

Inhaltsverzeichnis

Abkürzungsverzeichnis	XXV
Literaturverzeichnis	XXXIII
A. Einleitung	1
I. Vernetzte Informationstechnik und gesellschaftlicher Wandel	1
II. Die Alltagswirklichkeit der Digital Natives.....	2
III. Konzentrierte Informationen und ihr Schutz gegen Begehrlichkeiten Dritter.....	3
IV. Die Aushöhlung überkommener Ermittlungswerkzeuge.....	5
V. Neue Ermittlungsansätze mit neuen Problemlagen.....	5
VI. Bisherige Ansätze in der Praxis	6
VII. Die strafprozessualen Beschlüsse des 69. DJT	9
VIII. Untersuchungsziel	11
IX. Gang der Untersuchung	11
B. Der Begriff des IT-Systems	13
I. Zur Notwendigkeit einer Definition.....	13
II. Das IT-System in Rechtswissenschaft und Informatik.....	14
1. Computersystem und EDV-Anlage in der Rechtswissenschaft	14
2. Computersystem und IT-System in der Informatik	15
a) Hardwarekomponenten eines Computersystems.....	16
aa) Zentraleinheit (CPU).....	16
bb) Speicher	16
cc) Ein- und Ausgabeeinheiten.....	17
b) Softwarekomponenten eines Computersystems.....	18
aa) Programme	18
bb) Datenorganisation.....	19
(1) Dateien.....	19
(2) Daten auf Datenträgern.....	20
(3) Daten in CPU und Speicher.....	21
(4) Daten in Software-Caches.....	21
(5) Datenkopien.....	22
c) Hardware und Software im Zusammenspiel.....	23
aa) Datenübertragung	23
(1) Innerhalb eines Computersystems	23
(2) In Netzwerken	23
bb) Datenverarbeitung.....	25
(1) Zentrale Datenverarbeitung	25

Inhaltsverzeichnis

(2) Dezentrale Datenverarbeitung.....	25
d) Konsequenzen für den Begriff des IT-Systems.....	27
3. Übertragbarkeit der Definition aus der Informatik.....	29
a) Das IT-System im Begriffsverständnis des BMI.....	29
b) Ansätze im Schrifttum nach dem Online-Durchsuchungsurteil.....	30
c) Das IT-System im Grundgesetz.....	33
III. Zusammenfassung und Definition.....	34
C. Tatsächliche Zugriffsmöglichkeiten auf IT-Systeme.....	35
I. Zugriffe auf zentrale IT-Systeme.....	35
1. Beweisthemen mit Hardwarebezug.....	35
2. Unverschlüsselt permanent gespeicherte Daten.....	35
3. Verschlüsselt permanent gespeicherte Daten.....	36
a) Kryptographische Grundlagen.....	36
aa) Blockchiffre, Schlüssel und Passwort.....	37
bb) Symmetrische Datenträgerverschlüsselung.....	39
b) Zugriffsmöglichkeiten.....	41
aa) Hinterlegung der Schlüssel („Key Escrow“).....	41
bb) Schwächung von Verschlüsselungsprodukten.....	42
cc) Ermittlung des Passworts per Keylogger.....	42
dd) Schlüsselextraktion aus einem Arbeitsspeicherabbild.....	43
ee) Schlüsselrekombination aus dem Hardwareverhalten.....	44
ff) Sicherung und Auswertung während des Betriebs.....	44
(1) Per körperlichem Zugriff.....	44
(2) Per Fernzugriff über das Internet - „Online-Durchsicht“.....	45
(a) Nutzung von Exploits.....	46
(b) Installation durch den Beschuldigten selbst.....	47
4. Überwachung der Nutzung.....	48
a) Nutzung zur Internet-Kommunikation.....	49
aa) Technische Grundlagen der verschlüsselten Internet-Kommunikation.....	49
(1) Verbindungsverschlüsselung (Punkt-zu-Punkt- Verschlüsselung).....	51
(2) Inhaltsverschlüsselung (Ende-zu-Ende-Verschlüsselung).....	53
bb) Zugriffsmöglichkeiten.....	55
(1) Backdoors und Man in the middle-Angriffe.....	55
(a) Bei der Verbindungsverschlüsselung.....	56
(b) Bei der Inhaltsverschlüsselung.....	59
(c) Insbesondere: Abhören der Internet-Telefonie („VoIP“).....	60
(2) Im IT-System des Beschuldigten - „Quellen-TKÜ“.....	64

Inhaltsverzeichnis

(3) Einsatz externer technischer Mittel	65
(4) Zwischenergebnis	65
b) Sonstige Nutzungsarten	66
aa) Online-Überwachung	66
bb) Hardware-Keylogger und Van-Eck-Phreaking	66
5. „Analoge“ Überwachung mittels IT-Systems	66
II. Zugriffe auf dezentrale IT-Systeme	66
1. Zugriff auf dem Übertragungsweg	67
2. Inpflichtnahme des öffentlichen Cloud Computing-Anbieters	67
a) Bei SaaS- und PaaS-Lösungen	68
b) Bei IaaS-Lösungen (insbesondere: Cloud Storage)	68
3. Zugriff mit Zugangsdaten des Betroffenen	69
III. Zusammenfassung	71
D. Grundrechtsschutz bei Zugriffen auf IT-Systeme	73
I. Gemeinsame verfassungsrechtliche Anforderungen an strafprozessuale Grundrechtseingriffe	73
1. Zur verfassungsrechtlichen Legitimität strafprozessualer Ermittlungsmaßnahmen	74
a) Verfassungsrang des Strafverfahrens	74
aa) Vom privaten zum öffentlichen Strafrecht	74
bb) Verhältnis zwischen funktionstüchtiger Strafrechtspflege und Grundrechten	77
(1) Grundrechtsschutz durch materielles Strafrecht	77
(2) Grundrechtsschutz durch Ermittlungsbefugnisse	80
cc) Zwischenergebnis	80
b) Ausgleich zwischen Grundrechten und öffentlichem Strafverfolgungsinteresse	81
aa) Gewichtung des öffentlichen Strafverfolgungsinteresses	83
(1) Kriterien der Nr. 86 Abs. 2 RiStBV	83
(2) Schwere der Tat und Bedeutung der Sache	84
(3) Grad des Tatverdachts	86
(4) Öffentliches Interesse an bestimmten Ermittlungsmaß- nahmen	90
bb) Ermittlung der Schwere eines Grundrechtseingriffs	93
(1) Grundrechtsübergreifende Fallgruppen besonderer Eingriffsschwere	93
(a) Heimlichkeit und Eingriffsdauer	95
(b) Annähernde Totalüberwachung	97
(c) Potentielle Berührung des Kernbereichs der	

Inhaltsverzeichnis

privaten Lebensgestaltung.....	97
(aa) Ablehnung der Kernbereichskonzeption	98
(bb) Zweistufiges Schutzkonzept des BVerfG.....	99
(cc) Kernbereichsschutz im Strafverfahren.....	100
(dd) Zwischenergebnis.....	103
(d) Verletzung einer Vertraulichkeitserwartung	103
(e) Zwischenergebnis	104
(2) Wesensgehaltsgarantie des Art. 19 Abs. 2 GG.....	105
(a) Auffassungen im Schrifttum	105
(aa) Objektiv-rechtliche Theorien.....	105
(bb) Absolute subjektiv-rechtliche Theorien.....	106
(cc) Relative subjektiv-rechtliche Theorien	107
(b) Rechtsprechung des BVerfG.....	107
(c) Stellungnahme	108
(d) Zwischenergebnis	110
cc) Verhältnismäßigkeit strafprozessualer Ermittlungsmaß-	
nahmen	111
(1) Legitimer Zweck.....	112
(2) Eignung.....	112
(3) Erforderlichkeit.....	113
(4) Angemessenheit	113
2. Anforderungen an die Eingriffsgrundlage	114
a) Regelungstypus	116
aa) Wesentlichkeit als politische und grundrechtliche	
Wichtigkeit	117
bb) Wesentlichkeitstheorie und institutioneller Gesetzesvor-	
behalt.....	118
cc) Stellungnahme.....	119
(1) Wesentlichkeit bei Wichtigkeit?	119
(2) Parlamentsgesetz bei politischer Wichtigkeit	119
(3) Parlamentsgesetz bei jeder Grundrechtswichtigkeit	120
(4) Ausgleich zwischen Parlamentsvorbehalt und	
institutioneller Gewaltenteilung	122
dd) Zwischenergebnis.....	123
b) Regelungsdichte	124
aa) Analogieverbot und Ermittlungsgeneralklausel	124
(1) Ermittlungen in der Öffentlichkeitssphäre.....	125
(2) Ermittlungen ohne Zwangscharakter	126
(3) Keine Heimlichkeit der Ermittlungen.....	127

Inhaltsverzeichnis

bb)	Normenklarheit und Bestimmtheit	127
cc)	Annexkompetenzen.....	129
dd)	Zwischenergebnis.....	133
3.	Anforderungen an den Eingriff im Einzelfall.....	134
a)	Auslegung der Eingriffsbefugnis.....	134
aa)	Im klassischen Methodenkanon.....	134
bb)	Anhand des Grundgesetzes.....	136
b)	Prüfung der Verhältnismäßigkeit.....	136
4.	Zwischenergebnis	137
II.	Schutzbereiche und Eingriffsanforderungen im Einzelnen.....	138
1.	Objektbezogener Grundrechtsschutz	139
a)	Recht auf informationelle Selbstbestimmung, Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG	139
aa)	Eingriff in den Schutzbereich	140
bb)	Verfassungsrechtliche Rechtfertigung	140
(1)	Erkennbare Zweckbestimmung und strenge Zweck- bindung.....	143
(2)	Berücksichtigung der Persönlichkeitsrelevanz.....	143
(3)	Transparenzgebot.....	145
(4)	Technische Gewährleistung von Datensicherheit	146
b)	Exkurs: Datenschutz-Grundrecht?	147
c)	IT-Grundrecht, Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG.....	148
aa)	Eingriff in den Schutzbereich	148
(1)	Schutzobjekte: potentiell datenintensive IT-Systeme	148
(2)	Vertraulichkeit und Integrität	150
(a)	Schutz der Vertraulichkeit.....	150
(b)	Schutz der Integrität	153
(c)	Berechtigte Erwartungen an Vertraulichkeit und Integrität	157
(aa)	Nutzung des IT-Systems „als eigenes“	157
(bb)	Berechtigte Erwartungen und informations- technische Realität	159
[i]	Vertraulichkeit und Integrität als grund- rechtlich geschützter status quo?.....	159
[ii]	Vertraulichkeit und Integrität als objektive Schutzpflicht	162
(3)	Zwischenergebnis	165
bb)	Verfassungsrechtliche Rechtfertigung	166
d)	Eigentumsfreiheit gemäß Art. 14 Abs. 1 S. 1 GG.....	170

Inhaltsverzeichnis

aa)	Eingriff in den Schutzbereich	170
(1)	Entzug der Sachherrschaftsposition an Datenträgern.....	170
(2)	Veränderung von Datenträgern.....	171
(3)	Zugriff auf die Daten als solche	172
bb)	Verfassungsrechtliche Rechtfertigung	174
e)	Zwischenergebnis.....	174
2.	Umstandsbezogener Grundrechtsschutz	175
a)	Berufsfreiheit gemäß Art. 12 Abs. 1 GG.....	175
b)	Informationsfreiheit gemäß Art. 5 Abs. 1 S. 1, letzter Halbs. GG	176
aa)	Eingriff in den Schutzbereich	176
bb)	Verfassungsrechtliche Rechtfertigung	178
c)	Unverletzlichkeit der Wohnung gemäß Art. 13 Abs. 1 GG.....	178
aa)	Eingriff in den Schutzbereich	178
(1)	Betreten der Wohnung zum Zugriff auf ein IT-System.....	179
(2)	Optische und akustische Überwachung der Wohnung	179
(3)	Internet-Fernzugriff auf ein IT-System	179
bb)	Verfassungsrechtliche Rechtfertigung	180
d)	Fernmeldegeheimnis gemäß Art. 10 Abs. 1 GG	181
aa)	Eingriff in den Schutzbereich	181
(1)	Zum Begriff der Kommunikation i. S. d. Art. 10 GG.....	181
(2)	Wortsinn der Kommunikation.....	182
(aa)	Der Kommunikationsbegriff in der Rechtsprechung des BVerfG	183
[i]	Beschluss zur Mithörvorrichtung (Erster Senat)	183
[ii]	Nichtannahmebeschluss zum IMSI-Catcher (Zweiter Senat)	183
[iii]	Beschluss zur E-Mail-Beschlagnahme (Zweiter Senat).....	185
[iv]	Urteil zur Telekommunikationsüberwachung (Erster Senat)	185
[v]	Urteil zur Vorratsdatenspeicherung (Erster Senat)	186
[vi]	Online-Durchsuchungsurteil (Erster Senat)	186
[vii]	Zwischenergebnis.....	187
(bb)	Der Kommunikationsbegriff im Schrifttum	188
[i]	Formaler Kommunikationsbegriff.....	188
[ii]	Funktionaler Kommunikationsbegriff.....	189
(cc)	Stellungnahme	190
(dd)	Zwischenergebnis.....	195
(3)	Zur Vertraulichkeit der Kommunikation	195

Inhaltsverzeichnis

(4) Keine autorisierte Kenntnisnahme	195
(5) Zeitliche Reichweite	196
(6) Ort des Zugriffs	198
(7) Zwischenergebnis	199
bb) Verfassungsrechtliche Rechtfertigung	199
e) Zwischenergebnis	200
3. Zwischenergebnis	200
III. Eingriffe in subjektive Rechte auf internationaler Ebene.....	201
1. Europäische Menschenrechtskonvention.....	201
2. Grundrechte auf Ebene der Europäischen Union.....	204
a) Strafverfahrensrechtliche EU-Richtlinien	205
b) Schutzniveau von Grundgesetz und EGRC bei Zugriffen auf IT-Systeme	206
c) Konsequenzen für den deutschen Gesetzgeber	208
d) Zwischenergebnis	211
3. Zwischenergebnis	212
IV. Rechtsfolgen strafprozessualer Grundrechtsverletzungen	212
1. Grundrechtsverletzungen und Verfahrensfehler.....	213
2. Grundrechtsverletzungen und Beweisverwertungsverbote	214
a) Beweisverwertungsverbotslehren im Schrifttum	215
aa) Schutzzwecklehren.....	215
bb) Lehre von den Informationsbeherrschungsrechten.....	215
cc) Abwägungslehre bzw. normative Fehlerfolgenlehre	216
b) Beweisverwertungsverbote in der Rechtsprechung	217
c) Normative Erwägungen als gemeinsames Element.....	220
d) Konsequenzen aus dem verfassungsrechtlichen Verhältnis zwischen Grundrechtsschutz und funktionstüchtiger Strafrechtspflege.....	222
e) Zwischenergebnis	224
3. Kompensationsmöglichkeiten strafprozessualer Grundrechtsverletzungen.....	225
a) Fehlerkompensation mit Auswirkungen auf das Beweis- ergebnis	226
aa) Beweisverwertungsverbote.....	226
(1) Grundsätze	226
(2) Bedeutung normativer Erwägungen.....	226
(3) Bedeutung des Verhältnismäßigkeitsprinzips.....	227
(4) Einfluss des strafprozessualen Wahrheitsgrundsatzes	228
(5) Fernwirkung von Beweisverwertungsverbote.....	229

Inhaltsverzeichnis

bb) Beweiswürdigungslösung	231
cc) Einstellungslösung?	233
b) Fehlerkompensation ohne Auswirkungen auf das Beweis- ergebnis.....	235
aa) Disziplinar- und strafrechtliche Sanktionierung fehlerhaft handelnder Amtsträger	235
bb) Entschädigungslösungen	237
c) Zwischenergebnis	241
4. Konsequenzen für die Strafverfahrenspraxis	243
5. Konsequenzen für den Gesetzgeber	247
E. Verfassungsgemäße Zugriffsmöglichkeiten auf IT-Systeme nach derzeit bestehender Rechtslage	249
I. Zugriffe auf zentrale IT-Systeme.....	249
1. Körperliche Sicherstellung zentraler IT-Systeme bzw. einzelner Datenträger	249
a) Grundrechtseingriffe.....	249
aa) Durch den Zugriff auf die Hardware	249
bb) Durch den Zugriff auf die Daten	250
b) Ermittlungsbefugnisse.....	251
aa) Für die körperliche Sicherstellung von Hardware	251
(1) Art. 14 Abs. 1 GG.....	251
(2) Art. 5 Abs. 1 S. 1, letzter Halbs. GG.....	252
(3) Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG.....	253
(a) Erkennbare Zweckbestimmung und strenge Zweckbindung.....	253
(b) Transparenzgebot	254
(c) Berücksichtigung der Persönlichkeitsrelevanz	258
(aa) Bei Eingriffen in das Recht auf informationelle Selbstbestimmung.....	258
(bb) Bei Eingriffen in das IT-Grundrecht	259
(d) Technische Gewährleistung von Datensicherheit.....	262
bb) Für die Durchsuchung der Wohnung, einer Sache oder der Person des Betroffenen zur Sicherstellung von Hardware	263
cc) Zwischenergebnis	264
c) Einzelfragen zur Verhältnismäßigkeit.....	264
aa) Bei Sicherstellungsmaßnahmen.....	265
(1) Sicherstellung von Hardware bei Beweisthemen mit Datenbezug	265

Inhaltsverzeichnis

(a)	Erforderlichkeit aus technischer Sicht.....	265
(b)	Erforderlichkeit aus Gründen begrenzter Ressourcen	265
(c)	Ansatz der Praxis: „Vorläufige Sicherstellung zur Auswertung“	267
(2)	Exkurs: Beweisthemen mit Hardwarebezug.....	270
(3)	Sicherstellung vollständiger Datenbestände.....	271
(a)	Selektion vor der Auswertung	272
(b)	Selektion während der Auswertung.....	273
(4)	Angemessenheit der Auswertung unter Geltung des IT-Grundrechts	274
bb)	Bei Durchsuchungsmaßnahmen.....	278
d)	Rechtsfolgen bei Verfahrensverstößen	279
aa)	Unverhältnismäßige Dauer der Sicherstellung von Hardware.....	279
bb)	Keine Löschung beschlagnahmefreier Datenbestände.....	280
cc)	Keine Löschung von Kernbereichsinhalten und sonstigen irrelevanten Daten.....	281
2.	Zugriff auf verschlüsselt permanent gespeicherte Daten.....	281
a)	Ermittlungsbefugnisse	282
aa)	Brechung und Umgehung der Verschlüsselung.....	282
bb)	Mitwirkungspflichten.....	284
(1)	Herausgabepflicht gemäß § 95 Abs. 1 StPO	284
(2)	Zeugnispflicht gemäß §§ 48, 161a Abs. 1 StPO.....	285
(3)	Zwangsmittel bei behaupteter Unmöglichkeit der Mitwirkung?	286
cc)	Sicherung und Auswertung während des Betriebs.....	286
(1)	Sicherung von Daten per körperlichem Zugriff auf ein in Betrieb befindliches verschlüsseltes IT-System gemäß § 94 Abs. 1 StPO.....	286
(a)	Auslegung am Wortsinn	288
(aa)	Ansicht: Gegenstand meint nur körperliche Objekte	288
(bb)	Ansicht: Gegenstand meint körperliche und unkörperliche Objekte.....	289
(cc)	Stellungnahme	289
(b)	Systematische Auslegung.....	291
(aa)	Ansicht: Gegenstand meint nur körperliche Objekte	291
(bb)	Ansicht: Gegenstand meint körperliche und unkörperliche Objekte.....	292
(cc)	Stellungnahme	294

Inhaltsverzeichnis

(c)	Historisch-genetische Auslegung	297
(aa)	Ansichten im Schrifttum	297
(bb)	Auffassung des BVerfG	297
(cc)	Stellungnahme	298
(d)	Auslegung nach Sinn und Zweck	302
(aa)	Ansicht: Gegenstand meint nur körperliche Objekte	302
(bb)	Ansicht: Gegenstand meint körperliche und unkörperliche Objekte.....	303
(cc)	Stellungnahme	303
(e)	Verfassungskonforme Auslegung	304
(aa)	Intensivere Vertraulichkeitsbeeinträchtigung?.....	304
(bb)	Intensivere Integritätsbeeinträchtigung?	305
(cc)	Keine Heimlichkeit der Maßnahme.....	306
(f)	Zwischenergebnis	306
(2)	Online-Durchsicht.....	306
dd)	Hinterlegung der Schlüssel	308
ee)	Schwächung von Verschlüsselungsprodukten	308
ff)	Ermittlung des Passworts per Keylogger.....	309
gg)	Schlüsselrekombination aus dem Hardwareverhalten	310
b)	Einzelfragen zur Verhältnismäßigkeit	310
aa)	Brechung und Umgehung der Verschlüsselung.....	310
bb)	Mitwirkungspflichten.....	311
cc)	Sicherung und Auswertung während des Betriebs.....	312
c)	Rechtsfolgen bei Verfahrensverstößen	314
aa)	Brechung und Umgehung der Verschlüsselung.....	314
bb)	Mitwirkungspflichten.....	315
cc)	Maßnahmen ohne Rechtsgrundlage	315
3.	Überwachung der Nutzung	316
a)	Nutzung zur funktionalen Internet-Kommunikation.....	316
aa)	Grundrechtseingriffe.....	316
bb)	Ermittlungsbefugnisse.....	316
(1)	Abhören der Internet-Telefonie	316
(a)	Durch Inpflichtnahme von Anbietern und Mitwirkenden	316
(aa)	ISPs als Verpflichtete i. S. d. § 100b Abs. 3 S. 1 StPO	317
(bb)	Anbieter nutzerbasierter VoIP-Dienste als Verpflichtete i. S. d. § 100b Abs. 3 S. 1 StPO	317
(cc)	Zwischenergebnis.....	320
(b)	Im Wege der Quellen-TKÜ.....	321

Inhaltsverzeichnis

(aa)	Auffassungen der Rechtsprechung	321
(bb)	Auffassungen im Schrifttum.....	324
(cc)	Ansicht des Generalbundesanwalts.....	325
(dd)	Stellungnahme	326
[i]	Reichweite des Telekommunikationsvorgangs i. S. d. § 100a Abs. 1 StPO.....	326
[ii]	Beschränkung der §§ 100a, 100b StPO auf Maß- nahmen unter Mitwirkung des Tele- kommunikationsdiensteanbieters	328
[iii]	Anforderungen des IT-Grundrechts und der Eigentumsfreiheit.....	329
(c)	Durch akustische Überwachungsmaßnahmen	338
(2)	Überwachung textbasierter Kommunikation	338
cc)	Einzelfragen zur Verhältnismäßigkeit.....	342
dd)	Rechtsfolgen bei Verfahrensverstößen.....	343
b)	Sonstige Nutzungsarten	343
aa)	Grundrechtseingriffe.....	343
bb)	Ermittlungsbefugnisse.....	343
(1)	Online-Überwachung	343
(2)	Van-Eck-Phreaking	344
(3)	Überwachung der nicht funktional- kommunikativen Internetnutzung	344
cc)	Rechtsfolgen bei Verfahrensverstößen	348
(1)	Bei der Online-Überwachung und dem Van-Eck- Phreaking.....	348
(2)	Bei der Überwachung der nicht funktional- kommunikativen Internetnutzung	348
4.	„Analoge“ Überwachung mittels IT-Systems.....	349
II.	Zugriffe auf dezentrale IT-Systeme.....	350
1.	Grundrechtseingriffe	350
2.	Ermittlungsbefugnisse	350
a)	Zugriff auf dem Übertragungsweg.....	350
b)	Inpflichtnahme öffentlicher Cloud Computing-Anbieter	351
aa)	Gewahrsam i. S. d. §§ 94 ff. StPO	352
bb)	Herausgabe von Kopien als Mitwirkungspflicht	353
cc)	Zwischenergebnis	355
dd)	Insbesondere: öffentliche Cloud Computing- Anbieter mit Auslandsbezug.....	355
(1)	Ausschließlich im Ausland ansässige Anbieter.....	355

Inhaltsverzeichnis

(2) Auch im Inland ansässige Anbieter.....	357
(3) Zwischenergebnis	359
c) Zugriff mit Zugangsdaten des Betroffenen	359
aa) Am Ort einer Durchsuchungsmaßnahme.....	359
bb) Per Endgerät der Strafverfolgungsbehörde	364
(1) Mit Zugangsdaten aus einem sichergestellten Endgerät	365
(2) Nach Zugangsdatenauskunft gemäß § 100j Abs. 1 S. 2 StPO.....	367
(3) Nach Zugangsdatenauskunft gemäß §§ 161, 163 StPO i. V. m. § 14 Abs. 2 TMG.....	369
(4) Zwischenergebnis	371
3. Einzelfragen zur Verhältnismäßigkeit.....	371
a) Angemessenheit von Herausgabeverlangen gemäß § 95 Abs. 1 StPO an öffentliche Cloud Computing- Anbieter	371
aa) Beschränkung in Anlasstaten und Verdachtsgrad?	371
bb) Benachrichtigungspflicht	373
cc) Zwischenergebnis	376
b) Angemessenheit der Durchsicht gemäß § 110 Abs. 3 StPO bei betroffenen Dritten	376
4. Rechtsfolgen bei Verfahrensverstößen	377
a) Bei Zugriffen auf dem Übertragungsweg.....	377
b) Bei der Inpflichtnahme öffentlicher Cloud Computing- Anbieter	378
aa) Herausgabeverlangen an ausländische Anbieter	378
bb) Keine Benachrichtigung des Betroffenen	379
c) Bei Zugriffen mit Zugangsdaten des Betroffenen.....	382
aa) Keine Benachrichtigung eines betroffenen Dritten	382
bb) Heimliche Nutzung von Zugangsdaten nach Herausgabe durch den Anbieter.....	383
III. Zusammenfassung.....	384
F. Reformdiskussion und Reformvorschläge	385
I. Normierung von Online-Durchsuchung und Quellen-TKÜ?	385
1. Gesetzesentwürfe zur Online-Durchsuchung.....	385
a) Freistaat Bayern (2008).....	385
b) Gudermann (2009).....	388
c) Redler (2012).....	390
d) Stellungnahme.....	395
aa) Zum bayerischen § 100k StPO-E	395

Inhaltsverzeichnis

(1) Ermittlungspraktische Widersprüche	395
(2) Verfassungsrechtliche Bedenken	396
(a) Unzureichender Schutz des Kernbereichs der privaten Lebensgestaltung?.....	396
(b) Unverhältnismäßigkeit des Straftatenkatalogs	398
(c) Verstoß gegen Art. 13 Abs. 1 GG	399
(d) Verstoß gegen die Integritätskomponente des IT-Grundrechts.....	401
bb) Zum Vorschlag Gudermanns	402
(1) Ermittlungspraktische Bedenken.....	403
(2) Verfassungsrechtliche Bedenken	404
(a) Überbordender Kernbereichsschutz	404
(b) Unzureichender Straftatenkatalog	404
cc) Zum Vorschlag Redlers.....	405
(1) Systematische Bedenken	406
(2) Verfassungsrechtliche Bedenken	407
(a) Überbordender Kernbereichsschutz	407
(b) Unzureichender Straftatenkatalog	408
2. Gesetzesentwurf zur Quellen-TKÜ	409
a) Bratke (2013).....	409
b) Stellungnahme	411
3. Praktische Umsetzungsprobleme von Online-Durchsuchung und Quellen-TKÜ	415
4. Verfassungsrechtliche Bedenken gegen die derzeitige praktische Umsetzung	418
a) Eignung kommerzieller Überwachungssoftware.....	418
b) Staatliche Pflichtenkollision.....	420
5. Konsequenzen	422
a) Einsatz von Überwachungssoftware aus staatlicher Eigenentwicklung	422
b) Restriktiver Einsatz heimlicher Internet-Fernzugriffe.....	424
aa) Öffentliches Verfügbarkeitsinteresse.....	425
bb) Strafprozessuale Zwecke im Gesamtkontext staatlicher Sicherheitsarchitektur.....	427
6. Zwischenergebnis	432
II. Alternative Ermittlungsmaßnahmen	432
1. Heimliche Zugriffe auf Cloud-Inhalte?	432
2. Zugriffe auf verschlüsselt permanent gespeicherte Daten.....	433
a) Entschlüsselungspflicht des Beschuldigten?	433

Inhaltsverzeichnis

b)	Hinterlegung der Schlüssel?	437
c)	Schwächung von Verschlüsselungsprodukten?	438
d)	Hardware-Keylogger	439
e)	Schlüsselrekombination aus dem Hardwareverhalten	442
3.	Überwachung der Nutzung von IT-Systemen	443
a)	IP-gestützte ITÜ	443
b)	Hardware-Keylogger und Van-Eck-Phreaking	446
aa)	Begrenzung der Maßnahmen auf ein Ermittlungsziel?	447
bb)	Konsequenzen für die Befugnisnorm	449
(1)	Keine Unterscheidung zwischen Internet-Fernzugriffen und sonstigen Zugriffen mit technischen Mitteln	449
(2)	Restriktiver Straftatenkatalog	450
(3)	Subsidiaritätsklausel, Richtervorbehalt und Kernbereichsschutz	452
III.	Normvorschläge	452
G.	Fazit und Ausblick	457