# Inhaltsverzeichnis

**Vorwort** ... V

**Inhaltsübersicht** ... VII

**Abkürzungsverzeichnis** ... XIX

**Einleitung** ... 1

**Teil 1: Grundlagen des Internetstrafrechts** ... 5

**Kapitel 1: Das Internet und das Strafrecht** ... 5
I. Entwicklung und Funktionsweise des Internets ... 5
1. Vorbemerkung ... 5
2. Historischer Überblick ... 6
3. Funktionsweise des Internets ... 7
II. Herausforderungen aus strafrechtlicher Perspektive ... 8
1. Großer potenzieller Täterkreis ... 9
2. Technische Besonderheiten des Internets ... 10
3. Spezielle Angriffsformen ... 12

**Kapitel 2: Die Entwicklung des Internetstrafrechts in Deutschland** ... 14
I. Einleitung ... 14
II. Die wesentlichen Reformen des deutschen Internetstrafrechts ... 14
1. Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität ... 14
2. Informations- und Kommunikationsdienstgesetz ... 15
3. Gesetze zur Regelung des Urheberrechts in der Informationsgesellschaft ... 15
4. 41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität ... 16
5. Weitere Gesetzesreformen ... 16
III. Internationale Vorgaben ... 17
1. Convention on Cybercrime ... 18
2. Weitere internationale Vorgaben ... 19

**Kapitel 3: Materielles Strafrecht** ... 20
I. Einleitung ... 20
II. Der Begriff des Internetstrafrechts ... 21
III. Internationales Strafrecht ... 22
1. Grundlagen ... 22
2. Das Internationale Strafrecht, §§ 3 ff. StGB ... 23
a) Territorialitätsprinzip, § 3 StGB ... 23
aa) Handlungsort ... 23
bb) Erfolgsort ... 24
b) Schutzprinzip, § 5 Nr. 8 StGB ... 24
c) Weltrechtsprinzip, § 6 Nr. 6 StGB ... 24

IV. Schriftenbegriff ... 25
V. Straftaten gegen die Vertraulichkeit, Unversehrtheit und Verfügbarkeit von Computerdaten ... 25
1. Ausspähen von Daten, § 202a StGB ... 26
a) Tatbestand ... 26
b) Die Zugangsverschaffung in der Praxis ... 27
aa) Vorbereitungshandlungen ... 27
bb) Brute-Force-Angriffe ... 27
cc) Trojan-Horse ... 28
dd) Phishing ... 29
2. Abfangen von Daten, § 202b StGB ... 30
3. Vorbereiten des Ausspähens und Abfangens von Daten, § 202c StGB ... 31
4. Datenveränderung, § 303a StGB ... 31
5. Computersabotage, § 303b StGB ... 32
VI. Verbreitung illegaler Inhalte (Inhaltsdelikte) ... 32
1. Pornographiestrafrecht, §§ 184 ff. StGB ... 33
2. Extremistische Propaganda ... 34
VII. Computerbezogene Delikte ... 34
1. Der Betrug, § 263 StGB ... 34
2. Computerbetrug, § 263a StGB ... 35
3. Fälschung beweiserheblicher Daten, § 269 StGB ... 35
4. Weitere Delikte ... 36
VIII. Nebenstrafrecht ... 36
1. Urheberstrafrecht ... 36
2. Strafbarkeit nach dem BDSG ... 37

**Teil 2: Ausgewählte Problemfelder des Internetstrafrechts** ... 39

**Kapitel 1: Strafrechtliche Probleme im Web 2.0** ... 39
I. Grundlagen ... 39
1. Einführung ... 39
2. Entstehungsgeschichte und Begriffliches ... 40
a) Technische Perspektive ... 41
b) Wirtschaftliche Perspektive ... 42
3. Strafrechtliche Problemfelder ... 43
II. Tauschbörsen und Filesharing ... 43
1. Grundlagen ... 44
a) Filesharing-Netzwerke ... 45
b) File- bzw. Sharehosting ... 46
c) Sonderformen ... 47
2. Urheberstrafrecht ... 47
a) Anbieten von geschützten Werken in P2P-Systemen ... 48
b) Download von geschützten Werken in P2P-Netzwerken ... 48
c) Das Anbieten und Downloaden von Dateien mittels File- bzw. Sharehosting ... 49
d) Vorfeldkriminalisierung ... 50
3. Strafbare Handlungen der Plattformbetreiber ... 51
a) Betreiber eines Filesharing-Netzwerks ... 51
b) Betreiber eines Sharehosting-Portals ... 52

aa) Neutrale Beihilfe ... 52
(1) Rechtliche Kriterien der Neutralen Beihilfe ... 53
(a) Kriterien der objektiven Zurechnung ... 53
(b) Ansatz der „professionellen Adäquanz“ ... 54
(c) Objektiv-subjektiver Ansatz ... 54
(d) Stellungnahme ... 55
(2) Rechtliche Beurteilung des Sharehosting ... 55
(a) Sozialadäquanz des Sharehosting ... 55
(aa) Ansicht des OLG Hamburg ... 56
(bb) Rechtsprechung des BGH ... 56
(cc) Stellungnahme ... 57
(b) Subjektive Voraussetzungen der neutralen Beihilfe ... 58
(c) Beihilfevorsatz ... 59
bb) Sonderfall: Anonymisierungs-Modell ... 60
4. Weitere Straftaten im Zuge der Verbreitung geschützter Werke ... 60
5. Ausblick ... 61
III. Streaming-Websites am Beispiel kino.to ... 61
1. Technische Grundlagen ... 62
a) Möglichkeiten der dauerhaften Speicherung ... 63
b) Speicherorte ... 64
2. Urheberrechtsverstöße durch die Stream-Hoster ... 64
3. Urheberrechtsverstöße durch die Plattformbetreiber ... 65
a) Urheberrechtsverletzungen nach §§ 106, 108a UrhG ... 65
aa) Embedded Links ... 66
(1) Kein Ausschluss einer Verwertungshandlung ... 66
(2) Kriterien zur Abgrenzung von Täterschaft und Teilnahme ... 67
(3) Täterschaftliche Begehung durch „embedded links“ ... 68
(4) Mittäterschaftliche Zurechnung ... 68
bb) Hyperlinks ... 70
b) Gründung einer kriminellen Vereinigung, § 129 StGB ... 71
4. Urheberrechtsverstöße der Nutzer ... 71
a) Vervielfältigung i. S. v. § 16 UrhG ... 72
b) Rechtfertigung gem. § 44a UrhG ... 72
aa) Normzweck ... 73
bb) Grundvoraussetzungen von § 44a UrhG ... 73
cc) Rechtmäßige Nutzung gem. § 44a Nr. 2 UrhG ... 75
(1) Keine Anwendbarkeit des § 44a Nr. 2 UrhG ... 75
(2) Vergleich zum „Stufensystem zur mittelbaren Erfassung des Endverbrauchers“ ... 76
(3) Vermittelnder Ansatz von Busch ... 77
(4) Rechtsprechung des EuGH ... 78
(5) Stellungnahme ... 79
(a) Begriff der offensichtlichen Rechtswidrigkeit ... 80
(aa) Weitreichender Ansatz ... 80
(bb) Restriktiver Ansatz ... 81
(cc) Stellungnahme ... 81
(b) Zwischenergebnis ... 82
dd) Eigenständige Bedeutung ... 82
c) Rechtfertigung gem. § 53 Abs. 1 UrhG ... 83
d) Ergebnis ... 84

IV. Onlinespiele und e-Sports ... 84
1. Grundlagen ... 85
a) Der Begriff „e-Sport“ ... 85
b) Onlinespiele ... 86
c) Multi-Massively-Online-Role-Playing-Games (MMORPG) ... 86
aa) Erstellen eines Spielaccounts ... 87
bb) Spielprinzip ... 87
cc) Echtgeld-Auktionshäuser ... 88
2. Strafrechtliche Würdigung ... 88
a) Anwendbarkeit des deutschen Strafrechts ... 89
b) Ehrverletzungen ... 89
c) Account-Phishing ... 90
aa) Beschaffung der Daten ... 90
(1) Betrug, § 263 StGB ... 90
(a) Fehlende Vermögensverfügung ... 91
(b) Schadensgleiche Vermögensgefährdung ... 92
(c) Stellungnahme ... 92
(2) Fälschung beweiserheblicher Daten, § 269 StGB ... 93
bb) Verwendung der Daten ... 94
d) Entwendung von „Items“ ... 94
aa) Datenveränderung, § 303a StGB ... 95
(1) Unterdrücken ... 95
(2) Verändern ... 96
bb) Betrug, § 263 StGB ... 97
cc) Computerbetrug, § 263a StGB ... 97
(1) Computerspezifische Auslegung ... 97
(2) Betrugsspezifische Auslegung ... 98
(3) Abredewidriges Verhalten durch einen Dritten ... 98
e) Account-Diebstahl ... 99
aa) Account-Hack ... 99
bb) Veräußerung von Accounts ... 100
f) Echtgeld-Auktionshäuser ... 100
aa) Unerlaubtes Glücksspiel, § 284 StGB ... 101
bb) Online-Betrug ... 101
3. Fazit ... 101

**Kapitel 2: Soziale Netzwerke am Beispiel Facebook** ... 102
I. Grundlagen ... 102
1. Einführung ... 103
2. Funktionen ... 104
a) Gruppen- und Mikroblogfunktion ... 105
b) Event-Manager ... 105
c) Pinnwand-Funktion ... 106
d) „Gefällt Mir“-Funktion ... 106
e) „Teilen“-Funktion ... 107
3. Strafrechtlicher Bezug ... 107
II. Ausspähen von Nutzerdaten und Verbreitung von Schadsoftware ... 108
1. Ausspähen von Daten, § 202a StGB ... 109
a) Verbreitung von Schadsoftware via App ... 109
b) Zugriff auf die Nutzermailbox via App ... 109

aa) Disponibilität ... 110
bb) Reichweite des Einverständnisses ... 111
2. Datenveränderung und Computersabotage ... 112
a) Installation von Schadsoftware ... 112
aa) Keine Funktionsbeeinträchtigung ... 113
bb) Informationsgehalt des Gesamtdatenspeichers ... 113
cc) Stellungnahme ... 114
b) Denial of Service-Angriff ... 114
3. Fazit ... 115
III. Ehrverletzungen in sozialen Netzwerken ... 115
1. Beleidigungsdelikte der §§ 185 ff. StGB ... 116
2. Erscheinungsformen und besonderer Unrechtsgehalt ... 117
a) Cybermobbing ... 117
b) Erhöhter Unrechtsgehalt ... 118
3. Vorliegen einer Ehrverletzung ... 119
4. Ehrverletzung mittels „Gefällt Mir"-Funktion ... 120
a) Einordnung in Täterschaft und Teilnahme ... 121
b) Voraussetzungen der Beihilfe ... 122
aa) Kausale Hilfeleistung ... 122
bb) Zeitpunkt der Beihilfe ... 123
(1) Zulässigkeit der sukzessiven Beihilfe ... 123
(a) Rechtsprechung des BGH ... 124
(b) Entgegenstehende Meinungen in der Literatur ... 124
(2) Bedeutung für die vorliegende Problematik ... 125
(a) Fortbestehender Angriff auf das Rechtsgut ... 125
(b) Auseinanderfallen von Vollendung und Beendigung ... 126
(3) Annahme der sukzessiven Beihilfe ... 127
cc) Neutrale Beihilfe ... 128
5. „Teilen" von Inhalten ... 128
6. Fehlendes Unrechtsbewusstsein ... 129
7. Fazit ... 130
IV. Verbreitung illegaler Inhalte ... 130
1. Extremismus in sozialen Netzen ... 131
2. Verbreiten von Propagandamitteln verfassungswidriger Organisationen ... 132
a) Subtile Propaganda ... 132
b) Öffentliches Zugänglichmachen ... 133
aa) Publikation innerhalb einer Nutzergruppe ... 134
(1) Individuell-überschaubarer Personenkreis ... 134
(a) Bisherige Kriterien ... 134
(b) Übertragung auf geschlossene Nutzergruppen ... 135
(2) Persönliche Verbundenheit ... 136
bb) Publikation innerhalb eines Profils ... 137
(1) Öffentliche Profile ... 137
(2) Eingeschränkte Sichtbarkeit ... 138
cc) Ergebnis ... 139
3. Anleitung zur Begehung einer schweren staatsgefährdenden Gewalttat ... 139
4. Weitere Straftaten ... 140
V. Identitätsdiebstahl bzw. Identitätsmissbrauch ... 140
1. Begriffliches ... 141
2. Ausspähen von Daten, § 202a StGB ... 142

3. Beleidigungsdelikte, §§ 185 ff. StGB ... 143
a) Ehrverletzung durch Profilerstellung ... 143
aa) Inhalt des Ehrbegriffs ... 143
bb) Erstellung eines Fake-Profils ... 144
cc) Fake-Profile mit beleidigenden Inhalten ... 145
b) Handeln unter falscher Identität ... 146
4. Datenschutzstrafrecht ... 146
a) Anwendbarkeit des BDSG ... 147
aa) Negative Formulierung des Gesetzes ... 147
bb) Vergleich zu bisherigen persönlichen Tätigkeiten ... 147
cc) Kriminelle Zwecksetzung ... 148
dd) Vergleich mit der Datenschutzkonvention ... 148
b) Personenbezogene Daten ... 149
c) Allgemein zugängliche Daten ... 149
5. Weiteres Nebenstrafrecht ... 150
VI. Cyberstalking ... 151
1. Begriffliches ... 151
2. Erscheinungsformen ... 152
3. Nachstellung, § 238 StGB ... 152
a) Tathandlungen ... 153
b) Taterfolg: Schwerwiegende Beeinträchtigung ... 154
aa) Beeinträchtigung der Lebensgestaltung ... 154
bb) Schwerwiegend ... 156
c) Unbefugtheit ... 156
4. Fazit ... 157
VII. Verwertung urheberrechtlich geschützter Inhalte ... 157
1. Grundlegendes ... 158
2. Verwertung urheberrechtlich geschützter Inhalte ... 158
a) Verwertungshandlung ... 158
aa) Verwendung von Hyperlinks ... 159
bb) Verwirklichung durch Unterlassen ... 159
b) Schrankenregelungen ... 160
3. Fazit ... 160
VIII. Strafbare Handlungen des Portalbetreibers ... 161
1. Verwendung des Friend-Finders ... 161
a) Ausspähen von Daten, § 202a StGB ... 162
aa) Tatbestandsausschließendes Einverständnis ... 162
bb) Keine nachträgliche Berechtigung ... 163
b) Strafbarkeit nach dem BDSG ... 163
2. Datenerfassung durch Social-Plugins ... 164
3. Unterstützungshandlungen ... 164
4. Fazit ... 165
IX. Ausblick: Möglichkeiten der Strafverfolgung ... 166

**Kapitel 3: Cloud Computing** ... 167
I. Grundlagen des Cloud Computing ... 167
1. Begriffliches ... 167
2. Definition ... 168
a) Grundprinzip: Virtualisierung ... 169

b) Cloud-Modelle ... 170
aa) Public Clouds ... 170
bb) Private Clouds ... 170
cc) Mischformen ... 171
c) Cloud Services ... 171
d) Einbeziehung von Dritt-Services ... 173
e) Zusammenfassung ... 173
3. Vor- und Nachteile von Cloud Computing ... 174
4. Risiken beim Einsatz von Cloud Computing ... 175
a) Bekannte Cloud-Sicherheitsprobleme ... 175
b) Cloud-spezifische Sicherheitsprobleme ... 176
II. Rechtliche Aspekte des Cloud Computing ... 176
1. Zivilrecht ... 177
2. Öffentliches Recht ... 178
3. Datenschutzrecht ... 179
a) Anwendbarkeit des Datenschutzrechts ... 180
aa) Kein Anwendungsvorrang des TMG oder TKG ... 180
bb) Anwendungsbereich des BDSG ... 180
b) Verlagerung von personenbezogenen Daten in die Cloud ... 181
III. Cloud Computing als strafrechtliches Problem ... 182
1. Anwendbarkeit des deutschen Strafrechts ... 183
a) Strafbare Handlungen aus Deutschland ... 183
b) Straftaten im Zusammenhang mit inländischen Clouds ... 184
aa) Erfolgsdelikte ... 184
bb) Abstrakte Gefährdungsdelikte ... 185
(1) Ausdehnung des Handlungsorts ... 185
(2) Vergleich mit Erfolgsdelikten ... 186
(3) Anknüpfungspunkt: Physische Präsenz ... 187
(4) Lex Loci ... 187
(5) Stellungnahme ... 188
c) Straftaten aus dem Ausland auf bzw. mittels grenzüberschreitender Clouds ... 188
aa) Erfolgsdelikte ... 189
(1) Die Cloud als Erfolgsort ... 189
(2) Datenschutzrechtlicher Ansatz ... 189
(3) Stellungnahme ... 190
(4) Einsatz deutscher Cloud Services gegen ausländische Rechtsgüter ... 190
(a) Besonderer territorialer Bezug ... 191
(b) Subsumtion unter den Erfolgsort ... 191
(c) Ausblick: Erweiterte Auslegung des Erfolgsortes ... 192
bb) Abstrakte Gefährdungsdelikte ... 193
d) Fazit ... 193
2. Einschlägige Strafvorschriften ... 194
a) Ausspähen von Daten, § 202a StGB ... 194
aa) Differenzierung hinsichtlich der Dateninhaberschaft ... 195
bb) Tathandlung: Verschaffen ... 195
cc) Nicht für den Täter bestimmt ... 196
(1) Sealed Clouds ... 196
(2) Sonderfall: Einbindung von Drittanbietern ... 196

dd) Besondere Sicherung ... 197
ee) Fazit ... 198
b) Weitere Datendelikte ... 198
c) Verletzung von Privatgeheimnissen, § 203 StGB ... 199
aa) Strafbarkeit der Mitarbeiter des Unternehmens ... 199
(1) Nutzung von Cloud Computing innerhalb der Landesgrenzen ... 199
(a) Differenzierung nach Art der Cloud ... 202
(b) Tatbestandsausschluss: Sozialadäquanz ... 203
(c) Tatbestandsausschluss über eine Gehilfenstellung, § 203 Abs. 3 S. 2 StGB ... 203
(aa) Bezugspunkte: Direktionsrecht und Funktionseinheit ... 204
(bb) Erweiterung auf Externe bei organisatorischer Einbindung ... 205
(cc) Bezugspunkt: hinreichende Weisungs- und Kontrollrechte ... 205
(dd) Stellungnahme ... 207
(d) Straflosigkeit des Offenbarens im Zuge einer Einwilligung ... 209
(aa) Tatbestandsausschließendes Einverständnis ... 210
(bb) Mutmaßliches Einverständnis ... 210
(2) Nutzung von Cloud Computing durch ausländische Funktionsstellen ... 211
(3) Nutzung eines Cloud-Angebots unter Einbindung von Drittanbietern ... 212
(a) Begriffsauslegung des „Gehilfen“ i. S. v. § 203 Abs. 3 S. 2 StGB ... 212
(aa) Wortlaut und allgemeiner Sprachgebrauch ... 213
(bb) Historie ... 213
(cc) Gesetzliche Systematik ... 214
(dd) Innertatbestandliche Systematik ... 215
(ee) Vergleich mit dem Zivil- und Prozessrecht ... 216
(ff) Zwischenergebnis ... 217
(b) Ergebnis ... 217
(4) Sonderfall: Managed Private Cloud ... 217
(5) Bedeutung für die Praxis des Cloud Computing ... 218
bb) Strafbarkeit der Mitarbeiter des Cloud-Service-Providers ... 218
cc) Fazit ... 219
d) Urheberstrafrecht ... 220
IV. Gesamtbetrachtung ... 220

**Teil 3: Die Verantwortlichkeit von Internetdiensteanbietern** ... 223

**Kapitel 1: Die Verantwortlichkeitsregelungen des TMG** ... 223
I. Einleitung ... 223
II. Grundlagen der Providerhaftung ... 223
1. Zentrale Grundbegriffe ... 224
a) Information ... 224
b) Diensteanbieter ... 224
c) Verantwortlichkeit ... 225
2. Funktionale Einteilung nach dem TMG ... 227

III. Content-Providing ..... 227
1. Grundlagen ..... 227
2. Originäre und zu eigen gemachte Inhalte ..... 227
a) Weblogs ..... 228
b) Pinnwand-Funktion in sozialen Netzwerken ..... 229
c) Streaming-Angebote ..... 229
IV. Host-Providing ..... 230
1. Personeller Anwendungsbereich ..... 230
2. Fremde Informationen ..... 230
a) User-Generated-Content-Plattformen ..... 230
b) Ausnahme: Einräumung von Nutzungsrechten ..... 231
c) Sharehosting ..... 232
d) Cloud Computing ..... 234
3. Ausschluss der Verantwortlichkeit ..... 235
V. Access-Providing ..... 235

**Kapitel 2: Verantwortlichkeit von WLAN-, Hyperlink- und Suchmaschinen-Betreiber** ..... 236
I. Verantwortlichkeit für offene WLAN-Spots ..... 236
II. Hyperlinks ..... 237
1. Keine Anwendbarkeit der Haftungsprivilegien ..... 238
a) Interne Links ..... 238
b) Externe Links ..... 239
2. Embedded Objects ..... 239
3. Haftungsvermeidung ..... 240
III. Verantwortlichkeit für Suchmaschinen ..... 240
1. Grundlegendes ..... 241
2. Technische Darstellung ..... 242
a) Snippets ..... 242
b) Thumbnails ..... 243
c) Google AdWords ..... 243
d) Auto-Complete ..... 244
3. Einstufung in die Providertypologie ..... 244
a) Ansicht des BGH ..... 245
b) Stellungnahme ..... 246

**Zusammenfassung** ..... 247

**Literaturverzeichnis** ..... 251

**Verzeichnis der zitierten Internetseiten** ..... 294

**Über den Verfasser** ..... 295