

Schriften zum Prozessrecht

Band 254

Strafverfolgung und die Cloud

Strafprozessuale Ermächtigungsgrundlagen und
deren völkerrechtliche Grenzen

Von

Senta Bell



Duncker & Humblot · Berlin

SENTA BELL

Strafverfolgung und die Cloud

Schriften zum Prozessrecht

Band 254

Strafverfolgung und die Cloud

Strafprozessuale Ermächtigungsgrundlagen und
deren völkerrechtliche Grenzen

Von

Senta Bell



Duncker & Humblot · Berlin

Die Juristische Fakultät der Universität Würzburg
hat diese Arbeit im Sommersemester 2018
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.

Alle Rechte vorbehalten
© 2019 Duncker & Humblot GmbH, Berlin
Satz: L101 Mediengestaltung, Fürstenwalde
Druck: CPI buchbücher.de GmbH, Birkach
Printed in Germany

ISSN 0582-0219
ISBN 978-3-428-15620-7 (Print)
ISBN 978-3-428-55620-5 (E-Book)
ISBN 978-3-428-85620-6 (Print & E-Book)

Gedruckt auf alterungsbeständigem (säurefreiem) Papier
entsprechend ISO 9706 ☺

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

Vorwort

Die vorliegende Arbeit wurde im Sommersemester 2018 von der Juristischen Fakultät der Julius-Maximilians-Universität Würzburg als Dissertation angenommen. Für die Drucklegung wurde das Manuskript überarbeitet und auf den Stand von Juni 2018 gebracht.

An erster Stelle gebührt mein ganz besonderer Dank meinem Doktorvater Herrn Professor Dr. Frank Peter Schuster. Er stand mir während der gesamten Promotionszeit mit Rat und Tat zur Seite und hat durch seine klugen und konstruktiven Anmerkungen und wertvollen Hinweise ganz maßgeblich zum Gelingen dieser Arbeit beigetragen. Mein besonderer Dank gilt auch Herrn Professor Dr. Dr. Eric Hilgendorf, für die Erstellung des Zweitgutachtens.

Die Arbeit ist während meiner Zeit als wissenschaftliche Mitarbeiterin am Dekanat der Juristischen Fakultät der Julius-Maximilians-Universität Würzburg entstanden. Die Erstellung der Arbeit war für mich eine Herausforderung und eine außergewöhnlich bereichernde Erfahrung zugleich. Mein herzlicher Dank gilt den Menschen, die mich während dieser Zeit unterstützt und begleitet haben, insbesondere auch meinen lieben und geschätzten Kollegen, die mir bei der Erstellung der Arbeit in jeder erdenklichen Weise unterstützend zur Seite standen und dadurch ebenfalls maßgeblich am Gelingen der Arbeit beteiligt sind.

Ganz besonders danken möchte ich schließlich auch denjenigen Menschen, die während des Studiums zu besonderen Freunden wurden und nach dem Examen mit mir den Weg gemeinsam gegangen sind. Auch dank Euch werde ich die Promotionszeit immer in besonders schöner Erinnerung behalten.

Heilbronn, im Oktober 2018

Senta Bell

Inhaltsverzeichnis

Einleitung	15
I. Heranführung an den Untersuchungsgegenstand	16
II. Darstellung	17
<i>Erstes Kapitel</i>	
Grundlagen	
	19
A. Historie	19
B. Begriffsbestimmung	25
C. Technische Grundlagen	27
I. Servicemodelle	27
1. Infrastructure as a Service (IaaS)	28
2. Platform as a Service (PaaS)	28
3. Software as a Service (SaaS)	29
II. Erscheinungsformen	30
1. Public Cloud	30
2. Private Cloud	32
3. Hybrid Cloud	32
4. Community Cloud	33
III. Virtualisierung	33
1. Begriff	34
2. Virtuelle Maschine und Virtual Machine Monitor	35
3. Massenspeichervirtualisierung	36
IV. Résumé	37
D. Datenkategorisierung	38
I. Medienrechtliche Einordnung der beim Cloud Computing anfallenden Daten	39
1. Anwendbarkeit des TMG	39
2. Anwendbarkeit des TKG	40
a) Merkmale für Telekommunikationsdienste	40
b) Cloud-Angebote als Telekommunikationsdienste	41
c) Cloud Collaboration Tools als Telekommunikationsdienste	42
3. Zwischenergebnis	43
4. Bestandsdaten, § 14 Abs. 1 TMG	44
5. Nutzungsdaten, § 15 Abs. 1 TMG	44

6. Inhaltsdaten	45
II. Datenschutz nach der DSGVO	45
1. Räumlicher Anwendungsbereich	46
2. Sachlicher Anwendungsbereich	46
E. Lokalisierung der gespeicherten (Inhalts-)Daten	47
I. Durch den Nutzer	47
II. Durch den Cloud-Anbieter	48
III. Durch die Strafverfolgungsbehörden	49
F. Wesentliche Vor- und Nachteile des Cloud Computing – Tendenzen der Veränderung	49
I. Territorialer Kontrollverlust	50
II. Abhängigkeit von einer bestehenden Internetverbindung	51
G. Tatsächliche Zugriffsmöglichkeiten der Strafverfolgungsbehörden – denkbare Fallkonstellationen	52
I. Am Ort des verdächtigen Cloud-Nutzers	52
II. Am Ort des Cloud-Anbieters	54
III. In der Übertragungsphase	55
H. Résumé	56

Zweites Kapitel

Erarbeitung des rechtlichen Rahmens 58

A. Verfassungsrechtlicher Rahmen	58
I. Das Gebot des Vorbehalts des Gesetzes	58
II. Betroffene Grundrechte	60
1. Unverletzlichkeit der Wohnung, Art. 13 GG	60
2. Eigentumsfreiheit, Art. 14 GG	62
3. Berufsfreiheit, Art. 12 GG	64
4. Post- und Fernmeldegeheimnis, Art. 10 GG (Telekommunikationsgeheimnis)	65
a) Up- und Download der Daten als Telekommunikation im Sinne des Art. 10 Abs. 1 GG	66
b) Synchronisation der Daten als Telekommunikation im Sinne des Art. 10 Abs. 1 GG	67
c) Zugriff auf in der Cloud gespeicherte Inhalte als Telekommunikation im Sinne des Art. 10 Abs. 1 GG	68
d) Cloud Collaboration als Telekommunikation im Sinne des Art. 10 Abs. 1 GG	69
e) Zusammenfassung	71
5. Das Recht auf informationelle Selbstbestimmung, Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG	71

6. Das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG	73
B. Strafprozessuale Ermächtigungsgrundlagen und ihre Voraussetzungen	75
I. Maßnahmen am Ort des verdächtigen Cloud-Nutzers	76
1. § 102 StPO – Durchsuchung beim Verdächtigen	76
a) Zweck der Durchsuchung	77
b) Verdächtiger	78
c) Gegenstand der Durchsuchung	78
aa) Inbetriebnahme vorgefundener Endgeräte	80
bb) Überwinden der Zugangssicherung	81
cc) Zwischenergebnis – Durchsuchung „offline“	83
d) Verhältnismäßigkeit	84
e) Anordnung der Durchsuchung (§ 105 StPO)	84
aa) Inhalt	84
bb) Zuständigkeit	85
f) Beendigung der Durchsuchung	85
2. § 110 StPO – Durchsicht von Papieren und elektronischen Speichermedien	86
a) Zweck der Durchsicht	87
b) Zur Durchsicht befugte Personen	88
c) Mitnahme zur Durchsicht	90
d) Räumlich getrennte Speichermedien	91
aa) Entstehungsgeschichte	91
bb) Begriffsbestimmung „räumlich getrenntes Speichermedium“	92
cc) Arten von Daten	94
dd) Zugriff vom Speichermedium aus	95
ee) Kein Zugriff nach Mitnahme zur Durchsicht	98
ff) Zwischenergebnis – Zugriff „online“	99
gg) Zwischenergebnis – „Online-Durchsuchung light“	100
e) Verhältnismäßigkeit	101
f) Beendigung der Durchsicht	103
g) Auswirkungen der Durchsicht auf den Zeitpunkt der Beendigung der Durchsuchung	104
3. § 94 StPO – Sicherstellung und Beschlagnahme	105
a) Begriff	106
b) Der Sicherstellung unterliegende Gegenstände	107
aa) Körperliche Gegenstände	107
bb) Daten als nicht körperliche Gegenstände	107
c) Gewahrsam	109
aa) Allgemein	109
bb) Gewahrsam an Daten	109

d) Durchführung der Sicherstellung	112
e) Auswertung der sichergestellten Gegenstände	115
aa) „offline“	115
bb) „online“	116
cc) Desktopanwendungen	116
f) Verhältnismäßigkeit	117
g) Anordnung der Beschlagnahme, § 98 StPO	118
h) Beendigung	118
4. Online-Durchsuchung – § 100b StPO	120
a) Begriffsbestimmung	121
b) Gegenstand der Durchsuchung	122
c) Weitere Eingriffsvoraussetzungen	123
d) Betroffene der Maßnahme	124
aa) Bei einer exklusiv genutzten Cloud	125
bb) Bei einer gemeinsam genutzten Cloud	126
e) Schutz des Kernbereichs privater Lebensgestaltung	127
f) Anordnung der Online-Durchsuchung	128
aa) Form, Inhalt und Begründung	128
bb) Zuständigkeit	128
g) Beendigung, Verwendung und Berichtspflichten	129
II. Maßnahmen am Ort des Cloud-Anbieters im Bezug auf Inhaltsdaten	129
1. § 103 StPO – Durchsuchung bei Dritten	129
a) Der Cloud-Anbieter als „andere Person“	130
b) Erfolgsaussicht	132
c) Grundsatz der Verhältnismäßigkeit	132
d) Rechte des verdächtigen Cloud-Nutzers bei einer Durchsuchung am Ort des Cloud-Anbieters	133
aa) Anwesenheitsrecht gem. § 106 StPO	133
bb) Mitteilungspflichten gem. § 107 StPO	134
2. § 95 StPO – Herausgabeverlangen	136
a) Zuständigkeit	136
b) Gegenstand	137
c) Adressat	138
d) Verhältnismäßigkeit	139
III. Maßnahmen am Ort des Cloud-Anbieters im Bezug auf sonstige Daten	140
1. § 100g StPO – Verkehrsdatenauskunft	140
2. § 100j StPO – Bestandsdatenauskunft	141
a) Zuständigkeit	141
b) Adressat	142
c) Gegenstand des Auskunftsverlangens	143
d) Zwischenergebnis für in der Cloud gespeicherte Daten	143
3. §§ 161 Abs. 1, 163 Abs. 1 StPO	143

a) Umfang der Editionsspflicht	145
IV. Maßnahmen in der Übertragungsphase	146
1. § 100a StPO – Telekommunikationsüberwachung	146
a) Telekommunikation im Sinne des § 100a StPO	147
aa) Up- und Download als Telekommunikation im Sinne des § 100a StPO	147
bb) Cloud Collaboration als Telekommunikation im Sinne des § 100a StPO	148
b) Weitere Voraussetzungen	149
2. Quellen-Telekommunikationsüberwachung	150
a) Überwachung der Telekommunikation gemäß § 100a Abs. 1 S. 2 StPO	150
b) „Kleine Online-Durchsuchung“ gemäß § 100a Abs. 1 S. 3 StPO	152
V. Résumé zu den strafprozessualen Ermächtigungsgrundlagen	154

Drittes Kapitel

Völkerrechtliche Begrenzung der Ermittlungsbefugnisse 157

A. Das Territorialprinzip	158
B. Die Zulässigkeit extraterritorialer Ermittlungshandlungen	159
C. Der Zugriff auf im Ausland gespeicherte Daten	160
I. Allgemein	160
II. Öffentlich zugänglich gespeicherte Daten	161
1. Eingriff	162
2. Rechtfertigung	164
III. Nicht öffentlich zugänglich gespeicherte Daten	165
1. Eingriff	165
2. Rechtfertigung	165
a) Zugriff mit Zustimmung des Berechtigten	165
aa) Convention on Cybercrime	166
bb) Abseits der Convention on Cybercrime	167
b) Zugriff ohne Zustimmung des Berechtigten	168
aa) Convention on Cybercrime	168
bb) Abseits der Convention on Cybercrime	169
(1) Völkerrechtliche Übung	169
(2) Allgemeine völkerrechtliche Grundsätze	171
3. „Quick Freeze“	172
4. Ergebnis	173
D. Der Zugriff auf in der Cloud gespeicherte Daten bei grenzübergreifen- den Serververbunden	174
I. „Loss of (knowledge of) location“	174

II. Eingriff	176
1. Anknüpfungspunkt für die Beurteilung	176
2. Denkbare Fallkonstellationen	177
III. Rechtfertigung	178
1. Anwendbarkeit der Art. 31 f. der Convention on Cybercrime	178
2. Eigener Lösungsansatz	180
3. Abgrenzung zu den „Good faith“-Fällen	182
IV. Ergebnis	184
E. Herausgabeanspruch bezüglich im Ausland gespeicherter Daten	184
I. Eingriff	185
II. Rechtfertigung	185
1. Convention on Cybercrime	185
2. Abseits der Convention on Cybercrime	188
III. Weitere (datenschutz-)rechtliche Hürden	189
IV. Ergebnis	191
F. Résumé zur völkerrechtlichen Begrenzung der nationalen Ermittlungsbefugnisse	191

Viertes Kapitel

Untersuchung der Tragfähigkeit der bisherigen Ergebnisse und verbleibender Handlungsbedarf 195

A. Anwendung der bisherigen Ergebnisse auf die ausgewählten Fallkonstellationen	195
I. Zugriff beim verdächtigen Cloud-Nutzer	196
1. Auslesen des lokalen Datenbestands „offline“	196
a) Ohne Zugangssicherung vor Ort gemäß § 102 StPO	196
b) Ohne Zugangssicherung nach Mitnahme gemäß § 110 StPO	197
c) Mit Zugangssicherung vor Ort gemäß § 102 StPO	198
d) Mit Zugangssicherung nach Mitnahme	198
2. Beschlagnahme der gespeicherten Daten gemäß § 94 StPO	199
3. Auslesen „online“	201
a) Ohne Zugangssicherung vor Ort als Durchsicht gemäß § 110 Abs. 3 StPO	201
b) Ohne Zugangssicherung nach Mitnahme	202
c) Mit Zugangssicherung vor Ort als Durchsicht gemäß § 110 Abs. 3 StPO	202
d) Mit Zugangssicherung nach Mitnahme	203
4. Ausländischer Serverstandort	203
5. Grenzübergreifender Serververbund	205
6. Ausländischer grenzübergreifender Serververbund	206
7. Online-Durchsuchung gemäß § 100b StPO	207

II. Am Ort des Cloud-Anbieters	208
1. Zugriff am Ort des Cloud-Anbieters als Durchsuchung gemäß § 102 oder § 103 StPO	208
2. Nach Mitnahme des Cloud Servers als Beschlagnahme gemäß § 94 StPO	209
3. Herausgabeverlangen	210
a) Inhaltsdaten des Cloud-Nutzers gemäß § 95 StPO	210
b) Sonstige Daten (Bestands- und Nutzungsdaten) gemäß §§ 161 Abs. 1, 163 Abs. 1 StPO	211
c) Hinsichtlich im Ausland gespeicherter Daten gegenüber einem Anbieter mit Sitz in Deutschland	213
d) Hinsichtlich im Ausland gespeicherter Daten gegenüber einem Anbieter ohne Sitz in Deutschland	214
III. Zugriff in der Übertragungsphase	215
1. Überwachung des Datenübertragungsprozesses	215
2. Abfangen von Daten vor beziehungsweise nach dem Einsetzen des Verschlüsselungsprozesses als „Quellen-TKÜ“	217
B. Zusammenfassung und Bewertung der bisherigen Ergebnisse	218
I. Zusammenfassung der Ergebnisse	218
II. Bestehender Handlungsbedarf	220
1. Handlungsbedarf auf datenschutzrechtlicher Ebene	220
a) Verpflichtung des Anbieters zur Festlegung eines Server Pools ..	221
b) Verpflichtung des Anbieters zur Vorhaltung der Zugangsdaten in Klartext	222
2. Handlungsbedarf auf völkerrechtlicher Ebene	222
3. Entwurf eines zweiten Zusatzprotokolls zur Convention on Cyber- crime	224
Schlusswort	227
Literaturverzeichnis	230
Sachwortverzeichnis	251

Einleitung

„Ich mache mir wirklich große Sorgen, weil alles in die Datenwolke geht. Ich denke, es wird schrecklich. Wir werden innerhalb der nächsten fünf Jahre eine ganze Menge Probleme haben.“¹ Diese Worte stammen von *Steve Wozniak*, dem Mitbegründer von Apple, am Rande einer Theatervorstellung in der US-amerikanischen Hauptstadt Washington im Jahre 2012.

Der erste Teil von *Wozniaks* Warnung hat sich bereits bestätigt: Immer mehr Nutzer speichern ihre Daten in der Cloud. Allein Apple hat die Zahl seiner iCloud-Nutzer 2016 auf 782 Millionen ausgebaut.² Das 2008 gegründete Unternehmen Dropbox zählte im Juli 2016 500 Millionen Nutzer weltweit.³ 30 Millionen Nutzer alleine in Deutschland, Österreich und der Schweiz.⁴ Bis 2017 sollen 73% aller Daten „in der Wolke“ sein.⁵ Diese Zahlen belegen eindrücklich, dass Cloud-Dienste immer beliebter werden. Bei den Nutzern handelt es sich dabei nicht nur um Unternehmen, die den Vorteil nutzen, keine eigenen Ressourcen vorhalten zu müssen, sondern vor allem auch um Private, die mit dem angemieteten Cloud-Speicher die heimische Festplatte ersetzen oder ihre Endgeräte synchronisieren.

Diese Weiterentwicklung führt dazu, dass Ermittlungsbehörden bei ihrer Arbeit zwangsläufig zunehmend mit Cloud-Lösungen in Berührung kommen. Waren beweisrelevante Gegenstände bei einer Durchsuchung zunächst noch in körperlicher Form in den Räumen des Verdächtigen zu finden, werden die Informationen längst digital gespeichert. Nutzt der Verdächtige einen Cloud-Dienst und speichert so seine Daten über ein externes Datennetz, werden die zuständigen Behörden beim Verdächtigen nur ein Endgerät vorfinden, auf dem möglicherweise nichts gespeichert ist, über welches sie aber auf eine Cloud zugreifen können.

¹ Zitiert nach *Fuest*, Die Welt vom 11.08.2012, <https://www.welt.de/finanzen/article108575608/Wie-die-Datenwolke-zum-Albtraum-der-Nutzer-wird.html> (zuletzt besucht am 20.03.2018).

² *Beiersmann* ZDNet, 15.02.2016.

³ Quelle Dropbox: <https://de.statista.com/statistik/daten/studie/326447/umfrage/anzahl-der-weltweiten-dropbox-nutzer/> (zuletzt besucht am 20.03.2018).

⁴ Heise Online: <https://www.heise.de/newsticker/meldung/Dropbox-eroeffnet-erste-deutsche-Niederlassung-in-Hamburg-3213322.html> (zuletzt besucht am 20.03.2018).

⁵ *Kroker*, Wirtschaftswoche vom 12.08.2015.

Die vorliegende Arbeit widmet sich der Untersuchung, ob auch die Strafverfolgungsbehörden bei Ermittlungen „in der Cloud“ – um es mit *Wozniaks* Worten zu sagen – „eine ganze Menge Probleme haben“ und wie diese zu lösen sind.

I. Heranführung an den Untersuchungsgegenstand

Hinter dem Konzept des Cloud Computing verbirgt sich zwar keine neue Technik, jedoch eine neue Geschäftsidee, IT-Ressourcen nicht mehr zu besitzen, sondern sie bei Bedarf zuzuschalten, sie als Dienstleistung zu beziehen.⁶ Die hinter dem Cloud Computing stehende Virtualisierungstechnik abstrahiert logische Systeme von der physischen Implementierung. Datenspeicherungen oder Programmabläufe werden daher nicht mehr einem klar zu lokalisierenden Server, sondern schlicht der „Cloud“ zugeordnet.⁷ Auch wenn alle Vorgänge in der Cloud letztendlich auf eine physische Hardware zurückgeführt werden können, über die ein territorialer Bezug hergestellt werden kann, bereitet die Festlegung eines territorialen Anknüpfungspunktes große Probleme. Die Daten eines Nutzers werden meist nicht en bloc, sondern als Datenversatzstücke gespeichert. Um bei Störungen Dienstunterbrechungen zu vermeiden, legt der Cloud-Anbieter meist noch Sicherungskopien der gespeicherten Daten an, welche wiederum bruchstückhaft gespeichert werden. Auf welche Daten dann im Falle eines Abrufs tatsächlich zugegriffen wird, entscheidet die Virtualisierungstechnik nach Kapazitätsgesichtspunkten.

Für die Wahl der strafprozessualen Ermächtigungsgrundlage ist der tatsächliche Speicherort der Daten jedoch zunächst zweitrangig. Weder die Vorschriften zur Durchsuchung (§§ 102 ff. StPO) und Beschlagnahme (§§ 94 ff. StPO) noch die auf die Herausgabe von Daten gerichteten Normen (§ 95 StPO beziehungsweise §§ 161 Abs. 1, 163 Abs. 1 StPO) oder die Vorschriften zu den heimlichen Ermittlungsmaßnahmen (§ 100a und § 100b StPO) setzen einen bestimmten Speicherort der in Rede stehenden Daten voraus. Dennoch sind die Maßnahmen der Strafverfolgungsbehörden grundsätzlich auf das eigene Hoheitsgebiet beschränkt. Dies ergibt sich aus völkerrechtlichen Grundsätzen, namentlich dem Territorialprinzip, an welches die Ermittlungsbehörden gebunden sind. Findet ein Eingriff in fremde Souveränitätsrechte statt, bedarf dieser einer völkerrechtlichen Rechtfertigung. Ein Eingriff in fremde Hoheitsrechte setzt dabei keinesfalls voraus, dass der Hoheitsakt auf fremdem Staatsgebiet vorgenommen wird, die Behörden sich also physisch auf fremdes Staatsgebiet begeben. Ein Eingriff in fremde Hoheitsrechte liegt möglicherweise bereits dann vor, wenn eine Handlung aus

⁶ Vgl. *Schorer*, in: Hilber, Teil 1 C, Rn. 7.

⁷ So: *Giedke*, Cloud Computing, S. 48; *Lehmann/Giedke*, CR 2013, 608 (611).

dem Inland in fremdes Hoheitsgebiet hineinwirkt. Dies wäre vielleicht auch schon dann der Fall, wenn deutsche Strafverfolgungsbehörden von einem Rechner im Inland auf im Ausland gespeicherte Daten zugreifen. Eine Verletzung fremder Hoheitsrechte liegt ebenfalls vor, wenn die Ermittlungsbehörden eine Person – egal wo sich diese aufhält – zur Herausgabe von im Ausland gespeicherten Daten auffordern, denn in beiden Fällen werden Datenverarbeitungsprozesse im Ausland in Gang gesetzt, die – zumindest mittelbar – auf das Verhalten der Ermittlungsbehörden zurückzuführen sind.

II. Darstellung

Um sämtliche Ermittlungsmöglichkeiten der Strafverfolgungsbehörden im Zusammenhang mit dem Cloud Computing einer rechtlichen Beurteilung zuführen zu können, muss zunächst einmal festgestellt werden, in welchen Situationen die Behörden mit Cloud-basierten Diensten in Berührung kommen können. Im ersten Teil der Arbeit sollen daher zunächst die für die rechtliche Beurteilung der strafprozessualen Ermittlungsmöglichkeiten notwendigen Grundlagen des Cloud Computings erarbeitet werden. Nach einem kurzen Überblick über die historische Entwicklung, der Technologie und der Begriffsbestimmung findet eine Darstellung der technischen Grundlagen statt. Neben den einzelnen Servicemodellen und den verschiedenen Erscheinungsformen werden insbesondere die Virtualisierungstechnik und die damit verbundenen Schwierigkeiten der Lokalisierbarkeit der in der Cloud gespeicherten Daten eingehend beleuchtet. Anschließend werden die beim Cloud Computing anfallenden Daten medienrechtlich kategorisiert. Nach dieser Darstellung wird deutlich, wann die Behörden mit der Cloud des Verdächtigen in Berührung und welche tatsächlichen Zugriffsmöglichkeiten als ermittlungstechnische Ansatzpunkte in Betracht kommen. Zum Ende des ersten Kapitels werden daher denkbare Fallkonstellationen aufgeworfen, die im Fortgang der Arbeit unter allen Aspekten beleuchtet werden. Dabei wird stets davon ausgegangen, dass es sich bei dem Nutzer des Cloud-Dienstes um den Verdächtigen handelt, gegen den das Ermittlungsverfahren eingeleitet beziehungsweise die spätere Hauptverhandlung geführt werden soll. Die Untersuchung beschränkt sich dabei auf die Ermittlungen gegen Nutzer von Storage as a Service (StaaS)- beziehungsweise Infrastructure as a Service (IaaS)-Angeboten. Die denkbaren Fallkonstellationen werden einer Grobgliederung unterworfen, die für die weitere Struktur der Arbeit prägend ist. Anknüpfungspunkt ist der Zugriff am Ort des verdächtigen Cloud-Nutzers selbst über den unverdächtigen Cloud-Anbieter und in der Phase der Übertragung der Daten in und aus der Cloud.