207a Abs 3 letzter Satz angeglichen werden soll, stellt sich die Frage, warum nicht auch ein Besitzverbot für

2593 Siehe dazu bereits die ausf Auseinandersetzung iZm § 207a Abs 3.

2594 In den Erl zu § 278f wird ohnehin mehrfach auf § 207a verwiesen (ErlRV 674 BlgNR XXIV. GP, 6).

2595 Man beachte, dass in den GMat ausdrücklich auf die Höhe des Strafsatz für unmündige Minderjährige des § 207a Abs 3 Satz 2 verwiesen wird (ErlRV 674 BlgNR XXIV. GP, 6).

solche besonders gefährlichen Informationen normiert wurde. Schlüssigerweise müsste wohl gerade deshalb, weil der Gesetzgeber die Informationen und Medienwerke iSd § 278f Abs 1 der Gefährlichkeit von pornographischen Darstellungen unmündiger Minderjähriger gleichstellt, eine Besitzstrafbarkeit für ein solches verpöntes Material geschaffen werden.

§ 278f Abs 2 macht es im subjektiven Tatbestand erforderlich, dass sich der Täter die einschlägigen Medienwerke oder Informationen aus dem Internet dazu verschafft, um eine terroristische Straftat (iSd § 278c Abs 1 Z 1 bis 9 oder 10) zu begehen. Es handelt sich daher ebenfalls um ein Delikt mit überschießender Innentendenz, wobei dolus eventualis bereits ausreicht (Absichtsdelikt iwS). Da der Täter im Tatzeitpunkt lediglich die Zielvorstellung haben muss, mit diesen Informationen in weiterer Folge selbst eine terroristische Straftat zu begehen, kann man von einem »verkümmert zweiaktigen Delikt« sprechen.

B. Cyber-Stalking oder die Beharrliche Verfolgung (via Internet) iSd § 107a

> § 107a (1) Wer eine Person widerrechtlich beharrlich verfolgt (Abs. 2), ist mit Freiheitsstrafe bis zu einem Jahr zu bestrafen.
>
> (2) Beharrlich verfolgt eine Person, wer in einer Weise, die geeignet ist, sie in ihrer Lebensführung unzumutbar zu beeinträchtigen, eine längere Zeit hindurch fortgesetzt
>
> 1. ihre räumliche Nähe aufsucht,
>
> 2. im Wege einer Telekommunikation oder unter Verwendung eines sonstigen Kommunikationsmittels oder über Dritte Kontakt zu ihr herstellt,
>
> 3. unter Verwendung ihrer personenbezogenen Daten Waren oder Dienstleistungen für sie bestellt oder
>
> 4. unter Verwendung ihrer personenbezogenen Daten Dritte veranlasst, mit ihr Kontakt aufzunehmen.[2596]

§ 107a wurde durch das StRÄG 2006[2597] geschaffen, um einen adäquaten Schutz für »Stalking«-Opfer zu gewährleisten. Durch diese Strafbestim-

2596 BGBl 60/1974 idF I 93/2007.
2597 BGBl I 56/2006.

mung sollen beharrlich gesetzte Verhaltensweisen pönalisiert werden, die von anderen Bestimmungen, wie §§ 107, 109, 83 nicht erfasst sind, aber geeignet sind, beträchtlich in die Lebensführung des Opfers einzugreifen.[2598] § 107a wurde in den 3. Abschnitt des StGB bei den »Strafbare Handlungen gegen die Freiheit« eingegliedert[2599], schützt aber wohl überwiegend die Privatsphäre.[2600]

1. Zum Begriff »Stalking«

Der Begriff »Stalking« (engl für Anschleichen oder Nachstellen) wurde aus der Jägersprache entlehnt und bezeichnet das Heranschleichen des Jägers an das Wild.[2601]

Nach § 107a Abs 1 macht sich derjenige strafbar, der eine Person widerrechtlich[2602] beharrlich verfolgt. Was unter einer beharrlichen Verfolgung einer Person zu verstehen ist, definiert der Gesetzgeber in § 107a Abs 2. Demnach verfolgt eine Person beharrlich, wer in einer Weise, die geeignet ist, sie in ihrer Lebensführung unzumutbar zu beeinträchtigen, eine längere Zeit hindurch fortgesetzt 1. ihre räumliche Nähe aufsucht, 2. im Wege einer Telekommunikation oder unter Verwendung eines sonstigen Kommunikationsmittels oder über Dritte Kontakt zu ihr herstellt, 3. unter Verwendung ihrer personenbezogenen Daten Waren oder Dienstleistungen für sie bestellt oder 4. unter Verwendung ihrer personenbezogenen Daten Dritte veranlasst, mit ihr Kontakt aufzunehmen.

§ 107a ist gespickt mit unbestimmten Rechtsbegriffen, wie »beharrlich«, »unzumutbar beeinträchtigten«, »längere Zeit hindurch«.[2603]

2598 Vgl ErlRV 1316 BlgNR XXII. GP, 2.

2599 Wohl iSv »Freiheit von Furcht« oder der »Willensbetätigungsfreiheit« bezüglich menschlicher Kontakte; vgl ähnlich *Wach* in SbgK § 107a Rz 5 (Stand Mai 2008).

2600 Siehe *Heissenberger,* Straf- und zivilrechtliche Aspekte der »Beharrlichen Verfolgung« gem § 107a StGB, AnwBl 2006, 634; auch *Wach* in SbgK § 107a Rz 5.

2601 Siehe etwa ErlRV 1316 BlgNR XXII. GP, 4; *Wolfrum/Dimmel,* Das »Anti-Stalking-Gesetz«, ÖJZ 2006/29, 475; *Velten,* Stalking (Teil I), JSt 2003, 159; *Schwaighofer* in WK² § 107a Rz 4.

2602 Siehe zur Bedeutungsvielfalt dieses Begriffs im deliktsspezifischen Zusammenhang bei *Starzer,* Vom Jäger zum Gejagten – Thesen zur Interpretation und Reformierung des § 107a StGB unter Berücksichtigung dogmatischer und empirischer Ergebnisse (Dissertation 2010) 83.

2603 Vgl etwa *Sadoghi,* Stalking – eine differenzierte Betrachtung dogmatischer Probleme, AnwBl 2007, 340; *Schwaighofer* in WK² § 107a Rz 4; *Mitgutsch,* Ausgewählte Probleme der Freiheitsdelikte – Beharrliche Verfolgung und fortgesetzte Gewalt-

Mit dem Erfordernis der Beharrlichkeit wird auf die Hartnäckigkeit und gesteigerte Gleichgültigkeit des Täters bezüglich der Angst des Opfers in seinem Stalking-Verhalten Bezug genommen.[2604] Beharrlichkeit erfordert auch eine gewisse Intensität und Zeitdauer.[2605] Es ist daher ein wiederholtes oder andauerndes Verhalten[2606] angesprochen, das trotz Rückschlägen und Misserfolgen fortgesetzt wird.[2607] *Beclin* weist zu Recht daraufhin, dass darüber hinaus auch eine gewisse Regelmäßigkeit des Verhaltens erforderlich sein wird. Große Zeitabstände zwischen einzelnen inkriminierten Handlungen indizieren daher auch idR keine Beharrlichkeit.[2608] *Bertel/Schwaighofer* befinden, dass in harmlosen Fällen zehn Einzelhandlungen über mehrere Wochen ausreichend seien und bei schweren Fällen (zB bei § 107a Abs 2 Z 3) drei Handlungen über einen kürzeren Zeitraum zur Erfüllung des Tatbestands genügen dürften.[2609]

2. Unzumutbare Beeinträchtigung der Lebensführung

Stalking-Handlungen iSd § 107a Abs 2 Z 1 bis 4 sind überdies nur strafbar, wenn sie geeignet sind, die betroffene Person in ihrer Lebensführung unzumutbar zu beeinträchtigen (potentielles Gefährdungsdelikt).[2610] Dass die Lebensgestaltung des Opfers tatsächlich beeinträchtigt wird, ist nicht gefordert. Das Täterverhalten muss im Einzelfall betrachtet nur typischer Weise eine solche Beeinträchtigung erwarten lassen. Beispielsweise liegt eine deliktsspezifische Beeinträchtigung vor, wenn das Opfer sich nicht mehr traut, Telefonanrufe entgegenzunehmen, oder seine Wohnung nur unter Schutzvorkehrungen und schließlich nur noch selten verlässt, bestimmte Orte meidet,

---

ausübung, in Mitgutsch/Wessely (Hrsg), Strafrecht Besonderer Teil. Jahrbuch 2010 (2010) 21 (21); *Sautner/Unterlerchner,* Kriminalpolitische und dogmatische Bemerkungen zu einer Reform des StGB, ÖJZ 2014/10, 63 (67).

2604 Siehe ErlRV 1316 BlgNR XXII. GP, 5.

2605 Siehe dazu *Bertel/Schwaighofer,* BT I[12] § 107a Rz 4; *Fabrizy,* StGB[11] § 107a Rz 2.

2606 ErlRV 1316 BlgNR XXII. GP, 5.

2607 Siehe dazu ErlRV 678 BlgNR XXIII. GP, 25; *Schwaighofer* in WK[2] § 107a Rz 8.

2608 Vgl *Beclin,* § 107a StGB – Bekämpfung von »Stalking« auf Kosten der Rechtssicherheit?, in BMJ (Hrsg), 34. Ottensteiner Fortbildungsseminar aus Strafrecht und Kriminologie. Bd 127 (2006) 103 (116).

2609 Vgl *Bertel/Schwaighofer,* BT I[12] § 107a Rz 4.

2610 Siehe *Schwaighofer* in WK[2] § 107a Rz 11; *Birklbauer/Hilf/Tipold,* Strafrecht BT I[2] § 107 Rz 2 bzw 7; *Fabrizy,* StGB[11] § 107a Rz 8.

seine sozialen Kontakte einschränkt und sich im Extremfall zu einem Wohnungs- und/oder Arbeitsplatzwechsel gezwungen sieht.[2611] Auch wurde jüngst eine solche Situation angenommen, als jemand über etwa 3 Monate dem Opfer oftmals vor der Schule auflauerte, es mehrmals, teilweise mehrmals täglich, anrief und dabei in einem Fall mitteilte, dass es beschattet werde.[2612]

Das dabei erforderliche Element der Unzumutbarkeit schränkt das strafbare Verhalten auf schwerwiegende Eingriffe ein. In den Erl werden die Begehungsweisen nach Z 1 und 2 als grundsätzlich sozial adäquate Handlungen beschrieben, die erst durch ihre Häufigkeit, Kontinuität und Intensität für das Opfer unzumutbar werden und Anlass für eine Veränderung der Lebensumstände geben können. Aus diesem Grund seien in diesen Fällen auch eine Interessenabwägung und eine Abgrenzung der Freiheitssphären von Täter und Opfer vorzunehmen.[2613]

Die Unzumutbarkeitsgrenze soll nach den GMat aufgrund objektiver Kriterien bestimmt werden. Überschritten sei diese dann, wenn durch die einzelnen Tathandlungen in die konkrete Lebenssituation des Opfers durch eine Verletzung der verfassungsrechtlich gewährleisteten Persönlichkeitsrechte (Privat- und Familienleben, Wohnung und Brief- und Telefonverkehr) eingegriffen werde.[2614]

3. »Längere Zeit hindurch«

Der Gesetzesbegriff der »Fortsetzung über eine längere Zeit hindurch« ist – wie bereits im Fall des § 126b Abs 2 – unklar. Der Gesetzgeber liefert dazu im Grunde genommen keine verwertbaren Anhaltspunkte und überlässt dadurch die Auslegung der gerichtlichen Praxis. Er führt dazu lediglich aus, dass dieser Begriff nur in Relation zur Tathandlung festgelegt und jeweils nur nach den Besonderheiten des Einzelfalles gedeutet werden könne.[2615] Zutreffend hält *Schwaighofer* dazu fest, dass sich aus dem Wort »fortgesetzt« jedenfalls zwingend ergäbe, dass ein wiederholtes Handeln notwendig sei.[2616] Maßgeblich ist die Belastung

2611 Siehe ErlRV 1316 BlgNR XXII. GP, 6.
2612 Siehe OGH 17.10.2012, 15 Os 114/12x.
2613 ErlRV 1316 BlgNR XXII. GP, 6.
2614 Siehe ErlRV 1316 BlgNR XXII. GP, 6; *Fabrizy,* StGB[11] § 107a Rz 10.
2615 Vgl ErlRV 1316 BlgNR XXII. GP, 6 mwN.
2616 Siehe *Schwaighofer* in WK[2] § 107a Rz 9; weiters auch *Wach* in SbgK § 107a Rz 55.

für das Opfer, welche sich – neben der Art und Schwere der einzelnen Handlungen – auch aufgrund der Häufigkeit, Dauer und den dazwischen liegenden Zeitabständen ergibt.[2617]

4. Deliktstypus

Die vier Tathandlungen beschreiben § 107a Abs 1 iVm Abs 2 durch ihre rechtliche Gleichwertigkeit als alternatives Mischdelikt.[2618] § 107a Abs 1 ist nach hM in seiner äußeren Beschreibung ein schlichtes Tätigkeitsdelikt, das iZm § 107a Abs 2 bezüglich der Eignung der Begehungsweisen der Z 1 bis 4 zur unzumutbaren Beeinträchtigung der Lebensführung, darüber hinaus in Relation zum geschützten Rechtsgut ein potentielles Gefährdungsdelikt darstellt.[2619] Nach *Wach* sind jedoch alle Begehungsweisen der Z 1 bis 4 Erfolgsdelikte[2620], was auch zutreffend ist.

Obwohl der Gesetzgeber wohl bewusst aus einem zunächst noch vorgeschlagenen[2621] Erfolgsdelikt ein schlichtes Tätigkeitsdelikt machen wollte, um dem Umstand Rechnung zu tragen, »dass der Unwert des Stalking weniger durch einen eingetretenen Erfolg als durch ein intensives Täterverhalten gekennzeichnet ist«[2622], ist ihm dies mit dem geltenden Wortlaut des § 107a Abs 1 iVm Abs 2 nicht vollständig gelungen. Die Erl lassen allerdings darauf schließen, dass der »Erfolg« am Rechtsgut gemessen wird. Ein Erfolgsdelikt liegt aber nach hM dann vor, wenn eine von der Tathandlung zumindest gedanklich abtrennbare Wirkung in der Außenwelt hervorgerufen wird, was sich allein aus der Tatbestandsauslegung und daher aus der Struktur des Tatbestands ergibt.[2623] Dies bedeutet, dass ein tatbestandlicher Erfolg nicht unbedingt eine Beeinträchtigung des Rechtsguts verlangt. So ist mit dem Öffnen eines fremden, verschlossenen Briefes eine Veränderung in der Außenwelt (= Erfolg) eingetreten (da in der Außenwelt nunmehr ein

2617 Siehe *Schwaighofer* in WK² § 107a Rz 10; vgl auch *Wach* in SbgK § 107a Rz 57.
2618 Vgl ErlRV 1316 BlgNR XXII. GP, 5; auch *Wach* in SbgK § 107a Rz 8; *Schwaighofer* in WK² § 107a Rz 14.
2619 In diesem Sinne wohl auch *Schwaighofer* in WK² § 107a Rz 2; *Kienapfel/Schroll,* StudB BT I³ § 107a Rz 2; weiters *Birklbauer/Hilf/Tipold,* Strafrecht BT I² § 107 Rz 2; aA *Wach* in SbgK § 107a Rz 60, die in allen Begehungsweisen der Z 1 bis 4 Erfolgsdelikte erblickt.
2620 Vgl *Wach* in SbgK § 107a Rz 60.
2621 Siehe § 107a idF 349/ME XXII. GP bzw ErlME 349/ME XXII. GP, 18.
2622 Vgl ErlRV 1316 BlgNR XXII. GP, 4.
2623 Vgl generell zB *Fuchs,* AT I⁸, Rz 10/40; *Kienapfel/Höpfel/Kert,* AT¹⁴, Z 9 Rz 6 ff.

geöffneter Briefumschlag vorliegt), aber das Rechtsgut wurde dadurch bloß abstrakt gefährdet.[2624]

Betrachtet man nun den Gesamttatbestand des § 107a Abs 1 in seiner vollen Reichweite, ergibt sich durch die Verquickung des Tatbestandsmerkmals »beharrlich verfolgt« mit dessen normspezifischen Legaldefinition in Abs 2, dass zwar (nur) augenscheinlich eine schlichte Tätigkeit (arg »beharrlich verfolgt«) ohne Rücksicht auf eine von ihr bewirkte Veränderung in der Außenwelt beschrieben wird, welche wiederum ausschließlich Begehungsweisen der Z 1 bis 4 impliziert, die ihrerseits allerdings allesamt eine Veränderung der Außenwelt bewirken müssen. Man könnte diese Konstellation als ein »mittelbares Erfolgsdelikt« betrachten. *Triffterer* spricht in ähnlichem Zusammenhang, wenn in einem Tatbestand ein Zwischenerfolg mit einer abstrakten Gefährlichkeit oder einer konkreten Gefährdung kombiniert wird, von einem »erfolgsbedingten Gefährdungsdelikt«.[2625] Ob das Rechtsgut durch die einzelnen taxativ angeführten Verhaltensweisen des § 107a Abs 2 Z 1 bis 4 nun beeinträchtigt wird, ist idR für eine Deliktseinordnung – Erfolgsdelikt oder schlichtes Tätigkeitsdelikt –, die alleine durch Tatbestandsauslegung zu ermitteln ist, ohne Belang. Das Erfordernis einer Rechtsgutgefährdung resultiert nämlich erst aus der verhaltensgebundenen Handlungsbeschreibung des § 107a Abs 2 zweiter HS, die besagt, dass die beharrliche Verfolgung »in einer Weise« erfolgen muss, die geeignet ist, das Opfer unzumutbar in seiner Lebensführung zu beeinträchtigen, indem eine längere Zeit hindurch fortgesetzt Handlungen iSd Katalogs des § 107a Abs 2 getätigt werden. Trotz der für potentielle Gefährdungsdelikte üblichen Wortwahl für die im Einzelfall festzustellende generelle Gefährlichkeit einer Handlung (arg »[…] die geeignet ist, […] zu beeinträchtigen […]), ergibt sich in Zusammenschau, dass aus den Erfordernissen für eine beharrliche Verfolgung nicht nur eine aus der allgemeinen Erfahrung abzuleitende (abstrakte) Gefahr für ein Rechtsgut verlangt wird. »Geeignet« beschreibt nämlich an dieser Stelle keine generelle Gefährlichkeit. Vielmehr ist der Tatbestand nur erfüllt, wenn ein konkretes Handlungsobjekt[2626] tatsächlich in den Wirkungsbereich der gefährlichen Begehungsweisen nach § 107a Abs 2 Z 1 bis 4 gelangt ist, weshalb auch eine Rechts-

2624 Siehe dieses Beispiel zur Verletzung des Briefgeheimnisses in *Fuchs,* AT I[8], Rz 10/47.
2625 Siehe *Triffterer,* AT[2], 64.
2626 Arg »eine Person«.

gutverletzung in concreto mit hoher Wahrscheinlichkeit zu befürchten ist[2627] und dadurch ein konkreter Gefährdungserfolg indiziert ist. Die Handlungen iSd § 107a Abs 2 Z 1 bis 4 müssen sich auf ein ganz konkretes Tatobjekt (nämlich ausschließlich die gestalkte Person) beziehen und dort Zwischenerfolge herbeiführen, die sich nach Prüfung im Einzelfall zu einer »beharrlichen Verfolgung« in Intensität und Dauer verdichten müssen. Es ist grundsätzlich tatbestandlich unbeachtlich, wenn solche Handlungen des Täters bezüglich unterschiedlicher Tatobjekte vorgenommen werden. Nur in einem solchen Fall würde aber tatsächlich eine »abstrakte Gefährlichkeit« der Handlung(en) anzunehmen sein. Richtig ist vielmehr, dass § 107a voraussetzt, dass eine klar determinierte Person in den Wirkungsbereich fortgesetzter Täterhandlungen gelangen muss (»konkrete Gefährdung«).

Die Verletzung des betroffenen Rechtsguts ist aber weiterhin kein Faktum, sondern nur eine – wenn auch schon konkrete – Möglichkeit. Daher ist § 107a, was die Relation zum Rechtsgut betrifft, ein konkretes Gefährdungsdelikt.[2628] Aus diesem Grund muss dem Täter diese Gefährdung des Tatobjekts im Einzelfall ex post aus der Opferperspektive nachgewiesen werden. Demnach ist zu beurteilen, ob durch die Tathandlung(en) des Täters tatsächlich ein ernst zu nehmendes Risiko für die konkrete (gestalkte) Person geschaffen wurde. Die Gefahr ist folglich ein – wenn auch ungeschriebenes – dem Tatbestand des § 107a Abs 2 immanentes Merkmal. Es ließe sich der Gesamttatbestand des § 107a auch zu folgendem Unrechtstatbestand des Abs 1 umformulieren: »Wer eine Gefahr für die Freiheit von Furcht oder für die Privatsphäre einer Person dadurch herbeiführt, dass er diese beharrlich verfolgt, […]«.

Der Handlungskatalog des § 107a Abs 2 Z 1 bis 4 beschreibt ausschließlich Erfolgsdelikte, deren Erfolge – tatbestandlich betrachtet – tatsächlich und nicht nur potentiell in der Außenwelt eintreten müssen. Mit anderen Worten, zumindest ein solcher Erfolg muss tatsächlich eingetreten sein, damit überhaupt erst ein konkreter Gefährdungserfolg bei einem klar determinierten Rechtsgut bzw dessen konkretem menschlichen Träger in Betracht kommt. Im Ergebnis sind diese (Zwischen-)Erfolge«[2629] nach Z 1 bis 4 dafür maßgeblich, ob das konkrete

2627 Vgl etwa generell *Leukauf/Steininger,* StGB[3] § 17 Rz 11.

2628 AA *Wach,* die neben einem Erfolgsdelikt von einem abstrakten Gefährdungsdelikt spricht *(Wach* in SbgK § 107a Rz 6).

2629 Siehe zutreffend von »Zwischenerfolgen« sprechend *Wach* in SbgK § 107a Rz 6.

Tatobjekt in den Wirkungsbereich dieser gefährlichen Handlung iSd Abs 2 gelangt ist und dadurch das Tatbestandsmerkmal »beharrlich verfolgen« des § 107a Abs 1 erfüllt ist. § 107a besitzt daher in seinem Gesamttatbestand eine formale Tatbestandsstruktur, die nur in der eingeschränkten Betrachtung seines Abs 1 einem schlichten Tätigkeitsdelikt entspricht. Hingegen stellt er materiell gesehen ein Erfolgsdelikt dar, weil auf ein ganz konkretes Tatobjekt fokussiert wird, weshalb das als beeinträchtigend wahrgenommene, verhaltensgebundene Handeln des Täters – über die tatbestandlichen Erfolge nach § 107a Abs 2 Z 1 bis 4 – die Außenwelt gezwungener Maßen verändern muss. Ein beharrliches Verfolgen iSd § 107a Abs 1 ist somit nicht als schlichte Tätigkeit zu sehen, sondern verlangt durch die ausschließliche gesetzliche Ausfüllung dieser Tathandlung iSd Abs 2 einen bzw mehrere Erfolg(e). Dies lässt sich auch, was seine Beziehung zum Rechtsgut betrifft, stimmig mit der Einordung als ein konkretes Gefährdungsdelikt kombinieren.

Im Sinne des hier behandelten Untersuchungsgegenstands interessieren va die Begehungsweisen des sog »Cyber-Stalking« (Z 2) bzw des Verwendens personenbezogener Daten (Z 3 und 4), weshalb nur kurz auf die Begehungsweise des Aufsuchens der räumlichen Nähe der Z 1 hingewiesen wird.

5. Aufsuchen der räumlichen Nähe

§ 107a Abs 2 Z 1 erfasst Stalking-Handlungen, bei denen der Täter eine – für das Opfer wahrnehmbare[2630] – unmittelbare physische (räumliche) Kontaktaufnahme sucht. Ob ein »Kontakt« mit dem Opfer tatsächlich zustande kommt, ist unbeachtlich.[2631] Die Wortwahl »Kontakt« ist an dieser Stelle unpräzise, denn verlangt wird in dieser Deliktsvariante bloß das Aufsuchen der räumlichen Nähe, ob der Täter mit dem Opfer in Kontakt tritt ist irrelevant.[2632] Das »Aufsuchen der räumlichen Nähe des Opfers« verlangt eine Ortsveränderung des Täters.[2633] Wenn der Täter zB aus seiner eigenen Wohnung heraus das Tatobjekt beob-

2630 Siehe ErlRV 1316 BlgNR XXII. GP, 5; weiters *Birklbauer/Hilf/Tipold,* Strafrecht BT I² § 107a Rz 9.

2631 Vgl *Wach* in SbgK § 107a Rz 25 ff; *Schwaighofer* in WK² § 107a Rz 15 ff; *Beclin* in BMJ, 34. Ottensteiner Fortbildungsseminar, 103 (117).

2632 Siehe *Beclin* in BMJ, 34. Ottensteiner Fortbildungsseminar, 103 (117).

2633 Vgl statt vieler *Wach* in SbgK § 107a Rz 25.

achtet oder filmt, ist der Tatbestand nicht erfüllt.[2634] Das muss aber selbst dann gelten, wenn sich der Täter in einem Hotelzimmer gegenüber der Wohnung des Opfers einquartiert, um dieses aus der Ferne zu beobachten. In diesem Fall hat er zwar eine Ortsveränderung für seine Handlungen vorgenommen, nicht aber die »räumliche Nähe« zum Opfer hergestellt. So führt *Schwaighofer* aus, dass wer jemand anderen laufend mit einem Fernrohr aus 200 m Entfernung beobachtet, sich nicht in räumlicher Nähe desjenigen befindet, selbst dann nicht, wenn dieses Verhalten vom Opfer wahrgenommen wird.[2635]

Wach schlägt vor, die geforderte räumliche Nähe zum Tatobjekt dann anzunehmen, wenn sich der Täter dem Opfer physisch so weit angenähert hat, dass ein zwischenmenschlicher privater Kontakt möglich ist. Das ist dann der Fall, »wenn er auf Rufweite herangekommen ist oder zumindest ein Blickkontakt zwischen ihm und dem Opfer möglich erscheint«. Die konkrete Möglichkeit der Wahrnehmung reiche aus.[2636] Das Erfordernis, dass der Täter aber eine gewisse räumliche Sphäre des Opfers tatsächlich – von diesem auch wahrnehmbar – betreten muss, indiziert § 107a Abs 1 in dieser Begehungsweise als ein Erfolgsdelikt.[2637]

Das zufällige Aufhalten am selben Ort begründet keine Strafbarkeit, da das »Aufsuchen« ein gezieltes Vorgehen des Täters verlangt.[2638] Gefordert ist daher, dass der Täter die räumliche Nähe des Opfers nur aus dem deliktischen Grund betritt.

6. »Distanz-Stalking« iSd § 107a Abs 2 Z 2

Eine beharrliche Verfolgung »im Wege einer Telekommunikation« (§ 107a Abs 2 Fall 1) liegt bei jedem technischen Vorgang des Aussendens, Übermittelns und Empfangens von Nachrichten jeglicher Art in der Form von Zeichen, Sprache, Bildern oder Tönen mittels dazu dienender technischer Einrichtungen vor.[2639] Aus technischer Sicht handelt

2634 Siehe etwa *Schwaighofer* in WK² § 107a Rz 17; *Mitgutsch* in Mitgutsch/Wessely, Jahrbuch 2010, 21 (30).
2635 Vgl dazu *Schwaighofer* in WK² § 107a Rz 18.
2636 Siehe *Wach* in SbgK § 107a Rz 29.
2637 Überzeugend *Wach* in SbgK § 107a Rz 25.
2638 Siehe auch *Heissenberger,* AnwBl 2006, 634.
2639 Vgl ErlRV 1316 BlgNR XXII. GP, 5; zur Telekommunikation allgemein weiters auch ErlRV 1325 BlgNR XXII. GP, 6; ErlRV 1505 BlgNR XXIV. GP, 6.

es sich bei einer »Kommunikation« grundsätzlich um den Austausch von Informationen.[2640] Von einer »Telekommunikation« spricht man, wenn solche Kommunikationen über beliebige Entfernungen stattfinden.[2641] In Zusammenhang mit § 107a Abs 1 iVm § 107a Abs 2 Z 2 Fall 1 reicht aber wohl die Verwendung einer telekommunikationstechnischen Infrastruktur aus, selbst wenn es dabei nicht zu einem – der Definition entsprechenden – Transfer einer Nachricht bzw gedanklichen Mitteilung gekommen ist. Beim wiederholt fortdauernden »Läutenlassen« des Telefons des Tatobjekts, ohne dabei Nachrichteninhalte zu übermitteln, werden nämlich grundsätzlich[2642] keine »Nachrichten« – weder im kernstrafrechtlichen Sinn noch im telekommunikationsgesetzlichen Verständnis[2643] – ausgesendet, übermittelt oder empfangen. Letztlich wird nur die dafür vorgesehene Technologie einer Telekommunikation zum Verbindungsaufbau genutzt (zB der Signalisierungskanal bei ISDN-Technik zum Rufaufbau), um das Opfer widerrechtlich beharrlich zu verfolgen.

a. Telekommunikation

Unter den Begriff der »Telekommunikation« fallen etwa die klassische Sprachtelefonie über Fest- oder Mobilfunknetze, Nachrichten per Fernschreiber und Telegrafen[2644], Fax sowie sämtliche Formen der modernen IP-Telefonie[2645] und die informationstechnischen Datenübertragungen diverser Kommunikationsdienste (zB E-Mail, SMS, MMS).[2646] Anzumerken ist, dass auch einige »Internetdienste« bereits von dieser Tatbegehungsvariante erfasst werden, wie zB das Versenden von E-Mails oder VoIP. Andere Dienste wiederum, zB Chat-Foren, die nicht – bzw nicht überwiegend – die Übertragung von Signalen über Kommunikationsnetze zum Gegenstand haben, fallen wohl nicht vorrangig in diesen an das TKG weiterhin angedockten Begriff

2640 Siehe dazu ausf bereits oben zu §§ 119 und 120 Abs 2a.
2641 Siehe *Freyer,* Nachrichten-Übertragungstechnik[6], 13.
2642 Außer man würde einer bestimmten Konvention entsprechend zB adaptierte »Morsecodes« mittels Klingeltönen übertragen udgl.
2643 Vgl dazu ebenfalls die Ausführungen zu § 119 und § 120 Abs 2a.
2644 Siehe *Thiele* in SbgK § 119 Rz 39 mit weiteren Beispielen.
2645 Auch Internet-Telefonie oder Voice-over-IP (VoIP) genannt; dabei wird ein Gespräch in digitaler Form in Echtzeit über ein paketvermittelndes Datennetz mittels des IP-Protokolls übertragen (siehe *Hein/Reisner,* TCP/IP[2], 499 f).
2646 Vgl auch ErlRV 1316 BlgNR XXII. GP, 5.

der Telekommunikation.[2647] Eine solche Übertragung erbringt für die Chat-Teilnehmer idR der jeweilige Internet-Zugangsanbieter. Die Abgrenzung kann sich in der Praxis auf Grund des Zusammenwachsens verschiedener Technologien als schwierig erweisen. Beim Betreiber eines Chat-Forums handelt es sich nach dem VwGH nicht um einen Betreiber eines (öffentlichen) Telekommunikationsdienstes iSd § 3 Z 9 TKG 2003.[2648] Was allerdings nicht eindeutig unter eine »Telekommunikation« fällt, könnte unter die Auffangbeschreibung der »sonstigen Kommunikationsmittel« fallen.

Das Internet ist in den letzten Jahren »sozialer« geworden, was auf die interaktive Nutzbarkeit des »World Wide Web« anspielt. Die Veränderung des in seinen Anfängen weitgehend von statischen Internetauftritten geprägten WWW zum dynamischen »User generated Content« wird auch durch die Bezeichnung »Web 2.0« für eine neue Version des Internet hervorgehoben. Soziale Plattformen wie zB Facebook, Google+, Twitter, YouTube, aber auch Bewertungsportale, Blogs und E-Foren sind zu integrativen Bestandteilen dieser neuen Internetgeneration geworden.

Diese neuen Dienste ermöglichen auch Stalking-Handlungen, die idR als weniger gravierend einzustufen sind als konventionelle Formen des Nachstellens. Gleichwohl kann eine Verquickung von »virtueller Verfolgung« mit physischem Nachstellen eine Intensivierung ergeben, da so Stalking rund um die Uhr, weitgehend anonym[2649], von physischen Räumen losgelöst und von »zuhause aus« praktiziert werden kann. Dies geht soweit, dass sich Betroffene nicht mehr wagen ihre Computer einzuschalten oder ihre E-Mail-Postfächer abzurufen und letztlich gewisse Kommunikationsdienste nicht mehr nutzen können bzw wollen. Solche Dienste, welche überwiegend bereits unter die Begehungsweise des § 107a Abs 2 Z 2 Fall 1 fallen, können ggf ergänzend von § 107a Abs 2 Z 2 Fall 2 erfasst werden.

2647 Siehe ErlRV 1316 BlgNR XXII. GP, 5.

2648 Siehe dazu ausf VwGH 27. 05. 2009, 2007/05/0280, worin insb untersucht wurde, ob § 53 Abs 3a SPG idF BGBl I 158/2005 die Sicherheitsbehörden berechtigt auch von einem Betreiber eines Chat-Forums Auskunft über Name, Anschrift und Teilnehmernummer eines bestimmten Anschlusses zu verlangen, wenn sie diese Daten als wesentliche Voraussetzung für die Erfüllung der ihnen übertragenen Aufgaben benötigen.

2649 Vgl auch *Starzer,* Jäger, 33.

b. Cyber-Stalking

Der Begriff »Cyber[2650]-Stalking«[2651] ist bezüglich § 107a Abs 2 Z 2 aber nur eingeschränkt zutreffend, da lediglich neben den bereits unter Fall 1 fallenden Diensten des Internet (zB E-Mail), weitere Internetanwendungen »unter die Verwendung sonstiger Kommunikationsmittel« (Fall 2) subsumiert werden können. Aber selbst bei den sonstigen Kommunikationsmitteln könnte auch an völlig konventionelle (analoge) Mittel wie Zeitungsinserate und Flugblätter gedacht werden.[2652] Es fragt sich allerdings, wie der Begriff »unter Verwendung« eines sonstigen Kommunikationsmittels – im Vergleich zu »im Wege« einer Telekommunikation (Fall 1) – zu verstehen ist. Stellt jemand »Kontakt« zum Opfer her, in dem er diesem etwa ständig die Internetverbindung unterbricht oder dessen System durch DoS-Angriffe zum Absturz bringt, so hat er nicht »im Wege« eines bestimmten Kommunikationsdienstes im eigentlich Sinn agiert, dh »diesen ordnungsgemäß benützt«, sondern bloß einen solchen Dienst für seinen Angriff – zweckentfremdet – »verwendet«.[2653] Der Kontakt zum Opfer wäre dabei – anders als bspw bei einem heimlichen Peilsender[2654] – ebenfalls hergestellt, sobald das Opfer die Dienstunterbrechungen in seiner Sphäre (in concreto Com-

2650 Der im heutigen Sprachgebrauch manifestierte Begriff(-steil) »Cyber« wird als Kurzwort für »Cybernetics« (griech Kybernetes = Steuermann) verstanden und repräsentiert im Wesentlichen die »virtuelle bzw digitale Welt«, wie etwa das Internet. Der Begriff wurde grundlegend ua von *Norbert Wiener* geprägt, der 1948 in »Cybernetics or Control and Communication in the Animal and the Machine« Modelle der Rückführung von Informationen und Bedeutung für die Selbstorganisation und Selbststeuerung von Menschen und Lebewesen vorstellte (siehe zur Begrifflichkeit »Cyber« ausf *Faßler,* Cyber-Moderne, 28 f); der Begriff »Cyberspace« wiederum wurde im Science-Fiction-Roman »Neuromancer« (1984) des amerikanisches Autors *William Gibson* verwendet, der damit eine künstliche Welt im Computer bezeichnete (vgl *Brush* in Jones [Ed], Encyclopedia of New Media, 112 (112 ff); weiters *Seifert,* Guide, 106).

2651 Siehe *Mitgutsch,* Strafrechtliche Aspekte des »Anti-Stalking-Pakets«, RZ 2006, 186; *Mitgutsch,* Die geplante »Stalking«-Bestimmung des § 107a StGB, JSt 2006, 11; *Schwaighofer* in WK² § 107a Rz 20; *Wach* in SbgK § 107a Rz 32; siehe zum Phänomen Cyber-Stalking auch *Pittaro,* Cyber Stalking: Topology, Etiology, and Victims in Jaishankar (Ed), Cyber Criminology. Exploring Internet Crimes Criminal Behavior (2011) 277 (277 ff); weiters *Huber,* Cyberstalking und Cybercrime: Kriminalsoziologische Untersuchung zum Cyberstalking-Verhalten der Österreicher (2013) 67 ff.

2652 Ähnliche Beispiele bei *Wach* in SbgK § 107a Rz 35; *Schwaighofer* in WK² § 107a Rz 21.

2653 Man denke etwa an manipulierte Datenpakete eines Internetdienstes (siehe dazu auch die unterschiedlichen DoS-Methoden S 291 ff).

2654 Siehe dazu *Birklbauer/Hilf/Tipold,* Strafrecht BT I² § 107a Rz 9 (FN 10).

putersystem) zumindest wahrnimmt. Auch aus kriminalpolitischen Gründen sollten solche Handlungen, sofern sie die deliktsspezifische Eignung iSd § 107a Abs 2 erfüllen, von der Strafbestimmung erfasst werden.

Fall 3 zielt wiederum auf technologiefreie manuelle Botendienste ab. Im letztgenannten Fall stellt der Täter den Kontakt zum Opfer über eine weitere Person her. Dieser Dritte fungiert daher als »Kommunikationsmittler« zwischen Täter und Opfer.[2655]

Alle diese alternativen Begehungsweisen des § 107a Abs 2 Z 2 verlangen aber, dass dadurch der Kontakt mit dem Opfer hergestellt wird (Erfolgsdelikt[2656]). Der Kontakt zum Opfer ist iSd Falls 1 hergestellt, sobald etwa der Anruf am Telefon des Opfers eingegangen ist, unabhängig davon, ob das Opfer diesen durch das Abheben des Hörers »angenommen« hat. Mit dem Läuten des Telefons oder dem Eingang des E-Mails wurde der Kontakt hergestellt.[2657] Wesentliches Element ist dabei die »Kontaktherstellung zum Opfer« (arg »zu ihr herstellt«). Den Beispielen kann entnommen werden, dass ein Kontakt dann als hergestellt erachtet wird, wenn die inkriminierten Stalking-Handlungen für das Tatobjekt wahrnehmbar in dessen »Sphäre« reichen. Ob daher auch fortgesetzte beleidigende Postings in einem öffentlichen Internet-Forum, einem Blog, via sozialer Plattformen oder auf einer schlichten Website tatbestandsgemäß sein können, ist mE danach zu beurteilen, ob der Täter über diese Medien das Opfer konkret ansprechen und daher in die Sphäre desselben eindringen will oder ob er andere bzw unspezifizierte Adressaten seiner Äußerungen vor Augen hat.[2658] Als Beispiel kann die – sofern sichtbar geschaltete – individualisierte Pinnwand eines »Facebook-Profils« genannt werden, auf der der Täter für andere NutzerInnen (einschließlich der gestalkten Person) ersichtlich beleidigende Mitteilungen oder kompromittierende Bilder bezüglich der gestalkten Person veröffentlicht. Belässt der Stalker diese Postings über eine längere Zeit hindurch auf seiner Pinnwand, so dringt

2655 Siehe *Wach* in SbgK § 107a Rz 36; *Schwaighofer* in WK² § 107a Rz 22.

2656 Zutreffend *Wach* in SbgK § 107a Rz 31.

2657 Vgl *Wach* in SbgK § 107a Rz 32; *Schwaighofer* in WK² § 107a Rz 20; *Seling,* § 107a StGB. Eine Strafvorschrift gegen Stalking (2006) 61.

2658 Andernfalls wäre aber an andere klassische Delikte zu denken, wie etwa § 107 (Gefährliche Drohung), § 297 (Verleumdung), § 51 DSG 2000 (Datenverwendung in Gewinn- oder Schädigungsabsicht) oder die grundsätzlich als Privatanklagedelikte ausgestalteten Bestimmungen des § 111 (Üble Nachrede) oder § 115 (Beleidigung).

der Täter in die Sphäre des Opfers ein und stellt – ggf neben den iSd § 107a unbeachtlichen Kontakten zu anderen Personen – auch den Kontakt zum Opfer her. Selbst ein einmaliges Posting auf einem solchen Medium könnte den Tatbestand erfüllen[2659], da dem Merkmal »fortgesetzt« auch dann – wie generell bei Erfolgs-Dauerdelikten[2660] – Rechnung getragen wird, wenn der Täter durch einmaliges aktives Tun einen rechtswidrigen Zustand herbeiführt und es in weiterer Folge durch sein Verhalten[2661] – trotz Einwirkungsmöglichkeit – fortdauernd unterlässt[2662], diesen geschaffenen rechtswidrigen Zustand wieder abzuwenden, weshalb sich die Tathandlung – in einem Medium wie dem Internet – laufend perpetuiert.[2663]

Postet der Täter hingegen laufend solche Meldungen auf einer eigenen Website oder in einem Blog, die sich nicht in der Sphäre des Opfers befinden, sondern generell im Internet abrufbar sind, stellt der Täter keinen Kontakt mit dem Opfer iSd § 107a Abs 2 Z 2 her. Sollte der Täter aber in seinen Äußerungen unter der Verwendung von personenbezogenen Daten des Opfers Dritte dazu veranlassen, mit diesem Kontakt aufzunehmen (zB Heiratsanzeigen und Inserate sexueller Dienstleistungen), ist § 107a Abs 2 Z 4 einschlägig.[2664]

c. »Spamming«

Auch systematisches »Spamming« ist geeignet § 107a Abs 1 iVm § 107a Abs 2 Z 2 Fall 1 zu verwirklichen. Prinzipiell erfasst die Verwaltungsstraf-

---

2659 Überzeugend *Beclin* in BMJ, 34. Ottensteiner Fortbildungsseminar, 103 (116); *Wach* in SbgK § 107a Rz 49; aA *Starzer,* Dem Stalker auf der Spur – Ein Resümee über fast fünf Jahre § 107a StGB, in BMJ (Hrsg), 39. Ottensteiner Fortbildungsseminar aus Strafrecht und Kriminologie. Bd 150 (2011) 41 (47 ff); weiters *Seling,* Stalking, 67, der meint, dass das Tatbestandsmerkmal »fortgesetzt« eine mehrfache Wiederholung der Tathandlung zwingend voraussetze und daher in diesem Fall nicht erfüllt sei.

2660 § 107a ist ein solches Dauerdelikt; siehe statt aller *Birklbauer/Hilf/Tipold,* Strafrecht BT I² § 107a Rz 2 f.

2661 Obwohl der Täter die Löschung seines Posting vornehmen könnte, unterlässt er dies und hält den rechtswidrigen Zustand aufrecht.

2662 Siehe *Schmoller* in SbgK § 99 Rz 15.

2663 Siehe dazu *Schwarzenegger,* Hyperlinks und Suchmaschinen aus strafrechtlicher Sicht, in Plöckinger/Duursma/Mayrhofer (Hrsg), Internet-Recht (2004) 395 (420); sinngemäß *Reindl,* E-Commerce, 283; vgl auch sinngemäß *Beclin* in BMJ, 34. Ottensteiner Fortbildungsseminar, 103 (116).

2664 Siehe gleich im Anschluss.

bestimmung des § 107 Abs 2 TKG 2003 (Unerbetene Nachrichten)[2665] die Zusendung von elektronischer Post (einschließlich SMS-Nachrichten usw) zu Zwecken der Direktwerbung (Z 1) oder eine Zusendung, die an mehr als 50 Empfänger gerichtet ist (Z 2), wenn vorab keine (nicht einmal konkludente[2666]) Einwilligung[2667] des jeweiligen Empfängers eingeholt wurde. Es ist jedoch darauf hinzuweisen, dass ein Stalker eine solche Verwaltungsübertretung idR nicht begeht, da er seine »E-Mail-Bomben« weder zum Zweck der Direktwerbung, noch an mehrere[2668] Empfänger richtet. Der einzige Empfänger seiner systematischen Massen-E-Mails ist sein Opfer. Bei etwa 30 oder mehr E-Mails pro Tag über mehrere Wochen hinweg, wird der Tatbestand wohl erfüllt sein.[2669] Von einer unzumutbaren Beeinträchtigung der Lebensführung kann man in solchen Fällen dann ausgehen, wenn das Opfer sich nicht mehr anders zu helfen weiß, als seine E-Mail-Adresse zu ändern.[2670]

Was die Auswirkungen des Cyber-Stalking selbst betrifft (insb die Formen der Z 2), sind Beeinträchtigungen der Lebensführung des Opfers im Vergleich zu Handlungen in der analogen Welt – wie das Aufsuchen der räumlichen Nähe, Zusenden von Briefen im Postweg, ständiges Anrufen usw – wohl als minder gravierend einzustufen.[2671] Man wird daher für solche Stalking-Formen (zB Massen-E-Mails) die Voraussetzungen für eine Strafbarkeit – im Gegensatz zu massenhaften Telefonanrufen oder SMS-Nachrichten – wohl anheben müssen.

2665 Siehe dazu *Bergauer/Schmölzer* in Jahnel/Mader/Staudegger, IT-Recht[3], 635 (667 f).

2666 Vgl VwGH 24.03.2010, 2007/03/0177.

2667 Sog »Opt-in-Prinzip«.

2668 Zur Verwirklichung dieser Tatbegehungsalternative des § 107 Abs 2 Z 2 TKG 2003 müssten es mehr als 50 Empfänger sein.

2669 So auch *Mitgutsch,* die an dieser Stelle SMS-Nachrichten nennt (vgl *Mitgutsch* in Mitgutsch/Wessely, Jahrbuch 2010, 21 [30]); auch *Schwaighofer* in WK² § 107a Rz 10.

2670 Siehe *Bertel/Schwaighofer,* BT I[12] § 107a Rz 5.

2671 So auch *Soyer,* Über neue Kriminalitätsformen aus konsumentenpolitischer Perspektive – »de lege lata« und »de lege ferenda«, in Enthofer-Stoisser/Habersberger (Hrsg), Catch me if you can! Internet »abzocke«, »cold calls« und unseriöse Werbeveranstaltungen (2012) 107 (121); sinngemäß ebenso – aber zwischen Telefonaten und Briefen unterscheidend – *Heissenberger,* AnwBl 2006, 634.

7. Stalking durch »Identitätsmissbrauch« (§ 107a Abs 2 Z 3)

§ 107a Abs 2 Z 3 erfasst Fälle, in denen der Täter unter Verwendung personenbezogener Daten des Opfers Waren[2672] oder Dienstleistungen[2673] für diese Person bestellt. Im Wesentlichen wird dabei an den Identitätsmissbrauch gedacht, bei dem sich der Täter für das Opfer ausgibt und unter dessen Namen irgendwelche Waren oder Dienstleistungen bestellt.[2674] Der Täter missbraucht in diesem Zusammenhang personenbezogene Daten des Opfers als Rechnungs- und Lieferadresse. Die Beeinträchtigung für das Opfer ergibt sich dadurch überwiegend aus dem Erhalt der Rechnungsforderungen und nicht bestellter Waren, die er mit entsprechendem Aufwand abwehren bzw zurücksenden muss.[2675] Des Weiteren ist an Fälle zu denken, in denen der Täter zwar in seinem eigenen Namen Waren oder Dienstleistungen bestellt, diese aber unter Angabe personenbezogener Daten des Opfers der gestalkten Person liefern lässt. Der Täter verwendet in solchen Fällen, die Daten des Opfers als Lieferadresse.[2676] Hier wird das Opfer durch die Zusendung der nicht von ihm bestellten Waren belästigt. Genauso vom Wortlaut dieser Handlungsvariante (arg »für sie«) umfasst sind Fälle, in denen der Täter stellvertretend für das Opfer Waren oder Dienstleistungen bestellt, diese dann aber an dritte Personen (zB Freunde oder Feinde des Opfers) liefern lässt.[2677] *Wach* weist überzeugend darauf hin, dass solche Fälle ebenfalls eine unzumutbare Beeinträchtigung der Lebensführung hervorrufen können, wenn bspw das Opfer mit Rechnungen von Lieferanten konfrontiert werden, nachdem die belieferten Dritten die Waren bereits gutgläubig verbraucht haben.[2678]

2672 Zu denken wäre etwa an Sex-Spielzeug, Porno-Filme, Viagra, Pizza, Unterwäsche usw.

2673 Beispielsweise Beauftragung eines Hostessenservices, eines Strippers, einer Partnervermittlung.

2674 Vgl etwa *Schwaighofer* in WK² § 107a Rz 23.

2675 Vgl *Fuchs/Reindl-Krauskopf,* BT I⁴, 96.

2676 Siehe *Beclin* in BMJ, 34. Ottensteiner Fortbildungsseminar, 103 (120); weiters *Wach* in SbgK § 107a Rz 38 und 41.

2677 Siehe dazu *Wach* in SbgK § 107a Rz 41.

2678 Siehe *Wach* in SbgK § 107a Rz 41.

Das mit dieser Begehungsweise korrespondierende Beispiel in den Erl[2679] mit dem »Schalten unrichtiger Anzeigen« kann sowohl Z 3 als auch Z 4 erfüllen.[2680]

Unter Z 3 würde ein solches Verhalten dann fallen, wenn das Schalten eines kostenpflichtigen Inserats in einer Zeitung unter Verwendung der personenbezogenen Daten des Opfers als »Besteller« beauftragt wird. Unter Z 4 würde die Vorgehensweise dann fallen, wenn durch das Schalten eines (entgeltlichen oder unentgeltlichen) Inserats Dritte veranlasst werden sollen, mit dem Opfer Kontakt aufzunehmen.[2681]

Unter einer »Bestellung« kann der Ausdruck des Willens zum Vertragsschluss (iS einer Anbahnung eines Vertragsabschlusses) verstanden werden.[2682] Ob bei einer »invitatio ad offerendum«[2683] das Kaufangebot angenommen wird oder ob bereits die Bestellung selbst zum Abschluss des Vertrags führt, weil sich der Verkäufer bzw Anbieter durch sein Anbot schon gebunden hat, spielt keine Rolle.[2684]

Die Bestellung verlangt mE allerdings, dass sie dem Verkäufer zugänglich wird. Hat der Täter folglich Waren oder Dienstleistungen iSd § 107a Abs 2 Z 3 bestellt, ist damit eine von der Tathandlung abtrennbare Wirkung in der Außenwelt eingetreten (Erfolgsdelikt), nämlich das Eingehen einer außenwirksamen Willensbekundung, einen Vertrag (vgl zB Kauf- oder Dienstleistungsvertrag) mit dem entsprechenden Vertragspartner (Verkäufer bzw Anbieter) abschließen zu wollen. Ob ein Vertrag aufgrund dieser Bestellung in weiterer Folge tatsächlich zustande kommt, spielt keine Rolle. Auch die Auslieferung der Waren oder die Zustellung der Rechnung sind nicht (mehr) »erfolgsbegründend«, sondern nur mehr die Folge der Bestellung.[2685]

Darüber hinaus ist die Form der Bestellung unbeachtlich. So können Bestellungen persönlich, telefonisch, postalisch, per E-Mail, via Webshop im Internet oder auch durch andere beauftragte Personen durchgeführt werden.[2686]

2679 Vgl ErlRV 1316 BlgNR XXII. GP, 5.
2680 Siehe *Bertel/Schwaighofer,* BT I[12] § 107a Rz 3; aA offenbar noch *Schwaighofer* in WK[2] § 107a Rz 23.
2681 Siehe auch *Wach* in SbgK § 107a Rz 40.
2682 Siehe dazu ErlRV 1998 BlgNR XX. GP, 29.
2683 Was im Versandhandel zumindest in Ö der Regelfall ist (vgl ErlRV 1998 BlgNR XX. GP, 29).
2684 Vgl *Kathrein* in KBB[3] § 5i KSchG Rz 1 (Stand Juli 2010).
2685 In diesem Sinn aber mit anderer Begründung *Wach* in SbgK § 107a Rz 38.
2686 Vgl einige Beispiele bei *Bertel/Schwaighofer,* BT I[12] § 107a Rz 23.

a. Personenbezogene Daten

Hinsichtlich des Begriffs »personenbezogene Daten« gibt es insofern Unklarheiten, als dieser im StGB nicht näher definiert wird. Folgt man dem Weg der Interpretation der »Daten« über die Legaldefinition des § 74 Abs 2, so zeigt sich ein wortlautimmanenter Widerspruch. § 74 Abs 2 bestimmt nämlich, dass iSd StGB Daten »personenbezogen oder nicht personenbezogen« sein können und sogar Programme darstellen können. Vielmehr aber sind mit der Formulierung in § 107a Abs 2 Z 3 und 4 ausschließlich »personenbezogene Daten« iSd Datenschutzgesetzes 2000 gemeint, worauf aber im normspezifischen Zusammenhang nicht hingewiesen wird.[2687]

§ 4 Z 1 DSG 2000 definiert in seinem Anwendungsbereich »Daten« dahingehend, dass es sich dabei um Angaben über Betroffene handelt, deren Identität bestimmt bzw bestimmbar ist (§ 4 Z 1 erster HS; sog »direkt personenbezogene Daten«) und vermerkt dabei in einem Klammerausdruck, den Terminus »personenbezogene Daten«. Darunter fallen aber auch »indirekt personenbezogene Daten« iSd § 4 Z 1 zweiten HS, die vom konkreten Verwender nur mit rechtlich unzulässigen Mitteln auf eine Person zurückgeführt werden können.[2688] Dies wäre zB dann der Fall, wenn Daten einer Person nicht unter ihrem Namen, sondern unter einer Nummer gespeichert werden, die nur derjenige auf den Namen zurückführen kann, der rechtmäßig im Besitz des Namens und der dazugehörenden Nummer ist. Zu beachten ist dabei, dass jede Form der rechtlichen Unzulässigkeit zum bloß indirekten Personenbezug führt. Ein bestimmter Schwierigkeitsgrad für den rechtswidrigen Zugang wird nicht verlangt.[2689] Die Einschränkung der Entschlüsselung indirekt personenbezogener Daten auf legale Mittel fand auch in die Erl[2690] Eingang, wobei auch in ErwG 26 Datenschutz-RL von einem vernünftigen Mittel, also einem, das weder seiner Art, noch seinem Aufwand nach vollkommen ungewöhnlich ist, gesprochen wird.[2691]

2687 Siehe dazu bereits S 138 ff.

2688 Siehe zu dieser Datenkategorie krit *Bergauer* in Jahnel, Jahrbuch 2011, 55 (55 ff); *Drobesch/Grosinger,* Datenschutzgesetz, 117 bzw 140; auch *Dohr/Pollirer/Weiss/Knyrim,* DSG² § 4 Anm 2.

2689 Vgl *Löschnigg,* Datenermittlung, 143; *Löschnigg,* DRdA 2006, 459; vgl *Jahnel* in Jahnel, Jahrbuch 2008, 27 (36); *Jahnel,* Handbuch, Rz 3/78.

2690 Vgl ErlRV zum DSG 2000, 1613 BlgNR XX. GP, 37.

2691 Eine ausf Auseinandersetzung mit dem österr Kuriosum der »indirekt personenbezogenen Daten« findet sich bei *Bergauer* in Jahnel, Jahrbuch 2011, 55 (55 ff).

Jede Art personenbezogener Daten, daher auch – entgegen einiger strafrechtlicher Lehrmeinungen[2692] – Bildaufnahmen von Personen, sind von der Begrifflichkeit erfasst, sofern ein Personenbezug mit verhältnismäßigem Aufwand herstellbar ist.[2693] Die DSK hatte ebenfalls bereits mehrfach festgestellt, dass Bilddaten (bestimmbare) personenbezogene Daten iSd § 4 Z 1 DSG 2000 sind.[2694] Darüber hinaus könnte man bei Bildaufnahmen sogar von sensiblen Daten ausgehen, die gem § 4 Z 2 DSG 2000 als besonders schutzwürdig angesehen werden.[2695] Es handelt sich dabei um Daten natürlicher Personen hins ihrer rassischen und ethnischen Herkunft, politischen Meinung, Gewerkschaftszugehörigkeit, religiösen oder philosophischen Überzeugung, Gesundheit oder ihr Sexualleben. Der EuGH stellt dazu im Fall *Lindqvist*[2696] fest, dass der in Art 8 Abs 1 Datenschutz-RL verwendete Begriff »Daten über Gesundheit« weit auszulegen ist, sodass er sich auf alle Informationen bezieht, die die Gesundheit einer Person unter allen – körperlichen wie psy-

2692 Vgl etwa *Schwaighofer* in WK² § 107a Rz 26; auch *Beclin* in BMJ, 34. Ottensteiner Fortbildungsseminar, 103 (110); *Kienapfel/Schroll,* StudB BT I³ § 107a Rz 8; aber in der Rsp auch (noch) OGH 14.11.2000, 14 Os 128/00; aA OLG Wien 14.11.2013, 23 Bs 351/13 f = MR 2014, 246 *(Bauer)* = jusIT 2015/3, 9 *(Bergauer);* weiters LG Salzburg 29.04.2011, 49 Bl 17/11v = jusIT 2011/89, 185 *(Thiele*).

2693 Vgl auch ErwG 16 Datenschutz-RL; weiters OLG Wien 14.11.2013, 23 Bs 351/13 f = MR 2014, 246 *(Bauer)* = jusIT 2015/3, 9 *(Bergauer);* LG Salzburg 29.04.2011, 49 Bl 17/11v = jusIT 2011/89, 185 *(Thiele);* insb *Thiele,* Unbefugte Bildaufnahme und ihre Verbreitung im Internet – Braucht Österreich einen eigenen Paparazzi-Paragrafen?, RZ 2007, 2 mwN; weiters *Bergauer,* jusIT 2015/3, 9; auch *Bergauer/Schmölzer* in Jahnel/Mader/Staudegger, IT-Recht³, 635 (715); *Jahnel* in Jahnel, Jahrbuch 2008, 27 (45); *Dohr/Pollirer/Weiss/Knyrim,* DSG² § 4 Anm 2; ebenfalls *Wach* in SbgK § 107a Rz 48; *Birklbauer/Hilf/Tipold,* Strafrecht BT I² § 107a Rz 12; aA offensichtlich *Schwaighofer* in WK² § 107a Rz 26; auch OGH 14.11.2000, 14 Os 128/00; ebenso *Beclin* in BMJ, 34. Ottensteiner Fortbildungsseminar, 103 (110).

2694 Vgl DSK 12.05.2010, K202.094/0004-DSK/2010; DSK 21.01.2009, K121.425/0003-DSK/2009.

2695 Siehe etwa *Thiele,* RZ 2007, 2; *Bergauer/Schmölzer* in Jahnel/Mader/Staudegger, IT-Recht³, 635 (715); *Kunnert,* Big Brother in U-Bahn, Bus und Bim. Videoaufzeichnung in öffentlichen Verkehrsmitteln aus datenschutzrechtlicher Sicht, juridikum 2006, 42; wohl auch DSK 21.06.2005, K507.515–021/0004-DVR/2005; aA wohl *Schmoller,* Private Videoüberwachung – ein Beweismittel im Strafprozess?, in Bammer/Holzinger/Vogl/Wenda (Hrsg), Rechtsschutz gestern – heute – morgen, FS Machacek/Matscher (2008) 1065 (1069 f). Auch wäre es denkbar, dass sich aus Bildaufnahmen »strafrechtlich relevante Daten« iSd § 8 Abs 4 DSG 2000 ergeben können, welchen nach dem DSG 2000 eine mittlere Schutzwürdigkeit, angesiedelt zwischen nicht-sensiblen und sensiblen Daten, zugesprochen werden, siehe dazu auch DSK 21.06.2005, K507.515–021/0004-DVR/2005.

2696 EuGH 06.11.2003, C-101/01 (Lindqvist) = MR 2004, 83 *(Kronegger)* = ÖJZ 2004/45, 741 *(Hörlsberger*).

chischen – Aspekten betreffen. Im Fall von Bildaufnahmen einer Person lassen sich jedenfalls Gesundheitsdaten eruieren. So weisen etwa eine Brille auf Sehschwäche hin, Zahnregulierungen auf Zahn- bzw Kieferfehlstellungen, Hautausschläge auf etwaige akute Erkrankungen, Narben oder Wunden auf (offene) Verletzungen, Gipsverbände auf Knochenbrüche, Rollstuhl, Krücken, Rollator, Gehstock auf Gehbehinderungen und das Fehlen von Gliedmaßen auf generelle körperliche Behinderungen hin. Solche Daten sind nicht schon deshalb weniger schützenswert, weil sie faktisch in der Öffentlichkeit vom Betroffenen nicht verborgen gehalten werden können. Dies ändert nichts an der Tatsache, dass es sich bei Gesundheitsdaten um sensible Daten handelt.[2697] Und selbst wenn keine offensichtliche gesundheitliche Beeinträchtigung vorliegt, könnte auf einen »gesunden« Menschen geschlossen werden, was ebenfalls »Gesundheitsdaten« impliziert.[2698] Ähnliche Aussagen lassen sich auch bezüglich der Hautfarbe einer Person treffen, die jedenfalls Rückschlüsse auf die »rassische oder ethnische Herkunft« zulässt. Anders als eine Brille oder ein Schmuck mit religiösen Motiven, lässt sich die Hautfarbe eines Menschen auch nicht einfach »ablegen«.

Wesentlich ist, dass die Einordnung eines personenbezogenen Datums nach seiner datenschutzrechtlichen Schutzwürdigkeit nicht anhand des konkreten Verwendungszusammenhangs (datenschutzrechtlicher Zweck) einer Datenverwendung zu bestimmen ist, sondern nach rein objektiven Gesichtspunkten, nämlich, ob sich aus diesem Datum zB Aussagen über die Gesundheit einer Person ableiten lassen oder nicht.[2699] Daraus folgt, dass es nicht auf den tatsächlichen Informationsgehalt im »Klartext« ankommt, sondern es ausreichend ist, wenn die dadurch vermittelte Information auf besonders schutzwürdige Kategorien iSd § 4 Z 2 DSG 2000 schließen lässt.[2700]

2697 Siehe dazu überzeugend *Jahnel,* Handbuch, Rz 3/95.

2698 Siehe auch *Bergauer,* jusIT 2015/3, 9; weiters *Bergauer/Schmölzer* in Jahnel/Mader/Staudegger, IT-Recht[3], 635 (715).

2699 Vgl instruktiv *Jahnel* in Jahnel, Jahrbuch 2008, 27 (41 und 45); *Jahnel,* Handbuch, Rz 3/90; aA *Kotschy,* Datenschutzrechtliche Rechtsfragen der Videoüberwachung, in Bammer/Holzinger/Vogl/Wenda (Hrsg), Rechtsschutz gestern – heute – morgen, FS Machacek/Matscher (2008) 257 (262); weiters *König,* »Videoüberwachung und Datenschutz – ein Kräftemessen«, in Jahnel/Siegwart/Fercher (Hrsg), Aktuelle Fragen des Datenschutzrechts (2007) 109 (124).

2700 Siehe *Dammann/Simitis,* EU-Datenschutzrichtlinie. Kommentar (1997) Art 8 Anm 2 und 7; *Jahnel,* Handbuch, Rz 3/90.

b. Datenverwendung

Das Verwenden von personenbezogenen Daten ist – mangels eines ausdrücklichen Verweises auf das DSG 2000 und unter Berücksichtigung der Tatsache, dass nicht einmal in der einzigen datenschutzrechtlichen Strafbestimmung (§ 51 DSG 2000) die Terminologie des DSG 2000 Verwendung findet[2701], nach einem allgemeinen Verständnis iSd »Gebrauchens« zu verstehen. Im hier interessierenden Zusammenhang ließe sich allerdings genauso gut auf das spezifische datenschutzrechtliche Verständnis des »Verwendens von Daten« iSd § 4 Z 8 DSG 2000 zurückzugreifen. Dementsprechend wird jede Art der Handhabung von Daten darunter verstanden, also sowohl das Verarbeiten (einschließlich dem Ermitteln) als auch das Übermitteln von Daten.

8. Die Veranlassung zur Kontaktaufnahme (§ 107a Abs 2 Z 4)

Die Begehungsweise des § 107a Abs 2 Z 4 verlangt, dass der Täter unter der Verwendung personenbezogener Daten des Opfers, Dritte dazu veranlasst, mit dem Opfer Kontakt aufzunehmen. Darunter fallen daher insb Inserate, Kontaktanzeigen, Flugblätter, E-Mails, Aufrufe via Blogs, E-Foren oder Websites[2702], in denen Dritte aufgefordert werden, das Opfer zu kontaktieren.[2703] Zum Beispiel gibt der Täter eine Kontaktanzeige mit dem Angebot sexueller Dienstleistungen auf und führt in dieser die Telefonnummer des Opfers an.[2704] Welche personenbezogenen Daten des Opfers verwendet werden, ist dabei irrelevant. Zu denken wäre an Name, Anschrift, Telefonnummer, E-Mail-Adresse, Skype-Namen, Facebook-Profilname usw. Auch Kontaktinformationen des Opfers wie die Telefonnummer oder die Anschrift von Orten, an denen sich das Opfer nicht ständig aufhält (zB Arbeitsplatz, Ausbildungsort, Krankenanstalten bei stationärer Aufnahme, Urlaubsort) sind einschlägig.

Das Schalten eines einzigen Inserats soll nach den GMat für das Vorliegen dieser Begehungsweise nicht ausreichend sein, weil in einem

2701 Siehe dazu die Tathandlung des »Selbst-Benützens« in § 51 DSG 2000.

2702 Zur Veröffentlichung eines Inserats auf einer Website im Internet in Begehung eines »Erfolgs-Dauerdelikts« siehe zu § 107a Abs 2 Z 2 (S 554 ff).

2703 Vgl viele Beispiele bei *Wach* in SbgK § 107a Rz 44 ff; *Schwaighofer* in WK² § 107a Rz 25.

2704 Siehe ErlRV 1316 BlgNR XXII. GP, 5.

solchen Fall das Ende der Belästigungen für das Opfer absehbar sei.[2705] Erst durch das Hinzutreten eines Elements der zeitlichen Ungewissheit (arg »ein über eine längere Zeit hindurch fortgesetztes Verhalten des Täters«) werde eine Gleichwertigkeit mit den sonstigen Verhaltensweisen des § 107a Abs 2 hergestellt. Hierbei wird aber übersehen, dass die Veröffentlichung eines solchen »einzigen« Inserats im Internet, zB über eine Facebook-Pinnwand, private Website oder E-Forum und insb auch über Archive digitaler Tageszeitungen, durch die Persistenz dieser digitalen Veröffentlichungsformen mit keiner Absehbarkeit des Endes der Belästigung für das Opfer verbunden ist.

Beclin und *Wach*[2706] stellen für die Beurteilung eines einzigen Inserats auf das verwendete Publikationsmedium ab und vergleichen dabei die Schaltung eines Inserats in einer Zeitung mit jener via Internet.[2707] Dabei nehmen sie im Fall einer Interneteinschaltung bei bestehender Einwirkungsmöglichkeit des Täters – im Ergebnis ebenfalls wie oben bereits ausgeführt – eine »fortgesetzte« Begehung durch Unterlassen an. *Seling*[2708] und *Heissenberger*[2709] sehen aber darin lediglich eine Tathandlung, die es mangels tatbestandsgemäßer »Fortsetzung« (noch) nicht vermag, den Tatbestand (vollständig)[2710] zu erfüllen.

Meines Erachtens ist mit *Beclin* und *Wach* zuerst eine Differenzierung der Medien hins ihrer tatsächlichen Einwirkungsmöglichkeiten auf das Inserat durch den Täter indiziert. Dabei ist vorauszuschicken, dass es auch Online-Publikationsorgane gibt, bei denen der Täter ebenso wie bei analogen Printmedien (zB Tageszeitungen) keinen Einfluss mehr auf das Inserat nach seiner Veröffentlichung nehmen kann (zB diverse Online-Zeitungen, moderierte Chats oder Gästebucheinträge auf fremden Websites). Sind allerdings solche Einwirkungsmöglichkeiten weiterhin in hinreichendem Maß[2711] gegeben (wie zB bei eigenen Websites, E-Foren oder sozialen Plattformen), muss in weiterer

2705 Vgl ErlRV 1316 BlgNR XXII. GP, 5.
2706 Vgl *Wach* in SbgK § 107a Rz 49.
2707 Vgl *Beclin* in BMJ, 34. Ottensteiner Fortbildungsseminar, 103 (116).
2708 Siehe *Seling,* Stalking 67, der meint, dass das Tatbestandsmerkmal »fortgesetzt« eine mehrfache Wiederholung der Tathandlung zwingend voraussetze und daher in diesem Fall nicht erfüllt sei.
2709 Siehe *Heissenberger,* AnwBl 2006, 634.
2710 *Heissenberger* kommt aber dabei ggf zu einer Versuchsstrafbarkeit.
2711 Das heißt, der Täter muss insb auf den Inhalt des Inserats einwirken können, oder das Inserat insgesamt zu sperren oder zu löschen in der Lage sein.

Folge geprüft werden, ob – einem »allgemeinen Ingerenzprinzip«[2712] entsprechend – ein durch aktives Tun geschaffener rechtswidriger Zustand durch anschließendes Unterlassen des Täters (unter den Voraussetzungen des § 2[2713]) den rechtskonformen Zustand wiederherzustellen, fortdauernd aufrechterhalten wird.[2714] Nur dadurch würde der Tatbestand ununterbrochen solange weiter verwirklicht werden, bis der Störvorgang tatsächlich sein Ende gefunden hat (materielle Beendigung).

Genau genommen liegen zwei Delikte vor: eines, das die Herbeiführung eines rechtswidrigen Zustands durch aktives Tun betrifft und ein weiteres, was die Unterlassung der Beseitigung dieses rechtswidrigen Zustands durch den Täter als Garant (hier: der Beseitigung des inkriminierten Kontaktaufrufs im Internet-Inserat) kraft Ingerenz anlangt. In diesem Fall geht grundsätzlich ein strafbarkeitsausschöpfendes Tun rechtstechnisch betrachtet dem Unterlassen vor.[2715]

Im vorliegenden Fall wird allerdings durch das anschließende Unterlassen des Täters, der noch Einfluss auf das Geschehen hat, die Veranlassung der Kontaktaufnahme mit dem Opfer im Internet ständig wiederholt, weshalb das Unrecht durch die Fortdauer der Aufrechterhaltung der Veröffentlichung anhält und darüber hinaus noch vergrößert wird. Das einmalige Tun (hier: Hochladen des Inserats) als Handlungselement stellt im konkreten Fall nicht die für das Rechtsgut gefährlichere Begehung dar, weil im Zeitpunkt der Veröffentlichung (= Zeitpunkt der formellen Vollendung) gar kein Dritter das Inserat liest bzw mangels Kenntnis des genauen Veröffentlichungszeitpunkts lesen kann. Vielmehr wirkt sich folglich das anschließende fortgesetzte Un-

---

2712 In dem Sinn, dass jedermann die nachteiligen Folgen abzuwenden hat, die aus seinem (rechtswidrig oder rechtmäßigem) Tun entspringen können (vgl *Fabrizy,* StGB[11] § 2 Rz 3a). Mit anderen Worten, die Schaffung einer Gefahrenquelle erzeugt eine Handlungspflicht.

2713 Insbesondere sind das 1.) das Vorliegen eines Erfolgsdelikts; 2.) eine Garantenstellung; 3.) die Gleichwertigkeit des Unterlassens der Erfolgsabwendung gegenüber der Verwirklichung durch aktives Tun.

2714 Vgl zB *Schmoller* in SbgK § 99 Rz 15 mwN; *Leukauf/Steininger,* StGB[3] § 99 Rz 10; *Triffterer* AT[2], 65.

2715 Siehe zum »Primat des Tuns« allgemein *Fabrizy,* StGB[11] § 2 Rz 13; *Kienapfel/Höpfel/Kert,* AT[14], Z 28 Rz 25 ff. Im Urteil dürfte nicht über beide Deliktsbegehungen nebeneinander abgesprochen werden. Das unechte Unterlassungsdelikt wäre lediglich eine »mitbestrafte Nachtat«. Allerdings wäre bei der Strafzumessung die Fortsetzung über eine längere Zeit als etwaiger Erschwerungsgrund iSd § 33 Abs 1 Z 1 letzter Fall zu berücksichtigen.

terlassen (hier: Verweigerung des Löschens oder Sperren des Inserats) durch die »sukzessive Öffentlichkeit« und den Multiplikationseffekt der Verbreitung und Zugänglichkeit auf das Rechtsgut aus. Die Stalking-Bestimmung des § 107a ist insgesamt betrachtet ein Paradebeispiel für ein Delikt mit pauschalierender Handlungsbeschreibung (arg »beharrlich verfolgt«), für dessen Verwirklichung ein Komplex mehrerer Einzelhandlungen implizite Voraussetzung ist.[2716] Auch das einheitliche Vorgehen des Täters im Inserat-Beispiel ist idS als »tatbestandliche Handlungseinheit«[2717] zu betrachten (das einmalige Tun und die anschließenden ständigen Unterlassungen bilden gemeinsam »ein Tun«), weshalb die Tathandlung des § 107a Abs 2 Z 4 insgesamt nur einmal verwirklicht wird. Solange allerdings der rechtswidrige Zustand durch Tun oder anschließendes Unterlassen des Täters aufrechterhalten wird, ist von einer »fortgesetzten« Begehung (iS eines Dauerdelikts) auszugehen. Reicht nun auch noch die Intensität dieser Handlung aus, um die konkrete gestalkte Person in ihrer Lebensführung unzumutbar zu beeinträchtigen (vgl § 107a Abs 2), kann die Schaltung eines einzelnen Inserats über Internetdienste – Vorsatz und hinreichende Einwirkungsmöglichkeit des Täters auf das Inserat vorausgesetzt – den Tatbestand des § 107a Abs 1 vollständig verwirklichen. Es kann daher im spezifischen Zusammenhang des § 107a der Fall eintreten, dass zwar das einmalige aktive Tun iSd § 107a Abs 2 Z 4 durch das Schalten des Inserats noch nicht tatbestandlich iS einer beharrlichen Verfolgung ist, weil noch keine nahe Gefahr für das Rechtsgut vorliegt. Wohl aber kann das anschließende Unterlassen einer Löschung der Anzeige, das die Veröffentlichung derselben über einen langen Zeitraum und für viele Personen weiter aufrecht hält, das Gesamtgeschehen sukzessive zu einem rechtlich missbilligten Risiko bzw tatbestandlichen Unrecht gem § 107a Abs 1 werden lassen.

Zugegebenermaßen tritt bei dieser Auffassung wohl ein gravierendes deliktsspezifisches Problem auf. Die einzelnen Begehungsweisen des § 107a Abs 2 Z 1 bis 4 sind nicht notwendigerweise Handlungen, die per se sozial inadäquat und rechtswidrig sind. Wenn also durch die einmalige Schaltung eines Internet-Inserats eine Handlung iSd § 107a Abs 2 Z 4 gesetzt wird, bedeutet die Herbeiführung eines solchen Zustandes (noch) nicht, dass dieser auch rechtswidrig iSd § 107a Abs 1

2716 Siehe *Kienapfel/Höpfel/Kert,* AT[14], E 8 Rz 61.
2717 Vgl dazu generell etwa *Fuchs,* AT I[8], Rz 37/15.

bzw anderer Rechtsnormen ist. Führt daher jemand einen (tatbestandlichen) Erfolg iSd § 107a Abs 2 Z 4 herbei, wobei dieser für sich allein genommen noch gar nicht das Kriterium der beharrlichen Verfolgung iSd § 107a Abs 2 zu erfüllen vermag, indiziert dieser Erfolg noch keinen »rechtswidrigen« Zustand. Wird dieser Zustand von dieser Person durch anschließendes Unterlassen aufrechterhalten, ergeben sich folglich Schwierigkeiten, was die Begründung einer diese Person insb treffende Pflichtenstellung (iS einer Garantenstellung) anlangt. Ebenso stellt sich die Frage, ob dadurch überhaupt tatbestandliches »Unrecht« – iS eines Dauerdelikts – fortgesetzt werden kann. Selbst wenn grundsätzlich auch rechtmäßiges Vorverhalten eine Garantenstellung nach dem Ingerenzprinzip begründen kann[2718], wäre es geradezu absurd für jede Person, die die räumliche Nähe einer anderen Person aufsucht und dadurch ein (ex ante) Risiko bezüglich eines etwaigen gefährlichen Kausalprozesses einer *möglichen* (anschließenden) beharrlichen Verfolgung dieser Person schafft – eine Garantenstellung mit der Pflicht zu begründen, die räumliche Nähe zu dieser Person wieder aufzulösen. Eine solche Garantenpflicht wäre auch schon deshalb abwegig, weil gerade mehrere Einzelhandlungen (wie das mehrfache Aufsuchen des Aufenthaltsorts der Person samt wiederholtem Verlassen desselben zur pflichtgemäßen Erfolgsabwendung) die konkrete Gefahr für das Opfer erst begründen. Verlässt der Stalker nach erfolgtem Aufsuchen der räumlichen Nähe diesen Ort wieder, hätte er seiner Garantenpflicht entsprochen, und dennoch wäre ggf der konkrete Gefährdungserfolg iSd § 107a eingetreten.

Was die Aufrechterhaltung des tatbestandlichen »Unrechts« betrifft, das zum Zeitpunkt des aktiven Tuns ggf noch keines ist[2719], ist festzuhalten, dass – sofern man wie *Kienapfel/Höpfel/Kert* für die Begründung einer Garantenstellung aus gefahrenbegründendem Vorverhalten nur ein

---

2718 Vgl *Fabrizy,* StGB[11] § 2 Rz 3a; für Überwachungsgaranten allgemein *Fuchs,* AT I[8], Rz 37/60 f; weiters zustimmend bei Überwachungsgaranten, aber ablehnend bei »gefahrenbegründetem Vorverhalten« *Kienapfel/Höpfel/Kert,* AT[14], Z 30 Rz 22a bzw 21.

2719 Man stelle sich vor 10 Inseratschaltungen würden in einem bestimmten Fall eine »nahe Gefahr« für die Verwirklichung des § 107a Abs 1 schaffen bzw einen konkreten Gefährdungserfolg sehr wahrscheinlich machen, der Täter aber veröffentlicht gerade einmal die erste Anzeige. Eine Versuchsstrafbarkeit käme allerdings in Betracht, wobei eine solche bei einem prinzipiell sozial adäquaten objektiven Tatbestand ebenfalls problematisch ist und zu einer sehr weiten Vorverlagerung der Strafbarkeit führen würde.

rechtswidriges Vorverhalten akzeptiert[2720] – eine Garantenstellung kraft Ingerenz überhaupt ausscheidet. Dieses Ergebnis wird in erster Linie dadurch herbeigeführt, dass der Gesetzgeber in § 107a Abs 2 Z 4 Handlungen definiert hat, die per se noch kein tatbestandliches Unrecht darstellen müssen. Mangels Garantenstellung kann diesfalls keine Strafhaftung durch Unterlassen iSd § 2 entstehen, weshalb das fortdauernde Unterlassen des Täters aus strafrechtlicher Sicht belanglos ist.

Als weitgehend unproblematisch ist allerdings der Sachverhalt zu beurteilen, wenn der Täter eine Anzeige mit inkriminiertem Inhalt schaltet, die in einer Online-Zeitung im Internet veröffentlicht oder mittels eines uno actu-versendeten (Massen-)E-Mails Dritten zugänglich wird. In solchen Fällen liegt ein einmaliges aktives Tun vor. Der Täter kann hierbei aufgrund fehlender objektiver Einwirkungsmöglichkeit auf das Inserat den Tatbestand nicht mehr durch Unterlassen iSd § 2 (weiter-)verwirklichen. Er ist also rein faktisch nicht mehr imstande das gebotene Tun vorzunehmen, weshalb hier eine Strafbarkeit wegen Unterlassung per se entfällt.[2721]

Abschließend ist zu den Begehungsweisen nach § 107a Abs 2 Z 3 und 4 festzuhalten, dass diese mit § 51 DSG 2000 in echte Konkurrenz treten können. Da § 107a Abs 1 und § 51 DSG 2000 jeweils eine Freiheitsstrafe bis zu einem Jahr androhen, greift die Sperrwirkung der Subsidiaritätsklausel des § 51 DSG 2000 nicht, die zugunsten anderer Bestimmungen, welche mit strengerer Strafe bedroht sind, eingerichtet ist.

9. Subjektive Tatseite

Der Täter muss zumindest mit dolus eventualis bezüglich sämtlicher objektiver Tatbestandsmerkmale handeln. Dies schließt das konkrete Tatobjekt ein, die verhaltensgebundenen Tathandlungen nach § 107a Abs 2 Z 1 bis 4 samt deren wiederholten Begehungen, aber auch die Eignung, die Lebensführung des Opfers unzumutbar zu beeinträchtigen.

2720 Siehe *Kienapfel/Höpfel/Kert,* AT[14], Z 30 Rz 21.
2721 Siehe *Fuchs,* AT I[8], Rz 37/23.

10. Sonstiges

Mit dem BGBl I 93/2007 wurde § 107a Abs 3 aufgehoben[2722], weshalb § 107a nunmehr insgesamt ein (reines) Offizialdelikt ist, welches unabhängig von jeglicher Mitwirkung des Opfers von Amts wegen zu verfolgen ist.

§ 107a ist zwar mit Freiheitsstrafe bis zu einem Jahr bedroht, fällt aber gem § 31 Abs 4 Z 2 StPO iVm § 30 Abs 1 Z 3 StPO in die Eigenzuständigkeit des Einzelrichters am Landesgericht.

2722 Zuvor handelte es sich um ein partielles Antragsdelikt, da ausschließlich in den Fällen des § 107a Abs 2 Z 2 der Täter nur auf Antrag der beharrlich verfolgten Person zu verfolgen war (vgl BGBl I 56/2006; ErlRV 1316 BlgNR XXII. GP, 7).

3 Schlussbetrachtungen

I. Zusammenfassung der wesentlichsten Erkenntnisse

A. Thesen aus der Einleitung

1. Zum Begriff der Computerkriminalität

Der Begriff »Computerkriminalität« erfasst sinnvollerweise nicht alle strafwürdigen Verhaltensweisen, bei denen ein Computer als Tatmittel oder Tatobjekt in Erscheinung tritt, sondern ausschließlich solche, bei denen der Täter darüber hinaus IKT-spezifisch handelt. Als Korrelat zur Computerkriminalität hat sich der Begriff Computerstrafrecht eingebürgert, welcher aber nicht weiter definiert wird. Der hier vertretene Definitionsansatz versteht das »Computerstrafrecht in einem weiten und einem engen Sinn«.

2. Zum Begriff des Computerstrafrechts

Unter dem Computerstrafrecht im weiten Sinn wird die Gesamtheit der Rechtsvorschriften des Kriminalstrafrechts verstanden, die auf IKT-Sachverhalte angewendet werden. Deshalb fallen unter das Computerstrafrecht iwS neben speziell geschaffenen Computerdelikten auch klassische Strafbestimmungen, sofern das Substrat der Rechtsanwendung auf Sachverhalten mit Bezug zur Informationstechnologie beruht.

Das Computerstrafrecht im engen Sinn erfasst die spezifischen Delikte des Kern- und Nebenstrafrechts, die explizit dafür geschaffen wurden, computer- bzw datengestützte Begehungsweisen oder Tatmittel (computer- oder datengestützte Ausrichtung) und informationstechnische Angriffe auf IKT-Systeme bzw Daten als Tatobjekte (computer- bzw datenorientierte Ausrichtung) zu erfassen (sog »Computerdelikte«).

Computerdelikte können wiederum in zwei Kategorien geteilt werden: Solche, die strafbare Handlungen erfassen, welche ausschließlich durch IKT-Begehungsformen verwirklicht werden können bzw in ihrer grundsätzlichen Ausrichtung im Wesentlichen auf IKT-Begehungs-

weisen fokussieren[2723] (»echte Computerdelikte«) und solche, deren Tatbestände technikneutral sind, aber zumindest auch explizit Begehungsweisen enthalten, die wiederum IKT-bezogen sind (»unechte Computerdelikte«).

Für (echte) Computerdelikte wäre einerseits aufgrund ihrer IKT-spezifischen Besonderheiten und andererseits wegen der Tatsache, dass viele von ihnen durch ihre Strafdrohung in die sachliche Zuständigkeit des Bezirksgerichts fallen, wo ein Bezirksanwalt die Anklageseite vertritt, eine Sonderzuständigkeit beim Einzelrichter des Landesgerichts wünschenswert.

3. Zum Datenbegriff des Strafrechts

Der Legalbegriff »Daten« des Kernstrafrechts erweist sich als problematisch und sollte überarbeitet werden. Dazu wird folgender Formulierungsvorschlag unterbreitet: »Im Sinne dieses Bundesgesetzes sind Daten a) personenbezogene und nicht personenbezogene Informationen sowie b) deren computertechnische Darstellung (Computerdaten) einschließlich unmittelbar ausführbarer Computerprogramme.«

B. Thesen des Hauptteils

1. Zum Widerrechtlichen Zugriff auf ein Computersystem (§ 118a)

§ 118a Abs 1 sollte in Anbetracht der zunehmenden Virtualisierungskonzepte – wie Cloud Computing, Online-Speicher usw – allein auf die Verfügungsberechtigung über die Daten abstellen und nicht auch bezüglich des Computersystems, oder eines Teils davon.

Ein Computersystem iSd § 74 Abs 1 Z 8 kann über Eigentums- und Zuständigkeitsbereiche hinweg bestehen, was eine Abgrenzung und Feststellung in der Strafrechtspraxis erschwert. Das Tatobjekt Computersystem und seine Teilkomponenten müssen daher in einem kon-

2723 Als Beispiel dafür sei der Tatbestand des § 126a genannt, der etwa durch seine Handlungsalternative der Datenunterdrückung nicht ausschließlich auf eine IKT-Begehung abstellt. Man denke an die schlichte Wegnahme eines fremden Datenträgers, was auch die Unterdrückung seines Datenbestands impliziert.

kreten Sachverhalt stets dynamisch beurteilt werden, was zu einer einzelfallbezogenen »Skalierung des Tatobjekts« führt. Diese Beurteilung ist in weiterer Folge zur Klärung der Frage notwendig, ob eine tatbestandsgemäße spezifische Sicherheitsvorrichtung im gegenständlichen Computersystem überhaupt angebracht war.

Was das Überwinden dieser Vorkehrung anlangt, so erfordert eine solche während der Ausführungshandlung die »Konfrontation« des Täters mit derselben, zB durch Ausarbeitung eines Überwindungsplans und deren anschließende direkte Bezwingung. Bezüglich des Überwindens der Sicherheitsvorkehrung sind, auch was die kriminelle Energie des Täters betrifft, höhere Anforderungen zu stellen als bei einem bloßen Umgehen. Eröffnet sich daher eine zusätzliche Möglichkeit für einen Zugriff auf das System, ohne auf ein Hindernis zu stoßen, so liegt kein tatbestandliches Überwinden vor.

Im Zusammenhang mit § 118a Abs 1 wäre es treffender, den Wortlaut des Tatbestands an die Deliktsbezeichnung anzupassen und auf den »Zugriff auf« ein Computersystem abzustellen.

Der erste Teil des umfangreichen erweiterten Vorsatzes, die Spionageabsicht, verlangt, dass der Täter zum Tatzeitpunkt in der Absicht handelt, sich oder einem anderen Unbefugten Kenntnis von in »einem« Computersystem gespeicherten und nicht für ihn bestimmten Daten zu verschaffen. Daraus wird ersichtlich, dass sich die subjektive Zielvorstellung des Täters dem Wortlaut nach nicht ausschließlich auf die Daten des Systems richten muss, auf das sich der Täter auf der äußeren Tatseite widerrechtlich Zugriff verschafft hat. Sinnvollerweise wird man wohl die überschießenden Innentendenzen an den objektiven Tatbestand insoweit anschließen müssen, als die Absicht verfolgt werden muss, sich von den Daten Kenntnis zu verschaffen, die sich auch auf dem Computersystem befinden, zu dem sich der Täter (nach der Unrechtsbeschreibung des objektiven Tatbestands) Zugang verschafft hat. Der subjektive Tatbestand ist folglich teleologisch zu reduzieren.

Betrachtet man die Natur des § 118a Abs 1 unter Einbeziehung der kumulativ erforderlichen überschießenden Innentendenzen, so lassen sich insgesamt drei Erfolge erkennen. Die Erfüllung des objektiven Tatbestands führt tatbestandlich betrachtet zum Zwischenerfolg des Zugriffverschaffens auf ein fremdes Computersystem. Der anvisierte erste Enderfolg (die Datenspionageabsicht) und der beabsichtigte zweite Enderfolg (die Vermögensvorteilsverschaffung bzw Nachteilszufügung) müssen dagegen vom Täter nur angestrebt werden. Darü-

ber hinaus muss der Täter den zweiten Enderfolg dadurch erreichen wollen, dass er selbst eine weitere Handlung (iS einer Datenverwendung) vornehmen werde, was § 118a Abs 1 in Anbetracht der zweiten überschießenden Innentendenz zu einem verkümmert zweiaktigen Absichtsdelikt macht. Dies deshalb, weil auch diese Intention lediglich im Zeitpunkt der Handlungsvornahme vorliegen, nicht aber tatsächlich eintreten muss. Es handelt sich daher in § 118a Abs 1 insgesamt betrachtet um ein »verkümmert mehraktiges Delikt mit einem Taterfolg und spezifischen kupierten Enderfolgen«.

Unklar ist, warum der Gesetzgeber in einem Delikt, das das Rechtsgut »Privatsphäre« schützt, überhaupt (auch) eine Gewinnabsicht vorsieht. Die hohen Vorsatzanforderungen sind überzogen und führen zu einer gravierenden Minderanwendbarkeit der Bestimmung in der Strafrechtspraxis.

Eine Aufgliederung des Delikts in mehrere Deliktsfälle oder auch Qualifikationen mit entsprechenden differenzierten Vorsatzanforderungen – dem Schutzniveau der vom Täter anvisierten Daten entsprechend – wäre wünschenswert.

2. Zur Datenverwendung in Gewinn- oder Schädigungsabsicht (§ 51 DSG 2000)

Die überschießenden Innentendenzen beschreiben § 51 DSG 2000 als »kumulatives Mischdelikt über den erweiterten Vorsatz«. Durch die Zusammenführung verschiedener alternativ zu erfüllender subjektiver Unrechtsmerkmale besitzt die nebenstrafrechtliche Strafbestimmung des DSG 2000 Relevanz sowohl für vermögensrechtliche Bereicherungen (1. DF) als auch für bloße Schädigungen des Geheimhaltungsrechts (2. DF).

Bezieht man nämlich die Inhalte der überschießenden Innentendenzen als fiktive Erfolge in die Betrachtung mit ein, so führt die Tathandlung des »Selbst-Benützens« iVm der subjektiven Alternative des Bereicherungsvorsatzes dazu, dass § 51 erster Fall erste subj Alt DSG 2000 ein kupiertes Erfolgsdelikt (= Absichtsdelikt iwS) darstellt.

Dem objektiven Tatbestand fehlt generell eine sozial inadäquate Verhaltensbeschreibung. Daher fehlt eine hinreichende Abgrenzung zwischen strafbedürftigem und straffreiem Verhalten in der äußeren Beschreibung der Tat. Zum Zeitpunkt jeder Datenverwendung wird allerdings datenschutzrechtlich betrachtet bereits in das Grundrecht nach

§ 1 Abs 1 DSG 2000 eingegriffen. Dies betrifft jedoch nicht die (zulässige) Datenverwendung in Ausübung einer beruflichen Beschäftigung, da hier keine sozial inadäquate Handlung vorliegt, sofern sich diese innerhalb der Schranken des Datengeheimnisses nach § 15 DSG 2000 bewegt.

Richtigerweise handelt es sich bei § 51 DSG 2000 in der Variante als echtes Sonderdelikt um ein Sonderpflichtdelikt, da denjenigen, dem personenbezogene Daten Dritter beruflich überantwortet werden, eine besondere Rechtspflicht trifft, nämlich das Datengeheimnis (§ 15 DSG 2000) zu wahren. Unmittelbarer Täter im Sinne dieser Rechtspflicht kann nur derjenige sein, der das ihm aus beruflichen Gründen überantwortete Datengeheimnis als seine persönliche Sonderpflicht bricht, also der Qualifizierte selbst.

Zu kriminalpolitisch unbefriedigenden Ergebnissen gelangt man in den Fällen »aufgedrängter Information«, in denen dem »Täter« die schutzwürdigen Daten – außerhalb einer beruflichen Beschäftigung – »zugespielt« wurden, ohne dass sich dieser dabei diese Daten aktiv verschafft hat. Der eindeutige Wortlaut lässt keine Strafbarkeit des nunmehrigen Besitzers zu, was zu einer Perpetuierung von Unrecht führt, welche sich gerade in Anbetracht von ubiquitären (personenbezogenen ggf auch sensiblen) Daten im Rahmen des Geheimhaltungsgrundrechts nach § 1 Abs 1 DSG 2000 als äußerst sachwidrig und rechtspolitisch fragwürdig darstellt. Der Gesetzgeber könnte diese Lücke durch das Hinzufügen weiterer objektiver Kriterien bezüglich des Tatobjekts schließen, indem er neben dem Erfordernis, dass die Daten widerrechtlich verschafft worden sein müssen, auch eine »Auffanganforderung« normiert, wie zB »oder sonst unzulässiger Weise inne hat«.

Da der objektive (strafbarkeitsbegründende) Tatbestand kein sozial inadäquates Verhalten beschreibt und dadurch ein hohes Kriminalisierungspotenzial schon durch die äußere Tatbeschreibung indiziert ist, sollte man diese das Tatobjekt näher konkretisierenden Elemente iZm § 51 DSG 2000 als Allgemeindelikt als »objektive Bedingungen der Strafbarkeit« bewerten, die nicht vom Tatbildvorsatz umfasst sein müssen. Eine solche Interpretation bietet sich auch an, um Beweisschwierigkeiten im Bereich eines diesbezüglichen Tatbildvorsatzes, Kausalitätsproblemstellungen oder eine ggf doppelte Rechtswidrigkeitsprüfung zu vermeiden.

Die Vermischung von materienübergreifenden Begrifflichkeiten ist iZm einem speziellen Sachgesetz wie dem DSG 2000 abzulehnen. Die Rechtsanwendung wird dadurch unnötig erschwert.

Bei allen Tathandlungen des § 51 DSG 2000 beschreibt diese Bestimmung kumulative Mischdelikte. Eine Veröffentlichung von geheim zuhaltenden personenbezogenen Daten im Internet bzw für einen unbestimmten Empfängerkreis intensiviert die Rechtsgutbeeinträchtigung gegenüber dem bloßen Zugänglichmachen doch deutlich und stellt deshalb auch im hier interessierenden Zusammenhang einen verhältnismäßig größeren sozialen Störwert dar. Das Rechtsgut ist daher umso stärker beeinträchtigt, je mehr Personen das Tatobjekt zugänglich wird.

3. Zur Verletzung des Telekommunikationsgeheimnisses (§ 119)

§ 119a Abs 1 ist tatbestandlich betrachtet ein schlichtes Tätigkeitsdelikt, das unter Einbeziehung der überschießenden Innentendenz zu einem kupierten Erfolgsdelikt wird.

Das Abstellen auf eine spezifische, ausschließlich für illegale Zwecke bestimmte Vorrichtung führt zu einer massiven Strafbarkeitsbeschränkung, die kriminalpolitisch unerwünschte Ergebnisse hervorruft. Dies insb in Fällen, in denen der Täter sozial adäquate Standard-Programme bzw -komponenten von Betriebssystemsoftware als derartige Vorrichtungen benützt, die eben nicht explizit für tatbildliche Spionagehandlungen geschaffen oder adaptiert werden müssen.

Entgegen den Darstellungen im einschlägigen Schrifttum handelt es sich iZm § 119 Abs 1 bei der tatbestandlichen »Vorrichtung« um das Tatobjekt und beim »Inhalt der Nachricht« um das Bezugsobjekt des erweiterten Vorsatzes bzw des subjektiven Tatbestands. Die von der äußeren Tatseite geforderte Vorrichtung verkörpert weder das Rechtsgut, noch stellt sie das geschützte konkrete Objekt dar, weshalb sich das tatsächliche »Schutzobjekt« der Bestimmung (hier: Inhalt einer Nachricht und nicht auch bloß Nachricht) lediglich aus dem erweiterten Vorsatz ergibt.

Es spielt für eine Strafbarkeit nach § 119 keine Rolle, ob eine empfangsbereite, angebrachte Vorrichtung vom Täter benützt wird oder ob dieser eine andere Vorrichtung verwendet, die ohne physische Verbindung zum Zielsystem empfangsbereit ist. Es handelt sich dabei (mittlerweile) um eine vermeidbare Redundanz, die noch aus der historischen Zweiteilung der Tathandlung herrührt, in der das Anbringen oder Sonst-Empfangsbereitmachen (Abs 1) neben dem Benützen (Abs 2) der Vorrichtung selbstständig strafbar war. Ein tatbestandli-

ches Abstellen lediglich auf eine Vorrichtung, die empfangsbereit gemacht wurde, reicht zur Erfassung sämtlicher intendierten verpönten Handlungen aus.

Es gibt einen wesentlichen Unterschied zwischen »Nachricht« und »Inhalt einer Nachricht«, welcher sich anhand der Abgrenzung des einschlägigen kernstrafrechtlichen Verständnisses iZm den telekommunikationsrechtlichen Definitionen überzeugend veranschaulichen lässt.

Für § 119 und § 120 Abs 2a gilt, dass der Nachrichtenbegriff »autonom« zu verstehen ist und nicht unter Bezugnahme auf das TKG 2003 definiert werden darf. Obwohl gerade § 119 und zu einem Teil auch § 120 Abs 2a ausdrücklich auf den »Inhalt einer Nachricht« abstellen, muss in erster Linie der Begriff der »Nachricht« determiniert werden, da der Inhalt einer Nachricht auch das Schicksal der übergeordneten Nachricht teilt. Der »Inhalt einer Nachricht« wird dabei jedenfalls auf den zu vermittelnden Gedankeninhalt – der in dieser Arbeit als »Mitteilung« bezeichnet wird – beschränkt, folgt aber der Bewertung der in Übertragungszustand versetzten »Nachricht«.

Die Unterschiede des Nachrichtenbegriffs in §§ 119 und 120 Abs 2a lassen sich in drei Punkte zusammenfassen: 1.) Es werden auch private Nachrichtenübermittlungen geschützt; 2.) Es werden auch Übertragungen erfasst, die nicht gewerblich erfolgen; 3.) Grundsätzlich sind alle Formen der Nachrichtenübermittlung tatgegenständlich, und nicht nur jene, die in den Anwendungsbereich des TKG 2003 fallen.

In der Praxis könnten sich Probleme bei der »Inhaltserforschung« einer gedanklichen Mitteilung ergeben. Es wird daher vorgeschlagen in einem ersten Schritt die gegenständliche Übertragung in Anbetracht der gewohnten Sprache in syntaktischer und semantischer Hinsicht zu überprüfen. Dabei gilt es zu beachten, dass auch nur diese beiden Elemente in Form von Zeichen und Daten letztlich objektiv auf einem Übertragungsmedium feststellbar sind. Lässt sich aus dieser Betrachtung heraus aus Sicht der Allgemeinheit bereits erkennen, dass eine gedankliche Mitteilung vorliegt (zB E-Mail mit verständlichem Text), kann die Prüfung zu diesem Zeitpunkt beendet werden. Ergibt sich jedoch aus dieser Betrachtungsweise kein eindeutiges Ergebnis, weil etwa der Text eines E-Mails hins allgemein verständlicher Syntax oder Semantik nicht klar ist, muss in weiterer Folge die Intention des Senders ausgeforscht werden. Dazu muss auf die verwendete Syntax und die dazugehörige intendierte Semantik (iS einer Sondersprache, wie

zB der »Gaunersprache«) eingegangen werden, die eine Übertragung als bewusst vorgenommene Nachricht des Senders an den Empfänger offenlegt. Mit anderen Worten, es muss erkundet werden, was der Sender im konkreten Fall als seine Mitteilung bestimmt hat.

Es ist nicht hinreichend verständlich, warum der Gesetzgeber iZm dem Abfangen von elektromagnetischer Emission nicht weiterhin dem Regime des unterschiedlichen Schutzniveaus der anvisierten »Informationsqualität« treu bleibt. Dies insb hins den Tatbestandsanforderungen, welche die Unterscheidung zwischen Nachrichtenspionage (zB § 119) und Datenspionage (zB § 119a) betreffen. Es ist folglich unklar, warum gerade Inhaltsdaten, von denen sich ein Unbefugter im Wege der Rekonstruktion von aufgefangenen elektromagnetischen Wellen Kenntnis verschaffen will, nicht dem Regelungsmodell des § 119 entsprechend geschützt werden.

4. Zum Missbräuchlichen Abfangen von Daten (§ 119a)

§ 119a Abs 1 beschreibt in beiden Deliktsfällen ein schlichtes Tätigkeitsdelikt. Unter Einbeziehung der überschießenden Innentendenzen handelt es sich jedoch in beiden Fällen um ein »verkümmert zweiaktiges Delikt mit zwei spezifischen Enderfolgen«.

Was den zweiten Deliktsfall des § 119a Abs 1 anlangt, kommt man zum Ergebnis, dass dieser für das Auffangen der Abstrahlung elektromagnetischer Wellen während einer Kommunikation oder Datenübertragung gar nicht sinnvoll anwendbar sein kann. Der Tatbestand müsste daher auf das Auffangen von elektromagnetischer Abstrahlung »gespeicherter«, und nicht gerade im Transport befindlicher, Daten abzielen.

Zur Vermeidung von Wertungswidersprüchen und Auslegungsproblemen wäre der Gesetzgeber gut beraten, den zweiten Deliktsfall als ein eigenständiges Delikt zu konzipieren. Man könnte daher einen neuen Absatz bilden und dort durchaus für Daten und Nachrichten gleichermaßen das Auffangen der elektromagnetischen Emission mit dem Einleitungssatz »Wer außer in den Fällen der § 119 Abs 1 und § 119a Abs 1 […]« unter Strafe stellen.

Bei einer solchen Neufassung könnten mehrere Unklarheiten und Unangemessenheiten beseitigt werden: 1.) Rekonstruierbare Daten und Nachrichten könnten ihrem unterschiedlichen Schutzniveau entsprechend kriminalpolitisch tatsächlich angemessen Berücksichti-

gung finden. 2.) Die in § 119 Abs 1 und § 119a Abs 1 Fall 1 vorgesehene, und in § 119a Abs 1 Fall 2 nicht mehr tatbestandlich vorgesehene spezielle Vorrichtung könnte in nachvollziehbarer Weise für dieses neue Delikt entfallen und eine Überkriminalisierung durch weitere strafbarkeitseinschränkende Merkmale verhindert werden. 3.) Durch Neuformulierung sollte auch zum Ausdruck gebracht werden, dass elektromagnetische Emissionen selbst weder Daten im StGB-terminologischen Verständnis sind, noch eine geschützte Übertragungsform nach § 119 bzw § 119a Abs 1 Fall 1 darstellen.

5. Zu sonstigen Telekommunikationseingriffen (§ 120 Abs 2a)

§ 120 Abs 2a betrifft sowohl den bereits zu § 119 erörterten Begriff des »Inhalts einer Nachricht« in seiner überschießenden Innentendenz als auch den Begriff der »Nachricht« in seinem objektiven Tatbestand.

Aus seiner Überstellung aus dem TKG in das Kernstrafrecht und der damit verbundenen Preisgabe der speziellen Wertvorstellungen und Begrifflichkeiten dieses Sachgesetzes kann darauf geschlossen werden, dass nunmehr ebenfalls die autonome Begriffsbestimmung idZ für »Nachricht« und »Inhalt einer Nachricht« des 5. Abschnitts des StGB zu gelten hat.

Innerhalb der drei Begehungsweisen muss streng unterschieden werden, denn sie sind nicht rechtlich gleichwertig. Das Aufzeichnen der Nachricht ist von den Verbreitungshandlungen des Zugänglichmachens und Veröffentlichens streng zu unterscheiden. Letztere sollten nach Gewichtung und Einschätzung der »Multiplikationsgefahr« und »sukzessiven Zugänglichkeit« strenger bestraft werden.

Das tatbestandliche Erfordernis, wie es bei der Variante des Einem-anderen-Unbefugten-Zugänglichmachens verlangt wird, gibt es im Fall des Veröffentlichens nicht. Demnach muss es sich bei der Tathandlung des Veröffentlichens nicht um »Unbefugte« als Empfängerkreis handeln. Das ist aber nur schlüssig, solange man davon ausgeht, dass es sich beim Veröffentlichen um einen »unbestimmten« Personenkreis handelt. Stellt man allerdings – wie üblich – auf eine Mindestpublizität iSd § 69 ab, können unbillige und rechtspolitisch unerwünschte Ergebnisse hervortreten.

Es sollte aber zur Abgrenzung unterschiedlicher Verbreitungshandlungen durchaus am quantitativen Element festgehalten werden. Im deliktsspezifischen Zusammenhang müsste dann allerdings – neben

einer tatbestandlichen Ergänzung durch den Gesetzgeber – eine teleologische Reduktion dieser Tatbegehungsvariante in der Praxis in Erwägung gezogen werden.

Releviert man den »Inhalt einer Nachricht« als Schutzobjekt dieser Bestimmung, kommt man nicht an der Frage vorbei, warum nicht auch das Weiterleiten von Teilinhalten der Nachricht (zB durch »Copy and Paste«) nicht vom Tatbestand erfasst sein soll, weil es sich dann nicht mehr um die ursprüngliche Nachricht handelt. Das »Schutzobjekt« der Bestimmung ist doch gerade der »Inhalt einer Nachricht«.

6. Zur Datenbeschädigung (§ 126a)

Nach der formellen Ratifikation der CCC im Jahr 2012 sollte nun auch jeder Zweifel ausgeräumt sein, dass § 126a – wie bereits von einem Teil der Lehre in Erwägung gezogen wurde – neben dem Rechtsgut Vermögen auch das »Interesse am Fortbestand und der Verfügbarkeit von Daten« schützt.

Das tatbestandliche Löschen erfordert einen »computertechnischen Eingriff«. Es ist daher ausschließlich ein technikspezifischer Löschvorgang angezeigt. Das Löschen elektronischer Daten ist vom »Zerstören« oder »Vernichten« (körperlicher Sachen) zu unterscheiden. Das Zerstören eines (körperlichen) Datenträgers stellt daher kein programmspezifisches Löschen von Daten dar, selbst wenn der Datenbestand dadurch »unbrauchbar« gemacht oder vernichtet wird.

Werden fremde Daten softwaregestützt – zB über einen Löschbefehl des Betriebssystems – vom Täter »gelöscht«, liegt allerdings in Wahrheit gar keine Löschung vor, da sich die Daten auch nach Ausführung dieses Befehls (vorerst) weiterhin am Datenträger befinden und sich nur ihre Organisation geändert hat (logisches Löschen).

Das tatbestandliche »Löschen« iSd § 126a Abs 1 stellt daher ausschließlich auf eine tatsächliche dauerhafte und unwiderrufliche Datenentfernung ab, die unmittelbar durch die Handlung realisiert werden muss.

Das »logische Löschen« beschreibt bloß ein Zwischenstadium vom computersystemspezifischen Löschbefehl bis zum vom Betriebssystem programmtechnisch durchzuführenden faktischen Überschreiben der Speicherbereiche mit neuen Daten.

Was das temporäre Unterdrücken von Daten im Vergleich zum zeitlich befristeten Unterdrücken bzw Entziehen einer körperlichen Sache

anlangt, ist festzustellen, dass das Tatobjekt »Computerdaten« (§ 126a) für den Gesetzgeber offenbar schutzwürdiger erscheint, als ein Tatobjekt körperlicher Konsistenz (§ 125).

Für das Unterdrücken von elektronischen Daten ist es nur erforderlich, dass der originäre Informationswert letztlich – nach Aufhebung der automationsunterstützten oder nicht automationsunterstützten Zugriffsblockade – wieder vollständig herstellbar ist. Andernfalls wären die Daten nämlich bereits »verändert« oder »sonst unbrauchbar«.

Aufgrund der Ubiquität und Virtualität von digitalen Daten ist es wohl unbeachtlich, ob die Daten (im engen oder weiten Sinn) während der Unterdrückung verändert werden oder nicht.

Auch spielt es bei einer Datenunterdrückung keine Rolle, dass der Berechtigte während des gesamten Tatzeitraums weiterhin rein faktisch die Daten im engen Sinn in seiner Verfügungsmacht hat.

Die Datenunterdrückung, insb in ihrer Ausprägung als nur vorübergehende Vorenthaltung, weist einen den anderen Handlungsvarianten verschiedenen Sinngehalt auf.

Die Anerkennung des Rechtsguts des »Interesses am Fortbestand und der Verfügbarkeit von Daten« indiziert aber auch – die längst notwendige Ausdehnung – der Schutzausrichtung des § 126a auf das Rechtsgut der »Privatsphäre« und den immateriellen »Informationswert« von Daten.

Im Zusammenhang mit der Schadensbewertung ist eine Abstraktion von der Identität der konkret betroffenen Daten indiziert. Die tatbildlich beschädigten Computerdaten müssen nämlich nicht allein auch den vermögenswerten Charakter besitzen. Das Löschen von Daten führt daher beim Vorhandensein aktueller und umfassender Sicherungskopien nicht zwangsläufig zu einem Vermögenschaden beim Opfer.

Die Qualifikationstatbestände des § 126a sind in Anbetracht der Analogie zur Sachbeschädigung in quantitativer Hinsicht zu bemängeln. Es sollten daher Qualifikationsnormen iSd § 126 Abs 1 Z 1, 4, 5, 6 auch im Bereich der Datenbeschädigung angedacht werden. Dies betrifft kritische Infrastrukturen, wie etwa gänzlich oder teilweise computergesteuerte Stromversorgungsanlagen, Kommunikationsinfrastrukturen, Verkehrsleitsysteme, Flugsteuerungsprogramme, Kraftwerke, Gaspipelines usw, die durch Hacker-Angriffe manipuliert werden.

Was eine Privilegierung durch analoge Anwendung des § 141 (iVm § 126a) anlangt, ist festzuhalten, dass in einigen Fällen kriminalpolitische Widersprüche zu Tage treten.

Auch kann grundsätzlich bei einer vollendeten Datenbeschädigung (samt Qualifikationen) eine Strafaufhebung durch Tätige Reue unter den Voraussetzungen des § 167 in Betracht kommen. Rechtspolitisch auffällig ist diese Bestimmung dann, wenn Daten mit bloßem Affektionswert unwiederbringbar gelöscht werden. In derartigen Fällen (zB wenn digitalisierte Personenfotos des Verletzten nicht wiederherstellbar sind) kann mangels objektiver Bestimmbarkeit auch keine finanzielle Schadensgutmachung mehr unternommen werden.

7. Zur Störung der Funktionsfähigkeit eines Computersystems (§ 126b)

Im Verhältnis zur Datenbeschädigung (§ 126a) bedeutet § 126b – trotz ausdrücklicher Subsidiarität des Grunddelikts (§ 126b Abs 1) – eine Vorverlagerung des Rechtsgüterschutzes. § 126a stellt auf die (vermögenswerteren) Daten und § 126b auf das diese verarbeitende Computersystem ab.

§ 126b kann auch als verhaltensgebundenes Dauerdelikt begangen werden. Übermittelt der Täter zB im Zuge eines DDoS-Angriffs permanent Datenpakete an das Zielsystem, um die schwere Funktionsstörung aufrechtzuerhalten, so ist zwar das Delikt mit Beginn der Funktionsstörung formell vollendet, aber erst dann materiell beendet, wenn der Täter mit der Übersendung der Datenpakte aufhört und dadurch der Störvorgang beendet wird.

Für die Schadensbestimmung soll der faktische Zustand eines gestörten Computersystems genügen, auf die Schwere des Schadens kommt es nicht an. Der Gebrauchswert des Systems wird dadurch in den Vordergrund gerückt, ein objektiv bestimmbarer Schaden ist nicht verlangt.

Als Rechtsgut wird neben gewissen Vermögensaspekten in erster Linie die Verfügbarkeit und Integrität informationstechnischer Systemen geschützt.

Darauf lässt ua auch die Qualifikationsbestimmung des § 126b Abs 2 erster Fall schließen, die faktisch eine – dem Vermögensstrafrecht grundsätzlich fremde – Strafverschärfung bezüglich einer über eine längere Zeit anhaltende Beeinträchtigung des Affektionsinteresses vorsieht.

Im Zusammenhang mit der Subsidiaritätsklausel (§ 126b Abs 1) und der Qualifikationsnorm (§ 126b Abs 2 erster Fall) stößt man auf

ein interessantes Problem bezüglich der Figur des »qualifizierten Versuchs«. Denn in der (bloß) versuchten einfachen Datenbeschädigung nach §§ 15, 126a Abs 1 kann in einem praxisnahen Fall eine qualifizierte Störung der Funktionsfähigkeit eines Computersystems iSd § 126b Abs 2 erster Fall enthalten sein. Diese würde allerdings – bei Ausdehnung der Subsidiaritätsklausel des § 126b Abs 1 auf dessen Qualifikationsnorm des Abs 2 – trotz höherer Strafdrohung und verschiedenartiger Rechtsgüter kraft gesetzlicher Anordnung hinter den einfachen Versuch der Datenbeschädigung zurücktreten. Die Besonderheit der Rechtsfigur des qualifizierten Versuchs liegt nun aber grundsätzlich darin, dass bei strafbefreiendem Rücktritt vom Versuch (§ 16) das darin vollendete Delikt unberührt bleibt und die Strafbarkeit ausnahmsweise wieder auflebt. Tritt der Täter vom Versuch zurück, entfiele daher die Sperrwirkung der Subsidiaritätsklausel, weil die Strafbarkeit der gleichzeitig verwirklichten (aber bislang verdrängten Norm der) länger andauernden Störung der Funktionsfähigkeit des betreffenden datenverarbeitenden Computersystems (§ 126b Abs 2 erster Fall) wieder reaktiviert wird.

Ein die Subsidiarität begründender Aushilfsgedanke lässt sich aufgrund der partiellen Verschiedenartigkeit der Rechtsgüter, der unterschiedlichen Stadien und Handlungsweisen des Angriffs und dessen jeweiliger unterschiedlicher Rechtsgutintensität weder im Grunddelikt noch in dessen Qualifikation erkennen.

Die Subsidiaritätsklausel in § 126b Abs 1 zugunsten § 126a erweist sich generell als unzweckmäßig und überflüssig, und ihre Anwendung bleibt de lege lata wohl ausschließlich auf das Grunddelikt beschränkt.

8. Zum Missbrauch von Computerprogrammen oder Zugangsdaten (§ 126c)

Auf die spezielle Tauglichkeit eines Computerprogramms zur Begehung der genannten Delikte sollte aus triftigen Gründen für die Einordnung als Tatobjekt des § 126c Abs 1 Z 1 verzichtet werden.

Der Gesetzgeber sollte die Formulierung des objektiven Tatbestands dahingehend abändern, dass das gegenständliche Computerprogramm nach seiner besonderen Beschaffenheit ersichtlich zur Begehung einer der genannten Straftaten »geeignet« sein muss, ganz gleichgültig zu welchem Zweck es (ursprünglich) geschaffen oder adaptiert wurde. Will der Gesetzgeber tatsächlich »Dual-use Devices« von der tatbestandlichen Er-

fassung ausnehmen, sollte er in der Tatumschreibung eine unmissverständliche Formulierung finden, die eine (rein objektive) Abgrenzung von sozialschädlichen Computerprogrammen und sozialverträglichen Dual-use Computerprogrammen ermöglicht.

Grundsätzlich ist jede – daher auch analoge – Form eines Passworts, das Zugang zu einem Computersystem gewährt, als Tatobjekt iSd § 126c Abs 1 Z 2 zu betrachten.

Gerade bei Zugangsdaten ist – im Vergleich zu Computerprogrammen – die Missbrauchsgefahr deutlich erhöht. Es sollte daher irrelevant sein, ob ein geheimes und gültiges Computerpasswort auf einem Papier aufgeschrieben oder in einer Textdatei auf einem Datenträger in codierter Form gespeichert wurde.

Was Zugangsdaten (§ 126c Abs 1 Z 2) betrifft, ist in Anbetracht des Schutzcharakters dieser Bestimmung wohl vorrangig auf den Inhalt des Passworts und nicht auf dessen spezifische Codierung abzustellen.

Der Begriff des »Herstellens« impliziert, dass ein »gebrauchsfertiges« Schadprogramm außenweltwirksam ursprünglich bzw zu einem schon existenten solchen Programm zusätzlich durch dessen Reproduktion neu entsteht (Erfolgsdelikt).

Bezüglich Computerprogramme ist anzumerken, dass nur das Programmieren der Software in einer unmittelbar »computerablauffähigen« Form gemeint sein kann. Das Verfassen einer Spezifikation des Computerprogramms auf Papier (oder auch in einer Textdatei) wäre noch eine straflose Vorbereitungshandlung. Deliktsspezifisch muss daher entweder ein Computerprogramm im Object Code oder ein mittels Interpreter unmittelbar ausführbarer Source Code hergestellt werden.

Diskussionsbedürftig ist die Frage der Beurteilung eines Vervielfältigungsvorganges von Zugangsdaten unter Einbeziehung eines »Systembruchs« von digitaler zu analoger Darstellung, zB das bloße Abschreiben der Information eines automationsunterstützt verarbeitbaren Computerpassworts auf ein analoges Blatt Papier.

Auch die Erlangung solcher unkörperlichen Sachen muss – ohne das Erfordernis einer Gewahrsamsbegründung an einem körperlichen Gegenstand – möglich sein. Betrachtet man etwa die Tathandlung des Sich-Verschaffens iVm Zugangsdaten des § 126c Abs 1 Z 2, so muss das Sich-Verschaffen von Zugangsdaten schlüssigerweise möglich sein. Dieses Vorbereitungsdelikt macht idZ aber nur dann Sinn, wenn bereits das Ablesen eines (fremden) Passworts als ein Sich-Verschaffen

anzusehen ist. Der Täter befindet sich nämlich dann bereits in dessen Kenntnis. Dass er auch den Zettel, als Träger der Schrift, an sich bringen muss, ist dabei wohl nicht erforderlich.

Dies hat aber zur Folge, dass mit dem Sich-Verschaffen von Zugangsdaten zwangsläufig keine von der Tathandlung – wenn auch nur gedanklich – abtrennbare Wirkung in der Außenwelt verbunden sein muss, weshalb sich daraus nicht unbedingt ein Erfolgsdelikt ableitet.

Um begrifflich nicht in Konflikt mit den klassischen strafrechtsdogmatischen Rechtsfiguren zu treten, wie zB dem strengen Gewahrsamsbegriff, könnte iZm ubiquitären, unkörperlichen Sachen auf ein »Quasi-Gewahrsam« iS einer Gewahrsamsähnlichkeit abgestellt werden.

Unter dem hier vorgeschlagenen »Quasi-Gewahrsam« ist iZm der Tathandlung des »Sich-Verschaffens« von Computerdaten die umfassende Kenntnisnahme- und Verfügungsmöglichkeit des Täters zu verstehen, deren Bedeutungsgehalt (= Information) wahrzunehmen und ihre technische Repräsentation (= Daten im engen Sinn) uneingeschränkt zu verarbeiten.

Obwohl die meisten Tathandlungen des § 126c Abs 1 (wie das Herstellen, Einführen, Vertreiben, Veräußern oder Sonst-Zugänglichmachen) Erfolgsdelikte beschreiben, was sich allein aus der Tatbestandsauslegung ergibt, liegt aus dem Blickwinkel der Beziehung zum teleologischen Schutzanliegen der Bestimmung auch ein »abstraktes Gefährdungsdelikt« vor.

Aus kriminalpolitischen Gründen wäre es aufgrund der Rechtsprechungslinie des OGH bezüglich der widerrechtlichen Bargeldbehebung an Bankomaten notwendig, den Straftatbestand des Diebstahls (§ 127) ebenfalls als eines der (Haupt-)Delikte in § 126c Abs 1 Z 1 aufzunehmen.

Der Tatbestand des § 126c Abs 1 sollte um das tatbestandsbegrenzende Merkmal »unbefugt« bzw »widerrechtlich« erweitert werden, sodass die Bestimmung tatsächlich nur denjenigen erfasst, der derartige Programme oder Zugangscodes unzulässigerweise herstellt, einführt, vertreibt, veräußert, sonst irgendwie zugänglich macht, sich verschafft oder besitzt, um eine der in Z 1 genannten strafbaren Handlungen zu begehen, und nicht auch autorisierte IT-Sicherheitsunternehmen, die sich auf das Testen von Sicherheitsvorkehrungen anderer gewerblich spezialisiert haben.

9. Zum Betrügerischen Datenverarbeitungsmissbrauch (§ 148a)

Dem Tatbestand des § 148a fehlt ein dem Betrugstatbestand vergleichbares objektives Gefährlichkeitselement der Tathandlung, was auch die hM mit ihrer Begründung einer »betrugsähnlichen« Konzeption durch teleologisch-systematische Erwägungen indirekt fordern müsste. Dass einzig der erweiterte Vorsatz und daher lediglich eine »sozial inadäquate Intention« als tatsächliches unrechtsbegründendes Element ausschlaggebend sein soll, erscheint inadäquat. Daraus folgt, dass nicht vorrangig die Gefährlichkeit des objektiven Verhaltens bestraft wird, sondern der Tatplan und somit faktisch die Gesinnung des Täters, was bedenklich erscheint.

Der Ansatz einer Lehrmeinung, für die Anwendung des § 148a eine »Mensch-anstelle-Maschine-Prüfung« vorzunehmen, die als interpretative Grundlage einen Vergleich mit Kerninhalten anderer Bestimmungen hat, ist rechtspolitisch wie dogmatisch problembehaftet.

Herausgearbeitete Unterschiede des § 148a zu § 146, die gegen eine Betrugsähnlichkeit sprechen sind: 1.) Beim Betrug handelt es sich um ein verhaltensgebundenes Delikt, das eine »Täuschung über Tatsachen« im äußeren Verhalten unverzichtbar erforderlich macht. Als Gegenstück dazu ist aus dem Wortlaut des § 148a lediglich die äußere Handlungsweise der Gestaltung eines Programms oder die Eingabe von Daten genannt, die zur Beeinflussung eines Ergebnisses führen muss. Zwischen einer Täuschung eines Menschen (iSd § 146) und der (bloßen) Eingabe von (zB richtigen) Daten ist jedoch zumindest ein deutlicher Unterschied im tatbestandlichen Unrecht erkennbar. 2.) Was das Maß der kriminellen Energie anlangt, ist die Täuschung eines Menschen gegenüber der bloßen Eingabe von Daten (wenn auch mit dem Vorsatz der Bereicherung) höher zu bewerten und daher auch mit einem höheren Unrechtsgehalt verbunden. 3.) § 146 ist von seiner Konzeption aus betrachtet ein Selbstschädigungsdelikt, § 148a aber ein Fremdschädigungsdelikt. 4.) Es gibt bezüglich § 148a kein dem »Notbetrug« (§ 150) vergleichbares Delikt. Bei Annahme einer Betrugsähnlichkeit ist eine adäquate Privilegierung auch für § 148a in den Fällen indiziert, in denen die Begehung aus Not mit einem nur geringen Schaden geschieht.

Aus kriminalpolitischer Sicht ist die Verneinung einer strafbaren Beteiligung an Delikten mit überschießender Innentendenz nach de-

ren formeller Vollendung gerade in Bereichen der Computerdelikte, welche außerhalb des Vermögensstrafrechts angesiedelt sind, mangels entsprechender Anschlussdelikte sachwidrig.

10. Zur Datenfälschung (§ 225a)

Problematisch zeigt sich iZm § 225a die allgemeine Begriffskonkretisierung des § 74 Abs 2. Diese besitzt nämlich keine Einschränkung auf »automationsunterstützt verarbeitete, übermittelte oder überlassene Daten« (Computerdaten). Da auch nicht alle Tathandlungen des § 225a ausschließlich über eine informationstechnische Manipulation realisierbar sind, muss in diesem Kontext über eine historische bzw konventionsgerechte Interpretation, aber auch aufgrund teleologischer Erwägungen rein auf »Computerdaten« abgestellt werden, um eine sinnvolle Anwendung der Bestimmung zu gewährleisten.

11. Zum Phishing und § 108 StGB iVm § 1 DSG 2000

Das Grundrecht auf Geheimhaltung personenbezogener Daten (§ 1 Abs 1 DSG 2000) ist ein konkretes Individualrecht, welches als Tatobjekt des § 108 StGB in Frage kommt. Täuscht daher der Täter zB in einem E-Mail über Tatsachen, sodass er das Opfer dadurch zu einer Handlung, nämlich der Preisgabe schutzwürdiger personenbezogener Daten, verleitet, so ist – Absichtlichkeit im Tatbildvorsatz vorausgesetzt – § 108 StGB iVm § 1 Abs 1 DSG 2000 verwirklicht.

Der Stärkegrad der Absicht (iSd § 5 Abs 2) ist dabei jedenfalls indiziert, kommt es doch dem Täter in der Phishing-Phase gerade darauf an, das Opfer in dessen Geheimhaltungsrecht nach § 1 Abs 1 DSG 2000 zu verletzen. Der Täter benötigt schließlich diese Daten tatplangemäß für sein weiteres Vorhaben, nämlich eine Vermögensschädigung durch Verwendung der Daten zum Geldtransfer via Online-Banking.

12. Zu unbaren Zahlungsmitteln (§§ 241a, 241b, 241c, 241d, 241e, 241f, 241g)

Bei Bankomatkarten stellt die auf der Karte verschlüsselt gespeicherte PIN ein Sicherheitsmerkmal dar, welches jedoch bei der Bezahlung mittels elektronischer Geldbörse (Quick-Chip-Funktion) gerade nicht Verwendung findet. Mangels Erfüllung der in § 74 Abs 1 Z 10 angeführ-

ten Kriterien ist somit entgegen der hM davon auszugehen, dass die elektronische Geldbörse – im Gegensatz zu einer Bankomat- bzw Kreditkarte – kein unbares Zahlungsmittel darstellt.

§ 241a ist im Verhältnis zum Rechtsgut betrachtet ein abstraktes Gefährdungsdelikt, bezüglich der tatbestandlichen Struktur – unter stringenter Anwendung der vorherrschenden Definition – ein Erfolgsdelikt. Unter Einbeziehung der überschießenden Innentendenz liegt darüber hinaus ein verkümmert zweiaktiges Delikt vor.

Die Gruppe der Tathandlungen des (sinngemäß) »An-sich-Nehmens« und »Besitzens« (§ 241b erster, zweiter, vierter und sechster Fall) indizieren § 241b als alternatives Mischdelikt. Dem gegenüber beschreiben § 241b dritter (arg »einem anderen verschaffen«) und fünfter Fall (arg »einem anderen überlassen«), die im Innenverhältnis selbst wiederum gleichwertig sind, allerdings einen kumulativen Mischtatbestand.

Die Strafbarkeit beider objektiv beschriebener Deliktsfälle des § 241e gründet sich im subjektiven Tatbestand auf zwei verschiedenartig konzipierte überschießende Innentendenzen. Diesbezüglich kann bei § 241e Abs 1 von einem »subjektiven Mischtatbestand« gesprochen werden. Die Tathandlung muss daher vom Täter mit dem erweiterten Vorsatz gesetzt werden, dass er oder ein Dritter durch die Verwendung des entfremdeten unbaren Zahlungsmittels im Rechtsverkehr unrechtmäßig bereichert (erste subj Alt bzw § 241e Abs 1 erster Satz), oder dass eine Fälschung unbarer Zahlungsmittel (§ 241a) ermöglicht werde (zweiter subj Alt bzw § 241e Abs 1 zweiter Satz). Beide Deliktsfälle beschreiben folglich auch kupierte Erfolgsdelikte, da das jeweilige Endziel (Bereicherung durch Verwendung des Tatobjekts bzw Fälschungsermöglichung) ein über den objektiven Tatbestand hinausreichender vom Täter bloß angestrebter Erfolg ist, der nicht (mehr) tatbestandsmäßig ist.

Die Bestimmung über die Tätige Reue des § 241g ist in Bezug auf § 241e Abs 3 aus mehreren Gründen unschlüssig: 1.) Der Täter iSd § 241e Abs 3 strebt – ebenso wie bei Inanspruchnahme des § 241g Abs 1 und 2 – gar nicht an, das unbare Zahlungsmittel im Rechtsverkehr zu verwenden. Vielmehr will er seine Verwendung sogar bewusst verhindern. 2.) § 241e Abs 3 erfasst keine Vorbereitungshandlungen zum Gebrauch entfremdeter unbarer Zahlungsmittel. Solche sind aber in der Systematik des StGB iZm Delikten der Urkunden-, Daten- und Geldfälschung (nun auch unbaren Zahlungsmitteln) sowie den Vermögens-

delikten gerade der typische Grund für Tätige Reue-Bestimmungen. 3.) Es stellt sich die Frage, warum nicht auch eine Beschädigung (iSd § 241e Abs 3 Fall 2) eines unbaren Zahlungsmittels, die zu einer endgültigen Beseitigung der Gefahr einer allfälligen missbräuchlichen Verwendung desselben führt, nicht – wie bereits dessen Vernichtung – ausdrücklich ausgeschlossen wurde.

13. Zu Pornographischen Darstellungen Minderjähriger (§ 207a)

Das »Anbieten« ist keine den anderen Tathandlungen des § 207a Abs 1 Z 2 gleichwertige Tathandlung, da es sich um eine der tatsächlichen Weitergabe der Darstellungen noch vorgelagerte Tätigkeit (iSd Anbahnung einer Weitergabe) handelt.

Für das Sich-Verschaffen pornographischer Darstellungen iSd § 207a Abs 3 Satz 1 Fall 1 und Satz 2 Fall 1, die durch Computerdaten repräsentiert werden, sollte nicht auf eine Gewahrsamsbegründung hins körperlicher Gegenstände abgestellt werden, sondern auf eine Art »Quasi-Gewahrsam« zurückgegriffen werden. Dies erscheint als Weiterentwicklung des »gelockerten bzw sozialen Gewahrsams« im sachlich sinnvollen Zusammenhang mit unkörperlichen Daten(inhalten) angebracht. Dadurch würde das Desiderat erfüllt, eine zweckmäßige Adaptierung der spezifischen Dogmatik vorzunehmen und iZm unkörperlichen Sachen eine Abstraktion von der körperlichen Substanz sinnvoll einzubeziehen. Insbesondere sind dabei auch dynamische technische Weiterentwicklungsprozesse zu berücksichtigen, wie sie bereits faktisch im »Cloud Computing«, »Online-Speicher« usw realisiert sind. Als ein neuer Anknüpfungspunkt kommt in diesen Fällen wohl bloß der »Access« in Frage. Der Datenträger, der hierbei ohnehin ausschließlich eine rein faktisch-notwendige Aufgabe erfüllt, sollte dafür keine Rolle mehr spielen.

In der Definition des Tatbestands des § 207a Abs 3a wird erstmals das »Internet« als Tatbestandsmerkmal ins StGB eingeführt, weshalb daraus aber auch ein Gesetzesbegriff wurde, der vom Gesetzgeber durch eine Legaldefinition gehörig determiniert werden sollte. De lega lata wird man allerdings, um unerwünschte Ergebnisse zu vermeiden, bei dessen Auslegung vom allgemeinen Sprachgebrauch dieses Begriffs – und nicht von der technischen Definition – ausgehen müssen.

14. Zu Pornographischen Darbietungen Minderjähriger (§ 215a)

§ 215a Abs 2a stellt ein schlichtes Tätigkeitsdelikt dar, da es ausschließlich auf eine Handlung und keinen tatbestandlichen Erfolg ankommt. Mit dem Betrachten der inkriminierten Darbietung ist das Delikt bereits verwirklicht.

Was die Wahrnehmung der Darbietung im Wege einer Direktübertragung zB im Internet anlangt, so sollte – wie bereits das »Zugreifen« in § 207a Abs 3a – auf eine Audio-Video neutrale Begrifflichkeit abgestellt werden, wie »wahrnehmen«, »zugreifen« bzw »sich zugänglich machen« oder »benützen«.

§ 215a Abs 2a erster Satz fällt aufgrund seiner Strafdrohung in die sachliche Zuständigkeit des Bezirksgerichts, was mE unsachlich ist und wohl auf ein Redaktionsversehen schließen lässt, da für die vergleichbare Bestimmung des § 207a Abs 3a (auch hins mündiger Minderjähriger) – wie auch für § 207a Abs 3 (auch Satz 1) – die (teils ausnahmsweise) Zuständigkeit des Einzelrichters am Landesgericht gem § 31 Abs 4 Z 2 iVm § 30 Abs 1 Z 9 StPO besteht. Dies sollte daher mE für § 215a Abs 2a Satz 1 nachgebessert werden.

15. Zur Anbahnung von Sexualkontakten zu Unmündigen (§ 208a)

Die Formulierung »unter Verwendung eines Computersystems« in § 208a Abs 1 Z 1 Fall 2 ist in dieser Form ungewöhnlich, zumal bisher in Ergänzung zur Telekommunikation überwiegend der Wortlaut »im Wege eines Computersystems« verwendet wurde. Daraus könnte methodengerecht geschlossen werden, dass der Gesetzgeber durch die Verwendung unterschiedlicher Formulierungen auch Unterschiedliches meint. Man könnte dem Wortlaut nach somit davon ausgehen, dass eine Strafbarkeit nach dieser Begehungsalternative selbst dann vorliegt, wenn der Täter das Kind zu einem Treffen dadurch überreden will, dass er ihm ein Computersystem als Geschenk in Aussicht stellt. In einem derartigen Fall würde – zB bei einem persönlichen Kontakt auf der Straße, in einem Brief usw – die erste Alternative des § 208a Abs 1 Z 1 erfüllt sein und nicht die eigentlich dafür intendierte zweite, bei der es – anders als bei den IKT-Kontaktformen der Z 1 – zu einer

Täuschung des Opfers kommen müsste. Die Formulierung sollte auf den spezifischeren und auch bisher verwendeten Wortlaut »im Wege eines Computersystems« abgeändert werden.

Der Gesetzgeber erachtet wohl den GMat zufolge in der Täuschung, die er bei der sonstigen Begehungsweise – dh außerhalb der IKT – verlangt, die »besondere Gefährlichkeit«, was für die Begehungsweise des § 208a Abs 1 Z 1 impliziert, dass eine besondere Gefährlichkeit bereits in der bloßen »Nutzung« informations- und telekommunikationstechnischer Systeme (iSd § 208a Abs 1 Z 1) liegt. Eine solche Betrachtung ist aber in Anbetracht der für sich gesehen sozial adäquaten Nutzung informations- und kommunikationstechnischer Systeme bzw des bloßen Betriebs solcher Systeme meiner Auffassung nach strikt abzulehnen.

Aus der offensichtlichen Verlagerung des spezifischen Unrechts auf die subjektive Tatseite fragt sich, ob die Sozialschädlichkeit des Täterverhaltens nicht hauptsächlich an der inneren Einstellung und daher an der Gesinnung des Täters ansetzt. Bejaht man eine solche Nähe zum Gesinnungsstrafrecht, ist zu klären, ob in diesem Fall tatsächlich die Tatbestandsumschreibung den strengen Erfordernissen des verfassungsrechtlichen Bestimmtheitsgebots Rechnung trägt.

Täuscht der Täter iZm der konventionellen Begehungsweise des § 208a Abs 1 Z 2 eine unmündige Person nicht über seine Absichten – spricht er diese ggf sogar explizit an – und schlägt etwa ein weiteres Treffen vor, macht sich der Täter nicht nach § 208a strafbar. Gerade aus dieser Überlegung und in Anbetracht der besonderen Eigenschaft des Tatobjekts sowie des intendierten Rechtsgüterschutzes liegt die »besondere Gefährlichkeit« dieser Begehungsweise jedoch wohl nicht in der Täuschung, sondern in jeder konkreten Handlung, die eine unmündige Person zu einem Treffen für sexuelle Übergriffe bewegt, ob nun mittels Täuschung oder nicht.

§ 208a Abs 1a fehlt jegliche sozial inadäquate Verhaltensweise im objektiven Tatbestand. Somit handelt jeder der mit Unmündigen über das Internet in Kontakt tritt, bereits (objektiv) tatbestandsgemäß. Wenn lediglich eine Kontaktaufnahme im Internet zu einer unmündigen Person erfolgt, muss der Inhalt der Kommunikation nicht einmal etwas mit dem Inhalt der überschießenden Innentendenz (dh der Absicht eine strafbare Handlung nach § 207a Abs 3 oder 3a an dieser unmündigen Person zu begehen) zu tun haben. Das Unrecht der Tat ergibt sich daher ausschließlich aus dieser überschießenden Innentendenz.

Eine solche Subjektivierung des Unrechts ist jedenfalls verfassungsmäßig bedenklich, insb was den strengen Bestimmtheitsgrundsatz bezüglich der Formulierung der konkret verpönten Handlungsweise betrifft.

§ 208a Abs 1a ist lediglich ein Vorbereitungsdelikt die Absicht des Täters betreffend, eine strafbare Handlung bezüglich »pornographischer Darstellungen« iSd § 207a Abs 3 und 3a iVm § 207a Abs 4 hins der unmündigen Person zu begehen. Dadurch wird iZm »pornographischen Darbietungen« iSd § 215a Abs 2a eine Gesetzeslücke aufgetan. Der Gesetzgeber sollte diese Lücke durch Ausweitung des Bezugsobjekts der überschießenden Innentendenz in § 208a Abs 1a um die strafbare Handlung nach »§ 215a Abs 2a« erweitern, sodass diese lautet: »[…] in der Absicht, eine strafbare Handlung nach § 207a Abs. 3 oder 3a in Bezug auf eine pornographische Darstellung (§ 207a Abs. 4) oder nach § 215a Abs. 2a in Bezug auf eine pornographische Darbietung (§ 215a Abs. 3) dieser Person zu begehen […]«.

§ 208a Abs 1a sollte – was die »Kontaktherstellung« zu einer unmündigen Person anlangt – als Erfolgsdelikt identifiziert werden, damit eine noch weitere (bzw sogar zu weite) Vorverlagerung der Vollendungsstrafbarkeit verhindert wird.

16. Zur Anleitung zur Begehung einer terroristischen Straftat (§ 278 f)

In dieser Strafbestimmung ist bemerkenswert, dass der Gesetzgeber in den einzelnen Wendungen »Informationen im Internet« (Abs 1) bzw »Informationen aus dem Internet« (Abs 2) jeweils zwei weitverbreitete, polysemische Begriffe als Rechtsbegriffe miteinander in einem Unrechtstatbestand kombiniert, ohne sie für das strafrechtliche Verständnis zu definieren.

Im deliktsspezifischen Verständnis wird wohl als »Information« der für den Menschen relevante Bedeutungsinhalt von Daten gemeint sein. Auf die technische Verarbeitungsform kommt es bei § 278 Abs 3 – im Gegensatz aber zu § 278f Abs 1 und 2 – nicht an. Anstelle der »Information« könnte auch mit dem (zwar in anderer Hinsicht umstrittene) Datenbegriff des § 74 Abs 2 das Auslangen gefunden werden. Durch die zusätzliche – dem StGB ohnehin neue – Begrifflichkeit der »Information« wird der Eindruck erweckt, es handle sich dabei im Hinblick auf »Daten« auf der einen und »Informationen« auf der anderen Seite um Verschiedenes.

Die Form der Erfassung der Weitergabetathandlungen ist, was gerade den Bezug zum Internet anlangt, untypisch, da das »Veröffentlichen« nicht gesondert als Tathandlung genannt ist.

Was das »Sich-Verschaffen« von inkriminierten Informationen gem § 278f Abs 2 betrifft, ist erneut darauf hinzuweisen, dass entgegen der in den GMat vertretenen Meinung keine Gewahrsamsbegründung an körperlichen Sachen zu verlangen ist; »Quasi-Gewahrsam« hat zu genügen.

17. Zu § 126a als terroristische Straftat

Durch die Erfassung der Datenbeschädigung nach § 126a als terroristische Straftat in § 278c Abs 1 Z 6 mit der Verquickung des Erfordernisses, dass dadurch eine Gefahr für Leib und Leben bzw insb eine Gefahr für »fremdes Eigentum in großem Ausmaß« herbeigeführt werden muss, räumt der Gesetzgeber indirekt ein, dass es durch eine »Datenbeschädigung« möglich sein muss, zumindest Eigentum (im strafrechtlichen Sinn) zu gefährden bzw zu verletzen. Daraus folgt, dass eine Datenbeschädigung iSd § 126a auch geeignet sein muss, Schäden an körperlichen Gegenständen zu verursachen.

Ist ein Schadprogramm lediglich in der Lage, unkörperliche Software zu löschen bzw zu gefährden, wäre das »Eigentum« nicht gefährdet. Im Zivilrecht geht die hL davon aus, dass die sachenrechtlichen Bestimmungen des ABGB grundsätzlich nur auf körperliche Sachen abzielen, weshalb durch die Unkörperlichkeit und Ubiquität von Software kein Eigentum (ieS) daran begründet werden kann. Die grundsätzliche Zivilrechtsakzessorietät des strafrechtlichen Eigentumsbegriffs iVm dem Analogieverbot verhindert, dass die Gefährdung von Software durch einen Computerwurm, selbst wenn der wirtschaftliche Wert von Software idR höher als jener der Hardware sein wird, eine Gefährdung von »Eigentum in großem Ausmaß« darstellen kann.

Es lässt uU auf ein Redaktionsversehen schließen oder an eine unbedachte Übernahme der gegenständlichen Wortfolge aus den Formulierungen der bestehenden Gemeingefährdungsdelikte (iSd §§ 169 ff) denken. Sollte nämlich tatsächlich nur eine Datenbeschädigung iSd § 126a gemeint sein, die durch die Manipulation von Daten zusätzlich auch körperliche Gegenstände (Hardware), an denen (zivilrechtliches) Eigentum bestehen kann, »gefährdet«, wäre die Nennung der Datenbeschädigung in § 278c Abs 1 Z 6 überflüssig, weil die (schwere) Sach-

beschädigung an körperlichen Sachen ohnedies von § 126 erfasst wäre. Der Gesetzgeber ist daher gefordert, die angesprochenen Unstimmigkeiten zu beseitigen und eine Vermengung der herkömmlichen strafrechtlichen Verwendung der Begriffe »Eigentum« und »Vermögen« zu vermeiden.

Es ist unverständlich, dass gerade § 126b (Störung der Funktionsfähigkeit eines Computersystems), welcher auch DoS-Attacken erfassen soll, die in der Praxis bereits mehrfach ihre Eignung für massive (zB auch terroristische) Angriffe unter Beweis gestellt haben, nicht in den Katalog der terroristischen Straftaten aufgenommen wurde. Man denke etwa an einen terroristischen DDoS-Anschlag auf kritische informationstechnische Systeme, die der Aufrechterhaltung gesellschaftlicher oder staatlicher Funktionen dienen.

18. Zur Beharrlichen Verfolgung (§ 107a)

§ 107a besitzt in seinem Gesamttatbestand eine formale Tatbestandsstruktur, die nur in der eingeschränkten Betrachtung seines Abs 1 einem schlichten Tätigkeitsdelikt entspricht. In Abstraktion seiner gesamten Tatbeschreibung liegt allerdings ein Erfolgsdelikt vor, weil die Bestimmung auf ein ganz konkretes Tatobjekt fokussiert und ein von diesem als beeinträchtigend wahrgenommenes, verhaltensgebundenes Handeln des Täters – über die tatbestandlichen Erfolge nach § 107a Abs 2 Z 1 bis 4 – die Außenwelt gezwungener Maßen verändern muss. Folglich ist ein beharrliches Verfolgen iSd § 107a Abs 1 nicht als schlichte Tätigkeit zu sehen, sondern durch die ausschließliche gesetzliche Ausfüllung dieser Tathandlung iSd Abs 2 als Erfolg zu verstehen. Dies lässt sich auch, was die Beziehung zum Rechtsgut betrifft stimmig mit der Einordung des § 107a als ein konkretes Gefährdungsdelikt kombinieren.

Trotz der für potentielle Gefährdungsdelikte üblichen Wortwahl für die im Einzelfall festzustellende generelle Gefährlichkeit einer Handlung ergibt sich in struktureller Zusammenschau des Gesamttatbestands des § 107a, dass aus den Erfordernissen für eine beharrliche Verfolgung nicht nur eine aus der allgemeinen Erfahrung abzuleitende (abstrakte) Gefahr für ein Rechtsgut verlangt wird. »Geeignet« beschreibt hier nämlich keine generelle Gefährlichkeit. Vielmehr ist der Tatbestand nur erfüllt, wenn ein konkretes Handlungsobjekt (nämlich ausschließlich die gestalkte Person) tatsächlich in den Wirkungs-

bereich der gefährlichen Begehungsweisen nach § 107a Abs 2 Z 1 bis 4 gelangt ist, sodass eine Rechtsgutverletzung mit hoher Wahrscheinlichkeit zu befürchten ist. Die Verletzung des betroffenen Rechtsguts ist aber weiterhin kein Faktum, sondern nur eine – wenn auch schon konkrete – Möglichkeit. Daher ist § 107a, was die Relation zum Rechtsgut anlangt, entgegen der hM als konkretes Gefährdungsdelikt zu qualifizieren.

Jede Art »personenbezogener Daten« (daher auch Bildaufnahmen von Personen) ist von dieser Begrifflichkeit erfasst, sofern ein Personenbezug mit verhältnismäßigem Aufwand herstellbar ist.

Im Zusammenhang mit § 107a Abs 1 iVm § 107a Abs 2 Z 4 können deliktsspezifische Probleme auftreten, wenn jemand via Aufruf im Internet Dritte dazu veranlasst, mit dem Opfer Kontakt aufzunehmen. Einerseits lässt sich in Fällen, in denen der Täter nach der Veröffentlichung weiterhin hinreichende Einflussmöglichkeiten auf das Inserat hat, das Erfordernis der »fortgesetzten Begehung« ggf durch die Kombination aus Tun und anschließendem pflichtwidrigen Unterlassen (iSd § 2) erfüllen. Da die einzelnen Begehungsweisen des § 107a Abs 2 Z 1 bis 4 nicht notwendigerweise Handlungen sind, die per se sozial inadäquat und rechtswidrig sein müssen, indiziert die einmalige Schaltung eines Internet-Inserats nicht die Herbeiführung eines rechtswidrigen Zustandes. Wird dieser Zustand von dieser Person durch anschließendes Unterlassen aufrechterhalten, ergeben sich folglich Schwierigkeiten, was die Begründung einer Garantenstellung anlangt, ebenso wie hins der Frage, ob dadurch überhaupt tatbestandliches »Unrecht« – iS eines Dauerdelikts – fortgesetzt werden kann.

II. Epilog oder fünf generelle abschließende Thesen

A. Zur Bedeutung der Computerkriminalität

Die Erscheinungsformen der Computerkriminalität haben in den letzten Jahrzehnten stark zugenommen. Auf staatlicher, politischer und internationaler Ebene lassen sich neue Betätigungsfelder für Cyber-Kriminelle erkennen, wie »Cyberwar«, »Cyberterrorismus« oder »Hacktivismus«. Auf gesellschaftlicher Ebene dominieren weiterhin die klassischen Computerkriminalitätsformen wie Beschädigungen von

Computerdaten und -systemen, Hacking und Datenspionage-Fälle, die sich zunehmend auf mobile Endgeräte und das »Internet der Dinge« ausdehnen werden. Darüber hinaus finden verstärkt IKT-Angriffe auf Einzelpersonen statt, wie es Fälle von Cyber-Stalking, Cyber-Mobbing, Cyber-Grooming, Identitätsmissbräuche oder Happy Slapping bestätigen. Proportional zur technischen Fortentwicklung werden auch die Phänomene zunehmen. Der Computerkriminalität wird in den nächsten Jahren viel höhere Aufmerksamkeit in der Strafrechtspraxis, aber auch in der Rechtswissenschaft gewidmet werden müssen, als ihr heute eingeräumt wird.

B. Zur Transformation und Expansion der Rechtsgüter

In den Anfängen des Computerstrafrechts der ersten Generation (vgl StRÄG 1987), galt das zentrale Anliegen bezüglich IKT-bezogener kriminologischer Entwicklungen in erster Linie dem Schutz des Rechtsguts »Vermögen«. Ob iZm der Datenbeschädigung (§ 126a) etwa neben dem Vermögen auch »das Interesse am Fortbestand und der Verfügbarkeit von Daten« generell geschützt wird und daher selbst das bloße Affektionsinteresse strafrechtlichen Schutz genießt, war lange Zeit umstritten (und ist es vereinzelt noch). Spätestens mit der Ratifikation der Cybercrime-Konvention des Europarats sollte in Österreich allerdings jeder Zweifel beseitigt sein, dass das Vermögen nicht mehr im Zentrum des Schutzes der Datenbeschädigung steht, sondern die Integrität und Verfügbarkeit von Computerdaten und Computersystemen. Dafür steht auch die Strafbestimmung des § 126b, die ihrem Wesen nach kaum noch auf Kriterien des traditionellen Vermögensstrafrechts abstellt und in konventionskonformer Auslegung sogar vordergründig das subjektive Gebrauchsinteresse iSd Integrität und Vertraulichkeit eines Computersystems als Rechtsgut schützt. Darüber hinaus erstreckt sich die Schutzausrichtung bezüglich Daten und Systemen nicht nur auf das Interesse eines Verfügungsberechtigten (wie zB des Verantwortlichen für die Daten oder des Eigentümers der Hardware), sondern auch auf das »informationelle Interesse der Allgemeinheit«. Man denke dabei etwa an informationstechnische Systeme, die im Interesse der Allgemeinheit stehen, wie intelligente, äußerst empfindliche dem Gemeinwohl dienende IKT-Infrastruktur. Der Trend bewegt sich – selbst wenn es die aktuelle Strafrechtswissenschaft noch nicht

so deutlich verorten mag – in Richtung eines Rechtsguts des »Schutzes von informations- und kommunikationstechnisch verarbeiteten Daten, deren Information und Infrastruktur«. Vereinzelt ist ein solches bereits in Teilbereichen evident, nämlich etwa im Datenschutzgesetz in Form der »informationellen Selbstbestimmung bezüglich personenbezogener Daten« (§ 51 DSG 2000), bei den Indiskretionsdelikten (§§ 119 ff) oder den Geheimnisdelikten (§§ 121 ff) des materiellen Strafrechts, da dort wohl letztlich »Informationen« und teilweise auch bloß deren technische Darstellung geschützt werden. Die Vermögensrelevanz ist in diesen Bereichen ohnehin sehr zurückhaltend und nur von untergeordneter Bedeutung. Die Anlehnung insb der Computerdelikte des §§ 126a, 126b und 126c an das Vermögensstrafrecht ist daher weitgehend unsachgerecht und überholt. Die Schaffung eines eigenen Abschnitts für solche Delikte im Strafgesetzbuch könnte bereits einen wesentlichen Teil dazu beitragen, das Rechtsgutkonzept für diese Materie aufzubrechen und den neuen Herausforderungen und Bedürfnissen der Gesellschaft anzupassen.

Wertigkeiten haben sich in diesem Bereich drastisch geändert. Den Rechtsunterworfenen geht es heute iZm IKT nicht primär um den Schutz des Vermögens (zB kommerzielle Computerprogramme) bzw Eigentums (zB Hardware), sondern um das Interesse an der Verfügbarkeit und dem Fortbestand der IKT-spezifisch verarbeiteten »Information« und deren informationstechnischer »Infrastruktur«.

Vereinzelt wird eine solche Richtungsänderung im Rechtsgutkonzept sowohl in der nationalen Rechtsordnung selbst (zB Datenschutz, Geheimnis- bzw Indiskretionsdelikte, Computersystemschutz) als auch über internationale und europäische Rechtsentwicklungen angezeigt. Die Herausforderung wird dabei sein, die strafrechtlich zu schützende Information und ihre informationstechnische Infrastruktur als Rechtsgut entsprechend zu definieren, diesbezügliche sozial inadäquate Verhaltensweisen in gesetzlichen Tatbildern zu erfassen und die bestehende Strafrechtsdogmatik sachgerecht der IKT angemessen zu adaptieren.

C. Zu traditionellen Rechtsinstituten der Strafrechtsdogmatik im Fokus der IKT

Aufgrund der einzigartigen Wesensmerkmale der IKT erweisen sich die traditionellen Rechtsinstitute nicht immer als sachgerecht. Dies betrifft insb den strengen strafrechtlichen Gewahrsamsbegriff, der in allen seinen ohnehin umstrittenen Auflockerungen (vgl gelockerter bzw sozialer Gewahrsam) an einer körperlichen Sache andockt. Es stellt sich in diesem Zusammenhang zB die Frage, ob das Sich-Verschaffen eines Zugangscodes zu einem Computersystem (vgl § 126c Abs 1 Z 2) tatsächlich nur strafbar sein soll, wenn der Täter den Zugangscode auf einem körperlichen Träger in seinen Besitz nimmt oder ob – was wohl rechtspolitisch gewünscht ist – auch die bloße Kenntnisverschaffung desselben dafür schon genügt. Ähnliche Überlegungen gilt es iZm pornographischen Darstellungen Minderjähriger anzustellen, wenn sich der Täter solche inkriminierten Bilddateien auf einen Online- bzw Cloud-Speicher im Internet abspeichert, welcher in seiner körperlichen Erscheinungsform beim Täter idR überhaupt nicht besitzwirksam werden kann. Dem grundlegenden Erfordernis des traditionellen Gewahrsamsbegriffs, dass über eine körperliche Sache – wenn auch nach einem gelockerten Verständnis – Herrschaft ausgeübt werden muss, kann in diesem Fall nicht Rechnung getragen werden. Vielmehr ist auf eine spezielle IKT-adaptierte Form des Gewahrsams abzustellen, die auf den »informationstechnischen Zugriff« bzw die vollständige Verfügungsberechtigung über die (Computer-)Daten abstellt (hier »Quasi-Gewahrsam« genannt).

Auch das Rechtsinstitut der Tätigen Reue nach § 167, welche ausschließlich im Vermögensstrafrecht ihre strafaufhebende Wirkung entfalten kann, lässt bei Daten- oder Systembeschädigungen, an welchen lediglich ein subjektives Affektionsinteresse – oder jedenfalls ein anderes als das bloße Vermögensinteresse – besteht, rechtspolitische Widersprüche zutage treten.

Ein Täter, der zwar eine qualifizierte Datenbeschädigung iSd § 126a Abs 2 Fall 2 mit einem Schaden von über € 50.000,– herbeigeführt hat, kann – die entsprechenden Anforderungen des § 167 vorausgesetzt – Tätige Reue üben und einer Bestrafung dadurch entgehen. Im Gegensatz dazu kann für einen Täter diese Möglichkeit der Strafaufhebung nicht in Betracht kommen, der lediglich eine einzige Bilddatei,

an der der Berechtigte ein anerkanntes Affektionsinteresse hat, unwiderruflich gelöscht hat und die weder rekonstruier- noch wiederbeschaffbar ist.

Einen weiteren Problembereich eröffnet die Frage nach der »Identität der Sache« iZm Tatbeständen, die auf Daten und deren Informationsgehalt abstellen. Wird § 126a durch das unwiederbringliche Löschen eines Computerprogramms verwirklicht, so ist damit nicht zwingend auch schon eine Vermögensschädigung verbunden. Das Vermögensinteresse liegt nämlich nicht in den vom Tatbestand anvisierten Daten im engen Sinn, sondern im Informationsgehalt, der durch diese Daten verkörpert wird (hier als »Daten im weiten Sinn« bezeichnet). Werden Computerdaten tatsächlich gelöscht, kann der geschützte »Informationswert« durch andere (zuvor reproduzierte) Daten mit derselben Information noch erhalten sein. Sofern kein ins Gewicht fallender Aufwand mit der Verschaffung dieser Information verbunden ist, bleibt ein Schaden trotz tatsächlicher Löschung von Daten aus. In der analogen Welt würde sich dieses Phänomen als Paradoxon zeigen, wenn nämlich der Täter eine spezielle antike Vase mit dem Hammer zerschlagen würde, genau eine solche Vase, die erst nach der Tat vermögenswirksam zu Tage tritt, mit allen besonderen Eigenschaften und Merkmalen dennoch unversehrt beim Eigentümer vorhanden wäre. Schon allein die Vorstellung eines solchen Beispiels mit körperlichen Gegenständen erweist sich als äußerst schwierig.

Bezüglich moderner Kriminalitätsformen werden sich daher klassische Rechtsfiguren der Strafrechtsdogmatik weiterentwickeln müssen, um auch hins der IKT-Spezifika sachgerechte Ergebnisse erzielen zu können.

D. Zur Unzulänglichkeit diverser Tatbestände und zur problembehafteten Gesetzestechnik

Die hohe polizeiliche Anzeigenanzahl auf der einen Seite und die niedrigen gerichtlichen Verurteilungen auf der anderen (vgl die Statistiken in der Einleitung dieser Arbeit), deuten auf mehrere Problemfelder des Strafrechts im Allgemeinen und der Strafverfolgung im Besonderen hin. Es kann sein, dass sich international agierende oder hinter Anonymisierungstools der IKT versteckende Täter schlicht nicht ausforschen

lassen, sei dies aufgrund fehlender Rechtshilfeabkommen mit diversen Staaten oder technischer Schwierigkeiten der Enttarnung und Aufenthaltsausforschung von Cyberkriminellen.

Darüber hinaus sind aber, wie die vorliegende Arbeit aufgezeigt hat, einige Tatbestände aufgrund ihrer sehr hohen Anforderungen im objektiven bzw subjektiven Tatbestand (vgl §§ 118a, 119a), andere wegen ihrer (unsachlichen) konkurrenzrechtlichen Stellung (zB § 126b) in der Praxis kaum je anwendbar.

Sehr komplex, unpraktikabel und rechtspolitisch auffällig präsentiert sich auch der Tatbestand des § 51 DSG 2000. Trotz der Aufwertung dieser Strafbestimmung zu einem (reinen) Offizialdelikt, dürfte auch diese Bestimmung in vielen strafwürdigen Praxisfällen von einer gravierenden Minderanwendbarkeit geprägt sein.

Aber auch weitere Strafbarkeitslücken sind seitens des Gesetzgebers zu schließen. So erfasst § 208a Abs 1a als Vorbereitungsdelikt nur die IKT-Kontaktherstellung zu Unmündigen in der Absicht, eine strafbare Handlung nach § 207a Abs 3 oder 3a in Bezug auf eine pornographische »Darstellung« (§ 207a Abs 4) dieser Person zu begehen. Nicht erfasst ist die Alternative, in der sich die überschießende Innentendenz auf eine strafbare Handlung nach § 215a Abs 2a bezüglich einer pornographischen »Darbietung« richtet.

In manchen Delikten verbergen sich aufgrund kumulativer Mischtatbestände selbstständige Delikte, die gesetzestechnisch besser in eigenen Absätzen gegliedert und ggf auch mit differenzierten – ihren spezifischem Unrechtsgehalt entsprechenden – Strafdrohungen ausgestattet werden sollten (zB § 51 DSG 2000, § 120a Abs 2a).

Auffällig häufig fehlt überhaupt eine Beschreibung sozial inadäquater Handlungen im objektiven Tatbestand, weshalb das deliktsspezifische Unrecht von der inneren Einstellung des Täters abhängt (vgl zB § 107a, § 148a, § 208a StGB bzw § 51 DSG 2000). Eine solche legistische Praxis lässt an ein Gesinnungsstrafrecht denken und stellt die notwendige hinreichende Bestimmtheit insb von Strafnormen in Frage.

Dass in vielen Einzelfällen der Beweis des Vorliegens der subjektiven Tatseite, insb was neben dem Tatbildvorsatz eine entsprechende Anzahl überschießender Innentendenzen mit den unterschiedlichsten Stärkegraduierungen anlangt (vgl §§ 118a, 119, 119a, 126c, 208a, 225a StGB bzw § 51 DSG 2000), nur schwer gelingen mag, ist nur der Vollständigkeit halber zu erwähnen.

§ 126c vereint überhaupt eine Vielzahl von Auffälligkeiten, welche die Norm weitgehend in ihrer Funktion als Vorbereitungsdelikt zu einem »zahnlosen Dasein« verkommen lassen. Punkten könnte § 126c wohl eher als Auffangtatbestand, da die sehr hohen Anforderungen der Hauptdelikte, denen § 126c vorgelagert ist, deren Anwendbarkeit in der Praxis sehr oft verhindern dürften. Daraus folgt, dass bei einem diesbezüglichen Versagen der Strafbarkeit der Hauptdelikte, zumindest § 126c diese rechtspolitische Lücke schließen könnte bzw aus Sachlichkeitsgründen sogar schließen müsste. Doch auch § 126c Abs 1 birgt tatbestandliche Einschränkungen, die zurzeit auch die Anwendbarkeit dieser Norm sehr stark begrenzen. Tatobjekte iSd § 126c Abs 1 Z 1 können nur Computerprogramme oder vergleichbare Vorrichtungen sein, die explizit zur Begehung der tatbildlich genannten Delikte hergestellt oder adaptiert wurden. Sogenannte »Dual-use Devices«, die sowohl für illegale als auch legale Zwecke eingesetzt werden können (zB typische Administratorwerkzeuge) scheiden a priori als Tatobjekte des § 126c Abs 1 Z 1 aus.

Das gilt im Übrigen auch für die spezielle Vorrichtung, die im Fall der § 119 Abs 1 bzw § 119a Abs 1 Fall 1 benützt werden muss. Werden etwa zur Nachrichten- bzw Datenspionage Standard-Programme verwendet, die eine solche Aufgabe ebenfalls erfüllen können, mangelt es schon an einer tatbildlichen Vorrichtung.

Um auf moderne Bedrohungen adäquat zu reagieren, wäre es notwendig, Qualifikationstatbestände zu normieren, welche – vergleichbar mit § 126 Abs 1 Z 5 – insb Angriffe auf IKT-Systeme oder Daten der öffentlichen Sicherheit, Katastrophenschutz, Gesundheitsdienst oder IKT-Infrastruktur, die der öffentlichen Versorgung (Wasser, Elektrizität, Wärme usw) dienen, qualifizieren. Freilich wären analog zur Durchdringung vieler Lebensbereiche mit IKT auch Qualifikationen im Sinne anderer Ziffern des § 126 Abs 1 denkbar. Auch kann dem Aufwertungsbestreben des Datenschutzes im Strafrecht Rechnung tragend eine Qualifikationsbestimmung des § 51 DSG 2000 in Bezug auf die inkriminierte Verwendung »sensibler Daten« angedacht werden, welche mit strengerer Strafe bedroht sein sollte.

Diese beispielhafte Aufzählung tatbestandlicher und gesetzestechnischer Unzulänglichkeiten zeugen von Handhabungsschwierigkeiten bezüglich der gesetzlichen Erfassung von IKT-Phänomenen. Dies spiegelt sich auch in den sehr geringen Verurteilungszahlen wider, wobei

letztlich überwiegend eine bloße Symbolwirkung – im Sinne eines umfangreichen, mit teilweise hohen Strafdrohungen versehenen Computerstrafrechts, das allerdings kaum Anwendung findet – verbleibt. Ob damit aber eine effektive generalpräventive Wirkung verbunden ist, ist mehr als fraglich. Meines Erachtens sollten viele der hier untersuchten Delikte seitens des Gesetzgebers – zumindest im Umfang der in dieser Arbeit vorgeschlagenen Empfehlungen – sachgerecht novelliert werden.

E. Zur Rechtsterminologie

Generell ist anzumerken, dass sich der Strafrechtgesetzgeber deutlicher um eine sachgerechte und eindeutige Terminologie bemühen sollte. In § 51 DSG 2000 werden klassische Tathandlungen des Strafrechts in ein Sachgesetz überstellt, welches diesbezüglich allerdings seine eigenen Begrifflichkeiten besitzt. Darüber hinaus stehen gleichlautende Termini in diesen Gesetzen für unterschiedliche Begriffe. Eine ähnliche Problematik tritt iZm den Begriffen »Nachricht« bzw »Inhalt einer Nachricht« und § 119 bzw § 120 Abs 2a auf. Dabei werden trotz mehrfachen Verweises auf das TKG diese Begrifflichkeiten strafrechtsautonom ausgelegt.

In jüngerer Zeit werden Alltagsbegriffe – wie »Internet« oder »Informationen« – als Legaltermini in Deliktstatbestände (§ 207a Abs 3a, § 278f) übernommen, wobei es gerade bei diesen beiden Begriffsbezeichnungen nicht gerechtfertigt erscheint, diese ohne Legaldefinition als eindeutig klar und hinreichend bestimmt vorauszusetzen und daher in die Terminologie des Kernstrafrechts aufzunehmen.

Die sprachliche Wendung in § 208a Abs 1 und 1a »unter Verwendung eines Computersystems« ist gerade deshalb so bemerkenswert, weil sie aufgrund ihres Wortlauts entgegen der Intention des Gesetzgebers auch konventionelle Handlungen erfasst, bei denen ein Computersystem gerade ohne seine IKT-Spezifika, nur als ein spezieller Gegenstand Verwendung finden kann. Wie auch in anderen Tatbeständen, in denen der Gesetzgeber die Kommunikation via Computersystem erfassen will (vgl §§ 119, 119a), sollte der hier kritisierte Wortlaut des § 208a durch die Formulierung »im Wege eines Computersystems« ersetzt werden.

Das Problem mit unsachlicher und mehrdeutiger Rechtsterminologie ist im hier interessierenden Themengebiet besonders stark ausgeprägt und verbreitet. Dass sich Legisten mit der Ausformulierung IKT-spezifischer Tatbestände schwer tun, liegt vermutlich ebenfalls in der IKT und deren spezifischer Terminologie begründet. Dennoch widerspricht die Verwendung unscharfer, mehrdeutiger oder bereits in anderen Sachgesetzen anders verwendeter Begriffsbezeichnungen den Prinzipien der Einheit der Rechtssprache und der Rechtssicherheit und sollte folglich bereinigt und in weiterer Folge vermieden werden. Gerade im Strafrecht, das als ultima ratio-Instrument des Gesetzgebers die schärfsten staatlichen Eingriffe in die Freiheit der Bürger ermöglicht, um einen effektiven Rechtsgüterschutz sicherzustellen, sollte der Terminologie und Bestimmtheit der Tatbestände seitens des Gesetzgebers besonderes Augenmerk gewidmet werden.

4 Ausblick »StRÄG 2015«

Mit dem Strafrechtsänderungsgesetz 2015 werden die seit dem Inkrafttreten des StGB 1975 eingetretenen Veränderungen der gesellschaftlichen Rahmenbedingungen, insbesondere der Werthaltungen, aber auch des technischen Fortschrittes im gerichtlichen Strafrecht so abgebildet, dass es auf gesellschaftliche Akzeptanz und Verständnis stößt und auf diese Weise in vollem Umfang die erforderliche Präventionswirkung entfalten kann. Unter anderem wird mit dem StRÄG 2015 auch die Richtlinie 2013/40/EU umgesetzt. Nachfolgend werden die Änderungen im Bereich des Computerstrafrechts, welche mit 01.01.2016 in Kraft treten werden, überblickshaft angesprochen.

A. Einführung einer Legaldefinition der »kritischen Infrastruktur« in § 74

Gem Art 9 Abs 4 lit c RL 2013/40/EU haben die Mitgliedstaaten die erforderlichen Maßnahmen zu treffen, um sicherzustellen, dass Straftaten iSd Artikel 4 und 5 mit Freiheitsstrafen im Höchstmaß von mindestens fünf Jahren geahndet werden, wenn sie gegen ein Informationssystem einer kritischen Infrastruktur verübt wurden. Da der Begriff der »kritischen Infrastruktur« in mehreren Bestimmungen des StGB enthalten sein soll, wurde die Einführung einer allgemeinen Legaldefintion in § 74 Abs 1 Z 11 als sinnvoll erachtet.[2724]

Die europäische Vorgabe versteht darunter Anlagen, Systeme oder deren Teile, die von wesentlicher Bedeutung für die Aufrechterhaltung grundlegender gesellschaftlicher Funktionen, der Gesundheit, der Sicherheit und des wirtschaftlichen oder sozialen Wohlergehens der Bevölkerung sind, wie etwa Kraftwerke, Verkehrsnetze oder staatliche

2724 Siehe ErlRV 689 BlgNR XXV. GP, 16.

Netze, und deren Störung oder Zerstörung erhebliche Auswirkungen auf einen Mitgliedstaat hätte, da diese Funktionen nicht aufrechterhalten werden könnten.[2725] Mit dieser Definition beziehen sich die Richtlinieneber schlüssigerweise auf Art 2 lit a der Richtlinie 2008/114/EG über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern.[2726]

Der zukünftige § 74 Abs 1 Z 11 definiert die »kritische Infrastruktur« als »Einrichtungen, Anlagen, Systeme oder Teile davon, die eine wesentliche Bedeutung für die Aufrechterhaltung der öffentlichen Sicherheit und der Landesverteidigung, die Funktionsfähigkeit öffentlicher Informations- und Kommunikationstechnologie, die Verhütung oder Bekämpfung von Katastrophen, den öffentlichen Gesundheitsdienst, die öffentliche Versorgung mit Wasser, Energie sowie lebenswichtigen Gütern, des öffentlichen Abfallentsorgungs- und Kanalwesens oder den öffentlichen Verkehr haben.«[2727]

In den GMat wird zum Begriff der »Informations- und Kommunikationstechnologie« angemerkt, dass jegliche Kommunikationsinstrumente oder Kommunikationsanwendungen, einschließlich Radio, Fernsehen, Mobiltelefonie, Hardware und Software für Computer und Netzwerke, Satellitensysteme sowie die verschiedenen Dienstleistungen und Anwendungen, die damit verbunden sind, davon umfasst seien. Als Beispiele werden die von staatlicher Seite geführten Rechenzentren oder der gesamte elektronische Zahlungsverkehr genannt.[2728]

Weiters wird klargestellt, dass der Begriff »öffentlich« idZ dahingehend zu verstehen ist, dass die kritische Infrastruktur der Allgemeinheit zugänglich bzw für diese bestimmt ist, unabhängig davon, ob ein Privater oder der Staat Betreiber der kritischen Infrastruktur ist.[2729] Dieser Hinweis sorgt jedenfalls für Klarheit hins der sachlich unumgänglichen Einbeziehung der vielen privaten Betreiber kritischer Infrastrukturen (vgl die Anbieter in den Bereichen Telekommunikation, Internetprovider, Radio, Fernsehen, Energie, Abfallentsorgung). Es kommt daher letztlich ausschließlich auf die wesentliche Bedeutung

2725 Vgl ErwG 4 RL 2013/40/EU.
2726 Richtlinie 2008/114/EG des Rates vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern, ABl L 2008/345, 75.
2727 RV 689 BlgNR XXV. GP, 3.
2728 Siehe ErlRV 689 BlgNR XXV. GP, 16.
2729 Vgl ErlRV 689 BlgNR XXV. GP, 16; weiters bereits ErlRV 99 BlgNR XXV. GP, 13.

der Infrastruktur für die Aufrechterhaltung grundlegender gesellschaftlicher Funktionen und insb deren Zugänglichkeit bzw Zweckbestimmung für die Allgemeinheit an.

Als Beispiele für kritische Infrastrukturen können wohl folgende genannt werden:

- Öffentliche Sicherheit und Landesverteidigung: Alarmsysteme der Polizei, der Zollbehörden und des Bundesheers, Notrufanlagen, Radarstationen, Waffensysteme, militärische Luftfahrt usw.
- Öffentliche Informations- und Kommunikationstechnologie: Telekommunikationssysteme, Internetproviding, Rundfunk, Fernsehen, e-Government- und e-Justice-Anwendungen, staatlich geführte Rechenzentren, elektronischer Zahlungsverkehr, Bankenwesen, Finanzmarkt udgl.
- Verhütung oder Bekämpfung von Katastrophen: Katastrophenhilfsdienste, Zivilschutz, Notfall- und Katastrophenmedizin, Rettungsleitstellen, Hubschrauberrettungsdienste und der jeweiligen Organisationsstrukturen uÄ.
- Öffentlicher Gesundheitsdienst: medizinische Einrichtungen, Rettungsdienste, aber nach Klarstellung in den GMat[2730] auch Sozialversicherungsträger.
- Öffentliche Versorgung mit Wasser, Energie sowie lebenswichtigen Gütern: zB Trinkwasser- und Lebensmittelversorgung, Elektrizitätssysteme, Energieversorgungseinrichtungen (wie etwa Kraftwerke oder die Öl- bzw Gasversorgung).
- Öffentliches Abfallentsorgungs- und Kanalwesen[2731]: Müllverbrennungsanlagen, Abfallsortierungs- bzw -deponierungssysteme, Abwasserentsorgungsanlagen usw.
- Öffentlicher Verkehr: Ampelsteuerungen bzw Verkehrsleitsysteme für Straßenverkehr (insb Bahn-, Bus- und Straßenbahnbetrieb), Tunnelanlagen, Flugsteuerungsprogramme uÄ.

2730 Siehe ErlRV 689 BlgNR XXV. GP, 16.

2731 Weil nach den Erl diesen Bereichen insbesondere in großen Städten eine wesentliche kommunale und im allgemeinen Interesse liegende Bedeutung zukommt (ErlRV 689 BlgNR XXV. GP, 16).

B. Schaffung von Qualifikationsbestimmungen betreffend die Kritische Infrastruktur

In Umsetzung des Art 9 Abs 4 RL 2013/40/EU werden Qualifikationsbestimmungen bezüglich kritischer Infrastrukturen iSd neuen Definition des § 74 Abs 1 Z 11 nicht nur für die Datenbeschädigung (§ 126a) und die Störung der Funktionsfähigkeit eines Computersystems (§ 126b) vorgesehen, sondern auch iZm dem Widerrechtlichen Zugriff auf ein Computersystem (§ 118a), sofern die Tat in Bezug auf ein Computersystem begangen wird, das einen wesentlichen Bestandteil der kritischen Infrastruktur (§ 74 Abs 1 Z 11) darstellt.[2732] In Anpassung an die neu geschaffene Definition in § 74 Abs 1 Z 11 wird auch die qualifizierte Sachbeschädigung in § 126 Abs 1 Z 5 nicht nur textlich auf »an einem wesentlichen Bestandteil der kritischen Infrastruktur (§ 74 Abs. 1 Z 11)« abgeändert, sondern durch die umfassendere Legaldefinition bezüglich des öffentlichen Abfallentsorgungs- und Kanalwesens wohl auch inhaltlich ausgedehnt.

Die Adaptierung des § 126 Abs 1 Z 5 schlägt sich auch auf den neu gestalteten § 274[2733] (Schwere gemeinschaftliche Gewalt) durch, der nunmehr neben § 126 Abs 2 konkret auch auf § 126 Abs 1 Z 5 in seiner neuen Fassung verweist. Dies bewirkt, dass in Hinkunft jede andere qualifizierte Form der Sachbeschädigung[2734] nicht mehr zur Strafbarkeit iSd § 274 führt.[2735]

Der Schwere Diebstahl (§ 128) wird aufgrund von Sachlichkeitsüberlegungen[2736] ebenfalls um einen entsprechenden Qualifikationstatbestand erweitert, indem der bisherige Wortlaut des § 128 Abs 1 Z 4 durch »an einem wesentlichen Bestandteil der kritischen Infrastruktur (§ 74 Abs. 1 Z 11), oder« ersetzt und die zuvor in Z 4 normierte erste Wertqualifikation (mit dem ebenfalls generell angehobenen Betrag iHv € 5.000,–[2737]) in eine neue Z 5 aufgenommen werden soll.

2732 Siehe zu den einzelnen Bestimmungen gleich im Anschluss.
2733 Bislang unter der Bezeichnung »Landfriedensbruch« bekannt.
2734 Ebenso wie eine leichte Körperverletzung.
2735 Siehe dazu ErlRV 689 BlgNR XXV. GP, 40.
2736 ErlRV 689 BlgNR XXV. GP, 23.
2737 Siehe dazu im Anschluss.

C. Neufassung des Widerrechtlichen Zugriffs auf ein Computersystem (§ 118a)

Wie bereits oben[2738] zum Widerrechtlichen Zugriff auf ein Computersystem (§ 118a) aufgezeigt wurde, handelt es sich dabei generell um eine umstrittene Bestimmung. In den Erl wird bezüglich einer Novellierung dieser Norm ausgeführt, dass bislang nicht alle Fälle des Phänomens »Hacking« – wie etwa auch die Einrichtung sog »Bot-Netzwerke« – strafrechtlich erfasst sind, sondern nur jene, bei denen in Spionage-, Benützungs- oder Verbreitungs- sowie Bereicherungs- oder Schädigungsabsicht gehandelt werde.[2739]

> § 118a[2740] (1) Wer sich zu einem Computersystem, über das er nicht oder nicht allein verfügen darf, oder zu einem Teil eines solchen durch Überwindung einer spezifischen Sicherheitsvorkehrung im Computersystem in der Absicht Zugang verschafft,
>
> 1. sich oder einem anderen Unbefugten Kenntnis von personenbezogenen Daten zu verschaffen, deren Kenntnis schutzwürdige Geheimhaltungsinteressen des Betroffenen verletzt, oder
>
> 2. einem anderen durch die Verwendung von im System gespeicherten und nicht für ihn bestimmten Daten, deren Kenntnis er sich verschafft, oder durch die Verwendung des Computersystems einen Nachteil zuzufügen,
>
> ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.
>
> (2) Wer die Tat in Bezug auf ein Computersystem, das ein wesentlicher Bestandteil der kritischen
>
> Infrastruktur (§ 74 Abs. 1 Z 11) ist, begeht, ist mit Freiheitsstrafe bis zu zwei Jahren zu bestrafen.
>
> (3) Der Täter ist nur mit Ermächtigung des Verletzten zu verfolgen.
>
> (4) Wer die Tat nach Abs. 1 im Rahmen einer kriminellen Vereinigung begeht, ist mit Freiheitsstrafe bis zu zwei Jahren, wer die Tat nach Abs. 2 im Rahmen einer kriminellen Vereinigung begeht, mit Freiheitsstrafe bis zu drei Jahren zu bestrafen.

2738 S 74 ff.
2739 Siehe ErlRV 689 BlgNR XXV. GP, 20.
2740 RV 689 BlgNR XXV. GP in der Fassung gem der Änderungen im Plenum des NR gegenüber dem ursprünglichen Entwurf (9403 BlgBR XXV. GP, 6).

Der objektive Tatbestand definiert inhaltlich unverändert das Sich-Zugang-Verschaffen zu einem Computersystem, über das der Täter nicht oder nicht allein verfügen darf, oder zu einem Teil eines solchen durch Überwindung einer spezifischen Sicherheitsvorkehrung im Computersystem. Der subjektive Tatbestand wird allerdings durch die Modifikation der überschießenden Innentendenzen deutlich abgeändert. § 118a Abs 1 Z 1 verlangt nunmehr vom Täter im Handlungszeitpunkt die Absicht, sich oder einem anderen Unbefugten Kenntnis von personenbezogenen Daten zu verschaffen, deren Kenntnis schutzwürdige Geheimhaltungsinteressen des Betroffenen verletzt. Damit referenziert diese 1. Alternative der überschießenden Innentendenzen auf »personenbezogene Daten« iSd § 4 Z 1 DSG 2000, an denen der Betroffene ein schutzwürdiges Geheimhaltungsinteresse haben muss.

Zum Begriff der »personenbezogenen Daten« hat unlängst der OGH ausgeführt, dass darunter »Informationen (im weitesten Sinn)« zu verstehen sind, die mit einer Person in Verbindung stehen oder gebracht werden können.[2741] Ob ein schutzwürdiges Geheimhaltungsinteresse an diesen Informationen besteht, ist schlüssigerweise iSd § 1 Abs 1 zweiter Satz DSG 2000 zu prüfen und lediglich dann auszuschließen, wenn Daten infolge ihrer allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind.[2742]

Als äußerst begrüßenswert ist das explizite Abstellen auf die »Kenntnisverschaffung« dieser Daten hervorzuheben, da es schließlich um den Geheimnischarakter solcher personenbezogener Informationen geht, der bereits mit Kenntnisnahme des Datengeheimnisses durchbrochen wird und nicht erst durch eine »körperliche Gewahrsamsverschaffung«.[2743] Auch kommt es nun – im Gegensatz zur aktuellen Fassung – nicht mehr darauf an, dass es der Täter beabsichtigen muss, die ausspionierten Daten »selbst zu benützen, einem anderen zugänglich zu machen oder zu veröffentlichen«, um sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen. In der neuen Fassung wird lediglich auf eine

2741 OGH 24.11.2014, 17 Os 40/14g (17 Os 41/14d) = jusIT 2015/30, 76 *(Bergauer)*.

2742 Vgl zum schutzwürdigen Geheimhaltungsinteresse jüngst OGH 24.11.2014, 17 Os 40/14g (17 Os 41/14d) = jusIT 2015/30, 76 *(Bergauer); Bernreiter,* Zum »StRÄG 2015« und den Änderungen im Bereich des Computerstrafrechts, jusIT 2015/52, 128 (128).

2743 Siehe dazu bereits ausf an mehreren Stellen oben.

(vom Täter anstrebte) Nachteilszufügung durch die anvisierte Geheimnisverletzung bezüglich schutzwürdiger personenbezogener Daten abgestellt, was die Strafbarkeit gegenüber der alten Fassung nun deutlich aber auch sachgerecht ausdehnt.

Die neugeschaffene Z 2 stellt nun auf die durch den Täter angestrebte (missbräuchliche) Daten- bzw Computersystemverwendung ab und verlangt, dass der Täter bei der Zugangsverschaffung zu einem fremden Computersystem in der Absicht handelt, »einem anderen durch die Verwendung von im System gespeicherten und nicht für ihn bestimmten Daten, deren Kenntnis er sich verschafft, oder durch die Verwendung des Computersystems einen Nachteil zuzufügen«. Damit soll dem Phänomen der »Bot-Netzwerke« Rechnung getragen werden.[2744]

In sprachlicher Hinsicht fällt auf, dass einmal nur vom »System« gesprochen wird, wobei nur ein »Computersystem« iSd § 74 Abs 1 Z 8 gemeint sein kann. Es wäre hier dennoch schon aus Homogenitätsgründen angebracht, den Terminus »Computersystem« anstelle des nicht in § 74 definierten Begriffs »System« zu verwenden. Darüber hinaus wird in der Definition des Tatbestands zweimal der Terminus »Verwendung« (einmal in Bezug auf Daten und ein weiteres Mal bezüglich des Computersystems) gebraucht, wobei dieser (nur) hins der »Datenverwendung« sachgerecht – den GMat zufolge – im Sinn des § 4 Z 8 DSG 2000[2745] auszulegen sei. Was die »Verwendung des Computersystems« anlangt, wäre wohl die Beibehaltung des Terminus »Benützen« sachgerechter gewesen, um nicht mit den hier unzutreffenden »Verwendungsmöglichkeiten von Daten« iSd DSG 2000 zu konfligieren.

Unter der »Verwendung des Computersystems« sind sämtliche Handhabungs- und Benützungsmöglichkeiten vom Wortlaut umfasst und nicht nur die rein computertechnische Bedienung. So wäre es denkbar, dass sich der Täter vor Ort durch Überwindung einer spezifischen, systemimmanenten Sicherheitsvorkehrung Zugang zu einem fremden Computersystem verschafft, um die körperlichen Bestandteile dieses Systems zum Nachteil des Eigentümers (zB durch deren Verkauf) zu »verwenden«.

2744 ErlRV 689 BlgNR XXV. GP, 21.

2745 Darunter versteht man »jede Art der Handhabung von Daten, also sowohl das Verarbeiten (Z 9) als auch das Übermitteln (Z 12) von Daten«.

Das erklärte gesetzgeberische Ziel[2746] ist allerdings die Erfassung des Phänomens der Einrichtung sog »Bot-Netzwerke«, weshalb es rein auf die computertechnische Nutzung des Systems ankommt. Aus diesem Grund ist der diesbezügliche überschießende Wortlaut dieser Variante des erweiterten Vorsatzes der ratio legis entsprechend, dh teleologisch, auf die »computertechnische Verwendung« zu reduzieren.

Interessant erweist sich Z 2 erster Fall auch in Bezug auf die Apposition »deren Kenntnis er sich verschafft«. Damit wird die Strafbarkeit in diesem Fall darauf eingeschränkt, dass es dem Täter darauf ankommen muss, einem anderen durch die Verwendung von im System gespeicherten und nicht für ihn bestimmten Daten, deren Kenntnis »er« sich verschafft, einen Nachteil zuzufügen. Übermittelt der Täter daher nach tatbestandsgemäßer Zugangverschaffung solche im System gespeicherten Daten lediglich pauschal einem Dritten, der sich Kenntnis von den Daten dieses Systems verschaffen will, ohne dass sich aber der Täter selbst »Kenntnis« von diesen Daten verschafft, macht er sich nach dieser Bestimmung nicht strafbar.

Die Verwirklichung des Tatbestands nach § 118a Abs 1 (Z 1 bzw Z 2) ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen bedroht.

In einem neuen Abs 2 des § 118a findet sich eine Qualifikation hins der Begehung von Taten nach Abs 1 in Bezug auf ein Computersystem, welches einen wesentlichen Bestandteil der kritischen Infrastruktur (iSd § 74 Abs 1 Z 11) darstellt. In diesem Fall beträgt die Strafdrohung bis zu zwei Jahre Freiheitsstrafe.

§ 118a Abs 4 normiert zwei weitere Qualifikationsbestimmungen, wobei einerseits die Tatbegehung nach Abs 1 im Rahmen einer kriminellen Vereinigung (nur mehr[2747]) mit einer Strafdrohung von bis zu zwei Jahren verbunden ist. Andererseits wurde eine neue Qualifikationsbestimmung bezüglich Taten nach Abs 2 im Rahmen einer kriminellen Vereinigung geschaffen, die eine Strafdrohung von bis zu drei Jahre Freiheitsstrafe beinhaltet.

Der Widerrechtliche Zugriff auf ein Computersystem (§ 118a) bleibt aber für Abs 1 und Abs 2 unverändert ein Ermächtigungsdelikt, wobei sich diese Anordnung nunmehr in Abs 3 befindet.

2746 ErlRV 689 BlgNR XXV. GP, 21.

2747 Aktuell ist bei Tatbegehung als Mitglied einer kriminellen Vereinigung eine Freiheitsstrafe bis zu drei Jahren vorgesehen.

Die Qualifikationsbestimmung des § 118a Abs 4 stellt hingegen ein Offizialdelikt dar.

D. Erweiterung bzw Abänderung der Qualifikationen der Datenbeschädigung (§ 126a)

§ 126a Abs 2 normiert in der neuen Fassung nur mehr die erste Wertgrenze, die – ebenfalls durch das StRÄG 2015 generell im Bereich der Vermögensdelikte[2748] – von € 3.000,– auf € 5.000,– angehoben wurde. Führt der Täter daher nunmehr durch die Tat an den Daten einen € 5.000,– übersteigenden Schaden herbei, ist er mit Freiheitsstrafe bis zu zwei Jahren zu bestrafen. Die bislang ebenfalls vorgesehene Geldstrafenalternative entfällt durch das StRÄG 2015 generell bei den Delikten, die eine Freiheitsstrafe von bis zu zwei bzw drei Jahren oder die Verhängung einer Geldstrafe vorsahen, mit der Begründung, dass ein solche nicht als äquivalent zu einer Strafdrohung von bis zu zwei bzw drei Jahren angesehen werden kann.[2749]

Bezüglich der Umsetzung der RL 2013/40/EU bestand lediglich noch hins Art 9 Abs 3 und 4 Änderungsbedarf im nationalen Recht, weshalb in § 126a ein neuer Abs 3 eingeführt wird, dessen Qualifikationstatbestand denjenigen erfasst, der durch die Tat viele Computersysteme unter Verwendung eines Computerprogramms, eines Computerpasswortes, Zugangscodes oder vergleichbarer Daten, die den Zugriff auf ein Computersystem oder einen Teil davon ermöglichen, sofern diese Mittel nach ihrer besonderen Beschaffenheit ersichtlich dafür geschaffen oder adaptiert wurden, beeinträchtigt. In diesem Fall ist die Tat mit bis zu drei Jahren Freiheitsstrafe bedroht.

Der nationale Gesetzgeber hat anstelle der Diktion des Art 9 Abs 3 RL 2013/40/EU »beträchtliche Anzahl« auf »viele« abgestellt, worunter den GMat zufolge eine Zahl von ca 30 zu verstehen sei.[2750] Um eine Gleichstellung mit § 126c zu erreichen und nunmehr auch zB elektronische Fingerprints erfassen zu können, wurden die Computerpasswörter und Zugangscodes auch in § 126a Abs 3 um »vergleichbare Daten« erweitert.[2751]

2748 Siehe dazu ErlRV 689 BlgNR XXV. GP, 21.
2749 ErlRV 689 BlgNR XXV. GP, 11.
2750 Siehe ErlRV 689 BlgNR XXV. GP, 22.
2751 In Art 7 lit b RL 2013/40/EU ist von »ähnlichen Daten« die Rede.

Die Beifügung »sofern diese Mittel nach ihrer besonderen Beschaffenheit ersichtlich dafür geschaffen oder adaptiert wurden« iZm Computerpasswörtern, Zugangscodes oder vergleichbaren Daten fällt dabei besonders in Auge. Es fragt sich, ob man einem Computerpasswort oder Zugangscode (zB einem PIN-Code »1234«), die besondere Beschaffenheit zur Beeinträchtigung vieler Computersysteme ansehen kann. Wird etwa ein Passwort widerrechtlich mittels »Brute force«-Methoden errechnet[2752], so unterscheidet es sich nicht vom tatsächlichen Original. Sachgerechter wäre es daher wohl diese besondere Beschaffenheit, sofern man eine solche nicht schon durch die generelle Geeignetheit näher definieren wollte[2753], lediglich für Computerprogramme zu verlangen, wie es auch in Art 7 RL 2013/40/EU der Fall ist.

Interessanter Weise ändert sich nun in dieser neu geschaffenen Qualifikationsbestimmung der »Datenbeschädigung« das Tatobjekt. Denn durch die Tat müssen nun viele »Computersysteme« beeinträchtigt werden, wobei sich auch der Wortlaut nicht mehr – wie noch in der aktuellen Fassung des § 126a Abs 2 oder der neu formulierte Abs 2 – auf »die Tat an den Daten« bezieht. Man kann deshalb davon ausgehen, dass es in diesem Qualifikationsfall nicht mehr auf den unmittelbar an den Daten herbeigeführten Schaden ankommt. Unterstützt wird eine solche Sichtweise wohl durch die im gegenständlichen Zusammenhang neue Tathandlung des »Beeinträchtigens«. Die Kennzeichnungskraft dieses Terminus bezüglich einer der Datenbeschädigung vergleichbaren Schädigung ist dabei äußert schwach. So wäre es durchaus denkbar, dass mittels eines Schadprogramms entsprechende Dienste eines Servers verändert werden, wodurch weitere mit diesem Server verbundene Systeme nun ebenfalls diese Serverdienste nicht mehr ordnungsgemäß in Anspruch nehmen können. Der bestimmungsgemäße Betrieb dieser weiteren Systeme ist daher »beeinträchtigt«. Dadurch, dass es offenbar in diesem Fall nicht mehr auf »die Tat an den Daten« ankommt, drängt sich wohl aus rechtspolitischer Sicht die Frage auf, ob ein solcher Angriff auf ein Computersystem, der mittelbar auch eine Beeinträchtigung 30 weiterer damit verbundener Computersysteme iSd § 74 Abs 1 Z 8 (zB auch Drucker, externe Festplatten

2752 Siehe oben.

2753 Siehe zur Problematik der »Dual-use Devices« oben zu den Ausführungen zu § 126c.

usw[2754]) herbeiführt, tatsächlich schon unter die Qualifikationsbestimmung fallen soll, die eine Strafdrohung von bis zu drei Jahren Freiheitsstrafe vorsieht, selbst wenn die »Beeinträchtigung« der »Daten« dieser angeschlossenen Systeme nicht auch die Tatbestandsmäßigkeit im Sinn des Abs 1 herstellt.

Darüber hinaus wird dieser Qualifikationstatbestand dem Wortlaut nach auch erfüllt, wenn der Täter mittels eines Schadprogramms lediglich 30 Computerprogramme löscht, die auf einem einzigen PC gespeichert sind, da auch ein (aktives) Computerprogramm ein Computersystem iSd § 74 Abs 1 Z 8 sein kann.[2755] Es bleibt hier wohl der Praxis überlassen, in welche Richtung diese Qualifikationsbestimmung ausgelegt wird.

Der neu eingeführte § 126a Abs 4 enthält nun drei Qualifikationstatbestände, deren Verwirklichung mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren bedroht ist. Z 1 beinhaltet die zweite Wertgrenze, welche – wie insgesamt für den Bereich der Vermögensdelikte – auf € 300.000,– angehoben wurde. Es fällt auch hier auf, dass gegenüber der ersten Wertqualifikation in § 126a Abs 2 nF nicht (mehr) auf den Schaden abstellt wird, der durch »die Tat an den Daten« herbeiführt wird. Es dürfte sich hier aber um ein Redaktionsversehen handeln, da es mE keinen erkennbaren Grund gibt, warum zwar die erste Wertqualifikation lediglich den unmittelbaren Schaden an den Daten erfasst, die zweite Wertqualifikation aber auch mittelbare Schäden, die durch die Tat versucht werden, einbeziehen soll.

§ 126a Abs 4 Z 2 nF stellt nun auf wesentliche Bestandteile der kritischen Infrastruktur (§ 74 Abs 1 Z 11) ab, wobei es auch hierfür ausreicht, dass diese wesentlichen Bestandteile »beeinträchtigt« werden. Die Tathandlung des »Beeinträchtigens« ist hierbei mE – wie auch schon iZm § 126a Abs 3 nF – im Sinne der Datenbeschädigungsmodalitäten des Abs 1 auszulegen. Als problematisch könnte sich die Beurteilung herausstellen, was als »wesentlicher« Bestandteil einer kritischen Infrastruktur iZm mit Datenbeschädigungshandlungen angesehen wird.

Dass iZm mit der Datenbeschädigung (§ 126a) als Bestandteile weniger körperliche Gegenstände (vgl § 126 Abs 1 Z 5 nF) als unkörperliche Programme einer kritischen Infrastruktur in Frage kommen, liegt

2754 Siehe zum Begriff »Computersystem« iSd § 74 Abs 1 Z 8 mehrfach im Hauptteil dieser Arbeit.

2755 Siehe dazu oben.

auf der Hand. Wesentlich sind solche Bestandteile immer dann, wenn sie für den bestimmungsgemäßen Betrieb unentbehrlich sind.

§ 126a Abs 4 Z 3 nF bezieht sich auf den vormals in § 126a Abs 2 dritter Fall normierten Qualifikationsfall der Tatbegehung als Mitglied einer kriminellen Vereinigung.

E. Erweiterung bzw Abänderung der Qualifikationen der Störung der Funktionsfähigkeit eines Computersystems (§ 126b)

§ 126b Abs 2 nF wurde auf den Qualifikationsfall beschränkt, in dem der Täter durch die Tat eine längere Zeit andauernde Störung der Funktionsfähigkeit eines Computersystems herbeiführt. Für diesen Fall ist eine Freiheitsstrafe bis zu zwei Jahren angedroht. Die bislang ebenfalls angedrohte Geldstrafe wird auch hier durch das StRÄG 2015 ersatzlos gestrichen.[2756]

Nach § 126b Abs 2 nF wird nunmehr ein neuer Qualifikationsfall in Abs 3 eingefügt, der für denjenigen eine Freiheitsstrafe bis zu drei Jahren androht, der durch die Tat viele Computersysteme unter Verwendung eines Computerprogramms, eines Computerpasswortes, eines Zugangscodes oder vergleichbarer Daten, die den Zugriff auf ein Computersystem oder einen Teil davon ermöglichen, sofern diese Mittel nach ihrer besonderen Beschaffenheit ersichtlich dafür geschaffen oder adaptiert wurden, schwer stört.

Der Wortlaut dieses Qualifikationstatbestands entspricht im Wesentlichen dem des § 126a Abs 3, wobei hier zutreffender Weise die Bezeichnung der Tathandlung des Grunddelikts (»schwer stören«) expressis verbis in den Gesetzestext Eingang gefunden hat.[2757]

Für weitere Anmerkungen zu dieser Qualifikationsbestimmung kann auf die obigen Ausführungen zu § 126a Abs 3 nF verwiesen werden.

Dies gilt im Wesentlichen auch für den neu eingefügten § 126b Abs 4, der sich lediglich in Z 2 von § 126a Abs 4 dahingehend unterscheidet, dass »die Tat gegen ein Computersystem verübt« werden

2756 Siehe dazu ErlRV 689 BlgNR XXV. GP, 11.

2757 Dies ist im Übrigen auch ein Indiz dafür, dass wohl das »Beeinträchtigen« in § 126a Abs 3 iSd Datenbeschädigungsvarianten des Grunddelikts (§ 126a Abs 1) zu interpretieren ist.

muss, das ein wesentlicher Bestandteil der kritischen Infrastruktur (§ 74 Abs 1 Z 11) ist. Auch in diesem Fall kommt als Computersystem iSd § 74 Abs 1 Z 8 ein Computerprogramm (zB Server- bzw Webdienst) in Betracht, sofern dieses einen unentbehrlichen Bestandteil der kritischen Infrastruktur darstellt. Nach dieser Formulierung des Tatbestands muss allerdings das Zielsystem des Angriffs auch das System sein, das selbst einen wesentlichen Bestandteil der kritischen Infrastruktur bildet. Es reicht nicht aus, dass ein solches Computersystem lediglich durch einen Angriff auf ein anderes Computersystem (mittelbar) »beeinträchtigt« wird, das keine solche Eigenschaft aufweist.

F. Einführung eines neuen Straftatbestandes, die »Fortgesetzte Belästigung im Wege einer Telekommunikation oder eines Computersystems« (§ 107c)

§ 107c[2758] (1) Wer im Wege einer Telekommunikation oder unter Verwendung eines Computersystems in einer Weise, die geeignet ist, eine Person in ihrer Lebensführung unzumutbar zu beeinträchtigen, eine längere Zeit hindurch fortgesetzt

1. eine Person für eine größere Zahl von Menschen wahrnehmbar an der Ehre verletzt oder

2. Tatsachen oder Bildaufnahmen des höchstpersönlichen Lebensbereiches einer Person ohne deren Zustimmung eine für eine größere Zahl von Menschen wahrnehmbar macht,

ist mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bis zu 720 Tagessätzen zu bestrafen.

(2) Hat die Tat den Selbstmord oder einen Selbstmordversuch der im Sinn des Abs. 1 verletzten Person zu Folge, so ist der Täter mit Freiheitsstrafe bis zu drei Jahren zu bestrafen.

Zu § 107c wird in den GMat das Phänomen »Cybermobbing« angesprochen, welches für die betroffenen Personen eine extreme Belastung bedeute und in schweren Fällen zur systematischen Zerstörung der Persön-

2758 RV 689 BlgNR XXV. GP.

lichkeit des Opfers führen könne.[2759] Dieses Phänomen ist de lege lata nur in einzelnen Facetten bzw Teilhandlungen strafrechtlich erfasst (wie etwa Delikte gegen die Ehre, Nötigung, Gefährliche Drohung, Pornographische Darstellung Minderjähriger, Anbahnung von Sexualkontakten zu Unmündigen, Beharrliche Verfolgung). Den Erl zufolge sei der bisherige strafrechtliche Schutz für das Phänomen »Mobbing« ausreichend, nicht hingegen aufgrund der breiten Öffentlichkeitswirkung, die mit den Handlungen im Internet einhergehen können, für das Cybermobbing, bei dem es auch kaum eine Rückzugsmöglichkeit für die Opfer gäbe.[2760]

Unter der Formulierung »im Wege der Telekommunikation« versteht man dabei den technischen Vorgang des Aussendens, Übermittelns und Empfangens von Nachrichten aller Art in Form von Zeichen, Sprache, Bildern oder Tönen mit den diesem Zweck dienenden Einrichtungen (wie etwa E-Mails, SMS und Telefonanrufe). Für die Begriffsklärung »Computersystem« ist auf die allgemeine kernstrafrechtliche Definition des § 74 Abs 1 Z 8 zurückzugreifen. Die Wendung »Verwendung eines Computersystems« ist – wie auch schon iZm § 208a – wenig treffsicher. Vielmehr sollte auf die »informations- bzw computertechnische« Verwendung abgestellt werden.[2761]

Die GMat erachten jede Verminderung des Ansehens und der Achtung einer Person in den Augen der für sie maßgeblichen Umwelt als eine Verletzung an der Ehre. Schutzobjekt ist dabei nicht das subjektive »Ehrgefühl« des Betroffenen im Sinne einer größeren oder geringeren Selbstachtung, sondern die Ehre eines Menschen in ihrer objektiven Bedeutung.[2762]

Die Wendung »längere Zeit hindurch fortgesetzt« ist nach den GMat dynamisch nach den Umständen des Einzelfalles zu beurteilen. Demnach könne es in manchen Fällen genügen, dass jemand ein einziges Mal eine Belästigung im Sinne der Bestimmung begeht und dadurch bereits dieses Tatbestandsmerkmal erfüllt, da es sich bei § 107c StGB um ein Dauerdelikt handle, welches auch durch Unterlassen begangen werden kann (siehe dazu bereits oben zu § 107a).[2763]

2759 ErlRV 689 BlgNR XXV. GP, 19.
2760 Siehe ErlRV 689 BlgNR XXV. GP, 19.
2761 Siehe dazu die Ausführungen oben zu § 208a.
2762 Vgl ErlRV 689 BlgNR XXV. GP, 19.
2763 Siehe ErlRV 689 BlgNR XXV. GP, 19.

Als Beispiel werden in den GMat Nacktfotos genannt, die ohne Zustimmung des Abgebildeten im Internet veröffentlicht und längere Zeit hindurch nicht gelöscht werden. Der Täter muss dabei jedoch die Möglichkeit besitzen, die Bilder zu löschen. Bei weniger massiven Handlungen solle nach den Erl im Einzelfall geprüft werden, ob von einer »über längere Zeit fortgesetzten« Begehung gesprochen werden kann.[2764] Bei Belästigungen durch E-Mails, SMS oder Telefonanrufe seien dazu nach den GMat jedenfalls wiederholte Tathandlungen erforderlich.

Die Tathandlungen müssen darüber hinaus aber auch die Eignung haben, »eine Person in ihrer Lebensführung unzumutbar zu beeinträchtigen«. Eine tatsächliche Beeinträchtigung der Lebensführung ist nach den GMat nicht erforderlich. Bei der Beurteilung sei ein gemischter (objektiv-subjektiver) Maßstab anzulegen, bei dem es darauf ankomme, ob das Verhalten derart unerträglich ist, dass bei einer ex-ante-Betrachtung auch ein Durchschnittsmensch in dieser Situation auf Grund der Handlungen möglicherweise seine Lebensgestaltung geändert hätte.[2765]

Auch in diesem Fall ist auf die konkreten Umstände im Einzelfall abzustellen. Bei der Bekanntgabe oder Veröffentlichung von Tatsachen oder Bildaufnahmen des höchstpersönlichen Lebensbereichs könne eine solche Eignung jedoch nur dann angenommen werden, wenn eine solche (objektiv) geeignet ist, das Opfer bloßzustellen.[2766]

Bildaufnahmen des höchstpersönlichen Lebensbereichs schließen nach den Erl auch Wohnräume des Opfers und Videoaufnahmen mit ein, wobei die Eingriffe in die Intimsphäre zumindest für eine größere Zahl von Menschen (etwa 10) wahrnehmbar sein müssen.[2767]

Was das Konkurrenzverhältnis von § 107c zu § 107a betrifft, so wird in den Erl darauf hingewiesen, dass aufgrund der grundsätzlich unterschiedlichen Fallkonstellationen regelmäßig echte Konkurrenz gegeben sein werde.[2768]

§ 107c Abs 2 sieht eine Qualifikation vor, wenn die Tat den Selbstmord oder einen Selbstmordversuch der im Sinn des Abs 1 verletzten Person zur Folge hat. In diesem Fall ist der Täter mit Freiheitsstrafe bis

2764 Siehe dazu ErlRV 689 BlgNR XXV. GP, 19 f.
2765 Vgl ErlRV 689 BlgNR XXV. GP, 20 mit Verweis auf *Schwaighofer* in WK² § 107a Rz 11.
2766 ErlRV 689 BlgNR XXV. GP, 20.
2767 Siehe ErlRV 689 BlgNR XXV. GP, 20.
2768 ErlRV 689 BlgNR XXV. GP, 20.

zu drei Jahren zu bestrafen. Bei dieser Qualifikationsbestimmung handelt es sich um ein erfolgsqualifiziertes Delikt, bei dem bereits Fahrlässigkeit ausreicht (vgl § 7 Abs 2).

G. Einführung einer Qualifikation des Selbstmordes für die »Beharrliche Verfolgung« (§ 107a Abs 3)

Neben der generellen Ergänzung einer alternativen Geldstrafdrohung (bis zu 720 Tagessätzen) bei Strafdrohungen bis zu einem Jahr Freiheitsstrafe durch das StRÄG 2015, wird auch ein neuer Abs 3 eingeführt.

Diese Qualifikation, die bereits für den neu geschaffenen Tatbestand der »Fortgesetzten Belästigung im Wege einer Telekommunikation oder eines Computersystems« in § 107c Abs 3 normiert wurde, ist für jene Fälle vorgesehen, in denen die Tat den Selbstmord oder Selbstmordversuch des Opfers zur Folge hat.[2769] Die GMat begründen die Aufnahme dieser Qualifikationsbestimmung in § 107a damit, dass es in Anbetracht der schweren Nötigung und der qualifizierte gefährlichen Drohung daher aus Gründen der Systematik sowie der Gleichwertigkeit der Rechtsgutverletzungen geboten erscheint, diese Qualifikation einzuführen.[2770]

H. Einführung einer neuen Strafbestimmung »Ausspähen von Daten eines unbaren Zahlungsmittels« (§ 241h)

§ 241h[2771] (1) Wer Daten eines unbaren Zahlungsmittels mit dem Vorsatz ausspäht,

1. dass er oder ein Dritter durch deren Verwendung im Rechtsverkehr unrechtmäßig bereichert werde oder

2. sich oder einem anderen eine Fälschung unbarer Zahlungsmittel (§ 241a) zu ermöglichen,

ist mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bis zu 720 Tagessätzen zu bestrafen.

2769 Siehe oben.
2770 Siehe ErlRV 689 BlgNR XXV. GP, 18 f.
2771 RV 689 BlgNR XXV. GP.

> (2) Wer die Tat gewerbsmäßig oder als Mitglied einer kriminellen Vereinigung begeht, ist mit Freiheitsstrafe bis zu drei Jahren zu bestrafen.
>
> (3) Der Täter ist nicht zu bestrafen, wenn er freiwillig, bevor die ausgespähten Daten im Sinne des Abs. 1 Z 1 und 2 verwendet wurden, die Gefahr ihrer Verwendung durch Verständigung der Behörde, des Berechtigten oder auf andere Weise beseitigt. Besteht die Gefahr einer solchen Verwendung nicht oder ist sie ohne Zutun des Täters beseitigt worden, so ist er nicht zu bestrafen, wenn er sich in Unkenntnis dessen freiwillig und ernstlich bemüht, sie zu beseitigen.

Mit der neuen Strafbestimmung unter der Deliktsbezeichnung »Ausspähen von Daten eines unbaren Zahlungsmittels« reagiert der Gesetzgeber vorwiegend auf das Phänomen »Skimming«, das nach den GMat bislang nicht vollständig erfasst werde.[2772]

Tatobjekt dieser Bestimmung sind »Daten eines unbaren Zahlungsmittels«. Die Wendung ist jedoch nicht unproblematisch, da der Datenbegriff nach § 74 Abs 2 sehr weit gehalten ist und daher auch Informationen eines unbaren Zahlungsmittels erfasst sind, die gar nicht als schutzwürdig erscheinen, wie etwa die Bezeichnung des Ausstellers, welche zB auf einer Bankomat- oder Kreditkarte aufgedruckt ist. Auf der einen Seite ist daher der Datenbegriff in dieser Bestimmung auf solche Daten (teleologisch) zu reduzieren, die einen Geheimnischarakter aufweisen und deren Kenntnisverschaffung in weiterer Folge überhaupt Missbräuche ermöglicht, wie etwa die verschlüsselt gespeicherte PIN, Hash-Werte, Kontonummer, Kartenlimit, Gültigkeitsdauer udgl. Auf der anderen Seite darf der Datenbegriff jedoch nicht auf bloße »Computerdaten« deliktsspezifisch eingeschränkt werden, da auch die bloße Kenntnisverschaffung durch Nachfrage beim Opfer oder durch bloßes Ansehen und Merken der Kartendaten einschließlich des Bezug habenden PIN-Codes neben dem Einsatz technischer Hilfsmittel nach den GMat schon für die Tathandlung des »Ausspähens« ausreichen soll.[2773] Dies macht durchaus Sinn, da es zB bei PIN-Codes ausschließlich um den Geheimnischarakter geht und nicht darum, in welcher Darstellungsform diese vorliegen.[2774]

Neben dem Tatbildvorsatz, der zumindest im Stärkegrad eines bedingten Vorsatzes vorliegen muss, werden alternativ in Z 1 bzw Z 2 zwei

2772 ErlRV 689 BlgNR XXV. GP, 39.
2773 Siehe ErlRV 689 BlgNR XXV. GP, 40.
2774 Siehe dazu bereits oben zu § 126c StGB bzw § 51 DSG 2000.

überschießende Innentendenzen vorgeschrieben. Z 1 stellt dabei auf den erweiterten Vorsatz ab, dass der Täter oder ein Dritter durch deren Verwendung im Rechtsverkehr unrechtmäßig bereichert werde. Z 2 erfasst den erweiterten Vorsatz, sich oder einem anderen eine Fälschung unbarer Zahlungsmittel (§ 241a) zu ermöglichen. Für die Verwirklichung dieser überschießenden Innentendenzen reicht jeweils bedingter Vorsatz aus.

§ 241h Abs 2 sieht zwei Qualifikationsfälle vor. Wer die Tat gewerbsmäßig oder als Mitglied einer kriminellen Vereinigung begeht, wird daher strenger, nämlich mit Freiheitsstrafe bis zu drei Jahren, bestraft.

Wie bereits bei den Delikten nach §§ 241a bis 241f wird in Abs 3 eine Möglichkeit der Tätigen Reue geschaffen, wobei sich der Wortlaut an §§ 241d bzw 241g orientiert.[2775]

Hervorzuheben ist dabei die Möglichkeit für den Täter, die Gefahr der Verwendung der ausgespähten Daten auch durch Verständigung »des Berechtigten« oder »auf andere Weise« zu beseitigen. Aus diesem Grund wäre es zB auch möglich das betreffende Bankinstitut zu verständigen.[2776]

I. Weitere Änderungen iZm Computerdelikten durch das StRÄG 2015

1. Einführung des Erschwerungsgrunds des »Identitätsmissbrauchs«

In § 33 Abs 1 Z 8 wird in Umsetzung von Art 9 Abs 5 RL 2013/40/EU ein neuer besonderer Erschwerungsgrund aufgenommen, der im Rahmen der Strafzumessung dann zum Tragen kommt, wenn die Tat unter Missbrauch der personenbezogenen Daten einer anderen Person begangen wurde, um das Vertrauen eines Dritten zu gewinnen, wodurch dem rechtmäßigen Identitätseigentümer ein Schaden zugefügt wurde. Die GMat begründen die Einführung dieses Erschwerungsgrunds im allgemeinen Teil damit, dass es nicht ausgeschlossen werden könne, dass ein solcher »Identitätsdiebstahl« auch außerhalb des Computerstrafrechts begangen wird.[2777]

2775 Vgl ErlRV 689 BlgNR XXV. GP, 40.

2776 Siehe ErlRV 689 BlgNR XXV. GP, 40.

2777 ErlRV 689 BlgNR XXV. GP, 8; Treffender wäre wohl die Bezeichnung »Identitätsmissbrauch«.

2. Neudefinition der »Gewerbsmäßigkeit«

Den Anregungen im JA folgend, wird die in der ursprünglichen RV vorgeschlagene Bezeichnung »Erwerbsmäßige Begehung« für die Neudefinition der »Gewerbsmäßigen Begehung« nun doch nicht eingeführt, weil zum einen keine Verbesserung durch die Umbenennung gesehen wird und sich zum anderen dadurch auch die Anpassung zahlreicher Bestimmungen über die Gewerbsmäßigkeit in Nebengesetze an die neue Bezeichnung erübrigt.[2778] Die neue Fassung der »Gewerbsmäßigen Begehung« lautet:[2779]

> § 70.[2780] (1) Gewerbsmäßig begeht eine Tat, wer sie in der Absicht ausführt, sich durch ihre wiederkehrende Begehung längere Zeit hindurch ein nicht bloß geringfügiges fortlaufendes Einkommen zu verschaffen, und
>
> 1. unter Einsatz besonderer Fähigkeiten oder Mittel handelt, die eine wiederkehrende Begehung nahelegen, oder
>
> 2. zwei weitere solche Taten schon im Einzelnen geplant hat oder
>
> 3. bereits zwei solche Taten begangen hat oder einmal wegen einer solchen Tat verurteilt worden ist.
>
> (2) Ein nicht bloß geringfügiges fortlaufendes Einkommen ist ein solches, das nach einer jährlichen Durchschnittsbetrachtung monatlich den Betrag von Euro 400,– übersteigt.
>
> (3) Eine frühere Tat oder Verurteilung bleibt außer Betracht, wenn seit ihrer Begehung oder Rechtskraft bis zur folgenden Tat mehr als ein Jahr vergangen ist. In diese Frist werden Zeiten, in denen der Täter auf behördliche Anordnung angehalten worden ist, nicht eingerechnet.

Diese Änderung wirkt sich nunmehr im Bereich der Computerdelikte auf die §§ 148a Abs 2, 207a Abs 2, 241a Abs 2, 241e Abs 2 sowie auf den ebenfalls durch das StRÄG 2015 neu geschaffenen § 241h Abs 2 aus.

2778 JAB 728 BlgNR XXV. GP, 9.

2779 Siehe dazu weiterführend *Bernreiter,* jusIT 2015/52, 128 (130 f).

2780 Siehe RV 689 BlgNR XXV. GP in der Fassung gem der Änderungen im Plenum des NR gegenüber dem ursprünglichen Entwurf (9403 BlgBR XXV. GP, 6).

3. Erweiterung der Aufzählung der Rechtsgüter in § 74 Abs 1 Z 5

Durch das StRÄG 2015 wird die Definition der »gefährlichen Drohung« in § 74 Abs 1 Z 5 durch Drohung mit einer Verletzung »des höchstpersönlichen Lebensbereiches durch Zugänglichmachen, Bekanntgeben oder Veröffentlichen von Tatsachen oder Bildaufnahmen« ergänzt. Mit dieser Erweiterung der Rechtsgüter um den Schutz des höchstpersönlichen Lebensbereichs wird – den GMat zufolge[2781] – der gesellschaftlichen Entwicklung Rechnung getragen, die bislang nicht mehr adäquat war. Ausgangspunkt bildete die E des OGH, in welcher dieser befand, dass die Ankündigung der Aufdeckung einer bestimmten sexuellen Orientierung alleine noch nicht als Drohmittel im Sinne des bisher in Geltung stehenden § 74 Abs 1 Z 5 angesehen werden kann.[2782] In der Zwischenzeit ergingen weitere einschlägige E, die sich im Wesentlichen mit der Androhung der Veröffentlichung von Nacktfotos im Internet und der »gefährliche Drohung« auseinandersetzen und auf zahlreiche Anmerkungen in der Lit gestoßen sind.[2783]

Zum Begriff des höchstpersönlichen Lebensbereichs dieser neu gefassten Definition führen die GMat[2784] aus, dass sich dieser mit dem des Privat- und Familienlebens in Art 8 EMRK decke. Beispielhaft werden dazu das Sexualleben, das Familienleben, Krankheiten, Behinderungen und religiöse Ansichten angeführt. Ergänzend wird darauf hingewiesen, dass dabei einzelfallbezogen zu prüfen sei, ob die Drohung geeignet ist, der bedrohten Person mit Rücksicht auf die Verhältnisse und ihre persönliche Beschaffenheit oder die Wichtigkeit des angedrohten Übels begründete Besorgnisse einzuflößen. Ausgenommen seien aber Angelegenheiten des Geschäfts- oder Berufslebens, wobei hier ohnehin zumeist eine Drohung mit einer Verletzung am Vermögen vorliegen dürfte.[2785]

2781 ErlRV 689 BlgNR XXV. GP, 15.

2782 OGH 23.01.2014, 12 Os 90/13x = JSt 2014, 26 *(Birklbauer/Oberlaber)* = ÖJZ 2014/59, 382 *(Anzenberger/Sprajc)* = ÖJZ 2014/144, 956 *(Swiderski)* = RZ 2014, 238 *(Riffel)* = juridikum 2014, 166 *(Smutny)* = AnwBl 2014/8380, 261 *(Schrott)* = ÖJZ EvBl 2014/48, 317 *(Ratz)* = JBl 2014, 336 *(Schmoller)*.

2783 Vgl etwa OGH 03.07.2014, 12 Os 56/14y = ÖJZ EvBl-LS 2014/155, 935 *(Ratz)* = JBl 2015, 63 *(Salimi)* = jusIT 2015/38, 98 *(Luef-Kölbl)* bzw OGH 25.09.2014, 12 Os 52/14k = jusIT 2015/38, 98 *(Luef-Kölbl)*.

2784 ErlRV 689 BlgNR XXV. GP, 15.

2785 Siehe ErlRV 689 BlgNR XXV. GP, 15.

Nach den GMat genüge für das »Zugänglichmachen«, dass die Möglichkeit des Zugriffs auf den Inhalt eröffnet wird. Der Täter müsse daher lediglich den Zugang zum Geheimnis eröffnen. Das Geheimnis werde »bekannt gemacht«, wenn es der Täter anderen unmittelbar (schriftlich oder mündlich) mitteilt. Ein »Veröffentlichen« liege nach den GMat vor, wenn die geheimen Tatsachen einem unbestimmten Personenkreis zugänglich gemacht werden.[2786]

Das Zugänglichmachen ist dem Bekanntmachen vorgelagert und stellt bereits auf die Eröffnung der Möglichkeit der Kenntnisnahme des Geheimnisses ab, ohne dass dabei tatsächlich das Geheimnis schon gebrochen worden sein muss. Bei der Bekanntmachung bricht der Täter unmittelbar selbst durch Mitteilung der Tatsachen das Geheimnis. Was das Veröffentlichen betrifft, ist auf die obigen Ausführungen zu verweisen.[2787]

Sachspezifisch erfasst der Begriff »Tatsache« hier auch unrichtige Tatsachen, »da eine Drohung mit der Veröffentlichung oder Bekanntgabe von falschen Behauptungen betreffend beispielsweise Krankheiten oder das Veröffentlichen von Nacktfotos, die mit Hilfe von Fotomontage erstellt worden sind, ebenso geeignet sein kann, dem Bedrohten begründete Besorgnis einzuflößen, wie eine Drohung mit der Bekanntgabe von beispielsweise tatsächlich bestehender Krankheiten«.[2788]

4. Erweiterung des Qualifikationstatbestands des § 147 Abs 1 Z 1 bezüglich § 241h StGB

Korrespondierend zur neu geschaffenen Bestimmung des § 241h wird der Qualifikationstatbestand des § 147 Abs 1 Z 1 um den Fall der »ausgespähten Daten eines unbaren Zahlungsmittels« erweitert.

5. Erweiterung der Privilegierung des § 166 um die Delikte der §§ 241a ff

Anregungen im Begutachtungsverfahren folgend, wird nun auch die Deliktsgruppe bezüglich der unbaren Zahlungsmittel (§§ 241a ff) in die Privilegierung der Begehung im Familienkreis (§ 166) einbezogen. Den

2786 ErlRV 689 BlgNR XXV. GP, 15.
2787 Siehe dazu oben.
2788 Vgl ErlRV 689 BlgNR XXV. GP, 15.

GMat zufolge sei dies »ungeachtet des von den §§ 241a ff ›eigentlich‹ geschützten Rechtsgutes lebensnah und sachgerecht«.[2789]

Dies führt allerdings auch dazu, dass erstmals Delikte in den Deliktskatalog des § 166 aufgenommen wurden, die in ihrem eigentlichen Sinn Universalrechtsgüter schützen.

6. Erweiterung der Strafausschließungsgründe des § 207a Abs 5

Im Wesentlichen werden die Strafausschließungsgründe des § 207a Abs 5 durch die Einfügung einer neuen Z 1a erweitert.

Nach § 207a Abs 1 und Abs 3 ist demnach neben den bisherigen Strafausschließungsgründen ebenfalls nicht zu bestrafen, wer eine pornographische Darstellung einer mündigen minderjährigen Person von sich selbst herstellt, besitzt, oder einem anderen zu dessen eigenen Gebrauch anbietet, verschafft, überlässt, vorführt oder sonst zugänglich macht.

7. Ergänzung einer Geldstrafdrohung als Alternative zur Freiheitsstrafe und Anhebung von bestehenden Geldstrafdrohungen

Die generelle Einführung einer Geldstrafenalternative (»oder mit Geldstrafe bis zu 720 Tagessätzen«) bei Delikten, deren Tatbestandsverwirklichung bislang ausschließlich mit einem Jahr Freiheitsstrafe bedroht war, wirkt sich nunmehr im Bereich des Computerstrafrechts für folgende Delikte aus: §§ 107a Abs 1, 207a Abs 3, 215a Abs 2a, 225a, 241b, 241c, 241e Abs 3, 241f. Diesbezüglich räumen die GMat ein, dass es dabei bei einzelnen Delikten, bei denen bisher alternativ zu einer bis zu einjährigen Freiheitsstrafe eine Geldstrafe bis zu 360 Tagessätzen vorgesehen war, zu einer gewissen Strafverschärfung komme.[2790]

Einer Erhöhung der bisherigen Geldstrafdrohung von 360 auf 720 Tagessätze wird dabei § 208a Abs 1a unterzogen.

2789 ErlRV 689 BlgNR XXV. GP, 32.
2790 Siehe ErlRV 689 BlgNR XXV. GP, 11.

8. Erhöhung der Wertgrenzen

Die generelle Erhöhung der Wertgrenzen von derzeit € 3.000,– auf € 5.000,– bzw von € 50.000,– auf € 300.000,– betreffen im hier gegenständlichen Zusammenhang § 126a Abs 2 (€ 5.000,–) und Abs 3 (€ 300.000,–) sowie § 148a Abs 2 (€ 5.000,– und € 300.000,–).

5 Quellenverzeichnis

A. Literaturverzeichnis

1. Monographien

- *Balzert Helmut,* Lehrbuch Grundlagen der Informatik2 (Spektrum Akademischer Verlag 2005) [Lehrbuch]
- *Bergauer Christian,* Malware aus strafrechtlicher und verwaltungsstrafrechtlicher Sicht (Dissertation 2005) [Malware]
- *Berka Walter,* Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit, 18. ÖJT Band I/1 (Manz 2012) [Datenschutz]
- *Berka Walter,* Lehrbuch Verfassungsrecht5 (Springer 2013) [Verfassungsrecht]
- *Bertel Christian/Schwaighofer Klaus,* Österreichisches Strafrecht. Besonderer Teil I (§§ 75 bis 168b StGB)12 (Verlag Österreich 2012) [BT I]
- *Bertel Christian/Schwaighofer Klaus,* Österreichisches Strafrecht. Besonderer Teil II (§§ 169 bis 321 StGB)11 (Verlag Österreich 2015) [BT II]
- *Betsch Denise,* Körperlichkeit im Chat (GRIN 2007)
- *Birklbauer Alois/Hilf Marianne/Tipold Alexander,* Strafrecht BT I2 (facultas. wuv 2012) [BT I]
- *Borges Georg/Schwenk Jörg/Stuckenberg Carl-Friedrich/Wegener Christoph,* Identitätsdiebstahl und Identitätsmissbrauch im Internet. Rechtliche und technische Aspekte (Springer 2011) [Identitätsdiebstahl]
- *Brodowski Dominik/Freiling Felix,* Computerkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft (Freie Universität Berlin 2011) [Computerkriminalität]
- *Burks Arthur/Goldstine Herman/von Neumann John,* Preliminary discussion of the logical design of an electronic computing instrument (Princeton's Institute of Advanced Studies 1946)
- *Chantelau Klaus/Brothuhn René,* Multimediale Client-Server-Systeme (Springer 2010)
- *Clarke Justin,* SQL Injection. Attacks and Defense (Syngress 2012)
- *Clough Jonathan,* Principles of Cybercrime (Cambridge University Press 2010) [Cybercrime]
- *Damjanovic Dragana/Holoubek Michael/Kassai Klaus/Lehofer Hans Peter/Urbantschitsch Wolfgang,* Handbuch des Telekommunikationsrechts (Springer 2006) [Telekommunikationsrecht]

- *Dembowski Klaus,* BIOS und Troubleshooting (Markt+Technik 2004)
- *Dhanjani Nitesh/Clarke Justin,* Network Security Tools (O'Reilly 2005)
- *Dickreiter/Dittel/Hoeg/Wöhr,* Handbuch der Tonstudiotechnik. Bd I8 (Walter de Gruyter 2014). [Tonstudiotechnik]
- *Drobesch Heinz/Grosinger Walter,* Das neue österreichische Datenschutzgesetz (Juridica 2000) [Datenschutzgesetz]
- *Durl Robert,* Die Pflicht zur Verhinderung von mit Strafe bedrohten Handlungen gemäß § 286 StGB (dbv-Verlag für die Technische Universität Graz 1999)
- *Duschanek Alfred,* Datenschutzgesetz (Österreichischer Wirtschaftsverlag 1978)
- *Duschanek Alfred/Rosenmayr-Klemenz Claudia,* Datenschutzgesetz 2000 (WKO 2000) [Datenschutzgesetz]
- *Eckert Claudia,* IT-Sicherheit. Konzepte – Verfahren – Protokolle9 (Oldenbourg Wissenschaftsverlag 2014) [IT-Sicherheit]
- *Eder-Rieder Maria,* Einführung in das Wirtschaftsstrafrecht[3] (NWV 2014) [Wirtschaftsstrafrecht]
- *Faßler Manfred,* Cyber-Moderne. Medienevolution, globale Netzwerke und die Künste der Kommunikation (Springer 1999)
- *Flora Margarethe,* Das Bankgeheimnis im gerichtlichen Strafverfahren (Springer 2007)
- *Freyer Ulrich,* Nachrichten-Übertragungstechnik[6] (Carl Hanser 2009)
- *Fuchs Helmut,* Strafrecht. Allgemeiner Teil I[8] (Verlag Österreich 2012) [AT I]
- *Fuchs Helmut/Reindl-Krauskopf Susanne,* Strafrecht Besonderer Teil I[4] (Verlag Österreich 2014) [BT I]
- *Gleißner Winfried/Grimm Rüdiger/Herda Siegfried/Isselhorst Hartmut,* Manipulation in Rechnern und Netzen. Risiken, Bedrohungen und Gegenmaßnahmen (Addison Wesley 1989) [Manipulation]
- *Gercke Marco/Brunst Phillip,* Praxishandbuch Internetstrafrecht (Kohlhammer 2009) [Internetstrafrecht]
- *Gollmann Dieter,* Computer Security[3] (John Wiley&Sons 2011)
- *Goos Gerhard/Zimmermann Wolf,* Vorlesungen über Informatik. Band I. Grundlagen und funktionales Programmieren[4] (Springer 2006)
- *Grimm Rüdiger,* Digitale Kommunikation (Oldenbourg Wissenschaftsverlag 2005)
- *Gumm Heinz-Peter/Sommer Manfred,* Einführung in die Informatik[10] (Oldenbourg Wissenschaftsverlag 2013). [Informatik]
- *Halsall Fred,* Computer Networking and the Internet[5] (Addison-Wesley 2005)
- *Hansen Hans Harald,* Sprachliches Handeln und Transaktionsanalyse. Die Psychologie im Sprechakt (Diplomica 2008)
- *Harley David/Slade Robert/Gattiker Urs E.,* Anti-Viren-Buch (mitp 2002)
- *Hein Mathias/Reisner Michael,* TCP/IP – Ge-packt[2] (mitp 2004)
- *Hilgendorf Eric/Valerius Brian,* Computer- und Internetstrafrecht[2] (Springer 2012)

- *Hinterhofer Hubert/Rosbaud Christian,* Strafrecht. Besonderer Teil II[5] §§ 169 – 321 StGB (facultas.wuv 2012)
- *Hochmayr Gudrun,* Strafbarer Besitz von Gegenständen (Manz 2005) [Besitz]
- *Huber Edith,* Cyberstalking und Cybercrime: Kriminalsoziologische Untersuchung zum Cyberstalking-Verhalten der Österreicher (Springer 2013)
- *Hunt Craig,* TCP/IP. Netzwerk-Administration[3] (O'Reilly 2002) [TCP/IP]
- *Jaburek Walter/Schmölzer Gabriele,* Computer-Kriminalität (EDVuR 1985)
- *Jahnel Dietmar,* Handbuch Datenschutzrecht (Jan Sramek 2010) [Handbuch]
- *Jahnel Dietmar/Sramek Jan,* NZR. Neue Zitierregeln (Jan Sramek 2012)
- *Janowicz Krzysztof,* Sicherheit im Internet[3] (O'Reilly 2007) [Sicherheit]
- *Jia Weijia/Zhou Wanlei,* Distributed Network Systems. From Concepts to Implementations (Springer 2005)
- *Keiler Stephan/Bezemek Christoph,* leg cit. Leitfaden für juristisches Zitieren[3] (Verlag Österreich 2014)
- *Kennedy David/O'Gorman Jim/Kearns Devon/Aharoni Mati,* Metasploit – Die Kunst des Penetration Testing (mitp 2012)
- *Kersken Sascha,* IT-Handbuch für Fachinformatiker[5] (Galileo Computing 2011) [IT-Handbuch]
- *Kienapfel Diethelm,* Grundriß des österreichischen Strafrechts. Besonderer Teil I[4] (Manz 1997) [BT I]
- *Kienapfel Diethelm,* Grundriß des österreichischen Strafrechts. Besonderer Teil II[3] (Manz 1993) [BT II]
- *Kienapfel Diethelm/Höpfel Frank/Kert Robert,* Strafrecht Allgemeiner Teil I[14] (Manz 2012)
- *Kienapfel Diethelm/Schmoller Kurt,* Grundriss des österreichischen Strafrechts. Besonderer Teil III (Manz 1999) [Grundriss BT III]
- *Kienapfel Diethelm/Schmoller Kurt,* Studienbuch Strafrecht. Besonderer Teil II (Manz 2003) [StudB BT II]
- *Kienapfel Diethelm/Schmoller Kurt,* Studienbuch Strafrecht. Besonderer Teil III[2] (Manz 2009) [StudB BT III]
- *Kienapfel Diethelm/Schroll Hans Valentin,* Grundriss des österreichischen Strafrechts. Besonderer Teil I[5] (Manz 2003) [Grundriss BT I]
- *Kienapfel Diethelm/Schroll Hans Valentin,* Studienbuch. Besonderer Teil I[3] (Manz 2012) [StudB BT I]
- *Kmetic Konrad,* Grundzüge des Computerstrafrechts (Linde 2014) [Grundzüge]
- *Köck Elisabeth,* Wirtschaftsstrafrecht. Eine systematische Darstellung[2] (facultas.wuv 2010) [Wirtschaftsstrafrecht]
- *Koller Peter,* Theorie des Rechts. Eine Einführung[2] (Böhlau 1997) [Theorie]
- *Koops Bert-Jaap,* The Crypto Controversy: A Key Conflict in the Information Society (Kluwer Law International 1998)

- *Korge Tobias,* Die Beschlagnahme elektronisch gespeicherter Daten bei privaten Trägern von Berufsgeheimnissen (Springer 2009) [Beschlagnahme]
- *Kröner Tonio,* Cyberterrorismus – Definition, Arten, Gegenmaßnahmen (GRIN 2011) [Cyberterrorismus]
- *Kruspel Ines,* Auf dem Weg zu einem tragfähigen Massenkommunikationsbegriff: Nachricht als vermittelte Mitteilung (GRIN 2008)
- *Kurose James F./Ross Keith W.,* Computernetzwerke. Der Top-Down-Ansatz[4] (Pearson 2008) [Computernetzwerke]
- *Lackner,* Softwareschutz in Österreich durch Urheberrecht? (Dissertation 1991)
- *Lee Won-Sang,* Die Verhältnismäßigkeit im Cyberstrafrecht – Überprüfung des Strafrechtseingriffs im Cyberspace anhand des Verhältnismäßigkeitsgrundsatzes (Logos 2010)
- *Lenckner Theodor,* Computerkriminalität und Vermögensdelikte (C.F. Müller 1981)
- *Lewisch Peter,* Strafrecht. Besonderer Teil I. §§ 75 – 168e[2] (WUV 1999) [BT I]
- *Lipski Marcus,* Social Engineering – Der Mensch als Sicherheitsrisiko in der IT (Diplomica 2009) [Social Engineering]
- *Löschnigg Günther,* Datenermittlung im Arbeitsverhältnis (ÖGB 2009)
- *Longolius Nikolai,* Web-TV. AV-Streaming im Internet (O'Reilly 2011) [Web-TV]
- *Malaka Rainer/Butz Andreas/Hußmann Heinrich,* Medieninformatik. Eine Einführung (Pearson 2009)
- *Malek Klaus/Popp Andreas,* Strafsachen im Internet[2] (C.F. Müller 2014)
- *Marberth-Kubicki Annette,* Computer- und Internetstrafrecht[2] (C.H. Beck 2010)
- *Mayer-Schönberger Viktor,* Information und Recht. Vom Datenschutz bis zum Urheberrecht (Springer 2001) [Information]
- *Moore Robert,* Cybercrime: Investigating High-Technology Computer Crime[2] (Anderson 2011) [Cybercrime]
- *Müller-Enbergs Helmut,* Inoffizielle Mitarbeiter des Ministeriums für Staatssicherheit. Teil 2: Anleitungen für die Arbeit mit Agenten, Kundschaftern und Spionen in der Bundesrepublik Deutschland[2] (Ch. Links 1998)
- *Nehmzow Ulrich,* Mobile Robotik (Springer 2002)
- OECD, Computer-Related Crime: Analysis of Legal Policy, ICCP Series No 10 (1986)
- *Olbrich Alfred,* Netze. Protokolle. Spezifikationen (Springer 2003) [Netze]
- *Oppliger Rolf,* Internet and Intranet Security[2] (Artech House 2002) [Internet]
- *Pfister Christa,* Hacking in der Schweiz (NWV 2008) [Hacking]
- *Rankl Wolfgang,* Chipkarten-Anwendungen (Hanser 2006)
- *Rankl Wolfgang/Effing Wolfgang,* Handbuch der Chipkarten[5] (Hanser 2008) [Handbuch]

- *Rauch Hans-Jörg,* Korruptionsstrafrecht (LexisNexis 2012)
- *Rebhahn Robert,* Mitarbeiterkontrolle am Arbeitsplatz (facultas.wuv 2009)
- *Reindl-Krauskopf Susanne,* Computerstrafrecht im Überblick² (facultas.wuv 2009)
- *Reindl Susanne,* E-Commerce und Strafrecht. Zur Strafbarkeit des Missbrauchs elektronischer Dienste (NWV 2003) [E-Commerce]
- *Reischl Gerald,* Gefährliche Netze (Ueberreuter 2001)
- *Reisinger Leo,* Strukturwissenschaftliche Grundlagen der Rechtsinformatik (Leykam 1987) [Rechtsinformatik]
- *Rey Enno/Thumann Michael/Baier Dominick,* Mehr IT-Sicherheit durch Pen-Tests (Vieweg+Teubner 2005) [IT-Sicherheit]
- *Richter Alexander,* IT-gestütztes Wissensmanagement² (Volker Derballa 2008)
- *Rohner Louis,* Computerkriminalität. Strafrechtliche Probleme bei »Zeitdiebstahl und Manipulationen (Schulthess Polygraphischer Verlag 1976)
- *Russell Ryan/Cunningham Stace,* Das Hacker-Buch (bhv 2001)
- *Schiffmann Wolfram/Bähring Helmut/Hönig Udo,* Technische Informatik 3. Grundlagen der PC-Technologie (Springer 2011)
- *Schmeh Klaus,* Das Trojanische Pferd. Klassische Mythen erklärt (Haufe-Lexware 2007)
- *Schmeh Klaus,* Elektronische Ausweisdokumente. Grundlagen und Praxisbeispiele (Hanser 2009)
- *Schuh Daniel,* Computerstrafrecht im Rechtsvergleich – Deutschland, Österreich, Schweiz (Duncker & Humblot 2012) [Computerstrafrecht]
- *Schwabach Aaron,* Internet and the law² (ABC-CLIO 2014) [Internet]
- *Seifert Dirk,* Electronic-Commerce – Mobile-Commerce – Social-Commerce Guide. Lexikon mit den relevanten Definitionen und KPIs in der digitalen Welt (BoD 2013) [Guide]
- *Seling Andreas,* § 107a StGB. Eine Strafvorschrift gegen Stalking (NWV 2006) [Stalking]
- *Seling Andreas,* Schutz der Privatsphäre durch das Strafrecht (LexisNexis 2010) [Privatsphäre]
- *Sieber Ulrich,* Computerkriminalität und Strafrecht² (Heymann 1980) [Computerkriminalität]
- *Sieber Ulrich,* The Handbook on Computer Crime, Computer-related Economic Crime and the Infringements of Privacy (John Wiley & Sons 1986)
- *Sikora Elisabeth,* Der strafrechtliche Schutz des bargeldlosen Zahlungsverkehrs (LexisNexis 2008) [Zahlungsverkehr]
- *Slade Robert,* Software Forensics. Collecting Evidence from the scene of a digital crime (Mcgraw-Hill 2004) [Software Forensics]

- *Solomon David,* Elements of Computer Security (Springer 2010) [Computer Security]
- *Staudegger Elisabeth,* Das Computerprogramm als Rechtsobjekt – zugleich ein Beitrag zum Sachbegriff im Informationszeitalter (Habilitationsschrift 2009) [Computerprogramm]
- *Starzer Barbara,* Vom Jäger zum Gejagten. Eine theoretische und empirische Untersuchung zum Phänomen Stalking – § 107a StGB (Manz 2010) [Jäger]
- *Stein Erich,* Rechnernetze und Internet[3] (Hanser 2008)
- *Street Jason E./Nabors Kent/Baskin Brian,* Forbidden Network. Anatomie eines Hacks (mitp 2011)
- *Studer Bruno,* Netzwerkmanagement und Netzwerksicherheit (vdf 2010) [Netzwerkmanagement]
- *Tanenbaum Andrew S.,* Computernetzwerke[5] (Pearson Studium 2012)
- *Tanenbaum Andrew S.,* Computerarchitektur[5] (Addison-Wesley 2006)
- *Tanenbaum Andrew S.,* Moderne Betriebssysteme[3] (Pearson Studium 2009)
- *Triffterer Otto,* Die österreichische Beteiligungslehre (Manz 1983)
- *Triffterer Otto,* Österreichisches Strafrecht. Allgemeiner Teil [2] (Springer 1994) [AT]
- *Thome Günter/Sollbach Wolfgang,* Grundlagen und Modelle des Information Lifecycle Management (Springer 2007) [Grundlagen]
- *von Gravenreuth Günter,* Computerviren – Technische Grundlagen und rechtliche Gesamtdarstellung[2] (Carl Heymanns 1998) [Computerviren]
- *von zur Mühlen Rainer A. H.,* Computer-Kriminalität, Gefahren und Abwehrmaßnahmen (Luchterhand 1972)
- *Walter Michel M.,* Österreichisches Urheberrecht. Handbuch. I. Teil (Medien und Recht 2008)
- *Wegscheider Herbert,* Strafrecht. Besonderer Teil. Eine multimediale Darstellung der Delikte des österreichischen Strafgesetzbuches[4] (Manz 2012) [BT]
- *Werner Martin,* Information und Codierung. Grundlagen und Anwendungen[2] (Vieweg+Teubner 2008) [Information]
- *Wiebe Andreas,* Know-how-Schutz von Computersoftware (C.H. Beck 1993)
- *Wiederin Ewald,* Privatsphäre und Überwachungsstaat (Manz 2003) [Privatsphäre]
- *Winterer Andreas,* Viren, Würmer & Trojanische Pferde (Data Becker 2002) [Viren]
- *Winterer Andreas,* Windows 7 Sicherheit (bhv 2011) [Windows]
- *Wobst Reinhard,* Abenteuer Kryptologie. Methoden, Risiken und Nutzen der Datenverschlüsselung[3] (Addison-Wesley 2001) [Kryptologie]
- *Zerbes Ingeborg,* Spitzeln, Spähen, Spionieren. Sprengung strafprozessualer Grenzen durch geheime Zugriffe auf Kommunikation (Springer 2010) [Spitzeln]

2. Festschriften und Sammelbände

- *Achenbach Hans/Ransiek Andreas* (Hrsg), Handbuch Wirtschaftsstrafrecht[3] (C.F. Müller 2012) [Wirtschaftsstrafrecht]
- *Akyürek Metin/Baumgartner Gerhard/Jahnel Dietmar/Lienbacher Georg/Stolzlechner Harald* (Hrsg), Staat und Recht in europäischer Perspektive, FS Schäffer (Manz 2006) [FS Schäffer]
- *Arbeitsgemeinschaft für Datenverarbeitung* (Hrsg), Quo vadis EDV? – Realität und Vision. 8. Internationaler Kongress Datenverarbeitung im Europäischen Raum (A. Riegelnik 1987) [Quo vadis EDV?]
- *Bammer Armin/Holzinger Gerhart/Vogl Mathias/Wenda Gregor* (Hrsg), Rechtsschutz gestern – heute – morgen, FS Machacek/Matscher (NWV 2008) [FS Machacek/Matscher]
- *Bauer Lukas/Reimer Sebastian* (Hrsg), Handbuch Datenschutzrecht (facultas. wuv 2009)
- *Bergauer Christian/Staudegger Elisabeth* (Hrsg), Recht und IT. Zehn Studien (Jan Sramek 2009) [Recht und IT]
- *Bundesministerium für Justiz* (Hrsg), 32. Ottensteiner Fortbildungsseminar aus Strafrecht und Kriminologie. Bd 117 (NWV 2005) [32. Ottensteiner Fortbildungsseminar]
- *Bundesministerium für Justiz* (Hrsg), 33. Ottensteiner Fortbildungsseminar aus Strafrecht und Kriminologie. Bd 118 (NWV 2005) [33. Ottensteiner Fortbildungsseminar]
- *Bundesministerium für Justiz* (Hrsg), 34. Ottensteiner Fortbildungsseminar aus Strafrecht und Kriminologie. Bd 127 (NWV 2006) [34. Ottensteiner Fortbildungsseminar]
- *Bundesministerium für Justiz* (Hrsg), 35. Ottensteiner Fortbildungsseminar aus Strafrecht und Kriminologie. Bd 132 (NWV 2007) [35. Ottensteiner Fortbildungsseminar]
- *Bundesministerium für Justiz* (Hrsg), 39. Ottensteiner Fortbildungsseminar aus Strafrecht und Kriminologie. Bd 150 (NWV 2011) [39. Ottensteiner Fortbildungsseminar]
- *Bundesministerium für Justiz* (Hrsg), Strafrechtliche Probleme der Gegenwart. 5. Strafrechtliches Seminar 1977 (BMJ 1978)
- *Bundesministerium für Justiz* (Hrsg), Strafrechtliche Probleme der Gegenwart. 16. Strafrechtliches Seminar 1988 (BMJ 1989)
- *Bundesministerium für Justiz* (Hrsg), Strafrechtliche Probleme der Gegenwart. 17. Strafrechtliches Seminar 1989 (BMJ 1990)
- *Bundesministerium für Justiz* (Hrsg), Strafrechtliche Probleme der Gegenwart. 26. Strafrechtliches Seminar 1998 (BMJ 1998)
- *Bundesministerium für Justiz* (Hrsg), Vorarlberger Tage 2003. Bd 115 (BMJ 2003)

- *Bundesministerium für Justiz* (Hrsg), Vorarlberger Tage 2005. Bd 125 (NWV 2006)
- *Brodil Wolfgang* (Hrsg), Datenschutz im Arbeitsrecht. Mitarbeiterüberwachung versus Qualitätskontrolle (Manz 2010) [Datenschutz]
- *Dax Peter/Hopf Gerhard* (Hrsg), AZR. Abkürzungs- und Zitierregeln[7] (Manz 2012)
- *Duschanek Alfred* (Hrsg), Datenschutz in der Wirtschaft (Signum 1981)
- *Enthofer-Stoisser Ruth/Habersberger Jasmin* (Hrsg), Catch me if you can! Internet«abzocke«, »cold calls« und unseriöse Werbeveranstaltungen (Verlag Österreich 2012)
- *Eberwein Helgo/Steiner Anna-Zoe* (Hrsg), Bitcoins (Jan Sramek 2014)
- *Gögele Sonja/Unger Kaja* (Hrsg), IT-Sicherheit aus rechtlicher, wirtschaftlicher und technologischer Perspektive (DWS 2010)
- *Hildebrand Knut/Gebauer Marcus/Hinrichs Holger/Mielke Michael* (Hrsg), Daten- und Informationsqualität[2] (Vieweg+Teubner 2011)
- *Holoubek Michael/Potacs Michael* (Hrsg), Handbuch des öffentlichen Wirtschaftsrechts[2]. Bd 1 (Springer 2008)
- *Jacobsson Markus/Ramzan Zulfikar* (Eds), Crimeware. Understanding New Attacks and Defenses (Addison-Wesley 2008) [Crimeware]
- *Jahnel Dietmar* (Hrsg), Datenschutzrecht und E-Government. Jahrbuch 2008 (NWV 2008) [Jahrbuch 2008]
- *Jahnel Dietmar* (Hrsg), Datenschutzrecht. Jahrbuch 2010 (NWV 2010) [Jahrbuch 2010]
- *Jahnel Dietmar* (Hrsg), Datenschutzrecht. Jahrbuch 2011 (NWV 2011) [Jahrbuch 2011]
- *Jahnel Dietmar* (Hrsg), Datenschutzrecht und E-Government. Jahrbuch 2012 (NWV 2012) [Jahrbuch 2012]
- *Jahnel Dietmar/Mader Peter/Staudegger Elisabeth* (Hrsg), IT-Recht[3] (Verlag Österreich 2012)
- *Jahnel Dietmar/Schramm Alfred/Staudegger Elisabeth* (Hrsg), Informatikrecht[2] (Springer 2003) [Informatikrecht]
- *Jahnel Dietmar/Siegwart Stefan/Fercher Natalie* (Hrsg), Aktuelle Fragen des Datenschutzrechts (facultas.wuv 2007) [Aktuelle Fragen]
- *Jaishankar Karuppannan* (Ed), Cyber Criminology. Exploring Internet Crimes Criminal Behavior (CRC Press 2011)
- *Jaksch-Ratajczek Wojciech* (Hrsg), Aktuelle Rechtsfragen der Internetnutzung (facultas.wuv 2010)
- *Jehle Jörg-Martin/Maschke Werner/Szabo Denis* (Hrsg), Strafrechtspraxis und Kriminologie[2], FS Göppinger (Forum Verlag Godesberg 1990) [FS Göppinger[2]]
- *Joerden Jan C./Scheffler Uwe/Sinn Arndt/Wolf Gerhard* (Hrsg), Vergleichende Strafrechtswissenschaft, FS Swarc (Duncker & Humblot 2009) [FS Swarc]

- *Jones Steve* (Ed), Encyclopedia of New Media (Sage Publications 2003)
- *Kilian Wolfgang/Lenk Klaus/Steinmüller Wilhelm* (Hrsg), Datenschutz. Juristische Grundfragen beim Einsatz elektronischer Datenverarbeitungsanlagen in Wirtschaft und Verwaltung (Toeche-Mittler 1973)
- *Landesgruppe Österreich der Internationalen Strafrechtsgesellschaft (AIDP) und Juristenverband* (Hrsg), Cyber Crime – Zunehmende Bedrohung der Informationsgesellschaft (BMJ 2012)
- *Lienbacher Georg/Wielinger Gerhart* (Hrsg), Öffentliches Recht. Jahrbuch 2008 (NWV 2008) [Jahrbuch 2008]
- *Mayer-Schönberger Viktor/Schneider-Manns-Au Lukas* (Hrsg), Der Jurist am Info-Highway. Über die Zukunft eines Berufsstandes (Orac 1997)
- *Mitgutsch Ingrid/Wessely Wolfgang* (Hrsg), Strafrecht. Besonderer Teil. Jahrbuch 2010 (NWV 2010) [Jahrbuch 2010]
- *Mitgutsch Ingrid/Wessely Wolfgang* (Hrsg), Strafrecht. Besonderer Teil. Jahrbuch 2012 (NWV 2012) [Jahrbuch 2012]
- *Moos Reinhard/Jesionek Udo/Müller Otto F.* (Hrsg), Strafprozessrecht im Wandel, FS Miklau (Studienverlag 2006) [FS Miklau]
- *Österreichische Juristenkommission* (Hrsg), Grundrechte in der Informationsgesellschaft (NWV 2001)
- *Österreichischer Juristentag* (Hrsg), Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit. Referate und Diskussionsbeiträge, 18. ÖJT Band I/2 (Manz 2012)
- *Plöckinger Oliver/Duursma Dieter/Helm Günther* (Hrsg), Aktuelle Entwicklungen im Internet-Recht (NWV 2002) [Aktuelle Entwicklungen]
- *Plöckinger Oliver/Duursma Dieter/Mayrhofer Michael* (Hrsg), Internet-Recht (NWV 2004)
- *Rechenberg Peter/Pomberger Gustav* (Hrsg), Informatik Handbuch[4] (Hanser 2006) [Informatik]
- *Schweighofer Erich/Liebwald Doris/Drachsler Mathias/Geist Anton* (Hrsg), e-Staat und e-Wirtschaft aus rechtlicher Sicht. Tagungsband des 9. Internationalen Rechtsinformatik Symposions IRIS 2006 (Boorberg 2006) [IRIS 2006]
- *Schweighofer Erich/Geist Anton/Staufer Ines* (Hrsg), Globale Sicherheit und proaktiver Staat – Die Rolle der Rechtsinformatik. Tagungsband des 13. Internationalen Rechtsinformatik Symposions IRIS 2010 (Boorberg 2010) [IRIS 2010]
- *Sieverts Rudolf/Schneider Hans J.* (Hrsg), Handwörterbuch der Kriminologie. Bd 5 (Walter de Gruyter 1998)
- *Staudegger Elisabeth/Thiele Clemens* (Hrsg), Geistiges Eigentum. Jahrbuch 2012 (NWV 2013)
- *Stiftung Dokumentationsarchiv des österreichischen Widerstandes* (Hrsg), Das Netz des Hasses (Stiftung Dokumentationsarchiv des österreichischen Widerstandes 1997)

- *Stavroulakis Peter/Stamp Mark* (Eds), Handbook of Information and Communication Security (Springer 2010) [Handbook]
- *Studiengesellschaft für Wirtschaft und Recht* (Hrsg), Geheimnisschutz – Datenschutz – Informationsschutz (Linde 2008) [Geheimnisschutz]
- *Terlitza Ulfried/Schwarzenegger Peter/Borić Tomislav* (Hrsg), Die internationale Dimension des Rechts, FS Posch (Verlag Österreich 1996) [FS Posch]
- *Weiß Norman* (Hrsg), Rechtentwicklungen im vereinten Deutschland (Universitätsverlag Potsdam 2011)
- *Wiebe Andreas* (Hrsg), Internetrecht. Zivilrechtliche Rahmenbedingungen des elektronischen Geschäftsverkehrs (Springer 2004)
- *Zankl Wolfgang* (Hrsg), Auf dem Weg zum Überwachungsstaat? (facultas. wuv 2009) [Überwachungsstaat]

3. Beiträge in Festschriften und Sammelbänden

- *Altenhain,* IT-Strafrecht – Entstehung eines Rechtsgebiets, in Weiß (Hrsg), Rechtentwicklungen im vereinten Deutschland (2011) 117
- *Beclin,* § 107a StGB – Bekämpfung von »Stalking« auf Kosten der Rechtssicherheit?, in BMJ (Hrsg), 34. Ottensteiner Fortbildungsseminar aus Strafrecht und Kriminologie. Bd 127 (2006) 103
- *Bergauer,* Ausgewählte Aspekte der strafrechtlichen Betrachtung von Spyware, in Schweighofer/Liebwald/Drachsler/Geist (Hrsg), e-Staat und e-Wirtschaft aus rechtlicher Sicht. Tagungsband des 9. Internationalen Rechtsinformatik Symposions IRIS 2006 (2006) 327
- *Bergauer,* Viren, Würmer, Trojanische Pferde – Computerstrafrecht auf dem Prüfstand, in BMJ (Hrsg), 35. Ottensteiner Fortbildungsseminar aus Strafrecht und Kriminologie. Bd 132 (2007) 27
- *Bergauer,* Phishing und Geldkuriere im Strafrecht, in Bergauer/Staudegger (Hrsg), Recht und IT. Zehn Studien (2009) 109
- *Bergauer,* Ehrenbeleidigungen im Web 2.0 aus strafrechtlicher Sicht, in Gögele/Unger (Hrsg), IT-Sicherheit aus rechtlicher, wirtschaftlicher und technologischer Perspektive (2010) 6
- *Bergauer,* Änderungen der strafrechtsrelevanten Bestimmungen des DSG 2000 durch die Novelle 2010, in Jahnel (Hrsg), Datenschutzrecht. Jahrbuch 2010 (2010) 73
- *Bergauer,* Indirekt personenbezogene Daten – datenschutzrechtliche Kuriosa, in Jahnel (Hrsg), Datenschutzrecht. Jahrbuch 2011 (2011) 55
- *Bergauer/Schmölzer,* Strafrecht, in Jahnel/Mader/Staudegger (Hrsg), IT-Recht[3] (2012) 635
- *Berka,* Geheimnisschutz – Datenschutz – Informationsschutz im Lichte der Verfassung, in Studiengesellschaft für Wirtschaft und Recht (Hrsg), Geheimnisschutz – Datenschutz – Informationsschutz (2008) 53

- *Blaschek,* Mensch-Maschine-Kommunikation, in Rechenberg/Pomberger (Hrsg), Informatik Handbuch[4] (2006) 839
- *Brandstetter,* Neues aus dem Besonderen Teil des StGB, in Mitgutsch/Wessely (Hrsg), Strafrecht. Besonderer Teil. Jahrbuch 2012 (2012) 13
- *Brush,* Cyberspace, in Jones (Ed), Encyclopedia of New Media (2003) 112
- *Durl,* Ausgewählte Aspekte des Normativs Zeit im StGB, in BMJ (Hrsg), 32. Ottensteiner Fortbildungsseminar aus Strafrecht und Kriminologie. Bd 117 (2005) 55
- *Duschanek,* Datenschutzrecht, in Holoubek/Potacs (Hrsg), Handbuch des öffentlichen Wirtschaftsrechts[2]. Bd 1 (2008) 299
- *Emigh/Ramazan,* Overview of Crimeware, in Jacobsson/Ramzan (Eds), Crimeware. Understanding New Attacks and Defenses (2008) 2
- *Engelmann/Großmann,* Was wissen wir über Information?, in Hildebrand/Gebauer/Hinrichs/Mielke (Hrsg), Daten- und Informationsqualität[2] (2011) 3
- *Feiler,* Die SPG-Novelle 2007, in Zankl (Hrsg), Auf dem Weg zum Überwachungsstaat? (2009) 43
- *Feiler,* Technische Aspekte der Online-Durchsuchung, in Zankl (Hrsg), Auf dem Weg zum Überwachungsstaat? (2009) 173
- *Fercher,* Manuelle Dateien im Datenschutzgesetz 2000, in Jahnel/Siegwart/Fercher (Hrsg), Aktuelle Fragen des Datenschutzrechts (2007) 33
- *Garstka,* Grundbegriffe für den Datenschutz, in Kilian/Lenk/Steinmüller (Hrsg), Datenschutz. Juristische Grundfragen beim Einsatz elektronischer Datenverarbeitungsanlagen in Wirtschaft und Verwaltung (1973) 209
- *Gildemeister,* Cyber Crime – Herausforderungen in der Praxis, in Landesgruppe Österreich der Internationalen Strafrechtsgesellschaft (AIDP) und Juristenverband (Hrsg), Cyber Crime – Zunehmende Bedrohung der Informationsgesellschaft (2012) 23
- *Glaser,* Bitcoins aus strafrechtlicher Sicht, in Eberwein/Steiner (Hrsg), Bitcoins (2014) 127
- *Hattenberger,* Videoüberwachung im Arbeitsverhältnis, in Jahnel (Hrsg), Datenschutzrecht. Jahrbuch 2010 (2010) 29
- *Heghmanns,* Straftaten gegen die betriebliche Datenverarbeitung, in Achenbach/Ransiek (Hrsg), Handbuch Wirtschaftsstrafrecht[3] (2012) 741
- *Hellwagner,* Arbeitsspeicher- und Bussysteme, in Rechenberg/Pomberger (Hrsg), Informatik Handbuch[4] (2006) 363
- *Hinterhofer,* Geheimnisschutz – Datenschutz – Informationsschutz im Strafrecht, in Studiengesellschaft für Wirtschaft und Recht (Hrsg), Geheimnisschutz – Datenschutz – Informationsschutz (2008) 169
- *Hoagland/Ramazan/Satish,* Bot Networks, in Jacobsson/Ramzan (Eds), Crimeware. Understanding New Attacks and Defenses (2008) 183

- *Hödl,* Ubiquitous Computing und soziale Gerechtigkeit, in Schweighofer/Geist/Staufer (Hrsg), Globale Sicherheit und proaktiver Staat – Die Rolle der Rechtsinformatik. Tagungsband des 13. Internationalen Rechtsinformatik Symposions IRIS 2010 (2010) 419
- *Hochmayr,* Besitz als strafbare Handlung, in BMJ (Hrsg), 33. Ottensteiner Fortbildungsseminar aus Strafrecht und Kriminologie. Bd 118 (2005) 87
- *Hochmayer,* Wert- und Schadensqualifikationen versus Regelbeispiele, in Joerden/Scheffler/Sinn/Wolf (Hrsg), Vergleichende Strafrechtswissenschaft, FS Swarc (2009) 235
- *Jahnel,* Datenschutzrecht, in Jahnel/Schramm/Staudegger (Hrsg), Informatikrecht[2] (2003) 241
- *Jahnel,* Datenschutzrecht, in Jahnel/Mader/Staudegger (Hrsg), IT-Recht[3] (2012) 415
- *Jahnel,* Das Grundrecht auf Datenschutz nach dem DSG 2000, in Akyürek/Baumgartner/Jahnel/Lienbacher/Stolzlechner (Hrsg), Staat und Recht in europäischer Perspektive, FS Schäffer (2006) 313
- *Jahnel,* Begriff und Arten von personenbezogenen Daten, in Jahnel (Hrsg), Datenschutzrecht und E-Government. Jahrbuch 2008 (2008) 27
- *Jahnel,* Dreifacher Datenschutz?, in Bergauer/Staudegger (Hrsg), Recht und IT. Zehn Studien (2009) 33
- *Jaksch-Ratajczek,* Urheberrechtliche Fragen zu im Internet bereitgestellten Lernmaterialien an Universitäten und Fachhochschulen, in Jaksch-Ratajczek (Hrsg), Aktuelle Rechtsfragen der Internetnutzung (2010) 99
- *König,* »Videoüberwachung und Datenschutz – ein Kräftemessen«, in Jahnel/Siegwart/Fercher (Hrsg), Aktuelle Fragen des Datenschutzrechts (2007) 109
- *Kotschy,* Grundrechte und staatliche EDV-Register, in ÖJK (Hrsg), Grundrechte in der Informationsgesellschaft (2001) 88
- *Kotschy,* Datenschutzrechtliche Rechtsfragen der Videoüberwachung, in Bammer/Holzinger/Vogl/Wenda (Hrsg), Rechtsschutz gestern – heute – morgen, FS Machacek/Matscher (2008) 257
- *Kotschy,* Das Grundrecht auf Geheimhaltung personenbezogener Daten, in Jahnel (Hrsg), Datenschutzrecht und E-Government. Jahrbuch 2012 (2012) 28
- *Lehner/Lachmayer,* Datenschutz im Verfassungsrecht, in Bauer/Reimer (Hrsg), Handbuch Datenschutzrecht (2009) 95
- *Lienbacher,* Datenschutzrecht und Staatsorganisation, in Österreichischer Juristentag (Hrsg), Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit. Referate und Diskussionsbeiträge, 18. ÖJT Band I/2 (2012) 17
- *Mader,* Neues zum Online Banking, in Bergauer/Staudegger (Hrsg), Recht und IT. Zehn Studien (2009) 67

- *Mitgutsch,* Ausgewählte Probleme der Freiheitsdelikte – Beharrliche Verfolgung und fortgesetzte Gewaltausübung, in Mitgutsch/Wessely (Hrsg), Strafrecht Besonderer Teil. Jahrbuch 2010 (2010) 21
- *Neubauer,* Technische Schutzmaßnahmen und Recht, in Wiebe (Hrsg), Internetrecht. Zivilrechtliche Rahmenbedingungen des elektronischen Geschäftsverkehrs (2004) 113
- *Piller,* die Chipkarte in Österreich, in Arbeitsgemeinschaft für Datenverarbeitung (Hrsg), Quo vadis EDV? – Realität und Vision. 8. Internationaler Kongress Datenverarbeitung im Europäischen Raum (1987) 374
- *Pittaro,* Cyber Stalking: Topology, Etiology, and Victims, in Jaishankar (Ed), Cyber Criminology. Exploring Internet Crimes Criminal Behavior (2011) 277
- *Plöckinger,* Internet und materielles Strafrecht – Die Convention on Cyber-Crime, in Plöckinger/Duursma/Helm (Hrsg), Aktuelle Entwicklungen im Internet-Recht (2002) 113
- *Plöckinger,* Die neuen Tatbestände zum Schutz unbarer Zahlungsmittel, in BMJ (Hrsg), 33. Ottensteiner Fortbildungsseminar aus Strafrecht und Kriminologie. Bd 118 (2005) 103
- *Rauch,* »Happy-Slapping« und Paparazzi – Die strafrechtliche Erfassung zweier ungleicher Phänomene, in Mitgutsch/Wessely (Hrsg), Strafrecht Besonderer Teil. Jahrbuch 2010 (2010) 89
- *Reindl,* Das neue Computerstrafrecht – ein Überblick, in BMJ (Hrsg), Vorarlberger Tage 2003. Bd 115 (2003) 63
- *Reindl-Krauskopf,* Strafrechtliche Aspekte der Datenverwendung, in Brodil (Hrsg), Datenschutz im
- Arbeitsrecht. Mitarbeiterüberwachung versus Qualitätskontrolle (2010) 73
- *Rill,* Das Grundrecht auf Datenschutz, in Duschanek (Hrsg), Datenschutz in der Wirtschaft (1981) 15
- *Rohling/May,* Informations- und Codierungstheorie, in Rechenberg/Pomberger (Hrsg), Informatik Handbuch[4] (2006) 211
- *Salimi,* Zahnloses Cyberstrafrecht? Eine Analyse der gerichtlichen Straftatbestände zum Daten- und Geheimnisschutz, in Landesgruppe Österreich der Internationalen Strafrechtsgesellschaft (AIDP) und Juristenverband (Hrsg), Cyber Crime – Zunehmende Bedrohung der Informationsgesellschaft (2012) 32
- *Schick,* Die Bekämpfung der Wirtschaftskriminalität in Österreich mit den Mitteln des Strafrechts, in BMJ (Hrsg), Strafrechtliche Probleme der Gegenwart. 5. Strafrechtliches Strafrecht 1977 (1978) 98
- *Schmölzer,* Computer-Kriminalität: Probleme und Reformbestrebungen – national/international, in Arbeitsgemeinschaft für Datenverarbeitung (Hrsg), Quo vadis EDV? – Realität und Vision. 8. Internationaler Kongress Datenverarbeitung im Europäischen Raum (1987) 724
- *Schmölzer,* Entwicklung von Gesetzgebung und Rechtsprechung in Computer-Strafsachen, in BMJ (Hrsg), Strafrechtliche Probleme der Gegenwart. 16. Strafrechtliches Seminar 1988 (1989) 195.

- *Schmölzer,* Computer-Kriminalität – kriminologische und kriminalpolitische Überlegungen, in Jehle/Maschke/Szabo (Hrsg), Strafrechtspraxis und Kriminologie², FS Göppinger (1990) 237
- *Schmölzer,* Computer-Netzwerke und Strafrecht – eine internationale Herausforderung, in Terlitza/Schwarzenegger/Boric (Hrsg), Die internationale Dimension des Rechts, FS Posch (1996) 321
- *Schmölzer,* Strafrechtliche Aspekte zum Thema Rassismus, Neonazismus und Rechtsextremismus im Internet, in Stiftung Dokumentationsarchiv des österreichischen Widerstandes (Hrsg), Das Netz des Hasses (1997) 246
- *Schmölzer,* Internet und Strafrecht, in BMJ (Hrsg), Strafrechtliche Probleme der Gegenwart. 26. Strafrechtliches Seminar 1998 (1998) 129
- *Schmölzer,* Überwachung von Nachrichten und Auskunft über Daten einer Nachrichtenübermittlung nach altem und nach neuem Recht. Von der Fernmelde- zur Telekommunikations-Überwachung – eine problemorientierte Genealogie, in Moos/Jesionek/Müller (Hrsg), Strafprozessrecht im Wandel, FS Miklau (2006) 467
- *Schmölzer,* Strafrecht, in Jahnel/Schramm/Staudegger (Hrsg), Informatikrecht² (2003) 335
- *Schmölzer,* Die neue Rolle des Strafrechts im Internet, in Bergauer/Staudegger (Hrsg), Recht und IT. Zehn Studien (2009) 1
- *Schmoller,* Zum Tatbestand der Täuschung – § 108 StGB nach dem StrafrechtsänderungsG 1987, in BMJ (Hrsg), Strafrechtliche Probleme der Gegenwart. 16. Strafrechtliches Seminar 1988 (1989) 1
- *Schmoller,* Private Videoüberwachung – ein Beweismittel im Strafprozess?, in Bammer/Holzinger/Vogl/Wenda (Hrsg), Rechtsschutz gestern – heute – morgen, FS Machacek/Matscher (2008) 1065
- *Schramm,* Zum Beispiel: Der Lehrgang für Rechtsinformatik an der Karl-Franzens-Universität Graz, in Mayer-Schönberger/Schneider-Manns-Au (Hrsg), Der Jurist am Info-Highway. Über die Zukunft eines Berufsstandes (1997) 161
- *Schramm,* Informationstechnologie: Ausgewählte Themen, in Jahnel/Schramm/Staudegger (Hrsg), Informatikrecht² (2003) 1
- *Schwarzenegger,* Hyperlinks und Suchmaschinen aus strafrechtlicher Sicht, in Plöckinger/Duursma/Mayrhofer (Hrsg), Internet-Recht (2004) 395
- *Siegwart,* Das Veröffentlichen von Daten, in Jahnel/Siegwart/Fercher (Hrsg), Aktuelle Fragen des Datenschutzrechts (2007) 211
- *Sonntag,* Informationstechnologie: Grundlagen, in Jahnel/Mader/Staudegger (Hrsg), IT-Recht³ (2012) 1
- *Soyer,* Über neue Kriminalitätsformen aus konsumentenpolitischer Perspektive – »de lege lata« und »de lege ferenda«, in Enthofer-Stoisser/Habersberger (Hrsg), Catch me if you can! Internet«abzocke«, »cold calls« und unseriöse Werbeveranstaltungen (2012) 107

- *Spenling,* Zivilverfahren und Datenschutz – Eine erste Orientierung zu den neuen §§ 83 bis 85 GOG, in BMJ (Hrsg), Vorarlberger Tage 2005. Bd 125 (2006) 135
- *Starzer,* Dem Stalker auf der Spur – Ein Resümee über fast fünf Jahre § 107a StGB, in BMJ (Hrsg), 39. Ottensteiner Fortbildungsseminar aus Strafrecht und Kriminologie, Bd 150 (2011) 41
- *Staudegger,* Sachenrechtliche Implikationen des »Internet der Dinge«, in Schweighofer/Geist/Staufer (Hrsg), Globale Sicherheit und proaktiver Staat – Die Rolle der Rechtsinformatik. Tagungsband des 13. Internationalen Rechtsinformatik Symposions IRIS 2010 (2010) 413
- *Staudegger,* Die Rechtsprechung des EuGH in Urheberrechtssachen im Jahr 2012, in Staudegger/Thiele (Hrsg), Geistiges Eigentum. Jahrbuch 2012 (2013) 1
- *Uthemann,* Computerkriminalität, in Sieverts/Schneider (Hrsg), Handwörterbuch der Kriminologie. Bd 5 (1998) 265
- *Wang/Aslam/Zou,* Peer-to-Peer Botnets, in Stavroulakis/Stamp (Eds), Handbook of Information and Communication Security (2010) 335
- *Wegscheider,* Computerstrafrecht, in BMJ (Hrsg), Strafrechtliche Probleme der Gegenwart. 17. Strafrechtliches Seminar 1989 (1990) 127
- *Wennig,* Cybercrime, in Landesgruppe Österreich der Internationalen Strafrechtsgesellschaft (AIDP) und Juristenverband (Hrsg), Cyber Crime – Zunehmende Bedrohung der Informationsgesellschaft (2012) 47

4. Beiträge in Zeitschriften

- *Bergauer,* Phishing – eine kernstrafrechtliche Betrachtung, RZ 2006, 82
- *Bergauer,* Sniffer-Tools – unwillkommene Spyware: Ein Sniffer-Angriff unter § 118a StGB subsumiert, RdW 2006/391, 412
- *Bergauer,* Kritische Anmerkungen zu § 126c StGB, ÖJZ 2007/45, 532
- *Bergauer,* Computerwürmer und Gemeingefährdungsdelikte im Strafrecht, jusIT 2008/2, 2
- *Bergauer,* Online-Durchsuchung: Rechtliche und technische Überlegungen, jusIT 2008/19, 47
- *Bergauer,* Verbreitung von Kinderpornografie und verbotene Veröffentlichung über das Internet, jusIT 2008/82, 175
- *Bergauer,* Aktuelles zum Computerstrafrecht – zugleich eine Buchbesprechung, jusIT 2010/58, 132
- *Bergauer,* OGH: Verletzung des Grundrechts auf Datenschutz unter Missbrauch der Amtsgewalt, jusIT 2012/13, 30
- *Bergauer,* OGH: Die üble Nachrede – ein Erfolgsdelikt?, jusIT 2012/26, 60
- *Bergauer,* Gesetzgebungsmonitor Computerstrafrecht: Ratifikation des Übereinkommens über Computerkriminalität, jusIT 2012/95, 205

- *Bergauer,* Der Handel mit Patientendaten – eine (datenschutzrechtliche) Straftat?, ÖJZ 2013/113, 958
- *Bergauer,* Das Betreiben eines Anonymisierungsdienstes im Internet als strafbarer Beitrag zur Verbreitung von Kinderpornografie? Zugleich eine Anmerkung zu LG für Strafsachen Graz 30.6.2014, 7 Hv 39/14p, jusIT 2014/77, 161
- *Bergauer,* Heimliche Nacktaufnahmen und deren Veröffentlichung im Internet in Anbetracht der Strafbestimmung des § 51 DSG 2000 – zugleich eine Anmerkung zu OLG Wien 14.11.2013, 23 Bs 351/13f, jusIT 2015/3, 9
- *Bergauer/Thiele,* Rezension zu *Farsam Salimi* in WK² DSG § 51. Auszug aus *Höpfel/Ratz* (Hrsg), Wiener Kommentar zum Strafgesetzbuch, jusIT 2012/74, 158
- *Bernreiter,* Zum »StRÄG 2015« und den Änderungen im Bereich des Computerstrafrechts, jusIT 2015/52, 128
- *Betzl,* Computerkriminalität – Dichtung und Wahrheit, DSWR 1972, 317
- *Betzl,* Computerkriminalität – Viel Lärm um Nichts, DSWR 1972, 475
- *Brandstetter,* Die tätige Reue in der Judikatur des OGH, JBl 1987, 545
- *Burgstaller,* Über den Verbrechensversuch, JBl 1969, 521
- *Burgstaller,* Der Versuch nach § 15, JBl 1976, 113
- *Burgstaller,* Die Scheinkonkurrenz im Strafrecht (I), JBl 1978, 393
- *Burgstaller,* Die Scheinkonkurrenz im Strafrecht (II), JBl 1978, 459
- *Burgstaller,* Wirtschaftsstrafrecht in Österreich, JBl 1984, 577
- *Cohen,* Computerviruses – Theory and Experiments, Computers and Security 1984, 22
- *Engin-Deniz/Grünzweig,* P-TV-Piraterie im Strafrecht, ecolex 2001, 587
- *Ernst,* Das neue Computerstrafrecht, NJW 2007, 2661
- *Evers,* Der Schutz des Privatlebens und das Grundrecht auf Datenschutz in Österreich, EuGRZ 1984, 290
- *Fuchs,* Zum Entwurf von Strafbestimmungen gegen die Computerkriminalität, RdW 1985, 330
- *Gordon/Ford,* On the definition and classification of cybercrime. Journal in Computer Virology 2006, 13
- *Haft,* Das neue Computerstrafrecht, DSWR 1986, 255
- *Heissenberger,* Straf- und zivilrechtliche Aspekte der »Beharrlichen Verfolgung« gem § 107a StGB, AnwBl 2006, 634
- *Hilgendorf,* Die Neuen Medien und das Strafrecht, ZStW 2001/113, 650
- *Hödl,* Die Macht der klugen Dinge. Überlegungen zu ubiquitous computing, RFID-Chips und smart objects, juridikum 2007, 210
- *Jahnel,* OGH: Kein Schutz von Unternehmensdaten nach dem DSG?, RdW 2005/244, 200
- *Jahnel,* Die Meldung von Gesundheitsdaten an die Führerscheinbehörde aus datenschutzrechtlicher Sicht, jusIT 2008/8, 18

- *Jahnel,* Gesetzgebungsmonitor Datenschutz: Ministerialentwurf zu einer DSG-Novelle 2014, jusIT 2013/32, 58
- *Jahnel,* Gesetzgebungsmonitor Datenschutz: DSG-Novellen 2013 und 2014 kundgemacht, jusIT 2013/66, 142
- *Kalteis,* Polizeiliche Ermittlung von IP-Adressen nur mit richterlicher Genehmigung?, ZfV 2013/246, 184
- *Kienapfel,* Vorschläge zur Abänderung des Besonderen Teils, RZ 1981, 117
- *Kienapfel,* Dauerdelikt und Dauerstraftat am Beispiel der Begehungsformen der Hehlerei. Zugleich eine Besprechung der grundlegenden E eines verstärkten Senats OGH 16.10.1990, 15 Os 71/90, JBl 1991, 435
- *Kunnert,* Big Brother in U-Bahn, Bus und Bim. Videoaufzeichnung in öffentlichen Verkehrsmitteln aus datenschutzrechtlicher Sicht, juridikum 2006, 42
- *Lampe,* Computerkriminalität – nur fauler Zauber, DSWR 1974, 242
- *Lichtenstrasser/Mosing/Otto,* Wireless LAN – Drahtlose Schnittstelle für Datenmissbrauch?, ÖJZ 2003/14, 253
- *Liebscher,* Grundfragen des Wirtschaftsstrafrechts, JBl 1979, 225
- *Löschnigg,* Datenschutz und Kontrolle im Arbeitsverhältnis, DRdA 2006, 459
- *Mahler,* »Grooming«: Anbahnung von Sexualkontakten zu Unmündigen, JSt 2012, 22
- *Maleczky,* Das Strafrechtsänderungsgesetz 2002, JAP 2002/2003, 115
- *McAllister,* Strafrechtliche Auswirkungen der neuen »PayPass«-Funktion von Kredit- und Bankomatkarten, JBl 2014, 224
- *Medigovic,* Unterlassung der Anzeige nach § 84 StPO – Amtsmißbrauch?, JBl 1992, 420
- *Messner,* Anbahnung von Sexualkontakten zu Unmündigen. Der neue Grooming-Paragraf in § 208a StGB, JAP 2011/2012/12, 132
- *Mitgutsch,* Die geplante »Stalking«-Bestimmung des § 107a StGB, JSt 2006, 11
- *Mitgutsch,* Strafrechtliche Aspekte des »Anti-Stalking-Pakets«, RZ 2006, 186
- *Öhlbäck/Esztegar,* Rechtliche Qualifikation von Denial of Service Attacken, JSt 2011, 126
- *Pfersmann,* Bemerkenswertes aus der SZ 2006/I, ÖJZ 2008/98
- *Plöckinger,* Die neuen Tatbestände zum Schutz unbarer Zahlungsmittel und deren Verhältnis zu den Urkunden- und Vermögensdelikten, ÖJZ 2005/14, 256
- *Popp,* Computerstrafrecht in Europa Zur Umsetzung der »Convention on Cybercrime« in Deutschland und Österreich, MR-Int 2007, 84
- *Popp,* IT-Outsourcing und Cloud Computing – zwei neue Herausforderungen für die Criminal Compliance, JSt 2012, 30
- *Proske,* Hacking im Strafrecht, EDVuR 1990, 102
- *Prunner,* Missbrauch der Bankomatkarte eines Angehörigen – kein § 166 StGB?, JAP 2014/2015/1

- *Reindl-Krauskopf,* Das Phänomen »Phishing«, SIAK-Journal 2007, 2
- *Reindl-Krauskopf,* Cyberstrafrecht im Wandel, ÖJZ 2015/19, 112
- *Reindl,* Die nachträgliche Offenlegung von Vermittlungsdaten des Telefonverkehrs im Strafverfahren (»Rufdatenrückerfassung«), JBl 1999, 791
- *Reindl,* Telefonüberwachung zweimal neu?, JBl 2002, 69
- *Rosenmayr-Klemenz,* Zum Schutz manuell verarbeiteter Daten durch das DSG 2000 – Gleichzeitig eine Bemerkung zum Beschluss des OGH vom 28.6.2000, 6 Ob 148/00h = ÖJZ 2001/1 (EvBl), ecolex 2001, 639
- *Sadoghi,* Stalking – eine differenzierte Betrachtung dogmatischer Probleme, AnwBl 2007, 340
- *Salimi,* Zahnloses Cyberstrafrecht? Eine Analyse der gerichtlichen Straftatbestände zum Daten- und Geheimnisschutz, ÖJZ 2012/115, 998
- *Sautner,* Neue Straftatbestände zum Schutz unbarer Zahlungsmittel, RZ 2004, 26
- *Sautner/Unterlerchner,* Kriminalpolitische und dogmatische Bemerkungen zu einer Reform des StGB, ÖJZ 2014/10, 63
- *Schick,* Rezension zu *Otto Triffterer,* Die österreichische Beteiligungslehre. Eine Regelung zwischen Einheitstäter- und Teilnahmesystemen?, ÖJZ 1984, 475
- *Schick/Schmölzer,* Das österreichische Computerstrafrecht – eine Bestandsaufnahme EDVuR 1992, 107.
- *Schmölzer,* Legistische Tendenzen im Computer-Strafrecht, RZ 1986, 178
- *Schmölzer,* Das neue Computer-Strafrecht (Strafrechtsänderungsgesetz 1987), EDVuR 1988, 20
- *Schmölzer,* Prozessuale Zwangsmittel im Fernmeldewesen – Beschlagnahme oder Überwachung, RZ 1988, 247
- *Schmölzer,* Die unbefugte Verwendung einer fremden Bankomatkarte – Strafrechtliche Aspekte, EDVuR 1990, 30
- *Schmölzer,* Geldspielautomaten im österreichischen Strafrecht, ÖJZ 1993, 507
- *Schmölzer,* Rückwirkende Überprüfung von Vermittlungsdaten im Fernmeldeverkehr – Anmerkungen zu OGH 6.12.1995, 13 Os 161/95, JBl 1997, 211
- *Schmölzer,* Straftaten im Internet: eine materiell-rechtliche Betrachtung, ZStW 2011/123, 709
- *Schmölzer/Mayer-Schönberger,* Das Telekommunikationsgesetz 1997 – Ausgewählte rechtliche Probleme, ÖJZ 1998, 378
- *Schroll,* Zu den reuefähigen Delikten des Vermögensstrafrechts, ÖJZ 1985, 357
- *Schuhr,* Analogie und Verhaltensnorm im Computerstrafrecht, ZIS 2012, 441
- *Schwaighofer,* Neue Ansichten des OGH zum Gewahrsamsbegriff – Bemerkungen zu 13 Os 69/11p, JSt 2012, 66
- *Seidl,* Debit Card Fraud: Strafrechtliche Aspekte des sog. »Skimmings«, ZIS 2012, 415

- *Seiler,* Kritische Anmerkungen zum StRÄG 1987 betreffend den Besonderen Teil des StGB, JB1 1989, 746
- *Sieben/von zur Mühlen,* Computerkriminalität – Viel Lärm um Nichts?, DSWR 1972, 252
- *Sieben/von zur Mühlen,* Computerkriminalität – nicht Dichtung, sondern Wahrheit, DSWR 1972, 397
- *Sieber,* Der strafrechtliche Schutz der Information, ZStW 1991/103, 780
- *Sieber,* Computerkriminalität und Informationsstrafrecht, CR 1995, 100
- *Sonntag,* Die EU-Richtlinie über Angriffe auf Informationssysteme, jusIT 2014/2, 8
- *Staudegger,* Zur Qualifikation von Verträgen, die der Überlassung von Computersoftware dienen, JBl 1998, 604
- *Staudegger,* Software-Erstellung: Vertragstyp und Quellcodeherausgabe, JBl 2006, 195
- *Staudegger,* Suche von Entscheidungen mit Aktenzeichen bzw »Geschäftszahl«, jusIT 2008/13, 33
- *Steininger H.,* Typische Erscheinungsformen der Wirtschaftskriminalität und ihre Bekämpfung, ÖJZ 1982, 589
- *Strauss,* Technische und organisatorische Maßnahmen zur Abwehr von Computerviren, EDVuR 1989, 130
- *Thiele,* Unbefugte Bildaufnahme und ihre Verbreitung im Internet – Braucht Österreich einen eigenen Paparazzi-Paragrafen?, RZ 2007, 2
- *Thiele,* Persönlichkeitsschutz in Neuen Medien – Facebook, Google & Co, AnwBl 2013, 11
- *Tiegs,* Computerkriminalität – Probleme ihrer legistischen Erfassung, JBl 1986, 708
- *Uepping,* Computermißbrauch ... aus Sicht der Informatik – Betrachtungen zur Computerkriminalität, DSWR 1985, 323
- *Vassilaki,* Multimediale Kriminalität – Entstehung, Formen und rechtspolitische Fragen der »Post-Computerkriminalität«, CR 1997, 297
- *Velten,* Stalking (Teil I), JSt 2003, 159
- *Venier,* Das neue Ermittlungsverfahren: Eine Reform und ihre Mängel, ÖJZ 2009/66
- *Venier,* Die Online-Durchsuchung. Oder: Die Freiheit der Gedanken, AnwBl 2009, 480
- *Wach,* »Unbare Zahlungsmittel« iSd § 74 Abs 1 Z 10 StGB – droht eine Ausuferung der Strafbarkeit?, RZ 2005, 130
- *Weiser,* The Computer for the Twenty-First Century, Scientific American 1991, 66
- *Weiser,* Some Computer Science Problems in Ubiquitous Computing, Communications of the ACM 1993, 75

- *Weiß,* Kritische Betrachtung des Täuschungstatbestandes aus straf- und verfassungsrechtlicher Sicht – zugleich ein Beitrag zur Bestimmtheit von Strafnormen (Teil I), AnwBl 1989, 185
- *Weiß,* Kritische Betrachtung des Täuschungstatbestandes aus straf- und verfassungsrechtlicher Sicht – zugleich ein Beitrag zur Bestimmtheit von Strafnormen (Teil II), AnwBl 1989, 246
- *Wessely,* Das Fernmeldegeheimnis – ein unbekanntes Grundrecht?, ÖJZ 1999, 491
- *Wiebe,* Das neue »digitale« Urheberrecht – Eine erste Bewertung, MR 2003, 309
- *Wieser,* Der Versuch beim Vorbereitungsdelikt (Teil I), JBl 1987, 497
- *Wolfrum/Dimmel,* Das »Anti-Stalking-Gesetz«, ÖJZ 2006/29, 475
- **Gesetzeskommentare:**
- *Dammann Ulrich/Simitis Spiros,* EG-Datenschutzrichtlinie. Kommentar (Nomos 1997)
- *Dohr Walter/Pollirer Hans/Weiss Ernst/Knyrim Rainer,* DSG. Datenschutzrecht[2] (Manz, Stand 04.06.2013)
- *Fabrizy Ernst E.,* StGB und ausgewählte Nebengesetze[11] (Manz 2013) [StGB]
- *Höpfel Frank/Ratz Eckart* (Hrsg), Wiener Kommentar zum Strafgesetz[2] (Manz, Stand Juni 2012) [WK[2]]
- *Kletečka Andreas/Schauer Martin* (Hrsg), ABGB-ON (Manz, Stand September 2014)
- *Korinek Karl/Holoubek Michael* (Hrsg), Österreichisches Bundesverfassungsrecht. Kommentar (Springer, 10. Lfg) [Bundesverfassungsrecht]
- *Koziol Helmut/Bydlinski Peter/Bollenberger Raimund* (Hrsg), Kommentar zum ABGB[3] (Springer 2010) [KBB]
- *Kucsko Guido* (Hrsg), urheber.recht (Manz, Stand Dezember 2007)
- *Leukauf Otto/Steininger Herbert,* Kommentar zum österreichischen StGB[3] (Prugg 1992) [StGB]
- *Laufhütte Heinrich Wilhelm/Rissing-van Saan Ruth/Tiedemann Klaus* (Hrsg), Leipziger Kommentar StGB[12]. Bd 9/1 (De Gruyter Recht 2012) [LK]
- *Matzka Manfred* (Hrsg), Datenschutzrecht für die Praxis. Kommentar (Orac 1986-1988) (3. Lfg) [Datenschutzrecht]
- *Röggla Werner/Wittmann Heinz/Zöchbauer Peter* (Hrsg), Medienrecht. Praxiskommentar (Medien und Recht 2012)
- *Rummel Peter* (Hrsg), ABGB I[3] (Manz 2000)
- *Schwimann Michael/Kodek Georg E.* (Hrsg), ABGB Praxiskommentar. Bd II[4] (LexisNexis 2012)
- *Triffterer Otto/Rosbaud Christian/Hinterhofer Hubert* (Hrsg), Salzburger Kommentar zum StGB (LexisNexis, Stand Dezember 2013) [SbgK]

5. Beiträge in Gesetzeskommentaren

- *Bachner-Foregger* in WK² § 254 (Stand November 2012)
- *Bertel* in WK² § 108 (Stand August 2000)
- *Bertel* in WK² § 109 (Stand August 2000)
- *Bertel* in WK² § 125 (Stand Dezember 2008)
- *Bertel* in WK² § 126 (Stand Dezember 2008)
- *Bertel* in WK² § 126a (Stand Dezember 2008)
- *Bertel* in WK² § 127 (Stand Dezember 2008)
- *Bertel* in WK² § 129 (Stand Dezember 2008)
- *Bertel* in WK² § 141 (Stand Dezember 2008)
- *Bertel* in WK² § 310 (Stand Mai 2010)
- *Daxecker* in SbgK § 126b (Stand Mai 2012)
- *Daxecker* in SbgK § 126c (Stand Mai 2012)
- *Eccer* in KBB³ § 353 (Stand Juli 2010)
- *Eder-Rieder* in SbgK § 254 (Stand November 2010)
- *Fabrizy* in WK² § 12 (Stand 01.05.2014)
- *Gaderer* in Kucsko (Hrsg), urheber.recht § 18a (Stand Dezember 2007)
- *Hager/Massauer* in WK² §§ 15, 16 (Stand Dezember 1999)
- *Hinterhofer* in SbgK § 207a (Stand November 2006)
- *Hinterhofer* in SbgK § 283 (Stand Februar 2001)
- *Hoffmann* in Schwimann/Kodek (Hrsg), ABGB Praxiskommentar⁴ § 292 Rz 3 (Stand Mai 2012)
- *Holzner* in Kletečka/Schauer (Hrsg), ABGB-ON § 353 (Stand September 2014)
- *Jerabek* in WK² § 69 (Stand Juli 2013)
- *Jerabek* in WK² § 70 (Stand Juli 2013)
- *Jerabek/Reindl-Krauskopf/Schroll* in WK² § 74 (Stand Juli 2013)
- *Kathrein* in KBB³ § 5i KSchG (Stand Juli 2010)
- *Kert* in SbgK § 146 (Stand Mai 2012)
- *Kienapfel/Schroll* in WK² § 223 (Stand Juli 2006)
- *Kienapfel/Schroll* in WK² § 224a (Stand Juli 2006)
- *Kienapfel/Schroll* in WK² § 229 (Stand Juli 2006)
- *Kirchbacher* in WK² § 146 (Stand September 2011)
- *Kirchbacher* in WK² § 164 (Stand September 2011)
- *Kirchbacher* in WK² § 165 (Stand September 2011)
- *Kirchbacher* in WK² § 167 (Stand Juli 2013)
- *Kirchbacher/Presslauer* in WK² § 148a (Stand November 2009)
- *Kirchbacher/Presslauer* in WK² § 149 (Stand November 2009)

- *Kirchbacher/Presslauer* in WK² § 150 (Stand November 2009)
- *Klicka* in Schwimann/Kodek (Hrsg), ABGB Praxiskommentar⁴ § 354 Rz 1 (Stand Mai 2012)
- *Komenda/Madl* in SbgK § 126a (Stand Juni 2013)
- *Komenda/Madl* in SbgK § 148a (Stand Dezember 2013)
- *Kotschy* in Matzka (Hrsg), Datenschutzrecht § 3 (Stand 3. Lfg)
- *Lambauer* in SbgK § 111 (Stand März 2009)
- *Lewisch* in WK² § 119 (Stand September 2008)
- *Lewisch* in WK² § 121 (Stand September 2008)
- *Lewisch/Reindl-Krauskopf* in WK² § 120 (Stand September 2008)
- *List* in SbgK § 215a (Stand November 2009)
- *Nimmervoll* in SbgK § 104a (Stand Mai 2010)
- *Nittel* in SbgK § 74 (Stand November 2006)
- *Oshidari* in SbgK § 241a (Stand April 2007)
- *Oshidari* in SbgK § 241b (Stand April 2007)
- *Oshidari* in SbgK § 241e (Stand April 2007)
- *Philipp* in WK² § 207a (Stand März 2014)
- *Philipp* in WK² § 208a (Stand März 2014)
- *Philipp* in WK² § 215a (Stand März 2014)
- *Plöchl* in WK² Vorbem §§ 274 ff (Stand Jänner 2014)
- *Plöchl* in WK² § 278 (Stand Jänner 2014)
- *Plöchl* in WK² § 278b (Stand Jänner 2014)
- *Plöchl/Seidl* in WK² § 295 (Stand September 2010)
- *Rainer* in SbgK § 70 (Stand Mai 1996)
- *Rainer* in SbgK § 167 (Stand Oktober 2003)
- *Rami* in WK² § 115 (Stand Dezember 2011)
- *Rami* in WK² MedienG § 1 (Stand Juli 2011)
- *Ratz* in WK² Vorbem §§ 28–31 (Stand Oktober 2011)
- *Reindl-Krauskopf* in WK² § 118a (Stand September 2008)
- *Reindl-Krauskopf* in WK² § 119a (Stand September 2008)
- *Reindl-Krauskopf* in WK² § 126b (Stand Dezember 2008)
- *Reindl-Krauskopf* in WK² § 126c (Stand Dezember 2008)
- *Reindl* in WK² § 225a (Stand Juli 2006)
- *Reindl-Krauskopf/Tipold/Zerbes* in WK-StPO § 134 (Stand Oktober 2009)
- *Salimi* in SbgK § 127 (Stand November 2012)
- *Salimi* in WK² DSG § 51 (Stand Mai 2012)
- *Schallmoser* in SbgK § 149 (Stand November 2011)

- *Schick* in WK² § 207a Rz 12 (Stand Mai 2007 aF)
- *Schmoller* in SbgK § 99 (Stand August 1993)
- *Schmoller* in SbgK § 108 (Stand Mai 1996)
- *Schroll* in WK² § 232 (Stand August 2007)
- *Schroll* in WK² § 233 (Stand August 2007)
- *Schroll* in WK² Vorbem §§ 241a – 241g (Stand Mai 2005)
- *Schroll* in WK² § 241a (Stand Mai 2005)
- *Schroll* in WK² § 241b (Stand Mai 2005)
- *Schroll* in WK² § 241c (Stand Mai 2005)
- *Schroll* in WK² § 241e (Stand Mai 2005)
- *Schroll* in WK² § 241 f (Stand Mai 2005)
- *Schwaighofer* in WK² § 107a (Stand November 2010)
- *Seiler* in SbgK § 125 (Stand August 1994)
- *Spielbüchler* in Rummel (Hrsg), ABGB I³ § 354 Rz 1 (Stand Jänner 2000)
- *Stockinger/Nemetz* in Kucsko (Hrsg), urheber.recht § 90c (Stand Dezember 2007)
- *Thiele* in SbgK Vorbem §§ 118 – 124 StGB (Stand März 2007)
- *Thiele* in SbgK § 118a (Stand März 2007)
- *Thiele* in SbgK § 119 (Stand März 2007)
- *Thiele* in SbgK § 119a (Stand März 2007)
- *Thiele* in SbgK § 120 (Stand Mai 2010)
- *Thiele* in SbgK § 225a (Stand März 2007)
- *Tiedemann/Valerius* in LK¹² (2012) § 263a (Stand Oktober 2011)
- *Tipold* in SbgK § 141 (Stand April 2004)
- *Tipold* in SbgK § 150 (Stand November 2004)
- *Triffterer* in SbgK § 126a (aF Stand Dezember 1992)
- *Triffterer* in SbgK § 148a (aF Stand Dezember 1992)
- *Triffterer* in SbgK § 278a (Stand Juni 1997)
- *Wach* in SbgK § 107a (Stand Mai 2008)
- *Wiederin* in Korinek/Holoubek (Hrsg), Bundesverfassungsrecht. Bd III Art 8 EMRK (5. Lfg 2002)
- *Wiederin* in Korinek/Holoubek (Hrsg), Bundesverfassungsrecht. Bd III Art 10a StGG (4. Lfg 2001)
- *Wittmann/Zöchbauer* in Röggla/Wittmann/Zöchbauer (Hrsg), Medienrecht. Praxiskommentar (2012) MedienG § 1

B. Judikaturverzeichnis

- OGH 01.02.1972, 10 Os 256/71
- OGH 03.05.1973, 10 Os 46/73
- OGH 05.03.1974, 10 Os 168/73
- OGH 30.09.1976, 9 Os 101/75
- OGH 08.03.1977, 9 Os 165/76
- OGH 21.06.1978, 10 Os 88/78
- OGH 07.09.1978, 12 Os 94/78
- OGH 10.10.1978, 11 Os 144/78
- OGH 24.11.1978, 13 Os 102/78
- OGH 03.07.1980, 12 Os 72/80
- OGH 29.07.1981, 11 Os 70/81
- OGH 28.01.1982, 12 Os 185/81
- OGH 09.09.1982, 12 Os 66/82
- OGH 11.01.1983, 10 Os 159/82
- OGH 06.10.1983, 12 Os 120/83
- OGH 19.12.1984, 11 Os 184/84
- OGH 12.02.1986, 9 Os 2/86
- OGH 22.05.1986, 12 Os 136/85
- OGH 26.06.1986, 12 Os 69/86
- OGH 02.09.1986, 11 Os 107/86
- OGH 30.10.1986, 12 Os 93/86
- OGH 19.11.1987, 13 Os 162/87
- OGH 23.06.1989, 16 Os 9/89
- OGH 24.10.1989, 15 Os 127/89
- OGH 21.11.1989, 15 Os 88/89
- OGH 20.12.1989, 14 Os 109/89 (14 Os 110/89)
- OGH 30.10.1990, 15 Os 79/90
- OGH 05.04.1991, 16 Os 6/91 (16 Os 7/91)
- OGH 18.09.1991, 1 Ob 22/91
- OGH 28.01.1993, 12 Os 128/92
- OGH 28.01.1993, 12 Os 135/92
- OGH 11.03.1993, 15 Os 156/92
- OGH 28.06.1994, 14 Os 78/94
- OGH 06.12.1995, 13 Os 161/95
- OGH 14.12.1995, 15 Os 131/95

- OGH 10.04.1996, 13 Os 17/96
- OGH 10.12.1996, 14 Os 71/96 (14 Os 78/96)
- OGH 13.02.1997, 12 Os 183/96
- OGH 17.06.1998, 13 Os 68/98
- OGH 13.10.1998, 14 Os 129/98 = JBl 2000, 554 *(Medigovic)*
- OGH 17.12.1998, 15 Os 175/98
- OGH 28.06.2000, 6 Ob 148/00h
- OGH 10.08.2000, 15 Os 64/00
- OGH 14.11.2000, 14 Os 128/00
- OGH 17.04.2002, 13 Os 179/01 = JBl 2003, 464 *(Schmoller)*
- OGH 13.06.2002, 8 ObA 288/01p = ASoK 2012, 172 *(Rauch)* = ASoK 2012, 300 *(Trattner)* = ÖJZ EvBl 2012/86, 604 *(Rohrer)* = DRdA 2013/16, 160 *(Eichinger)* = ZAS 2013/12, 75 *(Majoros)*
- OGH 03.09.2002, 11 Os 109/01
- OGH 17.12.2002, 4 Ob 248/02b = MR 2003, 33 *(Stomper)* = RdW 2003/298, 365 *(Handig)* = ecolex 2003/112, 254 *(Tonninger)* = MR 2003, 35 *(Krüger)*
- OGH 03.06.2003, 14 Os 51/03
- OGH 04.05.2004, 4 Ob 50/04p = RdW 2005/244, 200 *(Jahnel)* = ecolex 2004, 873 *(Knyrim)*
- OGH 21.10.2004, 15 Os 114/04
- OGH 11.01.2005, 11 Os 131/04
- OGH 02.03.2005, 13 Os 145/04 = JSt 2005/42, 201 *(Mitgutsch)*
- OGH 12.07.2005, 4 Ob 45/05d = ecolex 2005/445, 924 *(Braunböck)* = MR 2005, 379 *(Walter)*
- OGH 06.10.2005, 12 Os 82/05h (12 Os 83/05f)
- OGH 13.10.2005, 15 Os 99/05f
- OGH 22.11.2005, 14 Os 116/05y = JSt 2006/19, 52 *(Huber)* = JSt 2006/23, 93 *(Huber)* = AnwBl 2006/8056, 478 *(Hollaender)*
- OGH 14.12.2005, 13 Os 68/05g
- OGH 19.12.2005, 8 Ob 108/05y = ÖJZ EvBl 2006/67, 376 *(Noll)*
- OGH 23.02.2006, 12 Os 119/05z
- OGH 01.06.2006, 12 Os 45/06v
- OGH 08.06.2006, 15 Os 35/06w
- OGH 23.04.2007, 15 Os 6/07g
- OGH 28.06.2007, 12 Os 14/07m
- OGH 23.08.2007, 12 Os 88/07v
- OGH 27.09.2007, 12 Os 101/07f
- OGH 13.11.2007, 14 Os 123/07f

- OGH 01.04.2008, 11 Os 21/08k (11 Os 22/08g) = jusIT 2008/82, 175 *(Bergauer)*
- OGH 15.01.2009, 12 Os 151/08k
- OGH 19.02.2009, 2 Ob 107/08m = ecolex 2009, 577 *(Graf)* = ÖBA 2009/1551, 457 *(Bydlinski)* = jusIT 2009/69, 140 *(Mader)*
- OGH 24.02.2009, 9 Ob 3/08v = ecolex 2009, 577 *(Graf)* = ÖBA 2009/1564, 595 *(Bydlinski)*
- OGH 26.11.2009, 12 Os 79/09y
- OGH 28.09.2010, 14 Os 126/10a
- OGH 13.04.2011, 15 Os 172/10y (15 Os 173/10w) = jusIT 2011/44, 93 *(Karel)* = MR 2011, 153 *(Hasberger)* = JBl 2011, 726 *(Reindl-Krauskopf)*
- OGH 14.07.2011, 13 Os 61/11m = jusIT 2011/103, 220 *(Bergauer)* = JSt 2011, 201 *(Schwaighofer)*
- OGH 04.10.2011, 14 Os 107/11h
- OGH 18.10.2011, 12 Os 137/11f
- OGH 12.12.2011, 11 Os 152/11d
- OGH 25.01.2012, 15 Os 165/11w
- OGH 18.06.2012, 17 Os 1/12v = jusIT 2012/64, 138 *(Bergauer)* = JBl 2013, 193 *(Hinterhofer)*
- OGH 22.06.2012, 6 Ob 119/11k = jusIT 2012/61,134 *(Mader)* = ecolex 2012, 904 *(Anderl)* = ÖJZ EvBl-LS 2012/157, 974 *(Rohrer)* = ZIR 2013, 56 *(Briem)*
- OGH 05.07.2012, 13 Os 36/12m
- OGH 17.10.2012, 15 Os 114/12x
- OGH 10.10.2012, 12 Os 106/12y = JBl 2013, 536 *(Salimi)*
- OGH 16.11.2012, 6 Ob 126/12s = jusIT 2013/26, 52 *(Staudegger)* = ÖJZ EvBl-LS 2013/37, 239 *(Rohrer)*
- OGH 07.03.2013, 12 Os 5/13x
- OGH 30.08.2012, 13 Os 80/12g = ÖJZ EvBl 2013/7, 42 *(Ratz)* = JAP 2014/2015/1, 4 *(Prunner)*
- OGH 23.01.2014, 12 Os 90/13x = JSt 2014, 26 *(Birklbauer/Oberlaber)* = ÖJZ 2014/59, 382 *(Anzenberger/Sprajc)* = ÖJZ 2014/144, 956 *(Swiderski)* = RZ 2014, 238 *(Riffel)* = juridikum 2014, 166 *(Smutny)* = AnwBl 2014/8380, 261 *(Schrott)* = ÖJZ EvBl 2014/48, 317 *(Ratz)* = JBl 2014, 336 *(Schmoller)*
- OGH 25.09.2014, 12 Os 52/14k = jusIT *(Luef-Kölbl)*
- OGH 24.11.2014, 17 Os 40/14g (17 Os 41/14d) = jusIT 2015/30, 76 *(Bergauer)*
- RIS-Justiz RS0076658
- RIS-Justiz RS0077954
- RIS-Justiz RS0087720
- RIS-Justiz RS0087997
- RIS-Justiz RS0089333

- RIS-Justiz RS0089549
- RIS-Justiz RS0090516
- RIS-Justiz RS0090734
- RIS-Justiz RS0091000
- RIS-Justiz RS0093167
- RIS-Justiz RS0093560
- RIS-Justiz RS0093841
- RIS-Justiz RS0094297
- RIS-Justiz RS0094383
- RIS-Justiz RS0094395
- RIS-Justiz RS0095588
- RIS-Justiz RS0095639
- RIS-Justiz RS0095694
- RIS-Justiz RS0099100
- RIS-Justiz RS0102826
- RIS-Justiz RS0103999
- RIS-Justiz RS0108726
- RIS-Justiz RS0114037
- RIS-Justiz RS0115363
- RIS-Justiz RS0116322
- RIS-Justiz RS0118064
- RIS-Justiz RS0119780
- RIS-Justiz RS0120079
- RIS-Justiz RS0120525
- RIS-Justiz RS0120600
- RIS-Justiz RS0124174
- RIS-Justiz RS0124649
- RIS-Justiz RS0125232
- RIS-Justiz RS0125838
- OLG Linz 08.06.1989, 8 Bs 129/89 = AnwBl 1990/3375 *(Fromherz)*
- OLG Wien 21.11.1989, 23 Bs 201/89
- OLG Linz 07.01.1997, 7 Bs 350/96
- OLG Wien 03.10.2002, 17 Bs 249/02
- OLG Wien 22.11.2002, 17 Bs 263/02
- OLG Linz 16.07.2009, 3 R 101/09g
- OLG Wien 14.11.2013, 23 Bs 351/13f = MR 2014, 246 *(Bauer)* = jusIT 2015/3, 9 *(Bergauer)*

- OLG Innsbruck 16.12.2014, 11 Bs 353/14w
- LG Klagenfurt 10.01.2008, 7 Bl 121/07y = jusIT 2008/44, 95 *(Bergauer)*
- LG Salzburg 29.04.2011, 49 Bl 17/11v = jusIT 2011/89, 185 *(Thiele)*
- VfSlg 11.558/1987
- VfSlg 12.194/1989
- VfSlg 12.228/1989
- VfGH 12.10.1989, G 238/88
- VfSlg 12.880/1991
- VfSlg 15.273/1998
- VfSlg 16.369/2001
- VfSlg 17.065/2003
- VfGH 30.11.2005, B 1158/03
- VfSlg 17.940/2006
- VfGH 29.06.2012, B 1031/11
- VfGH 11.10.2012, B 1369/11 = jusIT 2012/104, 225 *(Jahnel)*
- VfGH 27.06.2014, G 47/2012 ua
- VwGH 25.02.1992, 88/07/0107
- VwGH 31.03.1992, 90/13/0131
- VwGH 25.02.1993, 92/04/0231
- VwGH 21.10.2004, 2004/06/0086
- VwGH 24.11.2006, 2006/02/0235
- VwGH 27.05.2009, 2007/05/0280
- VwGH 24.03.2010, 2007/03/0177
- VwGH 12.10.2010, 2008/05/0048
- VwGH 28.05.2013, 2011/17/0066 (2011/17/0067)
- DSK 10.11.2000, 120.707/7-DSK/00
- DSK 14.09.2001, K120.705/010-DSK/2001
- DSK 05.04.2002, K120.766/004-DSK/2002
- DSK 16.11.2004, K120.951/0009-DSK/2004
- DSK 20.05.2005, K120.986/0013-DSK/2005
- DSK 21.06.2005, K507.515–021/0004-DVR/2005
- DSK 26.10.2006, K121.218/0017-DSK/2006
- DSK 03.10.2007, K121.279/0017-DSK/2007
- DSK 16.11.2007, K121.311/0011-DSK/2007
- DSK 21.01.2009, K121.425/0003-DSK/2009
- DSK 18.11.2009, K121.501/0016-DSK/2009
- DSK 12.05.2010, K202.094/0004-DSK/2010

- DSK 13.07.2012, K212.766/0010-DSK/2012
- EuGH 07.12.1993, C-109/92 (Wirth/Landeshauptstadt Hannover)
- EuGH 06.11.2003, C-101/01 (Lindqvist) = MR 2004, 83 *(Kronegger)* = ÖJZ 2004/45, 741 *(Hörlsberger)*
- EuGH 16.12.2008, C-73/07 (Tietosuojavaltuutettu/Satakunnan Markkinapörssi Oy und Satamedia Oy) = MR-Int 2009, 14 *(Wittmann)*
- EuGH 22.12.2010, C-393/09 (Bezpečnostní softwarová asociace – Svaz softwarové ochrany/Ministerstvo kultury) = MR-Int 2011, 11 *(Savelka)* = MR 2011, 36 *(Marko/Hofmarcher)* = jusIT 2011/20, 44 *(Staudegger/Thiele)* = ÖBl-LS 2011/84, 164 *(Bücherle)*
- EuGH 04.10.2011, C-403/08, C-429/08 (Football Association Premier League Ltd ua bzw Murphy) = jusIT 2012/20, 49 *(Staudegger)*
- EuGH 02.05.2012, C-406/10 (SAS Institute Inc/World Programming Ltd) = ecolex 2012/257, 627 *(Anderl)* = jusIT 2012/45, 97 *(Staudegger)* = MR-Int 2012, 61 *(Appl)*
- EuGH 16.10.2012, C-614/10 (Kommission/Österreich) = = jusIT 2012/100, 211 *(Pachinger)* = AnwBl 2013, 71 *(Winkler)* = ZfRV 2014/7, 52 *(Bresich/Riedl/Souhrada-Kirchmayer)* = ÖZW 2013, 21 *(Pabel)*
- EuGH 08.04.2014, C-293/12, C-594/12 (Digital Rights Ireland Ltd bzw Kärntner Landesregierung ua/Bundesregierung ua) = ÖJZ 2014/54, 337 *(Lehofer)* = ecolex 2014, 397 *(Wilhelm)* = ecolex 2014, 576 *(Zankl)* = jusIT 2014/49, 96 *(Klaushofer)* = AnwBl 2014, 371 *(Schrott)* = NLMR 2014, 95 *(Heißl)* = ÖJZ 2014/74, 474 *(Lehofer)* = MR-Int 2014, 17 *(Otto)*
- BVerfG 15.12.1983, 1 BvR 209/83 ua
- BVerfG 27.02.2008, 1 BvR 370/07
- BVerfG 18.05.2009, 2 BvR 2233/07 (2 BvR 1151/08, 2 BvR 1624/08)
- BGH 12.05.2010, I ZR 121/08 = jusIT 2010/63, 138 *(Staudegger)*

C. Normenverzeichnis

1. Gesetze (alphabetisch)

- Budgetbegleitgesetz 2005, BGBl I 136/2004
- Bundesgesetz betreffend das Fernmeldewesen (Fernmeldegesetz 1993), BGBl 908/1993 aufgehoben durch BGBl I 100/1997
- Bundesgesetz über das Bankwesen (Bankwesengesetz), BGBl 532/1993 idF I 69/2015 [BWG]
- Bundesgesetz über das Urheberrecht an Werken der Literatur und der Kunst und über verwandte Schutzrechte (Urheberrechtsgesetz), BGBl 111/1936 idF I 99/2015 [UrhG]
- Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000), BGBl I 165/1999 idF I 83/2013 [DSG 2000]

- Bundesgesetz über den Schutz zugangskontrollierter Dienste (Zugangskontrollgesetz), BGBl I 60/2000 idF I 32/2001 [ZuKG]
- Bundesgesetz über die Ausgabe von E-Geld und die Aufnahme, Ausübung und Beaufsichtigung der Tätigkeit von E-Geld-Instituten (E-Geldgesetz 2010), BGBl I 107/2010 idF I 68/2015
- Bundesgesetz über die Beaufsichtigung von Wertpapierdienstleistungen (Wertpapieraufsichtsgesetz 2007), BGBl I 60/2007 idF I 69/2015 [WAG 2007]
- Bundesgesetz über die Erbringung von Zahlungsdiensten (Zahlungsdienstegesetz), BGBl I 66/2009 idF I 68/2015 [ZaDiG]
- Bundesgesetz über die Errichtung einer Buchhaltungsagentur des Bundes (Buchhaltungsagenturgesetz), BGBl I 37/2004 idF I 183/2013 [BHAG-G]
- Bundesgesetz über die Umsetzung völkerrechtlicher Verpflichtungen zur sicheren Verwendung von Informationen (Informationssicherheitsgesetz), BGBl I 23/2002 idF I 10/2006 [InfoSiG]
- Bundesgesetz über die Waffenpolizei (Waffengesetz 1996), BGBl I 12/1997 idF I 52/2015 [WaffG]
- Bundesgesetz vom 12. Juni 1981 über die Presse und andere publizistische Medien (Mediengesetz), BGBl 314/1981 idF I 101/2014 [MedienG]
- Bundesgesetz vom 13. Juli 1949, betreffend das Fernmeldewesen (Fernmeldegesetz 1949), BGBl 170/1949 aufgehoben durch BGBl 908/1993 [FG 1949]
- Bundesgesetz vom 18. Oktober 1978 über den Schutz personenbezogener Daten (Datenschutzgesetz 1978), BGBl 565/1978 aufgehoben durch BGBl I 165/1999 [DSG 1978]
- Bundesgesetz vom 23. Jänner 1974 über die mit gerichtlicher Strafe bedrohten Handlungen (Strafgesetzbuch), BGBl 60/1974 idF I 106/2014 [StGB]
- Bundesgesetz vom 25. November 1987, mit dem das Strafgesetzbuch, die Strafprozeßordnung, das Strafvollzugsgesetz, das Strafvollzugsanpassungsgesetz, das Einführungsgesetz zum Strafvollzugsgesetz, das Bewährungshilfegesetz, die Bewährungshilfegesetznovelle 1980, das Tilgungsgesetz 1972, das Strafregistergesetz 1968, das Gesetz zum Schutze der persönlichen Freiheit, das Militärstrafgesetz, das Geschwornen- und Schöffenlistengesetz, das Datenschutzgesetz, das Ausfuhrverbotsgesetz, das Devisengesetz, das Nationalbankgesetz 1984, das Außenhandelsgesetz 1984 und das Allgemeine Sozialversicherungsgesetz geändert werden (Strafrechtsänderungsgesetz 1987), BGBl 605/1987 [StRÄG 1987]
- Bundesgesetz vom 26. Juni 1958, betreffend das Finanzstrafrecht und das Finanzstrafverfahrensrecht (Finanzstrafgesetz), BGBl 129/1958 idF I 105/2014 [FinStrG]
- Bundesgesetz vom 27. Juni 1986, mit dem das Datenschutzgesetz und das Einführungsgesetz zu den Verwaltungsverfahrensgesetzen geändert werden (Datenschutzgesetznovelle 1986), BGBl 370/1986 [DSG-Nov 1986]
- Bundesgesetz vom 3. Juli 1968 über die Evidenthaltung strafgerichtlicher Verurteilungen (Strafregistergesetz 1968), BGBl 277/1968 idF I 107/2014

- Bundesgesetz vom 31. März 1950 über die Bekämpfung unzüchtiger Veröffentlichungen und den Schutz der Jugend gegen sittliche Gefährdung (Pornographiegesetz), BGBl 97/1950 idF I 50/2012 [PornG]
- Bundesgesetz zur Durchführung eines Informationsverfahrens auf dem Gebiet der technischen Vorschriften, der Vorschriften für die Dienste der Informationsgesellschaft und der Normen (Notifikationsgesetz 1999), BGBl I 183/1999 [NotifG 1999]
- Bundesgesetz, mit dem bestimmte rechtliche Aspekte des elektronischen Geschäfts- und Rechtsverkehrs geregelt werden (E-Commerce-Gesetz), BGBl I 152/2001 idF I 34/2015 [ECG]
- Bundesgesetz, mit dem das Bundes-Verfassungsgesetz, das Finanz-Verfassungsgesetz 1948, das Finanzstrafgesetz, das Bundesgesetz, mit dem das Invalideneinstellungsgesetz 1969 geändert wird, das Bundessozialamtsgesetz, das Umweltverträglichkeitsprüfungsgesetz 2000, das Bundesgesetzblattgesetz, das Verwaltungsgerichtshofgesetz 1985 und das Verfassungsgerichtshofgesetz 1953 geändert und einige Bundesverfassungsgesetze und in einfachen Bundesgesetzen enthaltene Verfassungsbestimmungen aufgehoben werden (Verwaltungsgerichtsbarkeits-Novelle 2012), BGBl I 51/2012
- Bundesgesetz, mit dem das Datenschutzgesetz 2000 geändert wird (DSG-Novelle 2013), BGBl I 57/2013
- Bundesgesetz, mit dem das Datenschutzgesetz 2000 geändert wird (DSG-Novelle 2014), BGBl I 83/2013 [DSG-Nov 2014]
- Bundesgesetz, mit dem das Datenschutzgesetz 2000 und das Sicherheitspolizeigesetz geändert werden (DSG-Novelle 2010), BGBl I 133/2009 [DSG-Nov 2010]
- Bundesgesetz, mit dem das Strafgesetzbuch geändert wird (Strafgesetznovelle 2011), BGBl I 130/2012 [StGB-Nov 2011]
- Bundesgesetz, mit dem das Strafgesetzbuch geändert wird (Strafgesetz-Novelle 1994), BGBl 622/1994 [StGB-Nov 1994]
- Bundesgesetz, mit dem das Strafgesetzbuch, die Strafprozessordnung 1975, das Strafvollzugsgesetz, das Suchtmittelgesetz, das Gerichtsorganisationsgesetz, das Waffengesetz 1996, das Fremdengesetz 1997 und das Telekommunikationsgesetz geändert werden (Strafrechtsänderungsgesetz 2002), BGBl I 134/2002 [StRÄG 2002]
- Bundesgesetz, mit dem das Strafgesetzbuch, die Strafprozessordnung 1975, das Gerichtsorganisationsgesetz, das Auslieferungs- und Rechtshilfegesetz und das Strafvollzugsgesetz geändert werden (Strafrechtsänderungsgesetz 2004), BGBl I 15/2004 [StRÄG 2004]
- Bundesgesetz, mit dem das Strafgesetzbuch, die Strafprozessordnung 1975, die Exekutionsordnung und das Sicherheitspolizeigesetz zur Verbesserung des strafrechtlichen Schutzes der Umwelt sowie gegen beharrliche Verfolgung und des zivilrechtlichen Schutzes vor Eingriffen in die Privatsphäre geändert werden (Strafrechtsänderungsgesetz 2006), BGBl I 56/2006 [StRÄG 2006]

- Bundesgesetz, mit dem das Strafgesetzbuch, die Strafprozessordnung 1975, das Strafvollzugsgesetz, das Bewährungshilfegesetz und das Jugendgerichtsgesetz 1988 geändert werden (Strafrechtsänderungsgesetz 2008), BGBl I 109/2007 [StRÄG 2008]
- Bundesgesetz, mit dem das Urheberrechtsgesetz geändert wird (Urheberrechtsgesetz-Novelle 1993), BGBl 93/1993 [UrhG-Nov 1993]
- Bundesgesetz, mit dem das Urheberrechtsgesetz geändert wird (Urheberrechtsgesetz-Novelle 2003), BGBl I 32/2003 [UrhG-Nov 2003]
- Bundesgesetz, mit dem die Exekutionsordnung, die Zivilprozessordnung, das Außerstreitgesetz, das Gerichtliche Einbringungsgesetz 1962, das Strafgesetzbuch, die Strafprozessordnung 1975, das Strafvollzugsgesetz, das Tilgungsgesetz 1972, das Staatsanwaltschaftsgesetz, das Verbrechensopfergesetz, das Strafregistergesetz, das Sicherheitspolizeigesetz und das Allgemeine Bürgerliche Gesetzbuch geändert werden (Zweites Gewaltschutzgesetz), BGBl I 40/2009 [2. GeSchG]
- Bundesgesetz, mit dem das Strafgesetzbuch und die Strafprozessordnung 1975 zur Verbesserung des strafrechtlichen Schutzes der sexuellen Integrität und Selbstbestimmung geändert werden (Sexualstrafrechtsänderungsgesetz 2013), BGBl I 116/2013
- Bundesgesetz, mit dem die Strafprozessordnung 1975 neu gestaltet wird (Strafprozessreformgesetz), BGBl I 19/2004
- Bundesgesetz, mit dem die Strafprozessordnung 1975, das Strafgesetzbuch, das Jugendgerichtsgesetz 1988 und das Finanzstrafgesetz geändert werden, BGBl I 93/2007
- Bundesgesetz, mit dem ein Telekommunikationsgesetz erlassen wird (Telekommunikationsgesetz 2003), BGBl I 70/2003 idF I 44/2014 [TKG 2003]
- Bundesgesetz, mit dem ein Telekommunikationsgesetz erlassen wird, das Telegraphenwegegesetz, das Fernmeldegebührengesetz und das Kabel- und Satelliten-Rundfunkgesetz geändert werden sowie ergänzende
- Bestimmungen zum Rundfunkgesetz und zur Rundfunkverordnung getroffen werden (Telekommunikationsgesetz 1997), BGBl I 100/1997 aufgehoben durch BGBl I 70/2003 [TKG 1997]
- Strafprozessordnung 1975, BGBl 631/1975 (WV) idF I 85/2015

2. Gesetzesmaterialien (chronologisch aufsteigend)

- Erläuterungen zum Strafgesetzbuch: ErlRV 30 BlgNR XIII. GP
- Bericht des Justizausschusses zum Strafgesetzbuch: JAB 959 BlgNR XIII. GP
- Bericht des Justizausschusses zur Änderung des Staatsgrundgesetzes: JAB 960 BlgNR XIII. GP
- Erläuterungen zum Datenschutzgesetz: ErlRV 72 BlgNR XIV. GP
- Bericht des Verfassungsausschusses zum Datenschutzgesetz: AB 1024 BlgNR XIV. GP

- Bericht des Justizausschusses zum Mediengesetz: JAB 743 BlgNR XV. GP
- Erläuterungen zu Datenschutzgesetznovelle 1986: ErlRV 554 BlgNR XVI. GP
- Initiativantrag betreffend ein Strafrechtsänderungsgesetz 1987: IA 2/A XVII. GP
- Bericht des Justizausschusses zum Strafrechtsänderungsgesetz 1987: JAB 359 BlgNR XVII. GP
- Erläuterungen zum Strafprozessänderungsgesetz 1993: ErlRV 924 BlgNR XVIII. GP
- Bericht des Justizausschuss zur Änderung des Strafgesetzbuchs: JAB 1848 BlgNR XVIII. GP
- Erläuterungen zum Datenschutzgesetz 2000: ErlRV 1613 BlgNR XX. GP
- Erläuterungen zum Notifikationsgesetz 1999: ErlRV 1898 BlgNR XX. GP
- Erläuterungen zum Fernabsatz-Gesetz: ErlRV 1998 BlgNR XX. GP
- Erläuterungen zum Zugangskontrollgesetz: ErlRV 99 BlgNR XXI. GP
- Ministerialentwurf eines Strafrechtsänderungsgesetzes 2002: 308/ME XXI. GP
- Erläuterungen zum E-Commerce-Gesetz: ErlRV 817 BlgNR XXI. GP
- Erläuterungen zum StRÄG 2002: ErlRV 1166 BlgNR XXI. GP
- Erläuterungen zum Strafprozessreformgesetz: ErlRV 25 BlgNR XXII. GP
- Erläuterungen zur Urheberrechtsgesetz-Novelle 2003: ErlRV 40 BlgNR XXII. GP
- Ministerialentwurf einer Änderung des Strafgesetzbuchs: 78/ME XXII. GP
- Erläuterungen eines Ministerialentwurfs zur Änderung des Strafgesetzbuchs: ErlME 78/ME XXII. GP
- Erläuterungen zum Zivilrechts-Änderungsgesetz 2004: ErlRV 173 BlgNR XXII. GP
- Erläuterungen des Strafrechtsänderungsgesetzes 2004: ErlRV 294 BlgNR XXII. GP.
- Regierungsvorlage der Änderung des Strafgesetzbuchs: RV 309 BlgNR XXII. GP
- Erläuterungen des Strafrechtsänderungsgesetzes 2004/2: ErlRV 309 BlgNR XXII. GP
- Erläuterungen zu einem Ministerialentwurf eines Strafrechtsänderungsgesetzes 2006: ErlME 349/ME XXII. GP
- Bericht des Justizausschusses zum Strafprozessreformgesetz: JAB 406 BlgNR XXII. GP
- Erläuterungen zum Budgetbegleitgesetz 2005: ErlRV 649 BlgNR XXII. GP
- Erläuterungen zur Änderung des Mediengesetzes: ErlRV 784 BlgNR XXII. GP
- Erläuterungen zum Strafrechtsänderungsgesetzes 2006: ErlRV 1316 BlgNR XXII. GP

- Erläuterungen zum Strafrechtsänderungsgesetzes 2006/2: ErlRV 1325 BlgNR XXII. GP
- Ministerialentwurf eines Strafrechtsänderungsgesetzes 2008: 92/ME XXIII. GP
- Ministerialentwurf einer Datenschutzgesetznovelle 2008: 182/ME XXIII. GP
- Erläuterungen zum Strafrechtsänderungsgesetzes 2008: ErlRV 285 BlgNR XXIII. GP
- Erläuterungen zum zweiten Gewaltschutzgesetz: ErlRV 678 BlgNR XXIII. GP
- Ministerialentwurf einer Änderung des Strafgesetzbuches: 82/ME XXIV. GP
- Erläuterungen zur Änderungen des Strafgesetzbuches: ErläutME 82/ME XXIV. GP
- Erläuterungen zum Übereinkommen des Europarats zur Verhütung des Terrorismus: ErläutStV 95 BlgNR XXIV. GP
- Bericht des Justizausschusses zum zweiten Gewaltschutzgesetz: JAB 106 BlgNR XXIV. GP
- Erläuterungen zur Datenschutzgesetznovelle 2010: ErlRV 472 BlgNR XXIV. GP
- Erläuterungen zur Änderung eines Terrorpräventionsgesetzes 2010: ErlRV 674 BlgNR XXIV. GP
- Erläuterungen zum Übereinkommen des Europarats zum Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch: ErläutStV 881 BlgNR XXIV. GP
- Erläuterungen zur Änderung des Telekommunikationsgesetzes 2003: ErlRV 1074 BlgNR XXIV. GP
- Bericht des Justizausschusses zur Änderung eines Terrorpräventionsgesetzes 2010: JAB 1422 BlgNR XXIV. GP
- Erläuterungen zur Strafgesetznovelle 2011: ErlRV 1505 BlgNR XXIV. GP
- Erläuterungen zum Übereinkommen über Computerkriminalität: ErläutStV 1645 BlgNR XXIV. GP
- Erläuterungen zur Datenschutzgesetznovelle 2014: ErlRV 2168 BlgNR XXIV. GP
- Erläuterungen zum Sexualstrafrechtsänderungsgesetz 2013: ErlRV 2319 BlgNR XXIV. GP
- Erläuterungen zur SPG-Novelle 2014: ErlRV 99 BlgNR XXV. GP
- Erläuterungen zum Strafrechtsänderungsgesetz 2015: ErlRV 689 BlgNR XXV. GP
- Bericht des Justizausschusses zum Strafrechtsänderungsgesetzes 2015: JAB 728 BlgNR XXV. GP

3. Europarecht (chronologisch aufsteigend)

- Richtlinie 91/250/EWG des Rates vom 14. Mai 1991 über den Rechtsschutz von Computerprogrammen, ABl L 1991/122, 42 in der kodifizierten Fassung RL 2009/24/EG des Europäischen Parlaments und des Rates vom 23. April 2009 über den Rechtsschutz von Computerprogrammen (kodifizierte Fassung), ABl L 2009/111, 16 [Computerprogramm-RL]
- Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl L 1995/281, 31 [Datenschutz-RL]
- Richtlinie 96/9/EG des Europäischen Parlaments und des Rates vom 11. März 1996 über den rechtlichen Schutz von Datenbanken, ABl L 1996/77, 20 [Datenbanken-RL]
- Richtlinie 98/84/EG des Europäischen Parlaments und des Rates vom 20. November 1998 über den rechtlichen Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten, ABl L 1998/320, 54 [Zugangskontroll-RL]
- Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt (»Richtlinie über den elektronischen Geschäftsverkehr«), ABl L 2000/178, 1
- Richtlinie 2001/29/EG zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft, ABl L 2001/167, 10 idF L 2002/6, 71 [Info-RL]
- Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl L 2002/201, 37 [Kommunikations-RL]
- Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, ABl L 2006/105, 54 [Vorratsdatenspeicherungs-RL]
- Charta der Grundrechte der Europäischen Union, ABl C 2007/303, 1 idF C 2012/326, 391 [GRC]
- Richtlinie 2008/114/EG des Rates vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern, ABl L 2008/345, 75
- Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universal-

dienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz, ABl L 2009/337, 11

- Richtlinie 2011/93/EU des Europäischen Parlaments und des Rates vom 13. Dezember 2011 zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie sowie zur Ersetzung des Rahmenbeschlusses 2004/68/JI des Rates, ABl L 2011/335, 1 idF L 2012/18
- Richtlinie 2011/36/EU des Europäischen Parlaments und des Rates vom 5. April 2011 zur Verhütung und Bekämpfung des Menschenhandels und zum Schutz seiner Opfer sowie zur Ersetzung des Rahmenbeschlusses 2002/629/JI des Rates, ABl L 2011/101, 1
- Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates vom 12. August 2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates, ABl L 2013/218, 8

4. Vorarbeiten, Stellungnahmen und Mitteilungen von Organen der EU

- Aktionsplan des Rates und der Kommission zur Umsetzung des Haager Programms zur Stärkung von Freiheit, Sicherheit und Recht in der Europäischen Union, ABl C 2005/198, 1
- Bericht der Kommission an den Rat auf der Grundlage von Artikel 12 des Rahmenbeschlusses des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme, KOM (2008) 448 endg
- Das Stockholmer Programm – Ein offenes und sicheres Europa im Dienste und zum Schutz der Bürger, ABl C 2010/115, 1
- Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – Ein Raum der Freiheit, der Sicherheit und des Rechts für die Bürger Europas – Aktionsplan zur Umsetzung des Stockholmer Programms, KOM (2010) 171 endg
- Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen Eine Digitale Agenda für Europa, KOM (2010) 245 endg/2
- Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses zu der »Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen über den Schutz kritischer Informationsinfrastrukturen — ‚Schutz Europas vor Cyber-Angriffen und Störungen großen Ausmaßes: Stärkung der Abwehrbereitschaft, Sicherheit und Stabilität' », KOM (2009) 149 endg, ABl C 2010/255, 130

- Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Angriffe auf Informationssysteme und zur Aufhebung des Rahmenbeschlusses 2005/222/JI des Rates, KOM (2010) 517 endg
- Mitteilung der Kommission an das Europäische Parlament und den Rat EU-Strategie der inneren Sicherheit: Fünf Handlungsschwerpunkte für mehr Sicherheit in Europa, KOM (2010) 673 endg
- Mitteilung der Kommission an den Rat und das Europäische Parlament Kriminalitätsbekämpfung im digitalen Zeitalter: Errichtung eines Europäischen Zentrums zur Bekämpfung der Cyberkriminalität, KOM (2012) 140 endg

5. EU-Rahmenbeschlüsse

- Rahmenbeschluss 2001/413/JI des Rates vom 28. Mai 2001 zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln, ABl L 2001/149, 1 [EU-RB 2001/413/JI]
- Rahmenbeschluss 2002/475/JI des Rates vom 13. Juni 2002 zur Terrorismusbekämpfung, ABl L 2002/164, 4 [EU-RB 2002/475/JI]
- Rahmenbeschluss 2004/68/JI des Rates vom 22. Dezember 2003 zur Bekämpfung der sexuellen Ausbeutung von Kindern und der Kinderpornografie, ABl L 2004/13, 44 [EU-RB 2004/68/JI]
- Rahmenbeschluss 2005/222/JI des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme, ABl L 2005/69, 67 [EU-RB 2005/222/JI]
- Rahmenbeschluss 2008/919/JI des Rates vom 28. November 2008 zur Änderung des Rahmenbeschlusses 2002/475/JI zur Terrorismusbekämpfung, ABl L 2008/330, 21 [EU-RB 2008/919/JI]

6. Konventionen und Erläuterungen des Europarats (chronologisch aufsteigend)

- European Convention on the Legal Protection of Services based on, or consisting of, Conditional Access (ETS 178), <conventions.coe.int/Treaty/en/Treaties/Html/178.htm> (01.04.2014)
- Convention on Cybercrime (ETS 185), <conventions.coe.int/Treaty/en/Treaties/Html/185.htm> (01.04.2014), BGBl III 140/2012 idF III 215/2014
- Convention on Cybercrime – Explanatory Report, <conventions.coe.int/Treaty/EN/Reports/Html/185.htm> (01.04.2014) [ER (ETS 185)]
- Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS 189), <conventions.coe.int/Treaty/en/Treaties/Html/189.htm> (01.04.2014)

- Convention on the Prevention of Terrorism (ETS 196), <conventions.coe.int/Treaty/en/Treaties/Html/196.htm> (01.04.2014), BGBl III 34/2010
- Convention on the Prevention of Terrorism – Explanatory Report, <conventions.coe.int/Treaty/EN/Reports/Html/196.htm> (01.04.2014) [ER (ETS 196)]
- Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201) <conventions.coe.int/Treaty/en/Treaties/Html/201.htm> (01.04.2014), BGBl III 96/2011
- Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse – Explanatory Report, <conventions.coe.int/Treaty/EN/Reports/Html/201.htm> (01.04.2014) [ER (CETS 201)]

7. Protokoll der Vereinten Nationen (UN)

- VN-Fakultativprotokoll zum Übereinkommen über die Rechte des Kindes betreffend den Verkauf von Kindern, die Kinderprostitution und die Kinderpornografie, BGBl III 93/2004

D. Web-Verzeichnis

- *BMJ,* <www.edikte.justiz.gv.at/> (01.04.2014)
- *Chip Online,* Creeper: Der erste Computer-Wurm wird 40, <www.chip.de/news/Creeper-Der-erste-Computer-Wurm-wird-40_51912666.html> (01.04.2014)
- *e-card,* <www.chipkarte.at/portal27/portal/ecardportal/channel_content/cmsWindow?action=2&p_menuid=51909&p_tabid=4> (01.04.2014)
- *Europol,* <www.europol.europa.eu/ec3> (01.04.2014)
- *Gülmen,* TEMPEST-Zertifizierung – der Weg zum abhörsicheren Gerät, <blog.gdsys.de/blog/2012/09/13/tempest-zertifizierung-der-weg-zum-abhorsicheren-gerat/> (01.04.2014)
- *Heise online,* Entwickler des Wurms Sasser steht vor Gericht, <www.heise.de/newsticker/meldung/61392> (01.04.2014)
- *Heuse,* PIN-Skimming bei Chipkarten möglich, <heise.de/-1209205> (01.04.2014)
- *Internet World Stats,* World internet usage and population statistics, <www.internetworldstats.com/stats.htm> (01.04.2014)
- *Janssen/Kuri/Schmidt,* Operation Payback: Proteste per Mausklick, <heise.de/-1150151> (01.04.2014).
- *Microsoft,* Land Attack, <support.microsoft.com/kb/165005/DE/> (01.04.2014)
- *NSA,* TEMPEST: a signal problem – The story of the discovery of various compromising radiations from communications and Comsec equipment,

<www.nsa.gov/public_info/_files/cryptologic_spectrum/tempest.pdf> (01.04.2014)

- *Van Eck,* »Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?«, Computer & Security 4, (1985), 269, <cryptome.org/jya/emr.pdf> (10.07.2013).
- Online-Festplatte von A1,<www.a1.net/hilfe-support/online-festplatte> (01.04.2014)
- *Paget,* Hacktivismus, <www.mcafee.com/de/resources/white-papers/wp-hacktivism.pdf> (01.04.2014)
- *Payment Service Austria,* <www.psa.at/karteninhaber/sicherheitstipps/geo-control/> (03.03.2015)
- *PC-Welt,* Internet-Kühlschrank im Test,<www.pcwelt.de/news/Internet-Kuehlschrank-im-Test-158989.html> (01.04.2014)
- *Pressetext-Austria,* Internet-Kühlschrank als Informationszentrum im Haushalt,<pressetext.at/news/010214032/internet-kuehlschrank-als-informationszentrum-im-haushalt> (01.04.2014)
- *Landgericht Verden,* Urteil im Sasser-Prozess,<www.landgericht-verden.niedersachsen.de/portal/live.php?navigation_id=13888&article_id=58136&_psmand=57> (01.04.2014)
- *Quick,* <www.quick.at/pay/overview.php> (01.04.2014)
- *Schmidt,* Dämme gegen die SYN-Flut, <heise.de/-270378> (01.04.2014)
- *Securelist,* <www.securelist.com/en/descriptions/56696/Virus.Boot.Joshi.a> (01.04.2014)
- *Statistik Austria,* <www.statistik.at> (01.04.2014)
- *Statistik Austria,* IKT-Einsatz in Haushalten 2012, <www.statistik.at/dynamic/wcmsprod/idcplg?IdcService=GET_NATIVE_FILE&dID=133091&dDocName=069000> (01.04.2014)
- *Statistik Austria,* IKT-Einsatz in Haushalten 2013, <www.statistik.at/web_de/statistiken/informationsgesellschaft/ikt-einsatz_in_haushalten/> (01.04.2014)
- *Statistik Austria,* IKT-Einsatz in Unternehmen 2012, <www.statistik.at/dynamic/wcmsprod/idcplg?IdcService=GET_NATIVE_FILE&dID=135731&dDocName=069554> (01.04.2014)
- *Stern.de,* <www.stern.de/digital/online/gefaehrliches-bot-netzwerk-tdl-4-es-ist-praktisch-unzerstoerbar-1701583.html> (01.04.2014)
- *Wikipedia,* <de.wikipedia.org/wiki/Brute-Force-Methode> (01.04.2014)
- *Wikipedia,* <de.wikipedia.org/wiki/Low_Orbit_Ion_Cannon> (01.04.2014)

Hinweise des Verlags

Dieses Dokument ist die vollständige, unveränderte Fassung von Christian Bergauer »Das materielle Computerstrafrecht«. Es ist kein e-book im technischen Sinn, sondern ein PDF. Denn auch wenn die für die Erstellung von e-books derzeit verfügbare Software für die Gestaltung von Romanen und damit idR glatten Satz völlig ausreicht, genügt sie nicht den Ansprüchen für die elektronische Veröffentlichung langer wissenschaftlicher Texte mit zahlreichen Überschriftsebenen und umfassendem Fußnotenapparat – zumindest nicht, wenn diese Tätigkeit auch nur annähernd adäquat entlohnt werden soll.

Wir haben uns daher entschieden, unser Drucklayout auch für die elektronische Ausgabe zu verwenden. Auch wenn es auf einem Smartphone mit einem 4.3-inch Display lesbar ist, komfortabel und ohne Ermüdungserscheinungen hat es sich für uns erst ab einer Display-Größe von 9.7-inch erwiesen.

Das PDF ist zoombar und enthält einige Elemente zur Navigation – die Kapitelüberschriften im Inhaltsverzeichnis führen zum jeweiligen Kapitel und ein Klick auf das Alinea-Zeichen in der Fußzeile jeder Seite führt an den Beginn des Inhaltsverzeichnisses.

Abhängig vom Lesegerät und der verwendeten Software können leichte Unterschiede in Aussehen und dem Gebrauch der Navigationselemente auftreten.

PCs mit Adobe Acrobat X/Reader X:
Alle Navigationselemente sind schwarz. Wird der Mauszeiger über ein solches Element bewegt, wird er zu einer kleinen Hand und ein Linksklick mit der Maus aktiviert das Navigationselement.

iPad mit Adobe Acrobat X/Reader X:
Alle Navigationselemente sind blau. Ein Linksklick mit der Maus aktiviert dieses Element.

iBook Reader on an iPad:
Alle Navigationselemente sind schwarz. Ein kurzer Klick auf ein Element in der Fußzeile blättert zurück bzw vor. Ein längeres Drücken führt zum Inhaltsverzeichnis. Elemente im Inhaltsverzeichnis werden mit einem kurzen Klick aktiviert.

Andere Lesegeräte können andere Abweichungen zeigen.

Jan Sramek Verlag

Sie können dieses Dokument im Rahmen der open-source Lizenz nutzen. (Details finden Sie hier).

Technisch können Sie mit diesem PDF Folgendes tun:

- Speichern und Weiterleitung an Dritte ohne ein Passwort zu verwenden;
- Das PDF drucken, wobei Sie bei Aufforderung das Passwort »none« eingeben müssen (die Anführungszeichen sind nicht Teil des Passworts). Dies scheint ein integraler Bestandteil der Software zu sein, denn wir haben zu unserem Bedauern bislang keinen Weg gefunden, dies zu umgehen;
- Kommentare einfügen und abspeichern; sowie
- Inhalte für die Weiterverwendung kopieren (die korrekte Quellenangabe ist erforderlich).

Technisch ist es mit diesem PDF nicht möglich Änderungen am Text vorzunehmen oder Textteile im PDF zu löschen.

Gerne können Sie uns unter kontakt@jan-sramek-verlag.at Feedback auch zu unserem zweiten Schritt in die Welt des elektronischen Publizierens geben. Wir können nicht versprechen, dass wir alle Nachrichten beantworten oder jede Anregung aufgreifen, aber wir lesen jede Nachricht und beziehen sie gerne in unsere weiteren Überlegungen ein.

Um zur Titelei zurückzukehren, klicken Sie bitte hier.