

# Inhaltsverzeichnis

<b>A. Einleitung</b> .....	15
I. Bedeutung der EDV-Beweissicherung .....	15
II. Grenzen der Auslegung .....	18
III. Einteilung der Zwangsmaßnahmen .....	20
<b>B. Eingriffe in die Telekommunikation</b> .....	23
I. Daten bei der Telekommunikation .....	24
1. Bestands- oder Benutzerdaten .....	26
a) Einzelne Inhalte .....	26
b) Bestandsdaten bei der Internet-Kommunikation ..	27
c) Fristen zur Datenspeicherung .....	27
2. Verkehrs- und Verbindungsdaten .....	28
a) Einzelne Inhalte .....	28
b) Verbindungsdaten nach der StPO .....	29
c) Standortdaten beim Mobilfunk .....	29
d) Fristen zur Datenspeicherung .....	30
e) Vorratsdatenspeicherung .....	33
aa) Bisherige Entwicklungen .....	33
bb) EU-Richtlinie zur Vorratsdatenspeicherung ..	35
cc) Umsetzung ins nationale Recht .....	37
3. Nutzungsdaten .....	38
a) Einzelne Inhalte .....	38
b) Behandlung der Access- und Service-Provider ..	39
c) Fristen zur Datenspeicherung .....	41
4. Inhaltsdaten .....	41
a) Einzelne Inhalte .....	41
b) Fristen für Datenspeicherung .....	42
5. Sonstige Daten: Zugangsdaten .....	42
a) PIN und Super-PIN/PUK .....	42
b) Sonstige Zugangskennungen .....	43
II. Überwachung der Telekommunikation (§ 100 a StPO) ..	44
1. Einzelne Eingriffsvoraussetzungen .....	45
a) Begriff der Telekommunikation .....	45
b) Netzbereich .....	47
c) Bestimmte Tatsachen für Katalogtat .....	48
d) Betroffener Personenkreis .....	50
e) Subsidiaritätsklausel .....	52
f) Verwertungsbeschränkungen .....	53
g) Einseitige Überwachung der Telekommunikation ..	55
h) Anordnungsvoraussetzungen und Dauer .....	56

i)	Umsetzung der Überwachungsmaßnahmen . . . . .	58
aa)	Anwendungsbereich und Begriffs- bestimmungen . . . . .	58
bb)	Auslandskopfüberwachung . . . . .	59
cc)	Kennungsart . . . . .	60
dd)	Bereitzustellende Daten . . . . .	60
ee)	Formelle Anforderungen . . . . .	61
2.	Einzelne aktuelle Rechtsfragen . . . . .	61
a)	IMEI-Nummer als Grundlage für Überwachung . .	62
b)	Handy im Stand-by-Betrieb . . . . .	65
c)	Roaming bei Mobilfunknetzen . . . . .	69
d)	„Raumgesprächsaufnahme“ . . . . .	71
e)	Kontrolle des E-Mail-Verkehrs . . . . .	73
aa)	E-Mail-Verkehr in vier Phasen . . . . .	74
bb)	Kontrolle in den Phasen 1 und 3 (Übertragungsvorgang) . . . . .	75
cc)	Kontrolle in der Phase 4 (empfangene Nachrichten) . . . . .	75
dd)	Kontrolle in der Phase 2 (Zwischenspeicherung) . . . . .	76
f)	Beschwerdeberechtigung des Netzbetreibers . . . .	81
g)	Verwertbarkeit von Erkenntnissen . . . . .	83
h)	Überwachung bei Voice-over-IP . . . . .	87
aa)	Technische Grundlagen . . . . .	87
bb)	Rechtliche Einordnung . . . . .	90
cc)	Rechtsgrundlagen für eine Überwachung . . . .	90
dd)	Umsetzung von Überwachungsmaßnahmen . .	92
i)	Kosten der Telekommunikationsüberwachung . . .	93
aa)	Entschädigung für konkrete Überwachungsmaßnahmen . . . . .	93
bb)	Entschädigung für Bereitstellung der technischen Einrichtungen . . . . .	95
j)	Begrenzungen durch Kernbereich des Persönlichkeitsschutzes . . . . .	96
aa)	BVerfG-Entscheidung zum „Großen Lauschangriff“ . . . . .	97
bb)	Folgen für die Überwachung der Telekommunikation . . . . .	99
k)	Bekanntgabe von Zugangsdaten (Super-PIN bzw. PUK) . . . . .	101
III.	Auskunft über Verbindungsdaten der Telekommunikation (§§ 100 g, h StPO) . . . . .	105
1.	Inhalt des Auskunftsanspruchs . . . . .	106

a)	Rufnummern und Kennungen .....	106
b)	Verbindungsdaten bei Internetkommunikation ..	107
c)	Verbindungsdaten beim Mobilfunk .....	108
d)	Abhängigkeit von Datenspeicherung .....	109
e)	Verwertung rechtswidrig gespeicherter Daten ...	110
2.	Eingriffsvoraussetzungen des § 100 g StPO .....	111
a)	Vorliegen bestimmter Tatsachen .....	111
b)	1. Alt.: Straftat von erheblicher Bedeutung .....	112
c)	2. Alt.: Straftat mittels Endeinrichtung begangen .	114
d)	Grundsatz der Verhältnismäßigkeit .....	116
3.	Dauer der Auskunftserteilung .....	116
4.	Betroffener des Auskunftsanspruchs .....	118
5.	Adressat der Auskunftsverpflichtung .....	118
6.	Anordnungskompetenz und formelle Voraussetzungen .....	119
7.	Verwertung der Daten im Strafverfahren .....	121
8.	Geltungsdauer .....	122
9.	Sonderformen des Auskunftsanspruchs .....	123
a)	Zielwahlsuche .....	123
b)	Funkzellenabfrage .....	125
10.	Einzelne Rechtsfragen .....	128
a)	Auskunftsanspruch bei Anonymisierungsdiensten .	129
b)	IMEI-Nummer als Grundlage für Auskunft ....	135
c)	IP-Adresse als Grundlage für Auskunft .....	136
d)	Auskunft bei Strafverfahren gegen „Unbekannt“ .	138
e)	Auskunftsanspruch bei gestohlenen Mobiltelefonen .....	140
f)	Personenauskunft zu dynamischer IP-Adresse ...	143
g)	Auswertungen von Mobiltelefonen .....	149
aa)	Kammerentscheidung vom 4. 2. 2005 .....	149
bb)	Kritik an der Entscheidung .....	150
cc)	Bindungswirkung der Entscheidung .....	153
dd)	Senatsentscheidung vom 2. 3. 2006 .....	154
h)	Auskunftsanspruch bei Mautdaten .....	156
i)	Zuständigkeit für die Anordnung .....	161
j)	Form der zu übermittelnden Daten .....	164
k)	Verwertung von Erkenntnissen gem. § 101 TKG .	166
l)	Fernmeldegeheimnis und Pressefreiheit .....	167
m)	Zugriff auf Nutzungsdaten bei Tele- und Mediendiensten .....	169
IV.	<b>Auskunft über Bestandsdaten der Telekommunikation</b> <b>(§§ 111 ff. TKG) .....</b>	<b>171</b>
1.	<b>Daten für Auskunftersuchen (§ 111 TKG) .....</b>	<b>172</b>

	a) Umfang der Speicherpflicht von Bestandsdaten . . .	173
	b) Bestandsdaten und Prepaid-Handys . . . . .	174
	c) Besonderheiten der Speicherpflicht . . . . .	175
2.	Automatisierte Auskunftsverfahren (§ 112 TKG) . . . . .	176
	a) Verpflichtete der automatisierten Auskunft . . . . .	176
	b) Auskunftsberechtigte Stellen . . . . .	177
	c) Technische Umsetzung und Kostentragung . . . . .	178
3.	Manuelles Auskunftsverfahren (§ 113 TKG) . . . . .	180
	a) Umfang der Auskunftsverpflichtung . . . . .	180
	b) Auskunftsberechtigte Stellen . . . . .	182
	c) Auskunft über Zugangsdaten von Mobiltelefonen . . . . .	183
	d) Kostentragung . . . . .	185
<b>C.</b>	<b>Einsatz sonstiger technischer Mittel</b> . . . . .	187
I.	Einsatz des IMSI-Catchers . . . . .	187
	1. Funktionsumfang des IMSI-Catchers . . . . .	188
	2. Diskussion um die Zulässigkeit des IMSI-Catcher- Einsatzes . . . . .	190
	3. Gesetzliche Anwendungsbereiche . . . . .	191
	a) Ermittlung der Geräte- und Kartenummer . . . . .	192
	b) Ergreifung des Täters . . . . .	193
	4. Formelle Voraussetzungen und Datenverwendung . . . . .	193
	5. Verfassungsrechtliche Zulässigkeit . . . . .	195
II.	Einsatz von GPS-Peilungen . . . . .	196
	1. Technische Grundlagen . . . . .	197
	2. Rechtliche Grundlagen für den Einsatz . . . . .	198
	3. Private standortbezogene Dienste . . . . .	200
	4. Kumulation von mehreren Eingriffsmaßnahmen . . . . .	201
III.	Einsatz von „Stiller SMS“ . . . . .	202
	1. Technische Voraussetzungen . . . . .	203
	2. Rechtsgrundlagen für Versendung der „stillen SMS“ . . . . .	204
	3. Abfrage der erzeugten Verkehrs-/ Verbindungsdaten . . . . .	206
	4. Zulässigkeit der Aufspaltung und Aufteilung von Maßnahmen . . . . .	207
IV.	Einsatz von „Readnotify“ . . . . .	208
	1. Technische Grundlagen . . . . .	208
	2. Rechtsgrundlagen für den Einsatz . . . . .	209
V.	Einsatz von Trojanern bzw. „Schnüffel-Programmen“ aller Art . . . . .	211
	1. Technische Grundlagen . . . . .	212
	2. Rechtsgrundlagen für den Einsatz . . . . .	214

VI.	Verfolgung von Angriffen auf drahtlose Netzwerke (WLAN) .....	218
1.	Technische Grundlagen für WLAN .....	219
2.	Angriffe gegen WLAN-Netze .....	220
3.	Strafbarkeit nach materiellem Recht .....	221
a)	Ausspähen von Daten (§ 202 a StGB) .....	221
b)	Computerbetrug (§ 263 a StGB) .....	222
c)	Erschleichen von Leistungen (§ 265 a StGB) .....	224
d)	Datenveränderung und Computersabotage (§§ 303 a, b StGB) .....	224
e)	Betriebsspionage (§ 17 UWG) .....	225
f)	Abhören von Nachrichten (§ 148 Abs. 1 Nr. 1 TKG) .....	226
g)	Datenschutzdelikte (§§ 43, 44 BDSG) .....	227
4.	Strafprozessuale Verfolgung .....	227
VII.	Verfolgung von „Phishing“-Angriffen .....	229
1.	Ablauf von „Phishing“-Angriffen .....	229
2.	Materielle Strafbarkeit .....	230
a)	E-Mail-Versendung .....	230
b)	Installation gefälschter Web-Seiten .....	232
c)	Verwendung der erlangten Zugangsdaten .....	233
d)	Behandlung von „Finanzmanagern“ .....	233
3.	Strafprozessuale Verfolgung .....	234
<b>D.</b>	<b>Durchsuchungen und Beschlagnahmen im EDV-Bereich</b> .....	237
I.	Durchsuchungen gem. §§ 102, 103 StPO .....	237
1.	Voraussetzungen des § 102 StPO .....	238
a)	„Verdächtiger“ i. S. d. § 102 StPO .....	238
b)	Durchsuchungszweck .....	239
c)	Durchsuchungsobjekte .....	240
d)	Grundsatz der Verhältnismäßigkeit .....	242
2.	Besonderheiten des § 103 StPO .....	243
a)	Beschränkung auf „bestimmte Gegenstände“ .....	243
b)	Abgrenzung zwischen § 102 und § 103 StPO .....	244
3.	Anordnung und „Gefahr in Verzug“ .....	245
4.	Spezielle Rechtsfragen im EDV-Bereich .....	249
a)	Inbetriebnahme fremder EDV-Anlagen .....	249
b)	Nutzung fremder Programme .....	252
c)	Durchsuchungen über Netzwerke .....	253
d)	Sonderproblem: Durchsuchungen mit Auslandsbezug .....	256
e)	Durchsuchungen bei Internet-Providern .....	260
f)	Durchsuchung zur Gewinnung von TK-Daten .....	262
g)	Berücksichtigung von Beschlagnahmeverboten .....	264

	5.	Umsetzung von Durchsuchungsanordnungen . . . . .	265
	a)	Unterbindung der Arbeit am Computer . . . . .	266
	b)	Unterbrechung der Kommunikations- einrichtungen . . . . .	267
	c)	Einsatz von WLAN-Scannern . . . . .	268
	d)	Heranziehung von anwesenden Personen . . . . .	270
	e)	Mitnahme der sichergestellten Gegenstände . . . . .	271
	6.	Durchsicht der Papiere . . . . .	272
II.		Beschlagnahme von EDV-Daten . . . . .	274
	1.	Gegenstände als Beweismittel . . . . .	275
	a)	Begriff des „Gegenstandes“ . . . . .	275
	b)	Folgen im EDV-Bereich . . . . .	277
	2.	Potenzielle Beweisbedeutung . . . . .	278
	3.	Grundsatz der Verhältnismäßigkeit . . . . .	280
	4.	Formen der Sicherstellung . . . . .	281
	5.	Beschlagnahmeverbote i. S. d. § 97 StPO . . . . .	282
	6.	Zusammentreffen von beschlagnahmbaren und beschlagnahmefreien Informationen . . . . .	286
	7.	Durchführung der Sicherstellung und Auswertung von EDV-Unterlagen . . . . .	289
	8.	Rückgabe beschlagnahmter Unterlagen . . . . .	291
III.		Sonderformen der Beschlagnahme . . . . .	292
	1.	Postbeschlagnahme . . . . .	292
	2.	Rasterfahndung . . . . .	294
<b>E.</b>		<b>Strafprozessuale Mitwirkungspflichten</b> . . . . .	297
	I.	Zeugenpflicht . . . . .	298
	1.	Reichweite der Zeugenpflichten . . . . .	298
	2.	Zeugenpflichten im EDV-Bereich . . . . .	299
	3.	Kurzfristige Zeugenladung . . . . .	300
	II.	Editionspflicht (§ 95 StPO) . . . . .	301
	1.	Reichweite der Vorlageverpflichtung . . . . .	302
	2.	Datenausdruck gem. § 261 HGB . . . . .	304
	3.	Kostenerstattung (§ 23 JVEG) . . . . .	305
<b>F.</b>		<b>Ermittlungen in Datennetzen</b> . . . . .	307
	I.	Polizeistreifen in Datennetzen . . . . .	308
	II.	Online-Zugriff auf gespeicherte Daten . . . . .	310
	1.	Abgrenzung Gefahrenabwehr und Strafverfolgung . . . . .	313
	2.	Einsatz verdeckter Ermittler . . . . .	315
	3.	Durchsuchung . . . . .	316
	a)	Offenheit als konstitutives Merkmal . . . . .	317
	b)	Eingriff in weitere Grundrechte . . . . .	320
	4.	Eingriffe in die Telekommunikation . . . . .	321
	5.	Rückgriff auf Ermittlungsgeneralklausel . . . . .	322

III.	Einsatz sonstiger technischer Mittel	323
1.	Technische Einsatzmöglichkeiten	324
2.	Eingriffsbefugnisse für den Einsatz	324
IV.	Folgerungen für Online-Zugriff auf Daten	325
<b>G.</b>	<b>Zugriff auf verschlüsselte Daten</b>	329
I.	Methoden der Datenverschlüsselung	330
1.	Vorhandene Programme	330
2.	Einzelne Verschlüsselungsverfahren	331
3.	Steganographie	332
II.	Bekanntgabe von Verschlüsselungsmechanismen	332
1.	Entschlüsselung durch Anbieter	333
2.	Rechtsgrundlagen zur Erlangung der „Schlüssel“	333
3.	Regelungen in anderen Ländern	334
<b>H.</b>	<b>Internationale Ermittlungen und Cyber-Crime-Konvention</b>	337
I.	Aufbau, Inhalt und Ziele der Konvention	338
II.	Umsetzungsbedarf im Strafprozessrecht	339
1.	Sicherung und Herausgabe gespeicherter Computerdaten	339
2.	Herausgabe- und Mitwirkungspflichten	340
3.	Durchsuchung und Beschlagnahme von Computerdaten	341
4.	Erhebung von Computer- und Inhaltsdaten in Echtzeit	343
III.	Internationale Zusammenarbeit	344
1.	Rechtshilfe bei vorläufigen Maßnahmen	344
2.	Rechtshilfe im Bezug auf Ermittlungsbefugnisse	345
<b>I.</b>	<b>Zusammenfassung und Ausblick</b>	347
<b>J.</b>	<b>Formularbeschlüsse</b>	349
I.	Überwachung der Telekommunikation (allgemein)	349
II.	Überwachung der Telekommunikation bei DSL	351
III.	Auslandskopfüberwachung	353
IV.	Telekommunikationsauskunft (allgemein)	356
V.	Telekommunikationsauskunft gestützt auf IMEI-Nummer	358
VI.	Zielwahlsuche	361
VII.	Funkzellenabfrage	363
VIII.	Telekommunikationsüberwachung mit -auskunft	365
IX.	Durchsuchung	368
X.	Beschlagnahme	370
XI.	Editionsbegehren	371
	Literaturverzeichnis	375
	Internet-Links	389
	Abkürzungsverzeichnis und Glossar	391
	Stichwortverzeichnis	395