



Bundesministerium
der Justiz und
für Verbraucherschutz

Der Verfahrensbevollmächtigte
der Regierung der Bundesrepublik Deutschland

The Agent of the Government
of the Federal Republic of Germany

L'Agent du Gouvernement
de la République Fédérale d'Allemagne

HAUPTANSCHRIFT Mohrenstraße 37, 10117 Berlin
POSTANSCHRIFT 11015 Berlin
BEARBEITET VON [REDACTED]
REFERAT IV C 1
TEL [REDACTED]
FAX [REDACTED]
E-MAIL [REDACTED]
AKTENZEICHEN IV C 1 - 9470/2 - 4 E (2623) 48 110/2016
DATUM Berlin, 7. September 2016

POSTANSCHRIFT Bundesministerium der Justiz und für Verbraucherschutz, 11015 Berlin

Europäischer Gerichtshof
für Menschenrechte
– Europarat –
F – 67075 STRASBOURG – CEDEX

NUR PER E-TRANSMISSION

Betreff: Europäischer Gerichtshof für Menschenrechte

hier: Individualbeschwerde Nr. 50001/12
Breyer J. Bundesrepublik Deutschland

Bezug: Schreiben des Gerichtshofs vom 5. April 2016

A. Sachverhalt

- 1 Die Beschwerdeführer greifen mit ihrer Beschwerde die Regelung des § 111 des Telekommunikationsgesetzes (TKG) in der Fassung des Änderungsgesetzes vom 21. Dezember 2007 an. Sie behaupten, dass die in § 111 TKG enthaltene Pflicht der Telekommunikationsdiensteanbieter, bei der Vergabe von Rufnummern für Telekommunikationsanschlüsse bestimmte persönliche Daten des Anschlussinhabers zu erheben und zu speichern, sie in ihren Rechten aus Artikel 8 und 10 EMRK verletze.
- 2 Die Pflicht zur Speicherung von persönlichen Daten auch beim Verkauf von sog. Prepaid-Mobilfunkkarten ist durch das von den Beschwerdeführern zitierte Gesetz vom 22. Juni 2004 eingeführt worden. Bis zum Inkrafttreten dieses Gesetzes waren Telekommunikationsdiensteanbieter nur berechtigt, die für das Vertragsverhältnis erforderlichen Daten zu erhe-

LIEFERANSCHRIFT Kronenstraße 41, 10117 Berlin
VERKEHRSANBINDUNG U-Bahn/Hof-/Museumsgleise 112

ben und zu speichern. Bei Prepaid-Mobilfunkkarten waren keine solchen Daten erforderlich. Durch das Gesetz vom 21. Dezember 2007 wurde die Pflicht zur Erhebung und Speicherung der Rufnummern, anderen Anschlusskennungen, Namen und Anschrift des Anschlussinhabers, bei natürlichen Personen deren Geburtsdatum, das Datum des Vertragsbeginns und für den Fall, dass mit dem Mobilfunkanschluss auch ein Mobilfunkendgerät zur Verfügung gestellt wird, auf die Gerätenummer dieses Geräts in § 111 des Telekommunikationsgesetzes eingeführt.

- 3 Die nach § 111 TKG erhobenen Daten sind nach § 111 Abs. 5 TKG mit Ablauf des auf die Beendigung des Vertragsverhältnisses folgenden Jahres zu löschen. Die Übermittlung der Daten durch staatliche Stellen ist nur an die in den §§ 112 und 113 TKG genannten Stellen und nur im Rahmen der jeweiligen gesetzlichen Aufgaben zulässig. Sie setzt also voraus, dass für die jeweilige Stelle eine Rechtsgrundlage für das Übermittlungersuchen besteht.
- 4 Die Bundesregierung akzeptiert, dass die Beschwerdeführer durch diese gesetzliche Regelung betroffen sein können. Im Hinblick auf die Rechtsprechung des Gerichtshofs, die es für die Zulässigkeit einer Beschwerde ausreichen lässt, dass der Beschwerdeführer durch die beanstandete Rechtslage in seinen Rechten aus der Konvention beeinträchtigt sein kann, sieht die Bundesregierung keinen Anlass, die Opfereigenschaft der Beschwerdeführer in Zweifel zu ziehen.
- 5 Die Beschwerdeführer haben gegen die beanstandeten gesetzlichen Regelungen im Wege der Verfassungsbeschwerde das Bundesverfassungsgericht angerufen, das mit Beschluss vom 24. Januar 2012 ihre Verfassungsbeschwerden abgewiesen hat (BVerfGE 130, 151). Ausweislich der Beschwerdeschrift ist der Beschluss des Bundesverfassungsgerichts dem Vertreter der Beschwerdeführer am 28. Februar 2012 zugestellt worden, so dass die Beschwerde beim Gerichtshof fristgerecht erhoben wurde.

B. Innerstaatliches Recht und innerstaatliche Praxis

Telekommunikationsgesetz in der Fassung des Gesetzes vom 21. 12. 2007 (Gegenstand der Beschwerde)

§111 Daten für Auskunftersuchen der Sicherheitsbehörden

(1) Wer geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt und dabei Rufnummern oder andere Anschlusskennungen vergibt oder Telekommunikationsanschlüsse für von anderen

vergebene Rufnummern oder andere Anschlusskennungen bereitstellt, hat für die Auskunftsverfahren nach den §§ 112 und 113

1. die Rufnummern und anderen Anschlusskennungen,
2. den Namen und die Anschrift des Anschlussinhabers,
3. bei natürlichen Personen deren Geburtsdatum,
4. bei Festnetzanschlüssen auch die Anschrift des Anschlusses,
5. in Fällen, in denen neben einem Mobilfunkanschluss auch ein Mobilfunkgerät überlassen wird, die Gerätenummer dieses Gerätes sowie
6. das Datum des Vertragsbeginns

vor der Freischaltung zu erheben und unverzüglich zu speichern, auch soweit diese Daten für betriebliche Zwecke nicht erforderlich sind; das Datum des Vertragsendes ist bei Bekanntwerden ebenfalls zu speichern. Satz 1 gilt auch, soweit die Daten nicht in Teilnehmerverzeichnisse (§ 104) eingetragen werden. Die Verpflichtung zur unverzüglichen Speicherung nach Satz 1 gilt hinsichtlich der Daten nach Satz 1 Nr. 1 und 2 entsprechend für denjenigen, der geschäftsmäßig einen öffentlich zugänglichen Dienst der elektronischen

Post erbringt und dabei Daten nach Satz 1 Nr. 1 und 2 erhebt, wobei an die Stelle der Daten nach Satz 1 Nr. 1 die Kennungen der elektronischen Postfächer und an die Stelle des Anschlussinhabers nach Satz 1 Nr. 2 der Inhaber des elektronischen Postfachs tritt. Wird dem Verpflichteten nach Satz 1 oder Satz 3 eine Änderung bekannt, hat er die Daten unverzüglich zu berichtigen; in diesem Zusammenhang hat der nach Satz 1 Verpflichtete bisher

noch nicht erhobene Daten zu erheben und zu speichern, sofern ihm eine Erhebung der Daten ohne besonderen Aufwand möglich ist. Für das Auskunftsverfahren nach §113 ist die Form der Datenspeicherung freigestellt.

(2) Bedient sich der Diensteanbieter nach Absatz 1 Satz 1 oder Satz 3 eines Vertriebspartners, hat der Vertriebspartner die Daten nach Absatz 1 Satz 1 und 3 unter den dort genannten Voraussetzungen zu erheben und diese sowie die nach § 95 erhobenen Daten

unverzüglich dem Diensteanbieter zu übermitteln; Absatz 1 Satz 2 gilt entsprechend. Satz 1 gilt auch für Daten über Änderungen, soweit sie dem Vertriebspartner im Rahmen der üblichen Geschäftsbewicklung zur Kenntnis gelangen.

(3) Für Vertragsverhältnisse, die am Tage des Inkrafttretens dieser Vorschrift bereits bestehen, müssen Daten im Sinne von Absatz 1 Satz 1 oder Satz 3 außer in den Fällen des Absatzes 1 Satz 4 nicht nachträglich erhoben werden.

(4) Die Daten sind mit Ablauf des auf die Beendigung des Vertragsverhältnisses folgenden Kalenderjahres zu löschen.

(5) Eine Entschädigung für die Datenerhebung und -speicherung wird nicht gewährt.

§ 112 Automatisiertes Auskunftsverfahren

(1) Wer öffentlich zugängliche Telekommunikationsdienste erbringt, hat die nach § 111 Abs. 1 Satz 1, 3 und 4 und Abs. 2 erhobenen Daten unverzüglich in Kundendateien zu speichern, in die auch Rufnummern und Rufnummernkontingente, die zur weiteren Vermarktung oder sonstigen Nutzung an andere Anbieter von Telekommunikationsdiensten vergeben werden, sowie bei portierten Rufnummern die aktuelle Portierungskennung aufzunehmen sind. Der Verpflichtete kann auch eine andere Stelle nach Maßgabe des § 11 des Bundesdatenschutzgesetzes beauftragen, die Kundendateien zu führen. Für die Berichtigung und Löschung der in den Kundendateien gespeicherten Daten gilt § 111 Absatz 1 Satz 4 und Abs. 4 entsprechend. In Fällen portierter Rufnummern sind die Rufnummer und die zugehörige Portierungskennung erst nach Ablauf des Jahres zu löschen, das dem Zeitpunkt folgt, zu dem die Rufnummer wieder an den Netzbetreiber zurückgegeben wurde, dem sie ursprünglich zugeteilt worden war. Der Verpflichtete hat zu gewährleisten, dass

1. die Bundesnetzagentur jederzeit Daten aus den Kundendateien automatisiert im Inland abrufen kann,
2. der Abruf von Daten unter Verwendung unvollständiger Abfragedaten oder die Suche mittels einer Ähnlichkeitsfunktion erfolgen kann.

Der Verpflichtete und sein Beauftragter haben durch technische und organisatorische Maßnahmen sicherzustellen, dass ihnen Abrufe nicht zur Kenntnis gelangen können. Die Bundesnetzagentur darf Daten aus den Kundendateien nur abrufen, soweit die Kenntnis der Daten erforderlich ist

1. für die Verfolgung von Ordnungswidrigkeiten nach diesem Gesetz oder nach dem Gesetz gegen den unlauteren Wettbewerb,
2. für die Erledigung von Auskunftsersuchen der in Absatz 2 genannten Stellen.

Die ersuchende Stelle prüft unverzüglich, inwieweit sie die als Antwort übermittelten Daten benötigt, nicht benötigte Daten löscht sie unverzüglich; dies gilt auch für die Bundesnetzagentur für den Abruf von Daten nach Satz 7 Nummer 1.

(2) Auskünfte aus den Kundendateien nach Absatz 1 werden

1. den Gerichten und Strafverfolgungsbehörden,
2. den Polizeivollzugsbehörden des Bundes und der Länder für Zwecke der Gefahrenabwehr,
3. dem Zollkriminalamt und den Zollfahndungsämtern für Zwecke eines Strafverfahrens sowie dem Zollkriminalamt zur Vorbereitung und Durchführung von Maßnahmen nach § 23a des Zollfahndungsdienstgesetzes,
4. den Verfassungsschutzbehörden des Bundes und der Länder, dem Militärischen Abschirmdienst, dem Bundesnachrichtendienst,
5. den Notrufabfragestellen nach § 108 sowie der Abfragestelle für die Rufnummer 124 124,
6. der Bundesanstalt für Finanzdienstleistungsaufsicht sowie

7. den Behörden der Zollverwaltung für die in § 2 Abs. 1 des Schwarzarbeitsbekämpfungsgesetzes genannten Zwecke über zentrale Abfragestellen nach Absatz 4 jederzeit erteilt, soweit die Auskünfte zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich sind und die Ersuchen an die Bundesnetzagentur im automatisierten Verfahren vorgelegt werden.

(3) Das Bundesministerium für Wirtschaft und Technologie wird ermächtigt, im Einvernehmen mit dem Bundeskanzleramt, dem Bundesministerium des Innern, dem Bundesministerium der Justiz, dem Bundesministerium der Finanzen sowie dem Bundesministerium der Verteidigung eine Rechtsverordnung mit Zustimmung des Bundesrates zu erlassen, in der geregelt werden

1. die wesentlichen Anforderungen an die technischen Verfahren
 - a) zur Übermittlung der Ersuchen an die Bundesnetzagentur,
 - b) zum Abruf der Daten durch die Bundesnetzagentur von den Verpflichteten einschließlich der für die Abfrage zu verwendenden Datenarten und
 - c) zur Übermittlung der Ergebnisse des Abrufs von der Bundesnetzagentur an die ersuchenden Stellen,
2. die zu beachtenden Sicherheitsanforderungen,
3. für Abrufe mit unvollständigen Abfragedaten und für die Suche mittels einer Ähnlichkeitsfunktion
 - a) die Mindestanforderungen an den Umfang der einzugebenden Daten zur möglichst genauen Bestimmung der gesuchten Person,
 - b) die Zeichen, die in der Abfrage verwendet werden dürfen,
 - c) Anforderungen an den Einsatz sprachwissenschaftlicher Verfahren, die gewährleisten, dass unterschiedliche Schreibweisen eines Personen-, Straßen- oder Ortsnamens sowie Abweichungen, die sich aus der Vertauschung, Auslassung oder Hinzufügung von Namensbestandteilen ergeben, in die Suche und das Suchergebnis einbezogen werden,
 - d) die zulässige Menge der an die Bundesnetzagentur zu übermittelnden Antwortdatensätze sowie
4. wer abweichend von Absatz 1 Satz 1 aus Gründen der Verhältnismäßigkeit keine Kundendateien für das automatisierte Auskunftsverfahren vorhalten muss; in diesen Fällen gilt § 111 Absatz 1 Satz 5 entsprechend.

Im Übrigen können in der Verordnung auch Einschränkungen der Abfragemöglichkeit für die in Absatz 2 Nr. 5 bis 7 genannten Stellen auf den für diese Stellen erforderlichen Umfang geregelt werden. Die technischen Einzelheiten des automatisierten Abrufverfahrens gibt die Bundesnetzagentur in einer unter Beteiligung der betroffenen Verbände und der berechtigten Stellen zu erarbeitenden Technischen Richtlinie vor, die bei Bedarf an den Stand der Technik anzupassen und von der Bundesnetzagentur in ihrem Amtsblatt bekannt zu machen ist. Der Verpflichtete nach Absatz 1 und die berechtigten Stellen haben die Anforderungen der Technischen Richtlinie spätestens ein Jahr nach deren Bekanntmachung zu erfüllen. Nach dieser Richtlinie gestaltete mangelfreie technische Einrichtungen müssen im Falle einer Änderung der Richtlinie spätestens drei Jahre nach deren Inkrafttreten die geänderten Anforderungen erfüllen.

(4) Auf Ersuchen der in Absatz 2 genannten Stellen hat die Bundesnetzagentur die entsprechenden Datensätze aus den Kundendateien nach Absatz 1 abzurufen und an die ersuchende Stelle zu über-

mitteln. Sie prüft die Zulässigkeit der Übermittlung nur, soweit hierzu ein besonderer Anlass besteht. Die Verantwortung für die Zulässigkeit der Übermittlung tragen

1. in den Fällen des Absatzes 1 Satz 7 Nummer 1 die Bundesnetzagentur und
2. in den Fällen des Absatzes 1 Satz 7 Nummer 2 die in Absatz 2 genannten Stellen.

Die Bundesnetzagentur protokolliert für Zwecke der Datenschutzkontrolle durch die jeweils zuständige Stelle bei jedem Abruf den Zeitpunkt, die bei der Durchführung des Abrufs verwendeten Daten, die abgerufenen Daten, ein die abrufende Person eindeutig bezeichnendes Datum sowie die ersuchende Stelle, deren Aktenzeichen und ein die ersuchende Person eindeutig bezeichnendes Datum. Eine Verwendung der Protokolldaten für andere Zwecke ist unzulässig. Die Protokolldaten sind nach einem Jahr zu löschen.

(5) Der Verpflichtete nach Absatz 1 hat alle technischen Vorkehrungen in seinem Verantwortungsbereich auf seine Kosten zu treffen, die für die Erteilung der Auskünfte nach dieser Vorschrift erforderlich sind. Dazu gehören auch die Anschaffung der zur Sicherstellung der Vertraulichkeit und des Schutzes vor unberechtigten Zugriffen erforderlichen Geräte, die Einrichtung eines geeigneten Telekommunikationsanschlusses und die Teilnahme an dem geschlossenen Benutzersystem sowie die laufende Bereitstellung dieser Vorkehrungen nach Maßgaben der Rechtsverordnung und der Technischen Richtlinie nach Absatz 3. Eine Entschädigung für im automatisierten Verfahren erteilte Auskünfte wird den Verpflichteten nicht gewährt.

§ 113 Manuelles Auskunftsverfahren

(1) Wer geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, darf nach Maßgabe des Absatzes 2 die nach den §§ 95 und 111 erhobenen Daten nach Maßgabe dieser Vorschrift zur Erfüllung von Auskunftspflichten gegenüber den in Absatz 3 genannten Stellen verwenden. Dies gilt auch für Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird. Die in eine Auskunft aufzunehmenden Daten dürfen auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse bestimmt werden; hierfür dürfen Verkehrsdaten auch automatisiert ausgewertet werden. Für die Auskunftserteilung nach Satz 3 sind sämtliche unternehmensinternen Datenquellen zu berücksichtigen.

(2) Die Auskunft darf nur erteilt werden, soweit eine in Absatz 3 genannte Stelle dies in Textform im Einzelfall zum Zweck der Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Aufgaben der in Absatz 3 Nummer 3 genannten Stellen unter Angabe einer gesetzlichen Bestimmung verlangt, die ihr eine Erhebung der in Absatz 1 in Bezug genommenen Daten erlaubt; an andere öffentliche und nichtöffentliche Stellen dürfen Daten nach Absatz 1 nicht übermittelt werden. Bei Gefahr im Verzug darf die Auskunft auch erteilt werden, wenn das Verlangen in anderer Form gestellt wird. In diesem Fall ist das Verlangen unverzüglich nachträglich in Textform zu bestätigen. Die Verantwortung für die Zulässigkeit des Auskunftsverlangens tragen die in Absatz 3 genannten Stellen.

(3) Stellen im Sinne des Absatzes 1 sind

1. die für die Verfolgung von Straftaten oder Ordnungswidrigkeiten zuständigen Behörden;
2. die für die Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung zuständigen Behörden;
3. die Verfassungsschutzbehörden des Bundes und der Länder, der Militärische Abschirmdienst und der Bundesnachrichtendienst.

(4) Derjenige, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, hat die zu beauskunftenden Daten unverzüglich und vollständig zu übermitteln. Über das Auskunftersuchen und die Auskunftserteilung haben die Verpflichteten gegenüber den Betroffenen sowie Dritten Still-schweigen zu wahren.

(5) Wer geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, hat die in seinem Verantwortungsbereich für die Auskunftserteilung erforderlichen Vorkehrungen auf seine Kosten zu treffen. Wer mehr als 100 000 Kunden hat, hat für die Entgegennahme der Auskunftsverlangen sowie für die Erteilung der zugehörigen Auskünfte eine gesicherte elektronische Schnittstelle nach Maßgabe der Technischen Richtlinie nach § 110 Absatz 3 bereit-zuhalten, durch die auch die gegen die Kennt-nisnahme der Daten durch Unbefugte gesicherte Übertragung gewährleistet ist. Dabei ist dafür Sorge zu tragen, dass jedes Auskunftsverlangen durch eine verantwortliche Fachkraft auf Einhaltung der in Absatz 2 genannten formalen Voraussetzungen geprüft und die weitere Bearbeitung des Verlangens erst nach einem positiven Prüfergebnis freigegeben wird.

Seit 30. Juli 2016

(in der Fassung des Gesetzes vom 26. Juli 2016, BGBl. I S. 1818)

Telekommunikationsgesetz (TKG)

§ 111 Daten für Auskunftersuchen der Sicherheitsbehörden

(1) Wer geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt und dabei Rufnum-mern oder andere Anschlusskennungen vergibt oder Telekommunikationsanschlüsse für von anderen vergebene Rufnummern oder andere Anschlusskennungen bereitstellt, hat für die Auskunftsverfahren nach den §§ 112 und 113

1. die Rufnummern und anderen Anschlusskennungen,
2. den Namen und die Anschrift des Anschlussinhabers,
3. bei natürlichen Personen deren Geburtsdatum,
4. bei Festnetzanschlüssen auch die Anschrift des Anschlusses,
5. in Fällen, in denen neben einem Mobilfunkanschluss auch ein Mobilfunkendgerät überlassen wird, die Gerätenummer dieses Gerätes sowie
6. das Datum des Vertragsbeginns

vor der Freischaltung zu erheben und unverzüglich zu speichern, auch soweit diese Daten für betriebliche Zwecke nicht erforderlich sind; das Datum des Vertragsendes ist bei Bekanntwerden ebenfalls zu speichern. Satz 1 gilt auch, soweit die Daten nicht in Teilnehmerverzeichnisse (§ 104) eingetragen werden. Bei im Voraus bezahlten Mobilfunkdiensten ist die Richtigkeit der nach Satz 1 erhobenen Daten vor der Freischaltung zu überprüfen durch

1. Vorlage eines Ausweises im Sinne des § 2 Absatz 1 des Personalausweisgesetzes,
2. Vorlage eines Passes im Sinne des § 1 Absatz 2 des Passgesetzes,
3. Vorlage eines sonstigen gültigen amtlichen Ausweises, der ein Lichtbild des Inhabers enthält und mit dem die Pass- und Ausweispflicht im Inland erfüllt wird, wozu insbesondere auch ein nach ausländischen Bestimmungen anerkannter oder zugelassener Pass, Personalausweis oder Pass- oder Ausweisersatz zählt,
4. Vorlage eines Aufenthaltstitels,
5. Vorlage eines Ankunftsnachweises nach § 63a Absatz 1 des Asylgesetzes oder einer Bescheinigung über die Aufenthaltsgestaltung nach § 63 Absatz 1 des Asylgesetzes,
6. Vorlage einer Bescheinigung über die Aussetzung der Abschiebung nach § 60a Absatz 4 des Aufenthaltsgesetzes oder
7. Vorlage eines Auszugs aus dem Handels- oder Genossenschaftsregister oder einem vergleichbaren amtlichen Register oder Verzeichnis, der Gründungsdokumente oder gleichwertiger beweiskräftiger Dokumente oder durch Einsichtnahme in diese Register oder Verzeichnisse und Abgleich mit den darin enthaltenen Daten, sofern es sich bei dem Anschlussinhaber um eine juristische Person oder Personengesellschaft handelt,

soweit die Daten in den vorgelegten Dokumenten oder eingesehenen Registern oder Verzeichnissen enthalten sind. Die Überprüfung kann auch durch andere geeignete Verfahren erfolgen; die Bundesnetzagentur legt nach Anhörung der betroffenen Kreise durch Verfügung im Amtsblatt fest, welche anderen Verfahren zur Überprüfung geeignet sind, wobei jeweils zum Zwecke der Identifikation vor Freischaltung der vertraglich vereinbarten Mobilfunkdienstleistung ein Dokument im Sinne des Satzes 3 genutzt werden muss. Bei der Überprüfung ist die Art des eingesetzten Verfahrens zu speichern; bei Überprüfung mittels eines Dokumentes im Sinne des Satzes 3 Nummer 1 bis 6 sind ferner Angaben zu Art, Nummer und ausstellender Stelle zu speichern. Für die Identifizierung anhand eines elektronischen Identitätsnachweises nach § 18 des Personalausweisgesetzes oder nach § 78 Absatz 5 des Aufenthaltsgesetzes gilt § 8 Absatz 1 Satz 6 des Geldwäschegesetzes entsprechend. Für das Ankunftsverfahren nach § 113 ist die Form der Datenspeicherung freigestellt.

(2) Die Verpflichtung zur unverzüglichen Speicherung nach Absatz 1 Satz 1 gilt hinsichtlich der Daten nach Absatz 1 Satz 1 Nummer 1 und 2 entsprechend für denjenigen, der geschäftsmäßig einen öffentlich zugänglichen Dienst der elektronischen Post erbringt und dabei Daten nach Absatz 1 Satz 1 Nummer 1 und 2 erhebt, wobei an die Stelle der Daten nach Absatz 1 Satz 1 Nummer 1 die Kennungen der elektronischen Postfächer und an die Stelle des Anschlussinhabers nach Absatz 1 Satz 1 Nummer 2 der Inhaber des elektronischen Postfachs tritt.

(3) Wird dem Verpflichteten nach Absatz 1 Satz 1 oder Absatz 2 eine Änderung bekannt, hat er die Daten unverzüglich zu berichtigen. In diesem Zusammenhang hat der nach Absatz 1 Satz 1 Verpflichtete bisher noch nicht erhobene Daten zu erheben und zu speichern, sofern ihm eine Erhebung der Daten ohne besonderen Aufwand möglich ist.

(4) Bedient sich ein Diensteanbieter zur Erhebung der Daten nach Absatz 1 Satz 1 und Absatz 2 eines Dritten, bleibt er für die Erfüllung der Pflichten nach Absatz 1 Satz 1 und Absatz 2 verantwortlich. Werden dem Dritten im Rahmen des üblichen Geschäftsablaufes Änderungen der Daten nach Absatz 1 Satz 1 und Absatz 2 bekannt, hat er diese dem Diensteanbieter unverzüglich zu übermitteln.

(5) Die Daten nach den Absätzen 1 und 2 sind mit Ablauf des auf die Beendigung des Vertragsverhältnisses folgenden Kalenderjahres zu löschen.

(6) Eine Entschädigung für die Datenerhebung und -speicherung wird nicht gewährt.

Anm:

In § 112 wurden durch das Änderungsgesetz lediglich die Verweise auf § 111 angepasst; § 113 blieb unverändert.

C. Zum Gegenstand der Beschwerde

1. Kein Recht auf anonyme Kommunikation

- 6 Die Beschwerdeführer sehen in der Verpflichtung der Telekommunikationsdiensteanbieter zur Erhebung und Speicherung bestimmter persönlicher Daten deswegen eine Verletzung ihrer Rechte aus der Konvention, weil sie schon durch diese Speicherung und die damit gegebene grundsätzliche Möglichkeit für staatliche Stellen, auf diese Daten zuzugreifen, ihr Privatleben und ihre Kommunikationsfreiheit gefährdet sehen. Letztlich behaupten die Beschwerdeführer, dass Artikel 8 der Konvention ein Recht darauf enthalte, jederzeit anonym durch frei gewählte Medien kommunizieren zu können. Ein solches Recht lässt sich aber weder der Konvention, der Rechtsprechung des Gerichtshofs noch irgendeiner anderen internationalen Norm entnehmen. Die Argumentation der Beschwerdeführer zeigt zwar ihr Interesse an einer solchen anonymen Kommunikation auf, begründet dies aber nicht mit rechtlichen, sondern mit gesellschaftspolitischen Erwägungen. Diese vermögen aber eine Rechtsgrundlage für ein Recht auf anonyme Kommunikation nicht zu ersetzen. Auf keinen Fall gibt es ein absolutes, also nicht einschränkbares Recht auf anonyme Kommunikation.

- 7 Es geht den Beschwerdeführern nicht um die Abwehr übermäßiger Eingriffe in ihre Rechte, sondern um eine grundsätzlich anonyme Kommunikation und ein Verbot für staatliche Stellen, Kommunikationsdaten auch dort, wo es zur Strafverfolgung oder Gefahrenabwehr notwendig ist, identifizierbar zu machen. Sie setzen in ihrer Beschwerde ihr Interesse an anonymer Kommunikation absolut. Eine Abwägung mit anderen Rechten kann nach dieser Argumentation nicht stattfinden. Gerade diese Abwägung wird aber in Artikel 8 Abs. 2 der Konvention verlangt – durch das Erfordernis der „Notwendigkeit in einer demokratischen Gesellschaft“. Eine solche Abwägung ist auch Pflicht der Mitgliedstaaten der Konvention: Es gehört zu den von der Konvention vorausgesetzten Aufgaben der Mitgliedstaaten, die öffentliche Sicherheit und den Schutz der Bürger vor Straftaten im Rahmen der Konvention so weit wie möglich zu gewährleisten (s. etwa M.C. vs. Bulgarien, 39272/98, Rn. 149 ff.). Würden die Mitgliedstaaten diese Abwägung verweigern – etwa indem auf jede Möglichkeit zur Verfolgung von Straftaten oder zum Schutz der öffentlichen Sicherheit durch Ermittlungen im Bereich der Telekommunikation durch Gewährung absoluter Anonymität verzichtet wird – so würden sie ihren in der Konvention vorausgesetzten Schutzpflichten nicht gerecht.
- 8 Im Gegensatz zur Ansicht der Beschwerdeführer ist gerade unter diesem Aspekt auch das Urteil K.U. vs. Finnland, 2872/02, durchaus vergleichbar und in diesem Zusammenhang relevant. Dort hat der Gerichtshof festgestellt (Rn. 49): „Although freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others.“ Selbst der nach der Konvention ausdrücklich gebotene Schutz des Privatlebens und der Meinungsfreiheit hat also gegebenenfalls gegenüber anderen Erwägungen wie dem Schutz vor Verbrechen oder Gefahren zurückzutreten.
- 9 Daraus folgt, dass es den Mitgliedstaaten grundsätzlich möglich sein muss, zur Verfolgung der in der Konvention aufgeführten legitimen Ziele im Rahmen der von der Konvention gesetzten Grenzen auf solche Daten zuzugreifen. Damit geht einher, dass für bestimmte „legitimate imperatives“ überhaupt Daten zur Verfügung stehen. Es kann nicht verboten sein, Daten überhaupt schon zu speichern, wenn auf diese Daten von staatlicher Seite legitimer Weise zugegriffen werden darf. Das gilt unabhängig davon, ob die Daten für den technischen Betrieb des Telekommunikationsdiensteanbieters notwendig sind. Wenn die Daten für die legitimen Zwecke notwendig sind und für diese Zwecke erhoben werden dürfen, können sie im Rahmen der Bedingungen, die der Gerichtshof für die Speicherung von Daten formuliert hat (s. unten Rn. 32) auch gespeichert werden.

2. Keine umfassende Überwachung des Kommunikationsverhaltens durch § 111 TKG

- 10 Die Behauptung der Beschwerdeführer, wonach die unter § 111 TKG gespeicherten Daten „die Überwachung alltäglichen Kommunikations- und Bewegungsverhaltens“ erlauben, entspricht nicht der Wahrheit. Die Beschwerdeführer verwischen hier die Unterschiede zwischen den zu speichernden Bestandsdaten, um die es in ihrer Beschwerde geht, und den Verkehrsdaten, also etwa der Aufzeichnung von Zeit, Dauer und Partner eines bestimmten Telefongesprächs. Bestandsdaten sind lediglich die Daten eines Telekommunikationsteilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden. Dies sind nach § 111 TKG lediglich die Rufnummern und anderen Anschlusskennungen, der Name und die Anschrift des Anschlussinhabers, das Datum des Vertragsbeginns, bei natürlichen Personen deren Geburtsdatum, bei Festnetzanschlüssen auch die Anschrift des Anschlusses sowie in Fällen, in denen neben einem Mobilfunkanschluss auch ein Mobilfunkendgerät überlassen wird, die Gerätenummer dieses Gerätes. Daten, die während des Kommunikationsvorgangs anfallen, die sogenannten Verkehrsdaten, sind nicht Gegenstand der Regelung des § 111 TKG. § 111 TKG gibt weder den Behörden das Recht, solche Daten zu erheben oder zu speichern, noch enthält er Regeln über die Verarbeitung solcher Daten überhaupt.
- 11 Wichtig ist in diesem Zusammenhang, dass § 111 TKG nicht isoliert gelesen werden darf. Die Bedeutung der dort enthaltenen Verpflichtung zur Speicherung von Daten lässt sich nur angemessen beurteilen, wenn zugleich nicht nur die in den §§ 112 und 113 TKG enthaltenen Beschränkungen für den Abruf und die Verarbeitung dieser Daten, sondern auch die in den jeweiligen Fachgesetzen (Strafprozessordnung, Polizeigesetze) enthaltenen strengen Voraussetzungen für Datenabruf und -verarbeitung in den Blick genommen werden. So beschränkt etwa die StPO in ihren §§ 100a ff. die Möglichkeiten der Strafverfolgungsbehörden zur Erhebung und Verwertung von Kommunikationsdaten erheblich. Diese rechtsstaatlich gebotenen und der Konvention entsprechenden Sicherungen sind Teil des gesamten Regelungskomplexes, den die Beschwerdeführer in ihrer Beschwerde nicht vollständig darstellen.
- 12 Während der hier angegriffene § 111 TKG also nur die grundsätzliche Pflicht zur Erhebung und Speicherung der Basisdaten enthält, regeln die §§ 112 und 113 TKG, welche staatlichen Stellen unter welchen Bedingungen Zugriff auf diese Daten erhalten können. § 112 Abs. 2 TKG enthält eine Liste derjenigen staatlichen Stellen, die über die Bundesnetzagentur die nach § 111 TKG gespeicherten Daten abrufen können. Sie können dies allerdings nur unter der Voraussetzung, dass die Daten zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich sind. Bei Polizeivollzugsbehörden und der Zollverwaltung ist die Abrufmöglichkeit beschränkt auf bestimmte Zwecke (§ 112 Abs. 2 Nr. 2, 3 und 7). In § 113 TKG wird die Abrufmöglichkeit

sowohl hinsichtlich der befugten Stellen als auch hinsichtlich der Voraussetzungen für den Abruf noch enger beschränkt.

- 13 Die abrufenden Behörden benötigen wiederum eine Rechtsgrundlage für den Abruf der Daten nach § 112 TKG. Im Bereich der Strafverfolgungsbehörden ist dies z.B. § 100 j StPO, der den Abruf zulässt, soweit es für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Beschuldigten erforderlich ist. Für weitergehende Eingriffe, etwa die Überwachung von Verkehrsdaten, die mit den nach § 111 TKG erhobenen Daten verknüpft werden könnten, sind weitere rechtsstaatliche Sicherungen vorgesehen, so etwa die gerichtliche Anordnung nach § 100 b StPO.
- 14 Die Frage, ob derartige Eingriffe im Einzelfall gerechtfertigt sind, ist aber im Rahmen der vorliegenden Beschwerde gerade nicht zu entscheiden. Vielmehr geht es hier nur darum, ob der Staat befugt ist, die Speicherung von Basisdaten anzuordnen, um einen rechtsstaatlich gesicherten Zugriff auf diese Daten zu den vorgesehenen legitimen Zwecken wie Strafverfolgung und Gefahrenabwehr überhaupt zu ermöglichen. Der Gerichtshof hat genau dies, nämlich dass der Staat grundsätzlich in der Lage sein muss, personenbezogene Daten im Rahmen der rechtmäßigen Ausübung seiner Befugnisse zu erheben, zu speichern und zu verarbeiten, stets vorausgesetzt (s. etwa Weber und Saravia vs. Deutschland, Entscheidung vom 29. Juni 2006, 54934/00, Nr. 122).

3. Kein Totalverbot anonymer Kommunikation

- 15 Anders als von den Beschwerdeführern behauptet führt die Verpflichtung der Anbieter aus § 111 TKG auch nicht zu einem „Totalverbot anonymer Kommunikation“. Wie die Beschwerdeführer auf S. 18 ihrer Beschwerdeschrift selbst einräumen, gibt es nach wie vor eine Vielzahl von Möglichkeiten, anonym im Internet zu kommunizieren. § 111 TKG betrifft in dem von den Beschwerdeführern geltend gemachten Zusammenhang mit den von ihnen geschlossenen Prepaidverträgen lediglich die Vergabe von der jeweiligen Mobilfunkkarte zugeordneten Rufnummern. Die von den Beschwerdeführern selbst aufgeführten Möglichkeiten zur anonymen Kommunikation über Internetcafés, Proxy-Server oder Anonymisierungsdienste sind gerade nicht betroffen.

D. **Zur ersten Frage des Gerichtshofs**

1. *Gab es einen Eingriff in das Recht der Beschwerdeführer auf Privatleben und Korrespondenz im Sinne des Artikels 8 Abs. 1 der Konvention? Beruhte ein etwaiger Eingriff auf*

gesetzlicher Grundlage und war er erforderlich im Sinne des Artikels 8 Abs. 2 der Konvention?

I. Eingriff in das Recht auf Privatleben und Korrespondenz

- 16 Der angegriffene § 111 TKG enthält keine unmittelbare Verpflichtung für die Beschwerdeführer. § 111 TKG verpflichtet vielmehr die Anbieter von Telekommunikationsdiensten, bei der Vergabe von Rufnummern – also auch bei der Vergabe von Prepaid-Mobilfunkkarten – bestimmte persönliche Daten des Karteninhabers zu erheben und zu speichern. Die Beschwerdeführer sind von dieser Verpflichtung mittelbar betroffen, da für den Erwerb von Rufnummern oder Anschlusskennungen die Angabe der in § 111 Abs. 1 TKG aufgeführten Daten erforderlich ist.
- 17 Der Gerichtshof hat in seiner Rechtsprechung betont, dass die Speicherung persönlicher Daten einen Eingriff in das Privatleben der Betroffenen darstellt (S. and Marper v. Vereinigtes Königreich, GK, Urteil vom 4. Dezember 2008, Nr. 30562/04 und 30566/04, Rn. 67). Die Speicherung der Daten erfolgt hier zwar nicht durch staatliche Behörden. Da der wesentliche Zweck der Speicherung aber darin besteht, eine Übermittlung dieser Daten für die Erfüllung gesetzlicher Aufgaben (Strafverfolgung, Gefahrenabwehr) zu ermöglichen – unter engen Voraussetzungen, s. oben Rn. 11 ff. – akzeptiert die Bundesregierung, dass die Vorschrift des § 111 TKG grundsätzlich einen Eingriff in das Privatleben der Beschwerdeführer im Sinne des Artikels 8 der Konvention darstellen kann.
- 18 Der Gerichtshof berücksichtigt bei der Beurteilung der Frage, ob und inwieweit ein Eingriff in die Rechte eines Beschwerdeführers aus Artikel 8 der Konvention vorliegt, den spezifischen Kontext, in dem die fragliche Information erhoben und gespeichert wurde, die Natur der jeweiligen Daten, die Methode ihrer Nutzung und Verarbeitung sowie die möglichen Ergebnisse (S. and Marper vs. Vereinigtes Königreich, Rn. 67). Im vorliegenden Kontext ergibt sich aus den Vorschriften des TKG im Zusammenhang mit möglichen Abfragen durch staatliche Stellen, dass die Speicherung der persönlichen Daten das Ziel verfolgt, diese für die Erfüllung bestimmter staatlicher Zwecke zur Verfügung zu haben. Darin – nicht in einer behaupteten umfassenden Überwachung oder einem Totalverbot anonymer Kommunikation – kann ein Eingriff in Artikel 8 der Konvention gesehen werden.
- 19 Ein Eingriff in das Recht auf Privatleben der Beschwerdeführer ist somit lediglich insofern gegeben, als sie für den Fall, dass sie eine Rufnummer von einem Telekommunikationsdiensteanbieter erwerben wollen, zur Angabe bestimmter, eng begrenzter persönlicher Daten verpflichtet sind und diese Daten gespeichert werden. Der Umfang des Eingriffs ist folglich weitaus geringer als von den Beschwerdeführern behauptet.

II. Rechtfertigung des Eingriffs

- 20 Nach Artikel 8 Abs. 2 der Konvention darf in die Ausübung der Rechte aus Artikel 8 Abs. 1 nur eingegriffen werden, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist.

1. Eingriff gesetzlich vorgesehen

- 21 Der Eingriff in die Rechte der Beschwerdeführer erfolgte, wie in Artikel 8 Abs. 2 der Konvention gefordert, auf gesetzlicher Grundlage. § 111 TKG erfüllt alle Anforderungen, die der Gerichtshof an eine solche gesetzliche Grundlage stellt. Hierzu hat der Gerichtshof festgestellt, dass dazu auch qualitative Anforderungen wie etwa die Vorhersehbarkeit der Anwendung und allgemeine Willkürfreiheit gehören (s. *Rekvenyi vs. Ungarn*, 25390/94 1999 III Nr. 59).

- 22 Die Anwendung der Vorschrift des § 111 TKG ist in diesem Sinne hinreichend vorhersehbar. Die Behauptung der Beschwerdeführer, § 111 TKG sei deswegen unbestimmt, weil der Begriff der „anderen Anschlusskennung“ unklar sei, ist für die Beschwerde irrelevant. Die Betroffenheit der Beschwerdeführer ergibt sich nach ihrem eigenen Vortrag aus der Tatsache, dass sie Prepaid-Mobilfunkkarten nutzen, die in jedem Fall von § 111 TKG erfasst werden („Rufnummern“). Die gesetzliche Grundlage für die Pflicht der Anbieter, die betreffenden Daten zu erfassen, ist also insoweit eindeutig und für die Beschwerdeführer vorhersehbar. Im Übrigen liegt eine hinreichende gesetzliche Grundlage nach der Rechtsprechung des Gerichtshofs auch dann vor, wenn die entsprechende Norm interpretationsbedürftig ist. Der Gerichtshof hat darauf hingewiesen, dass Normen in jedem Rechtssystem immer der Interpretation und der Anpassung an wechselnde Umstände bedürfen (*S.W. vs. Vereinigtes Königreich*, Serie A 336 B, Nr. 36).

2. Notwendig in einer demokratischen Gesellschaft

- 23 Ein Eingriff in die Rechte aus Artikel 8 der Konvention kann nach Artikel 8 Abs. 2 gerechtfertigt sein, wenn er in einer demokratischen Gesellschaft für einen der dort aufgeführten Zwecke notwendig ist. Dies ist dann der Fall, wenn es einem dringenden sozialen Bedürfnis entspricht, den Zweck zu erreichen und die dazu angewandten Mittel verhältnismäßig sind.
- 24 Der Eingriff in die Rechte der Beschwerdeführer ist im Rahmen des Artikels 8 Abs. 2 der Konvention gerechtfertigt. Er ist insbesondere verhältnismäßig, da er aus stichhaltigen und hinreichenden Gründen erfolgt und auf ein geringes Ausmaß beschränkt bleibt. Bei der Beur-

teilung der Verhältnismäßigkeit steht den staatlichen Behörden zudem ein weiter Beurteilungsspielraum zu.

a) Legitimer Zweck

- 25 Die Vorschrift des § 111 TKG dient einem legitimen Zweck. Wie das Bundesverfassungsgericht zutreffend dargelegt hat, soll § 111 TKG der Verbesserung der staatlichen Strafverfolgung und der Gefahrenabwehr dienen. Dabei handelt es sich unstreitig um legitime Ziele staatlicher Gesetzgebung, die sich unter verschiedene in Artikel 8 Abs. 2 aufgeführte Zwecke subsumieren lassen (öffentliche Sicherheit, Aufrechterhaltung der Ordnung, Verhütung von Straftaten, Schutz der Rechte und Freiheiten anderer). Die Frage, ob und in welchem Umfang die Vorschrift des § 111 TKG geeignet ist, diese Ziele zu erreichen, ist im nächsten Schritt zu prüfen.
- 26 § 111 TKG schafft die Voraussetzungen dafür, dass bestimmte Behörden, die in den §§ 112 und 113 TKG benannt sind, Telekommunikationsnummern bestimmten Anschlussinhabern zuordnen können. Eine solche Zuordnung kann sowohl zu Zwecken der Strafverfolgung als auch zur Gefahrenabwehr erforderlich sein. Sie dient damit der öffentlichen Sicherheit ebenso wie der Verhütung von Straftaten; beides Ziele, die in Artikel 8 Abs. 2 der Konvention als rechtfertigend für Eingriffe anerkannt sind. Die Beschwerdeführer räumen selbst ein, dass die Identifizierung von Kommunikationsteilnehmern zur Ermittlung und Verfolgung von Straftaten erforderlich sein kann. Das gleiche gilt für die Abwehr von Gefahren für die öffentliche Sicherheit, etwa die Aufklärung und Verhinderung geplanter Straftaten.
- 27 Es ist der Bundesregierung bewusst, dass auch eine Speicherung von Basisdaten wie nach § 111 TKG vorgesehen keine Garantie dafür bedeutet, dass die Teilnehmer eines Kommunikationsvorgangs identifiziert werden können. Auch nach der hier angegriffenen Fassung des § 111 TKG verbleiben Möglichkeiten zur Umgehung einer Identifikation; sei es durch Angabe falscher Daten oder auf anderen Wegen.
- 28 In diesem Zusammenhang weist die Bundesregierung darauf hin, dass § 111 TKG durch das am 30. Juli 2016 in Kraft getretene Gesetz zum besseren Informationsaustausch bei der Bekämpfung des internationalen Terrorismus dahingehend ergänzt worden ist, dass die Telekommunikationsdiensteanbieter verpflichtet sind, die zu speichernden Daten anhand eines amtlichen Identitätsdokuments zu überprüfen. Damit werden die Möglichkeiten zur Umgehung der Pflichten aus § 111 TKG weiter eingeschränkt. Daraus wird aber auch deutlich, dass Deutschland von Anfang an bemüht war und ist, die zur Erreichung der legitimen Ziele von Strafverfolgung und Gefahrenabwehr vorgenommenen Eingriffe so gering wie möglich zu halten. Erst nachdem die praktische Erfahrung gezeigt hat, dass die Anbieter von Tele-

kommunikationsdiensten die Angaben der Erwerber nicht hinreichend überprüfen, wird nunmehr auch eine Pflicht zur Verifikation eingeführt. Deutschland kann hier also im Hinblick auf die Regelung von 2004 allenfalls eine zu vorsichtige und datenschutzfreundliche Haltung vorgeworfen werden.

- 29 Trotz der bestehenden Umgehungsmöglichkeiten sind die in § 111 TKG niedergelegten Pflichten jedenfalls geeignet, die Verfolgung von Straftaten und den Schutz der öffentlichen Sicherheit zu verbessern. Durch die Erweiterung der Speicherungspflicht auf Prepaid-Mobilfunkkarten wird die Zuordnung von Mobilfunknummern in einem wesentlich weiteren Umfang als zuvor möglich. Damit haben die mit der Strafverfolgung und Gefahrenabwehr betrauten Behörden selbst dann, wenn eine sichere Zuordnung zu einem bestimmten Anschlussinhaber nicht möglich ist, jedenfalls einen Ansatz für weitere Ermittlungen.
- 30 Aus Sicht der Bundesregierung liegt es auf der Hand, dass die Möglichkeit der Zuordnung von Anschlussinhabern auch zu Prepaid-Mobilfunknummern zu einer effektiven Strafverfolgung und Gefahrenabwehr beiträgt. Sollte der Gerichtshof hierzu die Vorlage von Beispielfällen wünschen, bittet die Bundesregierung um einen entsprechenden Hinweis.

b) Verhältnismäßigkeit der Speicherungspflicht

- 31 Speziell für Eingriffe in die Rechte aus Artikel 8 der Konvention durch die Erhebung und Speicherung von persönlichen Daten hat der Gerichtshof eine Reihe von besonderen Voraussetzungen entwickelt. Dabei ist er davon ausgegangen, dass der Schutz persönlicher Daten fundamentale Bedeutung für das Recht auf Privat- und Familienleben hat und das nationale Recht daher für angemessene Schutzvorschriften gegen den Missbrauch solcher Daten sorgen muss (Z vs. Finnland, Rn. 95; S. and Marper vs. Vereinigtes Königreich, Rn. 103). Besonders wichtig ist der Schutz persönlicher Daten dann, wenn die fraglichen Daten in automatisierten Verfahren verarbeitet werden.
- 32 Das nationale Recht muss in diesem Fall, um den Vorgaben der Konvention zu genügen, zunächst sicherstellen, dass sich die Speicherung und Verarbeitung persönlicher Daten auf den erforderlichen Umfang beschränkt und nicht über das für den jeweiligen Zweck benötigte Maß hinausgeht. Bei der Speicherung muss sichergestellt werden, dass die Daten nicht länger aufbewahrt werden als es für den jeweiligen Zweck erforderlich ist. Zudem müssen hinreichende Vorsichtsmaßnahmen gegen Missbrauch der Daten getroffen werden (S. and Marper vs. Vereinigtes Königreich, Rn. 103). Alle diese Bedingungen erfüllt das deutsche Recht.

Beschränkung auf den erforderlichen Umfang

- 33 Wie oben unter Rn. 11 dargestellt, darf § 111 TKG nicht isoliert betrachtet werden. Die hier angegriffene Vorschrift ist Teil eines Gesamtsystems, in dem die Rechte der von Eingriffen durch Speicherung und Verarbeitung von Daten Betroffenen durch verschiedene rechtsstaatliche Sicherungen geschützt werden (s.o. Rn. 11 ff.).
- 34 § 111 TKG verlangt nur die Angabe und Speicherung weniger grundlegender Daten des Erwerbers einer Rufnummer: Name, Anschrift und Geburtsdatum und das Datum des Vertragsbeginns. Dazu kommt die erworbene Rufnummer sowie, falls gleichzeitig ein Mobilfunkgerät erworben wurde, dessen Gerätenummer. Es handelt sich also um das Minimum dessen, was zur Identifikation eines Anschlussinhabers erforderlich ist.
- 35 Die Speicherungspflicht ist auch nicht etwa deswegen ein unverhältnismäßiger Eingriff, weil sie, wie die Beschwerdeführer behaupten, zu weitergehenden Effekten führen könnte. Die insoweit dargestellten Befürchtungen der Beschwerdeführer entbehren jeder tatsächlichen Grundlage.
- 36 Auch die Behauptung, dass der minimale Datensatz des § 111 TKG einen höheren Aussagegehalt zur Identifikation von Personen habe als die in *S. and Marper vs. Vereinigtes Königreich* relevanten DNA-Daten und Fingerabdrücke, ist nicht nachvollziehbar. Soweit sich die Beschwerdeführer dabei darauf berufen, dass mit diesen Daten in anderen Zusammenhängen auch andere Informationen verknüpft werden können (Gesundheitsdaten etc.) ist dies im vorliegenden Kontext völlig irrelevant: Für alle diese Daten bestehen besondere Schutzvorschriften und strenge Regeln über Abruf und Verarbeitung. § 111 TKG hat keinerlei Zusammenhang mit solchen Daten und ermöglicht keine der von den Beschwerdeführern behaupteten Verknüpfungen oder Verarbeitungen. Die Möglichkeiten, die sich aus § 111 TKG im Zusammenhang mit anderen Regelungen zur Datennutzung ergeben können, haben die Beschwerdeführer dagegen nicht zum Gegenstand ihrer Beschwerde gemacht.

Keine Stigmatisierung

- 37 Die Behauptung der Beschwerdeführer, die Angabe dieses minimalen Datensatzes sei ein quantitativ und qualitativ einschneidenderer Eingriff in die Rechte aus Artikel 8 der Konvention als die Erhebung und Speicherung von Fingerabdrücken und DNA-Proben, um die es im Fall *S. and Marper vs. Vereinigtes Königreich* ging, ist für die Bundesregierung nicht nachvollziehbar. Die im Fall *S. and Marper vs. Vereinigtes Königreich* relevanten Daten konnten für sehr viel weitgehendere Zwecke benutzt werden als für die Identifikation von Kommunikationsteilnehmern (s. *S. and Marper vs. Vereinigtes Königreich*, Rn. 75). So konnte aus diesen

Daten die genetische Verwandtschaft unter verschiedenen Personen ermittelt werden. Nicht zuletzt deshalb sah der Gerichtshof hier eine besondere Sensibilität der Daten, die zu erhöhten Schutzverpflichtungen führte. Bei den nach § 111 TKG zu speichernden Daten entfallen alle diese zusätzlichen Elemente und Risiken. Aus Name, Anschrift und Geburtsdatum einer Person können weder Familien- noch Persönlichkeitsprofile, noch ethnische Zugehörigkeit entnommen werden.

- 38 Auch in anderer Hinsicht ist der Sachverhalt im Fall S. and Marper vs. Vereinigtes Königreich nicht mit der vorliegenden Konstellation vergleichbar. Die von den Beschwerdeführern angeführte Tatsache, dass die dort beanstandete Regelung zur Speicherung von DNA-Daten nur Personen betraf, die einer Straftat verdächtig waren, führte nach der zutreffenden Ansicht des Gerichtshofs gerade nicht zu einer geringeren Eingriffsintensität, sondern zu einer wesentlich höheren, denn dadurch entstand ein Effekt der Stigmatisierung (s. dort Rn. 122). Gerade die allgemeine Verpflichtung zur Speicherung von Daten, wie sie § 111 TKG vorsieht, und die die Beschwerdeführer hier angreifen, verhindert aber diese besondere Belastung derjenigen, deren Daten gespeichert werden. Ein Stigmatisierungseffekt, wie er in S. and Marper vs. Vereinigtes Königreich zu befürchten war, kann bei einer generellen Speicherungspflicht von Basisdaten für alle vergebenen Mobilrufnummern gerade nicht entstehen.

Dauer der Speicherung

- 39 Eine weitere Voraussetzung für die Zulässigkeit der Speicherung von persönlichen Daten ist, dass diese nicht länger als für den verfolgten Zweck erforderlich gespeichert werden dürfen. Dies ist nach dem deutschen Recht gleichfalls gewährleistet. § 111 Abs. 5 TKG sieht vor, dass die gespeicherten Daten spätestens am Ende des auf die Beendigung des Vertragsverhältnisses folgenden Kalenderjahres gelöscht werden müssen.
- 40 Damit legt das deutsche Recht eine zeitliche Obergrenze für die Speicherung der Daten fest. Auch darin liegt im Übrigen ein wesentlicher Unterschied zu dem im Fall S. and Marper vs. Vereinigtes Königreich entschiedenen Sachverhalt, in dem es um eine zeitlich unbefristete Speicherung sehr viel sensiblerer Daten ging; diesen Unterschied haben die Beschwerdeführer jedoch verschwiegen.
- 41 Die in § 111 Abs. 5 TKG bestimmte Frist ist auch nicht übermäßig lang. Es liegt auf der Hand, dass bei der Ermittlung von Straftaten eine zeitliche Verzögerung eintritt; wenn nach dem für die Ermittlung relevanten Kommunikationsakt das Vertragsverhältnis unmittelbar endet, müssen die Ermittlungsbehörden für eine gewisse Zeit auch im Nachlauf noch die Möglichkeit haben, die entsprechenden Inhaberdaten dem Kommunikationsakt zuzuordnen.

Gerade bei umfangreichen Ermittlungen zu schweren Straftaten ist die Frist mit dem Ende des auf die Beendigung folgenden Kalenderjahres jedenfalls nicht zu lang bemessen.

Schutz der Daten vor Missbrauch

- 42 Der vom Gerichtshof weiterhin geforderte Schutz gespeicherter Daten vor Missbrauch ist nach deutschem Recht gleichfalls gewährleistet. Dies geschieht dadurch, dass die §§ 112 und 113 TKG den Zugang zu den nach § 111 TKG gespeicherten Daten auf die dort genannten Behörden und öffentlichen Stellen beschränken. Alle diese Stellen unterliegen den strengen deutschen Datenschutzregeln, die hier nicht im Einzelnen dargestellt werden können.
- 43 Die Telekommunikationsdiensteanbieter wiederum sind nach den §§ 109 ff. TKG dazu verpflichtet, die bei ihnen gespeicherten Daten nach dem aktuellen Stand der Technik zu schützen. Diese Verpflichtung wird von der Bundesnetzagentur überwacht. Das gesamte System des TKG ist auf den größtmöglichen Schutz der Daten vor Missbrauch ausgerichtet.

Abwägung der betroffenen Interessen

- 44 Für den von § 111 TKG verfolgten Zweck – die Identifikation von Anschlussinhabern zum Zweck der Strafverfolgung und der Gefahrenabwehr im Rahmen der in den §§ 112 und 113 TKG geregelten Abrufmöglichkeiten – sind die dort aufgeführten Daten daher das absolute Minimum. Name, Anschrift, Geburtsdatum des Anschlussinhabers und das Datum des Vertragsbeginns sind erforderlich, um ihn zu identifizieren. § 111 TKG ist insoweit nicht nur „nicht übermäßig“, sondern bewegt sich – aufgrund des grundsätzlich sehr strengen deutschen Datenschutzrechts – am untersten Rand des zur Zweckerreichung Notwendigen.
- 45 Die vom deutschen Gesetzgeber verabschiedeten Regelungen sind daher offensichtlich bemüht, den Eingriff in die Rechte aus Artikel 8 – durch die Speicherung persönlicher Daten – auf das für das Funktionieren des Rechtsstaats absolut erforderliche Ausmaß zu beschränken.
- 46 Schließlich ist in diesem Zusammenhang auch der relativ weite Beurteilungsspielraum des deutschen Gesetzgebers zu berücksichtigen. Anders als in *S. and Marper vs. Vereinigtes Königreich* geht es im vorliegenden Fall nicht etwa um einen bahnbrechenden Einsatz neuer Technologien, bei dem die nationalen Behörden eine besondere Verantwortung tragen. Vielmehr wird mit der Verpflichtung zur Angabe der minimalen Basisdaten lediglich die bestehende und von niemandem in Zweifel gezogene Verpflichtung zur Erhebung und Speicherung der entsprechenden Daten der Inhaber von Festnetzanschlüssen auf den Erwerb von Mobilfunkkarten übertragen. Die deutschen Behörden haben hier eine Abwägung zwischen

verschiedenen konventionsrechtlich geschützten Positionen getroffen. Dabei wurde das Recht auf Privatleben angemessen berücksichtigt; insbesondere wurde der Umfang der anzugebenden Daten und die Abfragemöglichkeiten auf das Minimum beschränkt.

- 47 In einer derartigen Abwägungssituation zwischen verschiedenen von der Konvention geschützten Rechten und Pflichten ist der Beurteilungsspielraum der Staaten notwendigerweise relativ weit (s. etwa *Evans vs. Vereinigtes Königreich*, 2007-I, Nr. 77). Auch die aus den von den Beschwerdeführern vorgelegten Untersuchungen deutlich gewordene Tatsache, dass es in Europa keinen Konsens hinsichtlich der Identifizierungspflicht für Prepaid-Mobilfunkkarten gibt, spricht für einen relativ weiten Beurteilungsspielraum.
- 48 Das Ergebnis der Abwägung zwischen dem minimalen Eingriff in die Rechte aus Artikel 8 der Konvention durch die reine Speicherung weniger Basisdaten und der Notwendigkeit, zum Schutz zentraler öffentlicher Interessen und unter Einhaltung der konventionsrechtlichen Voraussetzungen Kommunikationsvorgänge den Anschlussinhabern zuordnen zu können, kann daher nur sein, dass der Eingriff jedenfalls verhältnismäßig ist. Die Rechte der Beschwerdeführer aus Artikel 8 der Konvention sind nicht verletzt.

E. Zur zweiten Frage des Gerichtshofs

2. *Gab es einen Eingriff in das Recht der Beschwerdeführer auf Freiheit der Meinungsäußerung im Sinne des Artikels 10 Abs. 1 der Konvention? War ein etwaiger Eingriff gesetzlich vorgesehen und war er erforderlich im Sinne des Artikels 10 Abs. 2 der Konvention?*

I. Kein Eingriff in das Recht auf Freiheit der Meinungsäußerung

- 49 Im Gegensatz zur Auffassung der Beschwerdeführer stellt die Verpflichtung aus § 111 TKG im Hinblick auf Artikel 10 der Konvention schon keinen Eingriff in die dort geschützten Rechte dar.
- 50 Artikel 10 der Konvention schützt das Recht auf freie Meinungsäußerung und damit das Recht eigene und andere Ideen und Informationen mitzuteilen, ohne daran durch den Staat gehindert zu werden. In diese Freiheit wird durch die Verpflichtung des Anbieters von Telekommunikationsdiensten, bestimmte persönliche Daten zu speichern, nicht eingegriffen. Die Beschwerdeführer haben nicht geltend gemacht, dass die Bundesrepublik Deutschland sie in irgendeiner Weise daran gehindert habe, eine Äußerung mitzuteilen oder zu verbreiten.

- 51 In ihrer Beschwerde behaupten die Beschwerdeführer auch lediglich, § 111 TKG greife abstrakt in ihr Recht „auf anonyme Meinungsäußerung“ ein. Ein solches Recht existiert nach der Konvention nicht. Es lässt sich auch nicht aus der Rechtsprechung des Gerichtshofs herleiten; das haben die Beschwerdeführer in ihrer Beschwerde auch gar nicht versucht. Stattdessen führen sie Rechtsprechung des Supreme Court der USA zur dortigen Verfassung an. Eine solche Diskussion über die Bedeutung anonymer Meinungsäußerung mag rechtspolitisch interessant sein. Sie ist aber nicht geeignet, den vom Gerichtshof seit langem klar definierten Inhalt von Artikel 10 der Konvention zu verändern. Die Angabe von Name, Anschrift und Geburtsdatum beim Erwerb einer Telefonkarte hindert niemanden an der freien Meinungsäußerung im Sinne des Artikels 10 der Konvention.
- 52 Wenn man im Sinne der Beschwerdeführer aus Artikel 10 ein Recht auf anonyme Meinungsäußerung konstruieren wollte, so würde dies den Sinngehalt von Artikel 10 deutlich verändern. Eine solche Konstruktion ginge nach Auffassung der Bundesregierung über das hinaus, was als dynamische Interpretation der Konvention bezeichnet werden könnte.
- 53 Selbst wenn man einer solchen Konstruktion folgen wollte, wäre hier aber schon zweifelhaft, ob ein Eingriff in die Rechte aus Artikel 10 der Konvention vorläge. Wie bereits oben ausgeführt wurde, schließt § 111 TKG anonyme Kommunikation gerade nicht völlig aus. Er führt lediglich dazu, dass durch die Identifizierbarkeit des Anschlussinhabers bei der Kommunikation über Mobilfunkkarten den Behörden generell Ansätze für die Ermittlung des tatsächlichen Nutzers eingeräumt werden. Dies kann jedoch nur unter engen, rechtsstaatlich kontrollierten Voraussetzungen geschehen. Die Verbreitung anonymer Meinungsäußerungen auch über das Internet bleibt aber grundsätzlich möglich.
- 54 Einen Bezug zu konkreten Meinungsäußerungen, die von Artikel 10 geschützt würden, haben die Beschwerdeführer nicht vorgetragen. Der Gerichtshof setzt aber in seiner Rechtsprechung – insbesondere bei der Prüfung der Frage, ob ein Eingriff in das Recht auf freie Meinungsäußerung nach Artikel 10 Abs. 2 der Konvention gerechtfertigt ist – den Bezug auf eine konkrete Meinungsäußerung voraus. Denn für die Frage, ob ein Eingriff in dieses Recht in einer demokratischen Gesellschaft notwendig war, berücksichtigt der Gerichtshof in ständiger Rechtsprechung die konkreten Umstände des Einzelfalls; dazu zählen vor allem Art, Gegenstand und Inhalt der Äußerung und der Zusammenhang, in dem sie gefallen ist. Wo kein Bezug zu einer konkreten Meinungsäußerung besteht, lassen sich diese Kriterien für die mögliche Rechtfertigung nicht anwenden. Mangels eines solchen Bezuges liegt kein Eingriff in das Recht auf freie Meinungsäußerung vor. Ein Recht auf anonyme Meinungsäußerung gerade über eine Mobilfunkkarte existiert nicht.

- 55 Schließlich ist auch hier die Argumentation des Gerichtshofs aus K.U. vs. Finnland (s. oben Randnummer 8 von Interesse. Hier hielt der Gerichtshof es schon für offen, ob alle Äußerungen den Schutz des Artikel 10 der Konvention verdienen (Nr. 49). Vor allem aber hat der Gerichtshof hier betont, dass ein absoluter Vorrang der Vertraulichkeit bzw. Anonymität nach der Konvention nicht in Frage kommt. Dass Ermittlungen wegen eines absoluten Vorrangs der Vertraulichkeit nicht möglich waren, stellte gerade einen Verstoß gegen die Konvention dar. Auch das zeigt, dass es im Gegensatz zur Ansicht der Beschwerdeführer keinen Anspruch auf absoluten Vorrang der Gewährleistung anonymer Kommunikation geben kann.

F. Antrag

- 56 Ich beantrage daher die Beschwerde als unbegründet zurückzuweisen.

