

Inhaltsverzeichnis

Abkürzungsverzeichnis	19
Erstes Kapitel:	
Einleitung	23
A. Rahmen der Forschungstätigkeit	26
B. Stand der Forschung	28
C. Methodische Vorgehensweise	30
Zweites Kapitel:	
Cloud Computing – Das neue Angebot zum Speichern	35
A. Erscheinungsformen des Cloud Computings	35
I. Definitionsansätze	38
1. Virtualisierung	40
2. Skalierbarkeit	42
3. Zugriff per Internet	42
II. Delivery Models	43
III. Deployment Models	46
IV. Cloud-Akteure	48
B. Vorteile und Nachteile für KMU und Behörden	49
I. Kleine und mittlere Unternehmen	49
II. Öffentlicher Sektor	52
III. Entwicklungsperspektiven für und durch Cloud Computing	54
IV. Drohende Risiken	56
C. Speichern in der Cloud – der technische Untersuchungsgegenstand	60
Drittes Kapitel:	
Rechtliche Einordnung des Cloud Computings	63
A. Straf-(prozess-)rechtliche Probleme beim Cloud Computing	63
B. Zivilrechtliche Einordnung des Cloud Computings	65
I. Anwendung des Schuldrechts auf IT-Services	65
1. Kaufvertrag	67

2. Dienstvertrag	67
3. Werkvertrag	69
4. Verwahrungsvertrag	70
5. Mietvertrag	71
II. Anwendbarkeit des Mietrechts auf Cloud-Verträge	73
1. Hauptleistungspflichten bei Cloud-Miete	74
2. Zahlung der Cloud-Miete	76
3. Mängelgewährleistungsrecht und Haftung	77
4. Beendigung und Rückabwicklung der Cloud-Miete	80
III. Mietvertragliche Einordnung von Cloud Computing	82
C. Medienrechtliche Einordnung der Cloud Computing-Daten	83
I. Anwendbarkeit des Telekommunikationsgesetzes auf Cloud Computing	85
II. Anwendbarkeit des Telemediengesetzes auf Cloud Computing	88
III. Daten beim Cloud Computing	89
1. Bestandsdaten nach TMG	90
2. Nutzungsdaten nach TMG	91
3. Inhaltsdaten	93
IV. Cloud-Daten ohne Recht auf Kenntnisnahme	95
D. Datenspeichermiete – der rechtliche Untersuchungsgegenstand	96
Viertes Kapitel:	
Strafrechtliche Risiken beim Cloud Computing	99
A. Strafrechtlich relevantes Verhalten und Cloud Computing	99
B. Anwendung der Strafgesetze auf Cloud Computing	102
I. Verletzung des Briefgeheimnisses gemäß § 202 StGB	104
1. Tatobjekt	104
2. Kein Strafbarkeitsrisiko wegen Verletzung des Briefgeheimnisses bei Nutzung von Cloud Computing	105
II. Ausspähen von Daten gemäß § 202a StGB	105
1. Tatobjekt	105
a) Daten	106
b) Nicht für den Täter bestimmt	106
c) Gegen unberechtigten Zugriff besonders gesichert	108
2. Tathandlung	115
a) Zugangsverschaffung	115
b) Überwinden der Schutzvorrichtung	116
3. Dritte und der Cloud-Anbieter handeln tatbestandsmäßig	117
4. Merkmal »unbefugt«	118
5. Sonstige Voraussetzungen	119

6. Strafbarkeitsrisiko für Cloud-Anbieter für Ausspähen von Daten	120
III. Abfangen von Daten gemäß § 202b StGB	121
1. Datenup- und -download	122
2. Cloud-Sharing	123
3. Subsidiarität wegen Abfangen von Daten	124
IV. Vorbereiten des Ausspähen und Abfangens von Daten gemäß § 202c StGB	124
1. Zugang des Cloud-Anbieters zu den Daten	125
2. Kein Strafbarkeitsrisiko des Cloud-Anbieters wegen Vorbereitungsstaten	126
V. Verletzung von Privatgeheimnissen gemäß § 203 StGB	128
1. Anvertrautes Geheimnis	130
2. Offenbarung durch Nutzung der Cloud	131
a) Tathandlung	132
b) Taterfolg	134
c) Zwischenergebnis	136
3. Gehilfe und Auftragsdatenverarbeitung	136
a) Direktionsrecht und dienstorganisatorische Einbindung?	137
b) Weisungsbindung	139
c) Verbindung der Gehilfenstellung zur Auftragsdatenverarbeitung	140
4. Einwilligung als Befugnis zur Offenbarung?	142
5. Schutz bei weiteren Akteuren	144
a) Schutz des Dritten nach Bundesdatenschutzgesetz	144
b) Schutzpflicht zugunsten des Dritten	145
c) Drittgeheimnisse	146
d) Offenbarungsketten	147
6. Strafbarkeitsrisiko für Berufsgeheimnisträger bei Cloud-Nutzung	148
VI. Verwertung fremder Geheimnisse gemäß § 204 StGB	149
1. Cloud-Nutzer als Täter	150
2. Cloud-Anbieter als Täter	151
3. Cloud-Nutzer als Teilnehmer	151
4. Kein Strafbarkeitsrisiko wegen Verwertung fremder Geheimnisse	153
VII. Verletzung des Post- oder Fernmeldegeheimnisses gemäß § 206 StGB	154
1. Strafbarkeit des Cloud-Anbieters	156
a) Cloud-Anbieter als Täter	157

aa) Dem Fernmeldegeheimnis unterliegende Tatsachen	157
bb) Unternehmen zum geschäftsmäßigen Erbringen von Telekommunikationsdiensten	162
b) Zwischenergebnis	164
2. Strafbarkeit des Cloud-Nutzers	165
a) Der Telekommunikationsanbieter als Täter	165
b) Tathandlung	168
c) Merkmal »unbefugt«	172
d) Zwischenergebnis	173
3. Strafbarkeitsrisiko wegen Verletzung des Fernmeldegeheimnisses	174
VIII. Datenveränderung gemäß § 303a StGB	175
1. Daten in der Cloud als Tatobjekt	175
a) Fremde Daten	177
b) Daten aus SaaS	178
c) Redundanzkopie	181
2. Tathandlung im Rahmen des Cloud Computings	182
a) Löschen von Daten	183
b) Unterdrücken von Daten	184
c) Unbrauchbarmachen von Daten	185
d) Verändern von Daten	185
e) Vermeidung doppelter Speicherung durch Cloud-Anbieter	187
3. Entgegenstehender Wille des Cloud-Nutzers	188
a) Zustimmung als tatbestandsausschließendes Einverständnis	189
b) Rechtswidrigkeit	191
aa) Technische Notwendigkeit	191
bb) Vertragliche Bedingungen	192
4. Strafbarkeitsrisiko bei ungerechtfertigter Datenveränderung	194
IX. Computersabotage gemäß § 303b StGB	196
1. Täter beim Cloud Computing	197
2. Cloud als Tatobjekt	197
3. Erhebliche Störung der Cloud als Taterfolg	200
4. Tathandlung beim Cloud Computing	201
a) Grundtatbestand der Störung einer Datenverarbeitung	201
b) Erfolgsqualifikation bei besonderer Schädigung	204
c) Besonders schwere Fälle	204
5. Der subjektive Tatbestand beim Cloud Computing	205

6. Strafbarkeitsrisiko der Cloud-Akteure wegen Computersabotage	206
X. Zerstörung wichtiger Arbeitsmittel gemäß § 305a StGB	207
XI. Verletzung des Dienstgeheimnisses und einer besonderen Geheimhaltungspflicht gemäß § 353b StGB	208
1. Täter	209
2. Anvertrautes Geheimnis als Tatobjekt	210
3. Offenbaren als Tathandlung	211
4. Gefährdung wichtiger öffentlicher Interessen als Taterfolg	213
5. Zurechnung der Tathandlung zum potentiellen Täterkreis	215
6. Merkmal »unbefugt«	216
7. Strafbarkeitsrisiko der Amtsträger wegen Verletzung des Dienstgeheimnisses und einer besonderen Geheimhaltungspflicht	217
XII. Verbotene Mitteilungen über Gerichtsverhandlungen gemäß § 353d StGB	217
1. Mitteilungen durch die Presse	218
2. Unbefugte Offenbarung im Fall von § 174 Abs. 3 GVG	220
3. Öffentliches Mitteilen amtlicher Schriftstücke	221
4. Strafbarkeitsrisiko des Cloud-Nutzers wegen verbotener Mitteilungen über Gerichtsverhandlungen gemäß § 353d Nr. 2 StGB	222
XIII. Verletzung des Steuergeheimnisses gemäß § 355 StGB	223
XIV. Landesverrat und Verrat oder Preisgabe von Staatsgeheimnissen	225
1. Landesverrat gemäß § 94 StGB	225
2. Offenbaren von Staatsgeheimnissen gemäß § 95 StGB	227
3. Landesverräterische Ausspähung und Auskundschaften von Staatsgeheimnissen gemäß § 96 StGB	228
4. Strafbarkeitsrisiko beim Cloud Computing bei Staatsgeheimnissen	229
XV. Relevante Strafnormen außerhalb des Strafgesetzbuchs	230
1. Datenschutzrechtliche Strafbarkeit gemäß §§ 43 und 44 BDSG	230
a) Das Bundesdatenschutzgesetz und seine Strafvorschriften	231
b) Die unbefugte Erhebung oder Verarbeitung nach Nr. 1	233
c) Unbefugtes Abrufen oder Verschaffen nach Nr. 3	235
d) Zweckentfremdung von übermittelten Daten nach Nr. 5	236

e) Verletzung von Informationspflichten bei Datenschutzverstößen nach Nr. 7	237
f) Sonstige Handlungsvarianten ohne Cloud-Relevanz	238
g) Besondere Absichten	239
h) Strafbarkeitsrisiken nach dem Bundesdatenschutzgesetz	240
i) Exkurs: Bußgeldvorschriften der EU-DS-GVO	241
2. Verrat von Geschäfts- und Betriebsgeheimnissen gemäß § 17 UWG	241
a) Geheimnisverrat nach Absatz 1	244
b) Betriebsspionage und Geheimnishehlerei nach Absatz 2	246
aa) Angriffe von außen	246
bb) Angriffe von innen	249
c) Strafbarkeitsrisiken wegen Betriebs- und Geschäftsgeheimnissen	251
C. Strafbarkeitsrisiken der Cloud-Akteure	252
I. Strafbarkeit des Cloud-Nutzers	253
II. Strafbarkeit des Cloud-Anbieters	255
III. Strafbarkeit Dritter	257
IV. Keine besonderen Strafbarkeitsrisiken trotz Cloud Computing	258
D. Speichern in der Cloud – ohne strafrechtliche Risiken	259
I. Strafbarkeitsrisiko des Cloud-Nutzers durch unbefugte Kenntnisverschaffung	260
1. Einholung einer Zustimmung	261
2. Auslegung des Strafrechts mithilfe anderer Gesetze	262
a) Datenschutzrechtliche Auslegung des Strafrechts	262
b) Telekommunikationsrechtliche Auslegung des Strafrechts	266
3. Technische Gestaltung der Cloud-Nutzung	267
a) Verschlüsselung der Daten in der Cloud	268
b) Langzeitproblem bei Verschlüsselung	269
c) Hybrid Cloud-Lösung für Geheimnispflichtige	270
d) Trotz Technik Restrisiko einer Strafbarkeit durch Cloud-Nutzung	271
4. Änderung oder Klarstellung der gesetzlichen Lage	271
II. Strafbarkeitsrisiko des Cloud-Nutzers wegen schädigender Zugriffe auf die Cloud	274
III. Strafbarkeitsrisiko des Cloud-Nutzers aus dem Datenschutzrecht	275

IV. Strafbarkeitsrisiko des Cloud-Anbieters wegen unerlaubten Zugriffen auf die Cloud-Daten	276
V. Strafbarkeitsrisiko des Cloud-Anbieters wegen Zugriffsverweigerung	278
VI. Strafbarkeitsrisiken Dritter	279
VII. Straffloses Cloud Computing	279
Fünftes Kapitel:	
Strafprozessuale Ermittlungen beim Cloud Computing	281
A. Strafprozessuale Ermittlungen bei Daten	283
I. Grundlagen des Strafprozesses	283
1. Ermittlungsgrundsatz	284
2. Gesetzesvorbehalt, Analogieverbot und Bestimmtheitsgebot	285
3. Zuständigkeit der Ermittlungsbehörden	287
4. Beweismittel im Strafprozess	290
5. Beweismittelkette bei elektronischen Beweismitteln	292
6. Beweismittel aus der Cloud	295
II. Verfassungsrechtliche Vorgaben im Strafprozess bei Cloud Computing	297
1. Computergrundrecht	298
2. Recht auf informationelle Selbstbestimmung	301
a) Cloud-Nutzer als Grundrechtsträger	301
b) Dritte als Grundrechtsträger	302
aa) Cloud-Anbieter als Grundrechtsträger	302
bb) Andere Grundrechtsträger	302
c) Zwischenergebnis	304
3. Post- und Briefgeheimnis	305
4. Fernmeldegeheimnis	306
a) Übertragung in die Cloud	307
b) Speicherung in der Cloud	307
c) Cloud-Nutzung zur Kommunikation	311
d) Zwischenergebnis	313
5. Berufsfreiheit	314
6. Unverletzlichkeit der Wohnung	316
7. Eigentum	317
III. Der Cloud-Nutzer in der Strafprozessordnung	320
1. Cloud-Nutzer als Betroffener von Ermittlungsmaßnahmen	320
2. Datenkategorien in der Cloud	323
a) Daten des Cloud-Nutzers	323
b) Daten des Cloud-Anbieters	324

B. Anwendung von Ermittlungsbefugnissen auf Cloud Computing	325
I. Überblick über strafprozessuale Ermittlungsbefugnisse	329
II. Durchsuchung gemäß §§ 102 ff. StPO	331
1. Anordnung der Durchsuchung	331
2. Durchsuchung am Ort des Cloud-Nutzers	333
a) Sache	334
b) Ihm gehörende Sache	336
aa) Ihm gehörend – der Datenträger	336
bb) Ihm gehörend – der fiktive Speicherplatz	338
c) Durchsuchung gemäß § 102 StPO beim Cloud-Nutzer	342
d) Durchsuchung auch im Ausland gemäß § 102 StPO	342
3. Durchsuchung am Ort des Cloud-Anbieters	344
a) Bestimmte Gegenstände zur Beschlagnahme	345
b) Verdacht des Auffindens	345
c) Ausnahme gemäß § 103 Abs. 2 StPO	346
d) Suche	347
4. Zwischenergebnis zur Durchsuchung	350
5. Durchsicht gemäß § 110 StPO	351
a) Durchsicht von Papieren	351
b) Durchsicht von externen Speichermedien	353
III. Beschlagnahme gemäß §§ 94 ff. StPO	359
1. Anordnung der Beschlagnahme	359
2. Beschlagnahmefreiheit	362
3. Beschlagnahme von Cloud-Daten	365
4. Anschließende Herausgabe	367
5. Ort der Beschlagnahme	369
6. Zwischenergebnis zur Beschlagnahme	373
IV. Telekommunikationsüberwachung gemäß §§ 100a ff. StPO	375
1. Voraussetzungen der Telekommunikationsüberwachung	376
2. Kommunikationsüberwachung bei Cloud-Nutzung	379
3. Keine Telekommunikationsüberwachung beim Cloud Computing	382
V. Bestandsdatenauskunft gemäß § 100j StPO	383
1. Erfordernis einer neuen Vorschrift zur Bestandsdatenauskunft	383
a) Doppeltürmodell	384
b) Der neue § 100j StPO	386
2. Ermittlungen gemäß § 100j StPO	387
a) Telekommunikationsanbieter	388
b) Bestandsdaten	388
c) Zugangsdaten	390

d) Gesetzliche Voraussetzungen für die Nutzung der Zugangsdaten	392
e) Dynamische IP	393
f) Übermittlungspflicht im Sinne von § 113 TKG	393
g) Benachrichtigung nur durch die Ermittlungsbehörden	394
h) Ermittlungsnotstand	395
i) Formelle Voraussetzungen	396
3. Bestandsdatenauskunft und Cloud Computing	397
a) Zugangsdaten zur Cloud als Bestandsdaten des TK-Anbieters?	397
b) Der Cloud-Anbieter als Telekommunikationsanbieter?	400
4. Zwischenergebnis zur neuen Bestandsdatenauskunft	401
VI. Verkehrsdatenauskunft gemäß § 100g StPO	402
VII. Bestandsdatenauskunft nach der Ermittlungsgeneralklausel	404
1. Passwort als Bestandsdatum	405
2. Nutzung der Bestandsdaten	406
C. Strafprozessuale Zugriffe bei den Cloud-Akteuren	408
I. Verschiedene Möglichkeiten zum Zugriff auf die Cloud	409
II. Ermittlungen beim Cloud-Nutzer vor Ort	410
1. Daten in der Desktop-Cloud	410
2. Daten in der reinen Cloud	413
III. Ermittlungen beim Cloud-Anbieter vor Ort	418
1. Kopie der Daten durch den Cloud-Anbieter	420
2. Richtervorbehalt für die Kopie	421
3. Anschließende Ermittlungen innerhalb der Daten des Cloud-Nutzers	423
4. Auffinden von Beweismitteln	426
IV. Ermittlungen übers Internet	427
1. Heimliche Ermittlungen bei gespeicherten Daten	427
2. Heimliche Ermittlungen bei der Datenübertragung	429
3. Offene Ermittlungen mithilfe des Internets	431
V. Ermittlungen im Ausland	433
D. Speichern in der Cloud – Strafprozessuale Zugriffsmöglichkeiten	438
 Sechstes Kapitel:	
Straf-(prozess-)rechtsverträgliches Cloud Computing	445
 A. Rechtliche Vorgaben für Cloud Computing	447
B. Rechtliche Gestaltungsempfehlungen	451
I. Gestaltungsempfehlungen für den Cloud-Nutzer	451
1. Vermeidung von Strafbarkeitsrisiken	451

a) Cloud-Nutzer aus bestimmten Geschäftsfeldern	452
b) Cloud-Nutzer, die das Datenschutzrecht beachten müssen	453
c) Sicherheitsaspekte des Cloud-Nutzers	453
2. Schutz hinsichtlich staatlicher Zugriffe	454
a) Heimliche Vorabmaßnahmen	454
b) Offene Zugriffe auf Daten	455
c) Verschlüsselung gegen ungerechtfertigte Zugriffe	456
II. Gestaltungsempfehlungen für den Cloud-Anbieter	457
1. Vermeidung von Strafbarkeitsrisiken	457
a) Cloud-Anbieter vermeidet Kenntnisnahme der Daten	457
b) Cloud-Anbieter verhindert Schäden beim Cloud-Nutzer	458
2. Schutz hinsichtlich staatlicher Zugriffe	459
a) Bestandsdatenauskunft	459
b) Kopieren von Daten des Cloud-Nutzers	459
c) Vermeidung staatlicher Kooperationspflichten	460
C. Mehrwert für KMU und öffentliche Verwaltung	461
I. KMU als Cloud-Nutzer und Cloud-Anbieter	461
1. Know-how für IT-Beschaffung aus der Cloud	461
2. Der Cloud-Anbieter als Know-how-Vermittler für den Cloud-Nutzer	462
3. Cloud Computing und Compliance	464
II. Sonderstellung des öffentlichen Sektors	466
1. Nutzung von IT aus der Cloud durch öffentliche Verwaltung	466
2. Einheitliche Anwendung von Gesetzen im Cloud Computing	468
D. Speichern in der Cloud – ein straf-(prozess-)rechtlicher Ausblick	469
Literaturverzeichnis	473