

Schriften zum Strafrecht

Band 378

Die Strafbarkeit des Card- und Account-Sharings

Zur strafrechtlichen Erfassung der
äußerlich regulären Nutzung von zugangsgesicherten
Inhalten durch hierzu nicht Befugte

Von

Felix Schmidhäuser



Duncker & Humblot · Berlin

FELIX SCHMIDHÄUSER

Die Strafbarkeit des Card- und Account-Sharings

Schriften zum Strafrecht

Band 378

Die Strafbarkeit des Card- und Account-Sharings

Zur strafrechtlichen Erfassung der
äußerlich regulären Nutzung von zugangsgesicherten
Inhalten durch hierzu nicht Befugte

Von

Felix Schmidhäuser



Duncker & Humblot · Berlin

Die Juristische Fakultät der Eberhard Karls Universität Tübingen
hat diese Arbeit im Jahre 2021 als Dissertation angenommen.

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in
der Deutschen Nationalbibliografie; detaillierte bibliografische Daten
sind im Internet über <http://dnb.d-nb.de> abrufbar.

D 21

Alle Rechte vorbehalten
© 2021 Duncker & Humblot GmbH, Berlin
Satz: 3w+p GmbH, Rimpf
Druck: CPI buchbücher.de gmbh, Birkach
Printed in Germany

ISSN 0558-9126
ISBN 978-3-428-18420-0 (Print)
ISBN 978-3-428-58420-8 (E-Book)

Gedruckt auf alterungsbeständigem (säurefreiem) Papier
entsprechend ISO 9706 ☼

Internet: <http://www.duncker-humblot.de>

Vorwort

Die Arbeit wurde von der Juristischen Fakultät der Eberhard Karls Universität Tübingen im Sommersemester 2021 als Dissertation angenommen. Die Disputation fand am 18.05.2021 ebendort statt. Literatur und Rechtsprechung konnten bis Anfang August 2021 berücksichtigt werden.

Mein besonderer Dank gilt zunächst meinem Doktorvater, Herrn Professor Dr. Bernd Hecker, an dessen Lehrstuhl ich während der Zeit meiner Promotion als Akademischer Mitarbeiter beschäftigt war. Sowohl in fachlicher als auch in persönlicher Hinsicht war seine Betreuung stets herausragend. Er gewährte großzügige Freiheiten zur wissenschaftlichen Entfaltung, stand dabei aber immer für Gespräche, Diskussionen und Rückfragen zur Verfügung und schenkte mir ein offenes Ohr, was insgesamt für das Gelingen des Promotionsvorhabens von essentieller Bedeutung war.

Ebenso herzlich danke ich Herrn Professor Dr. Bernd Heinrich für die zügige Erstellung des Zweitgutachtens sowie für seine Unterstützung bei der Erstellung der Arbeit, gerade durch Gespräche über urheberrechtliche Fragen, die für mich von außerordentlichem Wert waren.

Mein besonderer Dank gilt auch meinen Eltern, Claudia und Axel Schmidhäuser. Sie haben es mir durch ihre vorbehaltlose Unterstützung sowie ihren steten Rückhalt überhaupt erst ermöglicht, dort sein zu können, wo ich jetzt bin.

Mein größter Dank gilt schließlich meiner Frau Julia Schmidhäuser für deren unermüdliche Geduld, ihre Diskussionsbereitschaft, die Übernahme des Korrekturlesens sowie ihre immerwährende Unterstützung in vielfältiger Weise, ohne die die Anfertigung der vorliegenden Arbeit sicherlich nicht möglich gewesen wäre.

Tübingen, im August 2021

Felix Schmidhäuser

Inhaltsübersicht

Einleitung	27
A. Einführung	27
B. Ziel der Untersuchung	30
C. Gang der Untersuchung	30

Kapitel 1

Tatsächliche und technische Grundlagen 31

A. Beteiligte	31
B. Cardsharing	32
C. Account-Sharing	38
D. Aktualität der Phänomene, Gegenmaßnahmen und deren Bedeutung	40
E. Abgrenzung zu anderen Phänomenen	43

Kapitel 2

Zivilrechtliche Grundlagen 54

A. Das Verhältnis zwischen Anbieter und Sharer	54
B. Das Verhältnis zwischen Anbieter und Nutzer	82
C. Das Verhältnis zwischen Sharer und Nutzer	86
D. Zusammenfassung zu Kapitel 2	87

Kapitel 3

Strafbarkeit der am Sharing Beteiligten 88

§ 1

Straftaten gegen Vermögenswerte 89

A. Betrug – § 263 StGB	89
B. Computerbetrug – § 263a StGB	98

C. Vorbereitung eines Computerbetrugs – § 263a Abs. 3 StGB	152
D. Erschleichen von Leistungen – § 265a StGB	154
E. Untreue – § 266 StGB	183

§ 2

Straftaten gegen den Geheimnisbereich	184
A. Ausspähen von Daten – § 202a StGB	184
B. Vorbereiten des Ausspähens und Abfangens von Daten – § 202c StGB	213
C. Abfangen von Daten – § 202b StGB	225
D. Datenhehlerei – § 202d StGB	226
E. Verletzung von Geschäftsgeheimnissen – § 23 GeschGehG	227
F. Strafvorschrift des § 42 BDSG	247

§ 3

Straftaten wegen urheberrechtswidrigen Handelns	250
A. Unerlaubte Verwertung urheberrechtlich geschützter Werke – § 106 UrhG	250
B. Unerlaubte Eingriffe in verwandte Schutzrechte – § 108 UrhG	322
C. Unerlaubte Eingriffe in technische Schutzmaßnahmen und zur Rechtewahrnehmung erforderliche Informationen – § 108b UrhG	327
D. Strafvorschrift des § 33 KUG	337

§ 4

Weitere Straftaten, insbesondere aus dem Bereich der Cyberkriminalität	339
A. Strafvorschrift des § 4 ZKDSG	339
B. Fälschung beweiserheblicher Daten – § 269 StGB	346
C. Fälschung technischer Aufzeichnungen – § 268 StGB	357
D. Datenveränderung – § 303a StGB	358
E. Computersabotage – § 303b StGB	359
F. Störung von Telekommunikationsanlagen – § 317 StGB	359
G. Öffentliche Aufforderung zu Straftaten – § 111 StGB	360
H. Strafvorschrift des § 148 TKG	360

§ 5

Gesamtergebnis und Konkurrenzen zu Kapitel 3	361
A. Gesamtergebnis und Konkurrenzen hinsichtlich des Nutzers	361
B. Gesamtergebnis und Konkurrenzen hinsichtlich des Sharers	361

Kapitel 4

Bewertung der gefundenen Ergebnisse und Vorschlag zur Erfassung des Sharings de lege ferenda	364
A. Kriminalpolitisch unbefriedigende Rechtslage de lege lata	364
B. Erforderlichkeit eines das Sharing erfassenden Straftatbestandes de lege ferenda	365
C. Erweiterung des § 265a StGB als vorzugswürdige Lösung	384
Zusammenfassung der wesentlichen Ergebnisse	390
Literaturverzeichnis	393
Sachwortverzeichnis	410

Inhaltsverzeichnis

Einleitung	27
A. Einführung	27
B. Ziel der Untersuchung	30
C. Gang der Untersuchung	30

Kapitel 1

Tatsächliche und technische Grundlagen	31
A. Beteiligte	31
B. Cardsharing	32
I. Allgemeines	33
II. Regulärer Ablauf beim Empfang von Pay-TV	34
III. Technischer Ablauf beim Cardsharing	35
IV. Erscheinungsformen	37
C. Account-Sharing	38
D. Aktualität der Phänomene, Gegenmaßnahmen und deren Bedeutung	40
E. Abgrenzung zu anderen Phänomenen	43
I. Piratenkarten	43
1. Digital Pirate Smartcards	44
2. Modified Original Smartcards	45
3. Strafbarkeit des Einsatzes von Piratenkarten	46
4. Unterscheidung zum Cardsharing i. e. S.	47
II. P2P/Filesharing/Filehosting/Einstreamen	47
1. Live-Streaming	47
2. On-Demand-Streaming und Filesharing/Filehosting	47
3. Einstreamen	49
4. Unterschied zum Card- und Account-Sharing	49
III. Phishing	50
IV. Pharming	51

V. Skimming	52
VI. Carding	52
VII. Hacking	52

Kapitel 2

Zivilrechtliche Grundlagen 54

A. Das Verhältnis zwischen Anbieter und Sharer	54
I. Vertragsverhältnis	54
II. Rechte und Pflichten aus dem Abonnementvertrag	56
III. Folgen von Pflichtverletzungen	60
1. Entzug der „Sehberechtigung“	60
2. Vertragsstrafe	61
3. Schadensersatzpflicht aus Vertrag	62
a) Tatbestand	62
b) Anspruchsumfang	62
aa) Entgangener Gewinn als Schadensposten	63
bb) Sharergewinn	66
cc) Lizenzanalogie	67
c) Ergebnis	67
IV. Schadensersatz aus Delikt – § 823 Abs. 1 BGB	67
1. Recht am eingerichteten und ausgeübten Gewerbebetrieb	68
2. Urheberrecht	69
3. Daten	69
4. Ergebnis	71
V. Vorsätzlich sittenwidrige Schädigung – § 826 BGB	71
VI. Angemaßte Eigengeschäftsführung – §§ 687 Abs. 2 S. 1, 681 S. 2, 667 BGB	72
VII. Eingriffskondiktion – § 812 Abs. 1 S. 1 Var. 2 BGB	72
1. Keine Einschlägigkeit von § 816 BGB	73
2. Voraussetzungen des § 812 Abs. 1 S. 1 Var. 2 BGB	73
3. Rechtsfolge	75
4. Ergebnis	76
VIII. Sperrung der Sharingwebsite – § 7 Abs. 4 S. 1 TMG analog	76
IX. Ansprüche aus UWG	78
X. Weitere Ansprüche	81
1. Beseitigung und Unterlassung	81
2. Schadensersatz	81
XI. Zusammenfassung	82

B. Das Verhältnis zwischen Anbieter und Nutzer	82
I. Vertragliche Beziehung	82
II. Nichtvertragliche Ansprüche	84
1. Ansprüche auf Beseitigung und Unterlassung	84
2. Ansprüche auf Schadensersatz	85
3. Ansprüche auf Gewinnherausgabe und Lizenzanalogie	85
C. Das Verhältnis zwischen Sharer und Nutzer	86
D. Zusammenfassung zu Kapitel 2	87

Kapitel 3

Strafbarkeit der am Sharing Beteiligten 88

§ 1

Straftaten gegen Vermögenswerte 89

A. Betrug – § 263 StGB	89
I. Nutzer	89
II. Sharer	90
1. Ausdrückliche Täuschung	91
2. Konkludente Täuschung	91
a) Einordnung des Verbots des Sharens als Haupt- oder Nebenleistungspflicht	92
b) Einordnung des Verbots des Sharens als Geschäftsgrundlage	94
3. Täuschung durch Unterlassen	97
III. Ergebnis zu § 263 StGB	98
B. Computerbetrug – § 263a StGB	98
I. Daten	99
1. Allgemeines	99
2. Daten im Prozess des Cardsharings	99
a) Auf der Smartcard enthaltene Berechtigungsdaten	99
b) Das Kontrollwort bildende Daten	100
c) Die ECM bildende Daten	100
d) Vom Anbieter ausgestrahlte Sendeinhalte als Daten	101
3. Daten im Prozess des Account-Sharings	101
a) Benutzerkennung	101
b) Bereitgehaltene und abrufbare Sendeinhalte	102

II. Datenverarbeitungsvorgang	102
1. Cardsharing	103
2. Account-Sharing	104
III. Tathandlung	104
1. § 263a Abs. 1 Var. 1 StGB – Unrichtige Gestaltung eines Programms	105
a) Cardsharing	105
b) Account-Sharing	107
2. § 263a Abs. 1 Var. 2 StGB – Verwendung unrichtiger oder unvollständiger Daten	108
3. § 263a Abs. 1 Var. 3 StGB – Unbefugte Verwendung von Daten	109
a) Datenverwendung im Sinne von § 263a Abs. 1 Var. 3 StGB	109
b) Das Merkmal „unbefugt“ im Sinne von § 263a Abs. 1 StGB	111
c) Unbefugte Datenverwendung des Cardsharers	114
aa) Weiterleitung des Kontrollworts als unbefugte Verwendung von Daten	115
bb) Einstecken der Smartcard als unbefugte Datenverwendung	116
cc) Unbefugte Verwendung durch Einstecken und Entschlüsselungsprozess	118
d) Unbefugte Verwendung durch den Account-Sharer	119
e) Unbefugte Verwendung des Nutzers von Sharing-Diensten	120
aa) Problem der kommunikativen Beziehung zum Anbieter beim Cardsharing	121
bb) Unbefugte Datenverwendung durch den Account-Sharing-Nutzer	122
4. § 263a Abs. 1 Var. 4 – Sonst unbefugte Einwirkung auf den Ablauf	123
IV. Beeinflussung des Ergebnisses eines Datenverarbeitungsvorgangs durch unbefugte Verwendung von Daten	124
1. Anzunehmende Beeinflussung des Ergebnisses	124
2. Widerlegung der Argumentation u. a. Planerts	125
V. Vermögensrelevanz der Datenverarbeitungsvorgänge – unmittelbare Vermögensminderung	127
1. Taugliche Vermögensbestandteile	128
a) Anspruch auf Gegenleistung	128
b) Anspruch auf Schadensersatz	128
c) Leistung der Ausstrahlung der Programmdateien	129
d) Urheber- und Nutzungsrecht	130
e) Geschäftsgeheimnis	131
f) Umsatz- und Abonnentenrückgang	131
g) Vermögen der Kunden	132
2. Unmittelbare Vermögensminderung durch Aufspaltung der Sendesignale durch den Nutzer der Cardsharing-Dienste	132
3. Unmittelbare Vermögensminderung durch Entschlüsselung der Kontrollwörter durch den Cardsharer und anschließende Weiterleitung an den Nutzer	133

4. Unmittelbare Vermögensminderung durch Weitergabe der Zugangsdaten durch den Account-Sharer	135
5. Unmittelbare Vermögensminderung durch die Entschlüsselung beziehungsweise Auswahl der Sendeinhalte und deren Wiedergabe beim Card- und Account-Sharing	135
a) Anspruch auf vertragliche Gegenleistung	135
b) Anspruch auf Schadensersatz	136
c) Leistungserbringung ohne Erhalt einer Gegenleistung	136
aa) Gleichbleibende Aufwendungen des Anbieters	136
bb) Entreichungsschaden durch entgangenes Entgelt	137
(1) Entreichung aufgrund der Wiedergabe der Sendeinhalte	137
(2) Unmittelbarkeit dieser Entreichung	139
cc) Entreichung hinsichtlich des im Nutzungsrecht an den Sendeinhalten verkörperten Vermögenswertes	140
(1) Annahme einer Vermögensminderung über Gedanken der Wertminderung eines Nutzungsrechts	140
(2) Kein Ausschluss der Vermögensminderung wegen eigenverantwortlichen Verhaltens	142
(3) Keine taugliche Minderungsberechnung über die Grundsätze der Lizenzanalogie	144
(4) Keine messbare Vermögensminderung über die Anwendung der Grundsätze der Markttextpektanz	147
6. Unmittelbare Vermögensminderung durch den Login beim Account-Sharing	150
7. Ergebnis	151
VI. Ergebnis zu § 263a StGB	152
C. Vorbereitung eines Computerbetrugs – § 263a Abs. 3 StGB	152
I. Account-Sharing	152
II. Cardsharing	153
D. Erschleichen von Leistungen – § 265a StGB	154
I. Keine Einschlägigkeit von § 265a Abs. 1 Var. 3 und 4 StGB	154
II. Erschleichen einer entgeltlichen Leistung eines Automaten	154
1. Leistungsautomaten im Rahmen des Cardsharings	155
a) Smartcard	155
b) Receiver des Sharers als Smartcard-Server	155
c) Receiver des Nutzers	156
2. Leistungsautomaten im Rahmen des Account-Sharings	157
3. Zwischenergebnis	158
4. Entgeltlichkeit der Leistung der Automaten beim Cardsharing	158
5. Erschleichen der Automatenleistung	159
6. Ergebnis	161

III. Erschleichen der entgeltlichen Leistung eines öffentlichen Zwecken dienenden Telekommunikationsnetzes	161
1. Informationsübermittlung als erschlichene entgeltliche Leistung	163
a) Durch den Sharer	163
b) Durch den Nutzer	164
2. Inhaltszugriff als erschlichene entgeltliche Leistung	164
a) Durch den Sharer	165
b) Durch den Nutzer	165
aa) Entgeltliche Leistung	165
(1) Netzleistung nur Übermittlung	165
(2) Netzleistung auch Genusseinräumung der Inhalte	166
bb) Erschleichen dieser Leistung	169
(1) Passwortschutz als ausreichendes Zugangshindernis	170
(2) Tatbestandliches Erschleichen trotz äußerlich ordnungsgemäßen Handelns	172
(3) Extensive Auslegung der Tathandlung	173
(4) Verwendung der Kontroll- und Zugangsdaten zum Passieren der Zugangskontrolle als Erschleichen	174
(a) Vergleichbarkeit mit den Konstellationen kollusiven Zusammenwirkens bei § 265a Abs. 1 Var. 3, 4 StGB	175
(b) Vergleichbarkeit mit den bei § 263a Abs. 1 Var. 3 StGB diskutierten Fällen des Missbrauchs von Codekarten	176
(c) Gleichlauf mit der Behandlung der unbefugten Datenverwendung bei § 263a StGB	177
IV. Ergebnis	178
V. Beteiligung des Sharers	179
1. Einordnung der Sharerhandlung in den Fällen des Account-Sharings	179
2. Einordnung der Sharerhandlung in den Fällen des Cardsharings	181
3. Ergebnis	182
VI. Rechtsfolgen und Strafverfolgung	182
E. Untreue – § 266 StGB	183

§ 2

Straftaten gegen den Geheimnisbereich 184

A. Ausspähen von Daten – § 202a StGB	184
I. Cardsharing	184
1. Daten	185
2. Sicherung vor unberechtigtem Zugang	186

- 3. Nicht für den Täter bestimmt 187
 - a) (Nicht) für den Sharer bestimmte Daten 188
 - aa) Auf der Smartcard gespeicherte Berechtigungsdaten 188
 - bb) Kontrollwort 192
 - cc) Audio-Video-Daten 192
 - dd) Zwischenergebnis 195
 - b) (Nicht) für den Nutzer bestimmte Daten 195
 - aa) Berechtigungsdaten und Kontrollwort 195
 - bb) Audio-Video-Daten 197
 - cc) Zwischenergebnis 198
- 4. Tathandlung: unbefugtes Verschaffen von nicht für den Täter bestimmten Daten unter Überwindung der Zugangssicherung 199
 - a) Sharer: Verschaffen des Zugangs zu den Audio-Video-Daten unter Überwindung der Zugangssicherung 199
 - aa) Zugangsverschaffung zu den Audio-Video-Daten 199
 - bb) Unter Überwindung der Zugangssicherung 201
 - cc) Zwischenergebnis 201
 - b) Nutzer: Verschaffen des Zugangs zu den Audio-Video-Daten unter Überwindung der Zugangssicherung 201
 - aa) Tatsächliche Zugangsverschaffung trotz Ausstrahlung durch den Anbieter 202
 - bb) Zugangsverschaffung auch bei vom Berechtigten erhaltenen Schlüssel 202
 - cc) Überwinden einer besonderen Zugangssicherung 203
 - dd) Unbefugt 206
 - ee) Zwischenergebnis 207
- II. Account-Sharing 207
 - 1. Taugliches Tatobjekt 207
 - a) Zugangsdaten 207
 - b) Bereitgehaltene Sendeinhalte-Daten 208
 - aa) Datenqualität 208
 - bb) Nicht für den Täter bestimmt 208
 - cc) Gegen unberechtigten Zugang besonders gesichert 208
 - 2. Tathandlung 209
 - a) Sharer 209
 - b) Nutzer 210
 - 3. Ergebnis 211
- III. Beteiligung des Sharers 211
- IV. Ergebnis zu § 202a StGB 213
- V. Rechtsfolgen/Strafverfolgung/Strafantrag 213

B. Vorbereiten des Ausspähöns und Abfangens von Daten – § 202c StGB	213
I. Begrifflichkeiten	214
II. Cardsharing	215
1. Tatobjekte	215
a) Berechtigungsdaten	215
b) Kontrollwort	215
c) Cardsharingnetzwerk als Computerprogramm	215
d) Software auf dem Cardsharing-Server	215
e) Software auf dem Nutzer-Receiver	216
2. Tathandlung	216
a) Cardsharer	216
aa) Berechtigungsdaten	216
(1) Kein Tatbestandsausschluss wegen zivilrechtlich erlaubten Verhaltens	218
(2) Kein Ausschluss der Strafbarkeit aufgrund von Einverständnis oder Einwilligung	218
(3) Ausschluss der Strafbarkeit aus teleologischen Erwägungen	219
bb) Kontrollwort	219
cc) Software für den Cardsharing-Server	220
dd) Software für den Receiver des Nutzers	220
ee) Zur Vorbereitung einer Tat nach § 202a StGB	220
b) Nutzer	221
aa) Berechtigungsdaten	221
bb) Kontrollwort	221
cc) Software für den Cardsharing-Server	221
dd) Software für den Receiver des Nutzers	221
ee) Zur Vorbereitung einer Tat nach § 202a StGB	222
III. Account-Sharing	222
1. Zugangsdaten als taugliches Tatobjekt	222
2. Tathandlung im Sinne von § 202c Abs. 1 StGB	223
a) Account-Sharer	223
aa) Eigenbezogene Tathandlungen	223
bb) Drittbezogene Tathandlungen	223
b) Nutzer	224
IV. Täterschaft und Teilnahme	224
V. Ergebnis	225
VI. Rechtsfolgen und Strafverfolgung	225
C. Abfangen von Daten – § 202b StGB	225
D. Datenhehlerei – § 202d StGB	226

- E. Verletzung von Geschäftsgeheimnissen – § 23 GeschGehG 227
 - I. Vorliegen eines Geschäftsgeheimnisses 227
 - II. Tatbestandserfüllung in den hier interessierenden Konstellationen 229
 - 1. Cardsharing 229
 - a) Geschäftsgeheimnis 229
 - aa) Verschlüsselungstechnik der ausgestrahlten Sendeinhalte 229
 - bb) Verschlüsselt ausgestrahlte Audio-Video-Dateien 230
 - cc) Auf der Smartcard gespeicherte Berechtigungsdaten 232
 - dd) Kontrollwort zur Entschlüsselung der verschlüsselten Programminhalte 232
 - b) Erfüllung einer tatbestandlichen Handlung durch den Sharer 233
 - aa) Erlangen durch unbefugten Zugang gemäß § 4 Abs. 1 Nr. 1 GeschGehG 234
 - bb) Erlangen durch unbefugte Aneignung gemäß § 4 Abs. 1 Nr. 1 GeschGehG 236
 - cc) Erlangen durch unbefugte Kopie gemäß § 4 Abs. 1 Nr. 1 GeschGehG 236
 - dd) Nutzen oder Offenlegen eines Geschäftsgeheimnisses gemäß §§ 23 Abs. 1 Nr. 2, 4 Abs. 2 Nr. 1 lit. a) GeschGehG 237
 - ee) § 23 Abs. 2 in Verbindung mit Abs. 1 Nr. 2, 3 GeschGehG 237
 - ff) Zwischenergebnis 237
 - c) Erfüllung einer tatbestandlichen Handlung durch den Nutzer 238
 - aa) Erlangen durch unbefugten Zugang gemäß § 4 Abs. 1 Nr. 1 GeschGehG 238
 - bb) Erlangen durch unbefugte Aneignung gemäß § 4 Abs. 1 Nr. 1 GeschGehG 238
 - cc) Erlangen durch unbefugte Kopie gemäß § 4 Abs. 1 Nr. 1 GeschGehG 239
 - dd) Nutzen oder Offenlegen eines Geschäftsgeheimnisses im Sinne von §§ 23 Abs. 1 Nr. 2, 4 Abs. 2 Nr. 1 lit. a) GeschGehG 239
 - ee) § 23 Abs. 2 i. V.m. Abs. 1 Nr. 2, 3 GeschGehG 240
 - d) Ergebnis 240
 - 2. Account-Sharing 240
 - a) Geschäftsgeheimnis 241
 - aa) Bereitgehaltene Sendeinhalte 241
 - bb) Verschlüsselung der jeweiligen Anbieterseite oder des Anbieterservers 241
 - cc) Zugangsdaten 242
 - (1) Information 242
 - (2) Geheime Information 242
 - (3) Geschäfts- beziehungsweise Unternehmensbezug 243
 - dd) Ergebnis 246
 - b) Mögliche Tathandlung des Sharers 246
 - c) Mögliche Tathandlung des Nutzers 246

III. Ergebnis	247
F. Strafvorschrift des § 42 BDSG	247
I. Strafbarkeit nach § 42 Abs. 1 BDSG	247
II. Strafbarkeit nach § 42 Abs. 2 BDSG	248

§ 3

Straftaten wegen urheberrechtswidrigen Handelns	250
A. Unerlaubte Verwertung urheberrechtlich geschützter Werke – § 106 UrhG	250
I. Schutzobjekt: Werk	250
1. Grundsätzliche Voraussetzungen	251
2. Anwendung im Bereich des Sharings	251
a) Filmwerke	252
b) Sportübertragungen	252
c) Kontrollwort beziehungsweise Zugangs- und Berechtigungsdaten	253
aa) Kontrollwort als Werk in den Fällen des Cardsharings	254
bb) Kontrollwort generierender Algorithmus in den Fällen des Cardsharings	255
cc) Berechtigungs- und Zugangsdaten	255
3. Rechteinhaber	256
II. Tatbestandserfüllung durch den Nutzer	256
1. Tathandlung: Vervielfältigung	256
a) Allgemein	256
b) Technische Fragestellungen – körperliche Fixierung	257
aa) Fernsehsignale – Funksendungen	257
bb) Funktionsweise des Streamings	258
c) Erfüllung der Voraussetzungen des § 16 UrhG	259
2. Tathandlung: Verbreitung	260
3. Tathandlung: öffentliche Wiedergabe	261
4. Gesetzlich zugelassene Fälle	261
a) Privilegierte Nutzung wegen § 53 UrhG	261
aa) Allgemein	262
bb) Vorlage	262
(1) Offensichtlich rechtswidrig hergestellt	263
(2) Offensichtlich rechtswidrig öffentlich zugänglich gemachte Vorlage	263
(a) Vergleich mit den Fällen des Linkings	264
(b) Keine Auslegung des Merkmals im Sinne einer öffentlich wiedergegebenen Vorlage	265

(3) Rechtswidrigkeit der Vervielfältigung wegen Verstoßes gegen § 95a UrhG	267
(a) Normverhältnis	267
(b) Verstoß gegen § 95a UrhG als Ausschluss der Privilegierung nach § 53 UrhG?	268
(c) Verstoß gegen § 95a UrhG lässt Privilegierung nach § 53 Abs. 1 S. 1 UrhG unberührt	269
(d) Zwischenergebnis	271
b) Privilegierte Nutzung nach § 44a UrhG	271
aa) Allgemein	271
bb) Allgemeine Voraussetzungen des § 44a UrhG	272
cc) Keine eigenständige wirtschaftliche Bedeutung	273
dd) Nutzungszwecke nach § 44a Nr. 1 und 2 UrhG	273
(1) Zweck nach § 44a Nr. 1 UrhG	273
(2) Zweck nach § 44a Nr. 2 UrhG	274
(a) Rechtmäßige Nutzung	274
(b) Rechtmäßige Nutzung bei Umgehung einer technischen Schutzmaßnahme	275
5. Zwischenergebnis und eventuelle Versuchsstrafbarkeit	276
III. Tatbestandserfüllung durch den Sharer	277
1. Tathandlung: Vervielfältigung	277
2. Tathandlung: Verbreitung	277
3. Tathandlung: öffentliche Wiedergabe	278
a) Benannte Verwertungsrechte	278
b) Unbenanntes Verwertungsrecht i. S. v. § 15 Abs. 2 UrhG	279
aa) Eröffnung des Anwendungsbereichs der Richtlinie	280
bb) Voraussetzungen der öffentlichen Wiedergabe nach Art. 3 Abs. 1 InfoSoc-RL	281
(1) Handlung der Wiedergabe	281
(2) Öffentlichkeit der Wiedergabe	282
(3) Entwicklung des Merkmals der Öffentlichen Wiedergabe in der Judikatur des EuGH	283
(a) Ausgangsentwicklung	283
(b) Öffentliche Wiedergabe und Linking in der Rechtsprechung des <i>EuGH</i>	284
cc) Übertragung der Judikatur des <i>EuGH</i> auf die hier interessierenden Fälle	286
(1) Fälle des Account-Sharings	286
(2) Fälle des Cardsharings	286
(a) Handlung der Wiedergabe	286
(b) Öffentlichkeit der Wiedergabe	288

(c) Zwischenergebnis	290
(3) Kritik an einer solchen Auslegung der öffentlichen Wiedergabe	290
(4) Übertragbarkeit und Erfordernis eines restriktiven Verständnisses	292
dd) Lockerung der Akzessorietät bei § 106 UrhG in den Fällen harmonisierten Urheberzivilrechts	294
(1) Dogmatische Einordnung des Tatbestandsmerkmals „öffentliche Wiedergabe“	294
(2) Einfluss des Unionsrechts auf das Urheberstrafrecht	296
(a) Richtlinienziel	298
(b) Mittel zur Zielerreichung	298
(aa) Allgemeines zur Mindesttrias und dem Gleichstellungserfordernis	299
(bb) Schutz eines tauglichen Unionsinteresses im konkreten Fall	301
(cc) Erfüllung der Kriterien der Mindesttrias in den hier untersuchten Konstellationen	302
(α) Verpflichtung zur Schaffung strafrechtlicher Sanktionen durch die InfoSoc-RL?	302
(β) (Urheber-)Zivilrechtliche Normen und Anforderungen der Richtlinie	307
(dd) Zwischenergebnis	313
ee) Lockerung der strengen Akzessorietät	313
(1) Lockerung der Urheberzivilrechtsakzessorietät aufgrund des Schutzzwecks der Norm	314
(a) Wortlaut der Norm	315
(b) Systematische Auslegung	316
(c) Teleologische Auslegung	317
(2) Verfassungskonforme Auslegung	317
(a) Kein Verstoß gegen das Analogieverbot	318
(b) Verstoß gegen das Bestimmtheitsgebot	318
(c) Ultima ratio-Grundsatz als Grund zur Einschränkung der Akzessorietät	319
(3) Eigenständige strafrechtliche Begriffsbestimmung des Merkmals der öffentlichen Wiedergabe	320
4. Ergebnis zu der Frage der Strafbarkeit des Sharers nach § 106 UrhG	322
IV. Ergebnis	322
B. Unerlaubte Eingriffe in verwandte Schutzrechte – § 108 UrhG	322
I. Strafbarkeit des Nutzers	323
1. Tatobjekt und Tathandlung	323
a) Leistungsschutzrecht der ausübenden Künstler – § 108 Abs. 1 Nr. 4 UrhG	323
b) Leistungsschutzrecht des Sendeunternehmens – § 108 Abs. 1 Nr. 6 UrhG	323
aa) Funksendung	324

- bb) Verwertung entgegen § 87 UrhG 325
 - c) Leistungsschutzrecht des Filmherstellers – § 108 Abs. 1 Nr. 7 UrhG 326
 - 2. Ergebnis für den Nutzer 326
- II. Strafbarkeit des Sharers 326
- III. Gewerbsmäßige Begehungsweise nach § 108a UrhG 327

C. Unerlaubte Eingriffe in technische Schutzmaßnahmen und zur Rechtewahrnehmung erforderliche Informationen – § 108b UrhG 327

- I. Strafbarkeit des Nutzers 328
 - 1. Wirksame technische Maßnahme 328
 - a) Cardsharing 329
 - b) Account-Sharing 330
 - 2. Tathandlung: Umgehung 331
 - a) Empfang des Sendesignals und Weiterleitung der ECM 332
 - b) Entschlüsselung der Sendeinhalte mit dem Kontrollwort/ Einsatz der Zugangsdaten 332
 - c) Kein anderes Ergebnis wegen äußerlich ordnungsgemäßen Handelns 332
 - 3. Tatbestandsausschluss bei privatem Handeln 334
 - 4. Ergebnis 335
- II. Strafbarkeit des Sharers 335
 - 1. Umgehungshandlung 335
 - 2. Privater Gebrauch und Ergebnis 337
 - 3. Vorbereitungshandlungen durch den Sharer 337

D. Strafvorschrift des § 33 KUG 337

§ 4

**Weitere Straftaten, insbesondere aus dem Bereich
der Cyberkriminalität**

339

- A. Strafvorschrift des § 4 ZKDSG 339
 - I. Strafbarkeit des Nutzers 340
 - II. Strafbarkeit des Sharers 340
 - 1. Begriffliche Klärungen 340
 - a) Umgehungsvorrichtung 340
 - b) Zugangskontrollierte Dienste 341
 - c) Zugangskontrolldienste 341
 - 2. Tatbestandserfüllung des § 4 ZKDSG in den Fällen des Sharings 341
 - a) Zugangskontrollierte Dienste und Zugangskontrolldienst als Vorbedingungen 341
 - aa) Cardsharing 342

bb) Account-Sharing	342
b) Umgehungsvorrichtung in den Fällen des Cardsharings	343
c) Verbotene Handlung gemäß §§ 4, 3 Nr. 1 ZKDSG in den Fällen des Cardsharings	344
d) Tatbestandserfüllung des § 4 ZKDSG durch den Account-Sharer?	345
III. Ergebnis und Rechtsfolgen	346
B. Fälschung beweisheblicher Daten – § 269 StGB	346
I. Strafbarkeit des Nutzers	347
1. Cardsharing	347
2. Account-Sharing	349
a) Login in Abgrenzung zur Account-Registrierung	349
b) Login als für § 269 StGB relevanter Vorgang	350
aa) Login als hinreichend perpetuierte Gedankenerklärung	350
bb) Beweiserheblichkeit des Login-Vorgangs	351
cc) Andere Bewertung hinsichtlich der Beweiserheblichkeit wegen ein- deutiger individueller Zuordnung der Zugangsdaten?	352
dd) Mangelnde Perpetuierung des Logins als Argument fehlender Be- weiserheblichkeit	353
c) Keine für § 269 StGB relevante Handlung durch Wahrnehmbarmachung der Inhalte am Bildschirm	355
d) Ergebnis	355
II. Sharer	356
1. Account-Sharing	356
2. Cardsharing	356
C. Fälschung technischer Aufzeichnungen – § 268 StGB	357
D. Datenveränderung – § 303a StGB	358
E. Computersabotage – § 303b StGB	359
F. Störung von Telekommunikationsanlagen – § 317 StGB	359
G. Öffentliche Aufforderung zu Straftaten – § 111 StGB	360
H. Strafvorschrift des § 148 TKG	360
§ 5	
Gesamtergebnis und Konkurrenzen zu Kapitel 3	361
A. Gesamtergebnis und Konkurrenzen hinsichtlich des Nutzers	361

B. Gesamtergebnis und Konkurrenzen hinsichtlich des Sharers 361
 I. Ergebnis zu den Straftaten 361
 II. Konkurrenzen 362

Kapitel 4

**Bewertung der gefundenen Ergebnisse und Vorschlag zur Erfassung
 des Sharings de lege ferenda** 364

A. Kriminalpolitisch unbefriedigende Rechtslage de lege lata 364

B. Erforderlichkeit eines das Sharing erfassenden Straftatbestandes de lege ferenda ... 365
 I. Notwendigkeit einer Sharing-Strafnorm de lege ferenda 365
 1. Aufgabe und Zweck des Strafrechts als Grenze strafrechtsbezogener Ände-
 rungen 365
 2. Sharing als strafwürdiges und strafbedürftiges Unrecht 366
 a) Nutzerverhalten 366
 b) Sharerverhalten 368
 c) Zwischenergebnis 371
 3. Bewertung der Entwürfe für die §§ 127, 202e StGB und zu § 202a StGB ... 372
 a) § 127 StGB-E – Betreiben krimineller Handelsplattformen im Internet .. 373
 b) § 202e StGB-E – Unbefugte Benutzung informationstechnischer Systeme 375
 c) Änderungsvorschlag zu § 202a StGB von Eisele/Nolte 376
 d) Bewertung der vorgestellten Entwürfe 378
 4. § 4 ZKDSG als ausreichender Schutz? 379
 II. Vergleichender Blick insbesondere auf die schweizerische Rechtslage 381

C. Erweiterung des § 265a StGB als vorzugswürdige Lösung 384
 I. Normtext 384
 II. Begründung und Erläuterung 385
 1. Zu § 265a Abs. 1 StGB-E 385
 2. Zu § 265a Abs. 4 und 5 StGB-E 386
 3. Zu § 265a Abs. 6 StGB-E 388
 III. Konkurrenzen zur im Übrigen bestehenden Sharerstrafbarkeit 388

Zusammenfassung der wesentlichen Ergebnisse 390

Literaturverzeichnis 393

Sachwortverzeichnis 410

Einleitung

A. Einführung

In einer 2016 ergangenen Entscheidung des *United States Court of Appeals for the Ninth Circuit* befand die Mehrheit des Gerichts, die Weitergabe von Zugangsdaten durch Mitarbeiter eines Unternehmens an solche Personen, deren Zugangsberechtigung zurückgenommen ist, sei ebenso strafbar wie deren spätere Verwendung durch die nicht berechtigten Empfänger.¹ Dabei stützte das Gericht seine Ansicht auf die Strafnorm des 18. U.S.C. § 1030(a)(4) Computer Fraud and Abuse Act (CFAA)², da als eine Zugangsberechtigung erteilende Stelle einzig das Unternehmen selbst beziehungsweise dessen gesetzliche Vertreter in Betracht kommen. Dies gelte ebenso für einen unternehmensbezogenen Privataccount von noch dort beschäftigten Personen. Die Entscheidung rief in US-amerikanischen Medien soweit ersichtlich ein breites Echo hervor, da sie in ihrer Reichweite nicht auf betriebsbezogene Accounts beschränkt war, sondern auch etwa den Zugang zu Streamingaccounts betraf. So war im Anschluss daran häufig davon zu lesen, dass nunmehr das Teilen eines Accounts des Streaminganbieters *Netflix* illegal und daher strafbar sei.³ Dem Medienecho kann entnommen werden, dass die Entscheidung Überraschung und Verunsicherung zugleich hervorrief, was sich daraus erklären könnte, dass die Zahl derer, die einen Account mit Personen teilen, die über diesen nicht nutzungsberechtigt sind, sehr hoch zu sein scheint. Wie aus einer Studie des Blogs *Cordcutting* hervorgeht, soll allein für den schon genannten Streamingdienst *Netflix* angenommen werden, dass im Jahr 2019 in den USA etwa 24 Millionen Personen den Account einer anderen Person benutzten, während es im Jahr 2020 immerhin noch etwa 21,5 Millionen waren.⁴ Nach einer von den Internetdiensten *CHIP* und *Civey* für Deutschland durchgeführten Umfrage teilen etwa 84 % von 1.210 Befragten ihr Nutzerkonto mit

¹ *United States vs. Nosal* 844 F.3d 1024 (9th Cir. 2016).

² Danach ist strafbar, „[w]hoever [...] knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value [...]“.

³ *Tepper*, <https://techcrunch.com/2016/07/11/a-court-ruled-that-it-could-be-a-federal-crime-to-share-your-netflix-password/>; *Williams*, <https://www.marketwatch.com/story/sharing-netflix-and-hbo-passwords-is-now-a-federal-crime-but-heres-why-not-to-worry-2016-07-12>; <https://blog.jipfel.law.nyu.edu/2018/04/is-using-a-shared-netflix-password-a-federal-crime/> (alle zuletzt abgerufen am 09.08.2021).

⁴ *Cordcutting*, <https://cordcutting.com/research/subscription-mooching/2020/>; *Lovely*, <https://cordcutting.com/research/subscription-mooching/> (alle zuletzt abgerufen am 09.08.2021).

einer dritten Person.⁵ Das Phänomen des Account-Sharing oder auch *subscription mooching* kann somit schon fast als ubiquitär bezeichnet werden. Der Richter Reinhardt schreibt nun aber in seiner *dissenting opinion*, letztlich vergleichbar einem Sondervotum, zu der eingangs erwähnten Entscheidung, dass Menschen regelmäßig Passwörter mit Dritten teilen und sie durch diese allgegenwärtige, nützliche und generell harmlose Handlung nicht zu Kriminellen werden.⁶ Dies spiegelt wohl die weit verbreitete Meinung der Nutzer wider, die ausweislich der genannten Schätzungen und Umfragen ein solches Teilen von Passwörtern, Zugangsdaten und letztlich Accounts betreiben. Während nun die einen ein solches Teilen von Zugangsdaten als nicht sonderlich verwerflich einordnen, sehen dies die Anbieter von entgeltpflichtigen Leistungen naturgemäß anders. Dies leuchtet insbesondere vor dem Hintergrund der enormen wirtschaftlichen Folgen solcher Handlungen ein. Wiederum bezugnehmend auf die Studie des Blogs *Cordcutting* ist anzunehmen, dass allein dem Dienst *Netflix* im Jahr 2020 monatlich geschätzte 131 Millionen US-Dollar an Abonnementgebühren dadurch entgangen sind, dass Abonnenten den Zugang zu den Diensten an Nichtberechtigte weitergeben beziehungsweise mit diesen teilen.⁷ Ein vergleichbares Problem stellt sich dem Pay-TV-Unternehmen der Sky Deutschland GmbH (*Sky*) mit dem noch zu erläuternden Phänomen des Cardsharings. Welches wirtschaftliche Ausmaß dies annimmt, zeigt etwa die Sachverhaltsdarstellung des LG Dresden, wonach ein Serverbetreiber fast 3,5 Millionen Euro von Nutzern seines Dienstes eingenommen hat.⁸ Diese Summen, wenn auch nicht eins zu eins, entgehen wiederum dem Anbieter der Programminhalte. Im Herbst des Jahres 2019 war daher zu lesen, dass der Medienkonzern *Sky* (die Sky Deutschland GmbH) den Empfang der von ihm ausgestrahlten Sendeinhalte mittels Drittanbieterreceivern technisch unterbindet.⁹ Wer mithin über die Satellitenübertragung entsprechende Sendeinhalte von *Sky* empfangen möchte, muss fortan den „hauseigenen“ Receiver „Sky Q“ verwenden. Hintergrund dieser Maßnahme ist ein neuerliches Vorgehen gegen Piraterie, um illegale Zugriffe auf die Sendeinhalte, insbesondere durch Cardsharing, zu unterbinden. Ob mit dieser Umstellung auf das

⁵ Hayon, https://www.chip.de/news/Umfrage-zeigt-wie-massiv-Netflix-Accounts-geteilt-werden_159677625.html (zuletzt abgerufen am 09.08.2021).

⁶ *United States vs. Nosal* 844 F.3d 1024 (9th Cir. 2016), S. 46 – „*People frequently share their passwords, notwithstanding the fact that websites and employers have policies prohibiting it. In my view, the Computer Fraud and Abuse Act („CFAA“) does not make the millions of people who engage in this ubiquitous, useful, and generally harmless conduct into unwitting federal criminals.*“ – Hervorhebungen nicht im Original.

⁷ Lovely, <https://cordcutting.com/research/subscription-mooching/> (zuletzt abgerufen am 09.08.2021).

⁸ LG Dresden, Urt. v. 12.01.2018 – 5 KLs 414 Js 6229/17.

⁹ Krieger, <https://www.infosat.de/digital-tv/schlag-gegen-pay-tv-piraterie-sky-aktiviert-unique-pairing; Szymanski, https://www.computerbild.de/artikel/avf-News-Fernseher-Sky-sperret-Receiver-Drittanbieter-24440287.html> (alle zuletzt abgerufen am 09.08.2021).

„unique pairing“ ein finaler Schlag gegen Cardsharing gelingt¹⁰, bleibt abzuwarten, erscheint aber im Hinblick auf das Fortbestehen der Cardsharing-Server nach Einführung des „Pairing“¹¹ durch Sky im Jahr 2014 als unwahrscheinlich. Auch hinsichtlich des Phänomens des Account-Sharings sind in letzter Zeit vermehrt Berichte zu lesen, nach denen etwa die Anbieter *Netflix* oder *Spotify* die Nutzung von Accounts durch hierzu Nichtberechtigte durch Implementierung verschiedener technischer Maßnahmen wie dem Tracking von IP-Adressen oder sonstiger Standortdaten verhindern wollen.¹²

Unbefugter Zugriff auf an sich verschlüsselte Sendeinhalte ist dabei mittlerweile kein junges Phänomen mehr. Man denke hierbei nur an die bekannt gewordenen Fälle der Piratenkarten¹³ oder der Streamingplattform kino.to¹⁴. Wie so oft zeigt sich aber auch im Bereich des Pay-TV, dass neue technische Möglichkeiten der Ausstrahlung und Verschlüsselung wiederum neue Möglichkeiten der Umgehung schaffen. Dennoch stellen die beiden hier genannten Phänomene des Card- und Account-Sharings insofern neue und von den bisherigen Formen der unbefugten Nutzung von Inhalten zu unterscheidende Formen dar, dass – verkürzt – ein an sich berechtigter Nutzer¹⁵ eines Anbieterdienstes die ihm überlassenen Berechtigungs- beziehungsweise Zugangsdaten mit Dritten, also nicht Vertragspartnern, teilt (engl. „to share“ = etw. teilen, gemeinsam benutzen). Die Verwendung der Daten zielt daher entweder auf die Überwindung einer Passwortkontrolle bei einem Login oder aber – letztlich – auf die Entschlüsselung von verschlüsselt ausgestrahlten Programminhalten. Einzelheiten der – unterschiedlichen – technischen Abläufe werden dabei in einem speziellen Unterkapitel erörtert (Kap. 1 B.).

¹⁰ So etwa *Sobiraj*, <https://tarnkappe.info/sky-stellt-verschluesselung-um-manche-legale-nutzer-sehen-nichts-mehr/> (zuletzt abgerufen am 09.08.2021).

¹¹ Als Pairing wird eine Technik bezeichnet, die es ermöglicht, dass eine Smartcard nach Verbindungsaufbau mit einem Endgerät mit keinem anderen Endgerät funktioniert, vgl. <https://sky-pairing.myblog.de/>. Beim Unique Pairing funktioniert die noch darzustellende Entschlüsselung der ausgestrahlten Sendeinhalte nur noch mit einem vom Anbieter ausgegebenen Gerät, etwa einem Receiver, *Deutschbein*, <https://www.techbook.de/entertainment/streaming/sky-unique-pairing-verschluesselung-receiver> (alle zuletzt abgerufen am 09.08.2021).

¹² *Birner/Mühlroth*, <https://www.techbook.de/entertainment/streaming/netflix-account-sharing-stop>; *Breithut*, <https://www.spiegel.de/netzwelt/apps/netflix-spotify-amazon-prime-dazn-sky-mit-wem-darf-ich-mein-abo-teilen-a-1252088.html>; *Laaff*, <https://www.zeit.de/digital/2019-09/spotify-streamingdienst-familienabo-wohndresse-pruefung?>; *Petzold*, <https://www.gamestar.de/artikel/neue-spotify-nutzungsbedingungen-family-nutzer-muessen-an-derselben-adresse-wohnen,3349021.html> (alle zuletzt abgerufen am 09.08.2021).

¹³ Vgl. hierzu etwa OLG Frankfurt a.M. NJW 1996, 264 f.; *Beucher/Engels*, CR 1998, 101 ff.; *Dressel*, MMR 1999, 390 ff.; *Scheffler*, CR 2002, 151 ff.

¹⁴ Vgl. hierzu etwa LG Leipzig ZUM 2013, 338 mit Besprechung von *Reinbacher*, NSTZ 2014, 57 ff.; AG Leipzig NZWiSt 2012, 390 ff.

¹⁵ Diese Arbeit verwendet aus Gründen der besseren Lesbarkeit das generische Maskulinum. Weibliche und diverse Geschlechteridentitäten werden dabei ausdrücklich mitgemeint, soweit es für die Aussage erforderlich ist.