Meinhard Starostik

Rechtsanwalt

Rechtsanwaltskanzlei:
Schillstr. 9 • 10785 Berlin
Tel.: 030 - 88 000 345
Fax: 030 - 88 000 346
email: Kanzlei@Starostik.de
USt-ID-Nr. DE165877648

RA Starostik, Schillstraße 9, 10785 Berlin

An das
Bundesverfassungsgericht
Schloßbezirk 3
76131 Karlsruhe

Kanzlei vereidigter Buchprüfer:
Schwarzenberger Str. 7 • 08280 Aue
Tel.: 03771-290 999

Berlin, den 05.Mai 2009

AZ: 42/05
(bitte stets angeben)

Verfassungsbeschwerde

- 1 BvR 1299/05 -

Der im Verfahren des einstweiligen Rechtsschutzes erlassene Beschluss des OVG Münster vom 17.02.2009 (Az. 13 B 33/09) gibt Anlass zur vertieften Erläuterung, weshalb die §§ 111-113 TKG Art. 10 GG beschränken.

Inhaltsübersicht

1 Bedeutung des § 113 TKG

Zunächst ist dem Beschluss des OVG Münster vom 17.02.2009 ausdrücklich darin zuzustimmen, dass § 113 TKG die **Identifizierung** des Teilnehmers an einer Internetverbindung erlaubt, selbst wenn diese Identifizierung nur durch Verarbeitung von Verbindungsdaten erfolgen kann (dynamische IP-Adresse und Zeitpunkt der Verbindung). Dies stützt die Auffassung der Beschwerdeführer, wonach § 113 TKG so weit formuliert ist, dass er Auskünfte über nähere Umstände einzelner Telekommunikationsverbindungen ebenso abdeckt wie eine „Rasterfahndung" durch den gesamten Bestand an Verbindungsdaten eines Telekommunikationsmittlers.

§ 113 TKG ermächtigt etwa zu den folgenden Anfragen, die weder einer gerichtlichen Kontrolle noch dem Erfordernis des Verdachts einer schweren Straftat unterliegen:

- Wer hat am 01.01.2009 um 12:01 an der **Internetverbindung** mit der IP-Adresse 101.101.101.101 teilgenommen (bitte nur Bestandsdaten mitteilen)?
- Wer hat am 01.01.2009 um 12:01 eine **Verbindung** zu dem Anschluss 072191010 hergestellt (bitte nur Bestandsdaten mitteilen)?
- Welche Personen haben im Januar 2009 **Verbindungen** zu dem Anschluss 072191010 hergestellt (bitte nur Bestandsdaten mitteilen)?
- Mit welchen Personen sind im Januar 2009 über den Anschluss 072191010 **Verbindungen** hergestellt worden (bitte nur Bestandsdaten mitteilen)?
- Welche Personen haben am 01.01.2009 zwischen 9.00 Uhr und 14.00 Uhr in den **Funkzellen** mobil telefoniert, welche den Schloßbezirk 3 in Karlsruhe abdecken (bitte nur Bestandsdaten mitteilen)?
- Wie lautet der Zugriffscode zum elektronischen **Anrufbeantworter** des Anschlusses 072191010?
- Wie lautet das Passwort zum **Postfach** des E-Mail-Kontos bverfg@bundesverfassungsgericht.de?
- Welche Adressen sind im elektronischen **Adressbuch** des E-Mail-Kontos bverfg@bundesverfassungsgericht.de verzeichnet?
- Welche **Rufnummern** hat der Inhaber des Anschlusses 072191010 angegeben, um im günstigen „Family and Friends"-Tarif zu telefonieren?

Weil § 113 TKG – ebenso wie § 100g StPO – formal auf die Art der übermittelten Daten abstellt und jede Mitteilung von Bestandsdaten abdeckt, ermöglicht er die unmittelbare und mittelbare Gewinnung **weitreichender Informationen** über Telekommunikationsteilnehmer und ihr Telekommunikationsverhalten.

2 Meinungsstand zum Schutz von Kommunikationsdaten durch das Fernmeldegeheimnis

Die weitere Frage, wie weit der Begriff „Fernmeldegeheimnis" in Artikel 10 GG reicht, ist **umstritten**. Dazu werden im Wesentlichen sechs Auffassungen vertreten:

Erstens könnte man vertreten, der staatliche Zugriff auf Bestandsdaten des Inhabers eines Telekommunikationsanschlusses greife **nie in das Fernmeldegeheimnis** ein.[1] Zur Begründung wird angeführt: In der Mitteilung von Bestandsdaten – auch zu einer bestimmten Telekommunikationsverbindung – verwirkliche sich keine spezifische Gefährdung der von Art. 10 GG gewährleisteten Vertraulichkeit der ausgetauschten Informationen und der

[1] öOGH, Beschluss vom 26.07.2005, Az. 11 Os 57/05z u.a., 7.

Umstände des Kommunikationsvorgangs.[2] Bestandsdaten fehle der Bezug zu einem konkreten Telekommunikationsvorgang.[3] Sie hätten die Kenntnis von einzelnen Telekommunikationsvorgängen nicht zum Gegenstand.[4] Wenn das Fernmeldegeheimnis Informationen über eine bloß empfangsbereites Endgerät nicht schütze,[5] obgleich die Empfangsbereitschaft notwendige Voraussetzung eines Telekommunikationsvorgangs sei, so müsse gleiches für Daten über das Vertragsverhältnis zum Anbieter gelten, welches ebenfalls Voraussetzung eines Telekommunikationsvorgangs sei.[6] Die Erhebung von Bestandsdaten sei am wenigsten eingriffsintensiv.[7] Bestandsdaten unterschieden sich nicht von Vertragsdaten eines beliebigen anderen Unternehmens.[8] Ihr Aussagegehalt weise keinen spezifischen Zusammenhang mit Telekommunikation auf; entsprechende Informationen könnten etwa auch über Zeugenaussagen erlangt werden.[9] Im Vergleich zum eigentlichen Kommunikationsvorgang verdiene das vorgelagerte Vertragsverhältnis nicht den gleichen Schutz.

Auch die **Identifizierung eines Anschlussinhabers** anhand bereits bekannter Verbindungsdaten greife nicht in das Fernmeldegeheimnis ein. Die Identifizierung eines Anschlussinhabers betreffe nicht unmittelbar Inhalt oder Umstände eines konkreten Telekommunikationsvorgangs.[10] Im Fall der Identifizierung des Teilnehmers an einem bestimmten Gespräch sei der konkrete Telekommunikationsvorgang bereits bekannt.[11] Die bekannten Daten individualisierten den Anschlussinhaber bereits eindeutig und unverwechselbar.[12] Der Gesprächsteilnehmer habe seine Verbindungsdaten gegenüber dem Gesprächspartner freiwillig preisgegeben.[13] Der Kommunikationsvorgang sei daher von vornherein nicht auf Vertraulichkeit angelegt gewesen. Bei dem Gesprächspartner unterlägen die Verbindungsdaten nicht dem Fernmeldegeheimnis, so dass ihre Zuordnung zu ebenfalls nicht dem Fernmeldegeheimnis unterliegenden Bestandsdaten keinen Eingriff in Artikel 10 GG begründen könne. Für die Identifizierung eines Anschlussinhabers anhand von Verbindungsdaten (z.B. dynamischer IP-Adresse) könne nichts anderes gelten als für seine Identifizierung anhand von Bestandsdaten (z.B. statischer IP-Adresse, Rufnummer).[14] Müsse der Mittler zur Auskunfterteilung Verkehrsdaten verarbeiten, so handele es sich um einen internen Vorgang, bei dem der um Auskunft nachsuchenden Stelle keine Kenntnis von den Verkehrsdaten vermittelt werde. An den verarbeiteten Verkehrsdaten habe der Staat auch kein Interesse.

Zweitens könnte man vertreten, die Erhebung von Bestandsdaten greife dann in das Fernmeldegeheimnis ein, wenn sie der **Vorbereitung und Ermöglichung eines Zugriffs** auf Verkehrsdaten oder Telekommunikationsinhalte diene,[15] insbesondere wenn dieser Zugriff

---

[2] OVG Münster, Beschluss vom 17.02.2009, Az. 13 B 33/09, Abs. 23.
[3] OVG Münster, Beschluss vom 17.02.2009, Az. 13 B 33/09, Abs. 23.
[4] OVG Münster, Beschluss vom 17.02.2009, Az. 13 B 33/09, Abs. 26.
[5] So der Kammerbeschluss des BVerfG vom 22.8.2006, 2 BvR 1345/03.
[6] Bevollmächtigter der Bundesregierung, Schriftsatz vom 22.01.2007, 28.
[7] öOGH, Beschluss vom 26.07.2005, Az. 11 Os 57/05z u.a., 10.
[8] Bevollmächtigter der Bundesregierung, Schriftsatz vom 22.01.2007, 30.
[9] Bevollmächtigter der Bundesregierung, Schriftsatz vom 22.01.2007, 31.
[10] OVG Münster, Beschluss vom 17.02.2009, Az. 13 B 33/09, Abs. 23.
[11] OVG Münster, Beschluss vom 17.02.2009, Az. 13 B 33/09, Abs. 25.
[12] Vgl. LG Stuttgart, Beschluss vom 04.01.2005, Az. 13 Qs 89/04, Abs. 7.
[13] Vgl. LG Darmstadt, Beschluss vom 09.10.2008, Az. 9 Qs 490/08.
[14] Vgl. LG Stuttgart, Beschluss vom 04.01.2005, Az. 13 Qs 89/04, Abs. 15 f.
[15] AK-GG-Bizer, Art. 10, Rn. 71.

ohne weitere Mitwirkung eines Dritten unmittelbar erfolgen soll (z.B. Erhebung eines Passworts, um auf ein E-Mail-Postfach zugreifen zu können).[16]

Drittens könnte man vertreten, die Identifizierung eines Gesprächsteilnehmers greife dann in das Fernmeldegeheimnis ein, wenn der Kommunikationsmittler bei ihm gespeicherte **Verbindungsdaten verarbeiten** muss, um die begehrte Auskunft erteilen zu können. Zur Begründung könnte man anführen, das Fernmeldegeheimnis schütze auch vor einer internen Auswertung von Verbindungsdaten durch den Mittler, soweit diese nicht zur Erbringung des Telekommunikationsdienstes erforderlich sei (vgl. § 88 Abs. 3 S. 2 TKG).[17]

Viertens könnte man vertreten, die Identifizierung eines Gesprächsteilnehmers greife in das Fernmeldegeheimnis ein, wenn sie anhand von Informationen erfolge, die **durch einen Eingriff in das Fernmeldegeheimnis erlangt** wurden.[18] Zur Begründung wird angeführt, das Fernmeldegeheimnis erfasse auch die Phasen der Verarbeitung, Speicherung und Übermittlung von Kommunikationsdaten.[19] Die Verknüpfung der Verbindungsdaten mit Bestandsdaten stelle eine solche Datenverarbeitung und damit Eingriffsvertiefung dar. Zum Teil wird auch argumentiert, bei der Erhebung von Verbindungsdaten und sodann den zugehörigen Bestandsdaten handele es sich um einen einheitlichen Grundrechtseingriff.

Fünftens könnte man die Auffassung vertreten, der staatliche Zugriff auf Bestandsdaten greife immer dann in das Fernmeldegeheimnis ein, wenn er **Aufschluss über die näheren Umstände eines konkreten Telekommunikationsvorgangs** geben solle, insbesondere über die Person der an dem Telekommunikationsvorgang Beteiligten.[20] Zur Begründung ließe sich anführen: Durch eine Namensauskunft würden die bereits bekannten Umstände einer Verbindung mit einer Person und diese somit mit einem konkreten Nutzungsvorgang und -zeitpunkt verknüpft.[21] Die Identifizierung des an einem Telekommunikationsvorgang Beteiligten berühre und offenbare daher die näheren Umstände des Telekommunikationsvorgangs.[22] Erst durch die Verknüpfung mit der Identität des Teilnehmers erlangten die übrigen Informationen über einen Kommunikationsvorgang ihre Bedeutung.[23] Das Fernmeldegeheimnis schütze die Kommunikation zwischen Menschen[24] und nicht zwischen Nummern. Die letztlich begehrte Information, dass und welche Verbindung zu welchem Zeitpunkt von welchem Teilnehmer hergestellt wurde, unterliege dem Fernmeldegeheimnis.[25] Es handele sich hierbei nicht um eine Information, die einem Eintrag in das Telefonbuch vergleichbar wäre, sondern um die Ermittlung, wer mit wem zu welchem Zeitpunkt worüber und wie lange kommuniziert habe.[26] Es sei weder interessen- noch sachgerecht und letztlich nicht nachvollziehbar, weshalb sich der Grundrechtsschutz des betroffenen Telekommunikationsteilnehmers an der einfachgesetzlichen Einstufung

---

16 LG Hamburg, MMR 2002, 403 (404 f.).

17 OLG Wien, Beschluss vom 28.02.2005, Az. 20 Bs 27/05z.

18 Bäcker in: Brink/Rensen, Linien der Rechtsprechung des Bundesverfassungsgerichts (2009); weitere Nachweise bei Bevollmächtigtem der Bundesregierung, Schriftsatz vom 22.01.2007, 32 f.

19 Bäcker in: Brink/Rensen, Linien der Rechtsprechung des Bundesverfassungsgerichts (2009).

20 OLG Wien, Beschluss vom 28.02.2005, Az. 20 Bs 27/05z – Internet; OLG Oldenburg, MMR 2009, 188 (189); Wiebe, MMR 2005, 827 (829 f.); Bär, MMR 2005, 626 (627); Sieber/Höfinger, MMR 2004, 575 (581 f.); Braun, jurisPR-ITR 4/2006 Anm. 6 zu LG Hamburg, MMR 2005, 711; Warg, MMR 2006, 77 (82); Gola/Klug/Reif, Datenschutz- und presserechtliche Bewertung der „Vorratsdatenspeicherung" (2007), 57; Dix, Schriftsatz vom 29.01.2007 in diesem Verfahren, 5 f.; in diese Richtung auch VG Köln, Beschluss vom 11.12.2008, Az. 21 L 1398/08, BeckRS 2009, 32522.

21 Vgl. OLG Zweibrücken, Beschluss vom 27.10.2008, Az. 3 W 184/08 m.w.N.

22 Vgl. OLG Zweibrücken, Beschluss vom 27.10.2008, Az. 3 W 184/08 m.w.N.; Wiebe, MMR 2005, 827 (829 f.).

23 Wiebe, MMR 2005, 827 (829).

24 Wiebe, MMR 2005, 827 (829).

25 Vgl. LG München, Beschluss vom 12.03.2008, Az. 5 Qs 19/08.

26 OLG Frankfurt, Urteil vom 01.07.2008, Az. 11 U 52/07; LG München, Beschluss vom 12.03.2008, Az. 5 Qs 19/08.

bestimmter Daten als Verkehrs- oder Bestandsdaten orientieren solle.[27] Die bereits bekannten Verbindungsdaten individualisierten die beteiligten Anschlussinhaber noch nicht; vielmehr erlaube erst die Verknüpfung mit den Daten des jeweiligen Telekommunikationsmittlers die Zuordnung zu einem bestimmten Anschlussinhaber.[28] Die zuvor bekannten Verbindungsdaten bildeten nur die notwendige Voraussetzung dafür, dass der Kommunikationsmittler die Individualisierung vornehmen könne;[29] erst die begehrte Auskunft führe also zur Individualisierung. Ohne diese Auskunft seien die zuvor bekannten Verbindungsdaten ein technisches und rechtliches Nullum, dem keine Aussagekraft zukomme.[30] Die Gegenansicht ermögliche es, den vom Fernmeldegeheimnis bezweckten Schutz zu umgehen.[31]

Sechstens könnte man schließlich vertreten, der staatliche Zugriff auf Daten, die ein Telekommunikationsanbieter zur Ermöglichung von Telekommunikationsverbindungen erhebt, verarbeitet oder nutzt, greife **immer in das Fernmeldegeheimnis** ein. Hierfür könnte man anführen: Art. 10 GG bezwecke, die Kommunizierenden vor den spezifischen Gefahren der Fernkommunikation zu schützen. Der spezielle Schutz des Fernmeldegeheimnisses durch Art. 10 GG schaffe einen Ausgleich für den technisch bedingten Verlust an Beherrschbarkeit der Privatsphäre, der durch die Nutzung von Anlagen Dritter zwangsläufig entstehe, und errichte eine besondere Hürde gegen den vergleichsweise wenig aufwendigen Zugriff auf die dabei anfallenden Daten.[32] Im Vergleich zur unmittelbaren Kommunikation resultierten bei der Fernkommunikation spezifische Vertraulichkeitsgefahren aus dem eingesetzten Übertragungsweg und aus der Einschaltung eines Kommunikationsmittlers.[33] Die Kommunizierenden sollen durch die notwendige Einschaltung des Mittelsmannes nicht schlechter gestellt werden als sie bei unmittelbarer Kommunikation stünden.[34] Bei unmittelbarer Kommunikation wären die Kommunizierenden nicht auf einen Vertrag über Telekommunikationsdienstleistungen angewiesen, zu dessen Abwicklung einem Dritten Informationen über die Gesprächsteilnehmer anvertraut werden müssten. In dem heimlichen staatlichen Zugriff auf Informationen, die ein Kommunikationsmittler aus betrieblichen Gründen über Kommunizierende vorhalte, realisiere sich daher die spezifische Gefahr einer Fernkommunikation im Vergleich zur unmittelbaren Kommunikation. Zweck des Fernmeldegeheimnisses sei es, eine freie und unbefangene Telekommunikation zu gewährleisten.[35] Das Grundrecht solle die Bedingungen einer freien Telekommunikation aufrechterhalten.[36] Gerade die fehlende Anonymität der Fernkommunikation wegen der Vorhaltung von Bestandsdaten bei einem Mittelsmann beeinträchtige die Bereitschaft zu vertraulicher Kommunikation auf elektronischem Wege.

3 Begriff der Bestandsdaten

Als Telekommunikations-Bestandsdaten bezeichnet man Daten, die ein Anbieter von Telekommunikationsdiensten von seinen Kunden erhebt, um mit ihnen ein Vertragsverhältnis über die Erbringung von Telekommunikationsdiensten zu begründen, es auszugestalten oder zu ändern (vgl. § 3 Nr. 3 TKG). Es handelt sich also um diejenigen **Kundendaten**, die der

[27] Vgl. LG Frankenthal, Beschluss vom 21.05.2008, Az. 6 O 156/08.

[28] LG Frankenthal, Beschluss vom 21.05.2008, Az. 6 O 156/08.

[29] LG Bonn, Beschluss vom 21.05.2004, Az. 31 Qs 65/04, Abs. 17; vgl. auch OLG Wien, Beschluss vom 28.02.2005, Az. 20 Bs 27/05z.

[30] LG Frankenthal, Beschluss vom 21.05.2008, Az. 6 O 156/08.

[31] LG Frankenthal, Beschluss vom 21.05.2008, Az. 6 O 156/08.

[32] Vgl. BVerfGE 115, 166 (186).

[33] BVerfGE 85, 386 (396); BVerfG, Beschluss vom 09.10.2002, Az. 1 BvR 1611/96, Abs. 20.

[34] BVerfG, Beschluss vom 12.3.2003, Az. 1 BvR 330/96, Abs. 48.

[35] BVerfG, Beschluss vom 27.7.2005, Az. 1 BvR 668/04, Abs. 81.

[36] BVerfG, Beschluss vom 12.3.2003, Az. 1 BvR 330/96, Abs. 47; Urteil vom 14.07.1999, Az. 1 BvR 2226/94, Abs. 162.

Anbieter für die Durchführung des Vertrags über die Vermittlung von Telekommunikation dauerhaft in seinem Datenbestand halten muss, etwa Name, Anschrift, Geburtsdatum und Kontoverbindung des Kunden.

Nach verbreiteter Ansicht sollen auch **dienstbezogene Merkmale** wie eine dem Nutzer vom Anbieter zugewiesene Rufnummer oder E-Mail-Adresse sowie Kenn- oder Passwörter des Nutzers (z.B. PINs und PUKs im Mobiltelefonbereich) einfachgesetzlich als Bestandsdaten einzuordnen sein.[37] Entgegen der gesetzlichen Definition (§ 3 Nr. 3 TKG) soll es keinen Unterschied machen, ob diese Daten von dem Kunden erhoben oder ihm von dem Anbieter zugewiesen werden. Nach anderer Ansicht sollen dienstbezogene Merkmale dagegen als Verkehrsdaten einzuordnen sein.[38] Es handele sich um Daten, die bei der Erbringung eines Telekommunikationsdienstes verarbeitet werden (§ 3 Nr. 30 TKG). Die Daten dürften nach § 96 Abs. 2 TKG bis zur Beendigung des Vertragsverhältnisses gespeichert bleiben, weil sie „zum Aufbau weiterer Verbindungen" erforderlich seien. Als Bestandsdaten seien sie nicht einzuordnen, weil sie nicht „Daten eines Teilnehmers" seien, die „erhoben" werden, wie es § 3 Nr. 3 TKG fordert. Erheben sei nur das Beschaffen von Daten über den Betroffenen (§ 3 Abs. 3 BDSG), während dienstbezogene Merkmale (z.B. Anschlussnummer) vom Anbieter erzeugt und zugewiesen würden, um den Telekommunikationsdienst erbringen zu können. – Im Folgenden wird der international gebräuchliche Begriff der „Telekommunikationsdaten" („communications data") verwendet, um alle personenbezogenen Informationen über Teilnehmer zu kennzeichnen, die ein Telekommunikationsanbieter zur Erbringung eines Telekommunikationsdienstes erhebt, verarbeitet oder nutzt.

Keine Bestandsdaten sind unstreitig der **Inhalt** und die veränderlichen Umstände einzelner Kommunikationsvorgänge (z.B. Rufnummer des Gesprächspartners, Zeit eines Anrufs).

4 Geltung des Fernmeldegeheimnisses für alle Telekommunikationsdaten

Einer vollständigen Einbeziehung aller Telekommunikationsdaten in den Schutzbereich des Art. 10 GG steht der **Wortlaut** „Fernmeldegeheimnis" zunächst nicht entgegen. Er erlaubt die Auslegung, dass das „Geheimnis" auch die Vertragsbeziehung umfassen soll, welche den einzelnen Fernmeldevorgängen zugrunde liegt.

Für eine Einbeziehung von Bestandsdaten in den Schutzbereich des Art. 10 GG spricht, dass die Information, wer über welche Kennung welches Anbieters telekommuniziert und wie das Vertragsverhältnis zu diesem Anbieter ausgestaltet ist, die im Rahmen dieses Vertragsverhältnisses abgewickelten Kommunikationsvorgänge inhaltlich näher beschreibt und damit einen **näheren Umstand der einzelnen Kommunikationsvorgänge** darstellt: Wer (Name, Anschrift, Geburtsdatum) hat die jeweilige Verbindung über welchen Anbieter und unter Verwendung welchen Anschlusses (Anschrift und Lage des Anschlusses, Art des Anschlusses, Gerätenummer des Mobiltelefons) hergestellt oder entgegen genommen? Unter Verwendung welcher PIN oder welchen Passworts? Wie hat er für die Herstellung der Verbindung bezahlt (Bankverbindung, Tarif)? Hat er mit einer bevorzugten Nummer oder Adresse kommuniziert („Family&Friends", elektronisches E-Mail-Adressbuch)?

---

[37] Etwa BeckTKG-Büttgen, § 95, Rn. 3 f.

[38] Riechert, Neue Online-Dienste und Datenschutz (2006), 168 ff.; Bizer, DuD 2007, 602 (602).

Dass das Fernmeldegeheimnis für die näheren Umstände einzelner Kommunikationsvorgänge gilt, ist allgemein anerkannt.[39] Bestandsdaten unterscheiden sich von Verbindungsdaten nur dadurch, dass sie die Umstände von Kommunikationsvorgängen **stets in gleicher Weise** wiedergeben, während sich Verbindungsdaten typischerweise von Verbindung zu Verbindung ändern. Dass darin kein relevanter Unterschied liegen kann, zeigt das Beispiel der Internetnutzung. Während manche Internet-Zugangsanbieter dem Nutzer eine Internetkennung (IP-Adresse) fest zuweisen (dann Bestandsdatum), teilen andere Dienste dem Nutzer für jede Verbindung eine andere IP-Adresse zu (dann Verbindungsdatum). Solche technischen Zufälligkeiten können für die Bestimmung des Schutzbereichs des Fernmeldegeheimnisses richtigerweise keine Rolle spielen.

Historisch betrachtet existierten die Begriffe „Bestandsdaten" und „Verbindungsdaten" noch nicht, als das Bundesverfassungsgericht in der G10-Entscheidung den Schutzbereich des Fernmeldegeheimnisses erstmals definierte.[40] Verbindungsdaten gab es damals noch nicht, weil die Deutsche Bundespost analoge Vermittlungsstellen einsetzte, bei denen keine Verbindungsdaten anfielen. Die Begriffe „Bestandsdaten" und „Verbindungsdaten" führte erstmals die Telekom-Datenschutzverordnung (TDSV) 1991 ein.[41] Nach § 30 Abs. 2 des Postverfassungsgesetzes vom 8. Juni 1989[42] hatte die Bundesregierung „Vorschriften für die Unternehmen der Deutschen Bundespost zum Schutz personenbezogener Daten der am Post- und Fernmeldeverkehr Beteiligten" zu erlassen. Dementsprechend bestimmte § 4 TDSV 1991, dass zur Begründung und Änderung eines Vertragsverhältnisses über Telekommunikationsdienstleistungen einschließlich dessen inhaltlicher Ausgestaltung personenbezogene Daten (Bestandsdaten) erhoben und verwendet werden durften und ihre Löschung mit Ablauf des auf die Beendigung folgenden Kalenderjahres zu erfolgen hatte. Nach § 5 TDSV 1991 durften personenbezogene Daten zur Bereitstellung von Telekommunikationsdienstleistungen (Verbindungsdaten) erhoben und verwendet werden; sie mussten allerdings grundsätzlich mit Ende der Verbindung gelöscht werden. Die einfachgesetzliche Unterscheidung zwischen Bestands- und Verbindungsdaten hatte also die Funktion, unterschiedliche Verwendungs- und Löschungsregelungen für die beiden Datenarten zu definieren. Die begriffliche Unterscheidung knüpft demgegenüber nicht an den Begriff des Fernmeldegeheimnisses oder an dessen Zweck an. Dementsprechend ist in § 88 TKG von Bestands- oder Verbindungsdaten keine Rede. Die einfachgesetzliche Unterscheidung zwischen Bestands- und Verbindungsdaten ist mithin für die Bestimmung des Schutzbereichs des Art. 10 GG ohne Bedeutung.

Entscheidend ist der **Schutzzweck des Fernmeldegeheimnisses**. Art. 10 GG bezweckt, die Kommunizierenden vor den spezifischen Gefahren der Fernkommunikation zu schützen. Der spezielle Schutz des Fernmeldegeheimnisses durch Art. 10 GG schafft einen Ausgleich für den technisch bedingten Verlust an Beherrschbarkeit der Privatsphäre, der durch die Nutzung von Anlagen Dritter zwangsläufig entsteht, und errichtet eine besondere Hürde gegen den vergleichsweise wenig aufwändigen Zugriff auf die dabei anfallenden Daten.[43] Im Vergleich zur unmittelbaren Kommunikation resultieren bei der Fernkommunikation spezifische Vertraulichkeitsgefahren aus dem eingesetzten Übertragungsweg und aus der Einschaltung eines Kommunikationsmittlers.[44] Die Kommunizierenden sollen durch die

---

[39] BVerfG, 2 BvR 1085/05 vom 17.6.2006, Abs. 4; BVerfG, 1 BvR 330/96 vom 12.03.2003, Abs. 47; BVerfGE 100, 313 (358); BVerfGE 85, 386 (396); BVerfGE 67, 157 (172).

[40] BVerfGE 67, 157 (172).

[41] Verordnung der Bundesregierung über den Datenschutz bei Dienstleistungen der Deutschen Bundespost TELEKOM (TELEKOM-Datenschutzverordnung – TDSV), BGBl. I 1991, 1390.

[42] BGBl. I 1989, 1026.

[43] Vgl. BVerfGE 115, 166 (186).

[44] BVerfGE 85, 386 (396); BVerfG, Beschluss vom 09.10.2002, Az. 1 BvR 1611/96, Abs. 20.

notwendige Einschaltung des Mittelsmannes nicht schlechter gestellt werden als sie bei unmittelbarer Kommunikation stünden.[45] Zweck des Fernmeldegeheimnisses ist es also, die an der Fernkommunikation Beteiligten so zu stellen, wie sie bei unmittelbarer Kommunikation miteinander stünden.[46]

Im Falle der unmittelbaren Kommunikation wäre der Kommunizierende nicht auf den Abschluss eines Vertrags über Fernmeldedienste angewiesen, zu dessen Abrechnung und Abwicklung er einem Kommunikationsmittler Informationen zu seiner Person anvertrauen muss, über die seine Gesprächspartner nicht verfügen. Bei unmittelbarer Kommunikation gäbe es keine Vertragsverhältnisse zu einem Kommunikationsmittler, in deren Rahmen personenbezogene Daten über die an der Kommunikation Beteiligten gespeichert würden. In dem heimlichen staatlichen Zugriff auf Informationen, die ein Kommunikationsmittler aus betrieblichen Gründen über Kommunizierende vorhält, realisiert sich daher die spezifische Gefahr der Fernkommunikation im Vergleich zu unmittelbarer Kommunikation. Das spezifische Risiko für die Vertraulichkeit der Kommunikation, das mit der Inanspruchnahme von Fernmeldediensten verbunden ist, realisiert sich in der Vorhaltung von Vertragsdaten bei Kommunikationsmittlern.

Dem lässt sich nicht entgegen halten, unmittelbare Kommunikation sei **gleichfalls nicht anonym** möglich, weil die Gesprächspartner einander wahrnehmen; der Staat könne die Identität eines unmittelbaren Gesprächspartners etwa durch Vernehmung des anderen Gesprächsteilnehmers als Zeuge in Erfahrung bringen. Diese Argumentation trägt von vornherein nicht für die meisten Bestandsdaten. Ein unmittelbarer Gesprächspartner kann regelmäßig weder über Geburtsdatum, noch über Bankverbindung oder über Passwörter und PIN-Zugriffscodes seiner Gesprächspartner Auskunft geben. Aber auch eine Identifizierung ihm unbekannter Gesprächspartner, die ihre Identität nicht freiwillig offen gelegt haben, wird der andere Teil regelmäßig weder vornehmen noch ermöglichen können. Wenn man seine Identität nicht offen legt, wird ein Gespräch auf einem Marktplatz, in einer Kneipe, auf einem Bahnhof usw. in aller Regel nicht zur nachträglichen Identifizierbarkeit führen. Es kann allenfalls der Gesprächspartner beschrieben werden. Solche Fahndungen bleiben oftmals erfolglos, gerade bei Betrugs- oder Äußerungsdelikten, wie sie bei der Aufklärung von Fernkommunikation im Vordergrund stehen. Bei öffentlichen Veranstaltungen und sonst in der Öffentlichkeit bleibt man regelmäßig in der Menschenmenge anonym. Man behält weitgehend die Kontrolle darüber, ob und gegenüber wem man seine Identität offen legt. Bei der Fernkommunikation kann eine Identifizierung mithilfe des Gesprächspartners sogar leichter möglich sein, etwa wenn die Stimme auf seinem Anrufbeantworter aufgenommen wurde oder eine E-Mail vorliegt, die man auf technische Daten des verwendeten Computers, typische Schreibweisen usw. analysieren kann.

Weitgehend anonym möglich ist auch die **unmittelbare verkörperte Kommunikation**. Wer einen Brief ohne Absenderangabe in einen Briefkasten einwirft, bleibt unerkannt. Wer hingegen denselben Text per E-Mail oder SMS verschickt, gibt dem Empfänger eine persönliche Absenderkennung preis, die eine Identifizierung jederzeit ermöglicht.

Die Nutzung von Fernkommunikationsmitteln begründet auch dann eine **erhöhte Gefahr für die Vertraulichkeit** eines Kontakts, wenn die Gesprächspartner einander kennen. Einer Ausforschung der persönlichen Kontakte eines Beschuldigten wird meist schon entgegen stehen, dass die Ermittlungsbehörden nicht wissen, mit wem ein Beschuldigter in Kontakt

[45] BVerfG, Beschluss vom 12.3.2003, Az. 1 BvR 330/96, Abs. 48.

[46] BVerfGE 85, 386 (396); BVerfGE 100, 313 (363); Gusy, JuS 86, 89 (90 f.); vgl. auch Dreier-Hermes, Art. 10 Rn. 47.

gestanden hat, so dass eine Zeugenvernehmung oder andere Ermittlungsmaßnahme von vornherein ausscheidet. Wurde ein Kommunikationsmittler genutzt, sind die Kommunikationspartner demgegenüber leicht mithilfe der zentral gespeicherten Verbindungsdaten herauszufinden. Zudem ist der Staat zur Ausforschung unmittelbarer Kommunikation auf die Kooperation des Kommunikationspartners angewiesen, der aber – etwa wenn er selbst Beschuldigter ist – von einem Aussageverweigerungsrecht Gebrauch machen oder als Zeuge lügen oder sich nicht mehr erinnern kann. Im Fall der Fernkommunikation verfügt der Staat demgegenüber über einen stets erreichbaren, stets kooperationswilligen und über objektive Aufzeichnungen verfügenden Dritten, der ihm jederzeit kostengünstig Auskunft erteilen kann.

Das Argument, die Identifizierung gegenüber dem Kommunikationsmittler trete nur an die Stelle der **Identifizierung gegenüber dem Gesprächspartner bei unmittelbarer Kommunikation**, erweist sich mithin als nicht tragfähig. Wer sich der Fernkommunikationsmittel bedient, ist technisch bedingt sehr viel leichter zu identifizieren als wer unmittelbar kommuniziert. Mit dem Risiko aber, dass aus den eigenen Kontakten jederzeit (nachteilige) Folgen erwachsen können, steht und fällt die Möglichkeit zu freier und unbefangener, in allem vertraulicher Kommunikation.

Ziel des Fernmeldegeheimnisses ist es gerade, eine freie und unbefangene Kommunikation auch über die Ferne zu gewährleisten.[47] Das Grundrecht soll die Bedingungen einer freien Fernkommunikation aufrechterhalten.[48] Es soll verhindern, dass der Meinungs- und Informationsaustausch mittels Telekommunikationsanlagen deswegen unterbleibt oder nach Form und Inhalt verändert verläuft, weil die Beteiligten damit rechnen müssen, dass staatliche Stellen sich in die Kommunikation einschalten und Kenntnisse über die Kommunikationsbeziehungen oder Kommunikationsinhalte gewinnen.[49] An diesem Ziel gemessen muss sich der Schutz des Art. 10 GG auf alle Kommunikationsdaten erstrecken. Die fehlende Anonymität der Fernkommunikation wegen der Vorhaltung von Vertragsdaten bei einem Mittelsmann beeinträchtigt die Bereitschaft zur vertraulichen Kommunikation auf elektronischem Wege, weil man gegebenenfalls Nachteile infolge der eigenen Verbindungen, Aussagen, Bewegungen oder Interessen befürchten muss. Der Erläuternde Bericht zur Empfehlung des Europarats zum Datenschutz in der Telekommunikation[50] führt in Abs. 5 aus, dass die technische Entwicklung „nicht nur die Privatsphäre von Teilnehmern und Nutzern allgemein gefährden kann, sondern auch deren Kommunikationsfreiheit behindern kann, weil sie das Maß an Anonymität mindert, der sich Teilnehmer und Nutzer unter Umständen bei der Benutzung des Telefons bedienen wollen, indem sie gezwungen werden, ihre Identitäten offenzulegen oder elektronische Spuren zu hinterlassen, die es ermöglichen, die Benutzung ihres Telefons zu überwachen."[51] Die fehlende Beherrschbarkeit elektronischer Empfangsvorrichtungen bei einem Mittelsmann (z.B. elektronischer Anrufbeantworter, E-Mail-Postfach) schreckt ebenfalls von einer Nutzung dieser elektronischen Kommunikationsmittel ab.

Art. 10 GG soll eine **in allem vertrauliche Fernkommunikation** ermöglichen.[52] Eine in allem vertrauliche Fernkommunikation ist aber nur im Schutz der Anonymität möglich. Art. 10 GG

---

[47] BVerfG, Beschluss vom 27.7.2005, Az. 1 BvR 668/04, Abs. 81.

[48] BVerfG, Beschluss vom 12.3.2003, Az. 1 BvR 330/96, Abs. 47; Urteil vom 14.07.1999, Az. 1 BvR 2226/94, Abs. 162.

[49] BVerfGE 100, 313 (359); BVerfG, Beschluss vom 12.3.2003, Az. 1 BvR 330/96, Abs. 47.

[50] Empfehlung R (95) 4 vom 07.02.1995.

[51] https://wcd.coe.int/ViewDoc.jsp?id=529277&Site=CM&BackColorInternet=9999CC&BackColorIntranet=FFBB55&-BackColorLogged=FFAC75.

[52] BVerfGE 100, 313 (359); BVerfGE 107, 299, Abs. 50; BVerfGK 5, 74, Abs. 23; BVerfGK 8, 219, Abs. 4.

muss dazu gewährleisten, dass die Fernkommunikation im Alltag anonym erfolgen kann (entgegen § 111 TKG), und dass eventuell bei dem Mittler vorliegende Personendaten vor staatlichem Zugriff geschützt sind (entgegen §§ 112, 113 TKG). Anonymität muss auch gegenüber dem Gesprächspartner gewährleistet sein, was etwa im Fall von Notleidenden und Hilfesuchenden, die sich über ihr höchstpersönliches Problem bei einer Beratungsstelle informieren wollen, oder bei Presseinformanten evident ist.

Das Bundesverfassungsgericht hat bereits entschieden, dass sowohl die Meinungsfreiheit als auch das allgemeine Persönlichkeitsrecht gewährleisten, dass man unter seinem eigenen Namen kommunizieren darf.[53] Da die Grundrechte anerkanntermaßen stets auch das negative Recht gewährleisten, von einer grundrechtlich geschützten Freiheit nicht Gebrauch machen zu müssen, muss das Persönlichkeitsrecht auch das Recht auf anonymes Handeln gewährleisten. Im Bereich der Telekommunikation geht Art. 10 GG dem allgemeinen Persönlichkeitsrecht als Spezialgrundrecht vor.

Dass das **Recht auf anonyme Meinungsäußerung** grundrechtlich geschützt ist, hat der US-amerikanische Oberste Gerichtshof (Supreme Court) schon früh anerkannt. Er hat in der Entscheidung Talley v. California[54] ausgesprochen, dass die „anonyme Meinungsäußerung" eine wertvolle Rolle für den „Fortschritt der Menschheit" gespielt habe. Verfolgte Gruppen seien im Lauf der Geschichte nur im Schutz der Anonymität in der Lage gewesen, Unterdrückungspraktiken und -gesetze zu kritisieren. Auch könne eine „Identifizierung und die Furcht vor Vergeltung von vollkommen friedlichen Diskussionen wichtiger öffentlicher Angelegenheiten abschrecken". Eine Pflicht zur Nennung der Verantwortlichen auf Flugzetteln hat der Gerichtshof daher als Verstoß gegen die Meinungsfreiheit verworfen. In einer späteren Entscheidung[55] hat der Oberste Gerichtshof ausgeführt, Anonymität stelle oft ein „Schutzschild vor der Tyrannei der Mehrheit" dar. Nur im Schutz der Anonymität könne man seine Meinung äußern, ohne dass sie allein wegen der Person des Äußernden abgelehnt werde. Auf diese Weise helfe die Anonymität der Verbreitung von Ideen. Anonyme Meinungsäußerungen „exemplifizieren den Zweck des Grundrechtskatalogs und insbesondere der Meinungsfreiheit: unbeliebte Personen vor Vergeltung in einer intoleranten Gesellschaft zu schützen – und ihre Ideen vor Unterdrückung". Der Oberste Gerichtshof hat auch anerkannt, dass Vereine die Liste ihrer Mitglieder nicht offen legen müssen.[56] Es müsse möglich bleiben, anonym Mitglied eines unbeliebten Vereins zu sein, um die Freiheit auch unpopulärer Meinungen zu gewährleisten. Zuletzt haben die US-amerikanischen Instanzgerichte das Recht auf Anonymität auch auf das Internet angewandt. Der Washington District Court entschied 2001,[57] das Recht auf anonyme Meinungsäußerung sei von grundlegender Bedeutung für die Verabschiedung der US-amerikanischen Verfassung selbst gewesen, weil sowohl Befürworter („Federalist Papers") wie auch Widersacher ohne Namensnennung über die Ratifizierung der Verfassung stritten. Das Gericht entschied wörtlich: „Das Internet begünstigt den reichhaltigen, vielfältigen und weitreichenden Austausch von Ideen. Die Möglichkeit, seine Meinung im Internet äußern zu können, ohne dass die andere Seite alle Tatsachen über die eigene Identität kennt, kann offene Kommunikation und robuste Debatte fördern."[58] Auch **in Deutschland** haben sich die politische Opposition und der Widerstand gegen die Obrigkeit immer wieder der Anonymität bedienen müssen. Berühmte Schriftsteller wie Erich Kästner oder Kurt Tucholsky

---

53 BVerfGE 97, 391 (397 ff.).

54 362 U.S. 60 (1960).

55 McIntyre v. Ohio Elections Commission, 514 U.S. 334 (1995).

56 NAACP v. Alabama ex. rel. Patterson, 357 U.S. 449 (1958).

57 Doe v. 2TheMart.com, 140 F.Supp.2d 1088.

58 Doe v. 2TheMart.com, 140 F.Supp.2d 1088.

schrieben nicht unter ihrem eigenen Namen. 1849 veröffentlichte der Rechtswissenschaftler Theodor Mommsen einen Kommentar über die in der neuen Verfassung von 1848 garantierten „Grundrechte des deutschen Volkes" – anonym. Im gleichen Jahr veröffentlichte Adolph Streckfuß sein Werk „Das freie Preußen. Geschichte des Berliner Freiheitskampfes vom 18. März 1848 und seine Folgen", ohne seinen Namen zu nennen.

Gewährleistet danach die Meinungsfreiheit das Recht auf anonyme Meinungsäußerung, so muss auch die von Art. 10 GG gewährleistete Telekommunikationsfreiheit das Recht auf **anonyme Fernkommunikation** umfassen.

Die Möglichkeit, sich anonym informieren und kommunizieren zu können, ist **für viele Menschen unverzichtbar**:

- Menschen in besonderen Situationen (z.B. **Notlagen**, Krankheiten) sind nur in vollständiger Anonymität bereit, Informationen und Hilfe zu suchen, sich untereinander auszutauschen und sich beraten zu lassen (z.B. Chatrooms für Opfer sexuellen Missbrauchs).
- **Unternehmen** kommunizieren anonym, um Wirtschaftsspionage im Zusammenhang mit Vertragsverhandlungen zu verhindern, aber auch um sich selbst bei Wettbewerbern zu informieren, ohne ihre Identität preisgeben zu müssen.
- **Regierungsbehörden** (z.B. Nachrichtendienste) kommunizieren anonym, um im Internet recherchieren zu können, ohne als Regierungsbehörde identifizierbar zu sein. Zugleich sind sie darauf angewiesen, dass Menschen Straftaten anonym anzeigen können, die andernfalls nicht gemeldet würden und unaufgeklärt blieben. Dies gilt für die anonyme Offenlegung verschiedenster Missstände wie Steuerhinterziehung oder Korruption (sogenanntes „Whistleblowing").
- Nur anonyme Telekommunikation erlaubt es der **Bevölkerung autoritärer Staaten**, sich über politische Nachrichten zu informieren, die in ihrem eigenen Land durch Zensurmaßnahmen gesperrt sind.
- Deutsche **Journalisten**, die in autoritären Staaten arbeiten, sind auf anonyme Fernkommunikation angewiesen, um Informationen sicher empfangen und nach Deutschland übermitteln zu können, ohne dass der Aufenthaltsstaat dies zum Anlass für Maßnahmen gegen sie nehmen kann. Auch im Inland sind Informanten zunehmend nur noch im Schutz der Anonymität bereit, Auskunft zu geben. Im Wege anonymer Kommunikation gelingt es dann nicht selten, gravierende Missstände an das Licht der Öffentlichkeit zu bringen.
- Deutsche **Menschenrechtsgruppen** brauchen anonyme Kommunikationstechnik für ihre Arbeit mit autoritären ausländischen Staaten, sei es, um von diesen Staaten aus unerkannt mit ihrem Heimatbüro zu kommunizieren, sei es, um unerkannt mit oppositionellen Gruppen in den entsprechenden Staaten in Verbindung zu treten. Eine offene Kommunikation ist hier regelmäßig mit einem nicht zu verantwortenden Sicherheitsrisiko für die Beteiligten verbunden.
- **Regierungskritiker**, Blogger, Journalisten und Oppositionelle in autoritären ausländischen Staaten (z.B. Iran, Burma, Tibet), die sich für demokratische Reformen in ihrem Land einsetzen, können nur mithilfe anonymer Netze untereinander kommunizieren und die Öffentlichkeit auf die Situation in ihrem Land aufmerksam machen. Ohne den Schutz der Anonymität sind sie Verhaftungen, Gefängnisstrafen und Folter ausgesetzt; anonyme Fernkommunikation schützt also Leben und Freiheit dieser Personen. Beispielsweise in Burma ist die demokratische Opposition auf die anonyme Kommunikation per Internet angewiesen.

Gary Marx nennt insgesamt 15 **Funktionen von Anonymität in unserer Gesellschaft**:[59]

[59] Marx, What's in a Name? Some Reflections on the Sociology of Anonymity (1999), http://web.mit.edu/gtmarx/www/anon.html.

1. Erleichterung des Informations- und Kommunikationsflusses über **öffentliche Angelegenheiten** durch Schutz des Informationsgebers (z.B. Hotlines zur anonymen Anzeige von Problemen oder Verstößen durch Whistle Blower, anonyme Informanten der Presse).
2. Ermöglichung der **wissenschaftlichen Erforschung** von Sachverhalten, über die nur im Schutz der Anonymität Auskunft gegeben wird (z.B. Telefonstudien über Sexualverhalten, strafbares Verhalten, Gesundheit).
3. Zu verhindern, dass die Offenlegung des Urhebers einer Nachricht die **Wahrnehmung ihres Inhalts verhindert** oder beeinflusst (z.B. wegen Vorurteilen gegen den Autor).
4. Förderung des Meldens, Informierens, Kommunizierens, Austauschs und der Selbsthilfe im Hinblick auf Zustände oder Handlungen, die **stigmatisieren**, nachteilig sind oder intim (z.B. Hilfe für und Austausch der Betroffenen von Drogenmissbrauch, Gewalt in der Familie, abweichender sexueller Identität, psychischer oder physischer Krankheiten, AIDS oder anderer Sexualkrankheiten, Schwangerschaft; Kauf von Verhütungsmitteln, Medikamenten oder bestimmten Magazinen).
5. Ermöglichung von **Hilfe** trotz Strafbarkeit oder gesellschaftlicher Verachtung (z.B. anonyme Beratung von Drogenabhängigen, anwaltliche Beratung von Beschuldigten).
6. Schutz der Unterstützer **unbeliebter Handlungen** vor Verpflichtungen, Forderungen, Vorverurteilung, Verwicklungen oder Rache (z.B. Schutz der Identität verdeckter Ermittler oder von Polizist/innen oder von Menschenrechtsorganisationen).
7. Wahrnehmung **wirtschaftlicher Interessen** durch Einschaltung von Mittelsmännern/-frauen, um zu vermeiden, dass der Hintergrund einer geschäftlichen Transaktion bekannt wird (z.B. anonyme Testkäufe, anonyme Versteigerungen).
8. Schutz der eigenen Zeit, des eigenen Raums und der eigenen Person vor **unerwünschtem Eindringen** (z.B. durch Stalker, Fans oder Werbetreibende).
9. Dafür zu sorgen, dass **Entscheidungen** ohne Ansehung der Person getroffen werden (z.B. anonyme Bewerbung).
10. Schutz der eigenen Reputation und Ressourcen vor **Identitätsdiebstahl** (Handeln anderer unter dem eigenen Namen).
11. **Verfolgten Personen** die sichere Teilnahme am öffentlichen Leben ermöglichen (z.B. sich illegal aufhaltende Flüchtlinge).
12. Durchführung von **Ritualen**, Spielen und Feiern, welche das Verbergen der eigenen Identität oder das Annehmen einer fremden Identität zum Gegenstand haben und denen eine förderliche Wirkung auf die Persönlichkeitsentwicklung und psychische Gesundheit zugeschrieben wird (z.B. Rollenspiele).
13. Förderung des **Experimentierens** und Eingehens von Risiken ohne Furcht vor Konsequenzen, Scheitern oder Gesichtsverlust (z.B. Auftreten unter dem anderen Geschlecht in einem Chatroom).
14. Schutz der eigenen **Persönlichkeit**, weil die eigene Identität andere schlichtweg nichts angeht.
15. Erfüllung **traditioneller Erwartungen** (z.B. die traditionelle Möglichkeit, anonym Briefe schreiben zu können).

In all diesen Situationen kann eine freie, unbefangene und im allem vertrauliche Kommunikation nur im Schutz der Anonymität erfolgen. Nur im Schutz der Anonymität können die Beteiligten darauf vertrauen, dass staatliche Stellen keine Kenntnisse über die Kommunikationsbeziehungen gewinnen können.[60] Die **spezifischen Risiken der Fernkommunikation** resultieren aus der notwendigen Einschaltung eines Mittlers, dem aus betrieblichen Gründen die Person der Kommunikationsteilnehmer und weitere Tatsachen

[60] Vgl. BVerfGE 100, 313 (359); BVerfG, Beschluss vom 12.3.2003, Az. 1 BvR 330/96, Abs. 47.

über sie bekannt sein müssen. Eben vor diesem kommunikationstechnisch bedingten Verlust an Privatheit schützt Art. 10 GG.

Dieser klaren Einschlägigkeit des Schutzzwecks des Fernmeldegeheimnisses halten die Vertreter der Gegenauffassung letztlich nur die **Art der in Rede stehenden Daten** entgegen: dass Vertragsdaten unmittelbar keinen Aufschluss über einzelne Kommunikationsvorgänge geben, sondern im Vorfeld und unabhängig von Fernkommunikation erfasst und vorgehalten werden. Im Folgenden kann aber gezeigt werden, dass Bestandsdatenauskünfte in vielen Fällen durchaus Auskunft über einzelne Fernkommunikationsvorgänge geben und sich die von der Gegenauffassung befürwortete rein technische, an der Art der Daten orientierte Abgrenzung des Schutzbereichs des Art. 10 GG nicht aufrecht erhalten lässt. Im Anschluss wird diskutiert, ob Art. 10 GG tatsächlich nur die Vertraulichkeit einzelner Fernkommunikationsvorgänge schützt.

4.1 Aufdeckung von Kommunikationsverbindungen als Eingriff in Art. 10 GG

Besonders augenfällig ist die Betroffenheit des Fernmeldegeheimnisses, wenn der Staat durch Befragung eines Kommunikationsmittlers nach Bestandsdaten ihm noch **unbekannte telekommunikative Kontakte einer Person ausforscht**.

§ 113 TKG ermöglicht etwa die folgenden Anfragen und beschränkt dadurch eindeutig das Fernmeldegeheimnis:

- Welche Personen haben im Januar 2009 **Verbindungen** zu Telekommunikationsanschlüssen des Herrn X. hergestellt (bitte nur Bestandsdaten mitteilen)?
- Mit welchen Personen sind im Januar 2009 über den Anschluss 072191010 **Verbindungen** hergestellt worden (bitte nur Bestandsdaten mitteilen)?
- Welche Personen haben am 01.01.2009 zwischen 9.00 Uhr und 14.00 Uhr in den **Funkzellen** mobil telefoniert, welche den Schloßbezirk 3 in Karlsruhe abdecken (bitte nur Bestandsdaten mitteilen)?

Dass § 113 TKG **in der Praxis** so ausgelegt und angewandt wird, dass er Auskünfte der genannten Art abdeckt, ist mir aus der Auskunft eines Staatsanwalts bekannt. Er schreibt, „daß in allen Fällen, in denen seitens der Strafverfolgungsbehörden vom Provider eine Auskunft nach einem Bestandsdatum verlangt wird, auch wenn diese Auskunft nur unter Verwendung von Verkehrsdaten gem. § 113a TKG erbracht werden kann, keine Maßnahme nach § 100g StPO, sondern eine solche gemäß §§ 161,163 StPO i.V.m. 113, 113b Satz1 Halbsatz 2 TKG vorliegt. Die Staatsanwaltschaften handeln pflichtgemäß bundesweit entsprechend, die Provider geben die Daten auch heraus." Dass Behörden und Unternehmen § 113 TKG so auslegen und anwenden, hat auf Anfrage auch der betriebliche Datenschutzbeauftragte eines großen deutschen Telekommunikationsunternehmens bestätigt.

Selbst die Gegenauffassung dürfte nicht bestreiten, dass mit Fragen der oben genannten Art einzelne **Kommunikationsverbindungen ausgeforscht** werden – obwohl dem Staat Verkehrsdaten weder bereits vorliegen noch mitgeteilt werden. Ermittlungsbehörden können vielmehr als allgemeine Ermittlungsmaßnahme – etwa in einem Mordfall – über § 113 TKG ausforschen, mit wem ein Beschuldigter fernkommuniziert hat, wer mit dem Beschuldigten Kontakt hatte, wer am Tatort fernkommuniziert hat usw.

Das Fernmeldegeheimnis schützt nach ständiger Rechtsprechung des Bundesverfassungsgerichts die Information, „**zwischen welchen Personen** oder Fernmeldeanschlüssen Fernmeldeverkehr stattgefunden hat".[61] Eben dies lässt sich mit gezielten Anfragen nach § 113 TKG in Erfahrung bringen. Auf den genauen Zeitpunkt, die Häufigkeit oder Dauer der einzelnen Kontakte kommt es oftmals nicht an, etwa dann, wenn telekommunikative Kontakte zu einer bestimmten Person lediglich ausgeschlossen werden sollen.

In dieser Fallgruppe lässt sich nicht behaupten, in der Mitteilung von Name und Anschrift der Kommunikationspartner verwirkliche sich keine **spezifische Gefährdung** der von Art. 10 GG gewährleisteten Vertraulichkeit der ausgetauschten Informationen und der Umstände des Kommunikationsvorgangs. Die Mitteilung, wer mit wem fernkommuniziert hat, hebt gerade die Vertraulichkeit der offengelegten Kommunikationsvorgänge auf. Der Schutzzweck des Art. 10 GG ist einschlägig, weil im Fall unmittelbarer Kommunikation kein Mittler vergleichbare Auskünfte erteilen könnte.

In dieser Fallgruppe lässt sich auch nicht behaupten, Bestandsdaten fehle der **Bezug zu einem konkreten Telekommunikationsvorgang**. Denn die auf eine Anfrage der oben genannten Art mitgeteilten Bestandsdaten geben durchaus Auskunft über konkrete Telekommunikationsvorgänge. Würde das Telekommunikationsgeheimnis nicht mehr die Vertraulichkeit der Information schützen, wer mit wem kommuniziert hat, wäre es sinnentleert.

Dass Name und Anschrift der Teilnehmer **im Vorfeld konkreter Kommunikationsvorgänge** erhoben werden, ist für den Schutzbereich des Art. 10 GG unerheblich. Die einem Teilnehmer zugewiesene Rufnummer, die bei seinem Kommunikationsmittler als Bestandsdatum gespeichert ist, unterliegt unstreitig dem Fernmeldegeheimnis, wenn sie in Bezug auf einen konkreten Kommunikationsvorgang aufgezeichnet oder mitgeteilt wird (als Verbindungsdatum). Auch die Zeit läuft unabhängig von konkreten Kommunikationsvorgängen und unterliegt doch als Verbindungsdatum dem Fernmeldegeheimnis, wenn sie in Bezug auf einen konkreten Kommunikationsvorgang aufgezeichnet oder mitgeteilt wird (Verbindungsanfang, Verbindungsende). Nichts anderes kann für Name und Anschrift eines Teilnehmers gelten, wenn sie in Bezug auf einen konkreten Kommunikationsvorgang aufgezeichnet oder mitgeteilt werden (Personalien eines Anrufers oder Angerufenen). Die Art eines Datums ist schlichtweg untauglich, um den Schutzbereich des Fernmeldegeheimnisses zu bestimmen.

Eingewandt wird weiter, die Erhebung von Bestandsdaten sei **am wenigsten eingriffsintensiv**.[62] Diese Behauptung ist sowohl unzutreffend als auch unerheblich. Dass die Erhebung von Bestandsdaten am wenigsten eingriffsintensiv sei, widerlegt die hier diskutierte Fallgruppe eindrucksvoll. Die Offenlegung von Kontaktpersonen ist in hohem Maße eingriffsintensiv, etwa wenn die Zielperson Kontakt zu einem auf Steuerstrafrecht spezialisierten Rechtsanwalt oder zu einer Aidshilfestelle hatte. Die Information, zu welchen Zeiten von einem bestimmten Anschluss aus telefoniert worden ist, unterliegt als Verbindungsdatum unstreitig dem Fernmeldegeheimnis. Die Verbindungszeiten sind für sich genommen aber regelmäßig kaum aussagekräftig und nutzbar. Es ist nicht zu begründen, dass selbst die belanglosesten Gesprächsfragmente und Verbindungsdaten besser geschützt sein sollen als die zentrale Information, wer denn eigentlich an dem Gespräch

---

[61] BVerfG, 2 BvR 1085/05 vom 17.6.2006, Abs. 4; BVerfG, 1 BvR 330/96 vom 12.03.2003, Abs. 47; BVerfGE 100, 313 (358); BVerfGE 85, 386 (396); BVerfGE 67, 157 (172).

[62] öOGH, Beschluss vom 26.07.2005, Az. 11 Os 57/05z u.a., 10.

beteiligt war. – Im Übrigen ist dem Argument der Eingriffsintensität entgegen zu halten, dass das Gewicht des Grundrechtseingriffs dogmatisch nur im Rahmen der Rechtfertigung von Grundrechseingriffen eine Rolle spielen kann, nicht aber bei der Bestimmung des Schutzbereichs eines Grundrechts. Der Schutzbereich ist nach dem Schutzzweck des Grundrechts zu bestimmen.

Unerheblich ist das weitere Argument, Bestandsdaten unterschieden sich nicht von **Vertragsdaten eines beliebigen anderen Unternehmens**. Das mag allenfalls bei isolierter Betrachtung zutreffen. Andere Unternehmen mögen zwar auch über Name, Anschrift, Geburtsdatum und Rufnummer ihrer Kunden verfügen. Sie verfügen aber nicht über Telekommunikations-Verkehrsdaten, anhand derer sie diejenigen Kunden benennen können, die mit einer bestimmten anderen Person oder an einem bestimmten Ort fernkommuniziert haben.

Dass der Aussagegehalt von Bestandsdaten keinen **spezifischen Zusammenhang mit Telekommunikation** aufweise, ist unrichtig, wenn die Übermittlung von Bestandsdaten der Auskunfterteilung über Telekommunikationsvorgänge dient.

Das weitere Argument, Auskünfte der hier diskutierten Art **könnten auch etwa über Zeugenaussagen** erlangt werden, ist bereits oben widerlegt worden.[63] Die Einschaltung eines Mittlers macht die Fernkommunikation ausforschungsanfälliger als wenn nur der Gesprächspartner als Informationsquelle zur Verfügung stünde. Denn der Mittler kann ohne Vorkenntnisse von Kontakten angegangen werden und die gesamten Fernkommunikationsbeziehungen einer Person anhand seiner eigenen technischen Aufzeichnungen aufdecken.

Im Übrigen trifft das Argument, entsprechende Informationen ließen sich auch auf andere Weise gewinnen, **gleichermaßen auf Kommunikationsinhalte** und Verbindungsdaten zu. Ebenso wie die Identität von Gesprächspartnern lassen sich auch Gesprächsinhalte und sonstige Gesprächsumstände im Einzelfall durch Zeugenaussagen oder anders bestimmen. Gleichwohl würde niemand daraus folgern, Art. 10 GG sei überflüssig. Denn die Fernkommunikation ermöglicht einen heimlichen, zentralen, beweiskräftigen, kooperationsbereiten und kostengünstigen Zugriff auf Kommunikationsbeziehungen, wie ihn andere Ermittlungsmethoden niemals möglich machen können.

Es wird weiter argumentiert, im Vergleich zum eigentlichen Kommunikationsvorgang verdiene das **vorgelagerte Vertragsverhältnis** nicht den gleichen Schutz. Dieses Argument ist nicht nur unerheblich, sondern zumindest in der vorliegenden Fallgruppe auch unzutreffend. Denn wenn über § 113 TKG die Identität von Gesprächspartnern erfragt wird, ist der Fernmeldeverkehr selbst betroffen und nicht nur allgemein die zugrunde liegende Vertragsbeziehung. Art. 10 GG soll insbesondere die Vertraulichkeit des Fernmeldeverkehrs schützen. In diese wird eingegriffen, wenn offengelegt wird, zu wem oder von wem in der Vergangenheit Verbindungen hergestellt wurden.

Unzutreffend ist weiter die Behauptung, der **unmittelbare Erkenntniswert einer Bestandsdatenauskunft** liege nicht in der Information über einen bestimmten Telekommunikationsvorgang. Auf Fragen der oben genannten Art werden nämlich nicht nur Bestandsdaten mitgeteilt, sondern die Auskunft nimmt stets die Anfrage auf und lautet daher etwa wie folgt: „Auf Ihre Anfrage vom 01.04.2009 teilen wir mir, dass im Januar 2009 die folgenden Personen Verbindungen zu dem Anschluss 072191010 hergestellt haben: ...“

[63] Seite 8.

Der Bevollmächtigte der Bundesregierung meint, eine **klare Abgrenzung des Schutzbereichs** von Art. 10 GG sei nur anhand der Art der betroffenen Daten – Bestandsdaten oder Verkehrsdaten – möglich. Dies ist unzutreffend. Eine klare Abgrenzung ist auch dann möglich, wenn Art. 10 GG umfassend vor der Aufdeckung und Ausforschung des Fernmeldeverkehrs schützt. Der Eingriff in die Vertraulichkeit des Fernmeldeverkehrs ist evident, wenn der Kommunikationsmittler eine Anfrage nach Name und Anschrift eines Teilnehmers nur durch Einsicht in seine Aufzeichnungen über hergestellte Verbindungen (Verkehrsdaten) beantworten kann. Die vorliegende Fallgruppe lässt sich von anderen Bestandsdatenauskünften also leicht abgrenzen.

Als Hilfsargument wird schließlich noch angeführt, dass selbst wenn man in Fällen der genannten Art das Fernmeldegeheimnis für einschlägig erachte, sich § 113 TKG wegen dessen Absatz 1 Satz 3 **verfassungskonform dahin auslegen** lasse, dass er für solche Anfragen nicht einschlägig sei. Diese Erwägung trägt nicht. Erstens ergibt sich aus der Entstehungsgeschichte des dritten Satzes, dass dieser Satz nur Fälle des Satzes 2 regeln sollte, in denen Codes zum Zugriff auf Kommunikationsinhalte erhoben wurden. Zweitens wäre der dritte Satz zu unbestimmt, um Anfragen zur Ausforschung von Fernmeldebeziehungen auszunehmen.[64] Dass die Praxis § 113 Abs. 1 S. 3 TKG eine derartige Ausnahme bislang nicht entnimmt, belegt, dass es mit dem Gebot der Normenklarheit unvereinbar wäre, der Vorschrift nachträglich ein solches Verständnis beizulegen. Drittens ist § 113 Abs. 1 S. 3 TKG schon seinem Wortlaut nach nicht einschlägig. Er nimmt nämlich nur Bezug auf die „hierfür einschlägigen gesetzlichen Vorschriften". Es gibt aber keine andere gesetzliche Vorschrift, welche Bestandsdatenanfragen nach bestimmten Fernmeldebeziehungen regelt. Insbesondere sehen die §§ 100a, 100g StPO, wie der Bevollmächtigte der Bundesregierung zutreffend ausführt, keine Auskünfte über Bestandsdaten vor.

4.2 Aufdeckung von Kommunikationsinhalten als Eingriff in Art. 10 GG

§ 113 TKG ermächtigt in gleicher Weise zur **Ausforschung von Kommunikationsinhalten**, indem er etwa Anfragen der folgenden Art möglich macht:

- In den E-Mail-Postfächern welcher Personen befinden sich **Nachrichten**, in denen der Name „X."/das Wort „Y" vorkommt (bitte nur Bestandsdaten mitteilen)?

§ 113 TKG ermächtigt den Staat zu Anfragen der genannten Art. Denn bei den angefragten Bestandsdaten handelt es sich um „Auskünfte über die nach den §§ 95 und 111 erhobenen Daten". § 113 TKG ermächtigt nach seinem Wortlaut zu sämtlichen Anfragen, deren Ergebnis die Übermittlung von Bestandsdaten ist. Er bestimmt – anders als § 100b Abs. 2 StPO – nicht, welche Angaben dem Mittler in dem Auskunftersuchen mitzuteilen sind. Er schließt es nicht aus, Kommunikationsteilnehmer anhand des Inhalts oder der näheren Umstände ihrer Telekommunikation ausfiltern zu lassen. Er lässt die selektive Anforderung von Bestandsdaten, die eine Rasterung von Verkehrs- oder Inhaltsdaten bedingt, zu.

Für diese Auslegung des § 113 TKG spricht der Wortlaut der Vorschrift und ihre Anwendung durch die Praxis in den zu 4.1 genannten Fällen. Dass § 113 Abs. 1 S. 3 TKG eine andere Auslegung nicht mit hinreichender Klarheit determiniert, ist bereits dargelegt worden. Für diese Auslegung des § 113 TKG spricht auch, dass es keine andere Vorschrift gibt, die zur Anforderung von Bestandsdatenauskünften ermächtigt. Insbesondere hat der Gesetzgeber

[64] Vgl. VG Köln, Beschluss vom 11.12.2008, Az. 21 L 1398/08, BeckRS 2009, 32522.

§ 100g StPO ausdrücklich auf die Erhebung von Verkehrsdaten beschränkt – getreu seiner Meinung, der Zugriff auf Bestandsdaten greife nie in das Fernmeldegeheimnis ein.

Eine **grundrechtsfreundliche Auslegung** des § 113 TKG ist zwar denkbar. Denn Bestandsdatenauskünfte, die das Ergebnis einer Durchsuchung von Inhalts- oder Verkehrsdaten sind, sind letztlich keine „Auskünfte über die nach den §§ 95 und 111 erhobenen Daten", sondern – in Verbindung mit dem Inhalt der Anfrage – Auskünfte über Inhalt oder nähere Umstände des Fernmeldeverkehrs. Doch eine solche Auslegung ist dem Wortlaut des § 113 TKG nicht mit hinreichender Deutlichkeit zu entnehmen und widerspräche dem Gebot der Normenklarheit. Zumal der Gesetzgeber für den Fall der Identifizierung von Internetnutzern anhand ihrer dynamischen IP-Adresse ausdrücklich erklärt hat, § 113 TKG solle die dazu erforderliche Rasterung des gesamten Verbindungsdatenbestandes abdecken.[65] Es kann nicht Aufgabe des Bundesverfassungsgerichts sein, eine vom Gesetzgeber zu weit gefasste Eingriffsnorm durch einschränkende Auslegung auf das verfassungsgemäße Maß zu beschränken. Das gilt erst recht, wenn der Gesetzgeber die Vorschrift bewusst weit gefasst und von einer Konkretisierung abgesehen hat.[66]

Die **Gegenansicht**, derzufolge die Mitteilung von Bestandsdaten nie in das Fernmeldegeheimnis eingreife, müsste auch in dem hier diskutierten Fall einen Eingriff in Art. 10 GG verneinen. Die beauskunfteten Bestandsdaten geben nämlich auch hier nicht unmittelbar Aufschluss über Inhalt oder Umstände eines konkreten Telekommunikationsvorgangs. Dass der Mittler zur Auskunfterteilung Inhalts- und Verkehrsdaten verarbeiten muss, soll unerheblich sein, weil es sich um einen internen Vorgang handele, bei dem der um Auskunft nachsuchenden Stelle keine Kenntnis von den Inhalts- oder Verkehrsdaten vermittelt wird.

Dass tatsächlich aber ein **Eingriff in das Fernmeldegeheimnis** vorliegt, obwohl ausschließlich Bestandsdaten erfragt und beauskunftet werden, liegt auf der Hand. Mit seiner Auskunft forscht der Staat nämlich mittelbar einzelne Fernkommunikationsvorgänge aus. Durch die Auskunft erfährt er, „zwischen welchen Personen (...) Fernmeldeverkehr" in Form von E-Mails eines bestimmten Inhalts „stattgefunden hat" und zwischen welchen nicht.

Erkennt man aber in diesem Beispielsfall an, dass das Fernmeldegeheimnis vor der internen Rasterung von Kommunikationsinhalten und der Offenlegung der daraus resultierenden Bestandsdaten schützt, so kann **für die Fallgruppe 4.1 nichts anderes** gelten: Hier erfolgt eine interne Rasterung von Verkehrsdaten und die Offenlegung der daraus resultierenden Bestandsdaten. In beiden Fällen geben die angefragten Suchkriterien in Verknüpfung mit den beauskunfteten Bestandsdaten Aufschluss über Inhalt oder nähere Umstände des Fernmeldeverkehrs.

4.3 Nähere Ausforschung von Telekommunikationsvorgängen als Eingriff in Art. 10 GG

Besonders augenfällig ist die Betroffenheit des Fernmeldegeheimnisses auch, wenn der Staat durch Inanspruchnahme eines Kommunikationsmittlers den Teilnehmer an einem ihm bekannten Fernkommunikationsvorgang **identifiziert** und dadurch die Anonymität des Fernkommunikationsvorgangs aufhebt.

---

[65] BT-Drs. 16/6979, 46.

[66] Vgl. BVerfG, 1 BvR 2074/05 vom 11.3.2008, Abs. 155.

§ 113 TKG ermöglicht etwa die folgenden Anfragen und beschränkt dadurch eindeutig das Fernmeldegeheimnis:

- Wer hat am 01.01.2009 um 12:01 eine **Verbindung** zu dem Anschluss 072191010 hergestellt (bitte nur Bestandsdaten mitteilen)?
- Wer hat am 01.01.2009 um 12:01 an der **Internetverbindung** mit der dynamischen IP-Adresse 101.101.101.101 teilgenommen (bitte nur Bestandsdaten mitteilen)?

Derartige Anfragen sind möglich, wenn der Staat von einem Fernkommunikationsvorgang **bereits Kenntnis** hat, etwa aus Aufzeichnungen oder Aussagen des Kommunikationspartners oder seines Endgeräts oder aus einer vorangegangenen Verbindungsdatenanfrage.

Der zweite Fall (**Internetverbindung**) ist nicht anders zu behandeln als der erste Fall (Telefonverbindung). Der Teilnehmer an einer bestimmten Telefonverbindung ist vor Identifizierung ebenso geschützt wie der Teilnehmer an einer bestimmten Internetverbindung. Das Grundgesetz sieht eine Differenzierung nach dem Inhalt der Telekommunikation nicht vor. Der zweite Fall unterscheidet sich auch nicht dadurch, dass bereits Verbindungsdaten bekannt sind, die eine Individualisierung des Teilnehmers ermöglichen (IP-Adresse und Verbindungszeit). Denn auch in dem ersten Fall sind Verbindungsdaten bekannt, die eine Individualisierung des Teilnehmers ermöglichen (Zielanschluss und Verbindungszeit).

Dass § 113 TKG **in der Praxis** so ausgelegt und angewandt wird, dass er Auskünfte der genannten Art abdeckt, ist für den zweiten Fall evident, gilt aber auch für den ersten Fall. Zum Beleg zitiere ich aus der mir vorliegenden Auskunft des Staatsanwalts, der ungenannt bleiben möchte:

> *„Als **Staatsanwalt** bin ich, wie viele andere auch, regelmäßig mit Ermittlungsverfahren befaßt, in denen ein Beschluss gem. § 100g StPO häufig den einzigen Ermittlungsansatz bietet. In diesem Zusammenhang ist mir aufgefallen, daß der Beschluss des BVerfG die in der Praxis sehr häufigen und bedeutsamen Fälle der Anschlussinhaberfeststellung bei behaupteten Rechtsverstößen nicht problematisiert. Ich darf zur Darstellung der Ihnen sicher bekannten Problematik auf zwei jüngst ergangene Entscheidungen des LG Offenburg und des LG Frankenthal verweisen (http://medien-internet-und-recht.de/volltext.php?mir_dok_id=1645 und http://medien-internet-und-recht.de/volltext.php?mir_dok_id=1601). Der letztgenannte Beschluss des LG Offenburg gibt m.E. die Rechtslage seit 01.01.08 korrekt wieder, so daß in allen Fällen, in denen seitens der Strafverfolgungsbehörden vom Provider eine Auskunft nach einem Bestandsdatum verlangt wird, auch wenn diese Auskunft nur unter Verwendung von Verkehrsdaten gem. § 113a TKG erbracht werden kann, keine Maßnahme nach § 100g StPO, sondern eine solche gemäß §§ 161,163 StPO i.V.m. 113, 113b Satz1 Halbsatz 2 TKG vorliegt. Die Staatsanwaltschaften handeln pflichtgemäß bundesweit entsprechend, die Provider geben die Daten auch heraus.*
>
> *(...) Beispiel: der A , Rufnummer bekannt, wird am 13.06.2008 um 11:10 MEZ von unbekanntem Anrufer massiv beleidigt. Bis zum 31.12.2007 wäre die Ermittlung des zur Tat verwendeten Anschlusses über einen **Suchlauf** gem § 100g StPO erfolgt, allerdings hätte es eines richterlichen Beschlusses bedurft. Häufig wurden solche Anträge in der Vergangenheit abgelehnt. Nach neuer Rechtslage genügt ein einfaches Auskunftsersuchen gem §§ 161,163 StPO iVm 113,113b TKG, da die begehrte Auskunft des zur Tat verwendeten Anschlusses fraglos ein Bestandsdatum ist, das bei Lieferung der schon bekannten Bestandsdaten (Angerufener Anschluss, genaue Uhrzeit) dem Provider*

die Möglichkeit eröffnet, unter Verwendung der bei ihm gespeicherten Verkehrsdaten die gewünschte Auskunft (Anschluss und Anschlussinhaber) zu erteilen."

Dass Behörden und Unternehmen § 113 TKG so auslegen und anwenden, hat auf Anfrage auch der betriebliche **Datenschutzbeauftragte** eines großen deutschen Telekommunikationsunternehmens bestätigt.

Art. 10 GG schützt die Anonymität der an einem Fernkommunikationsvorgang Beteiligten. Er gewährleistet die Vertraulichkeit der Information, „zwischen welchen Personen oder Fernmeldeanschlüssen Fernmeldeverkehr stattgefunden hat".[67] Dass Art. 10 GG das Recht auf – auch gegenüber dem Gesprächspartner[68] – anonyme Kommunikation garantiert, gewährleistet die Grundbedingungen einer freien Fernkommunikation in unserer Gesellschaft. Wie sehr etwa ratsuchende oder notleidende Menschen sowie Informanten von Presse oder Aufsichtsbehörden auf die Möglichkeit anonymer Kommunikation angewiesen sind, ist bereits umfassend ausgeführt worden. Soll Art. 10 GG aber die freie, unbefangene und in allem vertrauliche Fernkommunikation gewährleisten,[69] so muss er vor der Identifizierung der an einem Kommunikationsvorgang Beteiligten schützen. Die Gegenansicht wird dem Schutzzweck des Fernmeldegeheimnisses nicht gerecht.[70]

Durch eine Namensauskunft werden die bereits bekannten Verbindungsdaten mit einer Person und diese somit mit einem konkreten Nutzungsvorgang und -zeitpunkt verknüpft.[71] Die **Identifizierung des an einem Telekommunikationsvorgang Beteiligten** berührt und offenbart damit die näheren Umstände des betroffenen Telekommunikationsvorgangs.[72] Erst die Kombination der bekannten Verkehrsdaten mit den zu beauskunftenden Identitätsdaten gibt Aufschluss über die konkrete, an dem betreffenden Kommunikationsvorgang beteiligte Person.[73] Die letztlich begehrte Information, dass und welche Verbindung zu welchem Zeitpunkt von welchem Teilnehmer hergestellt wurde, unterliegt dem Fernmeldegeheimnis.[74] Es handelt sich hierbei nicht um eine Information, die einem Eintrag in das Telefonbuch vergleichbar ist, sondern um die Ermittlung, wer mit wem zu welchem Zeitpunkt worüber und wie lange kommuniziert hat.[75] Die Richtlinie 2006/24/EG zur Vorratsdatenspeicherung bezeichnet „Rufnummer" sowie „Name und die Anschrift des Teilnehmers" ausdrücklich als „zur Rückverfolgung und Identifizierung der Quelle einer Nachricht benötigte Daten" (Art. 5 Abs. 1 Buchst. a) und nimmt damit auf die näheren Umstände eines konkreten Kommunikationsvorgangs Bezug.

Die obigen Beispiele für die Ermittlung der Person eines Beteiligten an einem Kommunikationsvorgang wurden bewusst gewählt, um deutlich zu machen, dass die Anfragen keineswegs mit einem **Blick in das Telefonbuch** vergleichbar sind. Solange dem Anbieter keine statische Anschlusskennung benannt wird, muss er Verbindungsdaten konsultieren, um den gesuchten Kommunikationspartner zu ermitteln und mitzuteilen. Damit ist die Individualisierung des Kommunikationspartners untrennbar mit der Nutzung des

---

[67] BVerfG, 2 BvR 1085/05 vom 17.6.2006, Abs. 4; BVerfG, 1 BvR 330/96 vom 12.03.2003, Abs. 47; BVerfGE 100, 313 (358); BVerfGE 85, 386 (396); BVerfGE 67, 157 (172).

[68] BVerfGE 85, 386 (398 f.).

[69] BVerfGE 100, 313 (359); BVerfGE 107, 299, Abs. 50; BVerfGK 5, 74, Abs. 23; BVerfGK 8, 219, Abs. 4; BVerfG, Beschluss vom 27.7.2005, Az. 1 BvR 668/04, Abs. 81.

[70] LG Frankenthal, Beschluss vom 21.05.2008, Az. 6 O 156/08.

[71] Vgl. OLG Zweibrücken, Beschluss vom 27.10.2008, Az. 3 W 184/08 m.w.N.

[72] Vgl. OLG Zweibrücken, Beschluss vom 27.10.2008, Az. 3 W 184/08 m.w.N.

[73] Vgl. VG Köln, Beschluss vom 11.12.2008, Az. 21 L 1398/08, BeckRS 2009, 32522.

[74] Vgl. LG München, Beschluss vom 12.03.2008, Az. 5 Qs 19/08.

[75] OLG Frankfurt, Urteil vom 01.07.2008, Az. 11 U 52/07; LG München, Beschluss vom 12.03.2008, Az. 5 Qs 19/08.

Mediums im Einzelfall verbunden, so dass keine Vergleichbarkeit mit einer Telefonnummer besteht, welche unabhängig vom Zeitpunkt der Nutzung stets fix einer Person zugewiesen ist.

Auch die Gegenauffassung weist indes zutreffend darauf hin, dass es **keinen Unterschied machen kann**, anhand welcher Daten der Mittler den gesuchten Gesprächsteilnehmer identifiziert. Ob die Benennung des Gesprächsteilnehmers anhand von Verbindungs- oder Bestandsdaten erfolgt, ist gemessen am Schutzzweck des Fernmeldegeheimnisses unerheblich. In beiden Fällen ermittelt der Staat, zwischen welchen Personen Fernmeldeverkehr stattgefunden hat. Deswegen liegt auch in beiden Fällen ein Eingriff in das Fernmeldegeheimnis vor.

Ein **Eingriff** in das Fernmeldegeheimnis liegt daher auch in der folgenden Anfrage über § 112 TKG oder § 113 TKG:

- Wer war am 01.01.2009 **Inhaber der Rufnummer** 072191010 (über die um 12:01 eine Verbindung zu dem Anschluss 072191011 hergestellt worden ist)?

Wem eine Anschlusskennung (z.B. Rufnummer, E-Mail-Adresse, IP-Adresse) zugewiesen ist, muss zumindest dann dem Schutz des Fernmeldegeheimnisses unterliegen, wenn die Erhebung dieser Information der Identifizierung des Teilnehmers an einem konkreten Kommunikationsvorgang dient.[76] Nur wenn die Gesprächsteilnehmer vor einer Identifizierung geschützt sind, können sie ebenso anonym fernkommunizieren wie sie Menschen unmittelbar ansprechen können (wie anonyme Rufnummer), Briefe schreiben können (wie anonyme E-Mail-Adresse) und sich informieren können (wie anonyme IP-Adresse), ohne ihre Identität offenbaren zu müssen.

Die Gegenansicht führt zu **absurden Ergebnissen** in Fällen, in denen der Staat nähere Umstände eines Kommunikationsvorgangs kennt, nicht aber die Kennung oder Person des Anrufers: Fragt der Staat den Kommunikationsmittler, über welche Rufnummer am 01.01.2009 um 12:01 eine Verbindung zu dem Anschluss 072191010 hergestellt wurde, so liegt unstreitig ein Eingriff in das Fernmeldegeheimnis vor.[77] Denn mit Offenlegung der Rufnummer des anrufenden Anschlusses wird Auskunft über ein Verbindungsdatum erteilt (vgl. § 96 Abs. 1 Nr. 1 TKG). Die Identität des Inhabers der beauskunfteten Rufnummer kann dann in einem zweiten Schritt mithilfe einer Namensauskunft ermittelt werden. Fragt der Staat den Kommunikationsmittler hingegen sogleich, welche Person (Name, Anschrift) am 01.01.2009 um 12:01 eine Verbindung zu dem Anschluss 072191010 hergestellt hat, so wäre mit der Gegenansicht kein Eingriff in das Fernmeldegeheimnis anzunehmen, weil „nur" Bestandsdaten mitgeteilt würden. Es lässt sich nicht rational erklären, weshalb die nichtssagende Rufnummer eines Anrufers den Schutz des Fernmeldegeheimnisses genießen soll, nicht aber die Personalien des Anrufers. Dasselbe gilt für andere belanglose Verbindungsdaten einer bereits bekannten Verbindung (z.B. Gesprächsdauer, Datenvolumen). Wenn diese Details den Schutz des Fernmeldegeheimnisses genießen, muss es erst Recht die zentrale Angabe der Identität der Kommunikationspartner.

Wenn Vertreter der Gegenauffassung argumentieren, die Identität eines Anschlussinhabers sei einem bloßen **Eintrag in das Telefonbuch vergleichbar**, so ist dies sowohl unerheblich als auch falsch. Unerheblich ist das Argument, weil es auf die Schutzwürdigkeit der Daten abstellt, die dogmatisch von vornherein nicht für die Bestimmung des Schutzbereichs,

---

[76] Dix, Schriftsatz vom 29.01.2007 in diesem Verfahren, 6 und 8; Werg, MMR 2006, 77 (82) für E-Mail-Adressen.

[77] OVG Bremen, NJW 1994, 1769 (1770); BeckTKG-Büttgen, § 95, Rn. 3 f.

sondern erst für das Gewicht des Grundrechtseingriffs relevant sein kann. Falsch ist das Argument, weil die Aufnahme in ein Telefonbuch freiwillig (§ 45m TKG) und deswegen mit einer hoheitlichen Bestandsdatenanfrage nicht vergleichbar ist. Die Nutzer von Internetzugängen, E-Mail-Postfächern und Anonymisierungsdiensten werden ohnehin nicht in Telefonbüchern verzeichnet.

Das Fernmeldegeheimnis schützt selbstverständlich nicht davon, dass der Staat einen freiwilligen Telefonbucheintrag wie jede andere Person auf dem dafür vorgesehenen Weg durch **Konsultation eines Telefonbuchs** nutzt. Ein Eingriff in das Telekommunikationsgeheimnis scheidet anerkanntermaßen aus, wenn der Staat allgemein zugängliche Inhalte erhebt,[78] etwa aus einem Telefonbuch. Dies gilt auch dann, wenn der Blick in das Telefonbuch der Identifizierung eines Gesprächsteilnehmers dient. Weil die Aufnahme in ein Telefonbuch freiwillig ist, ist Art. 10 GG nach seinem Schutzzweck in diesem Fall nicht einschlägig.

Dies erlaubt aber keinen Rückschluss auf die Eingriffsqualität der **hoheitlichen Erhebung** nicht öffentlich zugänglicher Daten bei dem Kommunikationsmittler. Nur der Staat kann einen Kommunikationsmittler zwingen, einen Anschlussinhaber zu identifizieren. Die Identifizierung eines Gesprächsteilnehmers wird erst dadurch ermöglicht, dass der Kommunikationsmittler zur Ermöglichung und Abrechnung der Fernkommunikation entsprechende Bestandsdaten erheben und vorhalten muss. Der zugreifende Staat nutzt die spezifische Verletzlichkeit der Fernkommunikation zur Ermittlung eines Gesprächsteilnehmers aus; der Schutzzweck des Fernmeldegeheimnisses ist einschlägig. § 112 TKG etwa ermöglicht in Sekundenschnelle kostenlos automatisierte Suchverfahren und Rasterungen, Ähnlichkeitssuchen und Einblicke in nichtöffentliche Teilnehmerdaten.

Die Beschwerdeführer sind im Übrigen in keinem Telefonbuch verzeichnet und haben ihre Privatnummern auch sonst nicht veröffentlicht. Sie sind nicht damit einverstanden, dass staatliche Stellen ihre Diensteanbieter zwingen, ihre Rufnummer, E-Mail-Adresse oder IP-Adresse ohne ihren Willen und ohne ihr Wissen auf ihre Person zurückzuführen.

Dass die Identifizierung eines Anschlussinhabers **nicht unmittelbar Inhalt oder Umstände** eines konkreten Telekommunikationsvorgangs betreffe, ist danach falsch. In der vorliegenden Fallgruppe, in welcher der Teilnehmer an einem bestimmten Kommunikationsvorgang identifiziert werden soll, betrifft die Identifizierung des Teilnehmers durchaus den konkreten Kommunikationsvorgang. „Zwischen welchen Personen (...) Fernmeldeverkehr stattgefunden hat", ist ein näherer Umstand des Kommunikationsvorgangs.[79]

Dem lässt sich nicht entgegen halten, es könne keinen Unterschied machen, **zu welchem Zweck** der Inhaber einer Kennung erfragt werde. Es macht durchaus einen Unterschied, ob eine Auskunft zu dem Zweck eingeholt wird, die näheren Umstände eines konkreten Kontakts zu erforschen, oder ob nur allgemein die Person des Inhabers eines Anschlusses ausgekundschaftet werden soll. Denn für die Eingriffstiefe entscheidend ist die Nutzbarkeit der jeweils erhobenen Daten, auch in Verknüpfung mit anderen Erkenntnissen.[80] Zielt die Anfrage nach der Identität eines Anschlussinhabers darauf ab, ihn als Beteiligten an einem konkreten Kommunikationsvorgang zu ermitteln, so ist der Schutzzweck des Fernmeldegeheimnisses unzweifelhaft einschlägig. Denn das Fernmeldegeheimnis schützt

---

[78] BVerfG, Urteil vom 27.2.2008, Az. 1 BvR 370/07 , Abs. 293.

[79] BVerfG, 2 BvR 1085/05 vom 17.6.2006, Abs. 4; BVerfG, 1 BvR 330/96 vom 12.03.2003, Abs. 47; BVerfGE 100, 313 (358); BVerfGE 85, 386 (396); BVerfGE 67, 157 (172).

[80] BVerfGE 65, 1 (45).

jedenfalls vor der Ausforschung, wer an einem konkreten Kommunikationsvorgang beteiligt war.

Nicht richtig ist auch der Einwand, die Abgrenzung nach dem Zweck einer Datenerhebung sei **nicht praktikabel**. Bereits heute regeln viele Gesetze die Zulässigkeit von Datenerhebungen abhängig davon, zu welchem Zweck sie erfolgen (z.B. zur Strafverfolgung, zur Strafvollstreckung, zur Ermittlung des Aufenthaltsortes usw.). Es ist durchaus möglich, den Schutzbereich des Fernmeldegeheimnisses so zu definieren, dass es vor der Erhebung von Bestandsdaten zur Identifizierung von Beteiligten an einem konkreten Kommunikationsvorgang schützt, nicht aber vor der Erhebung von Bestandsdaten unabhängig von einem konkreten Kommunikationsvorgang.

Allerdings erfolgen diese Ausführungen nur vorsorglich für den Fall, dass man überhaupt die Auffassung vertritt, Art. 10 GG schütze nur die Vertraulichkeit konkreter Kommunikationsvorgänge. Wie an späterer Stelle näher auszuführen sein wird, schützt das Fernmeldegeheimnis nach seinem Zweck **umfassend vor jeder zwangsweisen Erhebung von Teilnehmerdaten** bei Kommunikationsmittlern. Das Fernmeldegeheimnis muss umfassend die Information schützen, dass jemand ein Vertragsverhältnis zu einem Fernmeldeunternehmen unterhält, welche Rufnummer ihm zur Kommunikation zugewiesen ist usw. Diese Schutzbereichsdefinition entzieht dem Abgrenzungsargument von vornherein die Grundlage. Es macht danach nämlich keinen Unterschied mehr, zu welchem Zweck die Identität des Inhabers einer Kennung hoheitlich erfragt wird, weil die Abfrage in jedem Fall in Art. 10 GG eingreift.

Gegen die Betroffenheit des Fernmeldegeheimnisses in der hier diskutieren Fallkonstellation wird weiter eingewandt, dass der fragliche **Kommunikationsvorgang dem Staat bereits bekannt** sei. Dieser Umstand ist indes unerheblich. Art. 10 GG schützt unstreitig die näheren Umstände der Telekommunikation, zu welchen auch die Information zählt, „zwischen welchen Personen oder Fernmeldeanschlüssen Fernmeldeverkehr stattgefunden hat oder versucht worden ist".[81] Wenn dem Staat einige Informationen über einen Kommunikationsvorgang bekannt sind, so schützt das Fernmeldegeheimnis gleichwohl vor der Ausforschung weiterer Umstände des Kommunikationsvorgangs. Dass Art. 10 GG vor der näheren Ausforschung eines bekannten Kommunikationsvorgangs schützt, ergibt sich auch aus dem Fangschaltungsbeschluss des Bundesverfassungsgerichts.[82] Hier hatte die Person, welche die Fangschaltung beantragt hatte, von den belästigenden Anrufen bereits Kenntnis. Gleichwohl hat das Bundesverfassungsgericht zutreffend entschieden, dass die Offenbarung des Anrufers in dessen Fernmeldegeheimnis eingriff.[83]

Nicht durchgreifend ist danach der Einwand, die Zielperson sei durch die bekannten Daten (Anschlusskennung und ggf. Verbindungszeit) **bereits unverwechselbar individualisiert**. Die zuvor bekannten Verbindungsdaten individualisieren die beteiligten Anschlussinhaber noch nicht, sondern bilden nur die notwendige Voraussetzung dafür, dass der Kommunikationsmittler eine Individualisierung des gesuchten Teilnehmers vornehmen kann.[84] Erst die Verknüpfung mit den Daten des Telekommunikationsmittlers erlaubt die Zuordnung der bekannten Verbindungsdaten zu einem bestimmten Anschlussinhaber.[85] Erst

---

[81] BVerfG, 2 BvR 1085/05 vom 17.6.2006, Abs. 4; BVerfG, 1 BvR 330/96 vom 12.03.2003, Abs. 47; BVerfGE 100, 313 (358); BVerfGE 85, 386 (396); BVerfGE 67, 157 (172).

[82] BVerfGE 85, 386 (398).

[83] BVerfGE 85, 386 (398).

[84] LG Bonn, Beschluss vom 21.05.2004, Az. 31 Qs 65/04, Abs. 17.

[85] LG Frankenthal, Beschluss vom 21.05.2008, Az. 6 O 156/08.

die begehrte Auskunft führt somit zur Individualisierung. Ohne diese Auskunft sind die zuvor bekannten Verbindungsdaten – ebenso wie zuvor bekannte Gesprächsinhalte – ein technisches und rechtliches Nullum, dem keine Aussagekraft zukommt.[86] Die Vorkenntnisse des Staates ändern nichts daran, dass mit der Auskunft über die Person des Teilnehmers die Umstände des maßgeblichen Kommunikationsvorgangs näher ausgeforscht werden.

Dass nicht ausschlaggebend sein kann, ob **Vorkenntnisse eine unverwechselbare Individualisierung ermöglichen** oder nicht, zeigt der folgende Vergleich: Würde zu einem bekannten Kommunikationsvorgang etwa die Gesprächsdauer oder gar der Kommunikationsinhalt (z.B. E-Mail) erfragt, so bestünde kein Zweifel daran, dass das Fernmeldegeheimnis vor der näheren Ausforschung des Kommunikationsvorgangs schützt – obgleich schon die Vorkenntnisse eine unverwechselbare Individualisierung des Kommunikationsvorgangs ermöglichen.

Deswegen ist auch das Argument nicht überzeugend, die Bestandsdatenauskunft habe **keinen konkreten Kommunikationsvorgang zum Gegenstand**, vielmehr sei der betreffende Kommunikationsvorgang bereits bekannt. Auch die Mitteilung der Verbindungsdauer oder des Datenvolumens zu einer bekannten Verbindung offenbart keinen neuen Kommunikationsvorgang, sondern nur nähere Umstände eines bereits bekannten Kommunikationsvorgangs. Gleichwohl sind auch bereits bekannte Verbindungen zu Recht vor näherer Ausforschung durch Befragung des Mittlers geschützt, um die Vertraulichkeit der Fernkommunikation zu gewährleisten.

Die Identität der Gesprächspartner nicht als näheren Umstand des Kommunikationsvorgangs zu behandeln, würde **Wertungswidersprüche** nach sich ziehen: Teilt etwa ein Anzeigeerstatter mit, er habe am 01.01.2009 gegen 11 Uhr einen beleidigenden Anruf erhalten, so schützt das Fernmeldegeheimnis unstreitig vor der Aufklärung, wann genau die Verbindung hergestellt und beendet wurde. Ist aber diese relativ belanglose Information vom Fernmeldegeheimnis geschützt, so wäre nicht zu vermitteln, dass die zentrale Frage, „zwischen welchen Personen oder Fernmeldeanschlüssen" die Verbindung stattfand, nicht dem Schutz des Fernmeldegeheimnisses unterliegen soll. Gleiches gilt für Internetverbindungen: Ist die relativ nichtssagende Informationen über das Datenvolumen einer Internetverbindung von Art. 10 GG geschützt, so muss erst recht dem Fernmeldegeheimnis unterliegen, wer die Verbindung hergestellt hat.

Dass die Zuordnung einer statischen Anschlusskennung zur Person des Kommunikationsteilnehmers unabhängig von konkreten Kommunikationsvorgängen **stets gleichbleibend** erfolgt, ist unerheblich für die Reichweite des Fernmeldegeheimnisses. Am Schutzzweck des Art. 10 GG gemessen ist es unerheblich, ob die näheren Umstände der Fernkommunikation von Verbindung zu Verbindung wechseln oder unverändert bleiben. Wie schon oben dargelegt, ist auch die Kennung der kommunizierenden Anschlüsse gleichbleibend und unterliegt gleichwohl, wenn sie den Teilnehmer an einem Kommunikationsvorgang kennzeichnet, unstreitig dem Fernmeldegeheimnis. Wenn die näheren Umstände eines einzelnen Kommunikationsvorgangs dem Fernmeldegeheimnis unterliegen, dann müssen es die näheren Umstände einer Vielzahl von Kommunikationsvorgängen erst Recht.

Dass die **Veränderlichkeit der näheren Kommunikationsumstände nicht maßgeblich** sein kann, zeigt auch das Beispiel von Internetverbindungen. Teilweise wird dem Kunden eine

[86] LG Frankenthal, Beschluss vom 21.05.2008, Az. 6 O 156/08.

feste Kennung (statische IP-Adresse) zugewiesen, teilweise eine von Verbindung zu Verbindung wechselnde Kennung (dynamische IP-Adresse). Auch von der Gegenansicht wird anerkannt, dass die Anwendbarkeit des Fernmeldegeheimnisses von solchen Zufälligkeiten nicht abhängen kann.

Durchschlagend ist schließlich ein letztes Beispiel: Internetnutzer können neben ihrem Internet-Zugangsanbieter einen zweiten Kommunikationsmittler einschalten („**Anonymisierungsdienst**"), der die vom Internet-Zugangsanbieter vergebene IP-Adresse durch eine andere IP-Adresse ersetzt. Anonymisierungsdienste müssen zwar protokollieren, welche IP-Adresse sie wann durch welche ersetzt haben (§ 113a Abs. 6 TKG). Sie zeichnen aber nicht auf, für welchen Kunden sie die Ersetzung vorgenommen haben. Zur Identifizierung eines Internetnutzers muss der Staat daher zunächst bei dem Anonymisierungsdienst die originäre IP-Adresse des Nutzers erfragen. Mit dieser Auskunft kann er dann von dem jeweiligen Internet-Zugangsanbieter verlangen, den Teilnehmer zu identifizieren und mitzuteilen.

Nach der Gegenansicht nun soll die **Identifizierung eines Internetnutzers** anhand einer bekannten IP-Adresse und Verbindungszeit keinen Eingriff in das Fernmeldegeheimnis darstellen. Schaltet der Internetnutzer aber einen zusätzlichen Kommunikationsmittler ein („Anonymisierungsdienst"), so soll die zur Identifizierung erforderliche Auskunft des Anonymisierungsdienstes über die originäre IP-Adresse des Nutzers in dessen Fernmeldegeheimnis eingreifen, weil Verbindungsdaten mitgeteilt würden.[87] Dieses Beispiel macht vollends deutlich, zu welchen unsinnigen Ergebnissen die Gegenansicht führt: In beiden Fällen wird ein Kommunikationsmittler in Anspruch genommen, um den Teilnehmer an einem Kommunikationsvorgang zu identifizieren. Dass die grundrechtliche Einordnung davon abhängen soll, ob ein oder zwei Kommunikationsmittler eingesetzt werden, und dass das Fernmeldegeheimnis die Identität des Teilnehmers nur bei dem zweiten, nicht aber bei dem ersten Kommunikationsmittler schützen soll, kann niemand sachlich begründen. Es ist weder interessen- noch sachgerecht und letztlich nicht nachvollziehbar, weshalb sich der Grundrechtsschutz des betroffenen Telekommunikationsteilnehmers an der Art bestimmter Daten (Verkehrs- oder Bestandsdaten) oder an der Datei, in der sie technisch gespeichert sind, orientieren soll.[88] Maßgeblich muss der Schutzzweck des Fernmeldegeheimnisses sein, der bei der Identifizierung eines Gesprächsteilnehmers einschlägig ist.

Weitere Argumente der Gegenauffassung beziehen sich nur auf Fälle, in denen der Staat den auszuforschenden Fernmeldekontakt mithilfe des Gesprächspartners oder sonst **ohne vorherigen Eingriff in Art. 10 GG** in Erfahrung gebracht hat.

Hier wird teilweise argumentiert, ein derart rückverfolgbarer Kontakt sei **von vornherein nicht auf Vertraulichkeit angelegt** gewesen. Mit der Nutzung eines derartigen Mediums begebe man sich des von Art. 10 GG gewährleisteten Schutzes der Vertraulichkeit. Dem ist zu widersprechen.[89] Ein wirksamer „Grundrechtsverzicht" kommt nur in Betracht, wenn dieser freiwillig erfolgt.[90] Von einer freiwilligen Einwilligung in die Grundrechtsbeeinträchtigung kann hier nicht gesprochen werden.[91] Die Telekommunikationsnetze sind heutzutage ein unverzichtbares Medium der Kommunikation. Um in ausreichender Weise an

---

[87] Bäcker, Die Vertraulichkeit der Internetkommunikation (2009), 14.

[88] Vgl. LG Frankenthal, Beschluss vom 21.05.2008, Az. 6 O 156/08.

[89] BVerwG, Urteil vom 22.10.2003, Az. 6 C 23.02, Abs. 21.

[90] Vgl. BVerfG, Beschluss vom 18. August 1981, Az. 2 BvR 166/ 81; Jarass/Pieroth, GG^{6}, Vorb. vor Art. 1 Rn. 36; Sachs in: ders. (Hrsg.), GG^{3}, Vor Art. 1 Rn. 56.

[91] Vgl. BVerfGE 85, 386 (398).

Kommunikationsvorgängen teilhaben und um diese veranlassen zu können, ist es notwendig, einen Vertrag mit einem Anbieter zu schließen oder sich des Endgerätes eines Dritten zu bedienen, der einen solchen Vertrag abgeschlossen hat. Deshalb kann in dem Abschluss eines Vertrags, der mit der Pflicht zur Offenbarung personenbezogener Daten verknüpft ist, oder in der Nutzung eines Mediums der Fernkommunikation kein freiwilliger Verzicht auf das durch die Datenerhebung beeinträchtigte Grundrecht gesehen werden.

Die Fernkommunikation ist **durchaus auf Vertraulichkeit angelegt**. Sie erfolgt zwar zumeist ohne Verschlüsselung und Authentifizierung der übertragenen Informationen. Dies eröffnet aber nicht jedermann, sondern nur den Kommunikationsmittlern und Kommunikationsbeteiligten Möglichkeiten der Kenntnisnahme. Dass der Schutzbereich des Art. 10 Abs. 1 Var. 3 GG auch unter diesen Umständen einschlägig ist, zeigt schon die traditionelle, analogen Sprachtelefonie, die mit Hilfe eines zwischengeschalteten Lautsprechers ohne Weiteres abhörbar ist, und zwar nicht nur für die eingesetzten Telefondienstunternehmen. Im Unterschied hierzu ist die Kenntnisnahme von digital abgewickelten Kommunikationsvorgängen erheblich schwieriger. Im Übrigen können auch verschlossene Briefe durch Einsatz von Wasserdampf zur Kenntnis genommen werden, ohne dass sie deswegen vom Schutzbereich des Briefgeheimnisses ausgenommen wären. Die Gegenansicht führte dazu, dass nur Experten, die sich professionell durch Anonymisierung und Verschlüsselung schützen können, vom Schutzbereich des Fernmeldegeheimnisses erfasst wären. Solche Experten bedürfen des Schutzes des Art. 10 GG aber am wenigsten. Das Fernmeldegeheimnis dient zuallererst dem Schutz des Normalbürgers. Dass elektronische Kommunikation unbefugt zur Kenntnis genommen werden kann, führt danach nicht zu einer Einschränkung des Schutzbereichs des Art. 10 Abs. 1 Var. 3 GG, sondern begründet umgekehrt eine besondere Schutzbedürftigkeit der Fernkommunikation. Der Schutzbereich des Fernmeldegeheimnisses ist eröffnet, wenn der Wille der Teilnehmer darauf gerichtet ist, ein regelmäßig übertragungssicheres Medium in Anspruch zu nehmen. Dies ist bei der Fernkommunikation der Fall.

Unerheblich ist weiter, wenn der auszuforschende Kontakt dem Staat **ohne Eingriff in das Fernmeldegeheimnis bekannt geworden** ist. Dieser Umstand ändert nichts daran, dass ein an den Mittler gerichtetes Identifizierungsverlangen die spezifische Verletzlichkeit der Fernkommunikation ausnutzt, um die an dem Kommunikationsvorgang Beteiligten zu identifizieren. Bei unmittelbarer Kommunikation ist eine derartige Identifikation des Kommunikationspartners typischerweise nicht möglich. In diesem Zusammenhang ist erneut auf den Fangschaltungsbeschluss des Bundesverfassungsgerichts zu verweisen: Auch hier sind die missbräuchlichen Anrufe der angerufenen Person ohne Eingriff in das Fernmeldegeheimnis bekannt geworden. Gleichwohl hat das Bundesverfassungsgericht in der Bekanntgabe der Person des Anrufers zurecht einen Eingriff in dessen Fernmeldegeheimnis gesehen.[92]

Insbesondere lässt sich nicht damit argumentieren, der Grundrechtsträger habe seine Verbindungsdaten **gegenüber dem Gesprächspartner freiwillig preisgegeben**. Erstens kann von Freiwilligkeit allenfalls im Fall der Rufnummernanzeige die Rede sein, die sich unterdrücken lässt. Nicht wirksam ist die Unterdrückung aber bereits bei Anrufen bei der Polizei oder Call Centern. Von vornherein keine zumutbare Unterdrückungsmöglichkeit besteht bei dem Versenden von E-Mails und dem Surfen im Internet. Selbst wenn der Grundrechtsträger die Rufnummernoffenlegung freiwillig aktiviert hat oder sie in Kauf nimmt, gibt er gegenüber dem Gesprächspartner nur seine Anschlusskennung preis und nicht seine

[92] BVerfGE 85, 386 (398).

Identität.[93] Gerade die Identität des Gesprächsteilnehmers will der Staat mit seiner Anfrage aber ausforschen.

Angeführt wird weiter, wenn die bekannten Verbindungsdaten ohne Eingriff in das Fernmeldegeheimnis erlangt worden seien, könne auch ihre **Verknüpfung mit Bestandsdaten** nicht in das Fernmeldegeheimnis eingreifen, denn Bestandsdaten seien ihrerseits nicht vom Schutz des Fernmeldegeheimnisses erfasst. Zu diesem Argument ist vorab anzumerken, dass schon die Prämisse unrichtig ist, Bestandsdaten seien nie vom Schutz des Fernmeldegeheimnisses erfasst. Richtigerweise greift der staatliche Zugriff auf Teilnehmerdaten bei einem Fernkommunikationsmittler immer in das Fernmeldegeheimnis ein. Selbst wenn man der Auffassung folgen wollte, dass Bestandsdaten – insbesondere die Inhaberschaft einer Kommunikationskennung – für sich genommen nicht von Art. 10 GG geschützt seien, greift der staatliche Zugriff auf Teilnehmerdaten jedenfalls in bestimmten Verwendungszusammenhängen in das Fernmeldegeheimnis ein. Die hier diskutierte Maßnahme dient der Ausforschung der Frage, zwischen welchen Personen Fernmeldeverkehr stattgefunden hat. Diese Information, die sich nur mithilfe einer Auskunft des Kommunikationsmittlers gewinnen lässt, genießt den Schutz des Fernmeldegeheimnisses. Der Staat erlangt mittelbar eine Information über einen bestimmten Kommunikationsvorgang, indem er sich die technisch zwingende Einschaltung eines Fernkommunikationsmittlers zunutze macht. Art. 10 GG ist nach seinem Schutzzweck einschlägig.

Ein weiteres Argument bezieht sich auf Fälle, in denen der Kommunikationsvorgang **freiwillig von einem der Gesprächspartner dem Staat mitgeteilt** worden ist und der Staat auf dieser Grundlage den anderen Teil identifizieren möchte. Zwar ist der Schutzbereich des Art. 10 GG ausgeschlossen, wenn ein Gesprächspartner den staatlichen Zugriff freiwillig ermöglicht.[94] Oftmals erfolgt der staatliche Zugriff aber ohne die freie Einwilligung eines Kommunikationspartners, etwa mithilfe von Informationen, die durch hoheitliche Zwangsmaßnahmen erlangt worden sind (z.B. Beschlagnahme, Zeugenvernehmung). In diesen Fällen ist Art. 10 GG einschlägig, weil der Staat nur im Fall der Fernkommunikation ohne Kenntnis beider Gesprächspartner (z.B. aufgrund einer Beschlagnahme) oder nach Einsatz von Zwangsmaßnahmen (z.B. Zeugenvernehmung) heimlich bei dem notwendig zwischengeschalteten Dritten anfragen kann, um die Kommunikationsbeziehung auszuforschen. Selbst wenn tatsächlich die freie Einwilligung eines Kommunikationspartners vorliegt (z.B. Anzeigeerstatter), schließt sie den Anwendungsbereich des Fernmeldegeheimnisses nur insoweit aus, wie der Kommunikationspartner auf dem technisch dafür vorgesehenen Weg Zugriff auf die Kommunikation nehmen kann.[95] Ein solcher Zugriff des Kommunikationspartners auf Bestandsdaten besteht nicht. Der Kommunikationspartner hat keinen Zugriff auf Vertragsdaten, die der Kommunikationsmittler für den anderen Kommunikationspartner vorhält. Der Kommunikationspartner kann daher nicht in ihre Erhebung einwilligen. Ein Fernsprechteilnehmer kann nicht auf die Wahrung des Fernmeldegeheimnisses seines Kommunikationspartners verzichten.[96]

Der Bevollmächtigte der Bundesregierung führt weiter die Entscheidung des Hohen Gerichts an, wonach die Ausforschung von Kommunikationsvorgängen etwa durch **Beschlagnahme von Mobiltelefonen** nicht in Art. 10 GG eingreife. In der Tat hat der Erste Senat dazu entschieden, der Grundrechtsschutz des Art. 10 Abs. 1 GG erstrecke sich nicht auf die nach

---

[93] OLG Wien, Beschluss vom 28.02.2005, Az. 20 Bs 27/05z.

[94] BVerfG, Urteil vom 27.2.2008, Az. 1 BvR 370/07 , Abs. 291.

[95] Vgl. BVerfGE 85, 386 (398); Bäcker, Die Vertraulichkeit der Internetkommunikation (2009), 9.

[96] BVerfGE 85, 386 (399).

Abschluss eines Kommunikationsvorgangs im Herrschaftsbereich eines Kommunikationsteilnehmers gespeicherten Inhalte und Umstände der Telekommunikation, soweit dieser eigene Schutzvorkehrungen gegen den heimlichen Datenzugriff treffen kann.[97] Art. 10 GG soll die Gesprächsteilnehmer nicht besser stellen als sie bei unmittelbarer Kommunikation miteinander stünden. Auch bei unmittelbarer Kommunikation kann der Gesprächspartner während des Gesprächs oder danach Aufzeichnungen oder Notizen vornehmen. Deswegen ist die bewusste Aufzeichnung solcher Daten durch den Gesprächspartner oder durch dessen Endeinrichtung kein Spezifikum von Fernkommunikation. Ein Spezifikum von Fernkommunikation ist demgegenüber, dass der Kommunikationsmittler dem Gesprächspartner regelmäßig ohne den Willen des Teilnehmers eine Anschlusskennung (z.B. IP-Adresse) übermittelt und Informationen vorhält, die eine Identifizierung des Teilnehmers ermöglichen. Deswegen ist die Auswertung von Aufzeichnungen des Gesprächspartners nicht vergleichbar mit der Anfrage bei einem Kommunikationsmittler.

Gleiches gilt für eine weitere vom Bevollmächtigten der Bundesregierung angeführte Entscheidung der 1. Kammer des Zweiten Senats. Danach soll das Fernmeldegeheimnis nicht vor der Erhebung von Kartennummer, Gerätenummer und Standort einer empfangsbereiten Fernkommunikationseinrichtung (Mobiltelefon) durch Einschaltung in den Übertragungsweg schützen (sog. „**IMSI-Catcher**"). Aus dieser Entscheidung will der Bevollmächtigte der Bundesregierung den allgemeinen Grundsatz herleiten, dass unabhängig von einem konkreten Kommunikationsvorgang anfallende Daten nicht von Art. 10 GG geschützt seien.

Die Entscheidung ist hier aus zwei Gründen **nicht einschlägig**: Erstens betrifft sie nicht die Inanspruchnahme des Kommunikationsmittlers, wie sie im Fall der Bestandsdaten in Rede steht.[98] Zweitens stellt auch jene Entscheidung nicht in Abrede, dass das Fernmeldegeheimnis die näheren Umstände einzelner Kommunikationsvorgänge schützt. Gerade um einen solchen Umstand geht es hier, wenn die Beteiligten an einem konkreten Kommunikationsvorgang identifiziert werden sollen.

4.4 Identifizierung eines Anschlussinhabers als Eingriff in Art. 10 GG

Wem eine Anschlusskennung (z.B. Rufnummer, E-Mail-Adresse, IP-Adresse) zugewiesen war, unterliegt somit dem Schutz des Fernmeldegeheimnisses zumindest dann, wenn die Auskunft der Ermittlung des Beteiligten an einem konkreten Kommunikationsvorgang dient. Denn das Fernmeldegeheimnis schützt unstreitig die Information, zwischen welchen Personen oder Fernmeldeanschlüssen Fernmeldeverkehr stattgefunden hat.

Wer über welche Kennung kommuniziert(e), unterliegt dem Schutz des Fernmeldegeheimnisses **aber auch in anderen Fällen**.

Die §§ 112, 113 TKG ermächtigen etwa zu den folgenden Anfragen und schränken dadurch das Fernmeldegeheimnis ein:

- Wer war am 01.01.2009 **Inhaber** der Rufnummer 072191010?
- Welche **E-Mail-Adresse** nutzt X gegenwärtig?

---

[97] BVerfG, Urteil vom 27.2.2008, Az. 1 BvR 370/07 , Abs. 185.

[98] Dix, Schriftsatz vom 29.01.2007 in diesem Verfahren, 6.

Diese Anfragen dienen zwar (noch) nicht notwendig der Ermittlung, ob, wann und wie oft zwischen welchen Personen oder Fernmeldeanschlüssen Fernmeldeverkehr stattgefunden hat. Sie **gefährden gleichwohl die Vertraulichkeit** und Unbefangenheit des Fernmeldeverkehrs, weil sie die Anonymität und Vertraulichkeit der zur Fernkommunikation erforderlichen Anschlusskennung aufheben und die Ausforschung der Fernkommunikation einer bestimmten Person ermöglichen.

Art. 10 GG bezweckt, die Kommunizierenden vor den spezifischen Gefahren der Fernkommunikation zu schützen. Im Vergleich zur unmittelbaren Kommunikation resultierten bei der Fernkommunikation spezifische Vertraulichkeitsgefahren aus der eingesetzten Technik.[99] Die Kommunizierenden sollen durch die Bedingungen der Fernkommunikation nicht schlechter gestellt werden als sie bei unmittelbarer Kommunikation stünden.[100] Bei unmittelbarer Kommunikation wären die Kommunizierenden nicht auf die Verwendung und Offenbarung eines Adressierungsmerkmals angewiesen, das einen eindeutigen Rückschluss auf ihre Person zulässt. Die Notwendigkeit eines personenbezogenen Adressierungsmerkmals ist der Fernkommunikation eigen und findet in der direkten Kommunikation keine Entsprechung. In dem heimlichen staatlichen Zugriff auf die Inhaberschaft einer Kommunikationskennung, die dem Kommunikationsmittler aus betrieblichen Gründen bekannt sein muss, realisiert sich daher die spezifische Gefahr der Fernkommunikation im Vergleich zur unmittelbaren Kommunikation.

Gegenstand des Fernmeldegeheimnisses ist es, vor den **spezifischen Nachteilen der Fernkommunikation** gegenüber direkter Kommunikation zu schützen. Ein spezifischer Nachteil der Fernkommunikation liegt darin, dass der Beteiligte an einer Fernkommunikation über eine eindeutige Fernmeldekennung des Kommunikationspartners verfügen muss (z.B. Rufnummer, E-Mail-Adresse, IP-Adresse). Diese Kennung wird auch bei ausgehenden Kommunikationen oft unfreiwillig offenbart (z.B. E-Mail-Adresse, IP-Adresse). Wo im direkten Kontakt unfreiwillig nur das (anonyme) Gesicht offenbart wird, wird im Fernkontakt eine eindeutige, personenbezogene Kennung offengelegt, die automatisiert gespeichert und ausgewertet werden kann und die sich jederzeit eindeutig der Person des Anschlussinhabers zuordnen lässt. Das technische Erfordernis einer eindeutigen Kommunikationskennung begründet daher eine spezifische Gefährdung der Anonymität der Fernkommunikation, wie sie das Fernmeldegeheimnis gewährleistet.

Zweck des Fernmeldegeheimnisses ist es, eine **freie und unbefangene Telekommunikation** zu gewährleisten.[101] Das Grundrecht soll die Bedingungen einer freien Telekommunikation aufrechterhalten.[102] Es soll verhindern, dass der Meinungs- und Informationsaustausch mittels Telekommunikationsanlagen deswegen unterbleibt oder nach Form und Inhalt verändert verläuft, weil die Beteiligten damit rechnen müssen, dass staatliche Stellen Kenntnisse über die Kommunikationsbeziehungen oder Kommunikationsinhalte gewinnen.[103] Gerade die fehlende Anonymität der Fernkommunikation wegen der technisch bedingten Verwendung eindeutiger Kennungen beeinträchtigt die Bereitschaft zur vertraulichen Kommunikation auf elektronischem Wege. Auch wenn der Staat das Pseudonym einer Kommunikationskennung nicht zur Ausforschung eines konkreten Kommunikationsvorgangs aufhebt, kann er die erhobene Information doch fortan jederzeit genau zu diesem Zweck nutzen. Bei dem Staat eingehende oder ihm zugetragene Kommunikationen können nun ohne Mitwirkung des

---

[99] BVerfGE 85, 386 (396); BVerfG, Beschluss vom 09.10.2002, Az. 1 BvR 1611/96, Abs. 20.

[100] BVerfG, Beschluss vom 12.3.2003, Az. 1 BvR 330/96, Abs. 48.

[101] BVerfG, Beschluss vom 27.7.2005, Az. 1 BvR 668/04, Abs. 81.

[102] BVerfG, Beschluss vom 12.3.2003, Az. 1 BvR 330/96, Abs. 47; Urteil vom 14.07.1999, Az. 1 BvR 2226/94, Abs. 162.

[103] BVerfGE 100, 313 (359); BVerfG, Beschluss vom 12.3.2003, Az. 1 BvR 330/96, Abs. 47.

Kommunikationsmittlers der Person des Anschlussinhabers zugeordnet werden. Die Anonymität der Kommunikationskennung ist aufgehoben. Eine freie, unbefangene in allem vertrauliche Fernkommunikation, die in bestimmten menschlichen Situationen auch anonym möglich sein muss, ist nicht mehr möglich. Eine jederzeit identifizierbare Kommunikation droht nach Art und Inhalt verändert zu verlaufen oder zu unterbleiben. Deswegen muss das Fernmeldegeheimnis gewährleisten, dass vertraulich bleibt, wer unter welcher Kennung kommuniziert.

Zwanglos ergibt sich die Anwendbarkeit des Fernmeldegeheimnisses, wenn man der Auffassung folgt, dass eine **Kommunikationskennung stets ein Verbindungsdatum** sei, weil sie nicht von dem Teilnehmer erhoben (§ 3 Nr. 3 TKG), sondern von dem Anbieter – als Bestandteil seines Kommunikationsdienstes – zugeteilt werde (§ 3 Nr. 30 TKG).[104] § 96 Abs. 1 Nr. 1 TKG bezeichnet „die Nummer oder Kennung der beteiligten Anschlüsse oder der Endeinrichtung" ausdrücklich als „Verkehrsdaten". Die Kommunikationskennung betrifft nicht die Person des Teilnehmers, sondern ermöglicht ein- und ausgehende Verbindungen. § 3 Nr. 30 TKG definiert „Verkehrsdaten" als „Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden". Die Zuweisung einer Kommunikationskennung und die Vorhaltung eines Anschlusses durch den Anbieter ist notwendiger Bestandteil des Kommunikationsdienstes. Die Kommunikationskennung wird daher bei der Erbringung des Telekommunikationsdienstes gespeichert und ist Verkehrsdatum.

In seiner **Entscheidung zur Computerdurchsuchung** hat das Hohe Gericht anerkannt, dass Schutzlücken entstünden, würden die Grundrechte erst vor dem Zugriff auf und nicht schon vor der vorgelagerten Infiltration eines informationstechnischen Systems schützen.[105] Es hat einen Eingriff in das Persönlichkeitsrecht bereits dann angenommen, wenn „die entscheidende technische Hürde für eine Ausspähung (...) des Systems genommen" ist.[106] Was für die Ausspähung eines informationstechnischen Systems gilt, muss auch für die Ausspähung einer fernkommunizierenden Person gelten: Mit Aufdeckung der Zuordnung einer Kommunikationskennung zur Person ihres Nutzers ist „die entscheidende technische Hürde für eine Ausspähung" der Fernkommunikation dieses Nutzers genommen. Mithilfe dieser Zuordnungsfunktion kann der Staat nämlich Verbindungen des Nutzers, der seine Kennung technisch bedingt gegenüber seinen Kommunikationspartnern offen legen muss (z.B. E-Mail-Adresse, IP-Adresse, eingeschränkt auch Rufnummer), identifizieren und diesem zuordnen.

Grundrechtsträger haben ein **berechtigtes Interesse** daran, dass nicht im Telefonbuch veröffentlichte Privatnummern, private E-Mail-Adressen und private Internetkennungen geheim gehalten werden. Man denke nur an die Telefonnummern von Prominenten. Es ist überdies auch möglich, eine Fernkommunikation als von einer fremden Kennung ausgehend erscheinen zu lassen (z.B. gefälschte SMS-Absendernummer, gefälschte E-Mail-Absenderadresse, IP-Spoofing). Auch aus dieser Missbrauchsgefahr ergibt sich eine legitime Geheimhaltungserwartung. Wenn der Bevollmächtigte der Bundesregierung die eigene Telefonnummer als „Basisdatum" zu verharmlosen sucht, so verkennt er, dass eine Pflicht zur Angabe einer Telefonnummer etwa im Melderegister aus gutem Grund nicht besteht. Dass der Vergleich der Rufnummer mit einer Postanschrift oder einem Kfz-Kennzeichen nicht trägt, ist bereits ausführlich dargelegt worden.[107]

---

[104] Riechert, Neue Online-Dienste und Datenschutz (2006), 168 ff.; Bizer, DuD 2007, 602 (602).

[105] BVerfG, Urteil vom 27.2.2008, Az. 1 BvR 370/07 , Abs. 181.

[106] BVerfG, Urteil vom 27.2.2008, Az. 1 BvR 370/07 , Abs. 205.

[107] Schriftsatz vom 23.03.2007, 21 f.

Die Behauptung, die Inhaberschaft einer Kommunikationskennung sei **wenig aussagekräftig** und nicht mit Informationen über Inhalt und Umstände konkreter Kommunikationsvorgänge vergleichbar, ist sowohl falsch wie auch unerheblich. Falsch ist diese Darstellung, weil sie die Sensibilität der Information aus ihrer Art heraus beurteilen will, obwohl tatsächlich ihre Nutzbarkeit und Verwendbarkeit entscheidet.[108] Dass die Inhaberschaft einer Kommunikationskennung zur Aufhebung der Pseudonymität einzelner Kommunikationsvorgänge oder gar der gesamten Fernkommunikation genutzt werden kann, ist bereits ausgeführt worden. Im Übrigen ist die Schutzwürdigkeit der Information ohne Bedeutung für die Bestimmung des Schutzbereichs des Fernmeldegeheimnisses. Die Schutzwürdigkeit ist dogmatisch erst im Rahmen der Rechtfertigung eines Grundrechtseingriffs zu prüfen und nicht bei der Bestimmung des Schutzbereichs.

Die Gegenauffassung meint, im **Vergleich zum eigentlichen Kommunikationsvorgang** verdiene das zugrunde liegende Vertragsverhältnis nicht den gleichen Schutz. Oben ist jedoch bereits erläutert worden, dass die Identität eines Kommunikationsteilnehmers in der Regel sehr viel bedeutsamer ist als der (genaue) Inhalt oder einzelne Umstände (z.B. Verbindungsdauer, Datenvolumen) einer Kommunikation. Die Identität eines Kommunikationsteilnehmers ist also keineswegs weniger schutzwürdig als Inhalt und sonstige Umstände eines Kommunikationsvorgangs. Auch wenn der Staat die Inhaberschaft einer Kommunikationskennung unabhängig von einem konkreten Kommunikationsvorgang erhebt, ermöglicht die Information jederzeit die (künftige) Zuordnung der Kommunikation des Betroffenen. Deshalb ist die Inhaberschaft einer Kommunikationskennung ebenso schützenswert wie die einzelnen Kommunikationsvorgänge, die sich mit ihrer Hilfe zuordnen lassen.

Zugegebenermaßen ist die Einbeziehung der Identität eines Teilnehmers in den Schutzbereich des Fernmeldegeheimnisses zwingender, wenn ihre Aufdeckung der Ausforschung eines konkreten Kommunikationsvorgangs dient. Da der Kommunikationsmittler aber **oft nicht erkennen kann**, welchem Zweck ein Auskunftersuchen dient, muss das Fernmeldegeheimnis im Sinne der Effektivität umfassend die Information schützen, wer über welche Kennung kommuniziert. Eine Unterscheidung nach dem Zweck eines Eingriffs wäre zwar möglich, schaffte aber freiheitsgefährdende Abgrenzungsprobleme und Umgehungsgefahren. Zudem wäre die Möglichkeit einer nachträglichen Zweckänderung der einmal erhobenen Daten in Betracht zu ziehen und zu regeln. Insgesamt ist es einfacher und schützt die Grundrechtsträger wirksamer, die Identität eines Anschlussinhabers stets in den Schutzbereich des Fernmeldegeheimnisses einzubeziehen.

Dass der Rufnummerninhaberschaft **per se kein Bezug zu einem bestimmten Kommunikationsvorgang** inne wohnt und sie für sich genommen keine Rückschlüsse auf konkrete Kommunikationsvorgänge zulässt, ist am Schutzzweck des Fernmeldegeheimnisses gemessen unerheblich. Entscheidend ist, dass der Staat die notwendige Einschaltung eines Kommunikationsmittlers ausnutzt, um die einen Kommunikationsteilnehmer jederzeit identifizierbar zu machen.

Die Gegenauffassung beruft sich auf die Kammerentscheidung des Bundesverfassungsgerichts zum **IMSI-Catcher**, wonach das Fernmeldegeheimnis die zur Gewährleistung der Empfangsbereitschaft eines Mobiltelefons erforderlichen Daten nicht

[108] BVerfGE 65, 1 (45).

schützen soll.[109] Wenn das Fernmeldegeheimnis schon Informationen über eine empfangsbereites Endgerät nicht schütze, obgleich die Empfangsbereitschaft notwendige Voraussetzung eines Telekommunikationsvorgangs sei, so müsse gleiches für die notwendige Inhaberschaft einer Kommunikationskennung gelten, welche ebenfalls Voraussetzung für einzelne Telekommunikationsverbindungen sei.

Dieser Argumentation ist zunächst entgegen zu halten, dass das vorliegende Problem **anders liegt** als das technische Abfangen von Kennungen und Standorten. Denn nur die Identifizierung des Inhabers einer Kommunikationskennung erfolgt durch Inanspruchnahme des – notwendig eingeschalteten – Kommunikationsmittlers. Der genannten Kammerentscheidung lag keine Inanspruchnahme eines Kommunikationsmittlers zugrunde.

Wenn man sich dennoch auf den Vergleich einlassen wollte, so kann der **Kammerentscheidung inhaltlich nicht gefolgt** werden. Die Kammerentscheidung zum IMSI-Catcher, die bewusst von der ganz herrschenden Meinung einschließlich der Rechtsprechung des Bundesgerichtshofs abgewichen ist,[110] ist unzutreffend und vereinzelt geblieben. Der Erste Senat hat sich ihr zu Recht nicht angeschlossen.

Der vom Fernmeldegeheimnis geschützte **Fernmeldeverkehr ist im weitesten Sinne zu verstehen**. Es gibt keinen Anlass, den grundrechtlichen Telekommunikationsbegriff enger zu fassen als den einfachgesetzlichen. Nach § 3 Nrn. 22 und 23 TKG ist Telekommunikation der technische Vorgang des Aussendens, Übermittelns und Empfangens von Nachrichten jeglicher Art in der Form von Zeichen, Sprache, Bildern oder Tönen mittels technischer Einrichtungen oder Systemen, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können. Auch die Meldung der Empfangsbereitschaft durch das Mobiltelefon an die Empfangsstation und dann weiter an den Zentralrechner der Telefongesellschaft ist ein Vorgang, bei dem Zeichen – nämlich Daten – übertragen werden. Es handelt sich um eine Datenfernübertragung, also um Telekommunikation.[111]

Das Bundesverfassungsgericht bezieht in den Schutzbereich von Art. 10 Abs. 1 Var. 3 GG ausdrücklich die Information ein, ob und wann zwischen Fernmeldeanschlüssen **Fernmeldeverkehr versucht worden ist**.[112] Nicht anders kann die Information der Empfangsbereitschaft und des Standortes eines Mobiltelefons zu behandeln sein, die dem Mittler vorliegen muss, um Fernmeldeverkehr mittels des Apparats zu ermöglichen. Unstreitig schützt das Fernmeldegeheimnis sowohl Sender als auch Empfänger einer Meldung.[113] Es kann daher keinen Unterschied machen, ob jemand – der Formel des Bundesverfassungsgerichts entsprechend – versucht, Daten zu senden, oder ob jemand mit einem empfangsbereiten Mobiltelefon versucht, Daten zu empfangen. Darüber hinaus ist die Meldung von Empfangsbereitschaft und Funkzelle durch das Mobiltelefon – wie ausgeführt – auch für das aktive Senden von Daten, etwa das Anrufen anderer Anschlüsse, Vorbedingung.

---

[109] BVerfG, Beschluss vom 22.08.2006, Az. 2 BvR 1345/03.

[110] BVerfG, Beschluss vom 22.08.2006, Az. 2 BvR 1345/03, Abs. 59.

[111] Friedrich, Die Verpflichtung privater Telekommunikationsunternehmen, die staatliche Überwachung und Aufzeichnung der Telekommunikation zu ermöglichen (2001), 138.

[112] BVerfG seit E 67, 157 (172).

[113] AK-GG-Bizer, Art. 10, Rn. 48; Dreier-Hermes, Art. 10, Rn. 23: alle an dem fernmeldetechnisch vermittelten Kommunikationsvorgang Beteiligten; J/P[6]-Jarass, Art. 10, Rn. 10.

Diese Sichtweise entspricht auch der **Auffassung des Gesetzgebers**, der die „Kennung (...) der Endeinrichtung", die „Kartennummer" und „Standortdaten" als Verkehrsdaten einordnet (§ 96 Abs. 2 Nr. 1 TKG). § 3 Nr. 30 TKG definiert „Verkehrsdaten" als „Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden". Die Speicherung von Gerätenummer, Kartennummer, und Standort durch den Diensteanbieter ist notwendiger Bestandteil des Kommunikationsdienstes, zu dem die Ermöglichung ein- und ausgehender Verbindungen gehört. Die genannten Daten werden daher bei der Erbringung des Telekommunikationsdienstes erhoben und sind Verkehrsdaten. Dass Verkehrsdaten den Schutz des Fernmeldegeheimnisses genießen, ist unstreitig.

Teleologisch ist zu beachten, dass **im Fall der unmittelbaren Kommunikation** keine Standortdaten anfallen, dass der Schutzzweck des Fernmeldegeheimnisses also einschlägig ist. Art. 10 Abs. 1 Var. 3 GG schützt somit auch die Angabe, dass und wo ein Mobiltelefon empfangsbereit ist, welche SIM-Karte in das Telefon eingesteckt ist (IMSI) und um welches Mobiltelefon es sich handelt (IMEI).[114] Ein Widerspruch zur Einbeziehung der Rufnummerninhaberschaft in den Schutzbereich des Fernmeldegeheimnisses besteht mithin nicht.

Die Gegenauffassung wendet ein, aus der Inhaberschaft einer Kommunikationskennung könne lediglich geschlossen werden, **dass jemand die Möglichkeit habe**, in konkrete Kommunikationsvorgänge einzutreten. Dies erschöpft die Nutzbarkeit der Information jedoch nicht. Denn sie kann dazu verwendet werden, Kommunikationsinhalte und -umstände der Person der Kommunizierenden zuzuordnen. Auf diese Weise ermöglicht sie Rückschlüsse auf das Kommunikationsverhalten, auf Kommunikationsbeziehungen und auf Kommunikationsinhalte bestimmter Personen.

Das weitere Gegenargument, die Information lasse sich **auch auf andere Weise** (z.B. Zeugenaussagen, Beschlagnahme eines Adressbuchs) gewinnen, ist bereits entkräftet worden.[115] Denn auch Kommunikationsinhalte und –umstände können sich auf andere Weise gewinnen lassen. Nichtsdestotrotz schützt das Fernmeldegeheimnis davor, dass diese Informationen gerade durch Zugriff auf den Kommunikationsmittler erhoben werden, wovor sich die an einer Fernkommunikation Beteiligten nicht schützen können.

Gegen die Einbeziehung der Identität des Inhabers einer Kommunikationskennung in das Fernmeldegeheimnis wird schließlich eingewandt, dadurch würde der **Schutzbereich des Art. 10 GG ausufern** und würden seine Maßstäbe entwertet. Diese Befürchtung trifft nicht zu. Der Schutzbereich des Art. 10 GG bleibt klar abgegrenzt: Er schützt vor den spezifischen Gefahren der Fernkommunikation gegenüber direkter Kommunikation. Es ist unmittelbar einleuchtend, dass es im Fall direkter Kommunikation nicht möglich wäre, bei einem Mittler zu erfragen, wer unter welcher Kennung Gespräche führt. Bei direkter Kommunikation gibt es weder Mittler noch Kennungen. Das Fernmeldegeheimnis ufert daher nicht aus. Umgekehrt ufert das Grundrecht auf informationelle Selbstbestimmung aus, wenn ihm zugeschlagen würde, was thematisch eindeutig den Fernmeldeverkehr und damit Art. 10 GG betrifft. Die Gegenauffassung entleert Art. 10 GG entgegen seinem Wortlaut.

---

[114] So auch Schenke, AöR 125 (2000), 5 und 20 f.; AK-GG-Bizer, Art. 10, Rn. 66; Friedrich, Friedrich, Die Verpflichtung privater Telekommunikationsunternehmen, die staatliche Überwachung und Aufzeichnung der Telekommunikation zu ermöglichen (2001), 140; Landesbeauftragte für den Datenschutz der Länder Nordrhein-Westfalen, Berlin, Brandenburg, Sachsen-Anhalt und Schleswig-Holstein, zitiert bei ULD-SH, www.datenschutzzentrum.de/material/themen/divers/imsicat.

[115] Seite 8.

Auch werden die **Maßstäbe des Fernmeldegeheimnisses nicht entwertet**: Erstens ist richtigerweise für ein einheitliches, hohes Schutzniveau für alle Kommunikationsinhalte und -daten zu plädieren und bereits plädiert worden.[116] Selbst wenn man die Inhaberschaft einer Rufnummer für weniger schutzwürdig hielte, wäre es problemlos möglich, für solche Grundrechtseingriffe eigene Maßstäbe zu entwickeln, wie es im Übrigen auch im Rahmen des Rechts auf informationelle Selbstbestimmung nötig wäre. Schon heute wird Art. 10 GG ein unterschiedliches Schutzniveau von Kommunikationsinhalten und -umständen entnommen. Würde ein weiteres Schutzniveau für die zugrunde liegenden Vertragsdaten geschaffen, wäre dies nichts Neues.

4.5 Zugriff auf Kommunikationsdaten als genereller Eingriff in Art. 10 GG

Auch ohne Bezug zu einem konkreten Telekommunikationsvorgang und der Identität von Fernmeldeteilnehmern sind dem Kommunikationsmittler zum Zweck der Kommunikationsvermittlung anvertraute Informationen (Bestandsdaten) allgemein vom Fernmeldegeheimnis geschützt.

§ 113 TKG ermächtigt etwa zu den folgenden Anfragen und schränkt dadurch das Fernmeldegeheimnis ein:

- Welche Adressen sind im **elektronischen Adressbuch** des E-Mail-Kontos bverfg@bundesverfassungsgericht.de verzeichnet?
- **Welche Rufnummern** hat der Inhaber des Anschlusses 072191010 angegeben, um im günstigen „Family and Friends"-Tarif zu telefonieren?

Art. 10 GG bezweckt, die Kommunizierenden vor den spezifischen Gefahren der Fernkommunikation zu schützen. Im Vergleich zur unmittelbaren Kommunikation resultieren bei der Fernkommunikation spezifische Vertraulichkeitsgefahren aus dem eingesetzten Übertragungsweg und aus der Einschaltung eines Kommunikationsmittlers.[117] Die Kommunizierenden sollen durch die notwendige Einschaltung des Mittelsmannes nicht schlechter gestellt werden als sie bei unmittelbarer Kommunikation stünden.[118] Bei unmittelbarer Kommunikation wären die Kommunizierenden nicht auf einen Vertrag über Telekommunikationsdienstleistungen angewiesen, zu dessen Abwicklung Informationen über die Gesprächsteilnehmer festgehalten werden müssen. In dem heimlichen staatlichen Zugriff auf Informationen, die ein Kommunikationsmittler aus betrieblichen Gründen über Kommunizierende vorhält, realisiert sich daher die spezifische Gefahr einer Fernkommunikation im Vergleich zur unmittelbaren Kommunikation.

Zweck des Fernmeldegeheimnisses ist es, eine **freie und unbefangene Telekommunikation** zu gewährleisten.[119] Das Grundrecht soll die Bedingungen einer freien Telekommunikation aufrechterhalten.[120] Wären Vertragsdaten nicht vom Fernmeldegeheimnis geschützt, würde sich dies abschreckend auf die Bereitschaft zu freier und unbefangener Fernkommunikation auswirken. Form und Inhalt einzelner Kommunikationsvorgänge drohten verändert zu verlaufen. Bereits die Kenntnis der Tatsache, dass ein Bürger ein vertragliches Verhältnis mit einem bestimmten Diensteanbieter begründet hat und wie dieses ausgestaltet ist, kann zu unerwünschten Kommunikationsanpassungen seitens des Einzelnen führen.

---

116 Beschwerdeschrift, 79 ff.

117 BVerfGE 85, 386 (396); BVerfG, Beschluss vom 09.10.2002, Az. 1 BvR 1611/96, Abs. 20.

118 BVerfG, Beschluss vom 12.3.2003, Az. 1 BvR 330/96, Abs. 48.

119 BVerfG, Beschluss vom 27.7.2005, Az. 1 BvR 668/04, Abs. 81.

120 BVerfG, Beschluss vom 12.3.2003, Az. 1 BvR 330/96, Abs. 47; Urteil vom 14.07.1999, Az. 1 BvR 2226/94, Abs. 162.

Wer beispielsweise an der Teilnahme an einem **Internet-Chat für Muslime** in Deutschland interessiert ist, wird es in Erinnerung an Maßnahmen der „Anti-Terror-Rasterfahndung" mit anschließender Befragung der „Ausgefilterten" möglicherweise vorziehen, auf die Ausübung seiner Grundrechte (hier unter anderem der Religionsfreiheit) zu verzichten. Solche Chats sind regelmäßig anmeldepflichtig, so dass der Teilnehmerkreis durch eine Bestandsdatenauskunft in Erfahrung gebracht werden kann. Dasselbe kann etwa für die Anmeldung zur Teilnahme an einem Meinungsforum gelten, in dem Protestaktivitäten gegen die Atomkraft diskutiert werden (Meinungsfreiheit, Versammlungsfreiheit). Auch die Mitgliedschaft in sonstigen geschlossenen Netzen, bereitgestellt etwa von einer Aids-Selbsthilfegruppe oder einer Eheberatung, kann Rückschlüsse auf bestimmte Problemlagen erlauben.[121] Dasselbe gilt bereits für Standard-Telekommunikationsdienste.[122] Wer beispielsweise einen Internetzugang zum Pauschaltarif nutzt, wird von den Behörden als intensiver Internetnutzer angesehen werden. Wer bei der deutschen Telefongesellschaft „Alo Vatan" angemeldet ist, wird im Zweifel einen Bezug zu der Türkei aufweisen. Wer einen bestimmten Optionstarif im Mobilfunknetz nutzt, bei dem man fünf Festnetzanschlüsse vom Handy aus besonders preisgünstig erreichen kann (wird etwa von der Firma Eplus angeboten), gibt schon mit diesen Bestandsdaten preis, mit wem er oft telefoniert. Wer eine Partnerkarte nutzt, die unentgeltliche Gespräche zu einem anderen Anschluss ermöglicht, wird regelmäßig in einer partnerschaftlich oder sonst engen Beziehung zu dem anderen Anschlussinhaber stehen. Wer das elektronische Adressbuch seines Online-E-Mail-Dienstes nutzt, offenbart ebenfalls schon seine Kommunikationsbeziehungen, ohne die Kontrolle über sein Telefonbuch zu behalten. – Die genannten Beispiele zeigen, dass Bestandsdaten nicht nur besonders sensibel sein können, sondern auch weit gehende Rückschlüsse auf Inhalt und Umstände der Fernkommunikation einer Person erlauben können.

Dass die Erhebung von Bestandsdaten **am wenigsten eingriffsintensiv** sei,[123] ist danach sowohl unzutreffend als auch unerheblich. Dass für die Schwere eines informationellen Grundrechtseingriffs nicht allein auf die Art eines Datums abgestellt werden kann, sondern dessen Nutzbarkeit und Verwendbarkeit für die erhebende Stelle entscheidend ist, ist seit dem Volkszählungsurteil anerkannt.[124] Es gibt keine von vornherein „belanglosen" oder „belangloseren" Daten, weil je nach Erhebungszweck und Nutzbarkeit auch ein „für sich gesehen belangloses Datum einen neuen Stellenwert bekommen" kann.[125] Man denke daran, dass der Staat von einer Aidshilfestelle Auskunft über deren Kundendaten verlangt. Bei isolierter Betrachtung wird zwar nur eine Namens- und Adressliste übermittelt, aber niemand wird in Abrede stellen können, dass die mitgeteilten Personendaten wegen ihrer Auswahl hochbrisant sind. Im Übrigen ist dem Argument der Eingriffsintensität entgegen zu halten, dass das Gewicht des Grundrechtseingriffs dogmatisch nur im Rahmen der Rechtfertigung von Grundrechseingriffen eine Rolle spielen kann, nicht aber bei der Bestimmung des Schutzbereichs eines Grundrechts. Der Schutzbereich ist nach dem Schutzzweck des Grundrechts zu bestimmen, der hier einschlägig ist.

Die Einbeziehung von Bestandsdaten in das Fernmeldegeheimnis hat danach eine **dienende Funktion**: Nur, wenn die Anmeldung und Unterhaltung eines Telekommunikationszugangs oder -kontos in allem vertraulich möglich ist, kann darüber auch frei und unbefangen kommuniziert werden.

---

121 DSB-Konferenz vom 14./15.03.2000, www.bfd.bund.de/information/info5/anl/an06.html.

122 Vgl. ULD-SH, Sichere Informationsgesellschaft, www.datenschutzzentrum.de/material/themen/cybercri/cyberkon.htm, Punkt 7c.

123 öOGH, Beschluss vom 26.07.2005, Az. 11 Os 57/05z u.a., 10.

124 BVerfGE 65, 1 (45).

125 Vgl. BVerfGE 65, 1 (45).

Die Einbeziehung von Bestandsdaten in den Schutzbereich des Art. 10 GG ist auch **systematisch** zweckmäßig, weil das Fernmeldegeheimnis das thematisch einschlägige Grundrecht ist und die seit Jahren in Rechtsprechung, Literatur und Rechtsanwendung schwelenden Abgrenzungsschwierigkeiten und -streitigkeiten zum Recht auf informationelle Selbstbestimmung überzeugend überwunden werden. Sämtliche Daten, die einem Kommunikationsmittler in seiner Eigenschaft als solchem bekannt geworden sind, sind richtigerweise vom Fernmeldegeheimnis geschützt.

Die **historische Betrachtung** der Rechtsprechung zum Fernmeldegeheimnis ergibt, dass sich das Bundesverfassungsgericht zur Einbeziehung des Vertragsverhältnisses in den Schutzbereich des Grundrechts noch nicht eindeutig geäußert hat. Im grundlegenden G10-Beschluss aus dem Jahr 1984 heißt es, das Grundrecht umfasse „auch die näheren Umstände des Fernmeldeverhältnisses." Dazu gehöre „insbesondere die Tatsache, ob und wann zwischen welchen Personen und Fernmeldeanschlüssen Fernmeldeverkehr stattgefunden hat oder versucht worden ist".[126] Mit dem Wort „insbesondere" ist deutlich gemacht, dass die letztgenannte Definition nicht abschließend sein sollte. Auch Vertragsdaten betreffen die „näheren Umstände des Fernmeldeverhältnisses".[127]

Dabei muss auch die **technische Entwicklung** seit dem Jahre 1984 bedacht werden: Damals existierten keine Verbindungsdaten, die in Verknüpfung mit einer Bestandsdatenauskunft Rückschlüsse auf den Telekommunikationsverkehr zuließen. Es gab keine Bestandsdaten über die Mitgliedschaft in themenbezogenen Internet-Chatrooms (z.B. Drogen-Selbsthilfegruppe). Es gab keine elektronischen E-Mail-Adressbücher oder „Friends&Family"-Rufnummern als Bestandsdaten. 1984 hatte ein Bürger gewöhnlicherweise nur einen Festnetz-Telefondienstvertrag mit der Deutschen Bundespost. Heute hat ein Bürger normalerweise auch Mobiltelefonverträge, Internetzugangsverträge, E-Mail-Verträge und ist Mitglied in Internet-Chats. Im Zuge der technischen Entwicklung hat sich nicht nur die gesellschaftliche Bedeutung der Telekommunikation gewandelt. Auch die Sensibilität der anfallenden Bestandsdaten hat sich im Vergleich zu 1984 entscheidend erhöht. Dieser technischen Entwicklung darf sich die Auslegung des Art. 10 GG nicht verschließen, will sie entsprechend der Konzeption des Grundgesetzes einen Grundrechtsschutz auf der Höhe der Zeit gewährleisten.

Falsch ist der Einwand, Bestandsdaten unterschieden sich nicht von den **Vertragsdaten eines beliebigen anderen Unternehmens**. Der Unterschied liegt in der Funktion der Daten: Die Vertragsdaten eines Kommunikationsmittlers ermöglichen erst Fernkommunikation. Weil nun der freien Kommunikation eine herausragende Bedeutung in unserer Gesellschaft zukommt, müssen Informationen bei Kommunikationsmittlern besonders geschützt werden. Dies gilt selbst dann, wenn sie auch andernorts erhoben werden könnten, wie es übrigens nicht nur bei Bestandsdaten, sondern ebenso bei Kommunikationsumständen und -inhalten möglich sein kann. Die anderweitige Erhebung ist im Übrigen keineswegs so einfach wie die Möglichkeit eines zentralen, heimlichen, beweiskräftigen, kooperationsbereiten und kostengünstigen Zugriffs durch Inanspruchnahme eines Kommunikationsmittlers.

Art. 10 GG will die **Vertraulichkeit der Kommunikation** besonders schützen, weil sie die Grundlage unserer freiheitlichen Gesellschaft bildet. Deshalb – als Reflex – sind Kundendaten bei Kommunikationsmittlern besser geschützt als bei sonstigen Gesprächs- und Geschäftspartnern. Kommunikationsmittler sind keine beliebigen Unternehmen wie

---

[126] BVerfGE 67, 157 (172); ebenso etwa BVerfG, 1 BvR 330/96 vom 12.03.2003, Abs. 47.

[127] Seite 6.

andere auch, sondern haben eine besondere Funktion in unserer Gesellschaft, die einen besonderen Schutz der ihnen anvertrauten Informationen verlangt. Die vor dem Hintergrund historischer Missbräuche getroffene Entscheidung des Verfassungsgebers, das Fernmeldeverhältnis besonders zu schützen, ist zu respektieren.

Selbst wenn der Staat nicht die Ausforschung eines konkreten Kommunikationsvorgangs beabsichtigt: Niemand würde von einem **Rechtsanwalt oder Steuerberater** die Auskunft verlangen, welche Bankverbindung oder welches Geburtsdatum ein Mandant hat. Diese Daten könnten zwar bei jedem beliebigen Unternehmen vorliegen, sie unterliegen in besonderen Vertrauensverhältnissen aber aus gutem Grund einem besonderen Schutz.

Es besteht noch ein weiterer Unterschied zu den Kundendaten anderer Unternehmen: Auf Fernkommunikation ist der Mensch heutzutage **zwingend angewiesen**. Er muss seine persönlichen Daten einem Kommunikationsmittler anvertrauen. Bei anderen Unternehmen hat er hingegen die Wahl, ob und welchem Unternehmen er seine Daten anvertraut, zumal Geschäfte des täglichen Lebens auch anonym in Läden und Supermärkten erledigt werden können. Teilweise schreibt der Staat die Nutzung von Fernkommunikation sogar vor, etwa im Fall von Gewerbesteuer-Voranmeldungen über das Internet.

Im Übrigen: Wenn Personendaten wirklich auch **bei jeder anderen Firma** erhoben werden könnten, soll sie der Staat doch bei den anderen Firmen erheben. Wenn der Staat die Daten wirklich unabhängig von Kommunikationsvorgängen verfügbar haben will, möge er ihre Aufnahme in das Melderegister vorschreiben. Wo der Bezug zu einem konkreten Kommunikationsvorgang fehlt, gibt es kein legitimes staatliches Interesse daran, Personendaten gerade von dem grundrechtlich besonders geschützten Kommunikationsmittler zu erheben. Wo der Bezug zu einem konkreten Kommunikationsvorgang besteht, ist das Fernmeldegeheimnis erst Recht einschlägig.

Rechtsvergleichend ist darauf hinzuweisen, dass etwa das britische Recht sämtliche Daten bei Kommunikationsmittlern – Verbindungs-, Bestands- und sonstige Kundendaten – als „Kommunikationsdaten" („communications data") einheitlich definiert (§ 21 Abs. 4 Regulation of Investigatory Powers Act 2000) und auch den staatlichen Zugriff darauf einheitlich regelt. Dasselbe gilt für andere Staaten.

Gleiches liegt der Empfehlung Nr. R (95)4 des **Europarates** zum Schutz persönlicher Daten im Bereich der Telekommunikationsdienste vom 7. Februar 1995 zugrunde.[128] Diese regelt die „Sammlung und Verarbeitung personenbezogener Daten im Bereich von Telekommunikationsdiensten" einheitlich (Grundsatz 3). Als Oberbegriff wird „Servicedaten" verwendet, womit Inhaltsdaten, Verkehrsdaten, Bestandsdaten und sonstige personenbezogene Daten gleichermaßen gemeint sind.[129] Auch die Weitergabe personenbezogener Daten wird einheitlich geregelt (Grundsatz 4). In Abs. 53 des Erläuternden Berichts heißt es, „die Verfasser dieser Empfehlung wollten Servicedaten innerhalb des Grundsatzes des Brief- und Kommunikationsgeheimnisses ansiedeln, wie er in Artikel 8 des Europäischen Menschenrechtskonvention niedergelegt ist". Auch die Verfasser der Empfehlung des Europarats gehen also davon aus, dass Bestandsdaten dem Fernmeldegeheimnis unterliegen.

---

[128] http://www.giodo.gov.pl/plik/id_p/31/j/en/.

[129] Abs. 25 des Erläuternden Berichts, https://wcd.coe.int/ViewDoc.jsp?id=529277&Site=CM&BackColorInternet=9999CC&-BackColorIntranet=FFBB55&BackColorLogged=FFAC75.

4.6 Zugriff auf Schlüssel zu Kommunikationsinhalten als Eingriff in das Fernmeldegeheimnis

Besonders einleuchtend ist die Betroffenheit des Fernmeldegeheimnisses ferner, wenn der Staat einen Kommunikationsmittler zwingt, ihm den **Schlüssel zu Kommunikationsinhalten**, die dem Kommunikationsmittler anvertraut sind (z.B. elektronischer Anrufbeantworter, E-Mail-Postfach), auszuliefern.[130]

§ 113 TKG ermöglicht etwa die folgenden Anfragen und beschränkt dadurch eindeutig das Fernmeldegeheimnis:

- Wie lautet der Zugriffscode zum **elektronischen Anrufbeantworter** des Anschlusses 072191010?
- Wie lautet das Passwort zum **Postfach des E-Mail-Kontos** bverfg@bundesverfassungsgericht.de?

Nach seinem **Zweck** schützt das Fernmeldegeheimnis vor der Beschaffung solcher Zugangsschlüssel. Denn im Fall der direkten Kommunikation hätte der Staat nicht die Möglichkeit, durch die heimliche Inanspruchnahme eines Dritten einen Schlüssel zu einem Nachrichten-Zwischenspeicher zu bekommen.

Bei unmittelbarer verkörperter Kommunikation durch Einwurf eines Briefes in den Briefkasten des Empfängers könnte der Staat sich zwar einen **Schlüssel zu dem Briefkasten** verschaffen. Der Empfänger kann aber eigene Schutzvorkehrungen gegen den heimlichen Zugriff auf seinen Briefkasten treffen, etwa indem er seinen Briefkastenschlüssel bei sich trägt oder den Briefkasten an die Innenseite seiner Wohnungstür montiert. Im Fall der Fernkommunikation kann sich der Staat den Schlüssel hingegen unbemerkt durch Inanspruchnahme des Kommunikationsmittlers verschaffen. Auch der anschließende Zugriff auf die Kommunikation kann unbemerkt bei dem Kommunikationsmittler erfolgen, ohne dass sich der Betroffene davor schützen kann. Deswegen wird die spezifische Verletzlichkeit der Telekommunikation ausgenutzt und ist Art. 10 GG einschlägig.

Bereits entschieden hat das Hohe Gericht, dass der Zugriff auf Kommunikationsinhalte in einem E-Mail-Postfach oder einem geschlossenen Chat in Art. 10 GG eingreift, wenn der erforderliche Zugangscode ohne oder gegen den Willen der Kommunikationsbeteiligten erhoben worden ist.[131] Es würde nun dem Schutzzweck des Art. 10 GG nicht gerecht, wenn das Fernmeldegeheimnis erst vor der Nutzung des Schlüssels schützen würde und nicht schon vor seiner Aneignung bei dem Kommunikationsmittler, der notwendig über den Schlüssel verfügen muss.[132] Denn es beeinträchtigt die unbefangene, freie und in allem vertrauliche Nutzung von Telekommunikations-Zwischenspeichern unzumutbar, wenn man jederzeit befürchten muss, dass sich Staatsbeamte unbemerkt und unbemerkbar Zugang zu den eigenen Nachrichten verschaffen können. Diese Gefahr eines heimlichen, durch eigene Schutzvorkehrungen nicht abwendbaren Zugriffs besteht bei unmittelbarer Kommunikation nicht. Schon der Schlüssel in der Hand des Staates oder die Befürchtung, dass ihn der Staat ohne den Schutz des Fernmeldegeheimnisses jederzeit erlangen könnte, beeinträchtigt die freie Fernkommunikation unzumutbar, insbesondere im Bereich von E-Mail-Postfächern.

---

[130] Vgl. LG Hamburg, MMR 2002, 403 (404 f.); AK-GG-Bizer, Art. 10, Rn. 71.

[131] BVerfG, Urteil vom 27.2.2008, Az. 1 BvR 370/07 , Abs. 292.

[132] Ebenso LG Hamburg, MMR 2002, 403 (404 f.).

Nicht gelten lassen kann man dementsprechend das Argument, die hoheitliche **Beschaffung eines Wohnungsschlüssels** greife ebenfalls nicht in die Unverletzlichkeit der Wohnung ein. Erstens ist ein Eingriff in die „Unverletzlichkeit" der Wohnung hier durchaus anzunehmen, denn eine Wohnung, die nicht mehr vor staatlichem Zugriff gesichert ist, ist „verletzlich". Die räumliche Privatsphäre und der letzte Rückzugsraum des Menschen ist nicht mehr gewährleistet, wenn man jederzeit – auch in Abwesenheit – mit einem unerwünschten Eindringen in seinen räumlichen Rückzugsraum rechnen muss. Zweitens ist der Wohnungsschlüssel mit Nachrichtenschlüsseln schon nicht vergleichbar. Denn Art. 10 GG schützt vor der spezifischen Ausforschungsanfälligkeit der Fernkommunikation. Ein Kommunikationsmittler kann heimlich und kostengünstig zur Herausgabe eines Nachrichtenschlüssels gezwungen werden, woraufhin Nachrichten mitgelesen werden können. Notwendige Bedingung bestimmter Fernkommunikationsdienste (z.B. E-Mail) ist es, dass dem Mittler der vereinbarte Zugangsschlüssel vorliegt. Den eigenen Wohnungsschlüssel muss man demgegenüber nicht einem Dritten anvertrauen, um die eigene Wohnung benutzen zu können. Auch können Zutritte zur Wohnung vom Inhaber oder etwa von Nachbarn bemerkt oder gesehen werden, während der heimliche Zugriff auf gespeicherte Fernkommunikation nicht bemerkbar ist. Bei einer Wohnung kann man also eigene Schutzvorkehrungen gegen heimlichen Zugriff treffen. Bei einem Nachrichtenspeicher kann man sich hingegen kaum davor schützen, dass sich der Staat bei dem Kommunikationsmittler unbemerkt den Zugriffsschlüssel für den Nachrichtenspeicher verschafft.

In seiner **Entscheidung zur Computerdurchsuchung** hat das Hohe Gericht inzwischen anerkannt, dass Schutzlücken entstünden, würden die Grundrechte erst vor dem Zugriff auf und nicht schon vor der vorgelagerten Infiltration eines informationstechnischen Systems schützen.[133] Aus der großen Bedeutung der Nutzung informationstechnischer Systeme für die Persönlichkeitsentfaltung und aus den Persönlichkeitsgefährdungen, die mit dieser Nutzung verbunden sind, folge ein grundrechtlich erhebliches Schutzbedürfnis.[134] Der Einzelne sei darauf angewiesen, dass der Staat die mit Blick auf die ungehinderte Persönlichkeitsentfaltung berechtigten Erwartungen an die Integrität und Vertraulichkeit derartiger Systeme achte.[135] Die grundrechtlichen Gewährleistungen in den bisher in der Rechtsprechung des Bundesverfassungsgerichts entwickelten Ausprägungen würden dem durch die Entwicklung der Informationstechnik entstandenen Schutzbedürfnis nicht hinreichend Rechnung tragen.[136] Das Bundesverfassungsgericht hat daher entschieden, dass das Persönlichkeitsrecht schon vor einer Infiltration schützt, die einen späteren Zugriff ermöglicht: „Ein Eingriff in dieses Grundrecht ist zudem dann anzunehmen, wenn die Integrität des geschützten informationstechnischen Systems angetastet wird, indem auf das System so zugegriffen wird, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können; dann ist die entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems genommen."[137]

Nichts anderes gilt nun für den Bereich der **zeitversetzten Fernkommunikation**. Aus der heutigen Bedeutung der Fernkommunikation – etwa von elektronischer Post – für die Persönlichkeitsentfaltung und aus den Persönlichkeitsgefährdungen, die mit dieser Nutzung verbunden sind, folgt gleichfalls ein hohes Schutzbedürfnis. Der Einzelne ist darauf angewiesen, dass der Staat die mit Blick auf die ungehinderte Persönlichkeitsentfaltung

---

[133] BVerfG, Urteil vom 27.2.2008, Az. 1 BvR 370/07 , Abs. 181.
[134] BVerfG, Urteil vom 27.2.2008, Az. 1 BvR 370/07 , Abs. 181.
[135] BVerfG, Urteil vom 27.2.2008, Az. 1 BvR 370/07 , Abs. 181.
[136] BVerfG, Urteil vom 27.2.2008, Az. 1 BvR 370/07 , Abs. 181.
[137] BVerfG, Urteil vom 27.2.2008, Az. 1 BvR 370/07 , Abs. 205.

berechtigten Erwartungen an die Integrität und Vertraulichkeit von Nachrichten-Zwischenspeichern achtet. Das Fernmeldegeheimnis in den bisher in der Rechtsprechung des Bundesverfassungsgerichts entwickelten Ausprägungen trägt dem durch die Entwicklung der Fernmeldetechnik entstandenen Schutzbedürfnis nicht hinreichend Rechnung. Kommunikationsmittler bieten erst seit einigen Jahren elektronische Nachrichten-Zwischenspeicher an. Insbesondere eine Adresse der elektronischen Post ist erst in den letzten Jahren zur weithin unverzichtbaren Voraussetzung für die Teilnahme am gesellschaftlichen und beruflichen Leben geworden. Das Fernmeldegeheimnis muss daher schon vor der Erhebung des Zugriffsschlüssels bei dem Kommunikationsmittler schützen, weil der Schlüssel einen späteren Zugriff auf die grundrechtlich geschützte Kommunikation ermöglicht. Ein Eingriff in das Fernmeldegeheimnis ist anzunehmen, wenn Schutzvorkehrungen eines Nachrichten-Zwischenspeichers angetastet werden, indem dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können, denn damit ist die entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Nachrichten-Zwischenspeichers genommen.

Besonders eindeutig ist der Eingriff in das Fernmeldegeheimnis bei **Schlüsseln, die keinen anderen Zweck haben als den Zugriff auf Nachrichten** zu ermöglichen, z.B. der PIN-Code eines elektronischen, anbieterseitigen Anrufbeantworters („Sprachmailbox"). Das Fernmeldegeheimnis schützt aber auch Schlüssel, die gleichzeitig anderen Funktionen dienen. Beispielsweise kann die Zugangskennung eines E-Mail-Postfachs nicht nur das Lesen von Nachrichten ermöglichen, sondern daneben auch den Zugriff auf ein E-Mail-Portal („Webmail") mit persönlichen Einstellungen (z.B. Filterlisten, E-Mail-Adressbuch). Wenngleich diese Einstellungen keinen Aufschluss über konkrete Kommunikationsvorgänge geben und das Fernmeldegeheimnis nach enger Auffassung nur konkrete Kommunikationsvorgänge schützt, greift die Aneignung eines solch multifunktionalen Schlüssels gleichwohl in das Fernmeldegeheimnis ein. Denn mit der Aneignung des Schlüssels ist die entscheidende Hürde genommen, jederzeit auf einzelne Nachrichten zugreifen zu können. Die Vertraulichkeit der Fernkommunikation wäre nicht effektiv gesichert, wenn der Staat den Schutz des Fernmeldegeheimnis mit der Begründung umgehen könnte, er werde den Schlüssel nicht oder nur mit späterem richterlichem Beschluss für den Zugriff auf gespeicherte Nachrichten nutzen und benötige den Schlüssel nur zu anderen Zwecken (z.B. Einsicht in das elektronische Adressbuch). Die weitere Verwendung eines derart erlangten Schlüssels ist nicht mehr kontrollierbar.[138] Die daraus erwachsende Unsicherheit des Nachrichtenadressaten verhindert die unbefangene Nutzung des Postfachs, die Art. 10 GG gewährleistet. Dasselbe gilt schon für das durch § 113 Abs. 1 S. 2 TKG begründete Risiko, dass Staatsbeamte Zugangsschlüssel jederzeit erlangen können, ohne dass der Nachrichtenadressat davon erfährt. Wegen § 113 Abs. 1 S. 2 TKG kann man nicht mehr darauf vertrauen, dass das Fernmeldegeheimnis bei dem Zugriff auf gespeicherte Kommunikationsvorgänge gewahrt wird. – Im Übrigen unterfallen nach richtiger Ansicht auch mithilfe des Schlüssels einsehbare Bestandsdaten dem Schutz des Fernmeldegeheimnisses. Schon deswegen lässt sich dem Eingriff in Art. 10 GG nicht entgegen halten, ein Schlüssel solle nicht zum Zugriff auf Inhalts-, Verkehrs- oder Standortdaten, sondern nur zum Zugriff auf Bestandsdaten genutzt werden.

Es ist zwar richtig, dass staatliche Maßnahmen nicht immer schon dann in ein Grundrecht eingreifen, wenn sie einen **Eingriff in das Grundrecht vorbereiten**. Falsch wäre aber die umgekehrte Aussage, die Grundrechte schützten nie vor Vorbereitungshandlungen und Grundrechtsgefährdungen. Für das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ist bereits ausgeführt worden, dass es einen

[138] Bundesdatenschutzbeauftragter, Schriftsatz vom 22.01.2007, 4 und 16.

Schutz schon vor der bloßen Infiltration gewährleistet. Auch das Grundrecht auf informationelle Selbstbestimmung schützt vor jeder Erhebung personenbezogener Daten, selbst wenn diese nur dazu dient, die eigentlich gesuchte Information mittels eines weiteren Eingriffs zu erlangen. Nicht anders muss das Fernmeldegeheimnis als Spezialgrundrecht vor jeder Erhebung personenbezogener Daten bei einem Kommunikationsmittler schützen, selbst wenn die Daten nur dazu dienen, die eigentlich gesuchten Kommunikationsinhalte in einem weiteren Schritt zu ermitteln.

Dass die Vorbereitung eines Grundrechtseingriffs nicht dem Grundrechtseingriff gleichzusetzen sei, ist letztlich ein **tautologisches Argument**. Denn ob die Ausforschung eines Kommunikationsschlüssels einen Eingriff in Art. 10 GG darstellt oder einen solchen erst vorbereitet, ist gerade die Frage.

Wenn der Bevollmächtigte der Bundesregierung weiter anführt, das Fernmeldegeheimnis schütze nach der Rechtsprechung des Bundesverfassungsgerichts **im Herrschaftsbereich des Teilnehmers gespeicherte Daten** nicht, so trifft das zu. Denn im eigenen Herrschaftsbereich kann man Nachrichten selbst vor heimlichem Zugriff schützen. Nicht möglich ist dies demgegenüber bei Nachrichten, die aus technischen Gründen bei einem Kommunikationsmittler zwischengespeichert werden müssen (z.B. eingehende E-Mail-Nachrichten), wo sie jederzeit dem heimlichen Zugriff des Staates ausgesetzt sind.

Interessanterweise sind selbst Vertreter der Gegenmeinung der Auffassung, bei Erhebung eines Nachrichtenschlüssels müssten jedenfalls die **materiellen Voraussetzungen des dadurch ermöglichten Zugriffs** gewahrt sein.[139] Anderenfalls würde die handelnde staatliche Stelle ermächtigt, ein Datum zu erheben, mit dem sie von vornherein nichts anfangen dürfe.[140] Wenn nun aber ohnehin die Eingriffsvoraussetzungen des Art. 10 GG Anwendung finden sollen, macht es keinen Sinn, diese Schranken aus Art. 2 Abs. 1 GG abzuleiten und nicht aus dem einschlägigen Spezialgrundrecht des Fernmeldegeheimnisses.

4.7 Identifizierungszwang für Anschlussinhaber als Eingriff in Art. 10 GG

Es ist oben erläutert worden, dass das Fernmeldegeheimnis den Teilnehmer davor schützt, dass ihn der Staat durch Inanspruchnahme seines Fernkommunikationsmittlers namhaft macht. Ein Grundrechtseingriff liegt aber auch darin, dass der Staat den Fernkommunikationsmittler zwingt, sich von der **Identität seiner Teilnehmer Kenntnis zu verschaffen** und diese Kenntnisse für einen etwaigen staatlichen Abruf verfügbar zu halten (§ 111 TKG).

Nach dem modernen Eingriffsbegriff schützen die speziellen Grundrechte auch vor **mittelbaren Eingriffen** durch staatliche Maßnahmen, welche die Beeinträchtigung eines grundrechtlich geschützten Verhaltens typischerweise und vorhersehbar zur Folge haben oder die eine besondere Beeinträchtigungsgefahr in sich bergen, die sich jederzeit verwirklichen kann.[141] Auf dieser Linie liegt das Bundesverfassungsgericht, wenn es bereits die einer Kenntnisnahme von Telekommunikation „vorangehenden Arbeitsschritte" als Eingriff ansieht, soweit es sich nicht um eine rein sachbedingte Speicherung handelt: „Für die Kenntnisnahme von erfassten Fernmeldevorgängen durch Mitarbeiter des Bundesnachrichtendienstes steht folglich die Eingriffsqualität außer Frage. Aber auch die

---

[139] Bäcker, Die Vertraulichkeit der Internetkommunikation (2009), 15.

[140] Bäcker, Die Vertraulichkeit der Internetkommunikation (2009), 15.

[141] Windthorst, § 8, Rn. 50 und 52 m.w.N.; Dreier, GG, Vorb., Rn. 82; Pieroth/Schlink, Rn. 240 ff.; Sachs, GG, Vor Art. 1, Rn. 83 ff.; Weber-Dürler, VVDStRL 57 (1998), 66 ff.

vorangehenden Arbeitsschritte müssen in ihrem durch den Überwachungs- und Verwendungszweck bestimmten Zusammenhang betrachtet werden. Eingriff ist daher schon die Erfassung selbst, insofern sie die Kommunikation für den Bundesnachrichtendienst verfügbar macht und die Basis des nachfolgenden Abgleichs mit den Suchbegriffen bildet. An einem Eingriff fehlt es nur, soweit Fernmeldevorgänge zwischen deutschen Anschlüssen ungezielt und allein technikbedingt zunächst miterfasst, aber unmittelbar nach der Signalaufbereitung technisch wieder spurenlos ausgesondert werden."[142]

Die Beurteilung einer **Vorratsspeicherung von Telekommunikationsdaten** kann nicht anders ausfallen,[143] denn auch die Erhebung und Speicherung von Telekommunikationsdaten macht diese für eine spätere staatliche Kenntnisnahme verfügbar und birgt damit die latente Gefahr späterer, weiterer Eingriffe. Ein Identifizierungszwang begründet die besondere Gefahr, dass der Staat die gespeicherten Daten aufgrund von staatlichen Zwangsbefugnissen wie den §§ 112, 113 TKG anfordert. Beeinträchtigungen der von Art. 10 Abs. 1 Var. 3 GG geschützten Vertraulichkeit der Telekommunikation vor dem Staat sind die typische und vorhersehbare Folge einer generellen Verkehrsdatenspeicherungspflicht. Damit stellt bereits die hoheitliche Anordnung einer generellen Erhebung von Telekommunikationsdaten für staatliche Zwecke einen Eingriff in Art. 10 Abs. 1 Var. 3 GG dar.

Jede staatliche „Kenntnisnahme, Aufzeichnung und Verwertung" von Informationen, die in den Schutzbereich des Fernmeldegeheimnisses fallen, ist als Grundrechtseingriff anzusehen.[144] Dasselbe muss auch für eine staatlich angeordnete „Kenntnisnahme, Aufzeichnung und Verwertung" solcher Informationen gelten, wenn sich der Staat gleichzeitig den Zugriff auf die gespeicherten Daten eröffnet.[145] Ordnet der Staat an, dass ein Privater in die Rechtssphäre eines Dritten einzugreifen habe, so ist ihm der Eingriff zuzurechnen.[146] § 111 TKG ist insoweit nicht anders zu behandeln, als wenn der Staat selbst die entsprechenden Daten erheben und vorhalten würde. Dass sich der Staat zur Datenerhebung und -speicherung privater Unternehmen bedient, kann keinen Unterschied machen, weil er sich gleichzeitig den Zugriff auf die gespeicherten Daten eröffnet. Andernfalls könnte der Staat seine Grundrechtsbindung durch ein bloßes „Outsourcing" umgehen. Die Inanspruchnahme Privater erhöht das Gewicht des Grundrechtseingriffs sogar noch, weil sich der Kreis von – weitgehend ohne Schuld – beeinträchtigten Personen durch den zusätzlichen Eingriff in Art. 12 GG noch vergrößert. Die Einschaltung des Privaten mindert das Gewicht des Grundrechtseingriffs auch nicht deshalb, weil der Staat nur unter bestimmten Voraussetzungen und in einem bestimmten Verfahren auf die gespeicherten Daten zugreifen darf. Denn dieselben Voraussetzungen und dasselbe Verfahren könnte auch im Fall der staatlichen Datenspeicherung vorgesehen werden. Gleichwohl würde niemand daran zweifeln, dass bereits in der staatlichen Datenerhebung ein Eingriff in das Fernmeldegeheimnis liegt.

Bereits entschieden hat das Bundesverfassungsgericht, dass die Übermittlung von Telekommunikation an staatliche Stellen durch einen privaten Kommunikationsmittler, der die Telekommunikation auf gerichtliche Anordnung gemäß § 100a StPO hin aufzeichnet und den **staatlichen Stellen verfügbar macht**, einen Eingriff in das Fernmeldegeheimnis der an

---

142 BVerfGE 100, 313 (366).

143 Ebenso für eine Pflicht zur generellen Speicherung von Telekommunikations-Bestandsdaten unter dem Aspekt des Grundrechts auf informationelle Selbstbestimmung BVerwGE 119, 123 (126).

144 BVerfGE 85, 386 (398) und BVerfGE 100, 313 (366) für „jede Kenntnisnahme, Aufzeichnung und Verwertung".

145 Vgl. Bizer, Forschungsfreiheit, 159 für das „Auf-Abruf-Bereithalten" von Daten.

146 Vgl. BVerfGE 107, 299 (313 f.).

dem Kommunikationsvorgang Beteiligten darstellt.[147] Die Tatsache, dass sich der Staat dabei eines Privaten bediene, sei unerheblich, da der Eingriff hoheitlich angeordnet werde und dem Privaten kein Handlungsspielraum zur Verfügung stehe.[148] Nicht anders verhält es sich mit § 111 TKG.

Die Empfehlung des **Europarats** über den Datenschutz in der Telekommunikation[149] bestimmt unter Ziff. 22 ausdrücklich: „Anonyme Zugangsmöglichkeiten zu Telekommunikationsnetzen und -diensten sollten bereit gestellt werden." Der Erläuternde Bericht führt in Abs. 26 aus, diese Empfehlung diene dem Schutz der Kommunikationsfreiheit. Telefondienste könnten Teilnehmer oder Nutzer davon abschrecken, telefonisch zu kommunizieren, weil sie zur „Untergrabung der Anonymität" tendierten. Bedroht die Identifizierung von Teilnehmern die Kommunikationsfreiheit, muss das Fernmeldegeheimnis vor einer solchen Identifizierung schützen.

5 Zusammenfassung

Es ist gezeigt worden, dass das Fernmeldegeheimnis jedenfalls insoweit vor der staatlichen Erhebung von Bestandsdaten bei einem Kommunikationsmittler schützt, wie die Auskunft unmittelbar noch **unbekannte Fernmeldevorgänge aufdeckt oder bereits bekannte Fernmeldevorgänge näher beschreibt**, insbesondere die an einem Fernmeldevorgang Beteiligten identifiziert.[150] Insoweit ist das Fernmeldegeheimnis in seiner klassischen Funktion als Garant der Vertraulichkeit der näheren Umstände einzelner Fernmeldevorgänge einschlägig.

Es ist gezeigt worden, dass das Fernmeldegeheimnis vor der staatlichen Erhebung von Bestandsdaten bei einem Kommunikationsmittler auch dann schützt, wenn die Daten **es ermöglichen, durch weitere Datenerhebungen** Fernmeldevorgänge aufzudecken oder näher auszuforschen. Ein wirksamer Schutz der Vertraulichkeit der Fernkommunikation erfordert schon die Einbeziehung dieser Schlüsseldaten in den Schutzbereich des Fernmeldegeheimnisses. Das Fernmeldegeheimnis schützt danach erstens davor, dass der Staat einen Kommunikationsmittler zu der Auskunft zwingt, welcher Teilnehmer unter welcher Kennung kommuniziert oder kommuniziert hat.[151] Das Fernmeldegeheimnis schützt zweitens davor, dass der Staat bei einem Kommunikationsmittler einen Schlüssel beschafft, der ihm unmittelbaren Zugriff auf zwischengespeicherte Nachrichten eröffnet.[152] In beiden Fällen überwindet der Staat die entscheidende technische Hürde für eine Ausspähung der Fernkommunikation des Betroffenen.

Es ist gezeigt worden, dass das Fernmeldegeheimnis auch unabhängig von einzelnen Fernmeldevorgängen davor schützt, dass sich der Staat **bei einem Kommunikationsmittler Kenntnisse verschafft**, über die der Mittler lediglich zur Ermöglichung und Abrechnung der Fernkommunikation verfügt.[153] Insoweit kann sich das Fernmeldegeheimnis nicht von anderen Berufsgeheimnissen unterscheiden, bei denen die gesamte Vertrags- und Vertrauensbeziehung einen besonderen Schutz genießt, um die Unbefangenheit der geschützten Kommunikation zu gewährleisten.

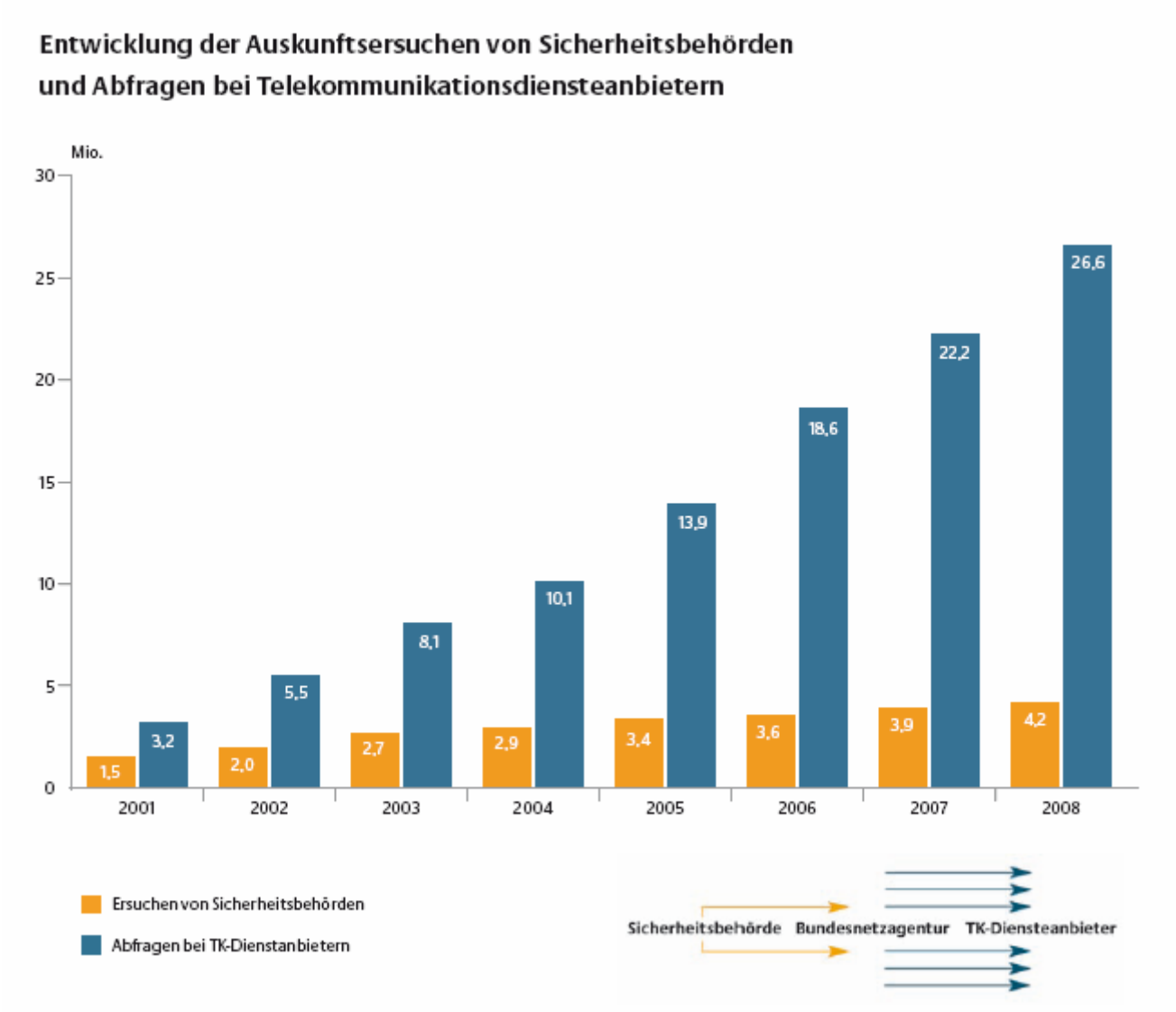
---

147 BVerfGE 107, 299 (313 f.).
148 BVerfGE 107, 299 (313 f.).
149 Empfehlung R (95) 4 vom 07.02.1995.
150 Seite 13 ff.
151 Seite 17 ff.
152 Seite 37 ff.
153 Seite 33 ff.

Abschließend ist gezeigt worden, dass das Fernmeldegeheimnis davor schützt, dass der Staat Kommunikationsmittler zur **Erhebung der Personalien von Teilnehmern und zur Vorhaltung** dieser Daten für staatliche Zugriffe zwingt.[154] Ein solches „Outsourcing" kann nicht anders zu beurteilen sein als wenn der Staat die Daten selbst erheben und vorhalten würde.

6 Empirische Erkenntnisse

Den bisher vorgetragenen empirischen Erkenntnissen ist hinzuzufügen, dass im Jahr 2008 schon **4,2 Millionen Auskunftsersuchen nach Bestandsdaten** im Verfahren nach § 112 TKG erfolgten: 8% mehr als im Vorjahr und doppelt so viele wie noch 2002.[155] Bei einem jährlichen Zuwachs um 8% erfolgt alle neun Jahre eine Verdoppelung der Zahl der Ausforschungen. Schon heute werden täglich über 10.000mal Bestandsdaten angefragt. Dass sich diese Entwicklung keineswegs mit der Marktentwicklung erklären lässt, ist bereits ausgeführt worden.[156]



[154] Seite 40 ff.

[155] Bundesnetzagentur, Jahresbericht 2008, http://www.bundesnetzagentur.de/media/archive/15901.pdf, 108.

[156] Schriftsatz vom 23.03.2007, Punkt 2.9.1.

Zugriff auf die Daten nach § 111 TKG haben inzwischen 1.000 Behörden.[157]

Starostik
-Rechtsanwalt-

[157] Bundesnetzagentur, Jahresbericht 2008, http://www.bundesnetzagentur.de/media/archive/15901.pdf, 108.