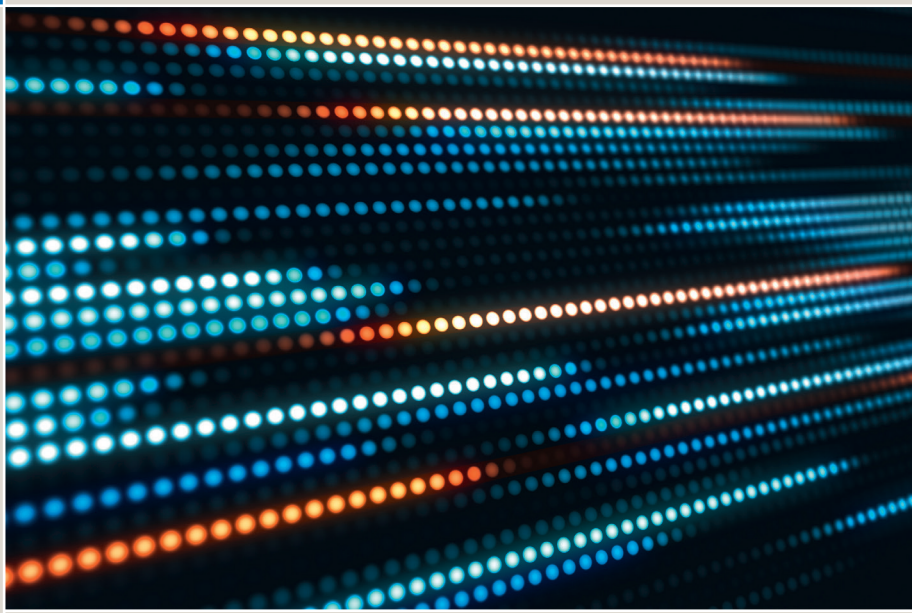
KELLER · BRAUN



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

BOORBERG

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

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

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 Vorauflage, 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)
Glitza	Observation-Praxisleitfaden für private und behördliche Ermittlungen, 4. Aufl. 2014 (zit. Glitza)

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 strafprozessuale 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 Ermittlungsmöglichkeiten in der Cloud, 2016 (zit. Wicker)
Wolter	SK-StPO Systematischer Kommentar zur Strafprozessordnung, 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 hinweist[1]: 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 fortbestehen[8], 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 Dienstanbieter 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, Übermittelns 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 an[14]; 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* bejaht[17]: 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 seien[19], 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, Übermittelns 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.