Inhaltsverzeichnis

Abkürzungshinweise IV

Vorwort V

A. Einleitung 1

B. Technische Grundlagen 6

I. Definition und grundlegende Charakteristika 6

1. Ressource-Pooling 6

2. Rapid Elasticity 7

3. On Demand self-service 8

4. Broad network-access 8

5. Measured service 9

II. Abgrenzung zu ähnlichen Technologien 9

1. Verteilte Systeme: Cluster- und Grid-Computing 10

2. IT-Outsourcing 11

3. Das Application-Service-Provider-Modell 11

4. Utility-Computing 12

III. Service-Modelle 12

1. Software-as-a-Service (SaaS) 13

2. Platform-as-a-Service (PaaS) 14

3. Infrastructure-as-a-Service (IaaS) 14

IV. Verschiedene Arten von Clouds 15

1. Öffentliche Cloud 15

2. Nichtöffentliche Cloud 16

3. Community-Cloud 17

4. Hybride Cloud 17

V. Technische Grundvoraussetzungen für Cloud Computing 18

1. (Breitband-)Internet, Hochleistungsserver, Multicore-Prozessoren und Web 2.0 18

2. Virtualisierung 20

VI. Technische Einzelheiten 21

1. Anforderungen an Cloud-Systeme und charakteristische Merkmale 21

a) Transparenz 21

b) Ausfallsicherheit und hohe Verfügbarkeit 22

c) Elastizität und Skalierbarkeit 23

2. Datensicherheit 23

a) Grundsätzliches 23

b) Datensicherungsstrategie ... 24
c) Arten der Datensicherung und Speichermedien ... 24
3. Datenlokalität ... 27
VII. Zusammenfassende Problemfokussierung und weiterer Gang der Untersuchung ... 29

C. Der verfassungsrechtliche Rahmen strafprozessualer Ermittlungsmaßnahmen ... 33
I. Verfassungsrechtliche Vorüberlegungen ... 33
1. Gesetzesvorbehalt und Eingriffsnorm ... 36
a) Allgemeiner Eingriffsvorbehalt und Wesentlichkeitskriterium ... 36
b) Analogieverbot und Bestimmtheitsgebot im Verfahrensrecht ... 40
2. Konsequenz: Notwendigkeit einer bereichsspezifischen Eingriffsnorm ... 44
II. Zwischenergebnis und Folgerungen für die Untersuchung 45

D. Strafprozessualer Zugriff auf Cloud Computing-Systeme *de lege lata* ... 46
I. § 94 StPO als Grundlage für Ermittlungen in Cloud Computing-Systemen ... 47
1. Mögliche Beschlagnahmegegenstände in Cloud-Sachverhalten ... 48
a) Hardware und Speichermedien als Beschlagnahmegegenstände ... 48
b) Daten als Beschlagnahmeobjekte ... 49
aa) Die ablehnende Ansicht von Bär ... 49
bb) Die bejahende Ansicht des BVerfG und der h. L. ... 50
cc) Stellungnahme ... 51
c) Verfahrensweisen zur Sicherstellung von Daten ... 52
2. Der Zugriff auf beim Provider zwischengespeicherte E-Mails als Blaupause für Cloud-Sachverhalte? ... 56
a) Technische Grundlagen der E-Mail-Kommunikation ... 56
aa) Übertragung zum Mail(out)Server ... 57
bb) Übertragung zum Mail(in)Server ... 57
cc) Der Abruf der E-Mail durch den Empfänger ... 58

b) Rechtsprechung und Schrifttum zum E-Mail-Zugriff im Überblick ... 58
aa) Hintergrund: Die Einteilung der E-Mail-Kommunikation in „Phasen“ ... 58
bb) E-Mail-Zugriff zwischen Beschlagnahme und TKÜ ... 61
(a) Rechtsprechung ... 61
(b) Literatur ... 63
(aa) Das Meinungsbild vor BVerfG NJW 2009, 2431 ff. ... 64
(bb) Die Reaktionen im Schrifttum auf BVerfG NJW 2009, 2431 ff. ... 67
(cc) Keine Ermächtigungsgrundlage für den Zugriff auf E-Mails ... 68
c) Folgerungen für die vorliegende Untersuchung ... 70
3. Die Unzulänglichkeit der §§ 94 ff. StPO als Ermächtigung zum Eingriff in die Cloud ... 71
a) „IT-spezifische“ Gefährdungslage in Cloud-Sachverhalten ... 72
aa) Das neue Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ... 72
(a) Schutzbereich ... 72
(aa) Schutz des Systems als System ... 73
(bb) Negative Abgrenzung: Das Verhältnis zu den Art. 2 Abs. 1, 10, 13 GG ... 75
(1) Art. 13 GG ... 76
(2) Art. 10 GG ... 78
(3) Recht auf informationelle Selbstbestimmung ... 80
(cc) Bestimmung des Schutzbereichs vom Eingriff her ... 81
(dd) Die Cloud als System i. S. d. IT-Grundrechts ... 82
(b) Schranken ... 84
bb) Untauglichkeit der Beschlagnahmevorschriften als Ermächtigungsnorm für den Zugriff auf die Cloud ... 87

cc) Zwischenergebnis: Unanwendbarkeit der §§ 94 ff. StPO ... 91
II. §§ 99 f. StPO (Postbeschlagnahme) ... 91
1. Norminhalt ... 92
2. Keine Anwendbarkeit beim Zugriff auf die Cloud ... 94
III. § 100a StPO (Überwachung der Telekommunikation) ... 96
1. Zur großen praktischen Relevanz der TKÜ in Cloud-Sachverhalten ... 97
2. Der Telekommunikationsbegriff ... 99
a) Der strafprozessuale Telekommunikationsbegriff ... 99
aa) Grundlagen ... 99
bb) Erweiterungen ... 101
b) Der Telekommunikationsbegriff im TKG ... 104
c) Eigene Stellungnahme zum Telekommunikationsbegriff ... 105
aa) Die Anwendung des Methodenkanons ... 105
bb) Grundrechtsspezifische Aspekte ... 109
cc) Probleme des Kernbereichsschutzes ... 112
dd) Abschließende kritische Würdigung ... 113
3. Zwischenergebnis ... 115
IV. Online-Durchsuchung und Quellen-TKÜ (§§ 100a Abs. 1 S. 2, S. 2, 100b StPO n.F.) ... 115
1. Die Rechtslage bis zum 24.08.2017 ... 116
a) Quellen-TKÜ ... 117
aa) Begriff und technischer Hintergrund ... 117
bb) Rechtliche Bewertung in Rechtsprechung und Schrifttum ... 118
cc) Bewertung des Diskussionsstandes ... 121
b) Die Online-Durchsuchung: Technische Grundlagen und rechtliche Bewertung vor der Neuregelung in § 100b StPO ... 123
aa) Technische Grundlagen ... 124
bb) Rechtliche Bewertung nach alter Rechtslage ... 128
(a) Strafrechtliche Rechtsprechung zur „Online-Durchsuchung" ... 128
(aa) Beschl. des Ermittlungsrichters v. 21.2.2006, StV 2007, 60 ... 128

(bb) Beschl. des Ermittlungsrichters vom 25.11.2006 129
(cc) BGH Beschl. v. 31.1.2007..... 130
(b) Die Behandlung der strafprozessualen Online-Durchsuchung im Schrifttum..... 132
2. Die Neuregelung durch das Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens . 137
a) Quellen-TKÜ nach §§ 100a Abs. 1 S. 2 und S. 3 StPO 138
aa) Inhalt der Neuregelung im Überblick..... 138
bb) Kritische Würdigung..... 139
b) Online Durchsuchung nach § 100b StPO n. F..... 143
aa) Inhalt der Neuregelung im Überblick..... 143
bb) Kritische Würdigung..... 144
V. § 110 Abs. 3 StPO und die transnationale Dimension des Zugriffs auf in der Cloud gespeicherte Daten..... 148
1. Die Anwendbarkeit von § 110 Abs. 3 StPO beim Zugriff auf inländische Clouds 149
2. § 110 Abs. 3 StPO und grenzüberschreitender Zugriff . 152
a) Der Souveränitätsgrundsatz..... 154
aa) Allgemeines 154
bb) Mögliche Rechtfertigungen bei Verstößen 155
(a) Gewohnheitsrecht..... 156
(b) Völkerrechtliche Vereinbarungen: Die Cybercrime-Konvention..... 157
b) Jüngste europäische Entwicklungen: Das Marktortprinzip 162
aa) Allgemeiner Inhalt des Kommissionsvorschlags 162
bb) Konkrete Ausgestaltung und Verfahren..... 165
cc) Kritische Würdigung..... 167
(a) Mangelnder Grundrechtsschutz 169
(b) Verstoß gegen den Souveränitätsgrundsatz. 170
(c) Beschränkung des einseitigen Vorgehens auf die Sicherungsanordnung..... 173
VI. Zusammenfassung der Ergebnisse: Derzeit keine Ermächtigungsgrundlage für Zugriff auf in der Cloud gespeicherte Daten/Übergangszeit 174

E. Verwertbarkeit unzulässig erlangter Daten 177
I. Grundlagen und Begrifflichkeiten..... 177
1. Der Aufklärungsgrundsatz..... 177
2. Die unterschiedlichen Kategorien der Beweisverbote.. 178
a) Kurzer Überblick über die Begrifflichkeiten..... 178
b) Zur Relevanz selbstständiger Beweisverwertungsverbote im vorliegenden Zusammenhang 179
II. Die unselbstständigen Beweisverwertungsverbote..... 183
1. Die Rechtsprechung (insbesondere Abwägungslehre) . 184
2. Einzelne Ansätze aus der Literatur im Überblick 186
III. Beweisverwertungsverbote bei Verstößen gegen Rechtshilfevorschriften..... 187
IV. Eigene Stellungnahme für die vorliegende Fallgruppe... 188
F. Zusammenfassung der Ergebnisse 191
Literaturverzeichnis XIII