

Inhaltsverzeichnis

Abkürzungsverzeichnis	21
§ 1 Einleitung	25
A. Die Cloud – ein junges Phänomen	25
B. Untersuchungsgegenstand	26
C. Gang der Untersuchung	28
§ 2 Grundlagen	30
A. Begriffliche Grundlagen	30
I. Cloud, Cloud-Computing und Cloud-Storage	30
1. Begriff und Definition	31
2. Von der Public Cloud über die Private Cloud zur Internal Cloud	33
3. Servicemodelle – IaaS, PaaS, SaaS	34
II. Akteure	35
III. Datenarten	36
1. Inhaltsdaten	36
2. Verkehrsdaten	36
3. Bestandsdaten	37
B. Technische Grundlagen und konkreter Untersuchungsgegenstand	37
I. Cloud-Computing und Cloud-Storage	37
II. Datenübertragung im Internet	40
1. Das Internet	40
2. Digitalisierung	41
3. Datenübertragung	41
III. Technische Umsetzung einer Überwachung	44
1. Live-Sicherung und Post-Mortem-Sicherung	44
2. Überwachung „an der Quelle“	45
a) Infiltration des Nutzersystems mit einer Überwachungssoftware	45
b) Van-Eck-Phreaking und Hardware-Keylogger	47

3. Überwachung des Übertragungswegs	48
a) Inanspruchnahme des Telekommunikationsdiensteanbieters	48
b) Man-in-the-Middle-Angriff (MitM-Angriff)	48
4. Überwachung der Cloud	49
IV. Die heimliche Überwachung von Cloud-Storage zum Zwecke der Strafverfolgung als Untersuchungsgegenstand	51
C. Die Vorteile der heimlichen Überwachung gegenüber anderen Ermittlungsmaßnahmen	52
I. Auslandsbezug	53
1. Völkerrechtliches Souveränitätsprinzip	53
2. Lange Verfahrensdauer	55
II. Schnelligkeit der Datenübertragung	55
III. Ungewisser Speicherort	57
IV. Vorteile der heimlichen Überwachung	58
§ 3 Regelungsbedürftigkeit der heimlichen Überwachung von Cloud-Storage	60
A. Verfassungsrechtliche Parameter	60
I. Der Vorbehalt des Gesetzes	60
II. Zum Eingriffsbegriff	61
1. Klassischer und moderner Eingriffsbegriff	61
2. Mittelbare Grundrechtseingriffe	62
III. Erörterungsbedürftige Grundrechte	63
IV. Zwischenergebnis	64
B. Der Schutz von Cloud-Storage durch das Grundrecht auf Unverletzlichkeit der Wohnung – Art. 13 GG	64
I. Schutzbereich	64
II. Der Schutz von Cloud-Storage durch das Grundrecht auf Unverletzlichkeit der Wohnung	65
III. Ergebnis	67
C. Der Schutz von Cloud-Storage durch das Telekommunikationsgeheimnis – Art. 10 Abs. 1 Var. 3 GG	67
I. Sachlicher Schutzbereich	68
1. Der Konsens: Grundsätzliches zum Telekommunikationsgeheimnis	68

2. Telekommunikation im Sinne von Art. 10 Abs. 1 Var. 3 GG	70
a) Individuelle Kommunikation	71
aa) Information	72
bb) Übermittlung und „laufende“ Telekommunikation	72
cc) Empfänger	76
(1) Die Rechtsprechung des BVerfG	76
(a) Das Urteil vom 27.07.2005 – 1 BvR 668/04	77
(b) Der Beschluss vom 22.08.2006 – 2 BvR 1345/03 (IMSI-Catcher-Entscheidung)	77
(c) Der Beschluss vom 16.06.2009 – 2 BvR 902/06 (IMAP-Entscheidung) und das Urteil vom 20.04.2016 – 1 BvR 966/09 – 1 BvR 1140/09 (BKAG-Entscheidung)	80
(d) Der Beschluss vom 06.07.2016 – 2 BvR 1454/13 (Entscheidung zur Überwachung des „Surfverhaltens“ im Internet)	83
(e) Zwischenergebnis	87
(2) Strömungen in der Literatur	87
(a) Formale Strömung	87
(b) Unipersonale Strömung	88
(c) Multipersonale Strömung	89
(3) Stellungnahme	91
(4) Zwischenergebnis	98
dd) Individualität des Empfängers	98
(1) Die Rechtsprechung des BVerfG	99
(2) Strömungen in der Literatur	100
(a) Individualisierung durch Schaffung von Zugangshindernissen	100
(b) Individualisierung aufgrund fehlender staatlicher Zugriffsautorisierung	101
(c) Individualisierung bei Bestehen einer einzelvertraglichen Vertragsbeziehung	102
(3) Stellungnahme	102
(4) Zwischenergebnis	105

ee)	Kommunikationswille	106
(1)	Die Rechtsprechung des BVerfG	106
(a)	Der Beschluss vom 22.08.2006 – 2 BvR 1345/03 (IMSI-Catcher-Entscheidung)	106
(b)	Der Beschluss vom 06.07.2016 – 2 BvR 1454/13 (Entscheidung zur Überwachung des „Surfverhaltens“ im Internet)	108
(c)	Zwischenergebnis	109
(2)	Strömungen in der Literatur	109
(a)	Formale Strömung	109
(b)	Funktionale Strömung	110
(3)	Stellungnahme	112
(a)	Willensbetätigung des Absenders	113
(b)	Willensbetätigung des Empfängers	116
(c)	Erkennbarkeit der Willensbetätigung nach außen	116
(4)	Zwischenergebnis	117
ff)	Zwischenergebnis	118
b)	Technikeinsatz	118
aa)	Technikeinsatz und körperlose Informationen	118
bb)	Einschaltung eines Dritten in den Übertragungsvorgang	119
(1)	Die Rechtsprechung des BVerfG	119
(2)	Stimmen in der Literatur	120
(3)	Stellungnahme	121
(4)	Zwischenergebnis	122
cc)	Abhängigkeit von der Verwendung eines Telekommunikationsmediums/ Wille hinsichtlich der Verwendung eines Telekommunikationsmediums	122
dd)	Zwischenergebnis	124
3.	Ergebnis	125
II.	Der Schutz von Cloud-Storage durch das Telekommunikationsgeheimnis	125
1.	Cloud-Storage durch eine Einzelperson	126
a)	Die Cloud als Speichermedium	126
b)	Verwendung der Freigabe- und Teilen-Funktion	128

c) Sonderfall: Van-Eck-Phreaking und der Einsatz von Hardware-Keyloggern	129
d) Zwischenergebnis	129
2. Cloud-Storage durch mehrere Personen (Public Cloud)	130
a) Cloud-Storage durch mehrere Personen ohne rechtliche Organisationsform	130
b) Cloud-Storage durch eine juristische Person im Sinne von Art. 19 Abs. 3 GG	131
c) Zwischenergebnis	132
3. Sonderfall: Internal Cloud	132
4. Ergebnis	133
III. Eingriffsqualität der Überwachung von Cloud-Storage	134
1. Zugriff „an der Quelle“	134
2. Zugriff auf dem Übertragungsweg	135
3. Zugriff auf die Cloud	136
4. Ergebnis	136
IV. Beschränkungsmöglichkeiten	137
V. Ergebnis	137
D. Der Schutz von Cloud-Storage durch das Grundrecht auf informationelle Selbstbestimmung – Art. 2 Abs. 1, 1 Abs. 1 GG	138
E. Der Schutz von Cloud-Storage durch das IT-Grundrecht- Art. 1 Abs. 1 i.V.m. Art. 2 Abs. 1 GG	141
I. Ein junges Grundrecht: Zur Funktion des IT-Grundrechts im Grundrechtsgefüge	142
II. Schutzbereich	144
1. Komplexes informationstechnisches System	145
a) Technische Komplexität	146
b) Persönlichkeitsrelevanz	146
c) Höhere Komplexität durch Vernetzung	147
2. Eigennutzung	147
3. Schutzrichtung	151
a) Vertraulichkeit	151
b) Integrität	152
4. Ergebnis	153
III. Der Schutz von Cloud-Storage durch das IT-Grundrecht	154
1. Das Endgerät des Nutzers	154
2. Die Cloud als informationstechnisches System	155

3. Die Cloud und das Endgerät des Nutzers als einheitliches informationstechnisches System	157
4. Ergebnis	160
IV. Eingriffsqualität der Überwachung von Cloud-Storage	161
V. Beschränkungsmöglichkeiten	162
1. Schrankentrias	162
2. Schranken-Schranken	163
a) Allgemeine Schranken-Schranken	163
b) Besonderheiten im Hinblick auf heimliche Eingriffe	164
aa) Anforderungen an heimliche Eingriffe zur Gefahrenabwehr	164
bb) Anforderungen an heimliche Eingriffe zur Strafverfolgung	165
3. Ergebnis	166
VI. Ergebnis	167
F. Grundrechtskonkurrenzen	167
I. Verhältnis von Art. 10 Abs. 1 Var. 3 GG und IT-Grundrecht	167
1. Die Rechtsprechung des BVerfG	168
a) Die Entscheidung des Ersten Senats vom 27.02.2008 – 1 BvR 370/07 – 1 BvR 595/07 (Entscheidung zur Online-Durchsuchung)	168
b) Die Entscheidungen des Zweiten Senats vom 16.07.2009 – 2 BvR 902/06 (sog. IMAP-Entscheidung)	169
c) Die Entscheidung des Ersten Senats vom 20.04.2016 – 1 BvR 966/09 – 1 BvR 1140/09 (BKAG-Entscheidung)	169
d) Die Entscheidung der 3. Kammer des Zweiten Senats vom 06.07.2016 – 2 BvR 1454/13 (Entscheidung zur Überwachung des „Surfverhaltens“ im Internet)	170
2. Bewertung und Ergebnis	170
II. Verhältnis von Art. 10 GG zum Grundrecht auf informationelle Selbstbestimmung	171
III. Verhältnis des IT-Grundrechts zum Grundrecht auf informationelle Selbstbestimmung	172
IV. Ergebnis	174
G. Fazit	174

§ 4 Die heimliche Überwachung von Cloud-Storage bis zum Inkrafttreten der StPO-Reform am 24.08.2017	176
A. § 100a StPO	176
I. Entstehungsgeschichte des § 100a StPO bis zum Inkrafttreten der StPO-Reform	176
II. Cloud-Storage als Telekommunikation i.S.d. § 100a StPO	181
1. Technischer Telekommunikationsbegriff	183
a) Rein technische Auslegung	185
b) Technikorientierte Auslegung	187
c) Cloud-Storage als Telekommunikation im Sinne von § 100a StPO?	188
aa) Rein technische Auslegung	188
(1) Zugriff „an der Quelle“	188
(2) Zugriff auf dem Übertragungsweg	189
(3) Zugriff auf die Cloud	190
(4) Zwischenergebnis	190
bb) Technikorientierte Auslegung	190
(1) Zugriff „an der Quelle“	190
(2) Zugriff auf dem Übertragungsweg	191
(3) Zugriff auf die Cloud	192
(4) Zwischenergebnis	193
cc) Zwischenergebnis	193
2. Materieller Telekommunikationsbegriff	194
a) Grundrechtsanaloge Auslegung	197
b) Genuin strafprozessualer Telekommunikationsbegriff	198
c) Cloud-Storage als Telekommunikation im Sinne von § 100a StPO?	202
aa) Grundrechtsanaloge Auslegung	202
bb) Genuin strafprozessualer Telekommunikationsbegriff	202
(1) Zugriff „an der Quelle“	203
(2) Zugriff auf dem Übertragungsweg	203
(3) Zugriff auf die Cloud	203
(4) Zwischenergebnis	204
cc) Zwischenergebnis	204
3. Zwischenergebnis	204
4. Stellungnahme	206
a) Bewertung der technischen Auslegung	206

b) Bewertung der materiellen Auslegung	210
c) Zwischenergebnis	215
5. Ergebnis	215
III. Die Überwachung und Aufzeichnung von Cloud-Storage	216
1. Überwachung und Aufzeichnung: Inhaltliche Bestimmung	217
a) Vorüberlegung: Der Überwachungsbegriff im System strafprozessualer Eingriffsbefugnisse	217
b) Zeitliche Grenzen	219
c) Bewegung des Überwachungsobjekts	224
d) Zielrichtung	226
e) Mitwirkung des Kommunikationsmittlers	227
f) Drei-Personen-Verhältnis	228
g) Ergebnis	230
2. Die Überwachung von Cloud-Storage	230
a) Überwachung „an der Quelle“ (sog. Quellen-Telekommunikationsüberwachung)	230
aa) Überwachung	231
bb) Umsetzung: Infiltration des Zielsystems	233
(1) Infiltration des Zielsystems gemäß §§ 100a, 100b StPO	233
(2) Infiltration des Zielsystems als Annexbefugnis zu § 100a StPO	234
(a) Zulässigkeit und Voraussetzungen einer Annexbefugnis	235
(b) Infiltration des Zielsystems als Annexbefugnis zu § 100a StPO?	236
cc) Zwischenergebnis	239
b) Überwachung des Übertragungswegs	239
aa) Inanspruchnahme des Internetproviders	240
bb) Man-in-the-Middle-Angriffe unter Einsatz eines Evil-Twin-Hotspots	240
cc) Zwischenergebnis	241
c) Überwachung der Cloud	241
aa) Überwachung	241
bb) Umsetzung: Überwindung von Zugangshindernissen	242
(1) Brute-Force und/oder Wörterbuchattacken	243

(2) Verpflichtung des Cloud-Storage-Anbieters zur Herausgabe der Zugangsdaten	244
(a) Bestandsdatenauskunft nach § 100j Abs. 1 S. 2 StPO	244
(b) Inanspruchnahme des Cloud-Storage- Anbieters gemäß §§ 161, 163 StPO i.V.m. § 14 Abs. 2 TMG	246
cc) Zwischenergebnis	248
d) Ergebnis	249
IV. Fazit	249
B. § 100c StPO	250
C. §§ 102 ff. i.V.m. 94 ff. StPO	251
D. § 110 Abs. 3 StPO	252
E. §§ 161 Abs. 1 S. 1, 163 Abs. 1 S. 2 StPO	253
F. Ergebnis	253
G. Analogieverbot im Strafprozess	254
H. Gesetzgeberischer Handlungsbedarf vor dem Inkrafttreten der StPO-Reform	255
I. Schaffung einer Rechtsgrundlage für heimliche Eingriffe in das IT-Grundrecht	255
II. Schaffung einer Rechtsgrundlage für die sog. Quellen- Telekommunikationsüberwachung	256
III. Schaffung einer Rechtsgrundlage für die heimliche Erhebung von Telekommunikation	257
I. Fazit	257
§ 5 Prozessuale Rechtsfolgen im Falle der rechtswidrigen Überwachung von Cloud-Storage	259
A. Kompensation auf Strafzumessungs- oder Vollstreckungsebene	259
B. Beweisverwertungsverbot	260
I. Die sog. Abwägungslehre	261
II. Ausschluss der Abwägung bei fehlender Rechtsgrundlage	261
III. „Heilung“ von Beweisverwertungsverboten – Zum Grundsatz des intertemporalen Verfahrensrechts	263
C. Fazit	264

§ 6 Die heimliche Überwachung von Cloud-Storage nach dem Inkrafttreten der StPO-Reform am 24.08.2017	265
A. Festgestellter Reformbedarf	267
B. Reform	268
I. § 100a Abs. 1 S. 2 und 3, Abs. 5 und 6 StPO n.F.	269
1. Inhaltliche Änderungen	269
2. Erläuterungen in der Gesetzesbegründung	270
II. § 100b StPO n.F.	272
1. Inhaltliche Änderungen	272
2. Erläuterungen in der Gesetzesbegründung	274
III. Kernbereichsschutz und Verfahren	275
C. Die heimliche Überwachung von Cloud-Storage	278
I. § 100a Abs. 1 S. 2, 3 StPO n.F.	278
1. Sachlicher Anwendungsbereich	278
a) Informationstechnisches System	278
b) Überwachung und Aufzeichnung	280
c) Eingreifen i.S.d. § 100a Abs. 1 S. 2 StPO n.F.	281
d) Notwendigkeit	282
2. Die heimliche Überwachung von Cloud-Storage gemäß § 100a Abs. 1 S. 2, 3 StPO n.F.	282
II. § 100b StPO n.F.	284
1. Sachlicher Anwendungsbereich	284
a) Informationstechnisches System	284
b) Eingreifen	284
c) Erheben	285
2. Die heimliche Überwachung von Cloud-Storage gemäß § 100b StPO n.F.	288
III. Ergebnis	288
D. Bewertung	289
I. Bewertung von § 100a StPO n.F.	289
1. Bewertung von § 100a Abs. 1 S. 2 StPO n.F. – Quellen-Telekommunikationüberwachung	290
a) Bewertungsmaßstab	290

b)	Unzulässige Übernahme des Straftatenkatalogs des § 100a Abs. 2 StPO	291
aa)	Größere Eingriffstiefe	291
(1)	Notwendigkeit einer Infiltration des Zielsystems	292
(2)	Gefahr des Missbrauchs und der Fehlfunktion des Trojaners	293
(3)	Umgehung von Selbstschutzmöglichkeiten	294
(4)	Beweismittelmanipulation	295
(5)	Gefahren für die IT-Sicherheit	296
bb)	Zwischenergebnis	296
c)	Ergebnis	297
2.	Bewertung von § 100a Abs. 1 S. 3 StPO n.F. – „kleine“ Systemüberwachung	297
a)	Bewertungsmaßstab	297
b)	Unzulässige Übernahme des Straftatenkatalogs des § 100a Abs. 2 StPO	299
aa)	Verstoß gegen die Maßstäbe des IT-Grundrechts	299
bb)	Größere Eingriffstiefe	300
(1)	Infiltration des Zielsystems	300
(2)	Umfassende Auswertung von Meta-Daten	301
(3)	Gefahr „zufälliger“ Rechtsverletzungen	302
cc)	Zwischenergebnis	302
c)	Ergebnis	303
3.	§ 100a Abs. 6 StPO n.F. – Protokollierungspflichten	303
4.	Ergebnis	304
II.	Bewertung von § 100b StPO n.F. – Online-Durchsuchung	304
1.	Bewertungsmaßstab	305
2.	Unzulässige Übernahme des Straftatenkatalogs des § 100c StPO	305
a)	Verstoß gegen die Maßstäbe des IT-Grundrechts	305
b)	Größere Eingriffstiefe	306
c)	Zwischenergebnis	308
3.	§ 100b Abs. 4 StPO n.F. Protokollierungspflichten	308
4.	Ergebnis	309
III.	Bewertung von § 100d n.F. – Kernbereichsschutz	309
1.	Kernbereichsschutz auf der Erhebungsebene	309
2.	Kernbereichsschutz auf der Auswertungsebene	312
3.	Schutz der Gehilfen von Berufsheimnisträgern	312

4. Ergebnis	315
IV. Bewertung von § 100e StPO n.F.	315
V. Ergebnis	316
E. Gesetzgeberischer Handlungsbedarf	317
I. „Entschlackung“ des Straftatenkatalogs des § 100b Abs. 2 StPO n.F.	317
II. Bezugnahme von § 100a Abs. 1 S. 3 StPO n.F. auf § 100b Abs. 2 StPO n.F.	317
III. Partieller Verweis von § 100a Abs. 1 S. 2 StPO n.F. auf § 100a Abs. 2 StPO n.F.	317
IV. Schutz des Kernbereichs privater Lebensgestaltung	318
V. Protokollierungspflicht	318
VI. Reformvorschläge	318
F. Fazit	321
§ 7 Zusammenfassung und Schlussbetrachtung	322
A. Zusammenfassung der Ergebnisse	322
Zu § 3	322
Zu § 4	323
Zu § 5	325
Zu § 6	325
B. Schlussbetrachtung	327
Literaturverzeichnis	329