

Das Recht der inneren und äußeren Sicherheit

Band 35

Präventiv-polizeiliche Zugriffe auf Telekommunikationsinhaltsdaten

Eine verfassungsrechtliche und einfach-gesetzliche Analyse unter
Einbeziehung kriminalistischer und technischer Implikationen

Von

Christoph Keller



Duncker & Humblot · Berlin

CHRISTOPH KELLER

Präventiv-polizeiliche Zugriffe auf
Telekommunikationsinhaltsdaten

Das Recht der inneren und äußeren Sicherheit

Herausgegeben von Prof. Dr. Dr. Markus Thiel, Münster

Band 35

Präventiv-polizeiliche Zugriffe auf Telekommunikationsinhaltsdaten

Eine verfassungsrechtliche und einfach-gesetzliche Analyse unter
Einbeziehung kriminalistischer und technischer Implikationen

Von

Christoph Keller



Duncker & Humblot · Berlin

Die Deutsche Hochschule der Polizei – Universität der Polizeien des Bundes und der Länder hat diese Arbeit Im Jahre 2024 als Dissertation angenommen.

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Alle Rechte vorbehalten

© 2026 Duncker & Humblot GmbH, Berlin

Satz: 3w+p GmbH, Rimpär

Druck: Beltz Grafische Betriebe GmbH, Bad Langensalza

ISSN 2199-3475

ISBN 978-3-428-19703-3 (Print)

ISBN 978-3-428-59703-1 (E-Book)

Gedruckt auf alterungsbeständigem (säurefreiem) Papier
entsprechend ISO 9706 ☺

Verlagsanschrift: Duncker & Humblot GmbH, Carl-Heinrich-Becker-Weg 9,
12165 Berlin, Germany | E-Mail: info@duncker-humblot.de

Internet: <http://www.duncker-humblot.de>

Vorwort

Die vorliegende Arbeit wurde von der Deutschen Hochschule der Polizei – Universität der Polizeien des Bundes und der Länder als Dissertation 2024 angenommen. Die mündliche Prüfung fand am 22. Juli 2025 statt.

Mein erster und herzlicher Dank gilt meinem geschätzten Doktorvater Prof. Dr. Dr. Markus Thiel für seine Unterstützung. Vor allem seine konstruktiven Anmerkungen und Hinweise haben wesentlich zum Gelingen der Arbeit beigetragen und waren für die Entstehung dieser Arbeit ebenso prägend wie bereichernd. Dabei hat Professor Thiel mir großen Freiraum bei der Auswahl des Themas und der Bearbeitung der Dissertation gelassen. Ohne ihn wäre diese Arbeit nicht möglich gewesen. Für die Aufnahme der Arbeit in die von ihm herausgegebene Schriftenreihe „Das Recht der inneren und äußeren Sicherheit“ bin ich ihm großen Dank schuldig.

Für die zügige Erstellung des Zweitgutachtens danke ich herzlich Prof. Dr. Claudio Franzius.

Auf dem Weg zu dieser Dissertation haben mich viele Menschen begleitet und in ihrer ganz eigenen Form unterstützt. Mein ganz besonderer Dank gilt dabei meiner Familie für ihre Unterstützung, Geduld und vor allem Nachsichtigkeit und damit der Gewährleistung meiner mentalen und emotionalen Stabilität während der Bearbeitungsphase. Ihr ist diese Dissertation gewidmet. Für eure uneingeschränkte Unterstützung danke ich euch von ganzem Herzen.

Im Hinblick auf die Veröffentlichung der Dissertation ergab sich das Erfordernis einer geringfügigen Überarbeitung. Ursächlich hierfür war der Koalitionsvertrag der Bundesregierung zwischen CDU, CSU und SPD vom 5.5.2025 sowie verfassungsgerichtliche Rechtsprechung, zuletzt die Entscheidungen des Bundesverfassungsgerichts zur polizeirechtlichen Ermächtigung der Telekommunikationsüberwachung nach § 20c PolG NRW (Beschl. v. 24.6.2025 – 1 BvR 2466/19 – Trojaner I) und zu den strafprozessualen Ermächtigungen zur Quellen-Telekommunikationsüberwachung und Online-Durchsuchung. (Beschl. v. 24.6.2025 – BvR 180/23 – Trojaner II).

Rechtsstand 15.8.2025

Mettingen, im August 2025

Dr. Christoph Keller

Inhaltsübersicht

Einleitung	27
A. Forschungsgegenstand	27
B. Begrenzung des Untersuchungsgegenstandes	32
C. Stand der Forschung	34
D. Forschungsziel	38
E. Gang der Darstellung	40

Teil 1

Technische und kriminalistische Grundlagen	42
A. Technischer Telekommunikationsbegriff	44
I. Begriffsinhalt	44
II. Begriffszweck: Regulierung der Telekommunikation, Datenschutz	45
III. Datenkategorien	48
IV. Technischer Ablauf einer (klassischen) TKÜ (TKÜV)	49
B. Datenkommunikation und Internet	54
I. Circuit Switched Networking	55
II. Packet Switched Networking	55
III. Infrastrukturen und Akteure des Internet	65
C. Systematisierung der (Tele-)Kommunikationsarten	69
I. Differenzierung nach zeitlichen Kriterien	70
II. Differenzierung nach funktionalen Kriterien	71
III. Kommunikationskonstellationen	74
D. Die Erhebung von Daten beim Diensteanbieter	76
I. Übertragungsphase	76
II. Speicherphase	104
E. Die Erhebung von Daten beim Nutzer	105
I. Übertragungsphase (Quellen-TKÜ)	105
II. Speicherphase	143
III. Smart Home-Technologie	151
F. Zusammenfassung	156

Teil 2

Verfassungsrechtliche Determinanten	158
A. Grundrechtsbetroffenheit	160
I. Telekommunikationsgeheimnis (Art. 10 GG)	160
II. Unverletzlichkeit der Wohnung (Art. 13 GG)	205
III. IT-System-Grundrecht (Art. 2 Abs. 1 i. V. m. 1 Abs. 1 GG)	208
IV. Recht auf informationelle Selbstbestimmung	231
V. Grundrechtskonkurrenzen zum Telekommunikationsgeheimnis	235
VI. Einzelfragen	244
VII. Quellen-TKÜ	315
B. Anforderungen an verfassungsrechtliche Rechtfertigung	342
I. Instrumente prozeduralen Grundrechtsschutzes	342
II. Verhältnismäßigkeit, Bestimmtheit und Normenklarheit	387
C. Staatliche Schutzpflichten	445
I. Schutzauftrag aus dem IT-System-Grundrecht	446
II. Schutzauftrag aus weiteren Verfassungsnormen	452
D. Zusammenfassung	454

Teil 3

Normativer Rahmen einfachgesetzlicher Ermächtigungen	457
A. Ermächtigungsgrundlagen des Bundes und der Länder im Überblick	458
I. Polizeigesetze des Bundes	458
II. Polizeigesetze der Länder	462
B. Die Erhebung von Daten beim Diensteanbieter	464
I. Gesetzliche Rechtsfolge: Telekommunikationsüberwachung	464
II. Einzelfragen	488
III. Eingriffsschwellen	525
IV. Polizeipflichtigkeit	565
V. Grundrechtsschutz durch Verfahren	569
C. Die Erhebung von Daten beim Nutzer	582
I. Datenerhebung in der Übertragungsphase: Quellen-TKÜ	583
II. Datenerhebung in der Speicherphase	629
III. Zugriff auf Smart Home-Technologie	654
D. Umgang mit IT-Sicherheitslücken	659
I. Zielkonflikt (Kryptokontroverse)	660
II. Fehlen spezieller Schutz- und Abwägungsmechanismen	682

III. Konzeptionelles Schwachstellenmanagement 701

IV. Unterstützung der Sicherheitsbehörden 714

E. EU-Cybersecurity-Rechtsrahmen 723

 I. NIS2-RL 724

 II. Cyber Resilience Act 726

F. Zusammenfassung 728

Teil 4

Thesen und Reformgesichtspunkte 732

Teil 5

Ausblick 755

Literaturverzeichnis 765

Sachwortregister 842

Inhaltsverzeichnis

Einleitung	27
A. Forschungsgegenstand	27
B. Begrenzung des Untersuchungsgegenstandes	32
C. Stand der Forschung	34
D. Forschungsziel	38
E. Gang der Darstellung	40

Teil 1

Technische und kriminalistische Grundlagen	42
A. Technischer Telekommunikationsbegriff	44
I. Begriffsinhalt	44
II. Begriffszweck: Regulierung der Telekommunikation, Datenschutz	45
III. Datenkategorien	48
IV. Technischer Ablauf einer (klassischen) TKÜ (TKÜV)	49
B. Datenkommunikation und Internet	54
I. Circuit Switched Networking	55
II. Packet Switched Networking	55
1. Systematisierung des Prozesses aus technischer Perspektive	55
2. Referenz-/Schichtenmodelle	59
a) ISO/OSI-Modell	59
b) TCP/IP-Modell (DoD-Schichtenmodell)	62
III. Infrastrukturen und Akteure des Internet	65
1. Nutzer und Provider	65
2. Wandel der Akteurskonstellationen	68
C. Systematisierung der (Tele-)Kommunikationsarten	69
I. Differenzierung nach zeitlichen Kriterien	70
1. Speicherungsphase	70
2. Übertragungsphase	70
II. Differenzierung nach funktionalen Kriterien	71
1. Interpersonelle Komponente	71

2. Intrapersonelle Komponente	71
3. Veranlassungsgrad des Übertragungsvorgangs	73
a) Klassischer Datenaustausch („unmittelbar veranlasst“)	73
b) Automatisierter Datenaustausch („mittelbar veranlasst“)	73
c) Autonomer Datenaustausch („nicht veranlasst“)	73
III. Kommunikationskonstellationen	74
1. Individualkommunikation: Mensch-zu-Mensch (H2H)	74
2. Datenkommunikation: Mensch-zu-Maschine (H2M und M2H)	74
3. Technische Kommunikation: Maschine-zu-Maschine (M2M)	75
4. Abgrenzung	75
D. Die Erhebung von Daten beim Diensteanbieter	76
I. Übertragungsphase	76
1. Technische Möglichkeiten der Paketanalyse	76
a) Daten-Header-Analyse	76
aa) Stateless Packet Inspection	76
bb) Stateful Packet Inspection	78
b) Nutzer-Daten-Analyse: Deep Packet Inspection (DPI)	79
2. Mitwirkungspflichten der Diensteanbieter	80
a) Access-Provider	80
b) Network-Provider	82
c) Hosting-Provider	83
3. Telekommunikation durch Individualkommunikation	83
a) E-Mail-Verkehr	84
aa) E-Mail-Anwendungen	84
bb) E-Mail-Protokolle	85
cc) Funktionsweise eines E-Mail-Systems	86
dd) Zugriff durch Sicherheitsbehörden	89
b) Sonstige textbasierte Kommunikationsformen	90
aa) Soziale Netzwerke	90
bb) Messenger-Dienste	91
4. Telekommunikation durch Datenkommunikation	95
a) Surfen im Internet	95
b) Browserfingerprinting	95
c) WLAN-Catching	98
d) Cloud Computing	101
II. Speicherphase	104
E. Die Erhebung von Daten beim Nutzer	105
I. Übertragungsphase (Quellen-TKÜ)	105
1. Sicherheitsgewährleistung durch kryptografische Verfahren	105
a) Nachrichtenschutz durch Verschlüsselung	106

b) Verschlüsselungssysteme	108
aa) Transportverschlüsselung	108
bb) Ende-zu-Ende-Verschlüsselung	111
c) Dechiffrierung verschlüsselter Kommunikationsdaten	114
2. Begriff und technischer Hintergrund der Quellen-TKÜ	117
3. Durchführung der Quellen-TKÜ	120
a) Primärmaßnahmen	120
b) Sekundärmaßnahmen	123
4. Infiltration des Zielsystems	125
a) Einsatz einer Backdoor	125
b) Nachträgliches Aufspielen einer Überwachungssoftware	126
aa) Physischer Zugriff	126
(1) Infiltration außerhalb der Wohnung	126
(2) Infiltration innerhalb der Wohnung	127
(3) Einsatz manipulierter Datenträger	127
bb) Fernzugriff mittels Überwachungssoftware	128
(1) Unbewusste Mitwirkung des Adressaten	128
(2) Man-In-The-Middle-Angriff	130
(3) Nutzung von Sicherheitslücken	130
(a) Software-Schwachstellen	130
(b) Klassifizierung von Sicherheitslücken und Exploits	135
(c) Schwachstellen-Ökosystem	139
c) De-Infiltration der Überwachungssoftware	142
II. Speicherphase	143
1. Fernzugriff	143
a) Erweiterte Quellen-TKÜ („Kleine Online-Durchsuchung“)	143
b) Online-Durchsuchung	144
2. Physischer Zugriff	145
a) Datensicherung	145
aa) Post-Mortem-Analyse	145
bb) Live-Sicherung	148
b) Datenanalyse	149
III. Smart Home-Technologie	151
F. Zusammenfassung	156

Teil 2

Verfassungsrechtliche Determinanten

158

A. Grundrechtsbetroffenheit	160
I. Telekommunikationsgeheimnis (Art. 10 GG)	160
1. Allgemeines, Historie	160
2. Übertragungsbezogener Schutz	164
a) Übermittlung „unkörperlicher“ Informationen	164
b) Zeitliche Reichweite	165
c) Entwicklungsoffene Grundrechtsgewährleistung	167
3. Sachlicher Schutzbereich	167
a) Inhaltliche Reichweite	167
aa) Schutz der Kommunikationsinhalte	168
bb) Schutz der Kommunikationsumstände	169
(1) Verkehrsdaten	169
(2) Kommunikationsbegleitende (technische) Daten	170
(3) Standortdaten	171
(4) Verwendung kryptographischer Verfahren	172
b) Beschränkung auf Individualkommunikation	173
c) Personale Begrenzung des (Tele-)Kommunikationsbegriffs	177
aa) Rechtsprechung des Bundesverfassungsgerichts	178
(1) BVerfG, Urt. v. 14. 7. 1999 – 1 BvR 2226/94 u. a.	178
(2) BVerfG, Beschl. v. 9. 10. 2002 – 1 BvR 1611/96 u. a.	178
(3) BVerfG, Urt. v. 27. 7. 2005 – 1 BvR 668/04	179
(4) BVerfG, Urt. v. 2. 3. 2006 – 2 BvR 2099/04	179
(5) BVerfG, Beschl. v. 22. 8. 2006 – 2 BvR 1345/03	180
(6) BVerfG, Urt. v. 27. 2. 2008 – 1 BvR 370, 595/07	181
(7) BVerfG, Beschl. v. 16. 6. 2009 – 2 BvR 902/06	182
(8) BVerfG, Urt. v. 20. 4. 2016 – 1 BvR 966/09 u. a.	183
(9) BVerfG, Urt. v. 2. 3. 2010 – 1 BvR 256/08 u. a.	184
(10) BVerfG, Beschl. v. 6. 7. 2016 – 2 BvR 1454/13	185
(11) BVerfG, Beschl. v. 24. 6. 2025 – 1 BvR 2466/19	187
bb) Literatur	191
(1) Formal-technische Betrachtung	191
(2) Unipersonale Betrachtung	193
(3) Multipersonale Betrachtung	195
cc) Stellungnahme	197
d) Erfordernis willensgesteuerter Kommunikation	199
aa) Rechtsprechung des Bundesverfassungsgerichts	199
(1) BVerfG, Beschl. v. 22. 8. 2006 – 2 BvR 1345/03	199

(2) BVerfG, Beschl. v. 6. 7. 2016 – 2 BvR 1454/13	200
bb) Literatur	201
(1) Formale Betrachtung	201
(2) Funktionale Betrachtung	201
cc) Stellungnahme	202
e) Zwischenergebnis	202
4. Verfassungsrechtliche Rechtfertigung	204
II. Unverletzlichkeit der Wohnung (Art. 13 GG)	205
1. Allgemeines, Historie	205
2. Schutzbereich	206
3. Verfassungsrechtliche Rechtfertigung	207
III. IT-System-Grundrecht (Art. 2 Abs. 1 i. V. m. 1 Abs. 1 GG)	208
1. Allgemeines, Historie	208
2. Schutz informationstechnischer Systeme	213
a) Das IT-System	213
b) Nutzung des IT-Systems „als eigenes“	216
3. Sachlicher Schutzbereich	219
a) Schutzziel: Vertraulichkeit	219
b) Schutzziel: Integrität	220
c) Schutzziele als eigenständige Schutzgewährleistungen	223
d) Heimlichkeit als Schutzbereichsbeschränkung?	226
4. Anwendbarkeit auf juristische Personen	228
5. Verfassungsrechtliche Rechtfertigung	230
IV. Recht auf informationelle Selbstbestimmung	231
1. Allgemeines, Historie	231
2. Schutzbereich	232
3. Verfassungsrechtliche Rechtfertigung	234
V. Grundrechtskonkurrenzen zum Telekommunikationsgeheimnis	235
1. Verhältnis zum IT-System-Grundrecht	235
2. Verhältnis zum Recht auf informationelle Selbstbestimmung	238
3. Verhältnis zur Unverletzlichkeit der Wohnung	240
4. IT-System-Grundrecht und Recht auf informationelle Selbstbestimmung	240
5. IT-System-Grundrecht und Unverletzlichkeit der Wohnung	242
VI. Einzelfragen	244
1. Internettelefonie und Messenger-Dienste	244
2. IP-basierte (intrapersonelle) Kommunikation	245
a) Charakteristika der Internetkommunikation	245
b) (Kein) Eingriff in Telekommunikationsgeheimnis	253
aa) BVerfG, Beschl. v. 6. 7. 2016 – 2 BvR 1454/13	253

bb) Literatur	258
(1) Surfen im Internet als Kommunikation	258
(2) Surfen im Internet als Nicht-Kommunikation	259
c) (Kein) Eingriff in IT-System-Grundrecht	260
d) Verbleibender Grundrechtsschutz	261
aa) Telekommunikationsgeheimnis als „Zweifelsregel“	261
bb) Recht auf informationelle Selbstbestimmung	262
e) Zwischenergebnis: Grundrechtseingriff „eigener Art“	266
3. Browserfingerprinting	272
4. E-Mail-Verkehr	273
a) Phasenmodell	273
b) Dynamische Übertragungsphase	277
aa) Versenden und Empfangen von E-Mails	277
bb) Schutz von versandten E-Mails über Verteiler	277
c) Statische Übertragungsphase	278
aa) Zwischenspeicherung beim Provider	278
bb) Endspeicherung beim Provider	280
(1) Abgrenzung von Zwischen- und Endspeicherung	280
(a) Abgrenzung anhand Lesestatus des Empfängers	280
(b) Abgrenzung anhand zeitlicher Kriterien	281
(c) Abgrenzung anhand Login des Empfängers	281
(2) Anwendbarkeit des Telekommunikationsgeheimnisses	282
(a) Formal-technischer Ansatz	282
(b) Funktionaler Ansatz	283
(c) Funktional-technischer Ansatz	284
(d) BVerfG, Beschl. v. 16. 6. 2009 – 2 BvR 902/06	285
(e) Caveat aus der Literatur	286
(f) Zwischenergebnis	290
(3) Anwendbarkeit des IT-System-Grundrechts	292
cc) Endspeicherung beim Nutzer: Schutz lokaler Daten	293
(1) BVerfG, Beschl. v. 4. 2. 2005 – 2 BvR 308/04	293
(2) BVerfG, Urt. v. 2. 3. 2006 – 2 BvR 2099/04	294
d) Zwischenergebnis	296
5. Soziale Netzwerke, Foren, Newsgroups	297
a) Schutz der Kommunikation in Sozialen Netzwerken	297
b) Schutz der Kommunikation in (Web-)Foren	298
c) Schutz der Kommunikation in Newsgroups	298
d) Zwischenergebnis	299

6. Cloud Computing	300
a) Cloud-Storage	300
aa) Zugriff auf dem Endgerät des Nutzers	300
bb) Zugriff auf den (Daten-)Übertragungsweg	300
(1) Up- und Download der Daten	300
(2) Synchronisation der Daten	301
(3) Stellungnahme	302
cc) Zugriff auf die Cloud	303
b) Cloud Collaboration	306
c) Zwischenergebnis	307
7. Smart Home-Technologie	308
a) Eingriff in Telekommunikationsgeheimnis	308
b) Eingriff in IT-System-Grundrecht	309
c) Eingriff in Wohnungsgrundrecht	310
d) Zwischenergebnis	311
8. WLAN-Netze (WLAN-Catching)	311
VII. Quellen-TKÜ	315
1. Klassische Quellen-TKÜ	315
a) Eingriff in Telekommunikationsgeheimnis	315
aa) Begrenzung auf laufende Kommunikation	315
bb) Verschlüsselungsspezifische Kommunikationsbezüge	319
b) Eingriff in IT-System-Grundrecht	322
c) Zwischenergebnis	326
2. Erweiterte Quellen-TKÜ („Kleine Online-Durchsuchung“)	328
a) Eingriff in Telekommunikationsgeheimnis	328
b) Eingriff in IT-System-Grundrecht	332
c) Zwischenergebnis	335
3. Vorbereitungshandlungen in Wohnung	339
B. Anforderungen an verfassungsrechtliche Rechtfertigung	342
I. Instrumente prozeduralen Grundrechtsschutzes	342
1. Kernbereich privater Lebensgestaltung	342
a) Inhalt und Schutzwirkung	343
aa) Historie	343
bb) Achtungsanspruch	345
b) Spezifizierung kernbereichsrelevanter Inhalte	346
aa) Begriff des Kernbereichs	346
bb) Anwendbarkeit auf Fälle elektronischer Kommunikation	349
c) Schutzkonzept	351
aa) Schutz auf erster Stufe	351
(1) Bedeutungsverlust des Kernbereichsschutzes	351

(2) Grundrechtsschutz durch technische Verfahren	362
(a) Informationstechnische Sicherungsmechanismen	362
(b) Einsatz künstlicher Intelligenz (KI)	364
bb) Schutz auf zweiter Stufe	375
2. Besonderer Schutz von Berufsgeheimnisträgern	378
3. Verfahrensvorkehrungen	380
a) Vorabkontrolle durch unabhängige Stelle	380
b) Aufsichtliche (Datenschutz-)Kontrolle	383
c) Dokumentation, Kennzeichnung, Berichtspflichten	384
d) Löschung	386
e) Effektiver Rechtsschutz durch Benachrichtigung	386
II. Verhältnismäßigkeit, Bestimmtheit und Normenklarheit	387
1. Der Dualismus von Eingriffsintensität und Eingriffsschwellen	387
a) Eingriffsintensität	387
b) Eingriffsschwellen	388
aa) Vorhersehbarkeit des Geschehensablaufs	388
bb) Rechtsgüterschutz	389
c) Maßnahmen unterschiedlicher Klassifikationsstufen	394
aa) Maßnahmen geringer und mittlerer Intensität	394
bb) Maßnahmen hoher Intensität	395
cc) Maßnahmen höchster Intensität	397
d) Extrapolationen durch Verfassungsrechtsprechung	399
aa) BVerfG, Urt. v. 20.4.2016 – 1 BvR 966/09 u.a.	399
bb) BVerfG, Beschl. v. 27.5.2020 – 1 BA 1873/13 u.a.	405
cc) BVerfG, Urt. v. 26.4.2022 – 1 BvR 1619/17	406
dd) BVerfG, Beschl. v. 9.12.2022 – 1 BvR 1345/21	406
ee) BVerfG, Urt. v. 16.2.2023 – 1 BvR 1547/19, 2634/20	407
e) Komplementäre Kategorien der Eingriffsqualität	408
aa) Additive Grundrechtseingriffe	408
bb) Überwachungsgesamtrechnung	412
(1) Begrifflichkeit und Genese	412
(2) Konzeptionelle Modelle	417
(a) Überwachungsatlas	417
(b) Periodischer Überwachungsbarometer	418
(c) Freiheitsbestandsanalyse	422
(d) Projekt „HEAT“	424
(e) Pragmatische Ansätze (Forum Privatheit)	425
(f) Mathematisch-ökonomische Analyse	426
(g) Variable Vergleichsmatrix („Bewegliches System“)	427

(3) Institutionalisierte Prozess	429
(a) Gesetzgebung und Gesetzesfolgenabschätzung	429
(b) Aufgabenübertragung an unabhängige Stellen	432
(c) Freiheitskommission	432
(4) Evaluation	436
cc) Stellungnahme	437
2. Bestimmtheit, Normenklarheit, Wesentlichkeitsvorbehalt	441
C. Staatliche Schutzpflichten	445
I. Schutzauftrag aus dem IT-System-Grundrecht	446
II. Schutzauftrag aus weiteren Verfassungsnormen	452
1. Art. 87 f GG: Post und Telekommunikation	452
2. Art. 91c GG: Informationstechnische Systeme	452
D. Zusammenfassung	454

Teil 3

Normativer Rahmen einfachgesetzlicher Ermächtigungen	457
A. Ermächtigungsgrundlagen des Bundes und der Länder im Überblick	458
I. Polizeigesetze des Bundes	458
1. Bundeskriminalamtgesetz (BKAG)	458
a) Klassische TKÜ	458
b) Quellen-TKÜ	459
2. Bundespolizeigesetz (BPolG)	459
3. Zollfahndungsdienstgesetz (ZfdG)	461
a) Klassische TKÜ	461
b) Quellen-TKÜ	461
II. Polizeigesetze der Länder	462
1. Klassische TKÜ	462
2. Quellen-TKÜ	463
B. Die Erhebung von Daten beim Diensteanbieter	464
I. Gesetzliche Rechtsfolge: Telekommunikationsüberwachung	464
1. Begriff der Telekommunikation	465
a) Technischer Telekommunikationsbegriff	465
b) Verfassungsrechtlicher Telekommunikationsbegriff	466
aa) Differenzierungsansätze	467
(1) Weiter Telekommunikationsbegriff	467
(2) Enger Telekommunikationsbegriff	467
bb) Schutzbereichseröffnung und Eingriffstatbestand	468

c)	Einfachgesetzlicher Telekommunikationsbegriff	470
aa)	Auslegungsziel	470
(1)	Objektive Auslegungstheorie	470
(2)	Subjektive Auslegungstheorie	472
(3)	Kombination objektiver und subjektiver Ansätze	473
bb)	Auslegungskriterien	475
(1)	Wortlaut des Gesetzes	475
(2)	Systematische Auslegung	476
(3)	Historische Auslegung	477
(4)	Teleologische Auslegung	478
cc)	Zwischenergebnis	479
2.	Gesetzlicher Begriff der Überwachung	481
a)	Die „Überwachung“ im System der Eingriffsbefugnisse	481
b)	Extensive Auslegung des Überwachungsbegriffs	482
c)	Restriktive Auslegung des Überwachungsbegriffs	484
d)	Zwischenergebnis	487
3.	Aufzeichnung der Telekommunikation	487
II.	Einzelfragen	488
1.	Internettelefonie und Messenger-Dienste	488
2.	IP-basierte (intrapersonelle) „Telekommunikation“	488
3.	Browserfingerprinting	492
4.	E-Mail-Verkehr	493
a)	Vorfeldphase	493
aa)	Client-basiertes Entwerfen von E-Mails	493
bb)	Server-basiertes Entwerfen von E-Mails	494
b)	Dynamische Übertragungsphase	495
c)	Statische Übertragungsphase	495
aa)	Zwischenspeicherung beim Provider	496
(1)	Datenerhebung durch TKÜ	496
(2)	Datenerhebung durch Sicherstellung	498
(3)	Datenerhebung durch Online-Durchsuchung	502
bb)	Endspeicherung beim Provider	503
(1)	Datenerhebung durch TKÜ	503
(2)	Datenerhebung durch Sicherstellung	508
(a)	Offener Zugriff	508
(b)	Verdeckter Zugriff	513
(3)	Datenerhebung durch Online-Durchsuchung	514
cc)	Endspeicherung beim Empfänger	515
dd)	Datenerhebung durch Postsicherstellung	515
d)	Zwischenergebnis	516

5. Soziale Netzwerke, Foren, Newsgroups	517
6. Cloud-Computing	518
a) Cloud Collaboration	518
b) Cloud-Storage	518
aa) Zugriff in der Übertragungsphase	518
bb) Zugriff in der Speicherphase	520
(1) Datenerhebung beim Nutzer	520
(a) Offene Maßnahmen	520
(b) Verdeckte Maßnahmen	520
(2) Datenerhebung beim Diensteanbieter	521
(a) Offene Maßnahmen	521
(b) Verdeckte Maßnahmen	521
c) Zwischenergebnis	522
7. WLAN-Catching	523
8. IMEI-gestützte Überwachung	524
III. Eingriffsschwellen	525
1. Vorbemerkungen: Polizeirechtliche Präemption	525
a) Klassisches Polizeirecht	525
b) Abkehr von der traditionellen Eingriffssystematik	528
c) Konkretisierte Gefahr für hinreichend gewichtiges Rechtsgut	533
aa) Terminus der konkretisierten (drohenden) Gefahr	533
bb) Dogmatische Einordnung der konkretisierten Gefahr	535
(1) Konkretisierte Gefahr als aliud zur konkreten Gefahr	535
(2) Konkretisierte Gefahr als Unterfall der konkreten Gefahr	536
2. Abwehr dringender oder gegenwärtiger Gefahren	540
3. Verhütung schwerer Straftaten	544
a) Tatsachenbasierte Gefahr einer Straftat	544
b) Verhaltensbasierte Gefahr einer Straftat	550
aa) BVerfG als „Ersatzgesetzgeber“	550
bb) Bestimmtheitsgebot	552
c) Rechtsgüterschutz	553
aa) Anknüpfung an strafrechtliche Wertungen	553
bb) Einbeziehung von Vorfeldstraftatbeständen	556
cc) Zu weit gefasste Straftatenkataloge	560
dd) Zielrichtung der Straftaten	562
IV. Polizeipflichtigkeit	565
1. Nachrichtenmittler	565
2. Technikmittler	566
3. Unbeteiligte Dritte	568

V.	Grundrechtsschutz durch Verfahren	569
1.	Kernbereichsschutz	569
a)	Schutz auf erster Stufe (Erhebungsphase)	570
aa)	Formelhafte Tatbestände	570
bb)	Einsatz informationstechnischer Sicherungen	572
b)	Schutz auf zweiter Stufe (Auswertungsphase)	573
c)	Schutz der Berufsheimlichkeitsinhaber	575
2.	Anordnung und Verfahren	577
3.	Benachrichtigungspflichten	577
a)	Grundsätze zur Benachrichtigung	577
b)	Benachrichtigung bei (laufender) Internetkommunikation	578
4.	Datenschutzrechtliche Vorkehrungen	579
a)	Aufsichtliche (Datenschutz-)Kontrolle	579
b)	Kennzeichnung	580
c)	Löschung	580
5.	Berichtspflichten und Befristungsregelungen	580
C.	Die Erhebung von Daten beim Nutzer	582
I.	Datenerhebung in der Übertragungsphase: Quellen-TKÜ	583
1.	Gesetzliche Rechtsfolge	583
a)	Primärmaßnahmen	583
aa)	Zugriff auf „laufende Kommunikation“	583
bb)	Erstellung von Application-Shots	585
b)	Sekundärmaßnahmen	586
aa)	(Heimliches) Betreten der Wohnung des Betroffenen	586
bb)	Infiltration der Überwachungssoftware auf dem Zielsystem	589
2.	Eingriffsschwellen	590
3.	Polizeipflichtigkeit	591
4.	Grundrechtsschutz durch Verfahren	591
a)	Kernbereichsschutz	591
b)	Anordnung, Verfahren, Datenschutz	592
5.	Anforderungen an Überwachungssoftware	592
a)	Technische Implikationen	592
aa)	Monofunktionalität der Software	592
bb)	Zugriffsbeschränkungen	596
(1)	Technische Beschränkungen	596
(2)	Rechtliche Beschränkungen	598
cc)	Zwischenergebnis	599
b)	Entwicklung der Software	600
aa)	Verwendung kommerzieller Software	601
(1)	Verstoß gegen Funktionsvorbehalt für Beamte	601

(2) Datensicherheitsrechtliche Friktionen	604
(3) Kontrolleinschränkung durch fehlenden Quellcode	605
(4) Vertrauenswürdigkeit privater Anbieter	608
bb) Entwicklung und Einsatz von Software durch das BKA	609
cc) Grundsatz der digitalen Souveränität	612
c) Vornahme (nur) unerlässlicher Systemveränderungen	613
d) Rückgängigmachung von Systemveränderungen	614
e) Schutz gegen unbefugte Nutzung	616
f) Schutz der kopierten Daten	620
g) Organisatorisch-prozedurale Sicherungen	621
aa) Vorabkontrolle der Software	621
(1) Zertifizierung durch unabhängige Stellen	621
(2) Offenlegung des Quellcodes	623
bb) Kontrolle der (konkreten) Überwachungsmaßnahme	625
cc) Ex-Post-Kontrolle (Unterrichtungspflicht)	627
dd) Protokollierungspflichten	627
II. Datenerhebung in der Speicherphase	629
1. Verdeckte Maßnahmen: Fernzugriff	629
a) Erweiterte Quellen-TKÜ („kleine Online-Durchsuchung“)	629
b) Online-Durchsuchung	632
c) Stellungnahme	636
2. Offene Maßnahmen: Physischer Zugriff	637
a) Durchsuchung von Speichermedien	637
b) Sicherstellung von Daten	642
c) Stellungnahme	650
III. Zugriff auf Smart Home-Technologie	654
1. Datenerhebung durch TKÜ	654
2. Datenerhebung durch Online-Durchsuchung	655
3. Datenerhebung durch Sicherstellung	657
4. Stellungnahme	659
D. Umgang mit IT-Sicherheitslücken	659
I. Zielkonflikt (Kryptokontroverse)	660
1. Auswirkungen auf die IT-Sicherheitslage	660
2. Staatliche (offensiv-defensiv) Dilemmata	671
3. Einschätzungsprärogative des Staates	674
4. Rechtsprechung des BVerfG (IT-Sicherheitslücken)	677
a) BVerfG, Beschl. v. 8. 6. 2021 – 1 BvR 2771/18	677
b) BVerfG, Beschl. v. 20. 1. 2022 – 1 BvR 1552/19	680
II. Fehlen spezieller Schutz- und Abwägungsmechanismen	682
1. Gesetzliche Schutzregelungen	682

2. Datenschutz-Folgenabschätzung	685
a) Risikoanalyse durch Datenschutzfolgenabschätzung	685
b) Anwendbarkeit des § 67 BDSG	687
aa) Vorliegen eines Datenverarbeitungsvorgangs	687
bb) Vorliegen einer neuen Technologie	689
cc) Bestimmtheitsgebot	689
dd) Fachkompetenz und Unabhängigkeit der Entscheider	690
3. Untergesetzliche Regelungen	691
4. Institutioneller Umgang mit Sicherheitslücken	692
a) Bundesamt für Sicherheit in der Informationstechnik (BSI)	692
aa) BSI als zentrale Ordnungsbehörde der IT-Sicherheit	692
bb) Unterrichtung des BSI als Meldestelle (Bund)	693
cc) Cyberabwehrbefugnisse	696
(1) Warnungen des BSI	696
(2) Untersuchungs-, Kontroll- und Anordnungsrechte	698
b) Cybersicherheitsagentur (Baden-Württemberg)	699
c) IT-Sicherheitsarchitektur	700
III. Konzeptionelles Schwachstellenmanagement	701
1. Kontrollprozesse	701
a) Vulnerability Equities Process (VEP)	701
b) Coordinated Vulnerability Disclosure (CVD)	705
2. Stellungnahme zum Schwachstellenmanagement	709
IV. Unterstützung der Sicherheitsbehörden	714
1. Unterstützung durch Behörden (ZITiS)	714
2. Unterstützung durch private Dienstleister	715
a) Ethisches Hacken „White Hat Hacking“	715
b) Ankauf von Sicherheitslücken	718
c) Gesetzliche Restriktionen als Alternative	720
aa) Bundes-Backdoor	720
bb) Regulierung von Verschlüsselung	722
(1) Key Escrow	722
(2) Verbot bestimmter Verschlüsselungsverfahren	722
E. EU-Cybersecurity-Rechtsrahmen	723
I. NIS2-RL	724
II. Cyber Resilience Act	726
F. Zusammenfassung	728

Inhaltsverzeichnis	25
--------------------	----

Teil 4

Thesen und Reformgesichtspunkte	732
--	-----

Teil 5

Ausblick	755
-----------------	-----

Literaturverzeichnis	765
-----------------------------------	-----

Sachwortregister	842
-------------------------------	-----

Abbildungsverzeichnis

Abbildung 1: ISO/OSI-Referenzmodell	60
Abbildung 2: Vergleich ISO/OSI- und TCP/IP-Referenzmodell	64
Abbildung 3: TCP/IP-Schichten und zugehörige Protokolle	65
Abbildung 4: Requests for Comments (RFCs)	86
Abbildung 5: Versenden und Abrufen einer E-Mail	88
Abbildung 6: Typischer Lebenszyklus von 0-Day-Schwachstellen	137
Abbildung 7: Verwendung von Schwachstellen: Nutzen und Risiken	142
Abbildung 8: E-Mail-Phasenmodell	275
Abbildung 9: Kategorien des Rechtsgutsgewichts	390
Abbildung 10: Der Vulnerability Equities Process in den USA	702
Abbildung 11: Staatlicher Schwachstellenmanagement-Prozess	704

Aus Gründen der besseren Lesbarkeit wird bei Personenbezeichnungen und personenbezogenen Hauptwörtern die männliche Form verwendet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter sowie auf diverse und non-binäre Personen. Die verkürzte Sprachform hat nur redaktionelle Gründe und beinhaltet keine Wertung.

Einleitung

A. Forschungsgegenstand

Zur staatlichen Aufgabe der Gewährleistung der Sicherheit und des Spezialgebiets der Cybersicherheit bedient sich der Staat insbesondere der Mechanismen der Gefahrenabwehr, also dem präventiven Einschreiten zur Verhinderung oder Minimierung von Schäden.¹ In diesem Aufgabenfeld gehören sicherheitsbehördliche Informationseingriffe zu den zentralen Arbeitsgrundlagen der Sicherheitsbehörden. Durch – vor allem verdeckte – Datenerhebungen wird primär der Zweck verfolgt, eine ausreichende Informationsgrundlage zu erhalten, um Gefahren näher auszuforschen und sodann die erforderlichen präventiven (und/oder repressiven) Maßnahmen zu treffen. Die Notwendigkeit verdeckter Datenerhebungen speziell zur Bekämpfung der Terrorismusbekämpfung oder der sog. Organisierten Kriminalität (OK) ergibt sich daraus, dass diesen Kriminalitätsphänomenen mit klassischen kriminalistischen Methoden wirksam nicht begegnet werden kann. Insbesondere im Bereich des internationalen Terrorismus ist zu beobachten, dass sich Personen moderner Technologien bedienen, um bei ihren Vorhaben einer Entdeckung zu entgehen und damit eine wirksame Gefahrenabwehr zu vereiteln.² Auch im militärpolitischen Geschehen sind entscheidende Änderungen eingetreten, die unter der Bezeichnung „hybride Kriegsführung“ diskutiert werden. Kennzeichnend ist die Verschleierung der Urheberchaft von schädigenden Maßnahmen, insbesondere auch Cyberattacken.³ Zunehmend werden elektronische Kommunikationswege genutzt, um Straftaten zu planen und zu begehen. Die Sicherheitsbehörden sind daher verstärkt auf Beweismittel in elektronischer Form angewiesen. So kommen derzeit bei 85 % aller strafrechtlichen Ermittlungen digitale Daten zum Einsatz.⁴ Bei den Informationseingriffen gehört die Kenntnisnahme der Sicherheitsbehörden von den Inhalten der Telekommunikation zu den tiefgreifendsten Eingriffen in die Rechte der von dieser Überwachung Betroffenen. Die Telekommunikationsüberwachung (TKÜ) gehört zu den bedeutsamsten Mitteln der verdeckten Informationsbeschaf-

¹ Vgl. *Brodowski*, in: Kipker, *Cybersecurity*, Kap. 17 Rn. 89.

² Vgl. *Graulich*, in: Lisen/Denninger, *Hdb Polizeirecht*, Kap. E. Rn. 794.

³ Vgl. *Spies-Otto*, in: Hornung/Schallbruch, *IT-Sicherheitsrecht*, § 19 Rn. 1 f.

⁴ Vgl. *Weiß/Pradel*, *CCZ* 2024, 102.

fung, ist aber zugleich in ihren verschiedenen Facetten ein rechtlich und technisch komplexer Ausschnitt verdeckter Datenerhebungen. Im Rahmen von TKÜ-Maßnahmen stoßen die Sicherheitsbehörden vor dem Hintergrund einer (stetig) fortschreitenden Digitalisierung allerdings dann an ihre Grenzen, wenn informationstechnologische Endgeräte unter Nutzung kryptologischer Verfahren zur Vorbereitung schwerer Straftaten genutzt werden. In diesem Zusammenhang steht insbesondere die Referenzgruppe der Messenger-Dienste („Instant-Messaging-Dienste“) im Fokus der Betrachtung, z. B. „WhatsApp“, „Telegram“ oder „Signal“. Sind solche kryptografischen Sicherungen standardmäßig in dem technischen Repertoire von Kommunikationsanwendungen integriert, ist der Zugriff auf den verwertbaren Inhalt der Information grundsätzlich nur noch an der Quelle (d. h. auf dem Endgerät des Absenders oder Empfängers) möglich, solange die Kommunikationsinhalte dort noch unverschlüsselt bzw. wieder entschlüsselt vorliegen. Messenger-Dienste sind einer der Hauptgründe für die Einführung von Befugnissen zur sog. Quellen-Telekommunikationsüberwachung (Quellen-TKÜ), bei der typischerweise – etwa durch das gezielte Ausnutzen von Sicherheitslücken – mit Überwachungssoftware („Staatstrojaner“) in von Zielpersonen genutzte informationstechnische Systeme eingegriffen wird, um Kommunikationsdaten von dort noch vor einer Verschlüsselung ausleiten zu können. Das zum Zwecke der Quellen-TKÜ vielfach erforderliche Ausnutzen von Sicherheitslücken birgt indes Risiken für die IT-Sicherheit. Der sich als (Schutz-)Pflichtenkollision darstellende Zielkonflikt („Kryptokontroverse“) zwischen Grundrechtsschutz und staatlicher Sicherheitsgewährleistung bedarf einer näheren Betrachtung. Im Diskussionskern steht die Frage, ob die „fragile Balance zwischen Sicherheit und Freiheit“⁵ gewahrt wird. Insbesondere stellt sich die Frage des Umgangs mit Sicherheitslücken, die vielfach erst ein unbemerktes „Einschleusen“ technischer Mittel („Trojaner“) in das informationstechnische System als Zielobjekt ermöglichen. Ein geordnetes und kontrollierbares Schwachstellenmanagement mit formalisierten Rahmenbedingungen gibt es bislang in Deutschland nicht. Im Hinblick auf die angesprochene Quellen-TKÜ ist zu untersuchen, ob die in einigen Polizeigesetzen (Mecklenburg-Vorpommern, Saarland, Zoll) eingeführte sog. „erweiterte Quellen-TKÜ“ („kleine Online-Durchsuchung“⁶) den verfassungsrechtlichen Maßstäben genügt. Der Gesetzgeber lässt zu, gespeicherte Inhalte und Umstände verschlüsselt erfolgender Telekommunikationsvorgänge („während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form“) zu überwachen, die hätten überwacht werden können, wenn sie unverschlüsselt erfolgt wären. Das Ergebnis ist von Bedeutung im Hinblick auf die an Eingriffsermächtigungen zu stellenden Anforderungen und führt zu der Frage, ob die derzeit angewandten Ermittlungsmethoden überhaupt durch vorhandene Eingriffsgrundlagen gedeckt sind bzw. ob die präventiv-polizeilichen Befugnisse für Zugriffe auf Telekommunikationsdaten mit den

⁵ Herrmann, Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, S. 21.

⁶ Thiel, in: Dietrich et al., Hdb Sicherheits- und Staatsschutzrecht, § 24 Rn. 14.

technologischen Entwicklungen Schritt gehalten haben. Während der rechtliche Umgang mit Technik in den vergangenen Jahrzehnten zur Routine geworden war – die ganz überwiegend abstrakt gefassten Gesetze, Verordnungen und Richtlinien konnten in einem mehr schleichenden Prozess auf durch Technik veranlasste Probleme konkretisiert werden –, gehört die Frage, ob das in Grundrechte eingreifende Recht mit der neuen Entwicklung Schritt halten kann, zu den derzeit vieldiskutierten Aspekten.⁷ Auszugehen ist davon, dass die enorme Geschwindigkeit der technologischen Entwicklung die Informations- und Kommunikationstechnologie zwar schneller und zuverlässiger gemacht hat, auf der anderen Seite aber neue Bedrohungen für die Cybersicherheit verursacht hat. Angesichts der zunehmenden Abhängigkeit moderner Gesellschaften von der Informations- und Kommunikationstechnologie ist Cybersicherheit zu einem vorrangigen Thema geworden und gilt als „komplexe globale Herausforderung“⁸. Ob Rechtsprechung und Rechtswissenschaft neue Techniken, ihre Wirkweisen, Gefahrenpotenziale sowie Möglichkeiten der Risikominimierung hinreichend berücksichtigen,⁹ bedarf einer näheren Untersuchung, vor allem im Hinblick auf die Frage, ob die derzeitigen Rechtsgrundlagen ausreichend sind, um neue (technisch-basierte) Eingriffe rechtssicher zu bewerten. Die herausragende Bedeutung von informationstechnischen Systemen für den Alltag der meisten Menschen hat für präventiv-polizeiliches Handeln essenzielle Informationen bereits seit längerem kontinuierlich in digitale Sphären verlagert.¹⁰ Die Datenerhebung durch Sicherheitsbehörden aus digitalen Sphären stellt inzwischen einen „Grundpfeiler moderner Gefahrenabwehr“¹¹ dar. Mittlerweile sehen sowohl der Bund als auch alle Bundesländer spezielle Ermächtigungsgrundlagen für präventiv-polizeiliche Eingriffe in das Telekommunikationsgeheimnis vor. Die Ermächtigungen legitimieren Eingriffe in das Grundrecht des Art. 10 Abs. 1 Var. 3 GG und knüpfen in ihrer Rechtsfolge an den Begriff „Telekommunikation“ an, der den sachlichen Anwendungsbereich der TKÜ-Ermächtigungen umschreibt und zugleich begrenzt. Während die TKÜ bei herkömmlichen Telefongesprächen vor allem auf Gesprächsinhalte beschränkt ist, können die Sicherheitsbehörden allerdings weitaus mehr Informationen erlangen, da in der Praxis nicht nur auf laufende („flüchtige“) Kommunikationsprozesse zugegriffen wird, sondern vielmehr auch – mitunter bereits seit Jahren – gespeicherte Nachrichten („Nicht-Kommunikationsdaten“) erhoben werden, die sich häufig auf alle Bereiche des privaten und beruflichen Lebens des Nutzers beziehen. In der Folge kann ohne größeren Aufwand anhand der Daten ein konkretes Persönlichkeits-, Kommunikations- und Bewegungsprofil des Betroffenen erstellt und in seiner Entwicklung nachverfolgt werden. Vor diesem Hintergrund ist Gegenstand der Untersuchung die Frage, ob derartige Formen der Datenkommunikation noch unter das Telekommunikationsgeheimnis

⁷ Vgl. *Ensthaler*, ZRP 2022, 55.

⁸ *Christen/Knieps/Inversini*, Kriminalistik 2022, 305.

⁹ Zweifelnd diesbezüglich *Ensthaler*, ZRP 2022, 55 (58).

¹⁰ Vgl. *Ruppert*, in: Dietrich et al., Hdb Sicherheits- und Staatsschutzrecht, § 23 Rn. 2.

¹¹ *Ruppert*, in: Dietrich et al., Hdb Sicherheits- und Staatsschutzrecht, § 23 Rn. 2.