

**ULRIKE DONAT**  
Rechtsanwältin

Holstenstr. 194 c  
22765 Hamburg  
Tel. 040 - 39 10 61 80  
Fax: 040 - 39 10 61 83  
Hamburger Sparkasse  
BLZ 200 505 50  
Kto-Nr. 1042-130 417  
Postbank Hamburg  
BLZ 200 100 20  
Kto-Nr. 33617-209  
Steuer-Nr.: 11-25-155-21189

U. Donat - Rechtsanwältin - Holstenstr. 194 c, 22765 Hamburg

An das  
Bundesverfassungsgericht  
Schloßbezirk 3  
76131 Karlsruhe

per Fax: 0721 / 910 1382

**Abschrift**

**Neue Anschrift ab 01.07.2008:**  
Kaiser-Wilhelm-Str. 93 VI  
20355 Hamburg  
Tel. 040 - 4118938-30  
Fax 040 - 4118938-37

11.06.2008  
28/08-Pol-do/do

### Verfassungsbeschwerde

1. der Gewerkschaft ver.di, vertreten durch den Bundesvorstand, dieser wiederum vertreten durch den Vorsitzenden Frank Bsirske und den stellvertretenden Vorsitzenden Gerd Herzberg,

(Beschwerdeführerin zu 1)

2. der Frau   


(Beschwerdeführerin zu 2)

3. der Frau 

(Beschwerdeführerin zu 3)

4. des Herrn 

(Beschwerdeführer zu 4)

5. des Herrn   


(Beschwerdeführer zu 5)

Prozessbevollmächtigte zu 1. bis 5.:

Rechtsanwältin Ulrike Donat  
Holstenstrasse 194 c, 22765 Hamburg

neue Anschrift ab 01.07.2008:  
Kaiser-Wilhelm-Str. 93 VI  
20355 Hamburg

gegen §§ 113a und 113b des Telekommunikationsgesetzes in der Fassung des Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24 EG vom 21.12.2007 (BGBl. I S. 3198 ff.).

### Inhaltsverzeichnis

|   |    |
|---|----|
| A. Vorbemerkung .....   | 3  |
| B. Sachverhalt .....  | 3  |
| C. Zulässigkeit und Annahmenvoraussetzungen .....               | 7  |
| I. Frist .....  | 7  |
| II. Grundrechtsverletzungen .....                               | 7  |
| III. Entscheidungskompetenz des Bundesverfassungsgerichts ..... | 8  |
| IV. Annahmenvoraussetzungen .....                               | 10 |
| D. Begründetheit der Verfassungsbeschwerde .....                | 10 |
| I. Grundrechtlicher Schutzbereich, Grundrechtseingriffe .....   | 10 |
| 1. Telekommunikationsfreiheit .....                             | 10 |
| 2. Koalitionsfreiheit .....                                     | 14 |
| 3. Pressefreiheit .....   | 17 |
| II. Verfassungswidrigkeit der Grundrechtseingriffe .....        | 19 |
| 1. Verletzung des Gebots der Normenklarheit .....               | 19 |
| 2. Unverhältnismäßigkeit der Vorratsdatenspeicherung .....      | 21 |
| 3. Unverhältnismäßigkeit von § 113a Abs. 6 TKG .....            | 39 |
| 4. Unverhältnismäßigkeit der Zugriffsmöglichkeiten .....        | 41 |
| E. Zusammenfassung .....  | 42 |

Namens der Beschwerdeführerinnen und Beschwerdeführer lege ich unter Vorlage besonderer Prozessvollmachten

#### Verfassungsbeschwerde

ein gegen die im Rubrum genannten Vorschriften. Ich rüge eine Verletzung des Telekommunikationsgeheimnisses (Art. 10 Abs. 1 GG), der Koalitionsfreiheit (Art. 9 Abs. 3 GG) und der Pressefreiheit (Art. 5 Abs. 1 S. 2 GG). Vollmachten liegen bei.

## A. Vorbemerkung

Die Verfassungsbeschwerde ergänzt die bereits anhängige Verfassungsbeschwerde des Herrn Prof. Dr. Christoph Gusy u. a., die sich ebenfalls gegen die angegriffenen Regelungen richtet (1 BvR 256/07; im Folgenden: Vb Gusy, zitiert nach dem im Internet veröffentlichten Text - <http://wiki.vorratsdatenspeicherung.de/images/verfassungsbeschwerde.pdf> - unter Angabe von Gliederungsnummer und Seitenzahl). Die Beschwerdeführer machen sich diese Verfassungsbeschwerde weitgehend zu Eigen und bekräftigen die darin vorgetragenen Grundrechtsverletzungen. Ihr Anliegen geht aber in einem wesentlichen Punkt darüber hinaus: Sie streiten als Gewerkschaft bzw. Gewerkschaftsmitglieder vor allem für ihre Koalitionsfreiheit. Dies Freiheitsrecht wird durch die angegriffenen Regelungen nachhaltig verletzt. Mit ihrer Verfassungsbeschwerde legen die Beschwerdeführer diese Grundrechtsverletzung im Einzelnen dar. Ohne angemessene Berücksichtigung der Koalitionsfreiheit bliebe die verfassungsrechtliche Überprüfung der angegriffenen Regelungen unvollständig.

Es wird angeregt, die vorliegende Verfassungsbeschwerde mit der anhängigen zu gemeinsamer Verhandlung und Entscheidung zu verbinden.

## B. Sachverhalt

Die Beschwerdeführerin zu 1) ist eine Gewerkschaft im Deutschen Gewerkschaftsbund. Ihr Organisationsgebiet erstreckt sich auf die Bundesrepublik Deutschland, ihr Organisationsbereich umfasst Unternehmen, Betriebe, Einrichtungen und Verwaltungen in den Bereichen Postdienste, Postbank, Telekommunikation, Handel, Banken, Versicherungen, Medien, Druck, Papier, Publizistik, Kunst, öffentliche Dienste, Transport und Verkehr. Die Beschwerdeführer zu 2 – 5 sind Mitglieder der Beschwerdeführerin zu 1). Die Beschwerdeführerin zu 2) ist Journalistin und Chefredakteurin der Zeitschrift PUBLIK, die von der Beschwerdeführerin zu 1) herausgegeben und an alle Mitglieder sowie auch öffentlich vertrieben wird. Die Beschwerdeführerin zu 3) ist Justitiarin des Bundesvorstandes der Beschwerdeführerin zu 1). Der Beschwerdeführer zu 4) ist als Rechtsschutzsekretär bei der Beschwerdeführerin zu 1) angestellt, der Beschwerdeführer zu 5) ist Arbeitnehmer bei der Telekommunikationsdienstleisterin T-online.

Mit den angegriffenen Regelungen werden alle Anbieter von Telekommunikationsleistungen (Telefon, elektronische Post, Internetzugang) verpflichtet, sämtliche Verkehrsdaten (§§ 3 Nr. 30, 96 Abs. 1 TKG) und

Standortdaten (§ 3 Nr. 19, 98 Abs. 1 TKG) ein halbes Jahr lang zu speichern, um den unverzüglichen Zugriff der staatlichen Strafverfolgungs- und Sicherheitsbehörden zu ermöglichen (§ 113a Abs. 1 – 5 TKG). Veränderungen dieser Daten durch die Dienstleister müssen dokumentiert, die Dokumentationen müssen gespeichert und für den Zugriff bereitgehalten werden (§ 113a Abs. 6 TKG). Die gespeicherten Daten sind den Strafverfolgungs- und Sicherheitsbehörden auf deren Verlangen im Rahmen der dafür geltenden gesetzlichen Bestimmungen zu übermitteln (§ 113b TKG). Die angegriffenen Bestimmungen lauten:

#### § 113 a

(1) Wer öffentlich zugängliche Telekommunikationsdienste für Endnutzer erbringt, ist verpflichtet, von ihm bei der Nutzung seines Dienstes erzeugte oder verarbeitete Verkehrsdaten nach Maßgabe der Absätze 2 bis 5 sechs Monate im Inland oder in einem anderen Mitgliedstaat der Europäischen Union zu speichern. Wer öffentlich zugängliche Telekommunikationsdienste für Endnutzer erbringt, ohne selbst Verkehrsdaten zu erzeugen oder zu verarbeiten, hat sicherzustellen, dass die Daten gemäß Satz 1 gespeichert werden, und der Bundesnetzagentur auf deren Verlangen mitzuteilen, wer diese Daten speichert.

(2) Die Anbieter von öffentlich zugänglichen Telefondiensten speichern:

1. die Rufnummer oder andere Kennung des anrufenden und des angerufenen Anschlusses sowie im Falle von Um- oder Weiterschaltungen jedes weiteren beteiligten Anschlusses,
2. den Beginn und das Ende der Verbindung nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone,
3. in Fällen, in denen im Rahmen des Telefondienstes unterschiedliche Dienste genutzt werden können, Angaben zu dem genutzten Dienst,
4. im Fall mobiler Telefondienste ferner:
  - a) die internationale Kennung für mobile Teilnehmer für den anrufenden und den angerufenen Anschluss,
  - b) die internationale Kennung des anrufenden und des angerufenen Endgerätes,
  - c) die Bezeichnung der durch den anrufenden und den angerufenen Anschluss bei Beginn der Verbindung genutzten Funkzellen,
  - d) im Fall im Voraus bezahlter anonymer Dienste auch die erste Aktivierung des Dienstes nach Datum, Uhrzeit und Bezeichnung der Funkzelle,

5. im Fall von Internet-Telefondiensten auch die Internetprotokoll-Adresse des anrufenden und des angerufenen Anschlusses.

Satz 1 gilt entsprechend bei der Übermittlung einer Kurz-, Multimedia- oder ähnlichen Nachricht; hierbei sind anstelle der Angaben nach Satz 1 Nr. 2 die Zeitpunkte der Versendung und des Empfangs der Nachricht zu speichern.

(3) Die Anbieter von Diensten der elektronischen Post speichern:

1. bei Versendung einer Nachricht die Kennung des elektronischen Postfachs und die Internetprotokoll-Adresse des Absenders sowie die Kennung des elektronischen Postfachs jedes Empfängers der Nachricht,
2. bei Eingang einer Nachricht in einem elektronischen Postfach die Kennung des elektronischen Postfachs des Absenders und des Empfängers der Nachricht sowie die Internetprotokoll-Adresse der absendenden Telekommunikationsanlage,
3. bei Zugriff auf das elektronische Postfach dessen Kennung und die Internetprotokoll-Adresse des Abrufenden,
4. die Zeitpunkte der in den Nummern 1 bis 3 genannten Nutzungen des Dienstes nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone.

(4) Die Anbieter von Internetzugangsdiensten speichern:

1. die dem Teilnehmer für eine Internetnutzung zugewiesene Internetprotokoll-Adresse,
2. eine eindeutige Kennung des Anschlusses, über den die Internetnutzung erfolgt,
3. den Beginn und das Ende der Internetnutzung unter der zugewiesenen Internetprotokoll-Adresse nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone.

(5) Soweit Anbieter von Telefondiensten die in dieser Vorschrift genannten Verkehrsdaten für die in § 96 Abs. 2 genannten Zwecke auch dann speichern oder protokollieren, wenn der Anruf unbeantwortet bleibt oder wegen eines Eingriffs des Netzwerkmanagements erfolglos ist, sind die Verkehrsdaten auch nach Maßgabe dieser Vorschrift zu speichern.

(6) Wer Telekommunikationsdienste erbringt und hierbei die nach Maßgabe dieser Vorschrift zu speichernden Angaben verändert, ist zur Speicherung der ursprünglichen und der neuen Angabe sowie des Zeitpunktes der Umschreibung dieser Angaben nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone verpflichtet.

(7) Wer ein Mobilfunknetz für die Öffentlichkeit betreibt, ist verpflichtet, zu den nach Maßgabe dieser Vorschrift gespeicherten Bezeichnungen der Funkzellen auch Daten vorzuhalten, aus denen sich die geografischen Lagen der die jeweilige Funkzelle versorgenden Funkantennen sowie deren Hauptstrahlrichtungen ergeben.

(8) Der Inhalt der Kommunikation und Daten über aufgerufene Internetseiten dürfen auf Grund dieser Vorschrift nicht gespeichert werden.

(9) Die Speicherung der Daten nach den Absätzen 1 bis 7 hat so zu erfolgen, dass Auskunftersuchen der berechtigten Stellen unverzüglich beantwortet werden können.

(10) Der nach dieser Vorschrift Verpflichtete hat betreffend die Qualität und den Schutz der gespeicherten Verkehrsdaten die im Bereich der Telekommunikation erforderliche Sorgfalt zu beachten. Im Rahmen dessen hat er durch technische und organisatorische Maßnahmen sicherzustellen, dass der Zugang zu den gespeicherten Daten ausschließlich hierzu von ihm besonders ermächtigten Personen möglich ist.

(11) Der nach dieser Vorschrift Verpflichtete hat die allein auf Grund dieser Vorschrift gespeicherten Daten innerhalb eines Monats nach Ablauf der in Absatz 1 genannten Frist zu löschen oder die Löschung sicherzustellen.

#### § 113b

Der nach § 113a Verpflichtete darf die allein auf Grund der Speicherverpflichtung nach § 113a gespeicherten Daten

1. zur Verfolgung von Straftaten,
2. zur Abwehr von erheblichen Gefahren für die öffentliche Sicherheit oder
3. zur Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes und des Militärischen Abschirmdienstes

an die zuständigen Stellen auf deren Verlangen übermitteln, soweit dies in den jeweiligen gesetzlichen Bestimmungen unter Bezugnahme auf § 113a vorgesehen und die Übermittlung im Einzelfall angeordnet ist; für andere Zwecke mit Ausnahme einer Auskunftserteilung nach § 113 darf er die Daten nicht verwenden. 2§ 113 Abs. 1 Satz 4 gilt entsprechend.

Nach bisheriger Rechtslage durften Verkehrsdaten nur zu Abrechnungszwecken und bei Störungen vorübergehend gespeichert werden (§§ 96 f., 100 TKG a. F.), Standortdaten durften nur anonymisiert und mit Einwilligung des Nutzers sowie nur für begrenzte Zwecke verarbeitet werden (§ 98 TKG a. F.). Zur praktischen Handhabung nach der al-

ten Rechtslage wird auf die eingehende Darstellung in der Vb Gusy (a. a. O. Ziff. E. 2, S. 33 ff.) verwiesen.

### **C. Zulässigkeit und Annahmenvoraussetzungen**

#### **I. Frist**

Die Verfassungsbeschwerden richten sich unmittelbar gegen die eingangs genannten Änderungen des Telekommunikationsgesetzes (TKG), die am 01.01.2008 in Kraft getreten sind (Art. 16 Abs. 1 TKGÄndG). Die Jahresfrist des § 93 Abs. 3 BVerfGG ist eingehalten.

#### **II. Grundrechtsverletzungen**

Die Beschwerdeführer machen geltend, durch die angegriffenen Regelungen selbst, gegenwärtig und unmittelbar in ihren Grundrechten verletzt zu sein. Das Gesetz wirkt ohne einen weiteren vermittelnden Akt in ihren Rechtskreis ein (vgl. BVerfGE 90, 128 <135 f.>). Sie telefonieren über das Festnetz und mit Mobiltelefonen und benutzen Internet und E-Mail-Dienste. Aufgrund der angegriffenen Regelungen müssen ihre sämtlichen Verkehrsdaten ein halbes Jahr lang beim Telekommunikationsdienstleister gespeichert werden, damit die Strafverfolgungs- und Polizeibehörden sowie die Geheimdienste jederzeit darauf zugreifen können. Diese Verpflichtung der Anbieter öffentlicher Telekommunikationsdienste beeinträchtigt die Freiheitsrechte der Beschwerdeführer mit dem Inkrafttreten des Gesetzes, ohne Zwischenschaltung weiterer staatlicher Anordnungen oder sonstiger Maßnahmen.

Die Pflicht der Telekommunikationsunternehmen zur Speicherung der Telekommunikationsdaten in dem vom Gesetz umschriebenen Umfang ergibt sich ohne besondere Vollzugsanordnung aus dem Gesetz selbst. Ein Rechtsweg zu den Fachgerichten steht den Beschwerdeführern nicht offen. Es gibt auch keine andere zumutbare Möglichkeit, gerichtlichen Rechtsschutz gegen die geltend gemachten Grundrechtsbeeinträchtigungen zu erlangen. Klagen gegen den betreffenden Telekommunikationsdienstleister müssten über den Umweg eines Vorlagebeschlusses ebenfalls vom Bundesverfassungsgericht entschieden werden. Inhaltlich könnte das angerufene Gericht der Grundrechtsbetroffenheit der Beschwerdeführer wegen ihrer Bindung an das Gesetz selbst nicht abhelfen. Der mit einer Klage gegen den Telekommunikationsdienstleister verbundene Zeitaufwand ist dem Beschwerdeführer nicht zuzumuten.

Gerügt werden Verletzungen von Art. 10 Abs. 1 GG, Art. 9 Abs. 3 GG, und Art. 5 Abs. 1 S. 2 GG. Alle Beschwerdeführer werden durch die Vorratsdatenspeicherung als Nutzer von Telekommunikationseinrichtungen in ihrem Grundrecht aus Art. 10 Abs. 1 GG, die Beschwerdeführerin zu 1) darüber hinaus als Gewerkschaft in ihrer kollektiven Koalitionsfreiheit (Art. 9 Abs. 3 GG) (vgl. etwa BVerfGE 84, 212 <224>). Die Beschwerdeführer zu 2) bis 5) sind als Mitglieder der Beschwerdeführerin zu 1) in ihrer individuellen Koalitionsfreiheit beeinträchtigt.

Die Beschwerdeführerin zu 1) und die Beschwerdeführerin zu 2) werden durch die angegriffenen Regelungen auch in ihrer Pressefreiheit (Art. 5 Abs. 1 S. 2 GG) verletzt. Die Beschwerdeführerin zu 1) verlegt die Zeitschrift ver.di-PUBLIK, die 9-mal im Jahr erscheint. Die Beschwerdeführerin zu 2) ist Chefredakteurin der Zeitschrift. Die Pressefreiheit umfasst auch den Schutz vor dem Eindringen des Staates in die Vertraulichkeit der Redaktionsarbeit sowie in die Vertrauenssphäre zwischen den Medien und ihren Informanten (BVerfGE 117, 244 <258>). Durch die angegriffenen Regelungen wird in diese Vertrauenssphäre störend eingegriffen. Redaktion und Informanten können nicht sicher sein, dass ihre Kontakte vertraulich bleiben, wenn diese ein halbes Jahr lang bei den Telekommunikationsdienstleistern gespeichert werden. Außerdem müssen sie damit rechnen, dass diese Kontakte von den verschiedensten Behörden verwertet werden, auch wenn sie an den Zugriffstatbeständen selbst nicht beteiligt sind.

### **III. Entscheidungskompetenz des Bundesverfassungsgerichts**

Der Umstand, dass die angegriffene Regelung der Umsetzung einer EG-Richtlinie dienen soll, stellt die sachliche Zuständigkeit des Bundesverfassungsgerichts jedenfalls insgesamt nicht in Frage. Zwar übt das Bundesverfassungsgericht seine Jurisdiktion über innerstaatliche Normen nach Maßgabe der Solange-II-Entscheidung nicht aus. Doch dies gilt nur für solche Regelungen, die ausschließlich auf Gemeinschaftsrecht beruhen (BVerfGE 118, 79 <95 ff.>).

Die Richtlinie 2006/24/EG ist jedoch wegen Kompetenzwidrigkeit nichtig. Der Europäische Gerichtshof ist deswegen von der Irischen Republik bereits angerufen worden (Rs. C 301/06). Die Nichtigkeitsklage wird zur Aufhebung der Richtlinie 2006/24/EG führen. Dazu beziehe ich mich auf die Ausführungen in der Vb Gusy (a.a.O. Ziff. D. III. 2 a), S. 22). Das Bundesverfassungsgericht sollte diese - vorgreifliche - Entscheidung abwarten, bevor es über die Verfassungsbeschwerde entscheidet. Andernfalls ist der Rechtsstreit insoweit gemäß Art. 234 S. 1

b, S. 3 EGV dem EuGH zur Klärung im Wege der Vorabentscheidung vorzulegen.

Zudem halten sich die angegriffenen Regelungen nur teilweise im Rahmen der gemeinschaftsrechtlichen Vorgaben: Die Richtlinie 2006/24/EG regelt nicht im Einzelnen, für welche Straftaten eine Vorratsdatenspeicherung vorzunehmen ist (vgl. Beschluss des Bundesverfassungsgerichts vom 11.03.2008 - 1 BvR 256/08 - Rz 136). Gemäß Ziff. 21 vor Art. I Richtlinie 2006/24/EG sollen die gespeicherten Daten „zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten, wie sie von jedem Mitgliedstaat in seinem nationalen Recht bestimmt werden“, zur Verfügung gestellt werden. Das Gemeinschaftsrecht gibt damit zwar dem nationalen Gesetzgeber nicht im Einzelnen vor, welche Straftaten als „schwer“ einzustufen sind. Der Begriff der „schweren Straftat“ kennzeichnet aber einen Rahmen, bei dessen Überschreitung der nationale Gesetzgeber sich nicht mehr auf seine gemeinschaftsrechtliche Verpflichtung berufen kann.

Solche Überschreitungen sind gegeben. § 113b S. 1 TKG begründet in Verbindung mit §§ 110g, 110a StPO eine Übermittlungspflicht der Telekommunikationsdienstleister auch bei Straftaten, die mittels Telekommunikation begangen werden (§ 110g Abs. 1 Nr. 2 StPO), ohne dass es auf ihre Schwere ankommt. Die Zugriffsermächtigung reicht damit bis in den Bagatellbereich einer einfachen Beleidigung am Telefon hinein. Soweit der Regelungsspielraum der Richtlinie 2006/24/EG vom Bundesgesetzgeber überschritten wird, ist das Bundesverfassungsgericht durch Gemeinschaftsrecht an einer Überprüfung nicht gehindert. Dasselbe gilt für § 113b Nr. 2 und 3 TKG, wonach der Zugriff auch zu Zwecken der Gefahrenabwehr und der Aufgaben der Geheimdienste ermöglicht wird (vgl. auch BVerfG, B. v. 11.08.2008 - 1 BvR 256/07 - Rz 136). Über die in der Richtlinie 2006/24/EG enthaltene Verpflichtung hinaus geht auch § 113a Abs. 6 TKG, der für den Fall einer Veränderung der Verkehrsdaten eine Dokumentation der Änderungen und eine Speicherung der Dokumentation zwingend vorschreibt.

Außerdem schränkt Ziff. 17 vor Art. I Richtlinie 2006/24/EG die Verpflichtung des nationalen Gesetzgebers dahin ein, dass von den Mitgliedstaaten die gemäß der Richtlinie gespeicherten Daten „nur in Übereinstimmung mit den innerstaatlichen Rechtsvorschriften und unter vollständiger Achtung der Grundrechte der betroffenen Personen an die zuständigen nationalen Behörden weitergegeben werden dürfen“. Damit wird die Umsetzungspflicht hinsichtlich der Weitergabe ausdrücklich unter den Vorbehalt der nationalen Grundrechte gestellt. Auch insoweit

wird die Entscheidungskompetenz der nationalen Gerichte im Hinblick auf die Wahrung der Grundrechte durch § 113b TKG offen gehalten.

#### **IV. Annahmeveraussetzungen**

Die Verfassungsbeschwerde ist gemäß § 93a Abs. 2 a BVerfGG zur Entscheidung anzunehmen. Ihr kommt grundsätzliche verfassungsrechtliche Bedeutung zu. Das Bundesverfassungsgericht hat die Frage, ob und unter welchen Voraussetzungen eine anlasslose, umfassende und zu den in § 113b TKG vorgesehenen Zwecken erfolgende Vorratsdatenspeicherung von sensiblen Daten, deren Erhebung in die Telekommunikationsfreiheit (Art. 10 Abs. 1 GG) eingreift, mit dem Grundgesetz vereinbar ist, noch nicht entschieden (vgl. BVerfG a.a.O. Rz 138). Außerdem ist die Verfassungsbeschwerde von allgemeiner Bedeutung. Von der grundrechtsbeschränkenden Wirkung des angegriffenen Gesetzes sind nahezu alle Einwohner der Bundesrepublik Deutschland betroffen.

#### **D. Begründetheit der Verfassungsbeschwerde**

Die angegriffenen Regelungen verletzen die Beschwerdeführer in ihrer Telekommunikationsfreiheit (Art. 10 Abs. 1 GG) und in ihrer Koalitionsfreiheit (Art. 9 Abs. 3 GG), die Beschwerdeführerinnen zu 1) und 2) außerdem in ihrer Pressefreiheit (Art. 5 Abs. 1 S. 2 GG).

#### **I. Grundrechtlicher Schutzbereich, Grundrechtseingriffe**

##### **1. Telekommunikationsfreiheit**

###### **a. Schutzbereich**

Art. 10 Abs. 1 GG begründet ein Abwehrrecht gegen das Abhören, die Kenntnisnahme und das Aufzeichnen des Inhalts der Telekommunikation sowie auch gegen die Erfassung ihrer Umstände, die Auswertung des Inhalts und die Verwendung gewonnener Daten. Die grundrechtliche Gewährleistung umfasst nicht nur den Inhalt der geführten Telefongespräche, sondern auch die näheren Umstände des Fernmeldeverhältnisses. Dazu gehört insbesondere, ob, wann, von wo aus und wie lange zwischen welchen Personen und Fernmeldeanschlüssen Fernmeldeverkehr stattgefunden hat oder versucht worden ist (vgl. BVerfGE 67, 157 <172>).

Der Schutz umfasst sämtliche mit Hilfe der verfügbaren Telekommunikationstechniken durchgeführten Übermittlungen von Informationen. Auf die konkrete Übermittlungsart (etwa über Kabel oder Funk, durch analoge oder digitale Vermittlung) und Ausdrucksform (etwa Sprache, Bilder, Töne, Zeichen oder sonstige Daten) kommt es nicht an. Das Grundrecht gewährleistet die freie Entfaltung der Persönlichkeit durch einen privaten, vor der Öffentlichkeit verborgenen Austausch von Kommunikation und schützt damit zugleich die Würde des Menschen (BVerfGE 115, 166 <182>). In den Schutzbereich von Art. 10 Abs. 1 GG fallen damit die Nutzung von Festnetz- und Mobiltelefon, E-Mail, Internet und Internettelefonie.

Geschützt wird auch die Nutzung des Internets als Medium der Massenkommunikation. Das ist der Fall, wenn etwa allgemein zugängliche Internetseiten aufgesucht werden. Zu diesem Punkt wird die Rechtslage in der Vb Gusy ausführlich dargelegt. Auf diese Ausführungen wird Bezug genommen (a.a.O., Ziff. E. 4. a) (1), S. 38 ff.). Dem Schutz des E-Mail-Verkehrs steht nicht entgegen, dass sie in der Regel unverschlüsselt, d. h. ungeschützt vor einer Einsichtnahme durch Kommunikationsmittel versandt wird. Die Möglichkeit einer Kenntnisnahme durch die Kommunikationsmittel macht sie ebenso wenig schutzlos gegen unbefugte Kenntnisnahme wie die Postkarte; außerdem sind die auch die durch Art. 10 Abs. 1 GG geschützten Verkehrsdaten der Telekommunikation den Kommunikationsmittlern ohne weiteres zugänglich (so im Ergebnis auch Vb Gusy, Ziff. E. 4. a) (1), S. 40).

Bei der Nutzung von Telekommunikationseinrichtungen ist die Kommunikation besonderen Gefährdungen der Kenntnisnahme durch Dritte ausgesetzt und unterliegt deshalb besonderem Schutz (vgl. BVerfGE 67, 157 <171f.>; 85, 386 <396>). Anders als bei einem Gespräch unter Anwesenden haben die Gesprächspartner nicht die Möglichkeit, die Rahmenbedingungen der Kommunikation allein festzulegen und dabei auch über deren Privatheit und über die beteiligten Personen selbst zu wachen. Die Kommunizierenden sind wegen der räumlichen Distanz zwischen ihnen auf einen technischen Übermittlungsvorgang angewiesen, der nicht in ihrem ausschließlichen Einflussbereich liegt. Das Risiko, dass sich Dritte Zugang zu den Inhalten und Übermittlungsdaten der Kommunikation verschaffen, ist besonders groß, wenn es vielfältige technische Möglichkeiten des Zugriffs durch Dritte gibt, wie dies gegenwärtig angesichts der Vernetzung moderner Infrastrukturen der Telekommunikation und der Einschaltung mehrerer Dienste für einen Übermittlungsvorgang typischerweise der Fall ist. Art. 10 Abs. 1 GG soll Gefahren für die Vertraulichkeit von Mitteilungen begegnen, die aus

dem Übermittlungsvorgang einschließlich der Einschaltung fremder Übermittler entstehen. Brief-, Post- und Fernmeldegeheimnis sind wesentlicher Bestandteil des Schutzes der Privatsphäre; sie schützen vor ungewollter Informationserhebung und gewährleisten eine Privatheit auf Distanz (vgl. BVerfGE 115, 166 <186>).

Das Telekommunikationsgeheimnis schützt vor einer Speicherung der Inhalte und der näheren Umstände der Verbindung, insbesondere auch der Verkehrsdaten im Sinne von § 113a TKG durch das Telekommunikationsunternehmen. Die Schutzwirkung des Art. 10 Abs. 1 GG erstreckt sich auch auf den Informations- und Datenverarbeitungsprozess, der sich an die Kenntnisnahme von geschützten Kommunikationsvorgängen anschließt, und den Gebrauch, der von den erlangten Kenntnissen gemacht wird (BVerfGE 100, 313 <359>). Insofern wird das Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG) bereits abschließend durch Art. 10 Abs. 1 GG geschützt.

Das Grundrecht umfasst auch den Schutz des Rechts auf informationelle Selbstbestimmung der Kommunikationsteilnehmer. Dieses Recht gewährleistet die aus dem Grundsatz der Selbstbestimmung folgende Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden. Es sichert seinen Trägern insbesondere Schutz gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe der auf sie bezogenen, individualisierten oder individualisierbaren Daten (BVerfGE 65, 1 <43> st. Rspr.). Soweit eine Ermächtigung sich auf staatliche Maßnahmen beschränkt, durch die der Inhalt und, wie hier, die Umstände der Telekommunikation erhoben werden, ist der Eingriff allein an Art. 10 Abs. 1 GG zu messen (vgl. BVerfG U. v. 27.02.2008 - 1 BvR 370/07 u. a. - Rz 184). Der von den Beschwerdeführern beanspruchte Schutz vor einer gesetzlich vorgeschriebenen halbjährigen Speicherung ihrer Telekommunikationsdaten wird daher in vollem Umfang durch Art. 10 Abs. 1 GG garantiert.

Die Beschwerdeführer werden durch Art. 10 Abs. 1 GG auch gegen die Pflicht der Telekommunikationsdienstleister zur Dokumentation von Anonymisierungsvorgängen und zur Speicherung dieser Dokumentation (§ 113a Abs. 6 TKG) geschützt. Die veränderten Daten können dadurch auf die ursprünglichen Verkehrsdaten des Nutzers zurückgeführt werden, die mit der Änderung bezweckte Anonymisierung wird für den behördlichen Zugriff vereitelt. Die Regelung bewirkt somit nichts anderes als die Speicherung der unveränderten Verkehrsdaten, wenn der Nutzer keinen Anonymisierungsdienst in Anspruch genommen hat. Sollte das

Bundesverfassungsgericht demgegenüber zu der Auffassung gelangen, dass der Dokumentationsvorgang selbst nicht mehr in den Schutzbereich des Art. 10 Abs. 1 GG fällt, rügen die Beschwerdeführer insoweit eine Verletzung ihres Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Das Recht der Beschwerdeführer, die von den Anonymisierungsdiensten geleistete Verarbeitung der Verkehrsdaten in Anspruch zu nehmen, fällt jedenfalls in den Schutzbereich dieses Grundrecht, das das Bundesverfassungsgericht aus dem erhöhten Schutzbedürfnis der Nutzer vernetzter Systeme und der darin stattfindenden Verarbeitungsprozesse entwickelt hat (Urteil vom 27.02.2008 - 1 BvR 370/07 u. a. - Rz 165 ff., 201 -).

Art. 10 Abs. 1 GG soll verhindern, dass der Meinungs- und Informationsaustausch mittels Telekommunikationsanlagen deswegen unterbleibt oder nach Form und Inhalt anders verläuft, weil die Beteiligten damit rechnen müssen, dass staatliche Stellen sich in die Kommunikation einschalten und Kenntnisse über die Kommunikationsbeziehungen oder -Inhalte gewinnen (BVerfGE 100, 313 <359>). Insofern umfasst der Schutzgehalt der Telekommunikationsfreiheit auch den Schutzbereich des Art. 5 Abs. 1 S. 1 GG. Einschränkungen, die die Meinungsfreiheit durch Eingriffe in das Telekommunikationsgeheimnis erleidet, sind daher im Zusammenhang mit einer Überprüfung am Maßstab des Art. 10 Abs. 1 GG mit zu berücksichtigen. Das Gewicht eines Eingriffs in das Telekommunikationsgeheimnis wird erhöht, wenn er gleichzeitig die Bildung und den Austausch von Meinungen sowie die Information aus allgemein zugänglichen Quellen beeinträchtigt. Im Übrigen scheidet eine Verletzung des Grundrechts aus Art. 5 Abs. 1 S. 1 GG aus, soweit die Betätigungen von Koalitionen und ihrer Mitglieder durch Art. 9 Abs. 3 GG als *lex specialis* geschützt sind (BVerfGE 28, 295 <310>).

#### **b. Eingriff**

Die angegriffenen Regelungen greifen in den Schutz des Telekommunikationsgeheimnisses der Beschwerdeführer ein: Ihre Verkehrs- und Standortdaten werden gegen ihren Willen gespeichert und dem Zugriff von Behörden verfügbar gemacht. Auch soweit die Daten nach einem halben Jahr gelöscht werden, ohne dass auf sie zugegriffen worden ist, wird bereits durch die Speicherung ein Einschüchterungseffekt bewirkt, der die Freiheit und Privatheit der Telekommunikationsteilnehmer beeinträchtigt (vgl. BVerfG U. v. 11.03.2008 - 1 BvR 2074/05 - Rz 62 ff.; BVerfGE 115, 320 <343>; BVerfG B. 11.03.2008 - 1 BvR 256/07 - Rz 138, 148 f.). Eine wirksame Anonymisierung Ihrer Verbindungsdaten wird ihnen verwehrt.

§§ 113a f. TKG richten sich zwar nicht unmittelbar an die Beschwerdeführer, sondern ausschließlich an Anbieter von Telekommunikationsdiensten. Diese werden verpflichtet, die Verkehrsdaten sämtlicher Kunden einschließlich der mitbetroffenen Empfänger sechs Monate zu speichern und sie auf Anfrage den zuständigen Behörden mitzuteilen. Den Diensteanbietern (§ 3 Nr. 6 TKG) bleibt aber gegenüber dem Gesetzesbefehl kein Handlungsspielraum. Die Speicherung und Übermittlung der Verkehrsdaten ist daher der öffentlichen Gewalt zuzurechnen (vgl. BVerfGE 107, 299 <313 f.>). Sämtliche Beschwerdeführer sind als Kunden der Telekommunikationsunternehmen von dieser Regelung betroffen. Speicherung und Übermittlung können die Beschwerdeführer nicht verhindern und nicht umgehen, von der Übermittlung erfahren sie nichts. Auch der Missbrauch seiner Daten bleibt dem Telekommunikationsteilnehmer verborgen.

## **2. Koalitionsfreiheit**

Die Beschwerdeführerin zu 1) wird durch die angegriffenen Vorschriften in ihrer kollektiven Koalitionsfreiheit verletzt, die Beschwerdeführerinnen zu 2) und 3) sowie die Beschwerdeführer zu 4) und 5) in der individuellen Ausprägung dieses Grundrechts.

### **a. Schutzbereich**

Als individuelles Freiheitsrecht gewährleistet Art. 9 Abs. 3 GG u. a. das Recht, einer Gewerkschaft beizutreten und durch koalitionsmäßige Betätigung die Arbeits- und Wirtschaftsbedingungen zu wahren und zu fördern, denen sie unterliegen (BVerfGE 64, 208 <213>). Dazu gehört auch das Recht, sich an Arbeitskämpfen zu beteiligen (vgl. BVerfGE 84, 212 <225>; 88, 103 <114>). Die Koalitionsfreiheit ist auch den Arbeitnehmern im öffentlichen Dienst gewährleistet, und zwar unabhängig davon, ob sie hoheitliche oder andere Aufgaben erfüllen (BVerfGE 88, 103 <114>). Dasselbe gilt für Beamte, soweit sie nicht durch Art. 33 Abs. 5 GG in ihrer Koalitionsfreiheit eingeschränkt sind und nicht streiken dürfen (s. dazu auch BVerfGE 88, 103 <113 ff.>).

Darüber hinaus schützt Art. 9 Abs. 3 GG die Koalition selbst in ihrem Bestand, ihrer organisatorischen Ausgestaltung und ihrer koalitionsmäßigen Betätigung (BVerfGE 84, 212 <224>). Der Staat muss den Koalitionen hinreichende Handlungsmöglichkeiten zur Verfügung stellen. Das gilt für ihre Binnenstruktur ebenso wie für ihre Wirksamkeit nach außen (BVerfGE 92, 365 <403>). Die Koalitionsfreiheit schützt nicht nur

die Koalitionstätigkeit im Außenverhältnis, sondern auch die Selbstbestimmung der Koalitionen über ihre eigene Organisation, das Verfahren ihrer Willensbildung und die Führung ihrer Geschäfte. In den Schutzbereich der Koalitionsfreiheit fallen damit auch Maßnahmen der Vereinigungen zur Aufrechterhaltung der Geschlossenheit nach innen und nach außen (BVerfGE 100, 214 <221>). Der Staat darf dem Selbstbestimmungsrecht der Koalitionen nur solche Schranken setzen, die zum Schutz anderer Grundrechte oder verfassungsrechtlich geschützter Güter geboten sind (BVerfGE 92, 395 <403>). Der Schutz des Art. 9 Abs. 3 GG beschränkt sich nicht auf diejenigen Tätigkeiten, die für die Erhaltung und die Sicherheit des Bestandes der Koalition unerlässlich sind; er umfasst alle koalitionsspezifischen Verhaltensweisen, wie etwa auch die Mitgliederwerbung durch die Koalition und ihre Mitglieder (BVerfGE 93, 352 <357 ff.>).

#### **b. Eingriff**

Die angegriffenen Regelungen greifen ungeachtet des Umstandes, dass sie sich unmittelbar nur an Anbieter von Telekommunikationsdienstleistungen richten, in die Koalitionsfreiheit der Beschwerdeführer ein. Dazu kann auf die obigen Ausführungen (S. 14) verwiesen werden (vgl. auch BVerfGE 107, 299 <313 f.>).

Die Vorratsdatenspeicherung greift in die kollektive Koalitionsfreiheit der Beschwerdeführerin zu 1) ein. Ihre Organisation lebt vom Kontakt mit den Mitgliedern, mit Vertrauensleuten in den Betrieben, mit Betriebs- und Personalräten. Diese Kontakte werden weitgehend über Telekommunikation abgewickelt. Dasselbe gilt für den Verkehr mit und unter den Landesverbänden. Die Verkehrsdaten zeichnen einen ganz wesentlichen Teil dieser innerorganisatorischen Kommunikation nach, bilden deren Strukturen ab, verraten Intensität und Schwerpunkte, deuten auf Verabredungen und Strategien hin und legen Kampfkraft und damit Verhandlungsgewicht bloß.

Die Beschwerdeführerin zu 1) ist eine Organisation, die in einer strukturell vorgegebenen Gegnerschaft zu den Arbeitgebern und ihren Verbänden steht. Dies macht die mit den Verkehrsdaten gegebenen Informationen besonders sensibel. Sie beeinträchtigen die Beschwerdeführerin zu 1) nicht zuletzt in ihrer Gegnerunabhängigkeit und damit in einem Wesensmerkmal, das Voraussetzung für ihre Rechtsstellung als Koalition im Sinne von Art. 9 Abs. 3 GG ist. Das gilt vor allem deswegen, weil nicht nur die Telekommunikationsdienstleister, sondern auch der gesamte öffentliche Dienst einschließlich der Ermittlungsbehörden

sowie der Geheimdienste zu den Tarifgegnern der Beschwerdeführerin zu 1) gehören. Gerade in deren Hände gelangen die Verkehrsdaten. Stehen damit die dadurch vermittelten Erkenntnisse ihren Tarifgegnern zur Verfügung, so ist eine unbefangene Nutzung von Telekommunikationseinrichtungen nicht ratsam. Die Beschwerdeführerin zu 1) wird bereits dadurch schwerwiegend in ihrer Koalitionsfreiheit beeinträchtigt.

Durch die Vorratsdatenspeicherung wird auch in den innergewerkschaftlichen Meinungs- und Willensbildungsprozess eingegriffen, indem Telefongespräche und andere durch Telekommunikation vermittelte Kontakte der Mitglieder untereinander und mit der Organisation auf Vorrat gespeichert werden. Dies betrifft auch die Beschwerdeführer zu 2) – 5) als Mitglieder der Beschwerdeführerin zu 1). Sie müssen damit rechnen, dass ihre Kontakte untereinander und mit der Beschwerdeführerin zu 1) wahrgenommen und daraus Schlussfolgerungen auf ihre Gewerkschaftszugehörigkeit sowie auf Art und Umfang ihres gewerkschaftlichen Engagements gezogen werden.

Der Eingriff wirkt sich besonders bei laufenden oder bevorstehenden Tarifauseinandersetzungen aus. Halten Telekommunikationsdienstleister die Verkehrsdaten auf Vorrat gespeichert, dann ist nicht sichergestellt, dass sie sich ihrer nicht bedienen, um ihre Arbeitnehmer als Gewerkschaftler und aktive Teilnehmer an der innergewerkschaftlichen Diskussion um Tarifziele und Arbeitskampfmaßnahmen zu identifizieren. Dies betrifft insbesondere den Beschwerdeführer zu 5) als Arbeitnehmer der Telecom. Die jüngst bekanntgewordenen Vorgänge um die Auswertung der Verkehrsdaten von Mitarbeitern und Journalisten durch ein von der Telekom beauftragtes Detektivbüro veranschaulichen dies Risiko.

Die Verkehrsdaten können durch die Arbeitgeber auch als Hinweise auf geplante Maßnahmen, etwa auf die zu bestreikenden Betriebe, auf Demonstrationen, PR-Maßnahmen oder Zeitpläne genutzt werden. Schließlich sind auch Rückschlüsse auf die Kampfstärke oder Mobilisierungsstrategien denkbar. Der Eingriff hängt nicht davon ab, ob und in welchem Maß der Arbeitgeber von seiner faktischen Zugriffsmöglichkeit tatsächlich Gebrauch macht. Die innergewerkschaftliche Kommunikation wird bereits durch die Besorgnis, dass von den Verkehrsdaten ein derartiger Gebrauch gemacht wird, nachhaltig beeinträchtigt. Allein durch diesen Einschüchterungseffekt wird anerkanntermaßen in das Grundrecht des Art. 10 Abs. 1 GG eingegriffen (BVerfGE 113, 29 <46>).

Nicht zuletzt kann sich der den Behörden der Gefahrenabwehr eingeräumte Zugriff auf die Verkehrsdaten nachteilig auf die Planung und Durchführung von Aktionen im Zusammenhang mit Tarifauseinandersetzungen oder mit anderen gewerkschaftlichen Forderungen auswirken. Unter den potentiellen Teilnehmern an derartigen Kundgebungen werden sich viele scheuen, telefonische Absprachen über ihre Beteiligung zu treffen oder einschlägige Internetseiten der Beschwerdeführerin zu 1) aufzusuchen.

Zu der durch Art. 9 Abs. 3 GG geschützten koalitionsmäßigen Betätigung gehört auch die Beratung der Mitglieder in arbeitsrechtlichen Angelegenheiten. Damit sind die Beschwerdeführerin zu 3) und der Beschwerdeführer zu 4) befasst. Insofern werden sie durch die angegriffenen Regelungen in besonderer Weise in ihrer Koalitionsfreiheit beeinträchtigt. Rechtsberatung wird auch mittels Telekommunikation erbracht. Bei laufenden Verfahren wird der Informationsaustausch zwischen den Beschwerdeführern zu 3) und 4) und mit den rechtsuchenden Mitgliedern ganz regelmäßig per Telefon oder über Fax geführt. Für die Rechtsuchenden ist die Vertraulichkeit dieser Gespräche besonders wichtig. Das gilt vor allem, soweit Rechtsrat außerhalb anhängiger Verfahren erteilt wird. Die Mitglieder sind häufig daran interessiert, dass ihr Arbeitgeber davon keine Kenntnis erhält. Müssen sie befürchten, dass dies nicht gewährleistet ist, werden sie zögern, telefonisch Kontakt mit den Rechtsschutzstellen der Beschwerdeführerin zu 1), also auch mit den Beschwerdeführern zu 3) und 4), aufzunehmen.

### **3. Pressefreiheit**

Die Beschwerdeführerin zu 1) und die Beschwerdeführerin zu 2) werden auch in ihrem Grundrecht aus Art. 5 Abs. 1 S. 2 GG verletzt. Die Pressefreiheit wird von der Telekommunikationsfreiheit nicht mit umfasst (vgl. BVerfGE 107, 299 <329>). Die Beschwerdeführerin zu 1) ist als Herausgeberin der Zeitschrift ver.di PUBLIK Trägerin dieses Grundrechts, die Beschwerdeführerin zu 2) wird als Chefredakteurin der Zeitschrift in diesem Grundrecht geschützt (vgl. BVerfGE 107, 244 <Rz 42 f.>).

#### **a. Schutzbereich**

Die Freiheit der Medien ist konstituierend für die freiheitliche demokratische Grundordnung. Eine freie Presse ist daher von besonderer Bedeutung für den freiheitlichen Staat (BVerfGE 117, 244 <258>).

Dementsprechend gewährleistet Art. 5 Abs. 1 Satz 2 GG den im Bereich von Presse und Rundfunk tätigen Personen und Organisationen subjektive Freiheitsrechte. Die Gewährleistungsbereiche der Pressefreiheit schließen diejenigen Voraussetzungen und Hilfstätigkeiten mit ein, ohne welche die Medien ihre Funktion nicht in angemessener Weise erfüllen können. Geschützt sind namentlich die Geheimhaltung der Informationsquellen und das Vertrauensverhältnis zwischen Presse und den Informanten (BVerfGE 117, 244 <259>). Dieser Schutz ist unentbehrlich, da die Presse auf private Mitteilungen nicht verzichten kann, diese Informationsquelle aber nur dann ergiebig fließt, wenn sich der Informant auf die Wahrung des Redaktionsgeheimnisses verlassen kann (BVerfGE 20, 162 <176>). Staatlichen Stellen ist es grundsätzlich verwehrt, sich Einblick in die Vorgänge zu verschaffen, die zur Entstehung von Nachrichten oder Beiträgen führen, die in der Presse gedruckt oder im Rundfunk gesendet werden. Geschützt ist auch der Kontakt zu Personen, die selbst Gegenstand der Berichterstattung sind.

Zur Presse im Sinn von Art. 5 Abs. 1 Satz 2 GG gehören auch Publikationen die im Wesentlichen gruppenintern vertrieben werden wie hier die Mitgliederzeitschrift ver.di-PUBLIK. Die freie individuelle und öffentliche Meinungsbildung, die Art. 5 Abs. 1 Satz 2 GG gewährleisten will (vgl. BVerfGE 57, 295 <319>), wird nicht nur von allgemein zugänglichen, sondern auch von gruppeninternen Publikationen gefördert. Entscheidend für den Grundrechtsschutz der Presse ist allein das Kommunikationsmedium, nicht der Vertriebsweg oder Empfängerkreis (vgl. BVerfGE 95, 28 <34 f.>). Ver.di-PUBLIK wird außerdem in gewissem Umfang auch öffentlich vertrieben und ist jedenfalls öffentlich zugänglich.

### **b. Eingriff**

Die angegriffenen Regelungen greifen in die Pressefreiheit der Beschwerdeführerinnen zu 1) und 2) ein. Das Grundrecht kann einer inländischen juristischen Person zustehen (BVerfGE 21, 271 <277 f.>; st.Rspr.). Grundrechtsträger sind alle im Pressewesen tätigen Personen (BVerfGE 117, 244 <259>).

Die Vorratsdatenspeicherung der Verbindungs- und Standortdaten ist ein Eingriff in das Grundrecht aus Art. 5 Abs. 1 Satz 2 GG. Dem Staat wird dadurch der Zugang zu Informationen über die Kommunikation der Beschwerdeführer mit Informanten ermöglicht, die die Beschwerdeführer nicht preisgeben wollen. Der freie Informationsfluss zwischen den Medien und Informanten wird bereits dadurch gefährdet, dass der In-

formant durch die Mitteilung an den Journalisten Schwierigkeiten oder Nachteile befürchtet. Solche Nachteile können aber bereits dadurch entstehen, dass den Strafverfolgungsorganen oder Sicherheitsbehörden der Zugriff auf die Verbindungs- und Standortdaten und damit auf wichtige Informationen wie die Identität des Informanten, seinen Aufenthaltsort oder ähnliche Tatsachen ermöglicht wird. Auch missbräuchliche Kenntnisnahme ist nicht auszuschließen (eingehend dazu S. 28). Durch deren befürchtete Offenlegung könnte der Informant sich von der Mitteilung an die Presse abschrecken lassen. Außerdem liegt in der Verschaffung staatlichen Wissens über die im Bereich journalistischer Recherche hergestellten Kontakte ein Eingriff in das Redaktionsgeheimnis, dem neben dem Vertrauensverhältnis der Medien zu ihren Informanten eigenständige Bedeutung zukommt (vgl. BVerfGE 107, 299 <330 f.>).

## **II. Verfassungswidrigkeit der Grundrechtseingriffe**

### **1. Verletzung des Gebots der Normenklarheit**

Die angegriffene Regelung steht teilweise mit dem Gebot der Normenklarheit nicht im Einklang. Das Bestimmtheitsgebot findet seine Grundlage im Rechtsstaatsprinzip (Art. 20, Art. 28 Abs. 1 GG; vgl. zu Art. 10 Abs. 1 GG in Verbindung mit Art. 2 Abs. 1 GG und Art. 1 Abs. 1 GG: BVerfGE 110, 33 <53 ff.>; 113, 348 <375 ff.>; 115, 320 <365>; zum Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme: U. v. 27.02.2008 - 1 BvR 370/07 u. 595/07 – Rz 208 ff.). Es soll sicherstellen, dass der demokratisch legitimierte Parlamentsgesetzgeber die wesentlichen Entscheidungen über Grundrechtseingriffe und deren Reichweite selbst trifft, dass Regierung und Verwaltung im Gesetz steuernde und begrenzende Handlungsmaßstäbe vorfinden und dass die Gerichte die Rechtskontrolle durchführen können. Außerdem muss der Betroffene die Rechtslage erkennen und sich auf mögliche belastende Maßnahmen einstellen können. Der Gesetzgeber hat Anlass, Zweck und Grenzen des Eingriffs hinreichend bereichsspezifisch, präzise und normenklar festzulegen.

Diesen Anforderungen wird § 113b TKG nicht uneingeschränkt gerecht. Darin wird geregelt, unter welchen Voraussetzungen Telekommunikationsdienstleister die gemäß § 113a TKG gespeicherten Daten weitergeben dürfen. Vorgesehen ist einmal die Weitergabe „zur Verfolgung von Straftaten“ (Nr. 1) an die zuständigen Stellen auf deren Verlangen, „so weit dies in den jeweiligen gesetzlichen Bestimmungen unter Bezug-

nahme auf § 113a TKG vorgesehen und die Übermittlung im Einzelfall angeordnet ist.“ Die einschlägige Regelung ist § 100g StPO. Voraussetzung für die Erhebung der Verkehrsdaten ist danach ein durch bestimmte Tatsachen begründeter Verdacht, dass der Betroffene „eine Straftat von auch im Einzelfall erheblicher Bedeutung“ als Täter oder Teilnehmer begangen hat. Außerdem wird „insbesondere“ auf § 100a Abs. 2 StPO verwiesen, der einen umfangreichen Straftatenkatalog enthält. Der Katalog lässt für sich genommen an Bestimmtheit nichts zu wünschen übrig. Welche Straftaten von „auch im Einzelfall erheblicher Bedeutung“ aber daneben noch den Zugriff auf die Verkehrsdaten rechtfertigen können, wird dadurch nicht klarer. Der Begriff impliziert, dass der Katalog nicht alle Straftatbestände von erheblicher Bedeutung umfasst; andernfalls hätte die Einschränkung, dass die Tat auch im Einzelfall bedeutsam sein muss, keinen Sinn. Welche Tatbestände dies sein könnten, ist - auch angesichts des Umfangs des Katalogs in § 100a Abs. 2 StPO - nicht erkennbar. Dem Normanwender bzw. den Betroffenen wird hier ein Erkenntnisprozess zugemutet, den der Gesetzgeber sich erspart hat. Mit der generalklauselartigen Erweiterung des Katalogs büßt die Norm insgesamt ihre Bestimmtheit ein. Jedenfalls entspricht sie dem Bestimmtheitsgebot insoweit nicht, als sie über die Katalogstraftaten hinaus weitere Straftaten von erheblicher Bedeutung einbezieht.

Weiterhin sieht § 113b TKG die Weitergabe der Verkehrsdaten „zur Abwehr von erheblichen Gefahren für die öffentliche Sicherheit“ vor. Darunter wird allgemein jegliche (konkrete) Gefahr für ein bedeutsames Rechtsgut verstanden, darunter der Bestand des Staates und seiner Einrichtungen, Leben, Gesundheit, Freiheit, Eigentum, nicht unwesentliche Vermögenswerte sowie andere strafrechtlich geschützte Güter (vgl. etwa § 2 Abs. 1 c) Nds. SOG v. 19.01.2005 <Nds. GVBl. S. 9>; Schenke, Polizei- und Ordnungsrecht, 5. Aufs. 2007, Rz 78). Der behördliche Zugriff auf die Verkehrs- und Standortdaten wird damit auf eine unbestimmte Vielzahl von auch minderschweren Fällen ausgedehnt und entsprechend randunscharf (vgl. dazu die Stellungnahme des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein zum Entwurf des TKG-Neuregelungs-Gesetzes vom 27.06.2007

[www.datenschutzzentrum.de](http://www.datenschutzzentrum.de) - im Folgenden: ULD -, S. 24). Die Regelung setzt zu ihrer Wirksamkeit landesrechtliche Vorschriften voraus, die einen klareren Gefahrenbegriff enthalten können, derzeit aber noch nicht erlassen sind. Insofern ist eine abschließende Entscheidung über die Bestimmtheit der Zugriffsbefugnis noch nicht möglich. Dasselbe gilt für die Verweisung auf die gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder in § 113b Nr. 3 TKG.

§ 113b Nr. 1 TKG in Verbindung mit § 100g Abs. 1 Nr. 2 StPO erlaubt den Zugriff auf die Verkehrsdaten auch zur Aufklärung von Straftaten, die mittels Telekommunikation begangen worden sind. Voraussetzung dafür ist allerdings, dass „die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht.“ Durch diese salvatorische Klausel wird der Eingriffstatbestand völlig verwischt. Der Gesetzgeber hat sich, anstatt klare Tatbestandsmerkmale zu umschreiben, auf eine Begrifflichkeit zurückgezogen, die nur durch komplexe Abschätzungen und Bewertungen operationalisiert werden kann. Das gilt bereits für die Einschätzung der „Bedeutung der Sache“. Einen Maßstab dafür gibt der Gesetzgeber nicht vor, so dass die Normkonkretisierung schon an dieser Stelle weitgehend vom Gutdünken des Anwenders abhängt. Noch weitaus komplexer ist die Klärung der Frage nach dem angemessenen Verhältnis zwischen Datenerhebung und der Bedeutung der Sache. Die Entscheidung impliziert eine Gewichtung beider Positionen unter dem Kriterium der Angemessenheit. Als gesetzliches Tatbestandsmerkmal ist dies an Unbestimmtheit nicht mehr zu überbieten.

## **2. Unverhältnismäßigkeit der Vorratsdatenspeicherung**

Die verfassungsrechtlichen Anforderungen an die Rechtfertigung von Grundrechtseingriffen hängen von Umfang und Schwere des Eingriffs ab. Greift ein Hoheitsakt gleichzeitig in mehrere Grundrechte ein, dann sind diese bei der Frage, ob die Eingriffe gerechtfertigt sind, zusammenhängend zu würdigen. Ein Eingriff ist umso umfassender und gewichtiger, je mehr Freiheitsrechte betroffen sind. In der Verfassungsbeschwerde Gusy wird zutreffend ausgeführt, dass sich die mit dem Eingriff verfolgten Gemeinwohlzwecke am gesamten Verlust an grundrechtlicher Freiheit messen lassen müssen und dass die Verhältnismäßigkeit einer Regelung davon abhängt, ob sie die Summe ihrer nachteiligen Wirkungen auf verschiedene Grundrechte aufwiegt (a.a.O. Ziff. E. 4. c), S. 45 f.). Die angegriffene Regelung greift nicht nur in die Telekommunikationsfreiheit der Beschwerdeführer einschließlich ihres Rechts auf informationelle Selbstbestimmung sondern ganz wesentlich auch in ihre Koalitionsfreiheit sowie in die Pressefreiheit der Beschwerdeführerinnen zu 1) und 2) ein. Die Regelung ist nur dann verhältnismäßig, wenn sie die Schwere und Tragweite sämtlicher Eingriffe aufwiegt.

### **a. Geschützte Rechtsgüter**

Mit der Vorratsdatenspeicherung wird nach der amtlichen Begründung „insbesondere die Gewährleistung einer wirksamen Strafverfolgung“ bezweckt. Die angegriffene Regelung sei dafür geeignet, weil sie sicherstelle, dass die relevanten Verkehrsdaten für einen bestimmten Zeitraum zu Strafverfolgungszwecken verfügbar seien, auch wenn sie von den Dienstbietern für geschäftliche Zwecke nicht oder nicht mehr benötigt würden. Die Möglichkeit, auf vorhandene Verkehrsdaten zuzugreifen, sei für eine wirksame Strafverfolgung von großer Bedeutung. Dieser Zugriff habe sich in vielen Kriminalitätsbereichen als wichtiges Ermittlungsinstrument erwiesen. Zur Aufdeckung komplexer Täterstrukturen, wie sie gerade für den internationalen Terrorismus und die organisierte Kriminalität kennzeichnend seien, und zur Aufklärung von mittels Telekommunikation begangener Straftaten sei die Kenntnis von Verkehrsdaten inzwischen weithin unverzichtbar.

Die Gewährleistung einer wirksamen Strafrechtspflege vermag für sich genommen Grundrechtseingriffe nicht zu rechtfertigen (s. dazu ausführlich Vb Gusy, Ziff. E. 4. c) (d), S. 50 ff.). Strafrechtliche Sanktionen bedürfen stets einer Rechtfertigung durch schutzwürdige Rechtsgüter (vgl. dazu etwa den Beschluss des 2. Senats des Bundesverfassungsgerichts zum Inzestverbot - 2 BvR 392/07 - vom 26.02.2008). Die Rechtfertigung strafprozessualer Eingriffsnormen hängt daher davon ab, ob sie der Aufklärung von verfassungskonform sanktionierten Straftaten dienen und, gemessen am Gewicht der damit geschützten Rechtsgüter, verhältnismäßig sind.

Die angegriffenen Regelungen dienen zweifellos der Ermittlung von verfassungskonformen Straftatbeständen, die u. a. auch den Schutz hochrangiger Rechtsgüter bezwecken. Diese ergeben sich im Wesentlichen aus § 110g StPO in Verbindung mit § 100a Abs. 2 StPO. Dort werden Straftaten aufgezählt, die u. a. dem Staatsschutz, der Landesverteidigung, dem Schutz von Leib und Leben der Bürger, ihrem Eigentum und Vermögen, der Abgabehoheit des Staates, der Einwanderungskontrolle sowie der Einschränkung einer Verbreitung von Kriegswaffen dienen. § 100g StPO gestattet darüber hinaus auch den Zugriff auf die gespeicherten Verkehrsdaten bei Straftaten, die mittels Telekommunikation begangen werden. Damit gerät auch u. a. auch der Schutz der persönlichen Ehre in den Kreis der geschützten Rechtsgüter. Außerdem soll die Regelung dem Schutz vor erheblichen Gefahren für die öffentliche Sicherheit dienen. Schließlich sind auch der Schutz vor verfassungsfeindlichen Bestrebungen, der Schutz vor Spionage (BND) und vor der

Ausspähung von militärischen Geheimnissen (MAD) in Rechnung zu stellen.

Für die in § 113a TKG geregelte Pflicht zur Speicherung sämtlicher Verkehrsdaten kann von einer Einzelwürdigung sämtlicher Schutzgüter abgesehen werden. Diese Regelung dient der Strafverfolgung für alle einbezogenen Straftatbestände sowie zur Abwehr erheblicher Gefahren für die öffentliche Sicherheit, für die verfassungsmäßige Ordnung, für den Bestand der Bundesrepublik Deutschland und für die Geheimnisse der Bundeswehr. Dies sind Rechtsgüter von hohem verfassungsrechtlichem Gewicht (vgl. BVerfGE 115, 320 <346>). Die Verhältnismäßigkeit des § 113a TKG hängt deswegen nicht davon ab, ob durch die Regelung auch weniger gewichtige Rechtsgüter geschützt werden.

### **b. Eignung**

Durch die Vorratsdatenspeicherung wird die Möglichkeit eröffnet, beim Auftreten des Verdachts einer Straftat oder von Hinweisen auf das Vorliegen einer Gefahr in jedem Fall auch rückwirkend die Verkehrsdaten der Betroffenen abzurufen und auszuwerten. Dass dies zur Aufklärung von Straftaten und zur Abwehr der Gefahren beitragen kann, ist ohne weiteres plausibel und soll hier nicht in Frage gestellt werden. Die Eignung scheitert auch nicht daran, dass sie im Vergleich zu ihrer allumfassenden Streubreite nur in ganz wenigen Fällen zu „Treffern“ führt (vgl. BVerfGE 115, 320 <345>; 100, 313 <374>).

### **c. Erforderlichkeit**

Die Vorratsdatenspeicherung soll den Zugriff von Ermittlungs- und Gefahrenabwehrbehörden sowie von Geheimdiensten auf die Verkehrsdaten in den Fällen ermöglichen, in denen sie bereits von den Telekommunikationsdienstleistern gelöscht worden sind. Ein milderer Mittel, das diesen Zweck in gleicher Weise erfüllt, könnte darin liegen, die Vorratsdatenspeicherung im Sinne eines „quick freeze“ schon bei einer Verdachtsschwelle unterhalb des § 110g Abs. 1 StPO vorzusehen, d. h. bei einschlägigen Vermutungen, die Anlass zu besonderer Achtsamkeit und Beobachtungen geben, oder bei Anzeigen, die noch keinen konkreten Anfangsverdacht begründen (vgl. dazu Meyer-Goßner, StPO, 50. Aufl. 2007, § 152 Rz 4). Mit einer Speicherung der Verkehrsdaten im Vorfeld eines Anfangsverdachts könnte einem Verlust der Daten in einschlägigen Fällen wirksam begegnet werden, die Zahl der Betroffenen würde in drastischer Weise gesenkt. Die vorgelagerte Verdachtsschwelle müsste allerdings eindeutig und nachvollziehbar definiert werden.

#### **d. Verhältnismäßigkeit im engeren Sinne**

Die in § 113a TKG vorgesehene Vorratsdatenspeicherung erweist sich jedenfalls in Abwägung mit den betroffenen Grundrechten als unzumutbar. Das Gebot der Verhältnismäßigkeit im engeren Sinne verlangt, dass die Schwere des Eingriffs bei einer Gesamtabwägung nicht außer Verhältnis zu dem Gewicht der ihn rechtfertigenden Gründe stehen darf (BVerfGE 115, 320 <345> st. Rspr.). Dabei spielt auf grundrechtlicher Seite eine Rolle, unter welchen Voraussetzungen welche und wie viele Grundrechtsträger wie intensiven Beeinträchtigungen ausgesetzt sind. Die Intensität der Beeinträchtigungen hängt davon ab, ob die Gesprächsteilnehmer als Personen anonym bleiben, welche Gespräche und welche Inhalte erfasst werden können und welche Nachteile ihnen aufgrund der Überwachungsmaßnahmen drohen oder von ihnen nicht ohne Grund befürchtet werden. Auf Seiten der Gemeinwohlinteressen ist das Gewicht der Ziele und Belange maßgeblich, denen die Vorratsdatenspeicherung dient. Es hängt unter anderem davon ab, wie groß die Gefahren sind, die mit Hilfe der Fernmeldeüberwachung erkannt werden sollen, und wie wahrscheinlich ihr Eintritt ist (vgl. BVerfGE 100, 313 <376>).

#### **e. Gewicht der geschützten Rechtsgüter**

Das Gewicht der geschützten Rechtsgüter ist höchst unterschiedlich. Der Katalog der strafrechtlich geschützten Rechtsgüter umfasst neben höchstrangigen wie Leib und Leben der Bürger, Bestand der Bundesrepublik Deutschland, Kriegsgefahr, Landesverteidigung usw. auch weniger gewichtige wie u. a. die Abgabehoheit, Lenkung der Einwanderung, Drogenmissbrauch. In vielen Fällen ist der Schutz auf besonders gefährliche Begehungsformen beschränkt, wie etwa bandenmäßiges, geschäftsmäßiges oder sonst wie organisiertes Handeln. Schlusslicht in der Rangfolge der strafrechtlich geschützten Rechtsgüter ist die persönliche Ehre bei Beleidigungen am Telefon.

Mit § 113b Nr. 2 und 3 TKG wird die Vorratsdatenspeicherung in den Dienst weiterer schützenswerter Rechtsgüter gestellt. Die „Abwehr erheblicher Gefahren für die öffentliche Sicherheit“ umfasst jedenfalls den Schutz von Leben, Freiheit und Gesundheit der Bürger sowie andere strafrechtlich geschützte Rechtsgüter (s. oben D. II. 1, S. 20). Die näheren Einzelheiten müssen zwar erst noch durch die Bundesländer festgelegt werden. Doch lässt sich schon jetzt feststellen, dass § 113b Nr. 2 TKG jedenfalls auch hochrangigen Rechtsgütern zu dienen bestimmt

ist. Allerdings fallen unter den Begriff der öffentlichen Sicherheit auch weniger gewichtige Rechtsgüter wie z.B. die Leichtigkeit und Sicherheit des Straßenverkehrs bei Versammlungen, Störungen des Eigentums, sowie leichte Ordnungswidrigkeiten.

Dasselbe gilt für § 113b Nr. 3 TKG. Die dort genannten Aufgaben der Geheimdienste bestehen in der Abwehr von Gefahren für den Bestand und die Sicherheit der Bundesrepublik Deutschland. Auch insoweit ist von höchstrangigen Rechtsgütern auszugehen, unabhängig davon, dass die einzelgesetzlichen Rechtsgrundlagen noch nicht geschaffen worden sind.

#### **f. Gewicht der Grundrechtseingriffe**

Für die Bemessung des Gewichts des Eingriffs in die Telekommunikationsfreiheit, die das Recht auf informationelle Selbstbestimmung einschließt, ist u. a. bedeutsam, wie viele Grundrechtsträger wie intensiven Beeinträchtigungen ausgesetzt sind und unter welchen Voraussetzungen dies geschieht, insbesondere ob diese Personen hierfür einen Anlass gegeben haben (vgl. BVerfGE 115, 320 <347>; vgl. auch U. v. 11.03.2008 - 1 BvR 2047/05 und 1 BvR 1254/07 - Rz. 169 ff.). § 113a TKG schreibt die Vorratsdatenspeicherung der Verkehrsdaten sämtlicher Telekommunikationsteilnehmer in Deutschland vor, ohne dass hierfür ein besonderer Anlass gegeben zu sein braucht. Betroffen sind nicht nur die Nutzer von Telefonanschlüssen des Festnetzes, sondern auch die Nutzer von Mobiltelefonen und des Internets. Die Eingriffe treffen mithin praktisch alle Einwohner der Bundesrepublik Deutschland. In Verbindung mit den durch § 113b TKG eröffneten Zugriffsmöglichkeiten handelt es sich um eine verdachtsunabhängige Fahndungsmaßnahme „ins Blaue hinein“, ergänzt um eine alle Bürger erfassende geheimdienstliche und polizeiliche Überwachung ohne den geringsten Anhaltspunkt für einschlägige Gefahrenbestände.

Das Bundesverfassungsgericht hat die heute in § 5 G10 vorgesehene verdachtlose Telefonüberwachung bestimmter internationaler Telekommunikationsbeziehungen durch den BND nur deswegen als gerechtfertigt angesehen, weil sie ausschließlich der Auslandsaufklärung im Hinblick auf bestimmte außen- und sicherheitspolitisch relevante Gefahrenlagen diene, bei denen es um die äußere Sicherheit der Bundesrepublik gehe, vom Ausland her entstehende Gefahrenlagen und nicht vornehmlich personenbezogene Gefahren- und Verdachtssituationen ihren Gegenstand ausmachten und entsprechende Erkenntnisse anderweitig nur begrenzt zu erlangen seien. Es fügt aber hinzu:

„Zwar würden selbst die großen Gefahren, denen mit Hilfe der Fernmeldeüberwachung begegnet werden soll, eine Überwachung der Telekommunikation zu Zwecken der Auslandsaufklärung ohne jegliche Voraussetzungen und Begrenzungen verfassungsrechtlich nicht rechtfertigen. Das Gesetz hat aber auf solche Voraussetzungen nicht verzichtet. Zu den materiellen Voraussetzungen gehört insbesondere, dass nur Nachrichten über Sachverhalte gesammelt werden dürfen, deren Kenntnis zur rechtzeitigen Erkennung der Gefahrenlagen notwendig ist. Verfahrensrechtlich setzen Bestimmung und Anordnung unter anderem die schlüssige Darlegung im Antrag des Bundesnachrichtendienstes voraus, warum die betroffenen Fernmeldeverkehrsbeziehungen rechtzeitig Aufschluss über eine der relevanten Gefahren geben könnten. Unter Berücksichtigung der Sicherungen, die im G 10 getroffen sind, erscheint die Erfassung und Aufzeichnung für die Zwecke der Unterrichtung der Bundesregierung nicht unangemessen. Die Zahl der erfassten Telekommunikationsbeziehungen ist zwar nicht gering, verglichen mit der Gesamtzahl aller oder auch nur der internationalen Fernmeldekontakte aber vergleichsweise niedrig. Dabei kommt insbesondere dem in § 3 Abs. 2 Satz 2 G 10 enthaltenen Verbot der gezielten Überwachung bestimmter individueller Anschlüsse Bedeutung zu. Ohne ein solches Verbot wäre die Verhältnismäßigkeit angesichts der Verdachtslosigkeit der Eingriffe, der Breite der erfassten Fernmeldekontakte und der Identifizierbarkeit der Beteiligten nicht gewahrt.“ (BVerfGE 100, 313 <383 f.>).

§ 113a TKG sieht demgegenüber eine allumfassende, verdachtsunabhängige 6-monatige Vorratsdatenspeicherung ohne jede Beschränkung auf bestimmte Gefahrenlagen und ohne verfahrensrechtliche Voraussetzungen vor. Nach den genannten Vorgaben des Bundesverfassungsgerichts kann ein Eingriff von solchem Gewicht selbst durch Gefahren von der Größenordnung eines bewaffneten Angriffs auf die Bundesrepublik Deutschland nicht aufgewogen werden.

Es kommt hinzu, dass die Verkehrs- und Standortdaten weitaus aussagekräftiger sind als die lediglich nach bestimmten Suchwörtern überprüfte Telefonüberwachung nach dem G 10. Die hohe Aussagekraft dieser Daten ergibt sich aus den folgenden Umständen: Heute verfügt praktisch jeder Haushalt über einen Telefonanschluss, und die meisten Bürger bis hin zu Schulkindern tragen ein Mobiltelefon ständig bei sich. Infolgedessen erfolgt ein ganz erheblicher Teil der privaten und geschäftlichen Kommunikation über das Telefon. Aus der Gesamtheit der

Kommunikationsdaten, die für die Anschlussnummer einer Person gespeichert sind, lassen sich insbesondere Informationen über das soziale Umfeld gewinnen, sogar begrenzte Rückschlüsse auf die Gesprächsinhalte sind möglich (BVerfGE 107, 299 <320>): Die gespeicherten Verkehrsdaten verraten umstandslos und flächendeckend, wer mit wem mit welcher Intensität Umgang pflegt, ob dies im Verlauf des Tages oder überwiegend in den Abend- und Nachtstunden geschieht, ob es sich um Wochenend- oder Ferienkontakte handelt, ob überwiegend Kurzgespräche geführt werden, die auf technische Verständigung oder Verabredungen hindeuten, oder ob ausführlich geplaudert oder verhandelt wird. Erkennbar ist auch von welchem Standort aus und wohin telefoniert oder sonst wie auf elektronischen Wege kommuniziert wird. Erkenntnisse über das politische oder gewerkschaftliche Engagement der Bürger lassen sich damit aus den Verkehrs- und Standortdaten leicht ablesen, ebenso Beziehungen zu religiösen Sekten, Geheimnisträgern oder Presseorganen. Telefonkontakte mit Ärzten geben Aufschluss über gesundheitliche Probleme. Offengelegt werden allein durch die Verkehrsdaten auch prekäre Einzelheiten aus der Intimsphäre, sei es die Beziehung zu einer oder einem heimlichen Geliebten, sei es die Inanspruchnahme von Telefonsexdiensten oder eine Kontaktaufnahmen mit Prostituierten („Callgirls“), wodurch gegebenenfalls auch Erkenntnisse über ausgefallene sexuelle Neigungen preisgegeben werden. Sartre legt Jupiter, dem Gottvater der Antike, das Geständnis in den Mund, dass selbst die Götter ihre „schmerzlichen Geheimnisse“ haben (Jean-Paul Sartre, „Die Fliegen“, 1. Akt). Das Arkanum des Menschen, das diese Geheimnisse birgt, ist als der Kernbereich privater Lebensgestaltung durch Art. 1 Abs. 1 GG absolut geschützt. Die Verkehrsdaten legen es bloß.

In der Vb Gusy wird die Sensibilität der Verkehrs- und Standortdaten eingehend dargelegt. Darauf kann hier verwiesen werden (a.a.O. Ziff. E. 4. c) (ff), S. 80 ff.). Besonders eindrucksvoll sind die Ergebnisse einer Studie des US-amerikanischen Forschungszentrums MIT, die in der Vb Gusy (a.a.O. Ziff. E. 4. c) (d) (ff) (ii), S. 82) wie folgt wiedergegeben werden:

„In einem Versuch des ... MIT wurden Telekommunikationsverbindungsdaten und auf 10 m genaue Standortdaten von 100 Versuchspersonen erhoben. Mit Hilfe dieser Daten gelang es, mit einer 90%igen Genauigkeit, die Arbeitskollegen, Bekannten und Freunde einer jeden Person zu identifizieren. Ferner waren umfangreiche Vorhersagen möglich. Anhand der Bewegungsdaten einer Person während eines Monats konnte mit 95%iger Genauig-

keit vorhergesagt werden, wann sich die Person am Arbeitsplatz, zu Hause oder an einem anderen Ort aufhalten würde. Weiter konnte mit 90%iger Genauigkeit vorhergesagt werden, ob sich zwei Personen innerhalb der nächsten Stunde begegnen würden. Anhand der Aktivitäten einer Person während der ersten 12 Stunden eines Tages konnten die Aktivitäten während der verbleibenden 12 Stunden mit etwa 80%iger Genauigkeit vorhergesagt werden. Auch die Zufriedenheit am Arbeitsplatz konnte anhand der Daten vorhergesagt werden. Die weitere Forschung arbeitet daran, das Verhalten großer Organisationen anhand solcher Kommunikations- und Standortdaten vorherzusagen.“

Das Gewicht dieses Eingriffs wird auch nicht dadurch gemildert, dass die Telekommunikationsdienstleister auch bisher schon zur Speicherung der Verkehrsdaten für Abrechnungszwecke befugt waren; denn diese Einschränkung beeinträchtigte die informationelle Selbstbestimmung schon deswegen nicht, weil jeder Benutzer sich ihr durch die Vereinbarung einer Pauschalabrechnung (flat-rate) entziehen konnte. Insofern konnte eine Speicherung nicht gegen seinen Willen geschehen, sie hielt sich im Rahmen seiner informationellen Selbstbestimmung. Außerdem bestand die Möglichkeit, den Zugang zu den Verkehrsdaten durch die Inanspruchnahme von Anonymisierungsdiensten zu verhindern. Diese Möglichkeit wird durch § 113a Abs. 6 TKG weitgehend versperrt.

Ins Gewicht fällt auch die Gefahr eines Missbrauchs der gespeicherten Verkehrsdaten (vgl. BVerfGE 65, 1 <45 f.>). Es gibt keine absolute Sicherheit vor illegalen Zugriffen auf die gespeicherten Daten. Durch die massenhafte Speicherung von Verkehrs- und Standortdaten wird das Risiko eines Datenmissbrauchs drastisch erhöht. Das Grundrecht soll den Einzelnen auch vor fehlerhafter, missbräuchlicher oder exzessiver Verwertung von Kommunikationsdaten durch die Post oder andere staatliche Stellen schützen (BVerfGE 85, 386 <397>).

Die Befürchtung, dass die Verkehrs- und Standortdaten von den Polizei- und Sicherheitsbehörden zur Überwachung missliebiger Personen benutzt werden, ist nicht von der Hand zu weisen. Auch die Mitarbeiter der Behörden sind nicht gegen die Versuchung zum Geheimnisbruch gefeit. Dies wird durch den vom Bundesverfassungsgericht entschiedenen Fall „Cicero“ veranschaulicht (BVerfGE 117, 244). Ein besonderer Risikofaktor sind die gemäß § 110 TKG einzurichtenden Überwachungsschnittstellen. Sie können vor einem Eindringen Privater („Hacker“), vor allem aber auch ausländischer Geheimdienste kaum wirksam

geschützt werden (vgl. dazu ausführlich Vb Gusy, Ziff. E. 4 c) (d) (ff) (v), S. 91 ff.).

Von einer missbräuchlichen Nutzung ihrer Verkehrsdaten können etwa Globalisierungsgegner betroffen sein oder Personen, die auf Demonstrationen aufgefallen sind. Der Einschüchterungseffekt ist für Bürger, die sich durch lautstarke öffentlichkeitswirksame Anteilnahme am politischen Geschehen missliebig gemacht haben, besonders groß. Sie werden von ihrer Telekommunikationsfreiheit keinen unbefangenen Gebrauch mehr machen, wenn es bei der Vorratsdatenspeicherung bleibt. In der Vb Gusy werden dazu weitere Ausführungen gemacht, auf die hier Bezug genommen wird (a.a.O. Ziff. E. 4. c) (d) (ff) (iv), S. 90 f.).

Eine missbräuchliche Verwendung droht auch von Privaten. Das Risiko eines Missbrauchs der Verkehrsdaten durch Dritte, die sich unbefugt Zugang zu ihnen verschaffen ist nicht auszuschließen (vgl. BVerfG B.v.27.10.2006 - 1 BvR 1811/99 -). Das gilt zunächst für die Telekommunikationsunternehmen selbst, die sich leicht Zugang zu den gespeicherten Daten verschaffen können. Die Telekom hat sich der bei ihr gespeicherten Verkehrsdaten, wie gerichtsbekannt sein dürfte, in den vergangenen Jahren in reichlichem Maße bedient (vgl. etwa DER SPIEGEL Nr. 23/08 S. 20 ff.). Die Deutsche Bahn wird in der Presse eines ähnlichen Missbrauchs verdächtigt. Sicherer Schutz dagegen gibt es nicht. Inwieweit die Strafdrohung des § 206 StGB greift, dürfte wohl in erster Linie vom (finanziellen) Anreiz und vom Entdeckungsrisiko abhängen.

An Anreizen für den unerlaubten Zugriff auf die gespeicherten Verkehrs- und Standortdaten fehlt es nicht. Für die Telekom war anscheinend der Ärger über undichte Stellen in der Chefetage ein hinreichendes Motiv, in flagrant rechtswidriger Weise auf die Verkehrsdaten auch von Journalisten zuzugreifen. Erkenntnisse aus dem Privatleben von Prominenten aus Politik und Gesellschaft versprechen hohen Gewinn, weil die Sensationspresse entsprechende Indiskretionen gern und lukrativ vermarktet und weil sie von politischen und geschäftlichen Gegnern als Waffe gebraucht werden. Die Folge ist häufig eine ruinöse gesellschaftliche Ächtung, die meist mit dem Verlust angesehener Positionen einhergeht. Die jüngst - anscheinend gegen die Zahlung hoher Geldbeträge - den Ermittlungsbehörden zugänglich gemachten Datenbestände aus Staaten mit besonders streng gehütetem Bankgeheimnis veranschaulichen die Vergeblichkeit aller Bemühungen um Datensicherheit. In Italien haben Mitarbeiter der Telekommunikationsdienstleister über längere Zeiträume hinweg zahlreiche Telefongespräche gezielt abgehört und damit einen öffentlichen Skandal ausgelöst.

Die Vorratsdatenspeicherung beeinträchtigt die Telekommunikationsfreiheit durch den von ihr ausgehenden Abschreckungs- bzw. Einschüchterungseffekt. Alle Telekommunikationsteilnehmer müssen in Zukunft damit rechnen, dass jeder telefonische Kontakt und jede Internetverbindung ein halbes Jahr lang bei seinem Dienstleister gespeichert wird und dem Zugriff von Strafverfolgungsbehörden, Polizei und Geheimdiensten unterliegt. Niemand kann mehr sicher sein, dass er nicht durch ein Telefongespräch als Unbeteiligter ins Visier der Behörden gerät oder dass er sich durch das Aufrufen einer Internetseite, durch Zugang zu einer home-page oder einem chat-room verdächtig macht oder Indiskretionen ausgesetzt wird. In der Folge und in dem Maße, in dem die Vorratsdatenspeicherung ins allgemeine Bewusstsein dringt, wird sich diese Unsicherheit auf die Wahrnehmung der Telekommunikationsfreiheit auswirken. Das Vertrauen in das Telekommunikationsgeheimnis wird weiter schwinden.

Besonders schwerwiegend wirkt sich der Einschüchterungseffekt für die Wahrnehmung der individuellen Koalitionsfreiheit aus: Arbeitgeber wollen bekanntlich gern wissen, welche Arbeitnehmer einer Gewerkschaft angehören. Diese haben andererseits ein erhebliches praktisches Interesse daran, dass dies dem Arbeitgeber nicht zur Kenntnis gelangt. Daher werden sie Telekommunikationskontakte, die auf ihre Mitgliedschaft oder koalitionsmäßige Aktivitäten hindeuten, tunlichst vermeiden, wenn sie damit rechnen müssen, dass diese Kontakte ein halbes Jahr lang auf Vorrat bei ihrem Telekommunikationsdienstleister gespeichert werden. Besonders gewichtig ist der Eingriff insoweit gegenüber dem Beschwerdeführer zu 5), der bei einem Telekommunikationsdienstleister angestellt ist. Er kann niemals sicher sein, dass seine Telekommunikationskontakte mit der Beschwerdeführerin zu 1) oder mit anderen Gewerkschaftsmitgliedern nicht von seinem Arbeitgeber systematisch erfasst und ausgewertet werden. Dadurch ist er in seiner koalitionsmäßigen Betätigung in besonders schwerwiegender Weise betroffen.

Um Tarifverhandlungen erfolgreich zu führen, muss in den jeweiligen Beschäftigungsgruppen unter Beteiligung der Beschwerdeführerin zu 1) eine intensive Diskussion über Probleme des Arbeitseinsatzes und der zeitlichen und sonstigen Belastung, über die Notwendigkeit neuer oder veränderter tariflicher Regelungen sowie über Verhandlungsstrategien geführt werden. Diese für die koalitionsmäßige Betätigung unentbehrlichen Diskussionen verlaufen zwangsläufig in weiten Teilen über Telekommunikationseinrichtungen. Sie werden stark behindert, wenn Mitglieder und Mitarbeiter der Beschwerdeführerin zu 1) befürchten müssen, dass die entsprechenden Verkehrsdaten der anderen Tarifver-

tragspartei zugänglich gemacht werden. Die Beschwerdeführerin zu 1) ist insoweit exemplarisch und besonders schwer betroffen. Sie vertritt u. a. die Interessen der Arbeitnehmer in der Telekommunikationsbranche. Ihre sämtlichen Verkehrsdaten werden mithin von ihren Tarifgegnern gespeichert und bleiben ihnen jeweils für ein halbes Jahr zugänglich. Die Befürchtung, dass innergewerkschaftliche Willensbildungsprozesse durch die Arbeitgeberseite ausgespäht werden, ist daher für die Beschwerdeführerin zu 1) bei Arbeitskämpfen in besonderer Weise begründet.

Diese Beeinträchtigungen der Koalitionsfreiheit sind im Zusammenhang mit der Vorbereitung und Durchführung von Arbeitskämpfen äußerst nachhaltig. In der konfliktgeladenen Situation ist einerseits das Interesse der Arbeitnehmer an einer Geheimhaltung ihrer Aktivitäten naheliegend und dringlich, andererseits hat auch der Arbeitgeber ein gesteigertes Interesse an Informationen über die gewerkschaftliche Betätigung seiner Arbeitnehmer. Bei Arbeitskämpfen lässt sich aus ihren Verkehrsdaten ablesen, wo und wann bestimmte Arbeitskampfmaßnahmen durchgeführt werden sollen und welche Mitglieder vor Ort damit zu tun haben. Die Beschwerdeführerin kann niemals sicher sein, dass Vorbereitungen unerkannt bleiben und dass Mitglieder, die sich aktiv an Arbeitskampfmaßnahmen beteiligen, nicht vom Arbeitgeber identifiziert und in der Folge auch diskriminiert werden. Allein diese Befürchtung muss sich nachteilig auf ihre Kampffähigkeit auswirken. Sie kann die Telekommunikationseinrichtungen besonders bei Tarifauseinandersetzungen nicht mehr sorglos nutzen, obwohl sie gerade dann in besonderem Maße darauf angewiesen ist. Auch die betroffenen Mitglieder werden in dieser Situation tendenziell durch die Vorratsdatenspeicherung eingeschüchtert und damit auch in ihrer Bereitschaft zur aktiven Wahrnehmung ihrer Koalitionsfreiheit gehemmt. Für den Beschwerdeführer zu 5) gilt das in besonderer Weise. Er sieht sich als Arbeitnehmer einer Telekommunikationsdienstleisterin bei Arbeitskämpfen der Gefahr ausgesetzt, dass seine Verkehrsdaten von dieser ausgewertet werden.

Behindert wird die Beschwerdeführerin zu 1) auch in ihrer koalitionsmäßigen Betätigung in den Betriebs- und Personalräten. Die in diesen Gremien geführten Verhandlungen setzen interne Beratungen der Betriebsparteien und Personalräte voraus, die auch telefonisch und über Internetverbindungen durchgeführt werden. Allein die Möglichkeit, dass sich die Arbeitgeberseite Kenntnis der gespeicherten Verkehrsdaten verschaffen kann, beeinträchtigt diese Kommunikation. Das gilt besonders für die Beschäftigten in der Telekommunikationsbranche, deren

Arbeitgeber selbst über die Verkehrsdaten verfügen und unkontrolliert darauf zugreifen können.

Die Beschwerdeführerin zu 1) vertritt auch die Interessen der Arbeitnehmer und Beamten in den Staatsanwaltschaften und den Geheimdiensten. In diesen Dienststellen werden die abgefragten Verkehrsdaten aktenkundig. Rund 70% betreffen Dritte, die an den Anlasstaten unbeteiligt sind (Albrecht, Grafe, Kilchling, Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO, Forschungsbericht des Max-Planck-Instituts für ausländisches und internationales Strafrecht, 2008, - MPI-Gutachten - [www.vorratsdatenspeicherung.de](http://www.vorratsdatenspeicherung.de), S. 405). Angesichts der zunehmenden Zahl der Abfragen (MPI-Gutachten, S. 77) besteht daher für die Bediensteten wohl begründeter Anlass zu der Befürchtung, dass ihre Verkehrsdaten der Dienststelle zur Kenntnis gelangen. Für sie ist der Einschüchterungseffekt der Vorratsdatenspeicherung mithin besonders groß. Dadurch können sie nicht nur allgemein von einer unbefangenen Nutzung von Telekommunikationseinrichtungen, sondern auch speziell von Telekommunikationskontakten mit der Beschwerdeführerin zu 1) oder mit Kollegen im Rahmen ihrer koalitionsmäßigen Betätigung abgehalten werden.

Der Einschüchterungseffekt der Vorratsdatenspeicherung wirkt sich auch negativ auf die Mitgliederberatung in arbeitsrechtlichen Fragen aus. Die außergerichtliche Beratung von Mitgliedern gehört ebenso wie die Vertretung im gerichtlichen Verfahren zu den traditionellen Tätigkeitsbereichen der Gewerkschaften und ist als koalitionsmäßige Betätigung durch Art. 9 Abs. 3 GG geschützt (BVerfGE 88, 5 <15>). Die Beschwerdeführer zu 3) und 4) sind in diesem Aufgabenfeld tätig und insoweit auch in ihrer individuellen Koalitionsfreiheit betroffen. Das Vertrauen in die Unverletzlichkeit des Telekommunikationsgeheimnisses ist auch dabei von erheblicher Bedeutung. Arbeitnehmer werden zögern, sich in einem Konflikt mit dem Arbeitgeber telefonisch Rechtsrat bei ihrer Gewerkschaft einzuholen, wenn sie befürchten müssen, dass diese Kontakte ein halbes Jahr lang gespeichert werden und damit grundsätzlich zugänglich bleiben.

Auch der Eingriff in die Pressefreiheit der Beschwerdeführerinnen zu 1) und 2) wiegt schwer. Die Zeitschrift ver.di-PUBLIK ist ein wesentliches Instrument der Mitgliederbetreuung für die Beschwerdeführerin zu 1). Sie dient der innergewerkschaftlichen Willensbildung sowie der Werbung neuer Mitglieder. Sie unterrichtet über die Aktivitäten der Beschwerdeführerin zu 1) und über gewerkschaftliche Aktionen ihrer Mitglieder. Darüber hinaus ist sie ein Forum, auf dem Missstände in den

Betrieben und Dienststellen offen gelegt und kritisiert werden wie kürzlich etwa illegale Überwachungen des Personals in Einzelhandelsbetrieben. Das Vertrauen der Informanten und Leser in die Integrität der Telekommunikationsverbindungen gehört zu den Grundvoraussetzungen dieser Tätigkeiten. Es wird durch die Vorratsdatenspeicherung nachhaltig beeinträchtigt. Der Schutz der Pressefreiheit als Strukturvoraussetzung für eine freie Gesellschaft und auch für die Wahrnehmung der Koalitionsfreiheit ist ein Belang, dem bei der Abwägung ein besonderes Gewicht zukommt.

### **g. Abwägung**

Im Ausgangspunkt ist zunächst festzuhalten, dass zumindest ein wesentlicher Teil der durch die Vorratsdatenspeicherung geschützten Rechtsgüter auch schwerwiegende Eingriffe in die Freiheitsrechte der Bürger zu rechtfertigen vermag. Bei der Abwägung sind aber das Maß der Eignung und der Förderlichkeit einer umfassenden Vorratsdatenspeicherung einzubeziehen. Die Bedeutung der angegriffenen Regelungen für den Rechtsgüterschutz hängt ganz wesentlich davon ab, welche positiven Wirkungen von der Vorratsdatenspeicherung ausgehen und in welchem Umfang sie neben den bereits vorhandenen Schutzinstrumenten als zusätzliche Maßnahme noch erforderlich ist (vgl. auch Vb Gusy, Ziff. E. 4. c) (a), S. 46).

Zweifel am Maß der Eignung ergeben sich aus dem Umstand, dass Täter mit hinreichender krimineller Energie, Spione oder Verfassungsfeinde sich vor einer Erfassung ihrer Verbindungsdaten leicht schützen können und davon auch jetzt schon häufig Gebrauch machen. Das geschieht etwa durch den Erwerb von Kommunikationsgeräten aus dritter Hand, durch häufiges Wechseln von Mobiltelefonen oder der SIM-Karte, durch die Benutzung von öffentlichen Telefonzellen oder Internetcafés und durch technische Vorkehrungen gegen die Speicherung von Internet-Protokoll-Adressen (Sierck/Schöning/Pohl, Zulässigkeit der Vorratsdatenspeicherung nach europäischen und deutschem Recht, Deutscher Bundestag - Wissenschaftlicher Dienst, 2006, S. 13; MPI Gutachten, S. 244: Wechsel der SIM-Karte). Im Einzelnen verweise ich dazu auf die ausführlichen und gut dokumentierten Ausführungen in der Beschwerdeschrift der Vb Gusy (a.a.O. Ziff. E. 4. c) (bb) und (cc) S. 60 ff.). Die dort wiedergegebenen empirischen Erkenntnisse lassen sich wie folgt zusammenfassen:

- Es gibt bereits jetzt kostengünstige, leicht erreichbare und effektive Mittel zur anonymen Nutzung der Kommunikationsnetze. Mit

ihrer Weiterentwicklung und Verbesserung ist in naher Zukunft zu rechnen. Durch die angegriffenen Regelungen wird sich mit dem steigenden Bedarf auch das Tempo der Entwicklung von Anonymisierungstechniken beschleunigen.

- Die anonyme Nutzung von Kommunikationsnetzen lässt sich in weiten Bereichen nicht verhindern.
- Die Nutzung von Möglichkeiten anonymer Telekommunikation setzt sich gerade in kriminellen Kreisen immer weiter durch.
- Der identifizierbare Gebrauch von Kommunikationseinrichtungen beschränkt sich schon jetzt im Wesentlichen auf Kleinkriminelle, während vor allem professionelle Tätergruppen selbst aufwändige Anonymisierungsstrategien regelmäßig nutzen.
- Sowohl bei der Strafverfolgung als auch bei der Gefahrenabwehr werden die erweiterten Zugriffsmöglichkeiten durch schwerwiegende Nachteile erkauft: Die Strafverfolgung wird in die Bereiche der unteren Kriminalität abgedrängt und gerät damit in ein Gerechtigkeitsdilemma.

Außerdem wird der Nutzen der Bevorratung sämtlicher Verkehrs- und Standortdaten dadurch relativiert, dass ihre Auswertung zum Zwecke der Strafverfolgung die Gefahr von Fehlentscheidungen erhöht, so etwa, wenn der Anschluss ohne Wissen des Inhabers missbraucht wird, oder wenn die Behörden nach dem Eliminierungsprinzip vorgehen, was durch die Auswertung der Verkehrs- und Standortdaten erleichtert wird und zu einer Inflation von Verdächtigen führt. Wegen der Einzelheiten wird auf die Vb Gusy verwiesen (a.a.O. Ziff. E. 4. c) (d) (ff) (iii), S. 85).

Im Ergebnis ist festzuhalten: Als Instrument zur Aufklärung oder Verhütung schwerer Verbrechen ist die Vorratsdatenspeicherung nur bedingt geeignet. Vor allem Klein- oder Gelegenheitstätern können die Behörden mit diesem Instrument auf die Spur kommen. Eine derartig selektiv wirkende Maßnahme ist ein wenig geeignetes Mittel zur Gewährleistung einer wirksamen Strafverfolgung. Ermittlungsmethoden, die nach dem Prinzip funktionieren „die kleinen Diebe hängt man, die großen lässt man laufen“, sind einer rechtsstaatlichen Strafrechtspflege nicht dienlich. Sie diskreditieren die Strafverfolgungspraxis und wirken dem eigentlichen Zweck des Strafens entgegen, der in der Bekräftigung der Normgeltung im allgemeinen Bewusstsein liegt. Der angeführte bittere Satz aus dem Volksmund stellt gerade die Unverbrüchlichkeit der für alle geltenden Strafnormen in Frage.

Dasselbe gilt für den Aufklärungsbedarf im Bereich der Gefahrenabwehr und der Geheimdienste. Spione und aktive Verfassungsfeinde werden den Behörden durch Zugriff auf die Verkehrsdaten selten ins Netz gehen. Realistischerweise sind Aufklärungserfolge nur im Randbereich verfassungsfeindlicher bzw. verfassungskritischer Aktivitäten oder bei Amateurspitzeln zu erwarten. Damit wirkt sich dieselbe selektive Wirkungsweise hier insgesamt sogar eher kontraproduktiv aus: Wenn die Behörden vor allem Amateure erfassen, professionelle Tätergruppen aber tendenziell verfehlen, werden diese vor unliebsamer Konkurrenz geschützt, ihr Tätigkeitsfeld und Einfluss wird gestärkt. Die Ermittlungsbehörden verschaffen sich im unteren bis mittleren Unrechtsbereich publikumswirksame Erfolge. Das kann ihrer Einsatzfreude bei schwierigeren Ermittlungsaufgaben sogar abträglich sein (s. dazu Vb Gusy, a.a.O., E. 4. c) (d) (bb) (ii), S. 64 und dort FN 419).

Abgesehen davon ist eine in diesem Sinne wirksame Selektion offensichtlich ungerecht. Auch hier gilt: Denkgesetzlich lässt sich nicht leugnen, dass die Vorratsdatenspeicherung Erfolge bei der Ermittlung von Straftaten und der Gefahrenabwehr im weitesten Sinne zeitigen kann und insofern geeignet ist, dem bezweckten Rechtsgüterschutz zu dienen. Bei einer wertenden Betrachtung ergibt sich jedoch ein anderes Bild: Bei der Gefahrenabwehr wirkt sich die Verwendung der gespeicherten Verkehrsdaten negativ auf die Struktur der typischen Gefahrenherde aus, indem sie den professionell handelnden Tätern Vorteile zuschanzt. Auch wenn man die Eignung des ungeachtet im Ergebnis bejaht, können die aufgezeigten Eignungsmängel bei einer Gesamtwürdigung nicht außer Betracht bleiben.

Das Gewicht des mit der Vorratsdatenspeicherung bezweckten Schutzzwecks wird weiter dadurch verringert, dass das vorhandene Arsenal an Ermittlungs- und Gefahrenabwehrinstrumenten ausreicht, um hinreichende Sicherheit zu gewährleisten. Ob eine Speicherung aller Verkehrs- und Standortdaten überhaupt zusätzliche Ermittlungserfolge zeitigen würde, lässt sich mit letzter Sicherheit nicht beantworten. Auch bereits vor Inkrafttreten der angegriffenen Regelungen konnten die Behörden gemäß § 100g StPO bei Vorliegen eines hinreichenden Tatverdachts oder nach § 2 Abs. 1 G 10 auf die aktuellen und künftigen (§ 110g Abs. 1 S. 3 StPO) Verkehrsdaten der betroffenen Personen zugreifen. Soweit sie von den Dienstleistern aus geschäftlichen Gründen gespeichert waren, konnte auch rückwirkend zugegriffen werden.

Die vom Max-Planck-Institut für ausländisches und internationales Strafrecht vorgenommene Auswertung eines großen Datenbestandes begründet erhebliche Zweifel am Nutzen einer allgemeinen Vorratsda-

tenspeicherung für eine effektive Strafverfolgung. Die Gutachter stellen fest, dass die Löschung der Verkehrsdaten jedenfalls keine erhebliche Rolle gespielt hat. Bereits erfolgte Löschungen betrafen etwa 2% der durch die Anordnungen erfassten Anschlüsse (MPI-Gutachten, S. 254). Bei insgesamt 4% der Anschlüsse konnten die Verkehrsdaten nicht erlangt werden, weil sie nicht, nicht mehr oder nicht mehr vollständig gespeichert waren (MPI-Gutachten, S. 253). In einer unter derselben Internetadresse publizierten Anmerkung zu dem genannten Gutachten wird, ausgehend von dieser Zahl, errechnet, dass die Verfolgung von Straftaten insgesamt nur zu 0,002% durch eine Vorratsdatenspeicherung von Verkehrsdaten hätte effektiviert werden können. Bei dieser Berechnung werden die Verfahren berücksichtigt, in denen die Abfragen ergebnislos blieben, die Straftaten jedoch auf anderem Wege aufgeklärt werden konnten. In Abzug gebracht werden weiterhin die Verfahren, die selbst bei Vorliegen der angeforderten Verkehrsdaten eingestellt worden wären.

Diesem hypothetischen Ansatz und damit auch der Zahl von 0,002% mag man skeptisch gegenüberstehen, jedenfalls aber kann als Ergebnis festgehalten werden, dass eine allumfassende Vorratsdatenspeicherung - bezogen auf die Gesamtheit der verfolgten und erfolgreich abgeurteilten Straftaten - nur einen verschwindend geringen Nutzen für eine effektive Strafverfolgung verspricht. Im Regierungsentwurf zum TKG von 1996 (BT Drucks. 13/4438 S. 39) wurde seinerzeit noch eine entsprechende Forderung des Bundesrats mit folgender Begründung zurückgewiesen:

„Die Forderung des Bundesrates, neben den ‚Höchstfristen‘ auch ‚Mindestfristen‘ für die Speicherung von personenbezogenen Daten der an der Telekommunikation Beteiligten vorzusehen sowie neben den Interessen der Unternehmen und Betroffenen auch diejenigen der in Abs. 6 Nr. 1 genannten Stellen einzubeziehen, wird abgelehnt.

Damit würde (im Original ‚wurde‘) den in § 86 Abs. 1 Satz 2 normierten Grundsätzen der Verhältnismäßigkeit, Erforderlichkeit und Zweckbindung beim Erlass von Datenschutzvorschriften widersprochen. Die Verarbeitung von Telekommunikationsdaten ist regelmäßig auf den betrieblich erforderlichen Zweck der Abwicklung der jeweiligen vertraglich vereinbarten Telekommunikationsdienstleistung beschränkt. Das Anliegen des Bundesrates würde vom Ergebnis her auf eine mangels aktuellen Bedarfs unzulässige Vorratsspeicherung von Daten hinauslaufen. Die Rufnummorauskünft-

te an Strafverfolgungs- oder Sicherheitsbehörden für die Erfüllung ihrer gesetzlichen Aufgaben sind ohnehin bereits in § 87 geregelt.“

Weiterhin ist zu bedenken: Nahezu jede Erweiterung staatsanwaltlicher oder (geheim-) polizeilicher Mittel kann mit einer gewissen vordergründigen Plausibilität als „erforderlich“ hingestellt werden: Straftaten (oder Gefahrenlagen), die mit Hilfe eines neuen Instrumentariums aufgeklärt werden könnten, lassen sich leicht konstruieren. Das war bei der Rasterfahndung, dem Kennzeichenabgleich, dem Lauschangriff und der Online-Durchsuchung nicht anders, und das wird sich im Zuge fortschreitender IT-Technik auch in Zukunft ergeben. Eine Nutzung der zur Erhebung der LKW-Maut eingerichteten Erfassungseinrichtungen zu Zwecken der Strafverfolgung und Gefahrenabwehr war schon im Gespräch, desgleichen eine Zentraldatei für die digitalisierte Fingerabdrücke aller Bürger, die für die Ausstellung eines Personalausweises benötigt werden. Die von einem zunehmend unersättlichen und häufig irrationalen Sicherheitsbedürfnis der Bevölkerung sowie einem übertriebenen Effektivitätsstreben der Behörden beförderte Tendenz, Freiheiten zugunsten scheinbar besserer Gefahrenbekämpfung zu opfern, kann nur dann wirksam im verfassungsrechtlichen Gleichgewicht gehalten werden, wenn auch der tatsächliche Nutzen eines technisch möglichen Aufklärungsinstrumentes vom Bundesverfassungsgericht kritisch überprüft und mit dem weiteren Freiheitsverlust abgewogen wird.

Es kommt hinzu, dass die präventive Wirkung der Strafverfolgung und damit der von ihr geleistete Rechtsgüterschutz nicht überschätzt werden darf. Spezialprävention ist nur für die Dauer des Vollzuges einer Freiheitsstrafe zuverlässig gegeben, wenn man von der notorischen Kriminalität innerhalb der Strafvollzugsanstalten einmal absieht. Die resozialisierende Wirkung einer Verurteilung oder Vollzugsmaßnahme wird von den heutigen Kriminologen ebenso skeptisch beurteilt wie ihre Abschreckungseffekte. Im Einzelnen kann dazu auf die ausführliche Erörterung dieser Fragen in der VB Gusy (a.a.O., Ziff. E. 4 (d) (bb), S. 60 ff.) verwiesen werden. Insofern ist in hohem Maße zweifelhaft, ob die angegriffenen Regelungen, soweit sie der Strafverfolgung dienen, überhaupt einen nennenswerten Beitrag zur inneren Sicherheit der Bundesrepublik Deutschland und zum Rechtsgüterschutz leisten.

Der Eingriff beeinträchtigt die Beschwerdeführerin zu 1) in ihrer durch Art. 9 Abs. 3 GG gewährleisteten Organisationsautonomie, darüber hinaus auch bei ihrer koalitionsmäßigen Betätigung, insbesondere bei Wahrnehmung der Tarifautonomie sowie der Mitgliederbetreuung und -beratung. Zusätzliches Gewicht erhält der Eingriff auch für die Beschwerdeführerin zu 1) durch die Beeinträchtigung ihrer Pressefreiheit.

In allen Bereichen ist sie auf die Nutzung von Telekommunikationsleistungen angewiesen. Die Wahrung des Telekommunikationsgeheimnisses ist für sie von hoher Bedeutung. Das gilt für innerorganisatorische Kontakte nicht weniger als für Mitgliederbetreuung, Rechtsberatung und die redaktionelle Arbeit an ihrem Presseorgan ver.di PUBLIK. Wenn sie sich nicht mehr sicher sein kann, dass ihre Verbindungsdaten vor fremdem Zugriff geschützt sind, muss sie sich Beschränkungen auferlegen, die sie bei der Wahrnehmung ihrer Koalitionsfreiheit behindern. Insgesamt erleidet der durch Art. 9 Abs. 3 GG geschützte Freiheitsraum der Beschwerdeführerin zu 1) schwere Einbußen.

Als schwerwiegend ist auch der Eingriff in die Koalitionsfreiheit der Beschwerdeführer zu 2) – 5) einzustufen. Sie werden insgesamt in der Wahrnehmung dieses vorbehaltlos gewährleisteten Freiheitsrechts beeinträchtigt, weil sie befürchten müssen, dass ihre gewerkschaftlichen Kontakte von Dritten wahrgenommen werden können. Sie können die Telekommunikationsdienstleistungen in diesen Zusammenhängen nicht mehr arglos in Anspruch nehmen. Für die Beschwerdeführerin zu 2) kommt hinzu, dass sie um die Preisgabe von Informanten fürchten muss und dass diese sich in der Folge scheuen werden, mit ihr Kontakt aufzunehmen.

Die Beschwerdeführer zu 3) und 4) trifft die Vorratsdatenspeicherung in ihrer Funktion als Rechtsberater für die Mitglieder der Beschwerdeführerin zu 1). Dieser Aspekt der koalitionsmäßigen Betätigung ist deswegen besonders sensibel, weil er in aller Regel das Arbeitsverhältnis der Rechtsschutzsuchenden betrifft, die bei Zweifeln an der Vertraulichkeit ihrer Anfragen Nachteile am Arbeitsplatz fürchten. Das gilt in besonderer Weise für den Beschwerdeführer zu 5). Er arbeitet bei einem Telekommunikationsdienstleister, in dessen Betrieb die Verkehrsdaten gespeichert werden.

Schließlich ist auch der Eingriff von erheblichem Gewicht, den alle Beschwerdeführer in ihrer Telekommunikationsfreiheit erleiden. Das Gewicht dieses Eingriffs ist hoch, weil die Speicherung hochsensibler personenbezogener Daten ohne jeden in ihrer Person begründeten Anlass erfolgt. Ihnen werden im Interesse fragwürdiger Perfektionierung allgemeiner Verbrechensbekämpfung schwere Rechtseinbußen auferlegt und erhebliche Risiken für legale und illegale Zugriffe auf Daten u. a. auch aus dem Kernbereich privater Lebensgestaltung aufgebürdet.

Nicht außer Betracht bleiben kann auch die enorme Streubreite der freiheitsbeeinträchtigenden Wirkung der Vorratsdatenspeicherung. Nahezu alle Einwohner der Bundesrepublik Deutschland sind von ihr be-

troffen, es handelt sich um eine bundesweite, unterschiedslose, permanente Grundrechtsbeschränkung, eine Fahndungsmaßnahme „ins Blaue hinein“. Die Beschränkung betrifft wegen ihrer Streubreite nicht nur die von den Beschwerdeführern geltend gemachten Grundrechte, sondern gegenüber anderen Telekommunikationskunden auch etwa Berufsfreiheit und Eigentum – eine Verletzung dieser Grundrechte wird in der Vb Gusy geltend gemacht –, darüber hinaus aber auch die Religions-, Meinungs- und Versammlungsfreiheit sowie den Schutzbereich von Ehe und Familie. Insgesamt führen die angegriffenen Regelungen zu einer generellen Absenkung des Grundrechtsstandards der Bundesrepublik Deutschland. Die Staatsmacht dringt tiefer in den Freiheitsraum der Bürger ein, diesmal auf breitester Front. Der Machtzuwachs konzentriert sich in den Apparaten der Sicherheitsbehörden. Sie sind auch die treibende Kraft für die ständige Ausweitung der Ausforschungsbefugnisse.

Das Gewicht dieser Beeinträchtigungen kann durch den Nutzen einer Vorratsdatenspeicherung nicht aufgewogen werden. Sie ist, wie dargelegt, als Mittel der Verbrechensverköpfung nur eingeschränkt geeignet und insgesamt jedenfalls entbehrlich. Zur Sicherheit der Bürger wird durch sie kein wesentlicher Beitrag geleistet, andererseits schafft sie neue Risiken für kriminelle Verletzungen von Geschäfts- und Berufs- und Dienstgeheimnissen und von Privatheit.

Im Ergebnis erweist sich die Vorratsdatenspeicherung nach alledem als unverhältnismäßig. Der zusätzliche Schutz, den sie gewähren soll, ist minimal, zudem wirkt die Maßnahme selektiv in dem Sinne, dass sie gerade schweren Bedrohungen gegenüber tendenziell versagt. Die vorhandenen Ermittlungsmöglichkeiten reichen jedenfalls aus, um eine wirksame Strafverfolgung und den damit bezweckten Rechtsgüterschutz zu gewährleisten.

### **3. Unverhältnismäßigkeit von § 113a Abs. 6 TKG**

In dieser Vorschrift wird die Pflicht von Telekommunikationsdienstleistern begründet, eine Veränderung der Verkehrsdaten zu dokumentieren und die Dokumentation zu speichern. Damit soll die Speicherpflicht auf die Dienstleister ohne eigene Endnutzerbeziehung auch für den Fall der Datenänderung erstreckt werden. Gleichzeitig soll aber auch den Anonymisierungsdiensten das Handwerk gelegt werden. In dieser Funktion verstärkt die Regelung den Eingriff in das Telekommunikationsgeheimnis, weil dem Nutzer ein Ausweg aus der Speicherfalle erschwert wird.

Die Regelung erweist sich jedoch in soweit als nahezu ungeeignet. Sie vermag eine Anonymisierung der Verkehrsdaten durch Kriminelle nicht wirksam zu verhindern, weil im Ausland betriebene Internet-Anonymisierungsdienste kostenlos zur Verfügung stehen und damit eine Vorratsdatenspeicherung in Deutschland jedenfalls von den potentiellen Straftätern leicht umgangen werden kann (Arbeitskreis Vorratsdatenspeicherung/Netzwerk Neue Medien/Neue Richtervereinigung e.V., Stellungnahme zum Referentenentwurf usw. 2007, S. 26, [www.vorratsdatenspeicherung.de](http://www.vorratsdatenspeicherung.de)). Zur Erforderlichkeit und Zumutbarkeit kann auf das oben Gesagte verwiesen werden.

Der den Anonymisierungsdiensten auferlegte Zwang, die Veränderungen der Daten lückenlos zu dokumentieren und ihren Service damit selbst zu entwerten, ist, soweit er als ein geeignetes Mittel zum Schutz der einschlägigen Belange angesehen wird, jedenfalls unverhältnismäßig; denn viele Menschen sind auf anonyme Telekommunikation angewiesen. Das gilt, insbesondere für die folgenden Personengruppen:

- Viele Menschen in besonderen Notlagen sind nur unter Wahrung der Anonymität bereit, Hilfe zu suchen,
- Unternehmen, die sich gegen Wirtschaftsspionage schützen wollen,
- Behörden sind häufig auf anonyme Anzeigen und Informationen angewiesen, „Whistleblower“ können sich nur durch anonyme Offenbarung schützen, wenn sie Missstände aus ihrem beruflichen Umfeld öffentlich machen wollen,
- Menschen in autoritären Staaten können sich weitgehend nur im Schutz der Anonymität sicher vor Verfolgung informieren und artikulieren,
- Journalisten und Menschenrechtsgruppen, Regierungskritiker in autoritären Staaten können bei Lebensgefahr nur anonym kommunizieren.

Wegen der Einzelheiten verweise ich auf die ausführlichen Darlegungen in der Vb Gusy (vgl. a.a.O. Ziff. E 4. c) (d) (ff) (vi), S. 95 ff.).

Diesen Personengruppen gegenüber wirkt sich § 113a Abs. 6 TKG verheerend aus. Sie werden im Gebrauch zentraler Grundrechte gehindert. Der Eingriff hat damit ein solches Gewicht, dass sie durch den Schutz der mit der Regelung bezweckten Belange nicht aufgewogen werden können.

#### **4. Unverhältnismäßigkeit der Zugriffsmöglichkeiten**

Gegenstand der folgenden Erörterungen ist der Zugriff auf die Verkehrs- und Standortdaten, die allein in Folge der Pflicht zur Vorratsdatenspeicherung zur Verfügung stehen. Die Frage nach der Verhältnismäßigkeit stellt sich hier nur für den Fall, dass das Gericht die Vorratsdatenspeicherung insgesamt oder teilweise als verfassungskonform ansieht, sei es, weil es sie zum Schutz hochrangiger Rechtsgüter für gerechtfertigt hält; sei es weil es die Bundesrepublik Deutschland insofern durch die Richtlinie 2006/24/EG als gebunden erachtet und sich selbst deswegen keine Entscheidungskompetenz beimisst.

##### **a. Zugriff wegen der Katalogstraftaten**

Hinsichtlich der Katalogstraftaten ergeben sich insoweit keine Besonderheiten: Wenn die Vorratsdatenspeicherung als solche einer verfassungsrechtlichen Überprüfung im Lichte der angeführten Grundrechte standhalten sollte, dann kommen als Rechtfertigungsgrund allenfalls die mit den Katalogstraftaten geschützten Rechtsgüter in Betracht. Die Zugriffsbefugnis wegen dieser Taten auf die infolge der Vorratsdatenspeicherung zur Verfügung stehenden Verkehrs- und Standortdaten liegt dann in der Konsequenz dieser Entscheidung.

##### **b. Zugriff wegen der „anderen Straftaten“**

Nicht unter diesen Katalog fallen einmal die in § 100g Abs. 1 Nr. 1 StPO genannten „anderen Straftaten von (auch im Einzelfall) erheblicher Bedeutung“. Welche Straftaten dies sein könnten, ist jedoch nicht mit hinreichender Bestimmtheit feststellbar. Infolgedessen lässt sich auch zum Gewicht der damit geschützten Rechtsgüter nichts Sachdienliches darlegen. Es ist bereits dargelegt worden, dass § 110g Abs. 1 Nr. 1 StPO jedenfalls insoweit mit dem Gebot der Normenklarheit nicht im Einklang steht.

##### **c. Weitere Zugriffstatbestände**

Auch § 110g Abs. 1 Nr. 2 StPO, der den Zugriff zur Aufklärung von Straftaten vorsieht, die mittels Telekommunikation begangen wurden, ist bereits mangels hinreichender Bestimmtheit verfassungswidrig. Das ist weiter oben (S. 21) schon dargelegt worden. Entsprechendes gilt für die in § 113b Nr. 2 und 3 TKG geregelten Zugriffsbefugnisse von Polizei und Geheimdiensten. Eine Erörterung ist erst möglich, nachdem der

Bundes- und die Landesgesetzgeber entsprechende Regelungen getroffen haben. Insoweit behalten die Beschwerdeführer sich ergänzenden Vortrag vor.

### E. Zusammenfassung

Die Verfassungsbeschwerden sind in zulässiger Weise unmittelbar gegen die angegriffenen gesetzlichen Regelungen gerichtet, weil die Beschwerdeführer durch sie unmittelbar in ihren Grundrechten betroffen sind. Das Bundesverfassungsgericht ist durch Gemeinschaftsrecht nicht an einer verfassungsrechtlichen Überprüfung gehindert. Die Richtlinie 2006/24/EG steht nicht entgegen. Sie ist kompetenzwidrig ergangen und wird auf die anhängige Klage der Republik Irland vom Europäischen Gerichtshof aufgehoben werden. Geschieht dies nicht, ist das Bundesverfassungsgericht gehalten, den Rechtsstreit gemäß Art. 134 S. 1 b, S. 3 EGV dem EuGH vorzulegen. Im Übrigen gehen die angegriffenen Regelungen über die Vorgaben der Richtlinie 2006/24/EG in mehreren Punkten hinaus. Insofern unterliegen sie ohne weiteres der Entscheidungskompetenz des Bundesverfassungsgerichts.

Die angegriffenen Regelungen verletzen die Beschwerdeführer in ihren Grundrechten aus Art. 10 Abs. 1, Art. 9 Abs. 3 und Art. 5 Abs. 1 S. 2 GG. § 113b TKG verletzt zumindest teilweise den Grundsatz der Normenklarheit: Die in Bezug genommene Zugriffsnorm (§ 110g in Verbindung mit 110a StPO) enthält neben einem Straftatenkatalog eine generalklauselartige Erweiterung auf „Straftaten von auch im Einzelfall erheblicher Bedeutung“, die als strafprozessuale Eingriffsnorm zu unbestimmt ist. Außerdem erlaubt § 113b Nr. 1 TKG in Verbindung mit § 100g Abs. 1 Nr. 2 StPO den Zugriff auf die gemäß § 113a TKG gespeicherten Verkehrsdaten auch zur Aufklärung von Straftaten, die mittels Telekommunikation begangen worden sind, dies allerdings nur unter der Voraussetzung, dass „die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht.“ Durch diese salvatorische Klausel wird der Eingriffstatbestand völlig verwischt.

Die in § 113a TKG vorgesehene Vorratsdatenspeicherung greift in unverhältnismäßiger Weise in die Telekommunikationsfreiheit (Art. 10 Abs. 1 GG), die Koalitionsfreiheit (Art. 9 Abs. 3 GG) und die Pressefreiheit (Art. 5 Abs. 1 S. 2 GG) der Beschwerdeführer ein. Der schweren Beeinträchtigung dieser Grundrechte steht allenfalls ein geringfügiger Nutzen für die Strafverfolgung und eine noch geringere Schutzwirkung zugunsten der einschlägigen Rechtsgüter gegenüber.

Als Ergebnis ist festzuhalten: Die angegriffenen Regelungen verletzen die Beschwerdeführer in den genannten Grundrechten und sind daher verfassungswidrig und nichtig.

Rechtsanwältin