

KELLER · BRAUN



Telekommunikations- überwachung und andere verdeckte Ermittlungsmaßnahmen

3. Auflage

 BOORBERG

Telekommunikationsüberwachung und andere verdeckte Ermittlungsmaßnahmen

Christoph Keller
Polizeidirektor in Münster

Prof. Dr. Frank Braun
Fachhochschule für Öffentliche Verwaltung NRW, Hagen

3., erweiterte Auflage, 2019

Bibliografische Information der Deutschen Nationalbibliothek | Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über www.dnb.de abrufbar.

3. Auflage, 2019

ISBN 978-3-415-06552-9

E-ISBN 978-3-415-06553-6

E-Book-Umsetzung: Datagroup int. SRL, Timisoara

© 2008 Richard Boorberg Verlag

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsgesetz zugelassen ist, bedarf der vorherigen Zustimmung des Verlages. Dies gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Titelfoto: © flashmovie – stock.adobe.com | Satz: Thomas Schäfer, www.schaefer-buchsatz.de | Druck und Bindung: Esser printSolutions GmbH, Westliche Gewerbestraße 6, 75015 Bretten

Richard Boorberg Verlag GmbH & Co KG | Scharrstraße 2 | 70563 Stuttgart
Stuttgart | München | Hannover | Berlin | Weimar | Dresden
www.boorberg.de

Inhaltsverzeichnis

Vorwort zur 3. Auflage	11
Verzeichnis der abgekürzten Literatur	13
I. Kapitel	
Telekommunikationsüberwachung und Online-Durchsuchung	17
1. Fernmeldegeheimnis	17
2. Eingriffsbefugnisse der Strafprozessordnung	19
2.1 Überwachung der Telekommunikation	19
2.1.1 Telekommunikationsbegriff	19
2.1.1.1 Austausch von Informationen zu Kommunikationszwecken	19
2.1.1.2 Inhalt der laufenden Kommunikation	21
2.1.1.3 Verkehrs- und Standortdaten	21
2.1.2 Anordnungsvoraussetzungen	21
2.1.2.1 Erforderlicher Tatverdacht	21
2.1.2.2 Straftatenkatalog	21
2.1.2.3 Erheblichkeit im Einzelfall	22
2.1.2.4 Tatbeteiligung	22
2.1.2.5 Subsidiaritätsklausel	22
2.1.2.6 Defizite in der Praxis	23
2.1.3 Adressaten	24
2.1.4 Verfahren	25
2.1.4.1 Anordnungscompetenz	25
2.1.4.2 Dauer und Beendigung der Maßnahme	27
2.1.4.3 Durchführung der Anordnung	28
2.1.4.4 Berichtspflichten	28
2.1.4.5 Benachrichtigungspflicht	28
2.1.4.6 Löschung personenbezogener Daten	30
2.1.4.7 Schutz des Kernbereichs privater Lebensgestaltung	30
2.1.5 Verwertung von Erkenntnissen	35
2.1.6 Überwachungsmaßnahmen mit Auslandsbezug	38
2.2 Besonderheiten bei der Überwachung des E-Mail-Verkehrs	39
2.2.1 Zugriff auf den E-Mail-Verkehr nach dem sog. „Phasenmodell“	39
2.2.2 Kritik am Phasenmodell	42
2.3 Überwachung des „Surfverhaltens“ (DSL-Überwachung)	42
2.3.1 Überwachung von DSL-Anschlüssen	42
2.3.2 Rechtliche Bewertung	43
2.3.3 Prüfprogramm bei der Anordnung	44
2.4 „Quellen-TKÜ“ und „Kleine Online-Durchsuchung“	45
2.4.1 Begriff	45
2.4.2 Grundrechtsbetroffenheit	45
2.4.3 Strafprozessuale Eingriffsbefugnisse	46

2.4.3.1	Quellen-TKÜ i. S. d. § 100a Abs. 1 Satz 2 StPO	46
2.4.3.2	Kleine Online-Durchsuchung, § 100a Abs. 1 Satz 3 StPO	47
2.4.3.3	Verfahrensvorschriften – Anforderungen an die Überwachungs- software	49
2.4.3.4	Zulässige Begleitmaßnahmen	52
2.5	Erhebung von Verkehrsdaten	53
2.5.1	Erhebung allgemeiner Verkehrsdaten, § 100g Abs. 1 StPO . . .	54
2.5.1.1	Verkehrsdaten	54
2.5.1.2	Materielle Voraussetzungen der Datenerhebung	54
2.5.2	Erhebung von „Vorratsdaten“, § 100g Abs. 2 StPO	57
2.5.2.1	Einfachgesetzliche Lage	59
2.5.2.2	Verfassungsrechtliche Situation	61
2.5.3	Funkzellenabfrage, § 100g Abs. 3 StPO	62
2.5.4	Andere Maßnahmen nach Abschluss des Kommunikations- vorgangs, § 100g Abs. 5 StPO	63
2.5.5	Adressaten	64
2.5.6	Anordnungsbefugnis und besondere Verfahrensvorschriften .	64
2.5.6.1	Anordnungskompetenz	64
2.5.6.2	Verfahrensvorschriften	65
2.5.7	Besondere Arten der Verkehrsdatenerhebung	65
2.5.7.1	Zielwahlsuche	65
2.5.7.2	Stille SMS	65
2.5.7.3	IP-Tracking	65
2.5.7.4	IP-Catching	67
2.5.7.5	Mautdaten	67
2.6	IMSI-Catcher	68
2.6.1	Funktionsweise, Einsatzmöglichkeiten und Grundrechtsbezug	68
2.6.1.1	Funktionsweise	68
2.6.1.2	Einsatzmöglichkeiten	69
2.6.1.3	Stille SMS	69
2.6.1.4	Grundrechtsbezug	70
2.6.2	Tatbestandsvoraussetzungen	71
2.6.3	Maßnahmeadressat	71
2.6.4	Umgang mit „mit-erhobenen“ Daten Dritter	72
2.6.5	Anordnungskompetenz/Besondere Verfahrensvorschriften . .	72
2.6.6	Verhältnismäßigkeit	73
2.7	Bestandsdatenauskunft	73
2.7.1	Doppeltürprinzip	74
2.7.2	Materielle Voraussetzungen	75
2.7.2.1	Allgemeine Voraussetzungen	75
2.7.2.2	Besondere Formen der Bestandsdatenauskunft	75
2.7.3	Formelle Voraussetzungen	77
2.7.3.1	Richtervorbehalt	77
2.7.3.2	Benachrichtigung	78
2.7.3.3	Inhalt und Form der Anfrage beim Provider	78
2.7.4	Mitwirkungspflicht des Diensteanbieters	79

2.7.5	Verfassungsrechtliche Bedenken	79
3.	Online-Durchsuchung, § 100b StPO	80
3.1	Grundrechtsbetroffenheit	80
3.2	Eingesetzte Software und Installation	81
3.3	Eingriffsschwellen	82
3.3.1	Anfangsverdacht einer „besonders schweren“ Straftat	82
3.3.2	Subsidiaritätsklausel	83
3.3.3	Adressaten	84
3.3.4	Anordnungskompetenz	84
3.3.5	Besondere Verfahrensvorschriften und Kernbereichsschutz	85

II. Kapitel

Ermittlungen im Internet	87
1. Online-Streife	87
2. Ermittlungen in sozialen Netzwerken	88
2.1 Datenerhebung aus allgemein zugänglichen Quellen	90
2.2 Staatlich gelenkte Kommunikationsbeziehungen	92
2.3 Kriminalistische List	93
2.4 Abgrenzung: Nicht offen ermittelnder Polizeibeamter vs. Verdeckter Ermittler	95

III. Kapitel

Observation und Einsatz technischer Mittel	99
1. Einführung	99
2. Observation	99
2.1 Abgrenzung: Gefahrenabwehrrecht	100
2.2 Längerfristige Observation	102
2.2.1 Materielle Rechtmäßigkeit	102
2.2.2 Formelle Voraussetzungen	104
2.2.3 Rechtsfolge	105
2.3 Kurzfristige Observation	106
3. Einsatz technischer Mittel	107
3.1 Akustische Wohnraumüberwachung	107
3.1.1 Historie	107
3.1.2 Materielle Voraussetzungen	108
3.1.3 Formelle Voraussetzungen	109
3.1.4 Vorbereitungsmaßnahmen	109
3.1.5 Abhören von Selbstgesprächen (Krankenzimmer)	110
3.1.6 Abhören von Gesprächen zwischen Verteidiger und Mandanten	110
3.2 Einsatz technischer Mittel	111
3.2.1 Herstellung von Bildaufnahmen	111
3.2.2 Einsatz sonstiger technischer Mittel	113

3.2.3	Abhören des nichtöffentlich gesprochenen Wortes außerhalb von Wohnungen	115
3.2.4	Begleitmaßnahmen (Annexkompetenz)	118
3.2.5	Begleitmaßnahmen gegen Unbeteiligte	119
3.2.6	Verwertbarkeit von privaten Aufzeichnungen	119
3.2.6.1	Dashcam-Aufzeichnungen	119
3.2.6.2	Videokamera-Aufzeichnungen durch Privatpersonen	120
3.2.6.3	Videokamera-Aufzeichnungen durch Arbeitgeber	120
3.2.6.4	Daten automatisierter Fahrzeuge	121
3.2.6.5	Daten aus Carsharing-Modul	122
3.3	Kumulierung strafprozessualer Ermittlungsmaßnahmen	123
3.4	Schutz des Kernbereichs privater Lebensgestaltung	124
3.4.1	Akustische Wohnraumüberwachung	125
3.4.2	Observation und Einsatz technischer Mittel	126
3.4.3	Unverwertbarkeit von Äußerungen: Selbstgespräch in Pkw	127
4.	Verlesbarkeit polizeilicher Observationsprotokolle in der Hauptverhandlung	129
5.	Netzfahndung, Polizeiliche Beobachtung und Rasterfahndung	130
5.1	Netzfahndung	130
5.2	Polizeiliche Beobachtung	131
5.3	Rasterfahndung	132
5.4	Datenabgleich („Kleine Rasterfahndung“)	134

IV. Kapitel

Verdeckte personale Ermittlungen	135
1. Einleitung	135
2. Begriffsbestimmungen	135
3. Einsatz von V-Personen	137
4. Einsatz Verdeckter Ermittler	138
5. Einsatz nicht offen ermittelnder Polizeibeamter	140
6. Tatprovokation	141
7. Cold Case	142
8. Legendierte Kontrollen als kriminaltaktische Maßnahme	144
9. Heimliches Eindringen in Wohnung zwecks Vorbereitung einer Festnahme	146

V. Kapitel

Verfahrensvorschriften	151
1. Aktenführung	152
2. Kennzeichnungspflicht	153
3. Benachrichtigungspflicht	153
4. Gerichtliche Überprüfung	154
5. Löschung von Daten	154

VI. Kapitel

Schutz der Berufsgeheimnisträger	155
1. Beweiserhebungsverbot/Beweisverwertungsverbot (absolut)	156
1.1 Geistliche	157
1.2 Verteidiger/Rechtsanwälte	157
1.3 Abgeordnete	160
2. Beweiserhebungsverbot/Beweisverwertungsverbot (relativ)	160
3. Verstrickungsregelung	161
4. Vorrang speziellerer Regelungen	163

VII. Kapitel

Datenverwendung und Datenumwidmung	165
1. Verwendung von Daten aus nicht-straßprozessualen Maßnahmen	165
1.1 Dateneingangsermächtigung: § 163 StPO	166
1.2 Dateneingangsermächtigung: § 161 Abs. 2 StPO	166
1.3 Daten aus Eigensicherungsmaßnahmen	167
1.4 Datenerhebung aus Wohnungen	167
1.5 Systematik	168
2. Verwendung strafprozessual erhobener Daten im Ausgangsverfahren	168
3. Informationsübermittlung aus Akten und Übermittlungsverbote	169
4. Verwendung strafprozessual erhobener Daten in anderen Strafverfahren	169
4.1 Akustische Wohnraumüberwachung	170
4.2 IMSI-Catcher	171
5. Verwendung strafprozessual erhobener Daten zu anderen Zwecken	171
5.1 Gefahrenabwehr	171
5.2 Informationen an Verfassungsschutzbehörden	171
5.3 Forschungszwecke	172
6. Verwendung strafprozessual erhobener Daten zur Gefahrenabwehr	172
6.1 Generalklausel zur Zweckdurchbrechung	172
6.2 Daten aus akustischer Wohnraumüberwachung	173
6.3 Daten aus Telekommunikationsüberwachung	173
6.4 Daten aus Einsatz eines IMSI-Catchers	173
6.5 Daten aus längerfristiger Observation	174
6.6 Daten aus heimlichen Bildaufnahmen	174
6.7 Weitere Regelungen eingeschränkter Zweckänderung	174

VIII. Kapitel

Sonstiges	175
1. Zufallsfunde bei Durchsuchungen	175
2. Durchsuchung elektronischer Speichermedien	176
3. Transnationaler Zugriff auf Computerdaten	177
4. Postbeschlagnahme	178
5. Ausschluss der Beschlagnahmefreiheit	180
6. Gerichtliche Untersuchungshandlung	181
Stichwortverzeichnis	182

Vorwort zur 3. Auflage

Die vorliegende Einführung wendet sich gleichermaßen an Praxis und Studium. Angesprochen sind in erster Linie Polizeibeamte des höheren und gehobenen Dienstes, die sich einen schnellen Überblick über die – alles andere als leicht zugängliche – Rechtsmaterie verschaffen wollen. Zur weiteren Vertiefung ist vor allem die Kommentierung von *Graf* (Beck'scher Online-Kommentar Strafprozessordnung, 2019) empfohlen.

Die Neuauflage enthält wesentliche Änderungen im Vergleich zur Voraufgabe, die vor allem der „StPO-Reform 2017“ geschuldet sind. Am Ende der vergangenen Legislaturperiode wurde das „Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens“ beschlossen, das am 24.08.2017 in Kraft getreten ist. Dem Gesetz liegen im Wesentlichen zwei verschiedene Gesetzesentwürfe zu Grunde. Zum einen der recht überlegte Entwurf zur Umsetzung der Empfehlungen der StPO-Expertenkommission. Und zum anderen der Entwurf zur „Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze“. Buchstäblich „in letzter Minute“ wurde das Gesetzespaket um die verfassungsrechtlich so fragwürdigen Befugnisse zur Online-Durchsuchung und zur Quellen-Telekommunikationsüberwachung ergänzt. Gegen diese Befugnisse sind bereits mehrere Verfassungsbeschwerden beim Bundesverfassungsgericht anhängig; die Argumente der Kläger wiegen schwer (vgl. etwa *Braun/Roggenkamp*, PinG 2/2019, 51, oder *Roggan*, StV 2017, 821).

Der Autor Braun hat [Kapitel I](#) bearbeitet, der Autor Keller zeichnet für die [Kapitel II–VII](#) Verantwortung.

Für die 3. Auflage sind Gesetzgebung, Rechtsprechung und Schrifttum bis zum Stand 1. März 2019 eingearbeitet worden. Für Hinweise aus dem Leserkreis sind die Autoren stets dankbar.

Münster, Hofkirchen im Frühjahr 2019

*Christoph Keller
Frank Braun*

Verzeichnis der abgekürzten Literatur

Albers/Weinzierl	Menschenrechtliche Standards in der Sicherheitspolitik, 2010 (zit. A/W-Bearbeiter)
Albrecht (Hrsg.)	Informations- und Kommunikationsrecht, 2018 (zit. Albrecht/IuKR-Bearbeiter)
Artkämper/Schilling	Vernehmungen, 5. Aufl. 2018 (zit. Artkämper/Schilling)
Bär	TK-Überwachung, §§ 100a-101 StPO mit Nebengesetzen, 2010 (zit. Bär)
Beulke/Swoboda	Strafprozessrecht, 14. Aufl. 2018 (zit. Beulke/Swoboda)
Biemann	Streifenfahrten im Internet, 2013 (zit. Biemann)
Bode	Verdeckte strafprozessuale Ermittlungsmaßnahmen, 2012 (zit. Bode)
Bormann	Transnationale Informationsgewinnung durch Nachrichtendienste und Polizei, 2016 (zit. Bormann)
Burhoff	Handbuch für das strafrechtliche Ermittlungsverfahren, 7. Aufl. 2015 (zit. Burhoff)
Büchel/Hirsch	Internetkriminalität, 2014 (zit. Büchel/Hirsch)
Clages/Ackermann	Der rote Faden, 13. Aufl. 2017 (zit. C/A-Bearbeiter)
Dölling/Duttge/König/ Rössner (Hrsg.)	Gesamtes Strafrecht, 4. Aufl. 2017 (zit. HK/GS-Bearbeiter)
Eisenberg	Beweisrecht der StPO, 10. Aufl. 2017 (zit. Eisenberg)
Fehr	Social Media, Apps und Co., 2014 (zit. Fehr)
Gabor	Strafprozessordnung, 9. Aufl. 2018 (zit. Gabor)
Gercke/Julius/Temming/ Zöller (Hrsg.)	StPO-Kommentar, 6. Aufl. 2018 (zit. HK/StPO-Bearbeiter)
Glitzta	Observation-Praxisleitfaden für private und behördliche Ermittlungen, 4. Aufl. 2014 (zit. Glitzta)

- Götz/Geis Allgemeines Polizei- und Ordnungsrecht, 16. Aufl. 2017
(zit. Götz/Geis)
- Gola Datenschutz-Grundverordnung, 2. Aufl. 2018
(zit. Gola/DSGVO-Bearbeiter)
- Graf Beck'scher Online-Kommentar Strafprozessordnung, 2018
(zit. Beck OK/StPO-Bearbeiter)
- Hannich (Hrsg.) Karlsruher Kommentar zur Strafprozessordnung, 8. Aufl. 2019
(zit. KK/StPO – Bearbeiter)
- Hartmann-Wergen Grundlagen zum Strafprozessrecht, 9. Aufl. 2018
(zit. Hartmann-Wergen)
- Haug Grundwissen Internetrecht, 3. Aufl. 2016
(zit. Haug)
- Heckmann Internetrecht – juris Praxis-Kommentar, 5. Aufl. 2017
(zit. jurisPK/Internetrecht-Bearbeiter)
- Hornung/Müller-
 Terpitz (Hrsg.) Rechtshandbuch Social Media, 2015
(zit. H/M-T-Bearbeiter)
- Joecks Studienkommentar StPO, 4. Aufl. 2015
(zit. Joecks)
- Johannes/Weinhold Das neue Datenschutzrecht bei Polizei und Justiz, 2018
(zit. Johannes/Weinhold)
- Keller Eingriffsrecht Nordrhein-Westfalen, 3. Aufl. 2010
(zit. Keller, EingriffsR)
- Keller Verdeckte personale Ermittlungen, 2017
(zit. Keller)
- Kindhäuser Strafprozessrecht, 4. Aufl. 2016
(zit. Kindhäuser)
- Kirkpatrick Der Einsatz von Verdeckten Ermittlern – Handbuch für die Praxis der Strafverfolgungsbehörden, 2011
(zit. Kirkpatrick)
- Kleile Handbuch Internetrecherche, 2016
(zit. Kleile)
- König/Trurnit Eingriffsrecht, 3. Aufl. 2014
(zit. König/Trurnit)
- Kramer Grundbegriffe des Strafverfahrensrechts, 8. Aufl. 2014
(zit. Kramer)
- Leitner/Michalke Strafprozessuale Zwangsmaßnahmen, 2007
(zit. Leitner/Michalke)
- Lindner Der Begleitfund, Zu den Grenzen strafverfahrensrechtlicher Informationsverwertung beiläufig erlangter Informationen im Rahmen präventiv-polizeilicher Tätigkeit, 1998
(zit. Lindner)

Lisken/Denninger	Handbuch des Polizeirechts, 6. Aufl. 2018 (zit. L/D-Bearbeiter)
Meyer-Goßner/Schmitt	StPO-Kommentar, 61. Aufl. 2018 (zit. Meyer-Goßner/Schmitt)
Möllers	Wörterbuch der Polizei, 3. Aufl. 2018 (zit. Möllers-Stichwort)
Nimtz/Thiel	Eingriffsrecht, 2017 (zit. Nimtz/Thiel)
Kingreen/Poscher	Grundrechte – Staatsrecht II, 34. Aufl. 2018 (zit. Kingreen/Poscher, StaatsR)
Kingreen/Poscher	Polizei- und Ordnungsrecht, 10. Aufl. 2018 (zit. Kingreen/Poscher, POR)
Ostendorf	Strafprozessrecht, 3. Aufl. 2018 (zit. Ostendorf)
Paal/Pauly	DS-GVO/BDSG, 2. Aufl. 2018 (zit. P/P-Bearbeiter)
Rössner/Safferling	30 Probleme aus dem Strafprozessrecht, 3. Aufl. 2017 (zit. Rössner/Safferling)
Rottmeier	Kernbereich privater Lebensgestaltung und straf- prozessuale Lauschangriffe, 2017 (zit. Rottmeier)
Roxin/Schünemann	Strafverfahrensrecht, 29. Aufl. 2017 (zit. Roxin/Schünemann)
Satzger/Schluckebier/ Widmaier	StPO-Kommentar, 3. Aufl. 2018 (zit. SSW/StPO-Bearbeiter)
Schenke	Polizei- und Ordnungsrecht, 10. Aufl. 2018 (zit. Schenke)
Schön	Ermittlungsmaßnahmen über das Internet, 2. Aufl. 2019 (zit. Schön)
Schütte/Braun/Keller	Polizeigesetz Nordrhein-Westfalen, 2012 (zit. SBK/PolG-Bearbeiter)
Schütte/Braun/Keller	Eingriffsrecht, 2016 (zit. SBK/ER)
Soiné	Ermittlungsverfahren und Polizeipraxis, 2. Aufl. 2019 (zit. Soiné)
Tegtmeyer/Vahle	Polizeigesetz Nordrhein-Westfalen, 12. Aufl. 2018 (zit. Tegtmeyer/Vahle)
Teubert	Datenschutz und Polizei in Bayern, 2011 (zit. Teuber)
Tyszkiewicz	Tatprovokation als Ermittlungsmaßnahme, 2014 (zit. Tyszkiewicz)
Von der Grün	Verdeckte Ermittlungen, 2018 (zit. Von der Grün)
Wabnitz/Janovsky	Handbuch Wirtschafts- und Steuerstrafrecht, 4. Aufl. 2014 (zit. W/J-Bearbeiter)

- Wang Einsatz Verdeckter Ermittler zum Entlocken des
 Geständnisses eines Beschuldigten – Ein Prüfstein für
 das Täuschungsverbot des § 136a StPO und den nemo-
 tenetur-Grundsatz aus Art. 6 EMRK, 2015
 (zit. Wang)
- Wernert Internetkriminalität, 3. Aufl. 2017
 (zit. Wernert)
- Wicker Cloud Computing und staatlicher Strafanspruch.
 Strafrechtliche Risiken und strafprozessuale Ermitt-
 lungsmöglichkeiten in der Cloud, 2016
 (zit. Wicker)
- Wolter SK-StPO Systematischer Kommentar zur Strafprozess-
 ordnung, 5. Aufl. 2018
 (zit. SK/StPO-Bearbeiter)
- Würtenberger/
 Heckmann/
 Tanneberger Polizeirecht in Baden-Württemberg, 7. Aufl. 2017
 (zit. Würtenberger/Heckmann/Tanneberger)

I. Kapitel

Telekommunikationsüberwachung und Online-Durchsuchung

1. Fernmeldegeheimnis

Straftäter passen ihre Methoden den aktuellen technischen Entwicklungen an. Der Informationsaustausch zwischen ihnen erfolgt weitestgehend mit Hilfe moderner Kommunikationsmittel, wie Mobiltelefon, SMS-, Chat- und Messenger-Diensten, E-Mail oder Voice-Over-IP-Telefonie. Insoweit sind die Ermittlungsbehörden zur Aufklärung von Straftaten mehr denn je auf Inhalte und Umstände von Telekommunikationsvorgängen Verdächtiger angewiesen. Der Gesetzgeber stellt hierfür mittlerweile umfassende heimliche Ermittlungsbefugnisse zur Verfügung. Freilich sind diese angesichts ihrer Eingriffsintensität sowie ihrer Reichweite und Streubreite (regelmäßig werden auch personenbezogene Daten unverdächtiger Dritter miterhoben) einschränkend auszulegen und anzuwenden. Schließlich wird durch die betreffenden Maßnahmen regelmäßig in veritable Grundrechtspositionen der Betroffenen eingegriffen, namentlich in das Fernmeldegeheimnis (Art. 10 Abs. 1 GG), auf dessen Menschenwürdegehalt das *BVerfG* explizit hinweist¹: Durch Art. 10 Abs. 1 GG wird die freie Entfaltung der Persönlichkeit durch einen privaten, vor der Öffentlichkeit verborgenen Austausch von Kommunikation gewährleistet und damit zugleich die Würde des Menschen geschützt.²

Das Fernmeldegeheimnis sichert die individuelle Fernkommunikation und gewährleistet deren Vertraulichkeit, wenn die Beteiligten wegen der räumlichen Distanz zueinander auf eine Übermittlung durch Andere angewiesen sind und deshalb in besonderer Weise einem Zugriff Dritter ausgesetzt sein können; es schützt in erster Linie die Vertraulichkeit der ausgetauschten Information und damit den Kommunikationsinhalt vor unbefugten Zugriff.³ Dabei knüpft das Fernmeldegeheimnis an das Kommunikationsmedium an und tritt jenen Gefahren für die Vertraulichkeit, die sich gerade aus der Verwendung dieses Mediums ergeben, entgegen.

Der *Schutz des Fernmeldegeheimnisses endet* dementsprechend in dem Moment, in dem die Nachricht beim Empfänger angekommen und der Übertragungsvorgang abgeschlossen ist.⁴ Die *spezifischen Gefahren der Fern-*

1 BVerfG NJW 2005, 2603: Vorbeugende/vorsorgende TKÜ gegen Straftaten.

2 BVerfG NJW 2004, 2213: Brief- und Telefonüberwachung durch das Zollkriminalamt.

3 BVerfG MMR 2009, 673 (674); BVerfG v. 02.03.2006 – 2 BvR 2099/04; BVerfG NJW 2003, 1787 (1788); BVerfG NJW 2000, 55 (56 f.).

4 BVerfG MMR 2008, 315 (316); BVerfG v. 02.03.2006 – 2 BvR 2099/04.

kommunikation bestehen im Herrschaftsbereich des Empfängers, der selbst geeignete Schutzvorkehrungen gegen einen ungewollten Datenzugriff treffen kann, gerade nicht mehr.⁵ Der Grundrechtsschutz erstreckt sich grundsätzlich nicht auf die außerhalb eines laufenden Kommunikationsvorganges im Herrschaftsbereich des Kommunikationsteilnehmers gespeicherten Inhalte und Umstände der Kommunikation.⁶ Diese Dateien unterscheiden sich dann nicht mehr von solchen, die der Nutzer selbst angelegt hat. Schutz vor Zugriff auf diese Daten gewährleisten das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) und gegebenenfalls das Wohnungsgrundrecht (Art. 13 Abs. 1 GG).⁷ Z. B., wenn das Mobiltelefon eines dringend einer schweren Straftat Verdächtigen beschlagnahmt und die darauf gespeicherten SMS ausgelesen werden – Nach dem Vorgesagten kein Eingriff in Art. 10 Abs. 1 GG.

Der Schutz des Fernmeldegeheimnisses endet aber nicht stets nach Abschluss des Übertragungsvorganges. Nach der Rechtsprechung des *BVerfG* greift der grundrechtliche Schutz aus Art. 10 Abs. 1 GG, wenn die spezifischen Gefahren der Fernkommunikation (das ist die Kenntnisnahme der Kommunikation/Kommunikationsumstände durch Dritte, ohne dass der Kommunikationsteilnehmer dies verhindern kann) nach Abschluss des Kommunikationsvorganges fortbestehen⁸, etwa wenn E-Mails beim Provider auf dessen Mail-Server beschlagnahmt werden. Solange sich die gespeicherten E-Mails auf dem Mailserver des Providers befinden, fehlt es dem Nutzer an technischen Möglichkeiten, einen Zugriff, die Vervielfältigung oder Weitergabe durch den Provider zu verhindern. Gerade dieser *technisch bedingte Mangel an Beherrschbarkeit* begründet die Schutzbedürftigkeit durch das Fernmeldegeheimnis.⁹

Das Fernmeldegeheimnis schützt neben dem Inhalt der Kommunikation auch die näheren *Umstände* der übertragenen Mitteilungen. Zu diesen sog. *Verkehrsdaten* gehört vor allem die Tatsache, ob und wann sowie welche Personen über welche Anschlüsse Fernmeldeverkehr durchgeführt haben.¹⁰ „Verkehrsdaten“ werden in § 3 Nr. 30 TKG einfachgesetzlich legaldefiniert als Daten, die bei der Erbringung eines Telekommunikationsdienstes erho-

5 BVerfG MMR 2008, 315 (316); BVerfG v. 02.03.2006 – 2 BvR 2099/04.

6 BVerfG MMR 2009, 673 (674).

7 BVerfG NJW 2006, 976: Wohnungsdurchsuchung zur Ermittlung von Kommunikationsdaten.

8 BVerfG MMR 2009, 673.

9 BVerfG MMR 2009, 673. Dabei macht es keinen Unterschied, ob eine E-Mail auf dem Mailserver des Providers zwischen- oder endgespeichert ist, da der Nutzer in beiden Fällen aufgrund faktisch nicht zu unterscheidender Herrschaftsverhältnisse gleichermaßen schutzbedürftig ist.

10 BVerfG NJW 2007, 3055.

ben, verarbeitet oder genutzt werden und sind in § 96 Abs. 1 TKG beispielhaft präzisiert.¹¹

2. Eingriffsbefugnisse der Strafprozessordnung

2.1 Überwachung der Telekommunikation

Die strafprozessuale TKÜ ist Massenermittlungsmethode. Täglich ergehen im Schnitt mehr als 50 Erst- und Verlängerungsanordnungen.¹² § 100a Abs. 4 Satz 1 StPO bestimmt, dass aufgrund einer richterlichen Anordnung jeder, der Telekommunikationsdienste erbringt oder daran mitwirkt, dem Gericht, der STA und ihren im Polizeidienst tätigen Ermittlungspersonen Maßnahmen nach § 100a StPO zu ermöglichen und die erforderlichen Auskünfte unverzüglich zu erteilen hat. Diese Mitwirkungspflicht der Diensteanbieter wird in der Telekommunikationsüberwachungsverordnung (TKÜV) konkretisiert. Die TKÜV regelt die grundlegenden Anforderungen an die Gestaltung der technischen Einrichtungen, die für die Umsetzung der in §§ 100a, 100e StPO vorgesehenen Maßnahmen zur Überwachung der Telekommunikation erforderlich sind, sowie organisatorische Eckpunkte für die Umsetzung derartiger Maßnahmen mittels dieser Einrichtungen (§ 1 Nr. 1 TKÜV). Die technischen Einzelheiten der Datenweitergabe an die Ermittlungsbehörden ergeben sich aus der „Technischen Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation“ (TR TKÜV).

2.1.1 Telekommunikationsbegriff

2.1.1.1 Austausch von Informationen zu Kommunikationszwecken

§ 100a StPO gestattet die Überwachung der „Telekommunikation“. Es ist **nicht** der technische Telekommunikationsbegriff des § 3 Nr. 22 TKG heranzuziehen.¹³ §§ 100a, 100b StPO knüpfen vielmehr, wie auch Art. 10 Abs. 1

¹¹ Die Einbeziehung „personenbezogener Berechtigungskennungen“ (z. B. PIN = Personal Identity Number) gem. § 96 Abs. 1 Nr. 1 TKG wird mithin als „Fremdkörper“ im Katalog bloßer Verkehrsdaten betrachtet. Den Strafverfolgungsbehörden wird so mittelbar auch der Zugriff auf Inhalte der Telekommunikation oder weitergehende personenbezogene Daten ermöglicht, vgl. Zöller, GA 2007, 393 (401).

¹² Auf das Jahr 2016 summierten sich über 20.000 Überwachungsmaßnahmen, <https://www.bundesjustizamt.de/DE/Presse/Archiv/2017/20170911.html>

¹³ Anders ohne Begründung in einem obiter dictum BGH NStZ-RR 2011, 148; LG Ellwangen v. 28.05.2013 – 1 Qs 130/12, hierzu Braun, jurisPR-ITR 18/2013 Anm. 5; Albrecht/Braun, HRRS 12/2013, 500 ff. Nach § 3 Nr. 22 TKG ist Telekommunikation der technische Vorgang des Aussendens, Übermittels und Empfangens von Signalen mittels Telekommunikationsanlagen und mithin jeder Austausch von Datenpaketen, wie er bei sämtlichen Formen der Internetnutzung stattfindet. Danach läge auch dann „Telekommunikation“ vor, wenn diese aufgrund einer entsprechenden Programmierung autonom zwischen Rechnern oder mobilen Endgeräten stattfindet.

GG, an ein **materielles** Kommunikationsverständnis an¹⁴; die Auslegung des strafprozessualen Telekommunikationsbegriffs hat sich nach dem verfassungsrechtlich gebotenen Schutzniveau zu richten.¹⁵ Vom Schutzbereich des Telekommunikationsgeheimnisses werden danach – als verfassungsrechtlich unzweifelhaft geschützte „individuelle Fernkommunikation“ – neben den herkömmlichen Telefongesprächen auch die Nutzung von Internet-Kommunikationsdiensten wie **E-Mail, Messenger-Systeme und sonstige Chat-Formate** sowie sämtliche Arten der **Internet-Telefonie** erfasst. Ob dagegen auch der Abruf von Webseiten und die Nutzung von Cloud-Datenbanken (Up- und Download) als *nicht-kommunikative Nutzungen* des Internets dem Telekommunikationsbegriff unterfallen, ist umstritten.¹⁶ In einem Nichtannahmebeschluss hat dies die Dritte Kammer des zweiten Senats des BVerfG bejaht¹⁷: Das Telekommunikationsgeheimnis schützt davor, dass staatliche Stellen sich in die Kommunikation einschalten und Kenntnisse über die Kommunikationsbeziehungen oder Kommunikationsinhalte gewinnen.¹⁸ Da auch bei der Nutzung des Internets generell eine solches Gefährdungspotenzial besteht, erstreckt sich der Schutzbereich des Art. 10 Abs. 1 GG auch auf das „Surfen“ bzw. Abrufen von Web-Seiten. Den Einwand der Literatur, dass für eine schützenswerte Telekommunikation Voraussetzung ist, dass *Individuen miteinander kommunizieren*, da die Überwachungsvorschriften originär für die Überwachung der Kommunikation zwischen Menschen konzipiert seien¹⁹, lässt das Gericht nicht gelten. Der Schutz der Vertraulichkeit knüpft nicht an die Beteiligten der Kommunikation, sondern an den Übermittlungsvorgang und das dabei genutzte Medium an. Ein empfängergesteuerter Abruf von Informationen aus dem Netz ist eine Übermittlung von Informationen an einen individuellen Rezipienten, was in Abgrenzung zu einem nicht geschützten, rein maschinellen Datenaustausch (etwa beim Einsatz eines sog. IMSI-Catchers)²⁰ ausreicht, um einen schützenswerten Kommunikationsvorgang anzunehmen. Folgt man dem, stellt auch die Überwachung des Surfverhalten (dazu unten 2.3), einen Eingriff in das Telekommunikationsgeheimnis dar.

14 BVerfG v. 22.08.2006 – 2 BvR 1345/03; vgl. *Hiéramente*, StraFO 2013, 96 ff. m. w. N.; *Albrecht/Braun*, HRRS 2013, 500 ff.

15 *Braun*, jurisPR-ITR 18/2013 Anm. 5; *Hiéramente*, StraFo 2013, 96, 98; *Albrecht/Dienst*, JurPC Web-Dok. 5/2012 Abs. 22; *Löffelmann*, AnwBl 2006, 598, 600. Auch der BGH stellt fest, dass nicht jeder technische Vorgang des Aussendens, Übermittels oder Empfangens von analog oder digital codierten Daten dem Eingriffsbereich des § 100a StPO unterfällt, NJW 2003, 2034.

16 *Braun*, jurisPR-ITR 18/2013 Anm. 5.

17 BVerfG, Beschl. v. 06.07.2016 – 2 BvR 1454/1.

18 BVerfG, Beschl. v. 06.07.2016 – 2 BvR 1454/1.

19 Vgl. *Böckenförde*, JZ 2008, 925, 937; *Meinicke*, in: Taeger, Law as a Service – Recht im Internet- und Cloud-Zeitalter, 2013, 969, 971.

20 Hierzu BVerfG, Beschl. v. 22.10.2006 – 2 BvR 1345/03 – IMSI-Catcher.