

# Inhaltsüberblick

<b>Geleitwort.....</b>	<b>VII</b>
<b>Vorwort .....</b>	<b>IX</b>
<b>Erstes Kapitel: Einleitung.....</b>	<b>1</b>
A. Bedeutung der Thematik.....	1
B. Gegenstand der Untersuchung.....	2
C. Gegenstand der Untersuchung.....	7
<b>Zweites Kapitel: Straftaten im Internet – Ausgangspunkt strafprozessualer Ermittlungsmaßnahmen.....</b>	<b>11</b>
A. Kriminalität im und durch das Internet .....	11
B. Strafverfolgung im Internet im Kontext des Cybercrime.....	21
C. Bedeutung der Grundrechte für die Strafverfolgung im Internet.....	27
<b>Drittes Kapitel: Ermittlungsmaßnahmen im Internet – ein Überblick.....</b>	<b>39</b>
A. „Online-Streife“ – jede Recherche in Datennetzen?.....	40
B. Ausforschung sozialer Netzwerke.....	46
C. Die Auskunftsersuchen nach TMG, TKG und StPO .....	56
D. Überwachung der Telekommunikation.....	90
E. Einordnung des Zugriff auf „ruhende“ E-Mails beim Provider: Überwachung oder Beschlagnahme? .....	116
F. Rechtsprobleme bei Online-Durchsuchung und Quellen-Telekommunikationsüberwachung.....	134
<b>Viertes Kapitel: Einführung in das Cloud Computing .....</b>	<b>147</b>
A. Begriff und Architektur .....	148
B. Cloud Storage.....	159
C. Cloud Computing als Wirtschaftsfaktor.....	163
D. Rechtsfragen .....	170
E. Zusammenfassung.....	181

<b>Fünftes Kapitel: Zugriff der Strafverfolgungsbehörden auf Cloud-Speicher .....</b>	<b>183</b>
A. Möglichkeiten des Zugriffs auf Daten in der Cloud .....	183
B. Anwendung der herkömmlichen Ermittlungsmaßnahmen auf Clouds.....	187
C. Offener Zugriff auf Cloud Speicher gem. §§ 94 ff. StPO .....	212
D. Heimlicher Zugriff auf Cloud Storage Daten .....	215
E. Überwachung und Abfangen der Cloud-Kommunikation.....	225
F. Zusammenfassung .....	229
<b>Sechstes Kapitel: Internationale und transnationale Aspekte des Zugriffs auf Cloud Storage .....</b>	<b>233</b>
A. Praktische Probleme der Strafverfolgung in Clouds .....	234
B. Rechtliche Probleme der Strafverfolgung in Clouds.....	246
C. Lösungsmöglichkeiten .....	250
D. Exkurs: Bedeutung für die Befugnisse von Nachrichtendiensten .....	264
<b>Siebtes Kapitel: Ergebnisse und Zusammenfassung .....</b>	<b>267</b>
A. Generelle Forderungen zur Strafverfolgung im Internet .....	268
B. Die herausgehobene Bedeutung des IT-Grundrechts.....	271
C. Möglichkeiten, Herausforderungen und Chancen? .....	273
<b>Literaturverzeichnis .....</b>	<b>275</b>

# Inhaltsverzeichnis

**Geleitwort.....**.....VII

**Vorwort .....**.....IX

<b>Erstes Kapitel: Einleitung.....</b>	<b>1</b>
A. Bedeutung der Thematik.....	1
B. Gegenstand der Untersuchung.....	2
I. Notwendigkeit einer Auseinandersetzung .....	2
II. Die besondere Berücksichtigung des Cloud Storage.....	4
III. Rechtliche Auseinandersetzung mit dem behördlichen Zugriff in Clouds .....	5
IV. Probleme durch die externe Datenspeicherung in Clouds .....	6
C. Gegenstand der Untersuchung.....	7

## **Zweites Kapitel: Straftaten im Internet – Ausgangspunkt**

<b>strafprozessualer Ermittlungsmaßnahmen.....</b>	<b>11</b>
A. Kriminalität im und durch das Internet .....	11
I. Internet als Zuständigkeitsraum staatlicher Behörden.....	12
1. Internet als Zuständigkeitsraum der Strafverfolgungsbehörden.....	13
2. Rechtsquellen für die Strafverfolgung im Internet .....	14
3. Das Internet – kein rechtsfreier Raum .....	14
II. Straftaten im und durch das Internet – „Cybercrime“ als deutscher Rechtsbegriff .....	15
1. Begriff der Computer- und Internetkriminalität .....	16
a) Informations- und Kommunikationstechnologie- Kriminalität .....	17
b) Neuere Begriffsverwendung: Cybercrime (im engeren und weiteren Sinne) .....	18
c) Tatmittel Internet – „Katalysationseffekt des Internet“.....	19
d) Zusammenfassung .....	19
2. Cybercrime in der Bundesrepublik Deutschland .....	20
B. Strafverfolgung im Internet im Kontext des Cybercrime.....	21
I. Sinn und Zweck der Strafverfolgung im Internet.....	21

1.	Strafverfolgung des Cybercrime im engeren Sinne .....	21
2.	Strafverfolgung des Cybercrime im weiteren Sinne .....	22
3.	Strafverfolgung nicht-internetspezifischer Straftaten entlang der Kommunikationswege .....	22
4.	Erhöhtes Gefahrenpotential durch neue Kommunikationsformen .....	23
5.	Zusammenfassung .....	23
II.	Daten als Zugriffsobjekt .....	24
1.	Terminologie .....	25
a)	Bestandsdaten .....	25
b)	Verkehrsdaten .....	25
c)	Inhaltsdaten .....	26
2.	Zusammenfassung .....	27
C.	Bedeutung der Grundrechte für die Strafverfolgung im Internet .....	27
I.	Anwendbarkeit der klassischen grundrechtlichen Bereichsabgrenzung im Zeitalter digitaler Konvergenz .....	28
1.	Der Begriff „digitale Konvergenz“ .....	28
2.	Grundrechtsbetroffenheit im Rahmen der Strafverfolgung im Internet .....	29
II.	Das Brief-, Post- und Fernmeldegeheimnis .....	30
1.	Schutzbereich .....	30
2.	Eingriffe .....	31
III.	Das Recht auf informationelle Selbstbestimmung .....	32
1.	Schutzbereich .....	32
2.	Eingriffe .....	33
IV.	Das Recht auf Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme .....	33
1.	Schutzbereich .....	34
2.	Eingriffe .....	34
V.	Unverletzlichkeit der Wohnung .....	35
VI.	Konkurrenzen .....	36
VII.	Fazit .....	37

<b>Drittes Kapitel: Ermittlungsmaßnahmen im Internet – ein Überblick .....</b>	<b>39</b>
A. „Online-Streife“ – jede Recherche in Datennetzen? .....	40
I. Die anlassunabhängige Recherche in Datennetzen – „echte Online-Streife“ .....	41
1. Praktische Durchführung .....	42
2. Rechtsgrundlagen .....	42

II.	Die anlassbezogene Recherche in Datennetzen – „unechte Online-Streife“.....	43
1.	Praktische Durchführung.....	43
2.	Rechtsgrundlagen.....	44
III.	Ergebnis.....	45
B.	Ausforschung sozialer Netzwerke.....	46
I.	Praktische Durchführung der Ausforschung sozialer Netzwerke.....	46
II.	Rechtsgrundlagen.....	47
1.	Abgrenzung: Nicht offen ermittelnder Polizeibeamter (NoeP) – verdeckter Ermittler .....	47
1.1	a) Schutzwürdiges Vertrauen zwischen Teilnehmern sozialer Netzwerke? .....	48
1.2	b) Prüfungsraster: Schutzwürdiges Vertrauen im Internet .....	53
2.	Ergebnis: Abgrenzung NoeP – verdeckter Ermittler .....	53
3.	Fazit.....	55
C.	Die Auskunftsersuchen nach TMG, TKG und StPO .....	56
I.	Regelungsgehalt und Einordnung der Auskunftsersuchen.....	56
1.	Sinn und Zweck der Durchführung von Auskunftsersuchen .....	56
2.	Grundrechtseingriffe durch den Zugriff auf Daten im Auskunftsverfahren .....	57
3.	Zugriffsmöglichkeiten nach TKG, TMG und StPO.....	58
3.1	a) Anwendbarkeit des TKG .....	58
3.2	b) Geltung des TMG .....	59
3.3	c) Überschneidungen und Grenzfälle.....	60
3.4	d) Zugriffsmöglichkeiten nach StPO.....	61
II.	Die Auskunftsersuchen nach TMG .....	61
III.	Auskunftsersuchen nach TKG – die „Bestandsdatenauskünfte“ .....	62
1.	Das automatisierte Auskunftsverfahren gem. § 112 TKG .....	63
1.1	a) Verpflichtete .....	63
1.2	b) Abrufbare Daten gem. § 111 TKG .....	64
1.3	c) Verfahren .....	68
2.	Das manuelle Auskunftsverfahren gem. § 113 TKG i.V.m. § 100j StPO.....	69
2.1	a) Verpflichtete .....	69
2.2	b) Abrufbare Daten .....	70
2.3	c) Verfahren .....	74
IV.	Auskunftsersuchen nach StPO – die Verkehrsdatenabfrage gem. § 100g StPO .....	75
1.	Voraussetzungen.....	76
1.1	a) Adressat.....	76
1.2	b) Tatverdacht einer Straftat .....	76

2.	Abrufbare Daten .....	77
a)	Verkehrsdaten i.S.d. § 113a TKG .....	77
b)	Verkehrsdaten i.S.d. § 96 TKG .....	84
c)	Ergebnis: Keine beschränkte Vorratsdatenspeicherung für dynamische IP-Adressen .....	89
D.	Überwachung der Telekommunikation .....	90
I.	Anwendungsbereich des § 100a StPO .....	91
1.	Begriff der Telekommunikation .....	91
2.	Eingriff in das Telekommunikationsgeheimnis .....	93
3.	Anwendung auf spezielle Arten der Datenkommunikation .....	94
II.	Voraussetzungen .....	95
1.	Adressat der Maßnahme .....	95
2.	Tatverdacht einer Katalogstrafat, § 100a Abs. 2 StPO .....	95
a)	Verdachtsbegründung durch bestimmte Tatsachen .....	96
b)	Beteiligter einer schweren Straftat .....	96
c)	Anlasstat gem. Straftatenkatalog, § 100a Abs. 2 StPO .....	97
3.	Subsidiarität und Verhältnismäßigkeit .....	97
4.	Formelles Verfahren nach § 100b StPO .....	98
5.	Technische und organisatorische Voraussetzungen .....	98
III.	Anwendung des § 100a StPO auf die verschiedenen Arten der Internetkommunikation .....	99
1.	Überwachung des Surfverhaltens (Website-Aufrufe) .....	99
a)	Funktionsweise des HTTP .....	100
b)	Rechtsgrundlage .....	101
2.	Abfangen von Daten bei Nutzung des File-Transfer-Protocol .....	101
3.	Überwachung der W-LAN-Kommunikation .....	102
a)	Rechtsgrundlage .....	102
c)	Fazit: Keine Verwertung der gesamten Internetkommunikation .....	106
4.	Abfangen von E-Mails während des Übertragungsvorgangs .....	107
a)	Technische Funktionsweise des E-Mail-Verkehrs .....	108
b)	Einteilung in „Übermittlungsphasen“ .....	110
c)	Rechtsgrundlagen für den Zugriff in den Übermittlungsphasen .....	111
d)	Vereinfachung durch „Phasenmodelle“ .....	113
e)	Fazit: Begrenzter Nutzen von Phasen-Modellen .....	115
5.	Zugriff auf E-Mails außerhalb der Übermittlungsphasen .....	115
E.	Einordnung des Zugriff auf „ruhende“ E-Mails beim Provider: Überwachung oder Beschlagnahme? .....	116
I.	Beschluss des BGH vom 31.03.2009 – 1 StR 76/09 .....	117
1.	Argumentation des BGH .....	117

2. E-Mail-Beschlagnahme analog zur Postbeschlagnahme gem. § 99 StPO.....	118
II. Beschluss des BVerfG vom 16.06.2009 – 2 BvR 902/06 .....	119
1. achverhalt und Verfahrensgang .....	119
a) Auffassungen der Beteiligten .....	119
b) Rüge des Beschwerdeführers .....	120
2. Argumentation des BVerfG .....	120
a) Eingriff in das Telekommunikationsgeheimnis.....	121
b) Beschlagnahmeregelungen als geeignete Rechtsgrundlage für den Zugriff beim Provider .....	121
III. Rechtliche Würdigung der höchstrichterlichen Rechtsprechung .....	122
1. Würdigung des Beschlusses des BGH.....	123
2. Würdigung des Beschlusses des BVerfG .....	125
3. Fazit.....	128
4. Neuregelungsvorschlag für die heimliche E-Mail- Beschlagnahme .....	131
IV. Zusammenfassung: Zugriffsvoraussetzungen bei der offenen und der verdeckten Beschlagnahme.....	132
1. Offene Beschlagnahme von E-Mails nach §§ 94, 98 StPO .....	132
2. Verdeckter Zugriff auf E-Mails nach § 100a StPO .....	133
F. Rechtsprobleme bei Online-Durchsuchung und Quellen- Telekommunikationsüberwachung .....	134
I. Online-Durchsuchung .....	134
1. Begriff der Online-Durchsuchung .....	134
2. Unzulässigkeit der Online-Durchsuchung .....	135
II. Quellen-Telekommunikationsüberwachung .....	137
1. Begriff der Quellen-TKÜ.....	137
2. Rechtliche Grundlage .....	138
a) Zulässigkeit der Quellen-TKÜ nach § 100a StPO .....	138
b) Unzulässigkeit der Quellen-TKÜ .....	139
c) Vorzugswürdige Ansicht.....	139
3. Quellen-TKÜ gem. § 100a StPO: Korrektur durch die Inhaltlösung .....	144
<b>Viertes Kapitel: Einführung in das Cloud Computing .....</b>	<b>147</b>
A. Begriff und Architektur .....	148
I. Definition .....	148
1. Begriffsherkunft .....	148
2. Definitionsansätze .....	149
3. Definitionsvorschlag.....	150
II. Historie und Grundlagen des Cloud Computing .....	151

1. Entwicklung .....	151
2. Grundlagen.....	152
III. Architektur des Cloud Computing .....	154
1. Servicemodelle .....	154
a) Infrastructure-as-a-Service (IaaS) .....	154
b) Software-as-a-Service (SaaS) .....	154
c) Platform as a Service (PaaS).....	155
d) Everything-as-a-Service (EaaS).....	155
e) Weitere Service-Modelle.....	156
2. Liefermodelle .....	156
a) Private Cloud .....	157
b) Public Cloud .....	157
c) Community Cloud.....	158
d) Hybrid Cloud .....	158
B. Cloud Storage.....	159
I. Definition und Leistungsmerkmale des Cloud Storage .....	159
II. Service-Modell des Cloud Storage.....	161
III. Liefer-Modell des Cloud Storage .....	162
C. Cloud Computing als Wirtschaftsfaktor.....	163
I. Vorteile des Cloud Computing .....	163
1. Virtualisierung.....	163
2. Utility Computing.....	164
3. Ausfallsicherheit.....	165
II. Wachstumsprognosen.....	165
III. Cloud -Dienste: Beispiel aus Wirtschaft und Gesellschaft .....	166
1. SaaS: Salesforce .....	167
2. IaaS: Hewlett Packard.....	167
3. Cloud Storage: Dropbox .....	168
4. Facebook, Twitter, GMX, Rapidshare und Spotify .....	169
D. Rechtsfragen.....	170
I. Vertragstypologische Einordnung.....	171
1. Vertragstypologische Einordnung des Cloud Computing Vertrags.....	171
2. Vertragstypologische Einordnung des Cloud Storage Vertrags.....	172
II. Daten- und Datenschutzrecht.....	174
1. Cloud Computing-Dienste: Telekommunikations- oder Telemediendienst?.....	174
2. Sonderfall des Cloud Storage .....	176
3. Anwendung des BDSG .....	179
4. Ergebnis .....	179

III. Strafverfolgung.....	180
E. Zusammenfassung.....	181
<b>Fünftes Kapitel: Zugriff der Strafverfolgungsbehörden auf Cloud-Speicher .....183</b>	
A. Möglichkeiten des Zugriffs auf Daten in der Cloud .....	183
I. Praktische Möglichkeiten und rechtliche Ansatzpunkte des Zugriffs auf Cloud-Speicher .....	184
1. Zugriff auf Inhaltsdaten beim Cloud Provider .....	184
2. Zugriff auf Inhaltsdaten beim Nutzer .....	185
3. Abfangen der Daten auf dem Weg in die Cloud.....	186
4. Auskünfte über die Nutzung einer Cloud.....	186
II. Verfassungsrechtliche Rahmenbedingungen des Zugriffs auf Daten in der Cloud .....	186
B. Anwendung der herkömmlichen Ermittlungsmaßnahmen auf Clouds.....	187
I. „Online-Streife“ in der Cloud und Ausforschung der Cloud .....	188
II. Die Bedeutung der Bestandsdatenauskünfte für Cloud Storage Daten .....	189
1. Die Bestandsdatenauskünfte und das Cloud Storage: TMG oder TKG?.....	190
2. Bedeutung der Auskunftsverfahren des TKG für das Cloud Storage.....	191
a) Anwendung des automatisierten Auskunftsverfahren gem. § 112 TKG auf das Cloud Storage.....	192
b) Anwendung des manuellen Auskunftsverfahrens gem. § 113 TKG auf das Cloud Storage .....	196
3. Ergebnis.....	202
III. Bedeutung der Verkehrsdatenabfrage gem. § 100g StPO für Cloud Dienste .....	203
1. Auskunft über die Nutzung eines Cloud Speichers .....	203
2. Auskunft über die Nutzeranzahl der Cloud: Zweckentfremdung als Individualkommunikationsmittel? .....	204
a) Speicherung dynamischer IP-Adressen durch den Cloud Provider.....	205
b) Praktisches Vorgehen bei der Ermittlung der Anzahl der Cloud-Nutzer .....	206
3. Ergebnis.....	207
IV. Beschlagnahme von Inhaltsdaten beim Cloud Storage: Analogie zur E-Mail?.....	207
1. Übertragung der Rechtsprechung zur E-Mail-Beschlagnahme auf das Cloud-Storage.....	208

2. Vergleichbarkeit von E-Mail-Dienst und Cloud Storage-Dienst.....	208
a) Pro-Vergleichbarkeit von Web-Mail mit Cloud Storage ...	208
b) Contra-Vergleichbarkeit: Festplattenersatzfunktion der Cloud.....	209
c) Zwischenergebnis: Eingeschränkte Vergleichbarkeit von Web-Mail und Cloud Storage .....	210
3. Konsequenzen .....	211
C. Offener Zugriff auf Cloud Speicher gem. §§ 94 ff. StPO .....	212
I. Praktische Ausgestaltung der offenen Beschlagnahme .....	213
II. Anordnungsvoraussetzungen und -inhalt.....	213
III. Vollzug der Durchsuchung und Beschlagnahme.....	214
IV. Bedeutung der Online-Sichtung gem. § 110 Abs. 3 StPO .....	214
V. Fazit.....	215
D. Heimlicher Zugriff auf Cloud Storage Daten .....	215
I. Heimlicher Zugriff auf die Desktop-Cloud beim Nutzer .....	216
1. Praktische Ausgestaltung des heimlichen Desktop-Zugriffs ....	216
2. Rechtliche Ausgestaltung des heimlichen Zugriffs: Online-Durchsuchung .....	216
3. Ergebnis .....	217
II. Heimlicher Zugriff auf die Online-Cloud beim Cloud Storage Provider .....	217
1. Praktische Ausgestaltung des heimlichen Zugriffs .....	218
2. Rechtliche Ausgestaltung des heimlichen Zugriffs.....	218
a) Heimlicher Zugriff auf Cloud Storage als Individulkommunikationsmittel gem. § 100a StPO.....	219
b) Heimlicher Zugriff auf Cloud Storage als ausschließliches Speichermedium.....	222
3. Ergebnis .....	224
III. Zusammenfassung: Zugriff zumeist Eingriff in das IT-Grundrecht ..	224
E. Überwachung und Absfangen der Cloud-Kommunikation.....	225
I. Abfangen der Daten gem. § 100a StPO .....	225
II. „Endgerät – Cloud – Verbindung“ als eigenständiges informationstechnisches System .....	227
III. Ergebnis.....	229
F. Zusammenfassung .....	229

---

<b>Sechstes Kapitel: Internationale und transnationale Aspekte des Zugriffs auf Cloud Storage.....</b>	<b>233</b>
A. Praktische Probleme der Strafverfolgung in Clouds.....	234
I. Technische Probleme durch Gegenmaßnahmen des Nutzers.....	234
1. Anonyme und anonymisierte Internetnutzung .....	234
a) Analoge Verschleierungsmöglichkeiten.....	235
b) Digitale Verschleierungsmöglichkeiten .....	236
c) Einfluss des Cloud Computing auf digitale Verschleierungsmöglichkeiten.....	238
d) Lösungsmöglichkeiten für die Ermittlungsbehörden .....	239
2. Verschlüsselung von Daten und Hardware .....	240
3. Zusammenfassung.....	242
II. Technische Probleme durch die Architektur des Cloud Storage .....	243
1. Datenfragmentierung durch Virtualisierung.....	244
2. Lösungsmöglichkeiten.....	244
B. Rechtliche Probleme der Strafverfolgung in Clouds .....	246
I. Bestimmung der örtlich zuständigen Strafverfolgungsbehörden .....	246
II. Bestimmung des physikalischen Serverstandorts.....	246
III. Ermittlungen deutscher Strafverfolgungsbehörden im Ausland – die Rechtshilfeproblematik.....	247
1. Bedeutung des Souveränitätsprinzips .....	247
2. Datenspeicherort ausschlaggebend für Zuständigkeit.....	247
3. Kein Einfluss des Abruforts auf Zuständigkeit .....	248
4. Konsequenzen der Unbestimmbarkeit des Speicherorts: Beweisverwertungsverbot in engen Grenzen .....	249
C. Lösungsmöglichkeiten.....	250
I. Transnationale Strafverfolgung: Die Rechtshilfe .....	250
1. Allgemein anerkannte Grundsätze.....	250
2. Grundzüge für ausgehende Rechtshilfeersuchen deutscher Ermittlungsbehörden .....	251
II. Europarechtliche Ansätze.....	252
1. Das Europäische Rechtshilfeübereinkommen .....	252
2. Die europäische Beweisanordnung (EBA).....	254
3. Die europäische Ermittlungsanordnung (EEA) .....	255
III. Vereinfachung durch die Cybercrime-Konvention (CCK).....	256
IV. Konsequenzen für den Zugriff auf Cloud-Speicher im Ausland .....	258
1. Bedeutung der Eu-RhÜbk, EBA und EEA .....	258
2. Bedeutung der Cybercrime-Konvention .....	259
a) Bedeutung des Art. 19 Abs. 2 CCK – die Online-Durchsicht .....	260
b) Bedeutung des Art. 32 CCK.....	261

V.	Zusammenfassung.....	261
D.	Exkurs: Bedeutung für die Befugnisse von Nachrichtendiensten .....	264
<b>Siebtes Kapitel: Ergebnisse und Zusammenfassung .....</b>		<b>267</b>
A.	Generelle Forderungen zur Strafverfolgung im Internet .....	268
	I.    Beschränkte Vorratsdatenspeicherung.....	268
	II.    Quellen-TKÜ .....	269
	III.    Online-Durchsuchung .....	270
B.	Die herausgehobene Bedeutung des IT-Grundrechts.....	271
C.	Möglichkeiten, Herausforderungen und Chancen?.....	273
<b>Literaturverzeichnis .....</b>		<b>275</b>