



Andreas Grözinger

Die Überwachung von Cloud-Storage

Eine Untersuchung der strafprozessualen Möglichkeiten zur heimlichen Überwachung von Cloud-Storage vor und nach dem Inkrafttreten des Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens



Deutsches und Europäisches Strafprozessrecht
und Polizeirecht

herausgegeben von

Prof. Dr. Mark A. Zöller, Universität Trier

Band 9

Andreas Grözinger

Die Überwachung von Cloud-Storage

Eine Untersuchung der strafprozessualen Möglichkeiten zur heimlichen Überwachung von Cloud-Storage vor und nach dem Inkrafttreten des Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens



Nomos

Die Hohe Rechtswissenschaftliche Fakultät der Universität zu Köln hat diese Arbeit im Wintersemester 2017/2018 als Dissertation angenommen.

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

Zugl.: Köln, Univ., Diss., 2018

ISBN 978-3-8487-5448-9 (Print)

ISBN 978-3-8452-9604-3 (ePDF)

1. Auflage 2018

© Nomos Verlagsgesellschaft, Baden-Baden 2018. Gedruckt in Deutschland. Alle Rechte, auch die des Nachdrucks von Auszügen, der fotomechanischen Wiedergabe und der Übersetzung, vorbehalten. Gedruckt auf alterungsbeständigem Papier.

Meinen Eltern

Die vorliegende Arbeit wurde durch die Rechtswissenschaftliche Fakultät der Universität zu Köln im Wintersemester 2017/2018 als Dissertation angenommen. Inhaltlich befindet sich die Arbeit auf dem Stand von August 2018.

Herzlich bedanken möchte ich mich bei meinem Doktorvater Prof. Dr. Martin Waßmer, der mich bei der Wahl des Themas unterstützte und mir bei der Bearbeitung stets mit zahlreichen wertvollen Anregungen beiseite stand. Dank gebührt auch Herrn Prof. Dr. Dr. h.c. Michael Kubiciel für die zügige Erstellung des Zweitgutachtens und seine hilfreichen Anmerkungen.

Weiterer Dank gilt meinen Kollegen und Kolleginnen der Kanzlei Gercke|Wollschläger, hier insbesondere Prof. Dr. Björn Gercke und Dr. Sebastian Wollschläger, die stets ein offenes Ohr für meine Anliegen hatten.

Ich danke Mani Jaleesi, Dr. Jonas Dereje und Niklas Gräbener für ihre Kritik und ihre Impulse.

Mein besonderer Dank gilt Dr. Anna Eschbach, die mich während der gesamten Zeit der Entstehung vorbehaltlos unterstützte.

Schließlich danke ich meiner Familie. Ohne sie hätte diese Arbeit nicht entstehen können. Besonders danken möchte ich meinen Eltern Beate und Michael Grözinger, die mir zu jedem Zeitpunkt eine Stütze waren. Ihnen ist diese Arbeit gewidmet.

Köln, Herbst 2018

Andreas Grözinger

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 Speicherungsort	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-Telekommunikationsüberwachung	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 Berufsgeheimnisträgern	312

Inhaltsverzeichnis

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

Abkürzungsverzeichnis

a.A./a.A.	anderer Ansicht/andere Auffassung
a.F.	alte Fassung
Abs.	Absatz
AG	Amtsgericht
Anm.	Anmerkung
AöR	Archiv des öffentlichen Rechts
Art.	Artikel
Az.	Aktenzeichen
Beschl.	Beschluss
BGBI.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHSt	Entscheidung in Strafsachen des Bundesgerichtshofes
BT-Drs.	Bundestagsdrucksache
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidung des Bundesverfassungsgerichts
BVerfGK	Kammerentscheidung des Bundesverfassungsgerichts
CR	Computer und Recht
d.h.	das heißt
ders.	derselbe
dies.	dieselbe
DÖV	Die öffentliche Verwaltung
DRiZ	Deutsche Richter-Zeitung
DuD	Datenschutz und Datensicherheit
DVBl	Deutsches Verwaltungsblatt
f.	folgende
ff.	fortfolgende
Fn.	Fußnote
FS	Festschrift
GA	Goldammer's Archiv für Strafrecht
GG	Grundgesetz
ggf.	gegebenenfalls

Abkürzungsverzeichnis

h.M.	herrschende Meinung
HRRS	Höchstrichterliche Rechtsprechung im Strafrecht
Hrsg.	Herausgeber
Hs.	Halbsatz
i.d.F.	in der Fassung
i.d.R.	in der Regel
i.E.	im Ergebnis
i.S.d.	im Sinne des
i.V.m.	in Verbindung mit
JA	Juristische Arbeitsblätter
JR	Juristische Rundschau
JURA	Juristische Ausbildung
jurisPR-ITR	juris Praxisreport IT-Recht
JurPC	JurPC
JuS	Juristische Schulung
JZ	JuristenZeitung
K&R	Kommunikations & Recht
KritV	Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft
LG	Landgericht
Lit.	Literatur
m.w.N.	mit weiteren Nachweisen
MMR	MultiMedia und Recht
n.F.	neue Fassung
NJW	Neue Juristische Wochenzeitschrift
Nr.	Nummer
NStZ	Neue Zeitschrift für Strafrecht
NStZ-RR	NStZ-Rechtsprechungs-Report Strafrecht
OLG	Oberlandesgericht
Rn.	Randnummer
Rspr.	Rechtsprechung
s.	siehe
sog.	sogenannte/r
st. Rspr.	ständige Rechtsprechung
StGB	Strafgesetzbuch
StPO	Strafprozessordnung

str.	streitig
StraFo	Strafverteidiger Forum
StV	Strafverteidiger
u.	und
u.a.	unter anderem
u.U.	unter Umständen
Urt.	Urteil
v.	von/vom
Var.	Variante
vgl.	vergleiche
WM	Zeitschrift für Wirtschafts- und Bankrecht
z.B.	zum Beispiel
z.T.	zum Teil
ZD	Zeitschrift für Datenschutz
ZIS	Zeitschrift für Internationale Strafrechtsdogmatik
ZRP	Zeitschrift für Rechtspolitik
ZStW	Zeitschrift für die gesamte Strafrechtswissenschaft
ZUM	Zeitschrift für Urheber- und Medienrecht

§ 1 Einleitung

A. Die Cloud – ein junges Phänomen

Immer neue Phänomene der Informationstechnik schaffen Herausforderungen für das Recht und den Gesetzgeber.

Eines dieser Phänomene ist „die Cloud“ (zu deutsch: die Wolke). Zunächst noch als „Hypethema“¹ bezeichnet, kann die wachsende Bedeutung von Cloud-Computing und den damit einhergehenden rechtlichen Fragestellungen heute kaum noch geleugnet werden. So ist sie der Grund dafür, dass der herkömmliche Computer bereits als „Auslaufmodell“² bezeichnet und mit Cloud-Computing „die Zukunft“³ ausgerufen wird. Auch der prophezeite Siegeszug des Cloud-Computing zeichnet sich schon jetzt ab. Immer mehr Bürger*innen⁴ und Unternehmen nutzen die Cloud und haben diese in ihren Alltag integriert.⁵ Die Vorteile für den Nutzer sind enorm. So bietet der Cloud-Anbieter seinen Nutzern nicht nur die Möglichkeit zur flexiblen Nutzung seiner Speicherkapazitäten und sonstigen Ressourcen wie z.B. Rechenleistung. Darüber hinaus können die Nutzer von nahezu jedem internetfähigen Endgerät auf ihre Cloud zugreifen. Für Unternehmen ergeben sich schließlich erhebliche Kostenersparnisse, weil sie nicht selbst die erforderlichen Infrastrukturen betreiben müssen und beim Cloud-Anbieter entsprechend ihren gegenwärtigen Bedürfnissen Kapazitäten flexibel hinzu- oder abbuchen können.⁶

1 *Birk/Wegener*, DuD 2010, 641.

2 *Obenhaus*, NJW 2010, 651.

3 *Obenhaus*, NJW 2010, 651; *Söbbing*, MMR 2008, XII.

4 Soweit im Folgenden Berufs- Gruppen- und/oder Personenbezeichnungen Verwendung finden, beziehen sich diese auch stets auf die jeweils weibliche Form.

5 Allein im Jahr 2015 machten Cloud-Anbieter mit Soft- und Hardware sowie Dienstleistungen einen Umsatz von 183 Milliarden Dollar. Im selben Jahr wuchs der Markt im Vergleich zum Vorjahr damit um 17 Prozent, vgl. <http://blog.wiwo.de/look-at-it/2015/03/19/cloud-computing-2015-183-milliarden-dollar-umsatz-agilitat-und-kosten-als-hauptmotive/> (Stand: September 2018). Zu den Vorteilen der Cloud insbesondere für Unternehmen und Behörden *Wicker*, Cloud Computing und staatlicher Strafanspruch, S. 49 ff.

6 Vgl. <https://www.heise.de/download/blog/Die-Vorteile-und-Nachteile-des-Cloud-Computing-3713041> (Stand: September 2018).

Doch Wolken werfen bekanntlich auch Schatten.⁷ Längst haben Kriminelle die Vorteile der Cloud für sich entdeckt und sich in einen Wettlauf⁸ mit den Strafverfolgungsbehörden begeben. Um in diesem Wettlauf mithalten zu können, sind die Strafverfolgungsbehörden ihrerseits nicht nur auf die notwendigen informationstechnischen Werkzeuge zur Aufklärung des Sachverhalts angewiesen. Sie müssen sich zudem auf einem sicheren rechtlichen Fundament bewegen können. Schließlich ist zu berücksichtigen, dass es „kein Grundsatz der StPO [ist], daß [sic] die Wahrheit um jeden Preis erforscht werden müßte [sic]“⁹.

B. Untersuchungsgegenstand

Dieser Befund führt unweigerlich zu der Frage, ob die Strafverfolgungsbehörden Kriminellen im Wettlauf der Informationstechnik auf Augenhöhe begegnen können oder ob der Rechtsstaat mangels hinreichender rechtlicher „Ausstattung“ nicht bereits „hinterherhinkt“¹⁰.

Die jährlich steigende Zahl von Anordnungen der Telekommunikationsüberwachungen¹¹ und der vermehrte Einsatz des Internets als Fahndungsmittel¹² zeigen jedenfalls den Willen der Strafverfolgungsbehörden, den Blickkontakt zu Kriminellen im Internet nicht zu verlieren.

Dieser Ehrgeiz bringt aus der Perspektive der Bürger aber auch Gefahren mit sich.¹³ Die Anordnung von Telekommunikationsüberwachungen

7 Jotzo, Der Schutz personenbezogener Daten in der Cloud, S. 17; Valerius, in: Cybercrime und Cyberinvestigations, S. 67.

8 Vgl. Bäcker, Kriminalpräventionsrecht, S. 68.

9 BGH, NJW 1960, 1580, 1582.

10 Paeßgen, in: FS-Roxin, 1299, 1318; vgl. zur verstärkten Einbindung Privater bei der Rechtsdurchsetzung im Internet und zur Frage der Verwertbarkeit der so gewonnenen Informationen Kubiciel, GA 2013, 226.

11 Allein im Jahr 2013 betrug die Anzahl der Anordnungsbeschlüsse 19.398 und die der Verlängerungsbeschlüsse 3.519. Hält man sich nunmehr vor Augen, dass sich die Anzahl an Anordnungsbeschlüssen im Jahr 2010 noch auf 12.239 und an Verlängerungsanordnungen auf 337 belief, wird das inflationäre Ausmaß der Anordnung von Telekommunikationsüberwachung nach § 100a der StPO deutlich, vgl. https://www.bundesjustizamt.de/DE/SharedDocs/Publikationen/Justizstatistik/Uebersicht_TKUE_2013.pdf?__blob=publicationFile (Stand: September 2018).

12 Vgl. hierzu Pätzelt, NJW 1997, 3131; Soiné, NStZ 1997, 166 ff. und 321 ff.

13 Vgl. auch Zöller, ZStW 124 (2012), 411, 416.

ist heute bereits zum Massenphänomen geworden.¹⁴ Der Umstand, dass weite Teile der Bevölkerung das Internet und die Cloud mit der Attitüde benutzen, man habe nichts zu verbergen, kann vor dem Hintergrund umfassender Möglichkeiten zur Datenauswertung und -verarbeitung bis hin zur Erstellung von Persönlichkeitsprofilen nur als leichtfertig bezeichnet werden.¹⁵

Fehlen gegenwärtig erforderliche Rechtsgrundlagen zur heimlichen Überwachung der Cloud und versäumt der Staat durch die Schaffung notwendiger Rechtsgrundlagen „nachzurüsten“, ist zu befürchten, dass das rechtsstaatliche Fundament staatlichen Handelns Risse bekommt. Umso wichtiger ist es, dass staatlichem Handeln klare rechtliche Grenzen gesetzt und dadurch die verfassungsmäßigen Rechte der Bürger geschützt werden.

Originäres Ziel dieser Untersuchung ist es, das Speichern von Daten in der Cloud einem grundrechtlichen Schutzbereich zuzuordnen und – daran anknüpfend – die Frage zu beantworten, ob in der StPO eine Rechtsgrundlage für die heimliche Überwachung der Cloud existiert. Insoweit wird zunächst der Fokus auf die Rechtslage *vor* Inkrafttreten des Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 17.08.2017 (BGBl. I S. 3202) am 24.08.2017¹⁶ (im Folgenden: StPO-Reform) gelegt, bevor insbesondere die Verfassungsmäßigkeit der im Zuge dieser Reform neu eingeführten §§ 100a Abs. 1 S. 2 und 3, 100b StPO n.F.¹⁷ untersucht und deren Auswirkungen auf die Möglichkeiten zur heimlichen Überwachung der Cloud beleuchtet werden.

14 *Wolter*, in: SK-StPO, § 100a, Rn. 6.

15 *Sandfuchs*, Privatheit wider Willen?, S. 21.

16 BT-Drs. 18/12785.

17 Als „§ 100a StPO“ bzw. „100b StPO“ werden zur besseren Gewährleistung der Übersichtlichkeit die Vorschriften der §§ 100a, 100b StPO a.F., namentlich in ihrer Fassung bis zum Inkrafttreten des Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 17.08.2017 (BGBl. I S. 3202) (StPO-Reform), am 24.08.2017, bezeichnet. Die im Zuge der StPO-Reform geänderten bzw. eingeführten §§ 100a, 100b StPO werden trotz ihres zwischenzeitlichen Inkrafttretens als „§ 100a StPO n.F.“ bzw. „§ 100b StPO n.F.“ bezeichnet. § 100a Abs. 1 S. 1 StPO n.F. entspricht dem bisherigen § 100a Abs. 1 StPO.

C. Gang der Untersuchung

Die Analyse gliedert sich insgesamt in sieben Kapitel (§§ 1 – 7). Nachdem zunächst der Realbereich dargestellt und insbesondere die Begriffe Cloud, Cloud-Computing und Cloud-Storage erläutert werden (§ 2), widmet sich die Arbeit dem verfassungsrechtlichen (§ 3) Normbereich. Anschließend werden der einfach-gesetzlichen Normbereich *vor* Inkrafttreten der StPO-Reform (§ 4) untersucht und die prozessualen Rechtsfolgen im Falle der unzulässigen Überwachung von Cloud-Storage erläutert (§ 5). Schließlich befasst sich das sechste Kapitel mit den im Zuge der StPO-Reform eingeführten Eingriffsbefugnissen, die als denkbare Rechtsgrundlagen für die Überwachung von Cloud-Storage in Betracht kommen (§ 6).

Das zweite Kapitel legt zunächst die wesentlichen tatsächlichen und begrifflichen Grundlagen für die weitere Untersuchung. So erläutert es den Begriff der Cloud, ihre Ausprägungen und Erscheinungsformen und beleuchtet die technischen Grundlagen der Cloud und der Datenübertragung im Internet. Anschließend beschreibt es die unterschiedlichen Arten von Daten, die aus einer Überwachung gewonnen werden können und skizziert die technischen Möglichkeiten der Durchführung einer solchen. Sodann stellt es den eigentlichen Untersuchungsgegenstand dar. Schließlich zeigt es die Bedeutung auf, die die Möglichkeit zur heimlichen Überwachung der Cloud für die Strafverfolgungsbehörden vor dem Hintergrund der weltweiten Vernetzung des Internets hat und nimmt die Vorteile der heimlichen Überwachung gegenüber anderen Ermittlungsmaßnahmen in den Blick.

Das dritte Kapitel stellt die Frage nach der Regelungsbedürftigkeit einer entsprechenden Maßnahme in der StPO und bespricht den verfassungsrechtlichen Schutz des Cloud-Nutzers. Als betroffene Grundrechte behandelt dieses Kapitel insbesondere das Telekommunikationsgeheimnis sowie das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Am Ende beantwortet § 3 die Frage, wann und unter welchen Voraussetzungen der Nutzer sich auf den Schutz welchen Grundrechts berufen kann.

Das vierte Kapitel konzentriert sich auf die Frage, welche einfach-gesetzlichen Eingriffsermächtigungen innerhalb der StPO vor Inkrafttreten der StPO-Reform für die heimliche Überwachung von Cloud-Storage herangezogen werden konnten. Den Fokus legt § 4 auf die Telekommunikationsüberwachung gemäß § 100a StPO und fragt zunächst danach, was unter dem Begriff der Telekommunikation in diesem Sinne zu verstehen ist.

Nachdem insoweit ein Ergebnis gefunden worden ist, widmet sich § 4 dem Überwachungsbegriff und untersucht die Frage, welche (Begleit-) Maßnahmen vor der StPO-Reform konkret auf Grundlage von § 100a StPO durchgeführt werden durften. Schließlich wird die Anwendbarkeit weiterer strafprozessualer Eingriffsmächtigungen in Bezug auf die heimliche Überwachung von Cloud-Storage geprüft sowie die Frage beantwortet, ob entsprechende Vorschriften aus der StPO analog als Rechtsgrundlage für entsprechende Überwachungsmaßnahmen herangezogen werden dürfen. Am Ende des Kapitels wird der gesetzgeberische Handlungsbedarf aufgezeigt, der vor Inkrafttreten der StPO-Reform bestand.

Das fünfte Kapitel widmet sich den prozessualen Rechtsfolgen einer unzulässigen Überwachung der Cloud und beantwortet die Fragen nach dem Vorliegen eines Beweisverwertungsverbotes sowie der Möglichkeit der Heilung etwaiger Beweisverwertungsverbote durch die nachträgliche Schaffung einer bis dahin nicht vorhandenen aber erforderlichen gesetzlichen Regelung.

§ 6 untersucht schließlich die Rechtslage nach der StPO-Reform. Das Augenmerk der Untersuchung legt § 6 auf die neu eingeführten §§ 100a, 100b StPO n.F., die die sog. Quellen-Telekommunikationsüberwachung und die sog. Online-Durchsuchung regeln. Neben der Darstellung der Auswirkungen der §§ 100a, 100b StPO n.F. im Hinblick auf die Möglichkeiten zur heimlichen Überwachung von Cloud-Storage beantwortet § 6 die Fragen nach der Verfassungsmäßigkeit dieser Vorschriften und etwaig verbleibendem gesetzgeberischen Handlungsbedarf.

Das siebte und letzte Kapitel enthält eine Zusammenfassung der wesentlichen Ergebnisse der Untersuchung.

§ 2 Grundlagen

Der Markt von Cloud-Angeboten wächst rasant.¹⁸ Neben Unternehmen haben längst immer mehr Privatpersonen den Nutzen der Cloud erkannt. Das Speichern in der Cloud ist im Alltag angekommen. Der Begriff der Cloud ist inzwischen im allgemeinen Sprachgebrauch angelangt. Doch was bedeutet eigentlich Cloud? Wodurch charakterisiert sich die Cloud und wie funktioniert sie? Diese Fragen werden in der Folge näher beleuchtet. Nach Herausarbeitung des dieser Arbeit zugrundeliegenden Untersuchungsgegenstands werden sodann die verfassungsrechtlichen Grundlagen für die Überwachung der Cloud sowie die Vorteile der heimlichen Überwachung gegenüber anderen – insbesondere offenen – Ermittlungsmaßnahmen aufgezeigt.

A. Begriffliche Grundlagen

Da es eine Vielzahl von Definitionen und Verwendungen der Begriffe Cloud-Computing und Cloud-Storage gibt, sollen im Folgenden die dieser Arbeit zugrunde gelegten Begrifflichkeiten erläutert werden.

I. Cloud, Cloud-Computing und Cloud-Storage

Um Cloud-Storage zu verstehen ist es wichtig, zunächst eine Definition des Cloud-Computing herauszuarbeiten, das als Oberbegriff Cloud-Storage umfasst. Ferner werden die verschiedenen Bereitstellungs- und Service-Modelle des Cloud-Computing in der gebotenen Kürze erläutert.

18 Vgl. <http://blog.wiwo.de/look-at-it/2015/03/19/cloud-computing-2015-183-milliarden-dollar-umsatz-agilitat-und-kosten-als-hauptmotive/> (Stand: September 2018).

1. Begriff und Definition

Der Begriff „Cloud“ bedeutet ins Deutsche übersetzt „Wolke“ und beschreibt metaphorisch die undurchsichtige, in ständiger Bewegung befindliche und komplexe Infrastruktur, auf die netzbasierte Anwendungen zugreifen, ohne dass die Nutzer sie näher kennen oder gar kontrollieren können.¹⁹

Eine einheitliche Definition von Cloud-Computing und Cloud-Storage existiert nicht. Dennoch nähern sich die unterschiedlichen Definitionsversuche einander immer mehr an, sodass der Begriff der Cloud nicht mehr nur eine „diffuse Marketingworthülse“²⁰ ist.

Zum Teil wird Cloud-Computing als eine große Ansammlung von Ressourcen (z.B. Hardware, Dienste oder Entwicklungsplattformen) verstanden, die leicht nutzbar sind und auf die einfach zugegriffen werden kann.²¹ Kennzeichnend ist demnach, dass diese Ressourcen flexibel an die jeweiligen Bedürfnisse angepasst werden können, sodass eine optimale Auslastung der Ressourcen möglich ist.²²

Andere definieren Cloud-Computing als einen IT-Betrieb, bei dem erheblich skalierbare Ressourcen für externe Kunden über das Internet als Dienst zur Verfügung gestellt werden.²³

Das Bundesamt für Sicherheit in der Informationstechnik definiert Cloud-Computing wie folgt:

„Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die Spannbreite der im Rahmen von Cloud Computing angebotenen Dienstleistungen umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem

19 Vgl. *Federrath*, ZUM 2014, 1; *Hoffmann-Riem*, JZ 2008, 1009, 1011.

20 *Krcmar*, in: Borges/Meents (Hrsg.), *Cloud Computing*, § 1, Rn. 27.

21 *Vaquero et al.*, *A Break in the Clouds*, S. 51.

22 *Vaquero/Rodero-Merino/Caceres/Lindner*, a.a.O.

23 *Cearley*, Gartner, *Cloud computing: Key Initiative Overview*, S. 2.

§ 2 Grundlagen

Infrastruktur (z.B. Rechenleistung, Speicherplatz),²⁴ Plattformen und Software.“²⁵

Die Definition mit der wohl größten Akzeptanz in Fachkreisen²⁶ ist die Definition der US-amerikanischen Standardisierungsstelle National Institute of Standards and Technology (NIST). Cloud-Computing ist danach ein Modell, das es erlaubt, bei Bedarf jederzeit und überall bequem über ein Netz auf einen geteilten Pool von konfigurierbaren Rechnerressourcen (z.B. Netze, Server, Speichersysteme, Anwendungen und Dienste) zuzugreifen, die schnell und mit minimalem Managementaufwand oder geringerer Server-Provider-Interaktion zur Verfügung gestellt werden können.²⁷

Darüber hinaus legt die NIST fünf Charakteristika fest, die einen Cloud-Service beschreiben, nämlich On-Demand-Self-Service, Broad Network Access, Resource Pooling, Rapid Elasticity und Measured Services.²⁸

Unter On-Demand-Self-Service versteht man die automatische Bereitstellung der Ressourcen. Eine Interaktion mit dem Service Provider findet nicht statt.²⁹

Broad Network Access bedeutet, dass die Dienste nicht an einen bestimmten Client³⁰ gebunden, sondern mit Standard-Mechanismen über das Netz verfügbar sind.³¹

Resource Pooling beschreibt die Bündelung von Ressourcen, die in einem Pool zusammengetragen werden, aus dem sich viele Nutzer gleichzeitig bedienen können. Wo sich die Ressourcen befinden, ist den Nutzern grundsätzlich nicht bekannt. Etwas anderes gilt allenfalls dann, wenn vertraglich ein bestimmter Speicherort festgelegt worden ist.³²

24 Vgl. https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Grundlagen/Grundlagen_node.html;jsessionid=BD3E-FE636495D9C054CBC43ACF75D3C2.2_cid368 (Stand: September 2018).

25 Vgl. https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Grundlagen/Grundlagen_node.html;jsessionid=BD3E-FE636495D9C054CBC43ACF75D3C2.2_cid368 (Stand: September 2018).

26 *Süptitz/Utz/Eymann*, DuD 2013, 307.

27 NIST, Special Publication 800-145, S. 2.

28 Vgl. auch Darstellung in *Niemann/Paul*, Cloud Computing, S. 18.

29 NIST, Special Publication 800-145, S. 2.

30 Als Client wird ein Rechner innerhalb eines Netzwerks bezeichnet, der vom Server Dienste abrufen, vgl. Duden, Deutsches Universalwörterbuch.

31 NIST, Special Publication 800-145, S. 2.

32 NIST, Special Publication 800-145, S. 2.

Rapid Elasticity bedeutet, dass die unterschiedlichen Dienste schnell, elastisch und in manchen Fällen auch automatisch bereitgestellt werden. Aus der Sicht des Nutzers scheinen die Ressourcen unendlich zu sein.³³

Schließlich versteht man unter Measured Services, dass die Ressourcennutzung gemessen, überwacht und entsprechend bemessen den Nutzern zur Verfügung gestellt werden kann.³⁴

Aufgrund der hohen Akzeptanz der NIST-Definition und weil weitere hier besprochene Differenzierungen (Public Cloud und Private Cloud, Servicemodelle) von der NIST entwickelt worden sind, wird dieser Arbeit die NIST-Definition zugrunde gelegt.

2. Von der Public Cloud über die Private Cloud zur Internal Cloud

Das NIST teilt Cloud-Computing in vier Bereitstellungsmodelle ein, nämlich Public Cloud, Private Cloud, Community Cloud und Hybrid Cloud.

Für eine Private Cloud ist kennzeichnend, dass die Cloud-Infrastruktur exklusiv für eine Institution, also einen festgelegten Nutzerkreis, betrieben wird. Die Cloud kann von einem Dritten oder der Institution selbst organisiert und betrieben werden. Entsprechend kann die Cloud-Infrastruktur bei einem Dritten oder innerhalb der eigenen Institution stehen.³⁵ Steht die gesamte Cloud-Infrastruktur im Eigentum z.B. eines Unternehmens, spricht man von einer Internal Cloud, die einen Unterfall der Private Cloud darstellt. Die Internal Cloud kann als Unternehmensintranet in Cloud-Form bezeichnet werden.³⁶

In einer Public Cloud können die von einem Anbieter zur Verfügung gestellten Dienste von der Allgemeinheit oder einer großen Gruppe (z.B. einer ganzen Industriebranche) genutzt werden.

Von einer Community Cloud spricht man, wenn die Infrastruktur von mehreren Institutionen geteilt wird, die typischerweise ähnliche Interessen haben. Der Betreiber der Cloud kann ein Dritter oder die Institution selbst sein.³⁷ Treffend vergleicht *Krcmar* die Community Cloud mit einer Einkaufsgemeinschaft, die sich von einer Private Cloud insbesondere dadurch

33 NIST, Special Publication 800-145, S. 2.

34 NIST, Special Publication 800-145, S. 2.

35 NIST, Special Publication 800-145, S. 3.

36 *Bedner*, Cloud Computing, S. 33.

37 NIST, Special Publication 800-145, S. 3.

unterscheidet, dass sich der Benutzerkreis aus unterschiedlichen, rechtlich sowie wirtschaftlich unabhängigen Unternehmen zusammensetzt.³⁸

Eine Hybrid Cloud kennzeichnet sich schließlich dadurch aus, dass mehrere für sich eigenständige Cloud Infrastrukturen über standardisierte Schnittstellen gemeinsam genutzt werden können.³⁹ Insoweit kombiniert eine Hybrid Cloud die Modelle der Private Cloud und der Public Cloud. Eine Hybrid Cloud hat damit den Vorteil, dass ein Unternehmen es in der Hand hat, ob es sensible Daten und Anwendungen im eigenen Kontrollbereich belässt (Private Cloud) oder in die Public Cloud verschiebt, wenn mit einem erhöhten Ressourcenbedarf zu rechnen ist.⁴⁰

Auch wenn die vorgenannten Definitionen einen Großteil der Cloudmodelle erfassen, sind sie nicht abschließend.⁴¹

3. Servicemodelle – IaaS, PaaS, SaaS

Cloud-Computing lässt sich in drei wesentliche Servicemodelle unterteilen, nämlich Infrastructure-as-a-Service, Platform-as-a-Service und Software-as-a-Service.⁴²

Zu Recht wird jedoch eingewandt, dass die Grenzen zwischen den einzelnen Servicemodellen teilweise fließend sind, sodass sich nicht jeder angebotene Dienst ausschließlich einem Servicemodell zuordnen lässt.⁴³

Unter Infrastructure-as-a-Service (IaaS) versteht man ein Angebot zur Bereitstellung von physischen IT-Basisressourcen wie z.B. Datenspeicher, Rechenleistung oder Netze. Durch die Inanspruchnahme von IaaS erhält ein Nutzer die Möglichkeit, fremde Hardware-Kapazitäten für die eigenen Bedürfnisse zu nutzen. So kann er beispielsweise Rechenleistung, Arbeitsspeicher und Festplattenspeicher anmieten und über diese Cloud-Ressourcen ein Betriebssystem mit Anwendungen seiner Wahl ablaufen lassen.

Bei dem Servicemodell Platform-as-a-Service (PaaS) wird dem Kunden eine komplette Anwendungs-Infrastruktur bereitgestellt. Über standardi-

38 *Krcmar*, in: Borges/Meents (Hrsg.), *Cloud Computing*, § 1, Rn. 49.

39 NIST, *Special Publication 800-145*, S. 3.

40 *Krcmar*, in: Borges/Meents (Hrsg.), *Cloud Computing*, § 1, Rn. 50.

41 Vgl. https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Grundlagen/Grundlagen_node.html;jsessionid=BD3E-FE636495D9C054CBC43ACF75D3C2.2_cid368 (Stand: September 2018).

42 NIST, *Special Publication 800-145*, S. 2 f.

43 *Armbrust et al.*, *Communications of the ACM*, S. 50.

sierte Schnittstellen, die dem Nutzer zur Verfügung gestellt werden, kann dieser nunmehr auf der Plattform eigene Anwendungen laufen lassen. Allerdings hat er keinen Zugriff auf die darunterliegenden Schichten (Hardware, Betriebssystem).

Software-as-a-Service (SaaS) stellt dem Nutzer die Funktionalität einer vollwertigen Anwendung zur Verfügung.⁴⁴ Wartung und Betrieb der Software erfolgen bei diesem Servicemodell allein durch den jeweiligen Dienstleister und liegen außerhalb des Verantwortungsbereichs des Nutzers.⁴⁵

II. Akteure

Beim Cloud-Computing spielen verschiedene Akteure eine Rolle. Im Wesentlichen kann zwischen Cloud-Nutzern (Kunden), Cloud-Anbietern (alt.: Cloud-Providern), und Ressourcenanbietern unterschieden werden.⁴⁶ Daneben spielen die Telekommunikationsdiensteanbieter eine Rolle.

Cloud-Anbieter vermarkten ihre Ressourcen. Namhafte Cloud-Anbieter sind Amazon, Google, Microsoft oder Salesforce. Im Fall von Cloud-Storage wird insbesondere Speicherkapazität zur Verfügung gestellt. Cloud-Nutzer, die diesen Service in Anspruch nehmen, können Speicherkapazitäten beim Cloud-Anbieter nach Bedarf mieten.⁴⁷

Nicht immer verfügt ein Cloud-Anbieter über genug Kapazitäten, um die Nachfrage der Kunden zu befriedigen. Übersteigt die Kundennachfrage die vorhandenen Kapazitäten, kann ein Cloud-Provider seinerseits Speicher bei unabhängigen Ressourcenanbietern anmieten, um die Kundennachfrage befriedigen zu können. Der Kunde bekommt von diesem Vorgang grundsätzlich nichts mit. Ressourcenanbieter sind damit Subunternehmer der Cloud-Provider.⁴⁸

44 Vgl. https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Grundlagen/Grundlagen_node.html;jsessionid=BD3E-FE636495D9C054CBC43ACF75D3C2.2_cid368 (Stand: September 2018).

45 *Krcmar*, in: Borges/Meents (Hrsg.), *Cloud Computing*, § 1, Rn. 32.

46 *Weichert*, *DuD* 2010, 679, 680.

47 Vgl. zur zivilrechtlichen Einordnung des Cloud Computing ausführlich *Wicker*, *Cloud Computing und staatlicher Strafanspruch*, S. 65 ff.

48 *Eckhardt*, *DuD* 2015, 176, 179.