



Schleswig-Holsteinischer Landtag □
Umdruck 16/3171

An den
Vorsitzenden des Innen- und Rechtsausschusses
Herrn Werner Kalinka, MdL
im Hause

Ihr Zeichen:
Ihre Nachricht vom:

Mein Zeichen: L 204
Meine Nachricht vom:

Bearbeiter: Heiko Voß

Telefon (0431) 988-1022
Telefax (0431) 988-1037
parlamentsdienst@landtag.ltsh.de

20. Mai 2008

**Organstreitverfahren wegen der Verletzung von Rechten aus dem Beschluss
des Deutschen Bundestages über das Gesetz zur Neuregelung der Tele-
kommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnah-
men**

Sehr geehrter Herr Kalinka,

in der Anlage beigefügt übersende ich Ihnen die Ablichtung eines Schreibens des
Vorsitzenden des Zweiten Senats des Bundesverfassungsgerichts vom 30. April
2008 – Aktenzeichen 2 BvE 1/08 mit der Bitte um Kenntnisnahme.

Ich bitte, die Angelegenheit in Ihrem Ausschuss zu beraten und dem Landtag eine
Beschlussempfehlung zuzuleiten.

Mit freundlichen Grüßen

Martin Kreyer

BUNDESVERFASSUNGSGERICHT
Zweiter Senat
- Der Vorsitzende -
2 BvE 1/08

Karlsruhe, 30. April 2008
Durchwahl 9101-201

(Bei Antwort bitte angeben)

1. Landtag von Baden-Württemberg
vertreten durch den Präsidenten
Haus des Landtags
Konrad-Adenauer-Straße 3
70173 Stuttgart
2. Bayerischer Landtag
vertreten durch den Präsidenten
81627 München
3. Abgeordnetenhaus von Berlin
vertreten durch den Präsidenten
10111 Berlin-Mitte
4. Landtag Brandenburg
vertreten durch den Präsidenten
Postfach 60 10 64, 14410 Potsdam
5. Bremische Bürgerschaft
vertreten durch den Präsidenten
Haus der Bürgerschaft
Postfach 10 69 09, 28069 Bremen
6. Bürgerschaft der Freien und Hansestadt Hamburg
vertreten durch die Präsidentin
Postfach 10 09 02, 20006 Hamburg
7. Hessischer Landtag
vertreten durch den Präsidenten
Postfach 32 40, 65022 Wiesbaden
8. Landtag Mecklenburg-Vorpommern
vertreten durch die Präsidentin
Schloß Schwerin
Lennéstraße 1, 19053 Schwerin
9. Niedersächsischer Landtag
vertreten durch den Präsidenten
Postfach 44 07, 30044 Hannover
10. Landtag Nordrhein-Westfalen
vertreten durch den Präsidenten
Haus des Landtags
Postfach 10 11 43, 40002 Düsseldorf

Dienstgebäude: Schloßbezirk 3, 76131 Karlsruhe
Postfach 1771, 76006 Karlsruhe
Telefon 0721/9101-0 - Telefax 0721/9101-382

11. Landtag Rheinland-Pfalz
vertreten durch den Präsidenten
Postfach 30 40, 55028 Mainz
12. Landtag des Saarlandes
vertreten durch den Präsidenten
Postfach 10 18 33, 66018 Saarbrücken
13. Sächsischer Landtag
vertreten durch den Präsidenten
Postfach 12 07 05, 01008 Dresden
14. Landtag von Sachsen-Anhalt
vertreten durch den Präsidenten
Postfach 19 69, 39094 Magdeburg
15. Schleswig-Holsteinischer Landtag
vertreten durch den Präsidenten
Landeshaus
Postfach 71 21, 24171 Kiel
16. Thüringer Landtag
vertreten durch die Präsidentin
Postfach 9 41, 99019 Erfurt
17. Landesregierung Baden-Württemberg
vertreten durch den Ministerpräsidenten
Staatsministerium
Richard-Wagner-Straße 15, 70184 Stuttgart
18. Bayerische Staatsregierung
vertreten durch den Ministerpräsidenten
Staatskanzlei
Postfach 22 00 11, 80535 München
19. Senat von Berlin
vertreten durch den Regierenden Bürgermeister
Senatskanzlei
10173 Berlin
20. Regierung des Landes Brandenburg
vertreten durch den Ministerpräsidenten
Staatskanzlei
Postfach 60 10 51, 14410 Potsdam
21. Senat der Freien Hansestadt Bremen
vertreten durch den Präsidenten
Senatskanzlei, Rathaus
Postfach 10 25 20, 28025 Bremen

22. Senat der Freien und Hansestadt Hamburg
vertreten durch den Präsidenten
Senatskanzlei
Postfach 10 55 20, 20038 Hamburg
23. Hessische Landesregierung
vertreten durch den Ministerpräsidenten
Staatskanzlei
Georg-August-Zinn-Straße 1, 65183 Wiesbaden
24. Landesregierung Mecklenburg-Vorpommern
vertreten durch den Ministerpräsidenten
Staatskanzlei
19048 Schwerin
25. Niedersächsische Staatskanzlei
Planckstraße 2, 30169 Hannover
26. Landesregierung Nordrhein-Westfalen
vertreten durch den Ministerpräsidenten
Staatskanzlei
40190 Düsseldorf
27. Landesregierung Rheinland-Pfalz
vertreten durch den Ministerpräsidenten
Staatskanzlei
Postfach 38 80, 55028 Mainz
28. Regierung des Saarlandes
vertreten durch den Ministerpräsidenten
Staatskanzlei
Postfach 10 24 31, 66024 Saarbrücken
29. Sächsisches Staatsministerium
der Justiz
01095 Dresden
30. Landesregierung Sachsen-Anhalt
vertreten durch den Ministerpräsidenten
Staatskanzlei
Postfach 41 60, 39016 Magdeburg
31. Innenministerium
des Landes Schleswig-Holstein
Postfach 71 25, 24171 Kiel
32. Thüringer Justizministerium
Postfach 10 01 51, 99001 Erfurt

Verfahren über den Antrag festzustellen,

1. dass der Antragsgegner mit dem Beschluss vom 9. November 2007 über das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG (BGBl 2007 I S. 3198 ff.) die Rechte der Antragstellerinnen und Antragsteller aus Art. 38 Abs. 1 Satz 2 verletzt hat, in dem er

- a) Erbringer von öffentlich zugänglichen Telekommunikationsdiensten in § 113a TKG zur Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten verpflichtet und in § 113b TKG zu deren Verwendung für die dort genannten Zwecke berechtigt sowie
- b) in § 100g Abs. 1 StPO zur Erhebung von gemäß § 113a TKG gespeicherten Verkehrsdaten ermächtigt.

2. hilfsweise,

dass der Antragsgegner mit dem Beschluss vom 9. November 2007 über das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG (BGBl 2007 I S. 3198 ff.) die Rechte der Antragstellerinnen und Antragsteller aus Art. 38 Abs. 1 Satz 2 GG verletzt hat, in dem er über die zwingenden Vorgaben der Richtlinie 2006/24/EG hinaus

- a) Erbringer von öffentlich zugänglichen Telekommunikationsdiensten in § 113a TKG zur Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten verpflichtet und in § 113b TKG zu deren Verwendung für die dort genannten Zwecke berechtigt sowie
- b) in § 100g Abs. 1 StPO zur Erhebung von gemäß § 113a TKG gespeicherten Verkehrsdaten ermächtigt.

Antragsteller: Mitglieder des Deutschen Bundestages

- 1. [REDACTED]
- 2. [REDACTED]
- 3. [REDACTED]
- 4. [REDACTED]
- 5. [REDACTED]
- 6. [REDACTED]
- 7. [REDACTED]
- 8. [REDACTED]
- 9. [REDACTED]
- 10. [REDACTED]
- 11. [REDACTED]
- 12. [REDACTED]
- 13. [REDACTED]

14. [REDACTED]
15. [REDACTED]
16. [REDACTED]
17. [REDACTED]
18. [REDACTED]
19. [REDACTED]
20. [REDACTED]
21. [REDACTED]
22. [REDACTED]
23. [REDACTED]
24. [REDACTED]
25. [REDACTED]
26. [REDACTED]
27. [REDACTED]
28. [REDACTED]
29. [REDACTED]
30. [REDACTED]
31. [REDACTED]
32. [REDACTED]
33. [REDACTED]
34. [REDACTED]
35. [REDACTED]
36. [REDACTED]
37. [REDACTED]
38. [REDACTED]
39. [REDACTED]
40. [REDACTED]
41. [REDACTED]
42. [REDACTED]
43. [REDACTED]
44. [REDACTED]
45. [REDACTED]
46. [REDACTED]
47. [REDACTED]

Deutscher Bundestag, Platz der Republik 1, 11011, Berlin,

- Bevollmächtigter: Professor Dr. Jens-Peter Schneider,
Lürmannstraße 10, 49076 Osnabrück -

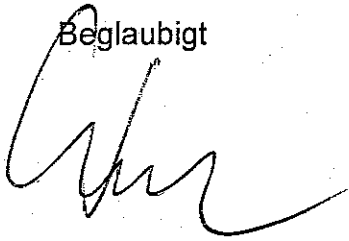
Antragsgegner: Deutscher Bundestag, vertreten durch den Präsidenten,
Platz der Republik 1, 11011 Berlin

Anl.: 1

Anliegender Abdruck der Antragsschrift vom 8. Februar 2008 wird übermittelt. Es wird anheim gestellt, hinsichtlich des Antrags bis zum 30. Juni 2008 Stellung zu nehmen und eine etwaige Stellungnahme in 30 Stücken einzureichen.

Prof. Dr. Dr. h.c. mult. Hassemer
Vizepräsident

Beglaubigt



(Heid)
Regierungsamtmann



E: 77-07-08

Prof. Dr. Jens-Peter Schneider

Lürmannstr. 10
49076 Osnabrück
Tel. 0541 / 6688208
Fax: 0541 / 6688207

An das
Bundesverfassungsgericht
Schlossbezirk 3
76131 Karlsruhe

Organstreitverfahren

der nachfolgend bezeichneten Antragstellerinnen und Antragsteller:

1. [REDACTED] Mitglied des Deutschen Bundestages
2. [REDACTED] Mitglied des Deutschen Bundestages
3. [REDACTED] Mitglied des Deutschen Bundestages
4. [REDACTED] Mitglied des Deutschen Bundestages
5. [REDACTED] Mitglied des Deutschen Bundestages
6. [REDACTED] Mitglied des Deutschen Bundestages
7. [REDACTED] Mitglied des Deutschen Bundestages
8. [REDACTED] Mitglied des Deutschen Bundestages
9. [REDACTED] Mitglied des Deutschen Bundestages
10. [REDACTED] Mitglied des Deutschen Bundestages
11. [REDACTED] Mitglied des Deutschen Bundestages
12. [REDACTED] Mitglied des Deutschen Bundestages
13. [REDACTED] Mitglied des Deutschen Bundestages
14. [REDACTED] Mitglied des Deutschen Bundestages
15. [REDACTED] Mitglied des Deutschen Bundestages
16. [REDACTED] Mitglied des Deutschen Bundestages
17. [REDACTED] Mitglied des Deutschen Bundestages
18. [REDACTED] Mitglied des Deutschen Bundestages
19. [REDACTED] Mitglied des Deutschen Bundestages
20. [REDACTED] Mitglied des Deutschen Bundestages
21. [REDACTED] Mitglied des Deutschen Bundestages

- 40
22. [REDACTED] Mitglied des Deutschen Bundestages
 23. [REDACTED] Mitglied des Deutschen Bundestages
 24. [REDACTED] Mitglied des Deutschen Bundestages
 25. [REDACTED] Mitglied des Deutschen Bundestages
 26. [REDACTED] Mitglied des Deutschen Bundestages
 27. [REDACTED] Mitglied des Deutschen Bundestages
 28. [REDACTED], Mitglied des Deutschen Bundestages
 29. [REDACTED], Mitglied des Deutschen Bundestages
 30. [REDACTED] Mitglied des Deutschen Bundestages
 31. [REDACTED], Mitglied des Deutschen Bundestages
 32. [REDACTED], Mitglied des Deutschen Bundestages
 33. [REDACTED] Mitglied des Deutschen Bundestages
 34. [REDACTED], Mitglied des Deutschen Bundestages
 35. [REDACTED], Mitglied des Deutschen Bundestages
 36. [REDACTED] Mitglied des Deutschen Bundestages
 37. [REDACTED], Mitglied des Deutschen Bundestages
 38. [REDACTED] Mitglied des Deutschen Bundestages
 39. [REDACTED], Mitglied des Deutschen Bundestages
 40. [REDACTED] Mitglied des Deutschen Bundestages
 41. [REDACTED] Mitglied des Deutschen Bundestages
 42. [REDACTED] Mitglied des Deutschen Bundestages
 43. [REDACTED], Mitglied des Deutschen Bundestages
 44. [REDACTED] Mitglied des Deutschen Bundestages
 45. [REDACTED] Mitglied des Deutschen Bundestages
 46. [REDACTED], Mitglied des Deutschen Bundestages
 47. [REDACTED] Mitglied des Deutschen Bundestages

Postadresse aller Antragstellerinnen und Antragsteller:

Deutscher Bundestag, Platz der Republik 1, 11011 Berlin

Verfahrensbevollmächtigter: Prof. Dr. Jens-Peter Schneider
Lürmannstr. 10, 49076 Osnabrück

gegen den

Deutschen Bundestag, vertreten durch den Präsidenten
Platz der Republik 1, 11011 Berlin.

Ich zeige an, dass mir die Antragstellerinnen und Antragsteller Vollmacht erteilt (Anlage) und mich mit der Wahrnehmung ihrer Interessen beauftragt haben. Namens und im Auftrag der Antragstellerinnen und Antragsteller beantrage ich hiermit festzustellen:

1. Der Antragsgegner hat mit dem Beschluss vom 9.11.2007 über das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG (BGBl. 2007 I S. 3198 ff.) die Rechte der Antragstellerinnen und Antragsteller aus Art. 38 I 2 GG verletzt, in dem er
 - a) Erbringer von öffentlich zugänglichen Telekommunikationsdiensten in § 113a TKG zur Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten verpflichtet und in § 113b TKG zu deren Verwendung für die dort genannten Zwecke berechtigt sowie
 - b) in § 100g I StPO zur Erhebung von gemäß § 113a TKG gespeicherten Verkehrsdaten ermächtigt.
2. hilfsweise: Der Antragsgegner hat mit dem Beschluss vom 9.11.2007 über das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG (BGBl. 2007 I S. 3198 ff.) die Rechte der Antragstellerinnen und Antragsteller aus Art. 38 I 2 GG verletzt, in dem er über die zwingenden Vorgaben der Richtlinie 2006/24/EG hinaus
 - a) Erbringer von öffentlich zugänglichen Telekommunikationsdiensten in § 113a TKG zur Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten verpflichtet und in § 113b TKG zu deren Verwendung für die dort genannten Zwecke berechtigt sowie
 - b) in § 100g I StPO zur Erhebung von gemäß § 113a TKG gespeicherten Verkehrsdaten ermächtigt.

Ferner rege ich, sofern der EuGH in der Rs. C-301/06 vor der Entscheidung des hohen Gerichts noch keine oder eine abweisende Entscheidung getroffen hat, an,

dem Europäischen Gerichtshof gemäß Art. 234 EGV die Frage vorzulegen, ob die Richtlinie 2006/24/EG wegen Verstoßes gegen Gemeinschaftsgrundrechte oder europäische Abgeordnetenrechte ungültig ist.

Begründung

A. Sachverhalt	5
I. Angaben zu den Antragstellerinnen und Antragstellern	5
II. Systematik und Inhalt der angegriffenen Regeln zur Vorratsdatenspeicherung im Überblick	5
B. Zulässigkeit des Organstreits	7
I. Allgemeine Zulässigkeitsvoraussetzungen	7
II. Antragsbefugnis	7
III. Keine Unzulässigkeit aufgrund zwingender Vorgaben der Richtlinie 2006/24/EG	10
1. Möglichkeiten der verfassungsrechtlichen Kontrolle außerhalb zwingender Vorgaben der Richtlinie 2006/24/EG	10
2. Umsetzungsspielräume nach der Richtlinie 2006/24/EG	11
IV. Zwischenergebnis zur Zulässigkeit des Organstreitverfahrens	14
C. Erweiterung des verfassungsgerichtlichen Prüfungsgegenstands bei Inexistenz oder Ungültigkeit der Richtlinie 2006/24/EG	14
I. Uneingeschränkte verfassungsrechtliche Überprüfung des Gesetzes vom 21.12.2007 bei Inexistenz der Richtlinie 2006/24/EG	15
II. Möglichkeit einer Gültigkeitsvorlage an den EuGH zur Beseitigung zwingender Vorgaben aus der Richtlinie 2006/24/EG	16
1. Zulässigkeit und Notwendigkeit einer Vorlage an den EuGH durch das BVerfG	16
2. Verstoß der Richtlinie 2006/24/EG gegen Gemeinschaftsgrundrechte	19
3. Verstoß der Richtlinie 2006/24/EG gegen europäische Abgeordnetenrechte	22
III. Folgen einer abweisenden EuGH-Entscheidung für den verfassungsgerichtlichen Schutz von Abgeordnetenrechten	23
IV. Subsidiäre kompetenzrechtliche Überprüfung der Richtlinie 2006/24/EG durch das BVerfG	24
D. Verletzung des freien Mandats gemäß Art. 38 I 2 GG durch die Regelungen zur Vorratsdatenspeicherung	25
I. Vorratsdatenspeicherung als Eingriff in das freie Mandat	25
II. Verfassungsrechtliche Rechtfertigung	27
1. Rechtsgüter von Verfassungsrang als Schranken des freien Mandats	27
2. Verhältnismäßigkeit	27
a) Eignung	27
b) Erforderlichkeit	29
c) Angemessenheit	30
aa) Unverhältnismäßigkeit von Spielraumentscheidungen des deutschen Gesetzgebers	31
(1) Schutzwürdigkeit von Verkehrsdaten und verdachtslose Vorratsdatenspeicherung	31
(2) Absenkung der strafverfolgungsrechtlichen Anordnungsvoraussetzungen	34
(3) Erweiterung der Verwendungszwecke auf Gefahrenabwehr sowie Verfassungsschutz und nachrichtendienstliche Nutzung	38
(4) Unzureichende Datensicherungsstrukturen bei der Vorratsdatenspeicherung	41
bb) Unverhältnismäßigkeit von zwingende Richtlinienvorgaben umsetzenden Bestimmungen	42

A. Sachverhalt

I. Angaben zu den Antragstellerinnen und Antragstellern

Alle Antragstellerinnen und Antragsteller¹ sind Abgeordnete des Deutschen Bundestages. Als Abgeordnete sind sie in vielfältiger Weise auf die Nutzung von Telekommunikationsdiensten angewiesen. Insbesondere müssen sie sich über politisch brisante Fragen informieren und sind auf die Bereitschaft von Informanten angewiesen, mit ihnen telefonisch oder über das Internet Kontakt aufzunehmen.

II. Systematik und Inhalt der angegriffenen Regeln zur Vorratsdatenspeicherung im Überblick

Die neuen Regelungen zur sogenannten Vorratsdatenspeicherung von Verkehrsdaten² richten sich einerseits an die verpflichteten Telekommunikationsunternehmen, legen deren Speicherpflichten fest (§ 113a TKG neu) und bestimmen, zu welchen Zwecken die verpflichteten Unternehmen die gespeicherten Daten verwenden dürfen (§ 113b TKG neu). Davon unabhängig ist andererseits geregelt (§ 100g StPO n.F.) bzw. wird zu regeln sein, unter welchen Voraussetzungen staatliche Behörden die Übermittlung gemäß § 113a TKG gespeicherter Daten durch die TK-Unternehmen anordnen dürfen. Ferner ist gesondert geregelt bzw. zu regeln, unter welchen Voraussetzungen Behörden hiernach übermittelte Verkehrsdaten an andere Behörden oder Private weiterleiten dürfen.

Die angegriffenen Bestimmungen zur Vorratsdatenspeicherung ergänzen die seit längerem bestehenden Regelungen zur Übermittlung von Teilnehmerbestandsdaten in den §§ 112, 113 TKG, die aber wegen der durch die Vorratsdatenspeicherung erweiterten Verknüpfungsmöglichkeiten³ einen erheblich größeren Anwendungsbereich mit zusätzlichen für die Statusrechte der Antragsteller relevanten Auswirkungen erhalten.

§ 113a TKG verpflichtet die Anbieter öffentlich zugänglicher Telekommunikationsdienste für Endnutzer unter Regelung weiterer Detailfragen zur

¹ Im Weiteren umfassen männliche Formen Frauen und Männer.

² Zur neuen Terminologie der Verkehrsdaten: Bundesregierung, Gesetzesbegründung, BT-Drs. 16/5846, S. 51.

³ S. näher unten D.II.2.c)aa)(1).

sechsmonatigen Speicherung verschiedener Typen von Verkehrsdaten aus den Bereichen Telefondienst, elektronische Post sowie Internetzugangsdienst und deren anschließender Löschung binnen eines weiteren Monats. Die Speicherung selbst verlangt keinerlei Anlass, erfolgt also verdachtslos und betrifft jegliche Kommunikation mittels Telekommunikation. Dadurch entfaltet sie eine ganz außergewöhnliche Breitenwirkung. Nach § 113b TKG darf der Speicherverpflichtete die Verkehrsdaten an staatliche Stellen auf deren Verlangen nur für Zwecke der Strafverfolgung, der Gefahrenabwehr sowie des Verfassungsschutzes bzw. der Nachrichtendienste übermitteln.

Außerhalb des TKG sind die Voraussetzungen für Auskunftsanordnungen und die Weiterverwendung der Verkehrsdaten durch die zuständigen Behörden unter Hinweis auf § 113a TKG in den einschlägigen speziellen Landes- oder Bundesgesetzen zu konkretisieren. Bislang sind zwar nur die Anordnungsbefugnisse der Strafverfolgungsbehörden detailliert geregelt. Die anderen Verwendungszwecke sind allerdings aufgrund der abstrakten Übermittlungsermächtigung für die speichernden TK-Unternehmen in § 113b TKG zumindest angedeutet.

Für die Verwendung zu Strafverfolgungszwecken ist vor allem der neugefasste § 100g I StPO relevant. Danach ist eine Verkehrsdatenverwendung nicht nur bei einem durch Tatsachen begründeten Verdacht auf Straftaten von auch im Einzelfall erheblicher Bedeutung zulässig, sondern auch bei minder schweren Straftaten, wenn diese mittels Telekommunikation begangen wurden, die Ermittlungen sonst aussichtslos wären und die Datenerhebung im angemessenen Verhältnis zur Bedeutung der Sache steht. § 100g StPO ist Teil der neuen Gesamtregelung zur Telekommunikationsüberwachung. Von dieser sind hier insbesondere die neuen prozeduralen Anwendungsvoraussetzungen gemäß den §§ 100b I bis IV 1 StPO, die differenzierenden Erhebungsverbote nach § 160a StPO, die Zweckbindungsregeln gemäß §§ 101 III, 477 II StPO und die Rechtsschutzmöglichkeiten gemäß § 101 IV bis VII StPO von Belang.

Bedeutsam sind ferner die Bestimmungen der StPO zur Datenweitergabe einerseits an andere staatliche Stellen – in den §§ 474, 481, 483, 487 mit dem neugefassten Zweckbindungsgebot aus § 477 II StPO – und andererseits an Private gemäß §§ 406e, 475 StPO. Bei letzteren ist besonders hervorzuheben, dass auf die Auskunftsansprüche von Verletzten gemäß § 406a StPO, die im Zusammenhang mit der Vorratsdatenspeicherung von besonderer Relevanz sein werden, die strengen

Übermittlungsbeschränkungen des § 477 II StPO ausweislich des ausdrücklich nur auf § 477 V StPO verweisenden § 406e VI StPO keine Anwendung finden⁴.

Die Vorratsdatenspeicherung ist lediglich einer von vielen Bausteinen im aktuellen sicherheitspolitischen Maßnahmenkatalog, die datenschutzrelevante Regelungen enthalten. Den Hintergrund zu den hier angegriffenen Regelungen bilden allein in der jüngsten Vergangenheit bzw. aktuellen rechtspolitischen Diskussion Regelungen bzw. Gesetzentwürfe über automatisierte Kennzeichenerfassungen, Onlinedurchsuchungen, Rasterfahndungen, Videoüberwachungen öffentlicher Räume, Mautdatennutzung oder Fluggastdatenspeicherung.

B. Zulässigkeit des Organstreits

I. Allgemeine Zulässigkeitsvoraussetzungen

Die Antragsteller sind als Abgeordnete des Deutschen Bundestags im Organstreitverfahren anerkanntermaßen parteifähig⁵. Statthafter Streitgegenstand kann auch der Erlass eines Gesetzes sein⁶, vorliegend der Gesetzesbeschluss des Antragsgegners vom 9.11.2007 über das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG⁷. Das Gesetz wurde am 31.12.2007 verkündet (BGBl. 2007 I S. 3198 ff.), so dass die Antragsfrist eingehalten ist.

II. Antragsbefugnis

Die Antragsbefugnis der Antragsteller folgt aus der Verletzung bzw. unmittelbaren Gefährdung ihres durch Art. 38 I 2 GG geschützten freien Mandats. Art. 38 Abs. 1 GG schützt nicht nur den Bestand, sondern auch die tatsächliche Ausübung des Mandats⁸. Abgeordnete sind – vom Vertrauen der Wähler berufen – Inhaber eines öffentlichen

⁴ Hierzu: Bundesregierung, Gesetzesbegründung, BT-Drs. 16/5846, S. 67.

⁵ BVerfGE 10, 4 (10); 60, 374 (378); 62, 1 (32); 70, 324 (350); 108, 251 (270).

⁶ BVerfGE 1, 208 (220); 4, 144 (148); 82, 322 (335); 92, 80 (87); 102, 224 (234); 103, 164 (169); Umbach, in: Umbach/Clemens/Dollinger (Hrsg.), BVerfGG-Mitarbeiterkommentar, 2. Aufl. 2005, §§ 63, 64 Rn. 139.

⁷ BRat-Drs. 798/07.

⁸ BVerfGE 80, 188 (218); 99, 19 (32).

Amtes, Träger eines freien Mandats und, gemeinsam mit der Gesamtheit der Mitglieder des Parlaments⁹, Vertreter des ganzen Volkes¹⁰. Sie haben einen repräsentativen Status inne, üben ihr Mandat in Unabhängigkeit, frei von jeder Bindung an Aufträge und Weisungen, aus und sind nur ihrem Gewissen unterworfen¹¹. Durch die vom Antragsgegner beschlossene Vorratsdatenspeicherung wird sowohl der repräsentative Status als auch die Unabhängigkeit der Antragsteller beeinträchtigt.

Die Repräsentationsmächtigkeit des Parlaments hängt auch von mandatsbezogenen Vertrauensverhältnissen in Kommunikationsbeziehungen zwischen einzelnen Abgeordneten und Dritten ab¹². Die Repräsentationsmöglichkeiten der Antragsteller leiden daher, wenn die Vertraulichkeit des Informations- und Meinungsaustauschs zwischen ihnen und den von ihnen repräsentierten Bürgern oder anderen Informanten durch staatliche Telekommunikationsüberwachungsmaßnahmen wie die Vorratsdatenspeicherung gefährdet wird. Insbesondere besteht die Gefahr, dass Dritte nicht mehr im bisherigen Umfang den Abgeordneten vertrauliche Informationen zur Verfügung stellen, was deren Möglichkeiten zur parlamentarischen Kontrolle des Handelns insbesondere von Regierung und sonstiger Exekutive erheblich beschneiden könnte¹³.

Das freie Mandat schützt die Unabhängigkeit der Abgeordneten vor zwangsweisen Einflussnahmen auf die Art ihrer Mandatsausführung auch gegenüber staatlichen Organen¹⁴. Wegen der hohen Bedeutung autonomer Informationsbeschaffung durch die Abgeordneten für ihre freie Meinungsbildung zur parlamentarischen Entscheidungsvorbereitung und bei der Kontrolle der Regierung muss das Abgeordnetenmandat unter den Bedingungen der Informationsgesellschaft deren Informations- und Kommunikationsbeziehungen nicht nur vor herkömmlichen, sondern ggf. auch vor neuartigen Überwachungsformen schützen¹⁵. Dabei sichern die separat in Einzelbestimmungen des Grundgesetzes verankerten Rechte der individuellen Abgeordneten zum Schutz ihres freien Mandats wie die Immunität (Art. 46 II bis IV GG),

⁹ BVerfGE 56, 396 (405).

¹⁰ BVerfGE 112, 118 (134).

¹¹ BVerfGE 40, 296 (314, 316); 76, 256 (341).

¹² BVerfGE 108, 251 (269) = NJW 2003, 3401 (3402); H.H. Klein, in: Maunz/Dürig, Grundgesetz-Kommentar, Art. 38 Rn. 235 (Stand: 49. Lfg. 2007); H.-P. Schneider, in: AK-GG, 3. Aufl. 2001 ff., Art. 47 Rn. 2.

¹³ Zur Kontrollfunktion des Parlaments und deren Informationsabhängigkeit: Morlok, in: Dreier, GG Band II, 2. Aufl. 2006, Art. 38 Rn. 41 f. und Rn. 131 zur Wahrnehmung der Kontrollfunktion durch die einzelnen Abgeordneten.

¹⁴ Morlok, in: Dreier, GG Band II, 2. Aufl. 2006, Art. 38 Rn. 142, 146 ff.; s. ferner: H.-P. Schneider, in: AK-GG, 3. Aufl. 2001 ff., Art. 38 Rn. 20.

¹⁵ Vgl. Trute, in: v. Münch/Kunig (Hrsg.), Grundgesetzkommentar Band 2, 5. Aufl. 2001, Art. 47 Rn. 17.

das Zeugnisverweigerungsrecht sowie das mit diesem verknüpfte Beschlagnahmeverbot (Art. 47 GG) das freie Mandat nur an seit langem bekannten prekären Stellen konkretisierend ab¹⁶. Sie sperren aber nicht den Rückgriff auf die Grundsatznorm des Art. 38 I 2 GG als Basis für neue rechtliche Konkretisierungen zum Schutz der Abgeordneten vor neuartigen Gefährdungen ihrer Unabhängigkeit. Alternativ wäre an eine erweiternde Auslegung etwa des Beschlagnahmeverbots aus Art. 47 S. 2 GG zu denken¹⁷, was allerdings unter anderem eine Abkehr von dessen Beschränkung auf den Schutz von Gegenständen im funktionellen Herrschaftsbereich der Abgeordneten¹⁸ verlangte, da die hier interessierenden Verkehrsdaten allein bei den Telekommunikationsdiensteanbietern anfallen und gespeichert werden.

Als Abgeordnete sind die Antragsteller in besonderem Maße auf Möglichkeiten zu vertraulicher Kommunikation mit Parteifreunden, Bürgern, Interessenvertretern, Medienvertretern und sonstigen Informanten oder Informationsmittlern angewiesen. Zudem können sie in hervorgehobenem Maße in das Visier von Ermittlungsbehörden oder Nachrichtendiensten geraten, wenn sie sich in ihrer parlamentarischen Funktion etwa regelmäßig über Inhalte rechtsextremer oder anderer von deutschen Sicherheitsbehörden beobachteter Internetseiten informieren sollten. Durch das Erhebungsverbot aus § 160a I i.V.m. § 53 I Nr. 4 StPO sind die Antragsteller nur hinsichtlich solcher Kommunikationen geschützt, für die ihnen ein Zeugnisverweigerungsrecht zusteht. Der Schutz reicht also nur so weit, wie ihnen in ihrer Eigenschaft als Abgeordnete von anderen Personen Tatsachen anvertraut werden. Er erfasst von vornherein nicht die Eigeninformation über das Internet. Ferner greift sein Schutz erst auf der Stufe der behördlichen Erhebung von Verkehrsdaten. Er bietet aber keinen Schutz auf der vorgelagerten Stufe der verdachtslosen und universellen Vorratsdatenspeicherung. Von dieser allein gehen aber bereits beschränkende Wirkungen auf das gesellschaftliche und individuelle Kommunikationsverhalten aus, die die Möglichkeiten der Antragsteller, ihr Mandat hinreichend unabhängig und effektiv auszuüben, deutlich reduzieren.

Deshalb ist das in Art. 38 I 2 GG begründete Statusrecht der Antragsteller auf eine effektive Wahrnehmung ihres freien Mandats durch einen umfassenden Schutz ihrer Kommunikationsbeziehungen vor staatlicher Überwachung durch Speicherung,

¹⁶ Vgl. Morlok, in: Dreier, GG Band II, 2. Aufl. 2006, Art. 38 Rn. 148.

¹⁷ Gutachten des Wissenschaftlichen Dienstes des LT Schleswig-Holstein v. 27.2.2006 zu den Auswirkungen des Richtlinienvorschlags KOM (2005) 438 endg. („Vorratsdatenspeicherung“) auf die Rechte der Abgeordneten, S. 14 ff.

¹⁸ Hierzu: BVerfGE 108, 251 (269 f.) = NJW 2003, 3401 (3402); zur diesbezüglichen Diskussion in der Literatur: Achterberg/Schulte, in: v. Mangoldt/Klein/Starck, GG II, 2005, Art. 47 Rn. 12; Trute, in: v. Münch/Kunig (Hrsg.), Grundgesetzkommentar Band 2, 5. Aufl. 2001, Art. 47 Rn. 13.

Auswertung, Nutzung und Übermittlung von Kommunikationsdaten auf die Bedingungen der Informationsgesellschaft einzustellen und zu konkretisieren. Dieser Schutz gilt selbstverständlich nicht schrankenlos. Insbesondere können sich aus dem Abgeordnetenstatus selbst, etwa der demokratischen Verantwortlichkeit der Abgeordneten¹⁹, Ausgestaltungsmöglichkeiten bzw. Eingriffsrechtfertigungen beispielsweise in Gestalt besonderer Transparenzpflichten ergeben²⁰. Vorliegend geht es aber nicht um die Wahrung demokratischer Transparenz, sondern den in der Regel verdeckten Zugriff staatlicher Behörden auf verdachtslos und universell auf Vorrat gespeicherte Daten. Ebenso wenig geht es den Antragstellern um ein besonderes oder gar persönliches Privileg gegenüber Ermittlungsbefugnissen der Sicherheitsbehörden. Entscheidend ist für sie vielmehr der rechtliche Schutz offener und vertrauensvoller Kommunikationsbeziehungen zu den durch sie repräsentierten Bürgern sowie ihrer autonomen Informationsmöglichkeiten im Interesse einer unabhängigen Mandatsausübung und der parlamentarischen Funktionsfähigkeit²¹.

Die als verletzt geltend gemachten Rechtspositionen gründen in einem aktuellen und konkreten Verfassungsrechtsverhältnis. Denn die Antragsteller streiten mit dem Antragsgegner um konkrete verfassungsrechtliche Positionen. Es handelt sich nicht um eine allgemeine, von eigenen Rechten des Antragstellers losgelöste, abstrakte Kontrolle der Verfassungsmäßigkeit des angegriffenen Gesetzes, was im Organstreit unzulässig wäre²².

III. Keine Unzulässigkeit aufgrund zwingender Vorgaben der Richtlinie 2006/24/EG

1. Möglichkeiten der verfassungsrechtlichen Kontrolle außerhalb zwingender Vorgaben der Richtlinie 2006/24/EG

¹⁹ Allg. hierzu *Trute*, in: v. Münch/Kunig (Hrsg.), Grundgesetzkommentar Band 2, 5. Aufl. 2001, Art. 38 Rn. 5, 79.

²⁰ S. hierzu die trotz ihrer unterschiedlichen dogmatischen Ausgangspunkte und sachlichen Wertungen jedenfalls derartige Regelungen gemeinsam nicht von vornherein für unzulässig erachteten Positionen der vier die Entscheidung tragenden und der vier abweichenden Richter in BVerfG v. 4.7.2007, 2 BvE 1/06 u.a., Tz. 271, 326 ff. einerseits und Tz. 345, 355 f. andererseits = NVwZ 2007, 916 (926, 931 f.; 932, 933).

²¹ Die grundsätzliche Unterscheidung der mit dem Abgeordnetenstatus verknüpften Funktionsrechte von Privilegien betont etwa auch: *H.H. Klein*, in: Maunz/Dürig, Grundgesetz-Kommentar, Art. 38 Rn. 235 (Stand: 49. Lfg. 2007).

²² BVerfGE 68, 1 (73); 73, 1 (30); 80, 188 (212); 104, 151 (193 f.).

Seit der Entscheidung des 1. Senats vom 13.3.2007 ist bis auf weiteres davon auszugehen, dass die Solange-Grundsätze des BVerfG zur Abschichtung der Wahrnehmung von Prüfungskompetenzen im Grundrechtsbereich zwischen BVerfG und EuGH auch für die verfassungsrechtliche Kontrolle nationaler Umsetzungsakte von EG-Richtlinien gelten. Deshalb wird eine innerstaatliche Rechtsvorschrift grundsätzlich nicht an den Grundrechten des Grundgesetzes gemessen, wenn das Gemeinschaftsrecht keinen Umsetzungsspielraum lässt, sondern zwingende Vorgaben trifft²³. Spielraumentscheidungen des Umsetzungsgesetzgebers außerhalb zwingender Richtlinienvorgaben überprüft das BVerfG jedoch am Maßstab der deutschen Grundrechte. Insbesondere hat der Umsetzungsgesetzgeber bei mehreren Umsetzungsoptionen den Verhältnismäßigkeitsgrundsatz zu beachten, also in der Formulierung der EU-Haftbefehlsentscheidung des 2. Senats Umsetzungsspielräume in einer grundrechtschonenden Weise auszufüllen²⁴.

Es ist bislang offen, inwieweit diese Grundsätze auf andere verfassungsrechtliche Kontrollmaßstäbe wie das hier geltend gemachte Abgeordnetenrecht der Antragsteller übertragbar sind. Hierauf ist zurückzukommen (C.III.). Jedenfalls steht einer Überprüfung von Spielraumentscheidungen des Antragsgegners bei der Umsetzung der Richtlinie 2006/24/EG an diesem Maßstab ebenso wenig im Wege wie im Grundrechtsbereich.

2. Umsetzungsspielräume nach der Richtlinie 2006/24/EG

Deshalb ist es von maßgeblicher Bedeutung, dass die Richtlinie 2006/24/EG den Mitgliedstaaten in erheblichem Umfang Umsetzungsspielräume belässt und nur wenige zwingende Mindestvorgaben trifft²⁵. Dies bedeutet, dass die Gesamtregelung der Vorratsdatenspeicherung im Gesetz vom 21.12.2007 in großem Umfang am Maßstab der deutschen Abgeordnetenrechte überprüft werden kann und ein Organstreitverfahren keinesfalls unzulässig ist. Im Einzelnen ist Folgendes festzuhalten:

²³ BVerfG, DVBl. 2007, 821 (Tz. 66 ff.).

²⁴ BVerfGE 113, 273 (300 ff.) = NJW 2005, 2289 (2291, 2293), wobei hieraus keine über den allgemeinen Verhältnismäßigkeitsgrundsatz und das Teilkriterium der Erforderlichkeit hinausgehenden Anforderungen aus dem Gebot der Grundrechtsschonung abgeleitet werden; in diesem Sinne zitiert auch die Entscheidung zur Umsetzung der Emissionshandelsrichtlinie 2003/87/EG zwar die entsprechende Formulierung aus der Haftbefehlsentscheidung, leitet daraus jedoch bei der Prüfung des Gleichheitsgrundsatzes keine erhöhten Anforderungen ab: BVerfG, DVBl. 2007, 821 (Tz. 70, 79 ff.).

²⁵ S. auch *Westphal*, EuR 2006, 706 (709 f.); zu eng: *Rusteberg*, VBilBW 2007, 171 (176 f.).

Zwingend festgelegt sind die mindestens zu speichernden Datenkategorien und Datentypen. Soweit das Umsetzungsgesetz über diese Mindestvorgaben hinausgehen sollte, erhöhen sich die mit dem vorliegenden Organstreitverfahren geltend gemachten Belastungen, soweit derzeit erkennbar, nur graduell. Ähnliches gilt für Regelungen im Umsetzungsgesetz, durch welche die gemeinschaftsrechtliche Mindestspeicherdauer von 6 Monaten überschritten wird. Die hierfür relevante Regelung in § 113a XI TKG dient zudem der Belastungsreduktion zugunsten der speicherverpflichteten TK-Unternehmen, ohne den Eingriff in die Abgeordnetenrechte der Antragsteller in qualitativ entscheidendem Umfang zu vertiefen. In beiden Bereichen ist die verfassungsrechtlich problematische Belastung somit bereits im Wesentlichen gemeinschaftsrechtlich vorgegeben.

Beträchtliche und vom deutschen Umsetzungsgesetzgeber in beachtlichem Maße genutzte Umsetzungsspielräume bestehen hingegen bezüglich der Speicher- und Verwendungszwecke, der zugriffsberechtigten Stellen, den Zugriffsvoraussetzungen und -verfahren, der Zweckbindung sowie den Anforderungen an die Datensicherheit.

Art. 1 I der Richtlinie 2006/24/EG erwähnt als Zweck der Vorratsdatenspeicherung die Gewährleistung, dass Verkehrsdaten zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten zur Verfügung stehen. Um Widersprüche zum bisher geltenden EG-Datenschutzrecht zu vermeiden, wurde durch Art. 11 der Richtlinie 2006/24/EG Art. 15 Ia in die TK-Datenschutz-Richtlinie 2002/58/EG eingefügt. Diese Vorschrift derogiert von den Anforderungen, die Art. 15 I der Richtlinie 2002/58/EG an Datenschutzbeschränkungen zugunsten der öffentlichen Sicherheit richtet. In der Folge wird zwar die mitgliedstaatliche Nutzung von auf Vorrat gespeicherten Verkehrsdaten für Zwecke der Verfolgung schwerer Straftaten im Sinne der Richtlinie 2006/24/EG allein durch diese Richtlinie selbst bestimmt. Wie der Erwägungsgrund 12 der Richtlinie 2006/24/EG in Übereinstimmung mit den vorangegangenen Verhandlungen auf europäischer Ebene klarstellt, gilt Art. 15 I der Richtlinie 2002/58/EG daneben aber unverändert weiter. Deshalb dürfen die Mitgliedstaaten zusätzliche Verwendungszwecke, wie die in § 113b I TKG genannten Zwecke der Gefahrenabwehr und der nachrichtendienstlichen Verwendung, in den gemeinschaftsrechtlichen Grenzen des § 15 I der Richtlinie 2002/58/EG einführen²⁶. Sie sind dazu aber keineswegs verpflichtet, weil Art. 15 I der Richtlinie 2002/58/EG nur Mindestanforderungen der Verhältnismäßigkeit begründet. Im Ergebnis unterliegt die mitgliedstaatliche Festlegung weiterer Verwendungszwecke für auf Vorrat gespeicherte Daten uneingeschränkter verfassungsrechtlicher Kontrolle.

²⁶

Bundesregierung, Gesetzesbegründung, BT-Drs. 16/5846, S. 28 f., 73.

Dies gilt partiell sogar für die Verwendung zu Strafverfolgungszwecken. Art. 1 I und Erwägungsgrund 21 der Richtlinie 2006/24/EG legen die Konkretisierung des unbestimmten Rechtsbegriffs der schweren Straftaten durch die Formulierung „wie sie von jedem Mitgliedstaat in seinem nationalen Recht bestimmt werden“ nämlich ausdrücklich weitgehend in die Hand der Mitgliedstaaten²⁷. Gemeinschaftsrechtlich zwingend vorgegeben ist durch verschiedene Bezugnahmen in den Erwägungsgründen 7 bis 10 lediglich²⁸, dass die Mitgliedstaaten insbesondere die Organisierte Kriminalität sowie terroristische Akte als schwere Straftaten einzustufen haben. Damit führt die Richtlinie 2006/24/EG die betonte Berücksichtigung nationaler Souveränität in Fragen der inneren Sicherheit fort, wie es ausweislich der Art. 3 II, 13 I der Richtlinie 95/46/EG und des Art. 15 I der Richtlinie 2002/58/EG im europäischen Datenschutzrecht seit langem üblich ist²⁹. Unabhängig davon, ob in anderen strafrechtsbezogenen Gemeinschaftsrechtsakten unter den Begriffen der „schweren Straftaten“ bzw. der „serious crimes“ auch minder schwere Delikte zu verstehen sind³⁰, begründet die angesprochene ergänzende Formulierung jedenfalls im hier allein interessierenden Zusammenhang einen beachtlichen Gestaltungsspielraum für die nationale Sicherheitspolitik³¹. Dabei beschränkt nur die gemeinschaftsrechtliche Grenze der mindestens als schwere Straftaten einzustufenden Kriminalitätsfelder (Organisierte Kriminalität und Terrorismus) die verfassungsgerichtliche Kontrolle. Sofern das Gemeinschaftsrecht umgekehrt die Speicherung und Datenverwendung für die Verfolgung nicht mehr als schwer einzustufender Straftaten verbieten sollte³², folgt daraus jedenfalls kein Hindernis für eine parallele Prüfung anhand des nationalen Verfassungsrechts³³.

Ein weitgehender Verweis auf Gestaltungsentscheidungen im innerstaatlichen Recht findet sich ferner in Art. 4 S. 1 der Richtlinie 2006/24/EG bezüglich der Festlegung der zuständigen nationalen Behörden sowie der Verfahren und materiellen Bedingungen für den Zugang zu den auf Vorrat gespeicherten Daten³⁴. Dass dabei u.a. Verhältnismäßigkeitsanforderungen sowie die EMRK zu berücksichtigen sind, ist

²⁷ S. auch *Westphal*, EuZW 2006, 555 (558).

²⁸ Ein entsprechender Hinweis am Ende von Art. 1 I fand sich auch noch im Kommissionsvorschlag, KOM 2005 (438) endg. Seine Streichung hat den Handlungsspielraum der Mitgliedstaaten weder erweitert noch verengt.

²⁹ Vgl. dazu auch *Simitis*, NJW 2004, 2011 (2012).

³⁰ Bundesregierung, Gesetzesbegründung, BT-Drs. 16/5846, S. 52 f.

³¹ S. auch *Gola u.a.*, NJW 2007, 2599 (2601).

³² Vgl. hierzu mit überzeugender Begründung: GA'in *Kokott*, Schlussanträge vom 18.7.2007 in der Rs. C-275/06, Tz. 124; *Gitter/Schnabel*, MMR 2007, 411 (415).

³³ Vgl. BVerfGE 115, 276 (316 f.)

³⁴ S. auch *Westphal*, EuZW 2006, 555 (556, 559).

erkennbar als grundrechtlicher Mindestmaßstab gemeint, der keinesfalls strengeren Anforderungen des nationalen Rechts etwa zum Schutz der Abgeordnetenrechte der Antragsteller entgegensteht.

Schließlich enthält Art. 7 der Richtlinie 2006/24/EG ausdrücklich („zumindest“) nur Mindestanforderungen an die Datensicherheit. Diese blockieren keine weiterreichenden Anforderungen oder Verfassungsgebote an die Datensicherheit oder die datenschutzrechtliche Zweckbindung³⁵.

IV. Zwischenergebnis zur Zulässigkeit des Organstreitverfahrens

Nach alledem ist der vorliegende Antrag im Organstreitverfahren zulässig. Insbesondere lässt die Richtlinie 2006/24/EG in großem Umfang Umsetzungsspielräume, deren Nutzung uneingeschränkt verfassungsgerichtlicher Kontrolle am Maßstab der hier geltend gemachten Abgeordnetenrechte aus Art. 38 I 2 GG unterliegt.

C. Erweiterung des verfassungsgerichtlichen Prüfungsgegenstands bei Inexistenz oder Ungültigkeit der Richtlinie 2006/24/EG

Zwar belässt die Richtlinie 2006/24/EG den Mitgliedstaaten, wie die vorstehenden Ausführungen gezeigt haben, im großen Umfang Umsetzungsspielräume. Zwingend vorgegeben sind jedoch insbesondere

- die sechsmonatige Speicherpflicht von Anbietern öffentlicher TK-Dienste für die in Art. 5 der Richtlinie 2006/24/EG aufgeführten Datenkategorien;
- die Verwendung dieser Daten zur staatlichen Verfolgung schwerer Straftaten jedenfalls in Gestalt der Organisierten Kriminalität und des Terrorismus.

Inwieweit die aus der Solange-Rechtsprechung folgende Sperre für eine grundrechtliche Überprüfung der Regelungen zur Vorratsdatenspeicherung auf die in diesem Verfahren von den Antragstellern angestrebte Überprüfung am Maßstab ihrer Abgeordnetenrechte zu übertragen ist, ist eine bislang kaum diskutierte und erst recht nicht geklärte Problematik³⁶.

³⁵ S. auch *Westphal*, EuZW 2006, 555 (559).

³⁶ Erste Überlegungen hierzu finden sich im Gutachten des Wissenschaftlichen Dienstes des LT Schleswig-Holstein v. 27.2.2006 zu den Auswirkungen des Richtlinienvorschlags KOM (2005) 438 endg. („Vorratsdatenspeicherung“) auf die Rechte der Abgeordneten, S. 22 ff.

Angesichts des vom BVerfG betonten Kooperationsverhältnisses zum EuGH kommt eine verfassungsgerichtliche Überprüfung sekundärrechtlich zwingend vorgegebener Regelungen jedenfalls erst in Betracht, wenn der EuGH zunächst Gelegenheit zu einer eigenen Prüfung der strittigen Regelungen hatte. Dabei ist auch eine Prüfung durch den EuGH an Maßstäben von Bedeutung, die im nationalen Verfahren hinsichtlich der Umsetzungsakte keine Anwendung finden können. Offenkundig ist dies bezüglich einer Prüfung der europäischen Kompetenzgrundlagen für Sekundärrechtsakte. Vergleichbares muss vorliegend aber auch für die im Organstreit nicht zulässige direkte Prüfung an (Gemeinschafts-)Grundrechten gelten.

Eine etwaige Sperrwirkung entfielen jedenfalls, wenn der EuGH aufgrund der Klage Irlands in der Rechtssache C-301/06³⁷ oder auf eine – wie nachfolgend gezeigt – zulässige Vorlage durch das hohe Gericht die Ungültigkeit der Richtlinie feststellte (II.). Gleiches wäre anzunehmen, sofern die Richtlinie im Sinne der EuGH-Rechtsprechung inexistent wäre (I.). Die Inexistenz oder Ungültigerklärung der Richtlinie führte nicht automatisch zur Unbeachtlichkeit des deutschen Umsetzungsgesetzes. Sie eröffnete nach der Rechtsprechung des BVerfG jedoch die Möglichkeit für eine umfassende Prüfung am Maßstab der deutschen Grundrechte³⁸, was auf die hier angestrebte Überprüfung anhand der Abgeordnetenrechte übertragbar ist. Bei einer abweisenden Entscheidung des EuGH wäre die oben aufgeworfene Grundsatzfrage nach der Sperrwirkung für einen verfassungsgerichtlichen Schutz von Abgeordnetenrechte zu diskutieren (III.). Ferner wäre eine Überprüfung der Kompetenz zum Erlass der Richtlinie 2006/24/EG nach den Grundsätzen der Maastricht-Entscheidung in Betracht zu ziehen (IV.).

I. Uneingeschränkte verfassungsrechtliche Überprüfung des Gesetzes vom 21.12.2007 bei Inexistenz der Richtlinie 2006/24/EG

Das Gesetz vom 21.12.2007 unterläge einerseits uneingeschränkter verfassungsrechtlicher Kontrolle, wenn die Richtlinie 2006/24/EG mit einem derart schweren und offenkundigen Rechtsfehler behaftet wäre, dass die Gemeinschaftsrechtsordnung selbst die Richtlinie als inexistent behandelte³⁹. Klare

³⁷ S. ABI. EU 2006 C 237/5.

³⁸ BVerfG, DVBl. 2007, 821 (827).

³⁹ Zur Kategorie der inexistenten Rechtsakte, gegen die eine Nichtigkeitsklage gemäß Art. 230 EGV unzulässig ist: EuGHE 1999, I-4643, Tz. 94; 2004, I-8923, Tz. 19; EuGE 1992, II-315, Tz. 65; aus der Literatur: Dörr/Lenz, Europäischer Verwaltungsschutz, 2006, Rn. 93 f.; C. Annacker, EuZW 1995, 755 ff.

Abgrenzungskriterien zum bloß fehlerhaften Rechtsakt sind bislang nicht entwickelt worden. Gründe der Rechtssicherheit werden dafür angeführt, die Kategorie inexisterter Rechtsakte auf Ausnahmefälle zu beschränken⁴⁰. In Betracht kommt eine Inexistenz vor allem bei offensichtlichen Zuständigkeitsüberschreitungen⁴¹.

Daher ist vorliegend das Urteil des EuGH zum Abkommen über Fluggastdaten⁴² bemerkenswert. In diesem Urteil hat der EuGH Kompetenzüberschreitungen festgestellt, weil die streitigen Rechtsakte auf Gemeinschaftskompetenzen gestützt wurden, obwohl ihre Regelungsziele schwerpunktmäßig strafrechtlicher Natur waren und sie daher nach den Bestimmungen der im EUV verankerten dritten Säule der europäischen Verträge hätten erlassen werden müssen. Die streitige Richtlinie 2006/24/EG wirft kompetenzrechtlich vergleichbare, aber nicht völlig identische Zweifelsfragen auf⁴³. Generell gilt die Abgrenzung zwischen der ersten und dritten Säule der europäischen Verträge als besonders komplexe Fragestellung, für die der EuGH auch mit der Fluggastdatenentscheidung noch keine klaren Vorgaben entwickelt hat⁴⁴. Im Ergebnis erscheint die Annahme einer Inexistenz der Richtlinie 2006/24/EG durch den EuGH zwar nicht als ausgeschlossen, aber doch eher unwahrscheinlich.

II. Möglichkeit einer Gültigkeitsvorlage an den EuGH zur Beseitigung zwingender Vorgaben aus der Richtlinie 2006/24/EG

Da die Richtlinie aber jedenfalls an beachtlichen Rechtsmängeln leidet, rege ich eine Gültigkeitsvorlage an den EuGH zur Beseitigung der zwingenden Vorgaben aus der Richtlinie 2006/24/EG an.

1. Zulässigkeit und Notwendigkeit einer Vorlage an den EuGH durch das BVerfG

⁴⁰ EuGHE 1994, I-2555, Tz. 50; 1999, I-4643, Tz. 95; 2004, I-8923, Tz. 20;; *Dörr/Lenz*, Europäischer Verwaltungsrechtsschutz, 2006, Rn. 94; *Ehricke*, in: Grabitz/Hilf, Art. 230 EGV Rn. 13 ff.; *W. Cremer*, in: Calliess/Ruffert (Hrsg.), EUV/EGV, 3. Aufl. 2007, Art. 230 EGV Rn. 9.

⁴¹ *W. Cremer*, in: Calliess/Ruffert (Hrsg.), EUV/EGV, 3. Aufl. 2007, Art. 230 EGV Rn. 9.

⁴² EuGHE 2006, I-4721 ff. = NJW 2006, 2029 ff.

⁴³ GA Léger, Schlussanträge vom 22.11.2005 in den Rs. C-317/04 und 318/04 Fn. 77; s. ferner: *Westphal*, EuZW 2006, 555 (557 f.); *Leutheusser-Schnarrenberger*, ZRP 2007, 9 (11 ff.).

⁴⁴ *Jour-Schröder/Konow*, EuZW 2006, 550 (550 f.); *Westphal*, EuZW 2006, 406 (406 f.).

Das BVerfG gehört nach seiner eigenen Rechtsprechung zu den vorlageberechtigten und ggf. vorlageverpflichteten Gerichten i.S.d. Art. 234 EGV⁴⁵. Die Frage nach der Ungültigkeit der Richtlinie 2006/24/EG wegen eines Verstoßes etwa gegen das europäische Grundrecht auf Privatheit ist ein zulässiger Vorlagegegenstand gemäß Art. 234 EGV⁴⁶. Eine Gültigkeitsvorlage verlangt nicht, dass das hohe Gericht von der Ungültigkeit der Richtlinie abschließend überzeugt ist. Für eine Vorlagebefugnis genügen bereits Zweifel an der primärrechtlichen Rechtmäßigkeit der Richtlinie⁴⁷.

Die seit 2006 anhängige Nichtigkeitsklage Irlands gegen die Richtlinie 2006/24/EG in der Rechtssache 301/06 schließt die Zulässigkeit einer Vorlage durch das BVerfG nicht aus, soweit sich diese auf in der irischen Klage nicht geltend gemachte besondere rechtliche Gesichtspunkte bezieht⁴⁸. Da sich die irische Klage auf die Wahl der Ermächtigungsgrundlage beschränkt⁴⁹, rege ich eine Vorlage jedenfalls wegen Verstößen der Richtlinie gegen Gemeinschaftsgrundrechte (2.) an. Ergänzend sollte in diesem Verfahren auch die Frage nach der Vereinbarkeit mit einem Schutz von Abgeordnetenrechten (3.) vorgelegt werden. Mangels Klagemöglichkeit Privater gegen generell-abstrakte Richtlinien wie der Richtlinie 2006/24/EG ist eine Vorlage im Vorabentscheidungsverfahren nicht nach den Grundsätzen der Deggendorf-Rechtsprechung des EuGH präkludiert⁵⁰.

Die Voraussetzung der Entscheidungserheblichkeit⁵¹ ist erfüllt, weil bei Gültigkeit der Richtlinie 2006/24/EG eine Überprüfung der zwingend vorgegebenen Regelungen des Gesetzes vom 21.12.2007 am Maßstab der deutschen Abgeordnetenrechten mindestens zweifelhaft ist (unten III.), während bei einer Nichtigserklärung der Richtlinie durch den EuGH zwar das deutsche Umsetzungsgesetz nicht automatisch unbeachtlich wird, jedoch eine Überprüfung durch das BVerfG anhand der deutschen Abgeordnetenrechte hinsichtlich aller Gesetzesregelungen zur Vorratsdatenspeicherung eröffnet wird⁵².

⁴⁵ BVerfGE 37, 271 (282); 52, 187 (200 f.)

⁴⁶ Zur Zulässigkeit und zum Prüfungsmaßstab einer Gültigkeitsvorlage s. *Kischel*, in: Hailbronner/Wilms (Hrsg.), Art. 234 EGV Rn. 7, 10.

⁴⁷ *Dörr/Lenz*, Europäischer Verwaltungsschutz, 2006, Rn. 262.

⁴⁸ Vgl. zu diesen Anforderungen: EuGHE 2000, I-11.369 Tz. 57; *B. Wegener*, in: Calliess/Ruffert (Hrsg.), EUV/EGV, 3. Aufl. 2007, Art. 234 EGV Rn. 15.

⁴⁹ S. ABl. EU 2006 C 237/5.

⁵⁰ Zu dieser Rechtsprechung statt vieler: *Kischel*, in: Hailbronner/Wilms (Hrsg.), Art. 234 EGV Rn. 21.

⁵¹ Hierzu: *Kischel*, in: Hailbronner/Wilms (Hrsg.), Art. 234 EGV Rn. 22.

⁵² Vgl. hierzu allg. für den Grundrechtsbereich: BVerfG, DVBl. 2007, 821 (Tz. 72).

Nach der vom BVerfG in den letzten Jahren praktizierten Aufgabenabschichtung zwischen ihm und dem EuGH erfolgt der Grundrechtsschutz gegenüber gemeinschaftsrechtlich zwingend vorgegebenen nationalen Umsetzungsakten primär durch die zuständigen Fachgerichte. Diese sind ihrerseits ggf. auch verfassungsrechtlich verpflichtet, die Prüfungs- und Verwerfungskompetenz des EuGH im Wege der Vorabentscheidung gemäß Art. 234 EGV zu beachten⁵³. Entsprechende fachgerichtliche Verfahren sind auch gegenüber der Vorratsdatenspeicherung nicht ausgeschlossen. In diesen können jedoch nicht die im Organstreitverfahren maßgeblichen Abgeordnetenrechte geltend gemacht werden.

Unter diesen besonderen Umständen ist das BVerfG – trotz seiner bisher eher restriktiven Praxis⁵⁴ – gehalten, die Kooperation mit dem EuGH nicht den Fachgerichten zu überlassen, sondern das in der Maastricht-Entscheidung proklamierte Kooperationsverhältnis zu aktivieren. Andernfalls würde die verfassungsgerichtliche Überprüfung der Regelungen über die Vorratsdatenspeicherung empfindlich beschnitten, weil das hohe Gericht – ohne eine vorherige Überprüfung der sekundärrechtlichen Vorgaben durch den EuGH – gemeinschaftsrechtlich daran gehindert wäre, die erste Stufe der verdachtslosen Speicherung von Verkehrsdaten isoliert für verfassungswidrig und damit nichtig zu erklären.

Auf diese Weise könnte das BVerfG im Übrigen mit einer eigenen Analyse zum europäischen Grundrechtsdiskurs in einer besonders bedeutsamen rechtsstaatlichen Frage beitragen. Dies erscheint gerade mit Blick auf die große Erfahrung des BVerfG bei der rechtsstaatlichen und datenschutzrechtlichen Überprüfung von Sicherheitsgesetzen geboten. Dies gilt um so mehr, weil entsprechende materielle Rechtsfragen aufgrund des bisherigen wirtschaftsrechtlichen Schwerpunkts der EuGH-Rechtsprechung auf europäischer Ebene noch eine entwicklungsbedürftige Materie darstellen und etwa auch in der Fluggastdaten-Entscheidung⁵⁵ nicht erörtert werden mussten. Gleichzeitig werden sie jedoch wegen der zunehmenden

⁵³ S. zusammenfassend: J.-P. Schneider, Verfassungsgerichtsbarkeit und Europäischer Gerichtshof, in: Masing/Erbguth (Hrsg.), Verfassungs- und Verwaltungsgerichtsbarkeit im Mehrebenensystem. Referate und Diskussionsbeiträge des XV. Deutsch-Polnischen Verwaltungskolloquiums vom 9.-12. September 2007 an der Universität Freiburg im Breisgau, Boorberg Verlag Stuttgart u.a. (i.E.).

⁵⁴ BVerfG, EuGRZ 2004, 216 (219 f.).

⁵⁵ EuGHE 2006, I-4721 (Tz. 61, 70) = NJW 2006, 2029 ff.

sicherheitspolitischen Aktivitäten auf europäischer Ebene⁵⁶ zukünftig in der Rechtsprechung der Gemeinschaftsgerichte größeres Gewicht erhalten.

2. Verstoß der Richtlinie 2006/24/EG gegen Gemeinschaftsgrundrechte

Erhebliche Zweifel an der Rechtmäßigkeit der Richtlinie 2006/24/EG bestehen jedenfalls wegen eines Verstoßes gegen das vom EuGH anerkannte Gemeinschaftsgrundrecht auf Datenschutz⁵⁷. Die Generalanwältin Kokott hat ausdrücklich und unter Hinweis auf die Richtlinie 2006/24/EG Zweifel an Vereinbarkeit einer verdachtslosen Vorratsdatenspeicherung mit europäischen Grundrechten geäußert, wie sie zuvor bereits von den europäischen Datenschutzbeauftragten und anderen vorgebracht wurden⁵⁸. Allerdings musste die Generalanwältin wegen mangelnder Entscheidungserheblichkeit in der ihr vorliegenden Rechtssache auf eine abschließende Prüfung der Gültigkeit der Richtlinie 2006/24/EG verzichten.

Einschlägig ist insbesondere das Urteil des EuGH in der Rechtssache C-465/00⁵⁹, in dem dieser die europäische Datenschutzrichtlinie 95/46 im Lichte des Grundrechts auf Schutz der Privatsphäre bei der Verarbeitung personenbezogener Daten auslegte. Dieses Gemeinschaftsgrundrecht wird vom EuGH jedenfalls in dieser Entscheidung mit dem Recht auf Privatheit gemäß Art. 8 EMRK, wie es in der Rechtsprechung des EGMR entwickelt wurde, gleichgesetzt⁶⁰. Daher erscheint es in besonderem Maße gerechtfertigt, zur nachfolgenden Konkretisierung des Gemeinschaftsgrundrechts die Rechtsprechung des EGMR heranzuziehen.

Dies gilt insbesondere für die Definition des Schutzbereichs und die Eingriffsfeststellung. Für vom EuGH bislang noch nicht (datenschutzrechtlich) erörterte Telekommunikationsüberwachungsmaßnahmen greift der EGMR auf die in Art. 8 EMRK parallel garantierten Rechte auf Achtung des Privatlebens und der Korrespondenz

⁵⁶ Hinzuweisen ist an dieser Stelle nur auf die aktuelle rechtspolitische Diskussion in den EU-Gremien über ein System zur langjährigen Speicherung von Fluggastdaten: EU skeptisch über Datenspeicherung, in: FAZ vom 26.1.2008, S. 8.

⁵⁷ EuGHE 2003, I-4989 (Tz. 68 ff.) – ORF; jüngst EuGH vom 29.1.2008, Rs. C-275/06 Tz. 63 ff. sowie die vorherigen Schlussanträge von GA in Kokott v. 18.7.2007 in der Rs. C-275/06, Tz. 50 ff.

⁵⁸ GA in Kokott, Schlussanträge v. 18.7.2007 in der Rs. C-275/06, Tz. 82 mit FN. 43; s. auch Westphal EuZW 2006, 555 (558 ff.).

⁵⁹ EuGHE 2003, I-4989 (Tz. 68 ff.) – ORF; s. ferner: EuGHE 1969, 419 – Stauder; 1985, 3359 – Adams; ausführlich: B. Siemen, Datenschutz als europäisches Grundrecht, 2006; s. auch M. Albers, Informationelle Selbstbestimmung, 2005, S. 285 ff.

⁶⁰ Ähnlich: Ruffert, EuGRZ 2004, 466 (470); Siemen, EuR 2004, 306 (314 f.).

zurück⁶¹, weshalb sich eine Zuordnung zu einem dieser beiden Rechte erübrigt. Dabei wird das Recht auf Privatheit sehr weit verstanden, so dass auch (öffentliche) Kommunikationen mit beruflichem Hintergrund oder im politischen Meinungskampf ggf. in den Schutz einbezogen werden⁶². Ergänzend wäre mit Blick auf die Speicherung von Internetverbindungsdaten noch ein Eingriff in die Informationsfreiheit gemäß Art. 10 I 2 EMRK zu erwägen.

Diskutiert wird teilweise, ob der EuGH bereits die bloße Datenspeicherung als rechtfertigungsbedürftigen Eingriff erachtet. Dies wird gelegentlich unter Hinweis auf die Tz. 74 des ORF-Urteils verneint⁶³, wodurch eventuell die grundrechtlichen Bedenken gegen die erste Stufe der Vorratsdatenspeicherung auf der europäischen Ebene nicht zum Tragen kämen. Der EuGH formuliert dort wie folgt:

„Zwar kann die bloße Speicherung personenbezogener Daten über die an das Personal gezahlten Gehälter durch einen Arbeitgeber als solche keinen Eingriff in die Privatsphäre begründen, doch stellt die Weitergabe dieser Daten an einen Dritten [...] unabhängig von der späteren Verwendung der übermittelten Informationen [...] einen Eingriff im Sinne von Art. 8 EMRK dar.“

Allerdings ist nach dem Wortlaut nicht eindeutig, ob der Eingriffscharakter generell für Datenspeicherungen vom EuGH verneint werden soll oder nur für den vorliegenden Sonderfall der – grundsätzlich selbstverständlichen – Lohn- und Gehaltsbuchung bzw. -dokumentation durch Arbeitgeber⁶⁴. Die besseren Gründe sprechen für die zweite

⁶¹ EGMR v. 6.9.1978 (Application no. 5029/71) Tz. 41 – Klass = NJW 1979, 1755; v. 25.6.1992 (17/1991/269/340) Tz. 39 – Lüdi = NJW 1992, 3088; v. 16.2.2000 (Application no. 27798/95) Tz. 44 – Amann; v. 29.6.2006 (Application no. 54934/00) Tz. 76 ff. – Weber and Saravia; v. 28.6.2007 (Application no. 62540/00) Tz. 54, 58 ff. – Association for European Integration and Human Rights.

⁶² EGMR v. 4.5.2000 (Application no. 28341/95) Tz. 42 f. – Rotaru; v. 25.9.2001 (Application no. 44787/98) Tz. 56 – P.G and J.H.; 17.7.2003 (Application no. 63737/00) Tz. 36 – Perry.

⁶³ Ruffert, EuGRZ 2004, 466 (470); Gutachten des Wissenschaftlichen Dienstes des LT Schleswig-Holstein v. 27.2.2006 zu den Auswirkungen des Richtlinienvorschlags KOM (2005) 438 endg. („Vorratsdatenspeicherung“) auf die Rechte der Abgeordneten, S. 26.

⁶⁴ Die französische und englische Fassung sind ebenfalls nicht eindeutig, deuten aber tendenziell noch stärker die nachfolgend begründete Auslegung an: „It necessarily follows that, while the mere recording by an employer of data by name relating to the remuneration paid to his employees cannot as such constitute an interference with private life, the communication of that data to third parties, in the present case a public authority, infringes the right of the persons concerned to respect for private life, whatever the subsequent use of the information thus communicated, and constitutes an interference within the meaning of Article 8 of the Convention.“ bzw. „orçe est de constater que, si la simple mémorisation par l'employeur de données nominatives relatives aux rémunérations versées à son personnel ne saurait, comme telle, constituer une ingérence dans la vie privée, la communication de ces données à un tiers, en

l
Variante. Zunächst umschließt der Richtlinienbegriff der Datenverarbeitung, wie der EuGH nur kurz zuvor in der Tz. 64 – und in Übereinstimmung mit der Definition in Art. 2 lit. b) Richtlinie 95/46/EG – festhält, auch die Stufe der Speicherung. Bei einem grundsätzlich anderen Verständnis des Art. 8 EMRK hätte hier zumindest eine kurze Begründung nahegelegen⁶⁵. Vor allem aber widerspräche ein solch genereller Ausschluss der Speicherung als Eingriffstatbestand, dem offenkundigen Bemühen des EuGH in diesem Urteil, die Straßburger Vorgaben exakt nachzuzeichnen⁶⁶. In der Rechtsprechung des EGMR wird nämlich die Datenspeicherung seit langem als eingriffsbegründende Maßnahme eingestuft⁶⁷. Bei geheimen Überwachungsmaßnahmen genügt im Übrigen bereits eine gesetzliche Ermächtigung zur Verwirklichung des Eingriffstatbestands, ohne dass es tatsächlich zu Überwachungsmaßnahmen – vorliegend also eine tatsächliche Speicherung von Internetzugangsdaten oder die Weitergabe an Behörden durch die speicherverpflichteten Unternehmen – gegenüber den Antragstellern gekommen sein müsste⁶⁸.

Nach alledem begründet bereits die schlichte Vorratsdatenspeicherung einen Eingriff in das Gemeinschaftsgrundrecht auf Privatheit und Korrespondenz. Wie bei der Prüfung der deutschen Grundrechte liegt der eigentliche Kern des Problems allerdings bei der Rechtfertigung der Grundrechtseingriffe. In ständiger Rechtsprechung hat der EGMR für das Recht auf Datenschutz in Konkretisierung von Art. 8 II EMRK Kriterien entwickelt, die vom EuGH im zitierten ORF-Urteil ebenfalls grundsätzlich übernommen worden sind⁶⁹. Danach bedarf es einer gesetzlichen Ermächtigung, die für die Betroffenen hinreichend zugänglich ist, Bestimmtheitserfordernissen genügt sowie in einer demokratischen Gesellschaft notwendig ist, also rechtsstaatliche Grundsätze der Verhältnismäßigkeit nicht verletzt. Die diesbezüglichen Maßstäbe weichen nicht signifikant von denen der deutschen Rechtfertigungsprüfung insbesondere im

l'occurrence une autorité publique, porte atteinte au droit au respect de la vie privée des intéressés, quelle que soit l'utilisation ultérieure des informations ainsi communiquées, et présente le caractère d'une ingérence au sens de l'article 8 de la CEDH."

⁶⁵ Insbesondere weil GA Tizzano aufgrund seiner Auffassung bezüglich der Unanwendbarkeit des EG-Datenschutzrechts zu diesen Auslegungsfragen überhaupt keine Aussagen trifft: GA Tizzano, EuGHE 2003, I- 4989 Tz. 40 ff.

⁶⁶ S. hierzu: *Ruffert*, EuGRZ 2004, 466 (471).

⁶⁷ EGMR v. 26.3.1987 (Application no. 9248/81), Tz. 48 – Leander; v. 4.5.2000 (Application no. 28341/95) Tz. 43, 46 – Rotaru; s. auch *Rustenberg*, VBIBW 2007, 171 (176).

⁶⁸ EGMR v. 29.6.2006 (Application no. 54934/00) Tz. 78 – Weber and Saravia; v. 28.6.2007 (Application no. 62540/00) Tz. 69 – Association for European Integration and Human Rights.

⁶⁹ EGMR v. 28.6.2007 (Application no. 62540/00) Tz. 71 ff. – Association for European Integration and Human Rights; v. 26.3.1987 (Application no. 9248/81), Tz. 50 ff. – Leander; EuGHE 2003, I- 4989 Tz. 76 ff. – ORF.

Grundrechtsbereich, aber auch bei Eingriffen in die vorliegend relevanten „subjektiven“ Abgeordnetenrechte ab. Deshalb kann an dieser Stelle auf die entsprechenden Ausführungen zum deutschen Verfassungsrecht verwiesen werden⁷⁰.

3. Verstoß der Richtlinie 2006/24/EG gegen europäische Abgeordnetenrechte

Das EG-Primärrecht kennt keine ausdifferenzierten geschriebenen Statusrechte für Abgeordnete. Regelungen gibt es allein zu den Abgeordneten des Europäischen Parlaments. Diese sind nach Art. 189 I EGV Vertreter der Völker der in der Gemeinschaft zusammengeschlossenen Staaten. Nach Art. 190 V EGV kann das Europäische Parlament die Regelungen für die Wahrnehmung der Aufgaben seiner Mitglieder festlegen. Auf dieser Grundlage hat es 2005 das Abgeordnetenstatut des Europäischen Parlaments beschlossen⁷¹, das ab der 2009 beginnenden Legislaturperiode gelten wird. Nach seinem Art. 2 I sind die Abgeordneten frei und unabhängig und nach seinem Art. 3 I 2 weder an Aufträge noch an Weisungen gebunden. Eine Art. 3 I 2 des Abgeordnetenstatuts entsprechende Regelung enthält bereits seit 1976 Art. 4 I 2 des Akts zur Einführung allgemeiner unmittelbarer Wahlen der Abgeordneten der Versammlung⁷². Diese Regelungen sowie entsprechende Regelungen in diversen nationalen Verfassungen werden als Grundlage für einen gemeineuropäischen Grundsatz des freien Mandats verstanden⁷³.

Damit liegen die Voraussetzungen für die Anerkennung eines ungeschriebenen Allgemeinen Rechtsgrundsatzes des Gemeinschaftsrechts zum Schutze des Abgeordnetenstatus und der Ausübung des freien Mandats nach der Methode der wertenden Rechtsvergleichung durch den EuGH vor⁷⁴. Offener sind die exakten Inhalte eines solchen Allgemeinen Rechtsgrundsatzes, etwa hinsichtlich der vorliegend bedeutsamen Funktionsrechte. Für klassische Grundsätze wie die Indemnität und Immunität existieren zwar europa- und sogar weltweit verbreitete, auch auf Gemeinschaftsebene verankerte Abgeordnetenrechte zur Wahrung der

⁷⁰ S. unten D.II.

⁷¹ ABl. EU 2005 L 262/1 ff.

⁷² ABl. EG 1976 L 278/1 ff., ebenfalls abgedruckt bei Kluth, in: Calliess/Ruffert (Hrsg.), EUV/EGV, 3. Aufl. 2007, Art. 190 EGV vor Rn. 1.

⁷³ Kluth, in: Calliess/Ruffert (Hrsg.), EUV/EGV, 3. Aufl. 2007, Art. 190 EGV Rn. 12, 14; Morlok, in: Dreier, GG Band II, 2. Aufl. 2006, Art. 38 Rn. 19 mit Rn. 17; s. ferner Fleuter, Mandat und Statut des Abgeordneten im Europäischen Parlament, 1991, S. 108 ff.; Hölscheidt, in: Grabitz/Hilf, EUV/EGV, Art. 190 EGV Rn. 40 ff. (Stand 2005); Uppenbrink, Das Europäische Mandat – Status der Abgeordneten des Europäischen Parlaments, 2004, S. 49 ff., 88, 121 ff., 241 f.

⁷⁴ Generell zu den Voraussetzungen Allgemeiner Rechtsgrundsätze des Gemeinschaftsrechts: Wegener, in: Calliess/Ruffert (Hrsg.), EUV/EGV, 3. Aufl. 2007, Art. 220 EGV Rn. 38.

parlamentarischen Funktionsfähigkeit⁷⁵. Vergleichbares lässt sich beispielsweise für Zeugnisverweigerungsrechte nach dem Muster von Art. 47 GG nicht feststellen, wenngleich ähnliche Verbürgungen zumindest in einigen anderen europäischen Verfassungen ebenfalls enthalten sind⁷⁶.

Da Allgemeine Rechtsgrundsätze nicht einen schematisch ermittelten gemeinsamen Nenner der verschiedenen nationalen Lösungen voraussetzen, sondern nach der Methode der wertenden Rechtsvergleichung die bereichsspezifisch beste Lösung verwirklichen sollen⁷⁷, ist es keineswegs ausgeschlossen, dass der EuGH den Schutz des freien Mandats von Abgeordneten entsprechend den hier für das deutsche Verfassungsrecht entwickelten Grundsätzen konkretisiert. Insoweit wird auf die vorstehenden und nachfolgenden Ausführungen verwiesen. Eine Grenze wäre erst erreicht, wenn ein Funktionsrecht mit den Verfassungstraditionen der Mitgliedstaaten unvereinbar wäre. Davon kann aber im hiesigen Zusammenhang angesichts der grundsätzlichen Anerkennung des freien Mandats in den Rechtsordnungen der Mitgliedstaaten und der Gemeinschaft keinesfalls die Rede sein. Im Ergebnis wird daher angeregt, dem EuGH auch die Frage vorzulegen, ob die Richtlinie 2006/24/EG wegen eines Verstoßes gegen einen Allgemeinen Rechtsgrundsatz des Gemeinschaftsrechts zum Schutz des freien Mandats von Abgeordneten ungültig ist.

III. Folgen einer abweisenden EuGH-Entscheidung für den verfassungsgerichtlichen Schutz von Abgeordnetenrechten

Sollte der EuGH wider Erwarten die Nichtkeitsklage Irlands abweisen und auf eine Vorlage des BVerfG die Gültigkeit der Richtlinie 2006/24/EG bestätigen, stellen sich grundsätzliche Fragen. Einerseits wäre zu fragen, ob die Solange-Grundsätze überhaupt für den Schutz von Abgeordnetenrechten gelten. Andererseits wäre zu prüfen, ob die Voraussetzungen für ein Wiederaufleben der eigenständigen Prüfungskompetenz des BVerfG für zwingend vom Gemeinschaftsrecht vorgegebene Regelungen in deutschen Umsetzungsakten nach der Solange-Rechtsprechung in Bezug auf einen generell unzureichenden Schutz von Abgeordnetenrechten gegeben

⁷⁵ *Schulze-Fielitz*, in: Dreier, GG Band II, 2. Aufl. 2006, Art. 46 Rn. 4 ff.; zu verbleibenden Immunitätsschwächen: *Hölscheidt*, in: Grabitz/Hilf, EUV/EGV, Art. 190 EGV Rn. 44 (Stand 2005).

⁷⁶ *Schulze-Fielitz*, in: Dreier, GG Band II, 2. Aufl. 2006, Art. 47 Rn. 2 f.; *Uppenbrink*, Das Europäische Mandat – Status der Abgeordneten des Europäischen Parlaments, 2004, S. 71 f., 108 ff., 245 f.

⁷⁷ Zur Gewinnungsmethode für Allgemeine Rechtsgrundsätze: EuGHE 1974, 491 Tz. 13 – Nold; *Craig/de Búrca*, EU Law, 3rd ed. 2003, S. 327 ff.; *Streinz*, Europarecht, 7. Aufl. 2005, Rn. 759 ff.; *Wegener*, in: Calliess/Ruffert (Hrsg.), EUV/EGV, 3. Aufl. 2007, Art. 220 EGV Rn. 38.

sind. Angesichts der hohen Begründungsanforderungen des BVerfG für ein Wiederaufleben seiner eigenständigen Prüfungskompetenzen nach der Solange-Rechtsprechung verbieten sich im gegenwärtigen Verfahrensstadium entsprechende (hypothetische) Ausführungen. Das hohe Gericht wird vielmehr gebeten, in einem solchen Fall in Kenntnis der Argumentation des EuGH ergänzend vortragen zu dürfen.

IV. Subsidiäre kompetenzrechtliche Überprüfung der Richtlinie 2006/24/EG durch das BVerfG

Die Kernaussagen der Solange-Rechtsprechung beziehen sich bislang auf einen Vorrang der Gemeinschaftsgerichte beim Grundrechtsschutz gegen zwingende Richtlinienvorgaben. Das BVerfG hat im kompetenzrechtlichen Zusammenhang in der Maastricht-Entscheidung aber auch die Redeweise vom „ausbrechenden Rechtsakt“ geprägt, der nicht mehr vom innerstaatlich maßgeblichen Rechtsanwendungsbefehl gedeckt und daher für die deutschen Staatsorgane unverbindlich sei⁷⁸. Die exakten Verwerfungskompetenzen mussten bislang nicht geklärt werden⁷⁹.

Eine Analyse der jüngeren EuGH-Rechtsprechung ergibt, dass dieser die Kompetenzproblematik für die Sekundärrechtsetzung zwar stärker wahrnimmt⁸⁰, aber gleichwohl sehr problematische Schwankungen in seiner Prüfungsdichte festzustellen sind. Dies wird insbesondere am Urteil zur zweiten Tabakwerberichtlinie deutlich⁸¹. Der EuGH bleibt daher aufgerufen, seine kompetenzrechtliche Rechtsprechung zu konsolidieren und sich ähnlich wie beim Grundrechtsschutz das Vertrauen der nationalen Verfassungsgerichte und Rechtsunterworfenen zu erarbeiten. Das BVerfG sollte deshalb jedenfalls nicht voreilig in Parallele zum Grundrechtsbereich seine letztlich nicht disponible Kontrollkompetenz⁸² in eine bloße Auffangkompetenz modifizieren.

Da die Kompetenzfrage bereits mit der Nichtigkeitsklage Irlands gegen die Richtlinie 2006/24/EG beim EuGH zur Entscheidung ansteht, wäre eine Erstreckung des

⁷⁸ BVerfGE 89, 155 (188).

⁷⁹ Vgl. *Streinz*, Europarecht, 7. Aufl. 2005, Rn. 248, 251; *Wegener*, in: Calliess/Ruffert (Hrsg.), EGV/EUV-Kommentar, 3. Aufl. 2007, Art. 220 EGV Rn. 30.

⁸⁰ Vgl. die Analyse von *F.C. Mayer*, ZaöRV 61 (2001), 577 (595 ff.).

⁸¹ EuGH vom 12.12.2006 – C-380/03 (EuZW 2007, 46 ff.) mit krit. Anm. von *T. Stein*, EuZW 2007, 54 (56) und *Maierhöfer*, JZ 2007, 463 (464 f.).

⁸² *Streinz*, Europarecht, 7. Aufl. 2005, Rn. 247.

Vorabentscheidungsverfahrens auch auf diesen Aspekt problematisch⁸³. Auf nähere eigene Ausführungen zu dieser Problematik soll daher vorerst verzichtet werden⁸⁴. Für den unwahrscheinlichen Fall einer abweisenden Entscheidung des EuGH wird jedoch um Gelegenheit gebeten, im Lichte der Argumentation des EuGH ergänzend zu dieser Problematik und den Reaktionsmöglichkeiten des BVerfG Stellung nehmen zu dürfen.

D. Verletzung des freien Mandats gemäß Art. 38 I 2 GG durch die Regelungen zur Vorratsdatenspeicherung

I. Vorratsdatenspeicherung als Eingriff in das freie Mandat

Im Rahmen der Ausführungen zur Antragsbefugnis (B.II.) wurde bereits ausführlich begründet, weshalb die Regeln über die Vorratsdatenspeicherung eine Verletzung bzw. unmittelbare Gefährdung des durch Art. 38 I 2 GG geschützten freien Mandats bedeuten. Dabei wurde das Statusrecht durch eine Gewährleistung umfassenden, aber keineswegs schrankenlosen Schutzes der Kommunikationsbeziehungen von Abgeordneten vor staatlicher Überwachung durch Speicherung, Auswertung, Nutzung und Übermittlung von Kommunikationsdaten auf die Bedingungen der Informationsgesellschaft eingestellt. Geschützt sind im Interesse einer unabhängigen Mandatsausübung und der parlamentarischen Funktionsfähigkeit einerseits die Offenheit und Vertraulichkeit ihrer Kommunikationsbeziehungen zu den durch sie repräsentierten Bürgern sowie andererseits ihre eigenen autonomen Informationsmöglichkeiten. Zur Vermeidung unnötiger Wiederholungen wird auf diese Ausführungen verwiesen.

Dieses kommunikationsbezogene Funktionsrecht schützt wie Art. 10 GG⁸⁵ und Art. 47 GG⁸⁶ nicht nur Kommunikationsinhalte, sondern auch die Vertraulichkeit der näheren Umstände des Kommunikationsvorgangs. Hierzu gehören Informationen über Beteiligte, Ort, Zeit sowie Art und Weise der Kommunikation oder von

⁸³ Vgl.: EuGHE 2000, I-11369 Tz. 57; B. Wegener, in: Calliess/Ruffert, (Hrsg.), EUV/EGV, 3. Aufl. 2007, Art. 234 EGV Rn. 15.

⁸⁴ Aus der bisherigen Diskussion: GA Léger, Schlussanträge vom 22.11.2005 in den Rs. C-317/04 und 318/04 Fn. 77; s. ferner: Westphal, EuZW 2006, 555 (557 f.); Leutheusser-Schnarrenberger, ZRP 2007, 9 (11 ff.).

⁸⁵ BVerfGE 115, 166 (183) = NJW 2006, 976, Tz. 70; seit BVerfGE 67, 157 (172) st. Rspr.

⁸⁶ Schulze-Fielitz, in: Dreier, GG Band II, 2. Aufl. 2006, Art. 47 Rn. 8.

Kommunikationsversuchen⁸⁷. Grund für den Schutz von Telekommunikationsverkehrsdaten⁸⁸ ist, dass diese einen eigenen Aussagegehalt haben. Zudem geben Häufigkeit, Dauer und Zeitpunkt von Kommunikationsverbindungen Hinweise auf Art und Intensität von Beziehungen und können sogar inhaltliche Schlussfolgerungen ermöglichen⁸⁹. Die nach § 113a II bis IV TKG zu speichernden Verkehrsdaten fallen somit in den Schutzbereich des hier geltend gemachten kommunikationsbezogenen Funktionsrechts.

In den dadurch gewährten Schutz der Verkehrsdaten greifen die angegriffenen Regeln zur Verkehrsdatenspeicherung, -erhebung und -übermittlung in mehreren zusammenwirkenden Schritten ein. Insbesondere handelt es sich nicht um nach anderen Maßstäben zu überprüfenden Ausgestaltungen des Abgeordnetenstatus. Solche mehraktigen, zumindest teilweise im Zusammenhang zu bewertenden Eingriffe durch Speicherung, Übermittlung, Verarbeitung, Verwendung und Weitergabe sowie Begrenzungen der Rechtsschutzmöglichkeiten sind typisch für verdeckte Telekommunikationsüberwachungsmaßnahmen⁹⁰. Darüber hinaus kommt jedenfalls durch Verknüpfung mit weiteren Datenerhebungen sogar ein Eingriff in den Schutz von Kommunikationsinhalten in Betracht.

Die durch § 113a TKG veranlasste, bis zu sieben Monaten dauernde Speicherung von personenbezogenen Daten besitzt Eingriffscharakter, unabhängig davon ob die gespeicherten Daten anschließend tatsächlich an staatliche Ermittlungsbehörden übermittelt werden. Denn erst infolge der staatlichen Speicheranordnung stehen diese über einen beachtlichen Zeitraum für staatliche Zwecke zur Verfügung⁹¹. Bereits hierdurch kann das Kommunikationsverhalten der Bürger und anderer Informanten der Antragsteller verändert werden, weil sie befürchten müssen, zu einem späteren

⁸⁷ Für Art. 10 GG: BVerfGE 100, 313 (358) = NJW 2005, 55 (56 f.); BVerfG-K, NJW 2007, 3055 (Tz. 12).

⁸⁸ Für Art. 10 GG: BVerfGE 115, 166 (183) = NJW 2006, 976, Tz. 71; BVerfG-K, NJW 2007, 3055 (Tz. 12); für das Recht auf informationelle Selbstbestimmung: BVerfGE 107, 299 (313) = NJW 2003, 1787 (1788 f.)

⁸⁹ Für Art. 10 GG: BVerfGE 115, 166 (183) = NJW 2006, 976, Tz. 70 f. m.w.N.

⁹⁰ Vgl. BVerfGE 100, 313 (366 f.) = NJW 2000, 55 (59). S. ferner BVerfGE 115, 320 (343) = NJW 2006, 1939 Tz. 74.

⁹¹ Dadurch unterscheidet sich die Betroffenheit durch die Vorratsdatenspeicherung ohne Datenübermittlung von der solcher Anschlussinhaber, deren Daten bei einer sogenannten Zielwahlsuche zwar von den TK-Unternehmen automatisch abgeglichen, aufgrund eines negativen Ergebnisses jedoch „spurenlos“ nicht an die Behörden übermittelt werden; es handelt sich bei der Vorratsdatenspeicherung keinesfalls um eine vergleichbar geringfügige Betroffenheit wie bei einer negativen Zielwahlsuche, die deshalb nach Ansicht des BVerfG (BVerfGE 107, 299 (328) = NJW 2003, 1787 (1792 f.)) noch keinen Eingriff darstellen soll.

Zeitpunkt aufgrund dann möglicher, heute noch nicht absehbarer Datenverknüpfungen zum Objekt staatlicher Ermittlungen zu werden. Ferner erstreckt sich die Schutzwirkung von Art. 38 I 2 GG auch auf Informations- und Datenverarbeitungsprozesse, die sich an die Kenntnisnahme von geschützten Kommunikationsvorgängen anschließen, sowie auf den Gebrauch, der von erlangten Kenntnissen gemacht wird⁹². Zusätzliche durch § 113b TKG ausdrücklich zugelassene und vorgezeichnete Eingriffe bestehen in der Übermittlung von Verkehrsdaten an staatliche Behörden etwa aufgrund einer Anordnung gemäß § 100g I StPO oder in der Übermittlung von Bestandsdaten gemäß §§ 161, 163 StPO i.V.m. §§ 112, 113 TKG, sofern diese erst unter Nutzung der auf Vorrat gespeicherten Verkehrsdaten von dem auskunftsverpflichteten TK-Dienstleister ermittelt werden konnten. Weitere Eingriffsakte sind die sich anschließende Auswertung und Verwendung dieser Daten durch die auskunftsberechtigten staatlichen Behörden. Schließlich erfolgen Eingriffe durch eine Weitergabe dieser Daten an andere Behörden (z.B. gemäß §§ 406e, 474, 481, 483 II, 487 StPO).

II. Verfassungsrechtliche Rechtfertigung

1. Rechtsgüter von Verfassungsrang als Schranken des freien Mandats

Die Freiheit des Mandats ist nicht schrankenlos gewährleistet. Begrenzungen müssen aber durch andere Rechtsgüter von Verfassungsrang legitimiert werden⁹³. Nach der Regierungsbegründung besteht der Zweck der Vorratsdatenspeicherung insbesondere in der Gewährleistung einer wirksamen Strafverfolgung⁹⁴. Dies ist zweifellos für einen Rechtsstaat ein legitimer Zweck, der auch Eingriffe in das freie Mandat rechtfertigen kann, wie schon der keineswegs absolute Schutz der Immunität von Abgeordneten zeigt.

2. Verhältnismäßigkeit

a) Eignung

Ein Gesetz ist nach der Rechtsprechung des BVerfG zur Zweckerreichung geeignet, wenn mit seiner Hilfe der erstrebte Erfolg gefördert werden kann⁹⁵. Die Eignung scheitert nicht an einer großen Streubreite von Erfassungsmethoden, selbst wenn diese

⁹² Für Art. 10 GG: BVerfGE 100, 313 (359) = NJW 2000, 55 (57).

⁹³ Morlok, in: Dreier, GG Band II, 2. Aufl. 2006, Art. 38 Rn. 151 ff.

⁹⁴ Bundesregierung, Gesetzesbegründung, BT-Drs. 16/5846, S. 30.

⁹⁵ BVerfGE 115, 320 (345) = NJW 2006, 1939 (1941) m.w.N.

nur in vergleichsweise wenigen Fällen Erkenntnisse versprechen⁹⁶. Für die Angemessenheit der Regelung kann dies allerdings einen relevanten Faktor darstellen.

Die Bundesregierung hält die Vorratsdatenspeicherung für ein Instrument von großer Wichtigkeit⁹⁷, das sogar in bestimmten Bereichen unverzichtbar sei⁹⁸. Diese Einschätzung ist allerdings nach den vorliegenden empirischen Untersuchungen zur Effektivität von Maßnahmen der Telekommunikationsüberwachung einerseits und zum Fehlen zusätzlicher Überwachungsinstrumente nach altem Recht andererseits erheblichen Zweifeln ausgesetzt⁹⁹. Vielmehr spricht manches dafür, dass die Vorratsdatenspeicherung zu einem kaum nutzbaren Datenfriedhof durch Überinformation führen wird¹⁰⁰ oder plastischer zu einer Anhäufung von Heuhaufen, um terroristische Stecknadeln zu suchen¹⁰¹. Angesichts des anerkannten gesetzgeberischen Einschätzungsspielraums wird man gegenwärtig die Eignung der Vorratsdatenspeicherung gleichwohl noch nicht verneinen können. Dies zeigt auch die Rechtsprechung zur Rasterfahndung, die nachweislich und bekanntermaßen keine strafrechtlich verwertbaren Erkenntnisse erbracht hatte, und gleichwohl vom hohen Gericht nicht als von vornherein ungeeignet eingestuft wurde¹⁰². Allerdings werden die hier vorgetragenen Bedenken bei der Angemessenheitsprüfung zu berücksichtigen sein.

⁹⁶ BVerfGE 115, 320 (345) = NJW 2006, 1939 (1941); BVerfGE 100, 313 (373) = NJW 2000, 55 (60 f.); 107, 299 (316).

⁹⁷ Bundesregierung, Gesetzesbegründung, BT-Drs. 16/5846, S. 30 f.; statt vieler: Seitz, Strafverfolgungsmaßnahmen im Internet, 2004, S. 147.

⁹⁸ Bundesregierung, Gesetzesbegründung, BT-Drs. 16/5846, S. 23, 31; Bundesrat, Stellungnahme, BT-Drs. 16/5846, S. 88.

⁹⁹ Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Stellungnahme vom 27.6.2007 zum Gesetzentwurf der Bundesregierung für ein Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG, S. 19 f. unter Bezugnahme auf die allerdings zu anderen Schlussfolgerungen kommende Untersuchung von Mahnken, Mindestspeicherfristen für Telekommunikationsverbindungsdaten – Rechtstatsachen zum Beleg der defizitären Rechtslage, hrsg. vom Bundeskriminalamt, Stand 15.11.2005.

¹⁰⁰ Westphal, EuZW 2006, 555 (558).

¹⁰¹ Dix, Vortrag vom 7.11.2007 (www.datenschutz-berlin.de unter Aktuelles/Datenschutznachrichten 2007), S.2.; ähnlich: Gola u.a., NJW 2007, 2598 (2599); s. auch „Kinderporno-Verdacht ohne Folgen?“, Neue Osnabrücker Zeitung v. 31.12.2007, S. 25 mit Berichten zu kritischen Stellungnahmen aus nordrhein-westfälischen Strafverfolgungsbehörden über eine bundesweite Operation gegen Kinderpornographie mit anfangs 12 000 Verdächtigen und sehr wenig Ertrag.

¹⁰² BVerfGE 115, 320 (329 ff.).

b) Erforderlichkeit

Die Erforderlichkeit ist nur zu verneinen, wenn der gesetzgeberische Zweck durch mildere Mittel ebenso wirksam erreicht werden kann. Dabei ist bei der Überprüfung von Gesetzen die Einschätzungsprerogative des Gesetzgebers hinreichend zu beachten.

Angesichts entsprechender Einwände in der rechtspolitischen Diskussion¹⁰³ setzt sich die Gesetzesbegründung ausführlich mit dem Instrument des sogenannten Quick-Freeze als Alternative auseinander, das etwa in Art. 16 II des Europarats-Übereinkommens zur Computerkriminalität u.a. zur Verfolgung von Urheberrechtsverletzungen (Art. 14 II iVm Art. 10 des Übereinkommens) vorgesehen ist¹⁰⁴.

Die Regierung bestreitet die gleiche Eignung dieser Methode damit, dass die Speicherung von Verkehrsdaten auf Einzelfallanordnung ins Leere gehe, wenn diese bereits gelöscht wären oder gar nicht erst gespeichert würden¹⁰⁵. Letzteres war nach bisheriger Rechtslage zB bei Pauschaltarifen sogar zwingend geboten¹⁰⁶. Ergänzend verweist sie auf ein kompliziertes und für die TK-Unternehmen aufwändigeres Nebeneinander von Vorratsdatenspeicherung bzgl. schwerer oder erheblicher Straftaten und Quick-Freeze für – nicht schwere bzw. nicht erhebliche – TK-Taten¹⁰⁷. Angesichts des dem Gesetzgeber eingeräumten Einschätzungsspielraums wird man nach gegenwärtigem Kenntnisstand die Erforderlichkeit noch nicht in Frage stellen können. Auch diesbezüglich ist allerdings der tatsächliche Mehrwert der Vorratsdatenspeicherung eher als gering einzustufen. Deshalb wird die immerhin partiell mögliche Ersetzung der Vorratsdatenspeicherung durch ein Quick-Freeze-Verfahren bei der Angemessenheitsprüfung zu berücksichtigen sein.

¹⁰³ Statt vieler *Gola u.a.*, NJW 2007, 2599 (2600); *Westphal*, EuR 2003, 706 (715); ders., EuZW 2006, 555 (558); Wissenschaftlicher Dienst des Deutschen Bundestages, Zulässigkeit der Vorratsdatenspeicherung nach europäischem und deutschen Recht, WD 3 – 282/06, S. 13 f.; *Zöller*, GA 2007, 393 (411 f.).

¹⁰⁴ Bundesregierung, Gesetzesbegründung, BT-Drs. 16/5846, S. 53 f.

¹⁰⁵ Bundesregierung, Gesetzesbegründung, BT-Drs. 16/5846, S. 31, s. auch S. 53; *Seitz*, Strafverfolgungsmaßnahmen im Internet, 2004, 242; s. ferner *Mahnken*, Mindestspeicherfristen für Telekommunikationsverbindungsdaten – Rechtstatsachen zum Beleg der defizitären Rechtslage, hrsg. vom Bundeskriminalamt, Stand 15.11.2005, 18 f.

¹⁰⁶ Zum diesbzgl. Speicherverbot BGH, MMR 2007, 37; s. auch die Vorinstanz: LG Darmstadt, MMR 2006, 330 ff.

¹⁰⁷ Bundesregierung, Gesetzesbegründung, BT-Drs. 16/5846, S. 54.

c) Angemessenheit

Die verfassungsrechtliche Kernfrage bezüglich der Rechtfertigung des Eingriffs in das freie Mandat durch die Vorratsdatenspeicherung ist demnach deren Angemessenheit bzw. Verhältnismäßigkeit im engeren Sinne. Wie zuvor gezeigt, wird das freie Mandat der Antragsteller sowohl durch eine eventuelle Überwachung ihrer direkten Informationsaktivitäten und Kommunikationsbeziehungen als auch durch die Gefährdung ihrer Repräsentationsfunktion infolge von durch die Vorratsdatenspeicherung allgemein veranlasste Verhaltensanpassungen der Bürger beeinträchtigt. Deshalb sind im Folgenden beide Wirkungspfade der Vorratsdatenspeicherung zu berücksichtigen. Auch grundrechtliche Gewichtungen sind zu berücksichtigen, sofern diese Rückschlüsse auf das Maß und die Wahrscheinlichkeit von Verhaltensanpassungen der Bürger mit Rückwirkungen auf die Kommunikationsbeziehungen zu den Antragstellern und anderen Abgeordneten zulassen. Zudem hat der Zweite Senat in seiner Entscheidung vom 4.7.2007 ungeachtet von Meinungsverschiedenheiten in der konkreten Gewichtung grundsätzlich anerkannt, dass bei der Geltendmachung von Statusrechten mit einer Organklage, zwar Grundrechte der Antragsteller nicht als eigenständige Prüfungsmaßstäbe herangezogen, diese aber sehr wohl abwägend mitberücksichtigt werden dürfen¹⁰⁸. Gleichwohl können die Ergebnisse einer grundrechtlichen Angemessenheitsprüfung, wie sie mit der parallel eingereichten Verfassungsbeschwerde angestrebt wird, hinsichtlich einzelner Regelungen zur Vorratsdatenspeicherung abweichend ausfallen, weil die grundrechtlichen Belange im Rahmen der statusrechtlichen Angemessenheitsprüfung nicht umfassend und nur vermittelt zur Geltung kommen.

Bei alledem empfiehlt es sich, zwischen den gemeinschaftsrechtlich zwingend vorgegebenen Aspekten und den Spielraumentscheidungen des deutschen Umsetzungsgesetzgebers zu unterscheiden. Letztere stehen im Zentrum der nachfolgenden Ausführungen (aa). Für den Fall, dass der EuGH die Richtlinie 2006/24/EG in der Rs. C-301/06 wegen Kompetenzverstößen oder auf eine Vorlage durch das BVerfG für unwirksam erklärt, finden sich nachfolgend auch Ausführungen zu den derzeit gemeinschaftsrechtlich zwingend vorgegebenen Aspekten (bb). Ihnen kommt zusätzliche Bedeutung für die tendenziell parallele Rechtfertigungsprüfung im Zusammenhang mit dem oben erörterten Eingriff in das Gemeinschaftsgrundrecht auf Datenschutz bzw. des europäischen Schutzes des freien Mandats zu.

¹⁰⁸ BVerfG, v.4.7.2007, 2 BvE 1/06 u.a., Tz. 197, 276, 338, 340 ff. = NVwZ 2007, 916 (918, 926, 931, 932).

aa) Unverhältnismäßigkeit von Spielraumentscheidungen des deutschen Gesetzgebers

(1) Schutzwürdigkeit von Verkehrsdaten und verdachtslose Vorratsdatenspeicherung

Die nachfolgend differenziert zu beurteilende Angemessenheit einzelner Spielraumentscheidungen des deutschen Gesetzgebers hängt von der generellen Schutzwürdigkeit von Verkehrsdaten und der mit der vorgelagerten verdachtslosen Vorratsdatenspeicherung verbundenen besonderen Eingriffsintensität ab. Zwar ist die Vorratsdatenspeicherung gemeinschaftsrechtlich bislang zwingend vorgegeben. Dadurch ist aber – bis zu einer gemeinschaftsgerichtlichen Ungültigerklärung der Richtlinie – nur ihre isolierte verfassungsrechtliche Beurteilung ausgeschlossen. Daneben steht ihre eingriffsvertiefende Wirkung bezüglich nicht gemeinschaftsrechtlich vorgegebener, sondern auf autonomen Entscheidungen des deutschen Gesetzgebers beruhender Befugnisse zur Verwendung gespeicherter Verkehrsdaten. Diese Intensitätssteigerung folgt aus der durch die verdachtslose und universelle Vorratsdatenspeicherung erheblich erhöhten Verfügbarkeit nutzbarer Verkehrsdaten und darf bei der verfassungsrechtlichen Überprüfung der Spielraumentscheidungen nicht ausgeblendet werden.

Bedeutsam für das Maß der hier relevanten Beeinträchtigung des parlamentarischen Funktionsrechts durch die verdachtslose Vorratsdatenspeicherung ist die Intensität der nachfolgend aufgezeigten individuellen Betroffenheit durch staatliche Datenverarbeitungsmaßnahmen mit großer Streuwirkung ohne qualifizierte Anwendungshürden, weil von diesen subjektiven Betroffenheiten Rückwirkungen auf gesamtgesellschaftliche Verhaltensmuster und damit auf die hier interessierenden kommunikativen Vertrauensbeziehungen sowie den allgemeinen demokratischen Diskurs ausgehen können¹⁰⁹. Dabei sind nicht nur aktuelle Rechtsbetroffenheiten, sondern auch nachvollziehbare Befürchtungen relevant¹¹⁰, die sich auch auf widerrechtlichen Missbrauch gespeicherter Daten durch Private oder staatliche Stellen beziehen können¹¹¹.

Verkehrsdaten werden oft als weniger schutzbedürftig als Inhaltsdaten eingestuft. Gleichwohl darf die mit ihrer Speicherung auf Vorrat verbundene Eingriffsintensität nicht unterschätzt werden. Verkehrsdaten haben schon isoliert einen besonders schutzwürdigen Aussagegehalt, da sie erhebliche Rückschlüsse auf das

¹⁰⁹ Vgl. BVerfGE 100, 313 (381).

¹¹⁰ Vgl. BVerfG, NJW 2003, 1787 (1793); E 100, 313 (376).

¹¹¹ Vgl. BVerfGE 65, 1 (46); 85, 386 (397, 400); BVerfG-K, NJW 2007, 3055 (3056 Tz. 17).

26

Kommunikations- oder Bewegungsverhalten der TK-Nutzer zulassen¹¹². Verkehrsdaten sind aufgrund ihrer unproblematischen automatischen Auswertbarkeit und relativen Überschaubarkeit für Rasterfahndungsmethoden bzw. strategische Überwachungen durch Nachrichtendienste sogar besonders geeignet und können dadurch Vorteile gegenüber nur mit erheblich größerem Aufwand auswertbaren Inhaltsdaten aufweisen. Sie sind somit ein naheliegendes Instrument zur Identifikation von Ermittlungsansätzen. Insbesondere können sie dazu dienen, soziale, politische oder wirtschaftliche Beziehungsnetzwerke zu rekonstruieren und diese anhand von Häufigkeit oder Dauer der Kommunikation auf ihre Intensität hin zu analysieren. Dabei sind Fehlbeurteilungen selbstverständlich nicht ausgeschlossen, wenn z.B. intensive individuelle Kommunikationsbeziehungen aus einem, etwa familiären oder politischen, sozialen Kontext als Teil einer ganz anderen, etwa kriminellen, Kommunikationsstruktur erscheinen. Die Folgen für die Betroffenen sind offenkundig, sie werden zum Gegenstand staatlicher Ermittlungen mit allen Belastungen, die diese unvermeidlich mit sich bringen.

Zusätzlich erhöht wird die Schutzbedürftigkeit von Verkehrsdaten durch vielfältige Möglichkeiten der Verknüpfung mit anderen, bei den Ermittlungsbehörden oder bei auskunftsberechtigten Privaten vorhandenen Daten beispielsweise zu Inhalten von Internetnutzungen. Vielfach diskutiert werden insoweit private Datensammlungen über die auf Tauschbörsen aktiven dynamischen IP-Adressen durch Urheberrechtsinhaber, die gemeinsam mit gespeicherten Verkehrsdaten zur Identifizierung der dahinterstehenden Anschlussinhaber genutzt werden¹¹³. Im Zusammenhang mit dem freien Mandat interessieren hingegen stärker Datenverknüpfungen bei der behördlichen Beobachtung politisch auffälliger Internetseiten z.B. neonazistischen Inhalts, auf die gerade auch die Antragsteller als politische Akteure zur informierten Bekämpfung solcher Inhalte gelegentlich zugreifen mögen. Durch derartige Verknüpfungen können letztlich umfassende Persönlichkeitsprofile erstellt werden. Mit guten Gründen hat daher das BVerfG sogar eine Schutzpflicht des Staates gegen ungerechtfertigte private Verkehrsdatenspeicherungen angenommen, selbst wenn die Speicherung nur wenige Tage andauert¹¹⁴. Damit hat das Gericht den Grundsatz der Datensparsamkeit als dem

¹¹² BVerfGE 115, 166 (190); BVerfGE 100 (313) = NJW 2000, 55 (64 ff.); s. auch: Bundesregierung, Gesetzesbegründung, BT-Drs. 16/5846, S. 31; die gegenteilige Bewertung von isolierten Kontostammdaten (BVerfG, NJW 2007, 2464 (2470 Tz. 136)), kann also keinesfalls auf die Verkehrsdaten übertragen werden.

¹¹³ Hierzu näher GA Kokott, Schlussanträge in der Rs. 275/06, Tz. 29 ff.; *Beck/Kreißig*, NSiZ 2007, 304 ff.; *Dietrich*, NJW 2006, 809 ff.; *Sankol*, MMR 2006, 361 ff.; „Tauschbörsen im Internet: Die Methoden der Abmahnanwälte – 10 000 Euro für das Lied, 3000 Euro für den Anwalt, FAZ v. 4.12.2007, S. T1.

¹¹⁴ BVerfG-K, NJW 2007, 3055 ff.

wirksamsten Mittel zur Wahrung der informationellen Selbstbestimmung betont. In der Informationsgesellschaft kann und darf dieser zwar nicht zu einem Gebot der Datenaskese überhöht werden¹¹⁵. Mit der verdachtslosen und universellen Vorratsspeicherung sensibler Telekommunikationsverkehrsdaten wird aber umgekehrt die Informationsvorsorge erheblich überspannt.

Besondere Bedeutung kommt dabei der Verdachtslosigkeit der Vorratsdatenspeicherung zu. Durch sie werden unter den Bedingungen der modernen Informationsgesellschaft die Antragsteller gemeinsam mit beinahe allen anderen Bürgern zum Objekt staatlich veranlasster Datenspeicherung, ohne dass sie dafür durch ihr Verhalten einen relevanten Anlass geboten haben. Die Speicherung erfolgt vielmehr ins Blaue hinein und entfaltet eine ganz außergewöhnliche Streubreite. Beide Aspekte wurden vom BVerfG in seiner bisherigen Rechtsprechung als Kriterien für eine besondere Eingriffsintensität bzw. ein besonderes Maß der Rechtfertigungsbedürftigkeit gewertet¹¹⁶. Angesichts einer Mindestspeicherdauer von sechs Monaten kann man auch keinesfalls von einer unverzüglichen, spurlosen Löschung von Verkehrsdaten unbeteiligter Dritter sprechen¹¹⁷. Ferner entfallen durch die deutsche Ausgestaltung der Vorratsdatenspeicherung bislang bestehende Ausweichmöglichkeiten etwa mittels Pauschaltarifen oder Anonymisierungsdiensten¹¹⁸. Zwar spricht alles dafür, dass dadurch Anreize zur Entwicklung neuer Anonymisierungstechniken entstehen¹¹⁹. Diese Techniken werden aber vermutlich einen größeren Aufwand etwa durch die Nutzung von Dienstleistungen oder Geräten aus Drittstaaten oder gar in gewissem Umfang kriminelle Energie verlangen. Dies bedeutet, dass die Antragsteller und andere Telekommunikationsnutzer nicht mehr durch einfache und legale Formen der Datenvermeidung ihr Abgeordnetenrecht auf ungestörte und effektive Information bzw. ihr Grundrecht auf informationelle Selbstbestimmung verwirklichen können, während Täter aus Kreisen der Organisierten Kriminalität bzw. des internationalen Terrorismus

¹¹⁵ Dazu *Bull*, NJW 2006, 1617 ff.

¹¹⁶ Zu Telekommunikationsüberwachungen bzw. Datenerhebungen ins Blaue hinein: BVerfG, NJW 2006, 1939 (1946); BVerfGE 107, 299 (321 f.); 109, 279 (353); zur Problematik der Streubreite u.a.: BVerfG, NJW 2005, 2603 (2609) – NdsSOG.

¹¹⁷ Dies war das zentrale Argument für eine geringe Eingriffsintensität in BVerfG, NVwZ 2007, 351 (356 Tz. 76).

¹¹⁸ Die erhebliche Einschränkung des Nutzens von Anonymisierungsdiensten durch § 113a VI TKG ist nicht gemeinschaftsrechtlich zwingend vorgegeben: Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Stellungnahme vom 27.6.2007 zum Gesetzentwurf der Bundesregierung für ein Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG, S. 21.

¹¹⁹ Vgl. hierzu auch *R. Hamm*, NJW 2001, 3100 (3101).

durchaus Möglichkeiten nutzen werden, sich der Ermittlung mittels Vorratsdatenspeicherung zu entziehen.

(2) Absenkung der strafverfolgungsrechtlichen Anordnungsvoraussetzungen

Wie oben herausgearbeitet, ist durch die Richtlinie 2006/24/EG zwingend nur vorgegeben, dass die gespeicherten Daten für Strafverfolgungsmaßnahmen gegenüber der Organisierten Kriminalität und Terroristen zur Verfügung stehen müssen. Hierüber geht die einschlägige Vorschrift des § 100g StPO in der Fassung des Gesetzes vom 21.12.2007 in erheblichem Maße hinaus. Dies gilt sowohl für die Alternative der Straftaten von auch im Einzelfall erheblicher Bedeutung, wie schon der hierbei in Bezug genommene Katalog des § 100a StPO belegt, als auch für die Variante der mittels Telekommunikation begangenen Straftaten. Auf einer autonomen Spielraumentscheidung des deutschen Gesetzgebers beruhen ferner die einfache Verdachtsschwelle für die Zulässigkeit einer ermittlungsrichterlichen oder ausnahmsweise strafbehördlichen Übermittlungsanordnung sowie die Erhebungsverbote gemäß § 160a StPO.

Bei der Angemessenheitsbeurteilung sind selbstverständlich die vom BVerfG in seiner Rechtsprechung mehrfach hervorgehobenen und gewichtigen rechtsstaatlichen Belange einer funktionstüchtigen Strafrechtspflege¹²⁰ sowie die Ansprüche von Beschuldigten auf Wahrheitsermittlung¹²¹ einzubeziehen. Dementsprechend hat das BVerfG in einem Urteil vom 12.3.2003¹²² richterliche Anordnungen gegenüber Telekommunikationsunternehmen zur Auskunft über die für Abrechnungszwecke vorhandenen Verkehrsdaten im grundrechtlichen Kontext für verhältnismäßig erachtet. Es hat dabei ausdrücklich auf den zwischen der letzten fachgerichtlichen Entscheidung und seinem eigenen Urteil erlassenen § 100g StPO a.F. Bezug genommen und dessen Begrenzung der Anordnungsbefugnis auf Straftaten von erheblicher Bedeutung als Anhaltspunkt für die rechtliche Bewertung und Konkretisierung von § 12 FAG herangezogen, der damals Auskunftsverlangen zu Strafverfolgungszwecken ohne ausdrückliche Beschränkungen dieser Art regelte. Im Ergebnis hat das Gericht einen Verdacht auf dreifachen Mord bzw. auf Wirtschaftsstraftaten mit einem Schaden von 2 bis 3 Mrd. DM für hinreichend gewichtige, eine Verkehrsdatenerhebung im Einzelfall rechtfertigende Straftaten eingestuft. Dabei musste das BVerfG aber weder die

¹²⁰ BVerfGE 100, 313 (388 f.); 107, 299 (316); 115, 166 (192); s. im hiesigen Zusammenhang: Bundesregierung, Gesetzesbegründung, BT-Drs. 16/5846, S. 22, 31.

¹²¹ Bundesregierung, Gesetzesbegründung, BT-Drs. 16/5846, S. 22

¹²² BVerfGE 107, 299 (318 ff.).

generelle Verfassungsmäßigkeit der Vorschriften prüfen, noch äußerte es sich zur zweiten Anordnungsalternative gemäß § 100g StPO a.F., also des Verdachts auf mittels Telekommunikationsendeinrichtung begangener Taten. Mit einer auf diese Anordnungsalternative beruhenden Auskunftsanordnung hat sich bislang lediglich eine Kammer des 2. Senats befasst¹²³. Dabei hat die Kammer ebenfalls auf den konkreten Einzelfall abgestellt und keine grundrechtlichen Bedenken gegen eine Anordnung erhoben, wenn ein Beschuldigter einer versuchten Strafreitelung Telekommunikationseinrichtungen – medienspezifisch die durch sie mögliche Anonymität ausnuzend – als Tatmittel einsetzt. Durch den gezielten Missbrauch von Telekommunikationseinrichtungen mindere sich nämlich der Anspruch auf Wahrung des Schutzes der Vertraulichkeit, insbesondere wenn entsprechende – auch mindere – Taten ohne Zugriff auf die Verkehrsdaten nicht aufklärbar seien. Zuletzt hat eine Kammer des Ersten Senats die Frage, wann eine (Vorrats-)Speicherung von Verkehrsdaten zu Strafverfolgungszwecken gerechtfertigt ist, ausdrücklich offen gelassen¹²⁴.

Die zuletzt erwähnte Kammerentscheidung berücksichtigt, dass die früheren genannten Entscheidungen jeweils verdachtsabhängige Einzelfallanordnungen zur Verkehrsdatenspeicherung betrafen, nicht aber Verpflichtungen zur generellen und verdachtslosen Vorratsdatenspeicherung zu weit gefassten Strafverfolgungszwecken. Nur diese werden aber vorliegend von den Antragstellern angegriffen.

Die verdachts- und ausnahmslose Vorratsdatenspeicherung stellt die Antragsteller und andere Telekommunikationsnutzer unter einen Generalverdacht. Die strafrechtlichen Anwendungsmöglichkeiten sind dabei derart weit, dass selbst mittlere Kriminalität auf die Vorratsdatenspeicherung aufbauende Ermittlungsmaßnahmen begründen kann. Dies gilt in besonderem Maß für die zweite Variante der mittels Telekommunikation begangenen Straftaten, wie das Beispiel von telefonischen Beleidigungen belegt. Nur bei Geringfügigkeit einer Beleidigung schließt das Erfordernis eines angemessenen Verhältnisses zur Bedeutung der Sache in § 100g I 2 StPO eindeutig eine Verkehrsdatenerhebung aus¹²⁵. Aber auch die erste Variante erheblicher Straftaten erfasst ausweislich des Katalogs von § 100a StPO keineswegs nur Delikte schwerer Kriminalität.

Dieser weite Anwendungsbereich steigert in großem Umfang das Risiko für Telekommunikationsnutzer einem unberechtigten Verdacht ausgesetzt zu werden und

¹²³ BVerfG, NJW 2006, 3197 (Tz. 17 f.).

¹²⁴ BVerfG-K, NJW 2007, 3055 (3057, Tz. 33).

¹²⁵ Vgl. Bundesregierung, Gesetzesbegründung, BT-Drs. 16/5846, S. 52.

dadurch zum Gegenstand von belastender Ermittlungsmaßnahmen zu werden¹²⁶. Auf die Vorratsdatenspeicherung aufbauende Datenerhebungen werden überdies in der Regel heimlich erfolgen. Erweist sich später der Verdacht als unbegründet, hätten die Maßnahmen die Antragsteller und andere Telekommunikationsnutzer in einer Situation vermeintlicher Vertraulichkeit getroffen¹²⁷, ohne dass diese im Sinne der erwähnten Kammerentscheidung des Zweiten Senats durch Medienmissbrauch tatsächlich einen besonderen Anlass dafür gegeben haben müssen. Zwar hat der Gesetzgeber insbesondere in § 100g II 1 i.V.m. § 100b sowie § 101 StPO eine Reihe wichtiger prozeduraler Sicherungen vorgesehen. Diese beziehen sich allerdings nicht auf die Stufe der Vorratsspeicherung und gewähren in der Regel nur einen nachträglichen, keineswegs ausnahmslosen Rechtsschutz, der zudem durch eine in der Praxis beobachtbare restriktive Benachrichtigungspraxis¹²⁸ geschwächt wird. Überdies ist die rechtsstaatliche Effektivität des Richtervorbehalts für Auskunftsanordnungen keineswegs unumstritten¹²⁹. Jedenfalls bedürfen diese auf den Einzelakt bezogenen Sicherungen der Rechtsstaatlichkeit der strukturellen Ergänzung durch den prinzipiellen Verzicht auf eine Verkehrsdatenspeicherung zu ausschließlich staatlichen Zwecken¹³⁰. Sie behalten selbstverständlich ihren Anwendungsbereich und ihre Bedeutung in anderen Konstellationen des Zugriffs auf Verkehrsdaten.

An dieser Stelle ist somit festzuhalten, dass von den über die zwingenden Gemeinschaftsvorgaben hinausgehenden strafprozessualen Verwendungsbefugnissen im Zusammenwirken mit der Vorratsdatenspeicherung erhebliche Belastungen für Telekommunikationsnutzer ausgehen, die vermuten lassen, dass es in relevantem Maße zu Verhaltensänderungen kommen kann. Solche generellen Verhaltensänderungen könnten sich selbst auf Kommunikationsbeziehungen zwischen Abgeordneten und ihren Informanten erstrecken, obwohl insoweit aufgrund einer Spielraumentscheidung des deutschen Umsetzungsgesetzgebers zumindest ein partiell wirksames Erhebungsverbot in § 160a I StPO existiert. Allerdings greift dieses erst auf

¹²⁶ Vgl. BVerfGE 107, 299 (321).

¹²⁷ Vgl. BVerfGE 107, 299 (321).

¹²⁸ Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Stellungnahme vom 27.6.2007 zum Gesetzentwurf der Bundesregierung für ein Gesetz zur Neuordnung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG, S. 16.

¹²⁹ Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Stellungnahme vom 27.6.2007 zum Gesetzentwurf der Bundesregierung für ein Gesetz zur Neuordnung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG, S. 10, spricht von einer zu beobachtenden Erosion des Richtervorbehalts.

¹³⁰ Anders zu beurteilen ist eine Verkehrsdatenspeicherung, welche die auf autonomen Entscheidungen von Diensteanbietern und -nutzern beruhende Vertragsdurchführung absichert.

der Ebene der Datenübermittlung durch die TK-Diensteanbieter an die Strafverfolgungsbehörden. Demgegenüber werden die Kommunikationspartner der Abgeordneten auf der Stufe der Verkehrsdatenspeicherung noch nicht gesondert geschützt. Schon hierdurch kann aber das Vertrauensverhältnis zwischen den Antragstellern und ihren Kommunikationspartnern beeinträchtigt werden¹³¹. Berücksichtigung verlangt insoweit auch der unter (4) erörterte Mangel an hinreichenden Datensicherungsstrukturvorgaben für die nach § 113a TKG zur Speicherung verpflichteten Diensteanbieter. Dieser Mangel begründet erhebliche Missbrauchsgefahren, die die sensiblen kommunikativen Vertrauensbeziehungen der Antragsteller besonders tangieren. Sofern keine Möglichkeiten existieren sollten, den besonderen Interessen von Abgeordneten durch eine Selektion bereits auf der Stufe der Vorratsdatenspeicherung zu entsprechen, folgen daraus grundsätzliche Bedenken gegen das Instrument insgesamt. Deshalb besteht die konsequenteste Lösung im Verzicht auf eine Vorratsdatenspeicherung.

Ergänzend ist insoweit darauf hinzuweisen, dass bereits die bislang zur Verfügung stehenden strafbehördlichen Zugriffsmöglichkeiten auf Verkehrsdaten in vielen Fällen zu einer effektiven Strafverfolgung ausreichend waren. Empirische Untersuchungen etwa des Bundeskriminalamtes¹³² verweisen nur auf eine vergleichsweise geringe Zahl von Fällen, in denen Ermittlungen an mangelnden Zugriffsbefugnissen scheiterten. Zudem sind alternative, weniger eingriffsintensive Ermittlungsmethoden wie das Quick-Freeze-Verfahren für die Angemessenheitsprüfung bedeutsam¹³³, selbst wenn diese im Vergleich zur Vorratsdatenspeicherung partiell weniger erfolgversprechend sind und deshalb nicht bereits die Erforderlichkeit der angegriffenen Regelungen ausschließen. Schließlich sind die bereits erörterten (s. oben (1)) spezifischen Belastungswirkungen einer Vorratsspeicherung von Verkehrsdaten einzukalkulieren.

In der Bilanz muss für strafverfolgungsrechtliche Auskunftsbefugnisse, die auf eine Vorratsdatenspeicherung aufbauen und über zwingende Gemeinschaftsvorgaben hinausgehen, die Angemessenheitsprüfung negativ ausfallen. Damit verlangt der Schutz des freien Mandats zwar eine partielle Beschränkung des rechtsstaatlichen Interesses an einer effektiven Strafverfolgung. Im freiheitlichen Rechtsstaat kann dieses

¹³¹ Ähnlich bezüglich der Presseangehörigen und ihrer Informanten: *Gola u.a.*, NJW 2007 2599 (2600 f.).

¹³² *Mahnken*, Mindestspeicherfristen für Telekommunikationsverbindungsdaten – Rechtstatsachen zum Beleg der defizitären Rechtslage, hrsg. vom Bundeskriminalamt, Stand 15.11.2005.

¹³³ S. auch *Gola u.a.*, NJW 2007, 2599 (2600); *Zöller*, GA 2007, 393 (411 f.); *Westphal*, EuR 2003, 706 (715); krit. allerdings: *Mahnken*, Mindestspeicherfristen für Telekommunikationsverbindungsdaten – Rechtstatsachen zum Beleg der defizitären Rechtslage, hrsg. vom Bundeskriminalamt, Stand 15.11.2005, 18 f.

82

Sicherheitsinteresse allerdings prinzipiell keinen uneingeschränkten Vorrang beanspruchen. Andernfalls mutierte der Rechtsstaat zum Polizeistaat, der die demokratische Freiheitlichkeit dem Streben nach Sicherheit opferte¹³⁴. Gewiss wäre dabei nur der Verlust der Freiheitlichkeit. Sicherheit garantieren kann aber selbst ein perfekter Polizeistaat nicht¹³⁵.

(3) *Erweiterung der Verwendungszwecke auf Gefahrenabwehr sowie Verfassungsschutz und nachrichtendienstliche Nutzung*

Noch problematischer sind die ebenfalls nicht von der Richtlinie 2006/24/EG zwingend vorgegebenen, in § 113b Nr. 2 und 3 TKG vorgesehenen Verwendungszwecke zur Gefahrenabwehr sowie für den Verfassungsschutz und die Nachrichtendienste. Allerdings existieren für diese Verwendungszwecke noch nicht die von § 113b TKG vorausgesetzten spezialgesetzlichen Befugnisnormen. Dies bedeutet jedoch nicht, dass von der geltenden Regelung keine verfassungsrechtlich bedeutsamen aktuellen (Vor-)Wirkungen ausgehen.

Angesichts des Ausmaßes der gegenwärtigen gesetzgeberischen Initiativen und des klar bekundeten rechtspolitischen Willens ist es für die Antragsteller und ihre Kommunikationspartner offenkundig, dass demnächst mit entsprechenden Regelungen zu rechnen sein wird. Die ohnedies in der sicherheitspolitischen Debatte beobachtbare Tendenz zur sukzessiven Ausweitung von verdeckten Ermittlungsmethoden und Verwendungszwecken für Datenbestände mit zunächst sehr eng begrenzten Einsatzbereichen¹³⁶, wie sie gegenwärtig etwa am besorgniserregenden Anstieg der Zahl von Telefonüberwachungen¹³⁷ oder auch bezüglich der Mautdaten¹³⁸ beobachtbar ist, wird mit § 113b Nr. 2 und 3 TKG durch den Gesetzgeber bereits weiträumig vorweggenommen. Insbesondere Menschen, die nicht ständig alle Facetten der sicherheitspolitischen Entwicklungen beobachten, können sich deshalb veranlasst sehen, sich bereits heute in ihrem Verhalten auf künftig zu erwartende Überwachungsbefugnisse einzustellen. Zu diesem Personenkreis gehören die

¹³⁴ Vgl. BVerwGE 26, 169 (170 f.).

¹³⁵ Ganz ähnlich bereits *Benjamin Franklin*: „Wer die Freiheit um der Sicherheit willen aufgibt, wird am Ende beides verlieren“, zitiert nach *Hohmann-Dennhardt*, NJW 2006, 545 (548).

¹³⁶ *Gola u.a.*, NJW 2007, 2599 (2600); *Westphal*, EuR 2006, 706 (722).

¹³⁷ Vgl. *Hohmann-Dennhardt*, NJW 2006, 545 (547).

¹³⁸ Vgl. Antwort der Bundesregierung vom 26.10.2006 auf die Kleine Anfrage der Abgeordneten Jan Korte, Kersten Naumann, Petra Pau und der Fraktion DIE LINKE. – Drucksache 16/2902 – Nutzung von LKW-Mautdaten für Fahndungszwecke, BT-Drs. 16/3171, S. 2

Antragsteller aufgrund ihrer Abgeordnetentätigkeit zwar nicht. Bedeutsam sind aber, wie bereits mehrfach betont, auch Verhaltensanpassungen ihrer Kommunikationspartner.

Im übrigen könnten die zuständigen Gesetzgebungsorgane geneigt sein, aufgrund der Ankündigung entsprechender Verwendungsbefugnisse durch § 113b Nr. 2 und 3 TKG von einem geminderten Vertrauensschutz der Regelungsadressaten auszugehen. Sie könnten daher Ausnahmen vom rechtsstaatlichen Rückwirkungsverbot für zulässig erachten, und einen direkten oder über Weitergabebestandteile einen indirekten Zugriff auf bereits vor Erlass entsprechender Normen gespeicherte Verkehrsdaten für die hier erörterten Verwendungszwecke außerhalb der Strafverfolgung ermöglichen. Angesichts des verschärften Bestimmtheitsgebots bei Eingriffen in das Fernmeldegeheimnis generell und bei der Vorratsdatenspeicherung im besonderen erscheinen solche Ausnahmen vom Rückwirkungsverbot zwar aus Sicht der Antragsteller als unzulässig. Dies ändert aber nichts an der gegenwärtigen Berechtigung einer Erwartung der Grundrechtsträger, dass sich im sicherheitspolitischen Gesetzgebungsprozess eine gegenteilige Position durchsetzen könnte. Eine solche Erwartung wird die hier erörterten Vorwirkungen vertiefen und die Tendenz zu vorgezogenen Verhaltensanpassungen verstärken.

Für die gefahrenabwehrrechtlichen Befugnisnormen eröffnet § 113b S. 1 Nr. 2 TKG die Möglichkeit zum Rückgriff auf die Vorratsdatenspeicherung bereits für erhebliche Gefahren für die öffentliche Sicherheit. Hierunter werden beispielsweise nach der Legaldefinition in § 2 Nr. 1c) NdsSOG Gefahren für ein bedeutsames Rechtsgut wie Bestand des Staates, Leben, Gesundheit, Freiheit, nicht unwesentliche Vermögenswerte, aber auch sehr unbestimmt andere strafrechtlich geschützte Güter verstanden¹³⁹. Soweit derzeit Landespolizeigesetze überhaupt Beschränkungen der Fernmeldefreiheit zulassen, bedeutete eine Übernahme dieser Maßstäbe eine Absenkung der materiellen Voraussetzungen etwa im Vergleich zum gegenwärtigen § 33 I, II Nr. 2 NdsSOG, der für die Verbindungsdatenerhebung eine gegenwärtige Gefahr für Leib, Leben oder Freiheit einer Person verlangt¹⁴⁰. Der Mehrwert einer Vorratsdatenspeicherung gegenüber den existierenden Sachverhaltsermittlungsbefugnissen ist jedenfalls für gegenwärtige Gefahrensituationen derart gering, dass dieser nicht die bereits dargelegten Beeinträchtigungen durch eine verdachtslose und universelle Vorratsdatenspeicherung aufwiegt.

¹³⁹ Krit. auch: Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Stellungnahme vom 27.6.2007 zum Gesetzentwurf der Bundesregierung für ein Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG, S. 24; s. ferner *Schenke*, Polizei- und Ordnungsrecht, 5. Aufl. 2007, Rn. 78 mit Nachweisen zu Legaldefinitionen anderer Bundesländer.

¹⁴⁰ Vgl. zum Ganzen: *Schenke*, Polizei- und Ordnungsrecht, 5. Aufl. 2007, Rn. 197a ff.

Während die gefahrenabwehrrechtlichen Befugnisse immerhin eine konkrete Gefahrensituation voraussetzen, erfolgen Überwachungsmaßnahmen durch Verfassungsschutz und Nachrichtendienste üblicherweise bereits im Vorfeld konkreter Gefahren. Zudem sind die Rechtsschutzmöglichkeiten in diesem Bereich traditionell deutlich abgesenkt¹⁴¹. In seiner Entscheidung zur strategischen Auslandsgesprächsüberwachung durch den Bundesnachrichtendienst hat das BVerfG allerdings die Befugnisse zur bloßen Erfassung und Aufzeichnung von Fernmeldevorgängen noch nicht als unverhältnismäßig eingestuft, weil Gefahren für eine freie Kommunikation erst durch die nachfolgende Auswertung und Weitergabe der Erkenntnisse ihr volles Gewicht erhielten und ihnen daher in den diesbezüglichen Befugnisnormen zu begegnen sei¹⁴². Diese Wertungen sind allerdings nicht auf die nachrichtendienstliche Nutzung von auf Vorrat gespeicherten Verkehrsdaten übertragbar. Bei der strategischen Auslandsgesprächsüberwachung durch den Bundesnachrichtendienst erfolgt nämlich vor einer dauerhaften Aufzeichnung und Speicherung eine Selektion anhand „verdachtsbegründender“ Suchbegriffe. Im Übrigen ist sie naturgemäß nur auf einen Ausschnitt der Fernmeldenutzungen, nämlich die mit Auslandsbezug beschränkt. Demgegenüber werden mit der Vorratsdatenspeicherung nach Einführung entsprechender Befugnisnormen dem Bundesnachrichtendienst, dem Militärischen Abschirmdienst und den Verfassungsschutzbehörden auf einen längeren Zeitraum verdachtslos die Verkehrsdaten sämtlicher Telefon-, Email- und Internetnutzung zur rückwirkenden Selektion zur Verfügung gestellt.

Insbesondere die Erwartung künftiger verfassungsschutzrechtlicher sowie nachrichtendienstlicher Befugnisse beeinträchtigt die Abgeordnetenrechte der Antragsteller in besonderem Maße. Inhaltlich ist anzumerken, dass bekanntermaßen auch Aktivitäten von Abgeordneten Beobachtungsgegenstand der Verfassungsschutzbehörden und Nachrichtendienste sind¹⁴³. Deshalb könnten Abgeordnete geneigt sein, ihr Kommunikationsverhalten zu ändern, um keinen Anlass zu derartigen Überwachungsmaßnahmen zu bieten. Deshalb müssen zwar Überwachungsmaßnahmen, etwa von verfassungsfeindlich gesinnten Abgeordneten, nicht generell unverhältnismäßig sein. Eine vollständig anlasslose Vorratsdatenspeicherung mit relativ offenen Voraussetzungen für daran anknüpfende Datenerhebungen überschreitet aber die Grenzen der Verhältnismäßigkeit. Zudem gibt es in den bisher üblichen Rechtsgrundlagen anders als in der StPO auch auf der

¹⁴¹ Vgl. hierzu: Kayzers, AöR 129 (2004), 121 ff.

¹⁴² BVerfGE 100, 313 (384) = NJW 2000, 55 (64).

¹⁴³ Vgl. nur VG Köln, v. 17.1.2008, Az. 20 K 3077/06, dazu „Beobachtung Ramelows rechtswidrig, FAZ v. 18.1.2008, S. 2.

zweiten Ebene der Datenauswertung keine expliziten Beschränkungen für die Telekommunikationsüberwachung von Abgeordneten¹⁴⁴. Es ist nicht damit zu rechnen, dass Gesetzentwürfe für die Nutzung der Vorratsdatenspeicherung durch diese Behörden ohne entsprechende verfassungsgerichtliche Hinweise mit dieser Tradition brechen.

Die vorstehend aufgeworfenen Problembereiche können mangels Existenz der exakten fachgesetzlichen Regelungen derzeit nicht weiter vertieft werden. Das Grundproblem der verdachtslosen Vorratsdatenspeicherung für die Zwecke der Gefahrenabwehr, des Verfassungsschutzes und der Nachrichtendienste zeichnet sich jedoch hinreichend deutlich mit Vorwirkungen in Gestalt vorgezogener Verhaltensanpassungen der Bürger und damit auf den demokratischen Diskurs ab, weshalb bereits heute die Unangemessenheit der entsprechenden Basisregelungen in § 113b S. 1 Nr. 2 und 3 TKG festgestellt werden kann. Diese ebnen den Weg in den eine ausgreifende Überwachung der Bürger, statt diesen in angemessenem Umfang einzudämmen oder wenigstens hinreichend präzise zu kanalisieren.

(4) Unzureichende Datensicherungsstrukturen bei der Vorratsdatenspeicherung

Gemäß § 113a X TKG müssen zwar die zur Speicherung Verpflichteten die in der Telekommunikation erforderliche Sorgfalt bei der Datensicherheit beachten sowie durch technische und organisatorische Maßnahmen sicherstellen, dass die gespeicherten Daten nur besonders ermächtigten Personen zugänglich sind. Trotz der immensen Menge besonders sensibler Daten werden diese Pflichten aber nicht näher konkretisiert. Insgesamt wird das Risiko eines Datenmissbrauchs durch das Absehen vom Gebot der Datenvermeidung und die Privatisierung der Speicherungspflicht erheblich erhöht, ohne dass der Gesetzgeber gleichzeitig seiner aus der Fernmeldefreiheit bzw. dem Grundrecht auf informationelle Selbstbestimmung folgenden Gewährleistungsverantwortung für die Datensicherheit hinreichend nachkommt¹⁴⁵. Besonders persönlichkeitsrelevante Missbräuche können beispielsweise durch die widerrechtliche Verknüpfung mit anderen privaten Datenbeständen etwa zur Internetnutzung, die ihrerseits oft illegal angelegt werden¹⁴⁶, erfolgen. Der Marktwert der

¹⁴⁴ Die Vorschrift des § 3 II 4 G 10 ist auf die Abgeordnetenpost beschränkt.

¹⁴⁵ Vgl. auch Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Stellungnahme vom 27.6.2007 zum Gesetzentwurf der Bundesregierung für ein Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG, S. 20.

¹⁴⁶ Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Stellungnahme vom 27.6.2007 zum Gesetzentwurf der Bundesregierung für ein Gesetz zur Neuregelung der

Verkehrsdaten wäre jedenfalls wegen ihrer vielfältigen Nutzbarkeit u.a. zur Entwicklung von Persönlichkeitsprofilen oder zur Wirtschaftsspionage erheblich. Die Anreize zum Missbrauch sind ebenso hoch, wie umgekehrt die Entdeckung und der Nachweis entsprechender Missbräuche oft schwer fällt. Daneben besteht schlicht das Risiko der Datenoffenbarung durch menschliches oder organisatorisches Versagen. Beispiele aus dem Ausland beweisen, dass dies keine unbegründeten Sorgen sind¹⁴⁷. Man mag annehmen, dass absichtliche Missbräuche von mandatsbezogenen Kommunikationsdaten durch Private weniger wahrscheinlich als wirtschaftlich nutzbare Datenverwendungen sind, ausgeschlossen sind sie dadurch aber keinesfalls. Beachtung verdient hierbei auch die besondere Sensibilität der mandatsbezogenen Kommunikationsbeziehungen. Als ein Faktor der Gesamtwürdigung der Vorratsdatenspeicherung verlangt allerdings auch dieser Aspekt Beachtung.

Missbrauchsgefahren bei der Datenspeicherung sind nach der Rechtsprechung des BVerfG besonders zu beachten¹⁴⁸. Deshalb hat das BVerfG bezüglich der Verkehrsdatenspeicherung durch die Diensteanbieter zu deren eigenen (Abrechnungs-)Zwecken bereits eine Schutzpflicht des Staates entwickelt¹⁴⁹. Elemente eines mindestens notwendigen Datenschutzmanagements wären Formen eines Datenschutzaudits¹⁵⁰ oder der unabhängigen Zertifizierung des verantwortlichen Personals. Der effektivste Schutz wäre allerdings eine Beachtung des Gebots der Datensparsamkeit durch einen Verzicht auf die Vorratsdatenspeicherung insgesamt, nachdem die Richtlinie 2006/24/EG durch den EuGH für ungültig erklärt wurde.

bb) Unverhältnismäßigkeit von zwingende Richtlinienvorgaben umsetzenden Bestimmungen

Jedenfalls wenn der EuGH die Richtlinie 2006/24/EG entweder auf eine hier angeregte Vorlage des BVerfG oder im Rahmen der Rs. C-301/06 für gemeinschaftswidrig erklärt, würde eine verfassungsgerichtliche Überprüfung der gegenwärtig noch zwingend vorgegebenen Elemente der Vorratsdatenspeicherung eröffnet.

Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG, S. 14, 21.

¹⁴⁷ Insbesondere in England häuften sich allein im letzten Jahr entsprechende Vorgänge, s. nur: „Neue Vorwürfe gegen Darling“, FAZ v. 23.11.2007, S. 6.

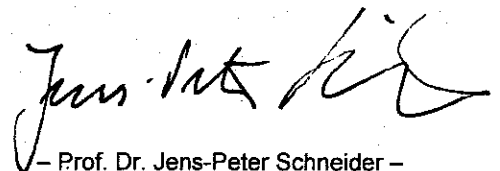
¹⁴⁸ BVerfG-K, NJW 2007, 3055 (3056, Tz. 17); BVerfG, NJW 2003, 1787 (1793); *Gola u.a.*, NJW 2007, 2601, 2602.

¹⁴⁹ BVerfG-K, NJW 2007, 3055 (3056, Tz. 13).

¹⁵⁰ Näher: *Roßnagel*, Datenschutzaudit, in: ders. (Hrsg.), Handbuch Datenschutzrecht, 2003, S. 437 ff.

Sicherlich kommt der strafrechtlichen Bekämpfung der Organisierten Kriminalität und des Terrorismus ein gesteigertes Gewicht zu. Zudem mögen in diesem Bereich telekommunikationsbezogene Ermittlungsmaßnahmen aufgrund der internationalen Verflechtungen in diesem Kriminalitätsformen besondere Bedeutung besitzen. Gleichwohl rechtfertigen diese Belange nicht die nun eingeführte verdachtslose und universelle Vorratsdatenspeicherung. Das Gewicht der hiermit verbundenen und im Vergleich zur bisherigen Rechtslage Beeinträchtigung der autonomen Informationsbeschaffung der Mandatsträger sowie die Risiken für das demokratisch bedeutsame Kommunikationsverhalten der Bürger wurde bereits ausführlich dargelegt. Diese Beeinträchtigungen werden nach Ansicht der Antragsteller nicht durch den kriminalistischen Mehrwert der Vorratsdatenspeicherung aufgewogen. Dieser dürfte sogar gerade in diesen Kriminalitätsfeldern aufgrund der besonderen kriminellen Energie der Täter und ihrem guten Organisationsgrad am geringsten sein. Auch die bisher bestehenden Zugriffsmöglichkeiten auf Verkehrsdaten ermöglichen in der ganz überwiegenden Zahl der Fälle eine kaum weniger effektive Strafverfolgung. Zusätzlichen Gewinn verspricht das bereits erwähnte Instrument des Quick-Freeze. Da dieses deutlich weniger grundrechtsbeeinträchtigend wirkt als die verdachtslose und universelle Vorratsdatenspeicherung, muss die mit ihm mögliche partielle Substitution der Vorratsdatenspeicherung auch bei der Angemessenheitsprüfung für die hier relevanten Verwendungsfelder Berücksichtigung finden. Zu bedenken ist schließlich, dass den Rückwirkungen auf den demokratischen Diskurs oder den Gefahren des Datenmissbrauchs allenfalls marginal oder jedenfalls nicht hinreichend durch eine Begrenzung der Verwendungszwecke begegnet werden kann. Notwendig ist vielmehr ein vollständiger Verzicht auf eine verdachtslose und universelle Vorratsdatenspeicherung von Verkehrsdaten.

Osnabrück, 8. Februar 2008



– Prof. Dr. Jens-Peter Schneider –

