

Zugriffe auf elektronische Kommunikation

Eine verfassungsrechtliche und
straßprozessrechtliche Analyse

Nicolas von zur Mühlen



Duncker & Humblot • Berlin

Inhaltsverzeichnis

Vorwort	V
English summary	VII
Inhaltsübersicht	IX
Abkürzungsverzeichnis	XXIV

Einleitung

I. Forschungsgegenstand	1
A. Telekommunikationssphären	4
1. Sachliche Reichweite	4
2. Zeitliche Reichweite	6
B. Verdeckte und offene Maßnahmen	7
C. Mitwirkungspflichten	8
D. Einschränkungen des Forschungsgegenstands	9
E. Stand der Forschung	10
II. Forschungsziel	12
III. Forschungsmethoden	13
IV. Gang der Untersuchung	15

Teil I Grundlagen

I. Wandel der Kommunikationsarchitektur	15
A. Historische Entwicklung	15
B. Charakteristika moderner Telekommunikation	17
1. Ubiquität	17
2. Geschwindigkeit	18
3. Massenhaftigkeit	19
4. Komplexität	19
5. Dezentralität	20
6. Kontrollresistenz	20

II. Technische Grundlagen	22
A. Schichtenmodelle	23
1. ISO/OSI-Schichtenmodell	23
2. TCP/IP-Modell	24
B. Akteure und Komponenten	25
1. Nutzer	25
2. Telekommunikationsnetzbetreiber (Network-Operator)	26
3. Internetzugangsanbieter (Access-Provider)	27
4. Carrier und Routing-Anbieter (Network-Provider)	28
5. Anbieter von Ressourcen und Anwendungen (Hosting-Provider)	30
6. Inhaltenanbieter (Content-Provider)	33
C. Arten der elektronischen Telekommunikation	34
1. Differenzierung anhand zeitlicher Kriterien	34
a) Speicherphasen	35
b) Übertragungsphasen	35
2. Differenzierung anhand funktionaler Idealtypen	36
a) Personelle Faktoren	37
aa) Interpersoneller Datenaustausch	37
(1) Voice- und Video-over-IP (synchroner Daten-	
austausch)	37
(2) E-Mail (asynchroner Datenaustausch)	39
(3) Chat- und Messaging-Dienste (gemischter Daten-	
austausch)	41
bb) Intrapersoneller Datenaustausch	42
b) Veranlassung	43
aa) Unmittelbar veranlasster („klassischer“) Datenaustausch	43
bb) Mittelbar veranlasster („automatisierter“) Datenaustausch	44
cc) Unveranlasster („autonomer“) Datenaustausch	45
III. Kriminalistische Grundlagen	46
A. Bedeutung der Telekommunikationsüberwachung	46
B. Erhebung von Daten in den Übertragungsphasen	49
1. Erhebung von Daten beim Provider	49
a) Technische Möglichkeiten der Paketanalyse	49
aa) Analyse der Datenheader mittels Stateless Packet Inspection	49
bb) Analyse der Datenheader mittels Stateful Packet Inspection	
(SPI)	51
cc) Analyse der Nutzerdaten mittels Deep Packet Inspection	52
b) Ausleitung bei Access-Providern	53

aa)	Technische Durchführung der Ausleitung	54
bb)	Informationsgehalt der ausleitbaren Daten	55
c)	Ausleitung bei Network-Providern (insb. Netzknoten)	56
d)	Ausleitung bei Anbietern von Anwendungen (Hosting-Provider)	59
e)	Ausleitung bei Anbietern von Infrastruktur (Server-Hosting- Provider und Housing-Provider)	60
2.	Erhebung von Daten beim Nutzer	61
a)	Generelle Funktionsweise der Quellen-TKÜ	62
b)	Analyse des sog. Bayern-Trojaners	64
C.	Erhebung von Daten in den Speicherphasen	68
1.	Erhebung von Daten beim Nutzer	68
a)	Physischer Zugriff	68
aa)	Vorbereitung	69
bb)	Datensammlung	69
(1)	Post-mortem-Analyse	70
(2)	Live-Sicherung	70
cc)	Datenanalyse	71
dd)	Dokumentation und Präsentation	72
b)	Fernzugriff (Online-Durchsuchung und Online-Überwachung)	72
2.	Erhebung von Daten beim Provider	75

Teil 2

Rechtlicher Schutz elektronischer Kommunikation

I.	Schutz durch Grundrechte	77
A.	Schutzbereiche	78
1.	Fernmeldegeheimnis	79
a)	Formelle Reichweite	81
b)	Materielle Reichweite	82
aa)	Schutz aller kommunikativen Inhalte	82
bb)	Schutz der näheren Umstände der Kommunikation	83
(1)	Kommunikationsbegleitende technische Daten	84
(2)	Anlässlich der Kommunikation anfallende Daten	85
(3)	Bestandsdaten	86
2.	Allgemeines Persönlichkeitsrecht	87
a)	Recht auf informationelle Selbstbestimmung	88
b)	Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme	89
aa)	Formelle Reichweite	91
(1)	Technische Konzeption	91
(2)	Ablehnung einer räumlichen Konzeption	94

bb)	Materielle Reichweite	96
(1)	Vertraulichkeit	96
(2)	Integrität	98
3.	Abgrenzung der Schutzbereiche	99
a)	Differenzierung anhand von Telekommunikationsphasen	99
aa)	Makroebene	100
(1)	Schutz lokaler Daten	101
(α)	Monistisches Modell	101
(β)	Dualistisches Modell	102
(2)	Schutz serverseitig gespeicherter Daten	103
(α)	Formal-technisches Modell	105
(β)	Funktionales Modell	106
(γ)	Gemischtes Modell	107
bb)	Mikroebene	111
(1)	Formale oder funktionale Abgrenzung?	112
(2)	Einordnung der Vorgänge bei der Quellen-TKÜ	114
b)	Differenzierung anhand funktionaler Faktoren	118
aa)	Daten in der Übertragung	119
(1)	Bisherige Differenzierungsansätze	120
(α)	Unterscheidung anhand der zugrunde liegenden Übertragungstechnik	120
(β)	Unterscheidung anhand der genutzten Anwendung	123
(2)	Technische Differenzierbarkeit	126
(3)	Verfassungsrechtliche Differenzierbarkeit	130
(α)	Übertragungsbezogener Schutz durch das Fernmeldegeheimnis	130
(β)	Systembezogener Schutz durch das IT-Grundrecht	136
(γ)	Datenbezogener Schutz durch das Recht auf informationelle Selbstbestimmung	137
(δ)	Konkurrenzen	138
bb)	Serverseitig gespeicherte Daten	141
(1)	Bisherige Differenzierungsansätze	141
(2)	Technische Differenzierbarkeit	142
(3)	Verfassungsrechtliche Differenzierbarkeit	143
(α)	Übertragungsbezogener Schutz durch das Fernmeldegeheimnis	143
(β)	Systembezogener Schutz durch das IT-Grundrecht	146
(γ)	Datenbezogener Schutz durch das Recht auf informationelle Selbstbestimmung	151
(δ)	Konkurrenzen	151
cc)	Zwischenergebnis	153

B.	Eingriffscharakter von Maßnahmen	155
1.	Grundlagen	155
2.	Invasive Überwachungsmaßnahmen	156
a)	Maßnahmen der Paketfilterung	156
aa)	Ausnahmen für technisch bedingte Datenerfassungen und -auswertungen	157
bb)	Materielle Kriterien zur Feststellung des Eingriffscharakters	159
b)	Manipulation von DNS-Servern	163
3.	Teilnahme an der Kommunikation	165
a)	Autorisierungskonzept	166
b)	Sphärenkonzept	170
aa)	Abgestuftes Persönlichkeitsschutzmodell	171
bb)	Konzepte zur Abgrenzung zwischen Privat- und Öffentlichkeitssphäre	174
cc)	Fallgruppen	178
C.	Rechtfertigung von Eingriffen	180
1.	Verhältnismäßigkeit	181
a)	Bestimmung anhand Telekommunikationsphasen	183
aa)	Providerseitig laufende Telekommunikation	183
(1)	Eingriffsschwellen	184
(2)	Verfahrensvorkehrungen	185
(α)	Generelle Vorkehrungen	185
(β)	Vorkehrungen bei Drittbezug (insb. Server-TKÜ)	186
bb)	Nutzerseitig laufende Telekommunikation	188
(1)	Eingriffsschwellen	189
(2)	Verfahrensvorkehrungen	190
(α)	Sicherstellung der Maßnahmenbeschränkung	190
(β)	Flankierende Sicherheitsanforderungen	192
cc)	Lokal gespeicherte Daten	193
(1)	Eingriffsschwelle	194
(α)	Verdeckter Vollzugriff auf Daten und Systeme ...	194
(β)	Verdeckter Teilzugriff auf Daten und Systeme	195
(γ)	Offener Zugriff	197
(2)	Verfahrensvorkehrungen	199
(α)	Verdeckte Maßnahmen	199
(β)	Offene Maßnahmen	199
dd)	Serverseitig gespeicherte Daten	200
(1)	Eingriffsschwellen	201
(2)	Verfahrensvorkehrungen	204
(α)	Aufschieben der Benachrichtigung	204
(β)	Abgrenzung zwischen verdeckten und offenen Maßnahmen	206

b)	Bestimmung anhand funktionaler Faktoren	207
aa)	Daten in der Übertragung	208
(1)	Eingriffsschwellen	209
(2)	Verfahrensvorkehrungen	214
bb)	Serverseitig gespeicherte Daten	215
(1)	Eingriffsschwelle	215
(2)	Verfahrensvorkehrungen	216
c)	Bestimmung anhand spezifischer inhaltlicher Faktoren	216
aa)	Kernbereich privater Lebensgestaltung	216
(1)	Anwendbarkeit auf einzelne Fälle elektronischer Kommunikation	218
(2)	Schutz auf der Erhebungsebene	220
(3)	Schutz auf Auswertungsebene	227
bb)	Berufsgeheimnisse	229
2.	Bestimmtheitsgebot	230
a)	Eingriffe in den Übertragungsphasen	231
b)	Eingriffe in den Speicherphasen	231
aa)	Lokal gespeicherte Daten	231
bb)	Serverseitig gespeicherte Daten	233
c)	Gefahr von Kernbereichsverletzungen	234
D.	Zusammenfassung	235
II.	Schutz durch internationales und supranationales Recht	236
A.	Völkerrechtliche Gewährleistungen	236
1.	UN-Menschenrechtserklärung	237
2.	Internationaler Pakt über bürgerliche und politische Rechte	237
3.	EMRK	239
B.	Unionsrechtliche Vorgaben	240
1.	Primärrecht	240
a)	Art. 7 GRCh	241
b)	Art. 8 GRCh	242
c)	Verhältnis zum Grundgesetz	244
2.	Sekundärrecht	245

Teil 3

Umfang und Grenzen strafprozessualer Eingriffsermächtigungen

I.	Grundlagen	247
A.	Rechtsrahmen	247

1.	Entwicklung in Deutschland	247
2.	Cybercrime Convention des Europarates	250
3.	Unionsrechtlicher Einfluss	251
B.	Auslegung strafprozessualer Normen	252
II.	Erhebung von Daten in den Übertragungsphasen	253
A.	Erhebung beim Diensteanbieter	253
1.	Anordnungsvoraussetzungen	254
a)	Formell	254
b)	Materiell	255
2.	Reichweite: Telekommunikation i.S.d. § 100a StPO	257
a)	Bestehende Differenzierungsansätze	257
aa)	Anwendungsorientierte Konzepte	258
bb)	Transportorientierte Konzepte	259
b)	Rechtliche Differenzierbarkeit	261
aa)	Semantische Reichweite des Telekommunikationsbegriffs	262
bb)	Systematische Auslegung	264
cc)	Historische Auslegung	265
dd)	Teleologische Auslegung	266
ee)	Ergebnis	269
3.	Mitwirkungspflichten	270
a)	Gesetzliche Verpflichtungsebenen	271
aa)	§ 100a Abs. 4 Satz 1 StPO	271
bb)	§ 100a Abs. 4 Satz 2 StPO i.V.m. § 110 Abs. 1 Satz 1 TKG	272
cc)	TKÜV	274
dd)	TR TKÜV	276
b)	Internet-Zugangsanbieter (Access-Provider)	277
aa)	Adressaten	277
bb)	Ausgestaltung der Mitwirkungspflicht	280
(1)	Ausleitung des IP-Datenstroms	280
(2)	Technische und organisatorische Anforderungen	282
c)	Carrier und Routing-Anbieter (Network-Provider)	283
aa)	Adressaten	283
bb)	Ausgestaltung der Mitwirkungspflicht	285
(1)	Verpflichtung von Netzknoten	286
(2)	Verpflichtung anderer Routing-Anbieter	290
d)	Anbieter von Anwendungen (Hosting-Provider)	291
aa)	Adressaten	292

(1) Ansätze zur Bestimmung des Anwendungsbereichs des i.S.d. § 3 Nr. 24 TKG	293
(α) Funktionale Differenzierung	294
(β) Technische Differenzierung	296
(2) Funktionale Differenzierung nach Art des Dienstes	299
(α) Vermittlung bei dezentralisierter Telekommunikationsinfrastruktur	301
(β) Vermittlung bei zentralisierten Telekommunikationsplattformen	306
(γ) Zwischenergebnis	309
bb) Ausgestaltung der Mitwirkungspflicht	310
e) Anbieter von Infrastruktur (Server-Hosting- und Housing- Provider)	312
4. Verfahren	313
a) Kennzeichnungs- und Protokollpflichten	314
b) Löschpflichten	314
c) Benachrichtigungspflichten	315
d) Schutz vertraulicher Kommunikationsinhalte	316
aa) Berufsgeheimnisse	316
(1) Absolut geschützte Berufsgeheimnisträger	316
(2) Relativ geschützte Berufsgeheimnisträger	317
bb) Schutz des Kernbereichs privater Lebensgestaltung	318
(1) Verfahren in Bezug auf die Erhebungsebene	319
(2) Verfahren in Bezug auf die Auswertungsebene	320
5. Verhältnismäßigkeit	321
a) Überwachung des IP-Datenverkehrs	321
b) Drittbezug bei Server-TKÜ	322
B. Erhebung beim Nutzer	325
1. Quellen-TKÜ (§ 100a Abs. 1 Satz 2 StPO)	325
2. Weitere Maßnahmen	327
III. Erhebung von Daten in den Speicherphasen	328
A. Erhebung beim Nutzer	328
1. Offene Maßnahmen	328
a) Durchsuchung von Räumlichkeiten (§ 102 StPO)	328
b) Durchsicht (§ 110 Abs. 1 StPO) von Systemen und Datenträgern	329
aa) Reichweite	330
(1) Daten als Papiere i.S.d. § 110 Abs. 1 StPO	330
(2) Inbetriebnahme und Nutzung von IT-Systemen	331
bb) Mitnahme zur Durchsicht	331

(1) Verfahren	332
(α) Löschpflichten	333
(β) Anwesenheitsrechte	334
(γ) Protokollpflichten	334
(δ) Schutz des Kernbereichs privater Lebens- gestaltung	335
(2) Verhältnismäßigkeit	336
(α) Mitnahme von Hardware	336
(β) Kopieren von Daten	337
c) Sicherstellung und Beschlagnahme (§ 94 StPO)	339
aa) Reichweite: Daten als Gegenstände i.S.d. §§ 94 ff. StPO	340
bb) Verfahren	342
cc) Verhältnismäßigkeit	342
2. Verdeckte Maßnahmen	343
a) § 100b StPO	344
b) § 100a Abs. 1 Satz 3 StPO	346
aa) Verhältnismäßigkeit	347
bb) Bestimmtheit	350
cc) Technische Umsetzbarkeit	351
3. Mitwirkungspflichten	351
a) Pflichten des Beschuldigten	351
b) Pflichten Dritter (insb. von Hard- und Softwareherstellern und -lieferanten)	352
aa) Zeugenpflicht	353
bb) Anordnung der Herausgabe (§ 95 StPO)	354
(1) Reichweite	355
(2) Adressaten	358
(3) Anordnungsvoraussetzungen	359
(4) Verfahren	359
(5) Verhältnismäßigkeit	359
cc) Materielle Mitwirkungspflichten	363
B. Erhebung beim Diensteanbieter	363
1. Offene Maßnahmen	364
a) Durchsuchung bei anderen Personen (§ 103 StPO)	365
aa) Datenbestände keine „Sache“ i.S.d. §§ 102 f. StPO	366
bb) Gewahrsam an Datenbeständen	367
cc) Erforderlicher Konkretisierungsgrad	370
b) Durchsicht	370
aa) Durchsicht vor Ort erlangter Datenspeicher (§ 110 Abs. 1 StPO)	370
(1) Verfahren	371

(α) Anwesenheitsrechte, Protokoll- und Informationspflichten	371
(β) Weitere Verfahrensanforderungen	375
(2) Verhältnismäßigkeit	375
(α) Mitnahme von Hardware	376
(β) Kopieren von Daten	376
bb) Durchsicht räumlich getrennter Datenspeicher (§ 110 Abs. 3 StPO)	379
(1) Reichweite	380
(α) Lokal vernetzte Speichersysteme	380
(β) Webbasierte Speicherdienste (insb. Cloud-Storage-Dienste)	380
(γ) Andere webbasierte Dienste	381
(δ) Grad der Zugriffsmöglichkeit	382
(ε) Auslandsbezug	384
(2) Verfahren	384
(3) Verhältnismäßigkeit	386
c) Sicherstellung und Beschlagnahme (§ 94 StPO)	386
aa) Reichweite	386
bb) Verfahren	388
cc) Verhältnismäßigkeit	390
d) Mitwirkungspflichten	391
aa) Zeugenpflicht	392
bb) Anordnung der Herausgabe von Daten (§ 95 StPO)	393
(1) Reichweite	394
(α) Umfang der Editionspflicht (insb. zur Entschlüsselung von Daten)	394
(β) Gewahrsamsinhaber als Adressat	395
(γ) Adressat bei Speicherung im Ausland	395
(δ) Umsetzung der Cybercrime Convention	397
(2) Anordnungsvoraussetzungen	398
(3) Verfahren	399
cc) Umgehende Sicherung gespeicherter Computerdaten („Quick-Freeze“)	400
2. Verdeckte Maßnahmen	401
a) Postbeschlagnahme (§ 99 StPO)	401
b) Telekommunikationsüberwachung (§ 100a StPO)	403
aa) Reichweite	403
bb) Mitwirkungspflichten	406
cc) Durchführung eigener Maßnahmen	407
c) Online-Durchsuchung (§ 100b StPO)	409

Teil 4
Reformvorschläge

I. Erhebung von Daten in den Übertragungsphasen	411
A. Erhebung beim Diensteanbieter (Telekommunikationsüberwachung)	411
1. Reichweite des § 100a StPO	411
2. Mitwirkungspflichten	411
a) Internet-Zugangsanbieter (Access-Provider)	411
b) Carrier und Routing-Anbieter (Network-Provider)	412
c) Anbieter von Anwendungen (Hosting-Provider)	413
3. Anordnungsvoraussetzungen	414
4. Verfahren	416
a) Protokollpflichten	416
b) Schutz des Kernbereichs	417
aa) Verfahren in Bezug auf die Erhebungsebene	417
bb) Verfahren in Bezug auf die Auswertungsebene	419
5. Spezielle Konstellationen	422
a) Überwachung des IP-Datenverkehrs	422
b) TKÜ mit Drittbezug (insb. Server-TKÜ)	424
B. Erhebung beim Nutzer (Quellen-TKÜ)	425
II. Erhebung von Daten in den Speicherphasen	426
A. Erhebung beim Nutzer	427
1. Offene Maßnahmen	427
a) Durchsuchung und Durchsicht von Systemen und Datenträgern	427
aa) Reichweite	427
bb) Anordnungsvoraussetzungen	428
cc) Verfahren	430
(1) Löschpflichten	430
(2) Anwesenheitsrechte	431
(3) Protokoll- und Informationspflichten	431
(4) Schutz des Integritätsinteresses	432
(5) Schutz des Kernbereichs privater Lebensgestaltung	432
dd) Verhältnismäßigkeit	433
b) Sicherstellung und Beschlagnahme	433
aa) Reichweite, Anordnungsvoraussetzungen und Verfahren	433
bb) Regelungsvarianten	435
2. Verdeckte Maßnahmen	436
3. Mitwirkungspflichten	437

B. Erhebung beim Diensteanbieter	439
1. Offene Maßnahmen	439
a) Durchsuchung und Durchsicht von Systemen und Datenträgern	439
aa) Durchsicht vor Ort erlangter Daten	439
(1) Anordnungsvoraussetzungen	440
(2) Verfahren	440
bb) Durchsicht dezentraler Datenspeicher	441
(1) Reichweite	441
(2) Verfahren	442
(3) Verzicht auf Akzessorietät	442
b) Sicherstellung und Beschlagnahme	444
c) Mitwirkungspflichten	445
aa) Anordnung der Herausgabe von Daten	445
(1) Reichweite	445
(α) Daten als Gegenstand	445
(β) Umfang	445
(γ) Bezugspunkt	446
(2) Anordnungsvoraussetzungen und Verfahren	447
bb) Umgehende Sicherung gespeicherter Computerdaten („Quick-Freeze“)	448
2. Verdeckte Maßnahmen	448
Zusammenfassung	451
Literaturverzeichnis	455