Schleswig-Holsteinischer Landtag
Umdruck 16/620

Der Präsident des
Schleswig-Holsteinischen Landtages

Wissenschaftlicher Dienst

Schleswig-Holsteinischer Landtag ▪ Postfach 7121 ▪ 24171 Kiel

An die
Mitglieder des Ältestenrates

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

An die Vorsitzende des Europaausschusses
Frau Astrid Höfs, MdL

im Hause

Ihr Zeichen:
Ihr Auftrag vom: 18.01.2006

Mein Zeichen: L 203 – 60/16
Meine Nachricht vom:

Bearbeiter/in:
Dr. Silke Ruth Laskowski

Telefon (0431) 988-1104
Telefax (0431) 988-1250
Silke-Ruth.Laskowski@landtag.ltsh.de

28. Februar 2006

Auswirkungen des Richtlinienvorschlags KOM (2005) 438 endg. („Vorratsdatenspeicherung") auf die Rechte von Abgeordneten

Sehr geehrte Damen und Herren,

zu der Frage, ob durch die Ausweitung der Vorratsdatenspeicherung von Telefon- und Internetverbindungen nach Maßgabe des von der Europäischen Kommission vorgelegten *Vorschlags für eine Richtlinie des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG*[1] vom 25.09.2005 in der dem Rat am 13.02.2006 zum Beschluss zugeleiteten konsentierten Fassung[2] die Verletzung von Rechten der Abgeordneten des Schleswig-Holsteinischen Landtags zu befürchten sind, überreichen wir das anliegende Gutachten, dem wir eine Zusammenfassung der Ergebnisse vorangestellt haben.

[1] KOM (2005) 438 endg.
[2] PE-CONS 3677/10/05 REV 10 (de) v. 13.02.2006 i.V.m. Rat der Europäischen Union, Interinstitutionelles Dossier: 2005/0182 (COD) v. 10.02.2006 (14.02) Dok. 5777/06 und Addendum zu Dok. 2005/0182 (COD) v. 16.02.2006 (17.02) Dok.5777/06 ADD 2 REV 1.

Zusammenfassung der Ergebnisse

Die künftige Richtlinie zur Vorratsdatenspeicherung, die der Ermittlung, Feststellung und Verfolgung von schweren Straftaten dient, bedarf der Umsetzung in nationales Recht, sodass Eingriffe in verfassungsrechtlich geschützte Abgeordnetenrechte erst durch den Umsetzungsakt des deutschen Gesetzgebers in Betracht kommen. In Bezug auf die durch die Richtlinie zwingend vorgegebene anlassunabhängige Vorratsspeicherung bestimmter Datenkategorien durch die Diensteanbieter für mindestens sechs Monate besteht für die Mitgliedstaaten kein Umsetzungsspielraum. Der nationale Gesetzgeber ist an diese Vorgaben gebunden.

Betroffen sind sowohl Verkehrs- als auch Standortdaten von natürlichen wie auch juristischen Personen, ferner alle damit im Zusammenhang stehenden Daten, die zur Feststellung der Teilnehmer und Teilnehmerinnen sowie der registrierten Nutzer und Nutzerinnen erforderlich werden. Zu den Verkehrsdaten zählen solche, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden – z. B. Telefon/Faxnummern, IP-Adressen, Datum, Uhrzeit oder Dauer einer Verbindung, ferner die Datenmenge. Durch Standortdaten lässt sich der Standort des Endgeräts eines Nutzers bzw. einer Nutzerin ermitteln. Die Speicherungspflicht betrifft auch Verkehrs- und Standortdaten solcher Personen, die als sog. Berufsgeheimnisträger/-innen durch das deutsche Recht in besonderer Weise geschützt werden. Dazu zählen Abgeordnete, deren Schutzrechte nicht nur einfachgesetzlich, sondern auch verfassungsrechtlich abgesichert sind (vgl. Art. 24 Abs. 3 LV; Art. 47 GG).

Die Richtlinie enthält keine Pflicht zur automatischen Weitergabe der gespeicherten Daten an nationale Behörden. Vorgesehen ist, die gespeicherten Daten nur in bestimmten Fällen und in Übereinstimmung mit dem innerstaatlichen Recht an die zuständigen nationalen Behörden weiterzuleiten. Das Verfahren und die Voraussetzungen für den behördlichen Datenzugriff sind von den Mitgliedstaaten im Einklang mit dem Gemeinschafts- und Völkerrecht sowie unter besonderer Beachtung des Verhältnismäßigkeitsgrundsatzes durch das innerstaatliche Recht festzulegen. Diesbezüglich enthält die Richtlinie keine Vorgaben, sodass dem deutschen Gesetzgeber ein entsprechender Umsetzungsspielraum verbleibt.

Angesichts der zwingenden Vorratsdatenspeicherung erscheint eine Beeinträchtigung der Abgeordnetenschutzrechte des Schleswig-Holsteinischen Landtags (Zeugnisver-

weigerungsrecht gem. Art. 24 Abs. 3 LV; Recht auf informationelle Selbstbestimmung, Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) insbesondere vor dem Hintergrund neuester Entwicklungen in Literatur und Rechtsprechung denkbar. Bereits die automatische Datenspeicherung vermag eine jederzeit realisierbare Beeinträchtigungsgefahr für die Vertraulichkeit der Kommunikation zwischen Abgeordneten und Bürgern/-innen hervorzurufen.

Die Frage, ob die anlassunabhängige Vorratsdatenspeicherung nach Maßgabe der Richtlinie gegen das deutsche Verfassungsrecht verstößt wird künftig auf die EU-Ebene „verlagert“ werden, denn sie betrifft vorrangig Fragen zur Auslegung der Richtlinie und des gemeinschaftsrechtlichen Grundrechtsschutzes. Maßgeblich wird somit die Rechtsprechung des *EuGH.* Dementsprechend wertet das *BVerfG* Verfassungsbeschwerden und Vorlagebeschlüsse, die die Grundrechtsverletzung durch abgeleitetes Gemeinschaftsrecht rügen, heute als „*von vornherein unzulässig“*, es sei denn in der Begründung ließe sich darlegen, dass die europäische Rechtsentwicklung einschließlich der Rechtsprechung des *EuGH* unter den erforderlichen Grundrechtsstandard abgesunken ist.

Im internationalen wie auch europäischen Vergleich lässt sich ein ausdrücklich normiertes Zeugnisverweigerungsrecht für Abgeordnete nur selten feststellen. Die Europäische Menschenrechtskommission (EMRK) enthält kein entsprechendes Schutzrecht für Abgeordnete. Eine gewohnheitsrechtliche Ableitung auf europäischer Ebene dürfte daher an den unterschiedlichen Verfassungslagen der Mitgliedstaaten scheitern. Anders als in Deutschland ist ein Zeugnisverweigerungsrecht für Abgeordnete auf verfassungsrechtlicher Ebene lediglich in einzelnen EU-Staaten normiert. Auch die europäische Charta der Grundrechte (GRC) sieht keine speziellen Abgeordnetenschutzrechte vor. Ob auf gemeinschaftsrechtlicher Ebene ein dem deutschen Verfassungsrecht entsprechender Schutz von Abgeordneten gewährleistet wird, hängt daher davon ab, ob andere Gemeinschaftsgrundrechte einen äquivalenten Abgeordnetenschutz bieten. Maßgeblich wird damit das durch Art. 8 GRC gewährleistete „Recht auf Schutz personenbezogener Daten“ i. V. m. Art. 7 GRC („Recht auf Achtung des Privat- und Familienlebens“) und Art. 8 EMRK („Achtung des Privatlebens“). Aus der Zusammenschau dieser Regelungen wird das „Recht auf informationelle Selbstbestimmung“ hergeleitet, das der EuGH erstmal 1969 („Stauder“) anerkannt hat. Anders als das *BVerfG* erkennt der *EuGH* in der bloßen Speicherung personenbezogener Daten aber noch keinen Grundrechtseingriff, sondern erst in der Weitergabe der Daten an

nationale Behörden. Friktionen zwischen dem Recht auf informationelle Selbstbestimmung nach Maßgabe der Rechtsprechung des *BVerfG* und dem durch den *EuGH* gewährten Schutz personenbezogener Daten, erscheinen nicht ausgeschlossen. In Konsequenz dessen sind künftige Einschränkungen der Abgeordnetenschutzrechte durchaus denkbar.

Diesbezüglich ist die Rechtsprechung des *EuGH* abzuwarten. Sollte sich herausstellen, dass das durch den *EuGH* gewährte Schutzniveau zu einer Absenkung des grundgesetzlich vorgegebenen Schutzniveaus führt, bleibt abzuwarten, ob das *BVerfG* vor diesem Hintergrund auf seine im „Maastricht"-Urteil 1993 formulierte „Reservebefugnis" zur Prüfung von Grundrechtsverletzungen durch Gemeinschaftsrecht möglicherweise zurückgreift. Insoweit wird es auf die Beurteilung der Frage ankommen, ob *„die europäische Rechtsentwicklung (…) unter den erforderlichen Grundrechtsstandard abgesunken (…) und der jeweils als unabdingbar gebotene Grundrechtsschutz generell nicht mehr gewährleistet ist".*[3]

Für weitere Fragen stehen wir Ihnen gern zur Verfügung.

Mit freundlichen Grüßen
Für den Wissenschaftlichen Dienst

gez. Dr. Silke Ruth Laskowski

[3] BVerfGE 101, 147, 164.

Schleswig-Holsteinischer Landtag
Wissenschaftlicher Dienst
L 203 – 60/16

Kiel, 27.02.2006

Gutachten

zu den Auswirkungen des Richtlinienvorschlags KOM (2005) 438 endg. („Vorratsdatenspeicherung“) auf die Rechte von Abgeordneten

Inhaltsverzeichnis

1. Zum Stand des Gesetzgebungsverfahrens

Der dem Rat aktuell zur Beschlussfassung vorliegende Richtlinienentwurf entspricht dem durch das Europäische Parlament am 14.12.2005 mit Änderungen angenommen Vorschlag,[4] welcher auf dem am 02.12.2005 formulierten Kompromiss der Justizminister/-innen der EU gründet.[5] Der Europäische Wirtschafts- und Sozialausschuss hat dazu am 20.01.2006 eine kritische Stellungnahme abgegeben.[6] Der zur Beendigung des Gesetzgebungsverfahrens (Art. 251 EG) noch ausstehende förmliche Beschluss des Rates wird von der österreichischen Ratspräsidentschaft noch für Februar 2006 anvisiert.[7]

Bereits am 07.02.2006 wurde die Bundesregierung durch einen gemeinsamen Antrag der Fraktionen CDU/CSU und SPD aufgefordert, der abschließenden Befassung des Rates zuzustimmen und alsbald einen Gesetzentwurf zur Umsetzung der Richtlinie vorzulegen. Der Antrag geht davon aus, *„dass die Verfassungsgrundsätze und insbesondere das Berufsgeheimnis bei der Anwendung dieser Richtlinie gewahrt bleiben.“*[8]

2. Zum Regelungsgehalt des Richtlinienvorschlags KOM (2005) 438 endg. i. d. F. der Ratsvorlage vom 13.02.2006

Die Richtlinie basiert auf Art. 95 EG und dient ausweislich der Entwurfsbegründung der Harmonisierung der nationalen Vorschriften über die Vorratsdatenspeicherung im Hinblick auf die Verwirklichung des Binnenmarktes für elektronische Kommunikationsdienste mit dem Ziel, den *„Zugriff auf Verkehrsdaten zum Zwecke der Terrorismusbekämpfung“* zu ermöglichen.[9] Vorgesehen ist zum einen die zwingend vorgeschriebene

---

[4] P6_TA-PROV(2005)0512 (Vorläufige Ausgabe).
[5] Council of the European Union, 15101/1/05 REV1.
[6] Europäischer Wirtschafts- und Sozialausschuss, TEN/230 „Datenvorratsspeicherung“.
[7] Vgl. BT-Drs. 16/545 v. 07.02.2006, S. 2 zu Zif. 2.
[8] BT-Drs. 16/545, S. 5 zu Zif. 15.
[9] KOM (2005) 438 endg., S. 2, 6 ohne nähere Begründung zu Art. 95 EG. Der Entwurf verweist statt dessen auf das *interne* Kommissions-Arbeitspapier SEK (2005) 420 v. 22.03.2005, welches eine rechtliche Würdigung der Rechtsgrundlage gem. Art. 95 EG enthalten soll, das aber im Internet für die Öffentlichkeit nicht zugänglich ist. Der Wissenschaftliche Dienst des Schleswig-Holsteinischen Landtags hat das Dokument am 09.02.2006 per E-mail angefordert, bislang jedoch noch nicht erhalten. Obgleich insb. die Juristischen Dienste des Rates und des Europäischen Parlaments die Auffassung der Kommission teilen, erscheint die Frage der Rechtsgrundlage nach wie vor offen, vgl. dazu auch BT-Drs. 16/545, S. 1 f. (dort auch zur Vorgeschichte des zuvor von Frankreich, Irland, Schweden und Großbritannien vorgelegten und gescheiterten Entwurfs eines Rahmenbeschlusses zur Einführung EU-weiter Mindestspeicherungspflichten für Telekommunikationsverkehrsdaten gem. Art. 31, 34 EU).

anlassunabhängige Vorratsdatenspeicherung von mindestens sechs Monaten, die ausnahmslos für alle Bevölkerungsgruppen gilt (a.), zum anderen die Weitergabe dieser Daten an nationale Sicherheitsbehörden auf Anfrage (b.). Die Richtlinie soll innerhalb einer Umsetzungsfrist von 18 Monaten umgesetzt werden.[10]

a. Vorratsspeicherungspflicht

Die angestrebte Harmonisierung betrifft die **Pflichten von Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste**[11] bzw. **Betreibern öffentlicher Kommunikationsnetze**[12] (im Folgenden: Diensteanbieter) zur Vorratsspeicherung der in Art. 5 genannten Datenkategorien. Diese dienen der

- Rückverfolgung und Identifizierung der Nachrichtenquelle, Art. 5 Abs. 1 lit. a)
- Indentifizierung der Nachrichtenadressaten/-innen, Art. 5 Abs. 1 lit. b),
- Bestimmung von Datum, Uhrzeit und Dauer einer Nachrichtenübermittlung, Art. 5 Abs. 1 lit. d),
- Bestimmung der Endeinrichtung bzw. vorgeblichen Endeinrichtung von Benutzern/-innen, Art. 5 Abs. 1 lit. e) und
- Bestimmung des Standorts mobiler Geräte, Art. 5 Abs. 1 lit. f).

Gem. Art. 1 Abs. 1 soll auf diese Weise gewährleistet werden, dass die gespeicherten Daten nationalen Behörden zur **Ermittlung, Feststellung und Verfolgung von schweren Straftaten** – letztgenannte bestimmen sich nach nationalem Recht –[13] zur Verfügung stehen[14].

---

[10] Es besteht jedoch gem. Art. 15 Abs. 3 für die Mitgliedstaaten die Möglichkeit, die Anwendung der Richtlinie bis zu 36 Monate aufzuschieben. Von dieser Option haben bislang die Niederlande, Österreich, Estland, Großbritannien, Griechenland, Luxemburg, Slowenien, Schweden, Litauen, Lettland und Tschechien Gebrauch gemacht und entsprechende Erklärungen mit unterschiedlichen Zeiträumen abgegeben, vgl. Rat der Europäischen Union, Interinstitutionelles Dossier: 2005/0182 (COD), Addendum zum I/A-Punkt –Vermerk v. 16.02.2006 (17.02) 5777/06 ADD 2 REV 1.

[11] Darunter werden „gewöhnlich gegen Entgelt“ erbrachte Dienste wie Telekommunikations- und Internetdienste verstanden, zum Begriff vgl. Art. 2 lit. d) RL 2002/58/EG. Der Entwurf nimmt in Art. 2 auf die Begriffsdefinitionen der RL 2002/58/EG, RL 2002/21/EG und RL 95/46/EG Bezug.

[12] Gemeint sind elektronische Kommunikationsnetze, die zumindest überwiegend der Bereitstellung öffentlich zugänglicher Kommunikationsdienste im o. g. Sinn dienen, zum Begriff vgl. Art. 2 lit. d) RL 2002/58/EG, ABl. EG Nr. L 201, 37, 43.

[13] „Schweren Straftaten, wie sie von jedem Mitgliedstaat durch nationales Recht selbst bestimmt werden“, Art. 1 Abs. 1). Die Konkretisierung obliegt damit den Mitgliedstaaten. Die *Bundesregierung* hat den Begriff als zu eng kritisiert, vgl. die Antwort der Bundesregierung v. 06.12.2005 auf eine Kleine Anfrage der Fraktion DIE LINKE, BT-Drs. 16/142, 4 zu Zif. 7.

[14] Die in der ursprünglichen Fassung enthaltene beispielhafte Nennung von „Terrorismus und organisierter Kriminalität“ wurde gestrichen.

Die Mitgliedstaaten haben im Rahmen der Umsetzung dafür zu sorgen, dass die Diensteanbieter zur Speicherung umfangreicher Daten auf Vorrat verpflichtet werden, unabhängig vom Verdacht auf eine bevorstehende Gefahr, Art. 3 Abs. 1. Betroffen sind sowohl **Verkehrs-** als auch **Standortdaten** von natürlichen wie auch juristischen Personen, ferner alle damit im Zusammenhang stehenden Daten, die zur Feststellung der Teilnehmer und Teilnehmerinnen sowie der registrierten Nutzer und Nutzerinnen erforderlich werden, Art. 2 Abs. 2 lit. a). Zu den Verkehrsdaten zählen solche, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden – z. B. Telefon/Faxnummern, IP-Adressen, Datum, Uhrzeit oder Dauer einer Verbindung, ferner die Datenmenge. Durch Standortdaten[15] lässt sich der Standort des Endgeräts eines Nutzers bzw. einer Nutzerin ermitteln. Betroffen sind auch Daten im Zusammenhang mit **erfolglosen Anrufversuchen,** sofern diese bereits von den Diensteanbietern erzeugt oder verarbeitet und gespeichert werden, Art. 3 Abs. 2.[16] **Nicht erfasst** wird hingegen der **Inhalt** elektronischer Nachrichtenübermittlungen, Art. 1 Abs. 2. Art. 5 Abs. 2 verbietet explizit die Vorratsspeicherung solcher Daten, die Aufschluss über den Inhalt einer Kommunikation geben.

Die **Mindestspeicherungsfrist** wurde auf **sechs Monate**, die **maximal** zulässige Speicherungsdauer auf **zwei Jahre** ab dem Zeitpunkt der Kommunikation festgelegt, Art. 6. Darüber hinaus können die Mitgliedstaaten aber gem. Art. 12 („zukünftige Maßnahmen") von der Option Gebrauch machen, im Falle nicht näher bezeichneter „*besonderer Umstände*" bei der Kommission die **Verlängerung der maximalen Speicherungsfrist** für einen ebenfalls nicht näher konkretisierten *„begrenzten Zeitraum"* zu beantragen, Art. 12 Abs. 1 und Abs. 2.

Eingefügt wurden Regelungen zum **Datenschutz** und zur **Datensicherheit** gem. Art. 7. Die dort genannten Mindestgrundsätze sind von den Diensteanbietern einzuhalten und von den Mitgliedstaaten sicherzustellen.[17] Durch den neu aufgenommenen Art. 9

---

[15] Der Begriff umschreibt Daten, die in einem elektronischen Kommunikationsnetz verarbeitet werden und den geographischen Standort des Endgeräts des Nutzers bzw. der Nutzerin eines öffentlich zugänglichen elektronischen Kommunikationsdienstes angeben, vgl. Art. 2 lit c) RL 2002/58 /EG, ABl. EG Nr. L 201, 37, 43.

[16] Als „nicht erforderlich" gilt hingegen die Datenspeicherung im Zusammenhang mit Anrufen, bei denen keine Verbindung zustande kommt, Art. 3 Abs. 2 lit. 2.

[17] Die gespeicherten Daten sind insb. durch *„geeignete technische und organisatorische Maßnahmen (...) gegen zufällige oder unrechtmäßige Zerstörung, zufälligen Verlust oder zufällige Änderungen sowie unberechtigte und unrechtmäßige Speicherung, Verarbeitung, Zugänglichmachung oder Verbreitung* zu schützen", Art. 7a lit. b).

werden die Mitgliedstaaten verpflichtet, eine oder mehrere unabhängige Kontrollstelle/-n zur Überprüfung der in Art. 7 niedergelegten Grundsätze einzurichten.

b. Weiterleitung der Vorratsdaten

Die Speicherungspflicht der Diensteanbieter steht in unmittelbarem Zusammenhang mit Art. 8, der die Weiterleitung der Daten betrifft. Die Mitgliedstaaten müssen dafür sorgen, dass die gespeicherten Daten sowie alle damit zusammenhängenden erforderlichen Informationen unverzüglich an die zuständigen Behörden auf deren Anfrage hin weitergeleitet werden können. Die Richtlinie enthält hingegen keine Pflicht zur automatischen Weitergabe der Verbindungsdaten. Vorgesehen ist, die gespeicherten Daten **nur in bestimmten Fällen** und **in Übereinstimmung mit dem innerstaatlichen Recht** an die **zuständigen nationalen Behörden weiterzuleiten,** Art. 4. Das entsprechende behördliche Zugangsverfahren sowie die insoweit einzuhaltenden Bedingungensind von den Mitgliedstaaten im Einklang mit dem gemeinschafts- und Völkerrecht sowie unter besonderer Beachtung des Verhältnismäßigkeitsgrundsatzes durch das innerstaatliche Recht festzulegen. In Bezug auf die „zuständigen Behörden", denen der Zugriff ermöglicht werden soll, enthält die Richtlinie keine Vorgaben. Die Konkretisierung erfolgt im Rahmen der Umsetzung unter Berücksichtigung der innerstaatlichen Rechtsordnung.[18]

c. Änderung der Richtlinie 2002/58/EG

Schließlich wird die Datenschutzrichtlinie für elektronische Kommunikation 2002/58EG geändert und Art. 15 Abs. 1a eingefügt. Dieser nimmt die Richtlinie zur Vorratsdatenspeicherung ausdrücklich vom Anwendungsbereich des Art. 15 Abs. 1 RL 2002/58/EG

[18] In Deutschland wird nach derzeit geltender Rechtslage der Zugang zu Telekommunikationsverkehrsdaten zum Zwecke der Strafverfolgung in den §§ 100g und 100h StPO geregelt. Nach Maßgabe dieser Regelungen können die Strafverfolgungsbehörden (Staatsanwaltschaft, Polizei, Gerichte) im Einzelfall von den Diensteanbietern Auskunft über Verkehrsdaten in Anspruch nehmen. Darüber hinaus sind Telekommunikationsverkehrsdaten auch im Rahmen von Telekommunikationsüberwachungsmaßnahmen gem. §§ 100a, 100b StPO zu übermitteln. Schließlich können Verkehrsdaten nach Maßgabe von § 2 des Artikel 10-Gesetzes, § 23 ZFdG, § 8 Abs. 8 BVerfSchG, § 8 Abs. 3a BNDG, § 10 Abs. 3 MADG sowie – falls darin vorgesehen – nach Maßgabe der Polizeigesetze der Länder erhoben werden. Da die Richtlinie keine Vorgaben für die „zuständigen Behörden" enthält, dürfte sich der deutsche Gesetzgeber im Rahmen der Umsetzung an den o. g. Regelungen orientieren. In diese Richtung weist auch die Antwort der Bundesregierung vom 06.12.2005 auf eine Kleine Anfrage der Fraktion DIE LINKE, BT-Drs. 16/142, S. 2 zu Zif. 1.

aus, welcher lediglich strikt zweckgebundene, verhältnismäßige Einschränkungen der Vertraulichkeit der Kommunikation zulässt. [19]

3. Rechtliche Auswirkungen der Richtlinie auf die Rechte von Abgeordneten

a. Durch die Richtlinie selbst

EU-Richtlinien sind für die Mitgliedstaaten gem. Art. 249 EG nur in Bezug auf das Ziel verbindlich, sie bedürfen daher der **Umsetzung in nationales Recht**. Insoweit besteht die Pflicht zur fristgemäßen und zielkonformen Umsetzung. Das nationale Recht ist entsprechend an das Gemeinschaftsrecht anzupassen.[20] Die Richtlinie zur Vorratsdatenspeicherung selbst vermag daher noch keinen Eingriff in Abgeordnetenrechte zu begründen. Allerdings lässt sich in Bezug auf die zwingenden Vorgaben zur Datenspeicherungspflicht, die den Mitgliedstaaten keinen Umsetzungsspielraum lassen, bereits erkennen, dass insoweit durchaus Auswirkungen auf bestehende Abgeordnetenrechte eintreten können. Als sekundärem Gemeinschaftsrecht kommt der Richtlinie zur Vorratsdatenspeicherung nämlich Vorrang vor jeder Art von nationalem Recht der Mitgliedstaaten zu, nationales Verfassungsrecht eingeschlossen.[21] Entgegenstehende nationale Regelungen, die keiner gemeinschaftsrechtskonformen Auslegung zugänglich und daher mit dem Gemeinschaftsrecht unvereinbar sind, unterliegen daher einem Anwendungsverbot und müssen entsprechend geändert werden.[22]

Die Pflicht zur Vorratsdatenspeicherung und die Festlegung der zu speichernden Daten wird im Wesentlichen eine Anpassung des **Telekommunikationsgesetzes (TKG)** erfordern, das derzeit keine Pflicht zur anlassunabhängigen, vorsorglichen Datenspei-

---

[19] Art. 15 Abs. 1 lässt Beschränkungen der Rechte und Pflichten gem. Art. 5, Art. 6, Art. 8 Abs. 1, 2, 3 und 4 sowie Art. 9 dieser RL nur aus Gründen der nationalen Sicherheit, Landesverteidigung öffentlichen Sicherheit oder zur Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder unzulässigen Gebrauchs von elektronischen Kommunikationssystemen zu, sofern diese Beschränkungen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig sind.

[20] *Streinz*, in: Ders. (Hrsg.), EUV/EGV, 2003, Art. 249 EGV Rn. 78, 80.

[21] Std. Rspr. des EuGH seit der Entscheidung „Costa/Enel" v. 15.07.1964, Slg. 1964, 1141. Im Hinblick auf die Bundesrepublik Deutschland ergibt sich aber eine letzte Grenze aus Art. 23 Abs. 1 GG.

[22] U. U. wird eine Verfassungsänderung erforderlich, vgl. EuGH, Slg. 2000, I-69 Rn. 12 („Tanja Kreil"). Das *Europäische Parlament* geht in seiner legislativen Entschließung vom 14.12.2005 (P6_TA-PROV(2005)0512, Ziff. 4) zwar von der Berechtigung der Mitgliedstaaten aus, „Berufsgeheimnisse" bei der Anwendung der Richtlinie zu wahren und die eigenen nationalen Verfassungsgrundsätze anzuwenden. Letzteres ist angesichts des generellen Vorrangs des Gemeinschaftsrechts vor nationalem Recht jedoch nur dann möglich, wenn das nationale Verfassungsrecht mit dem Gemeinschaftsrecht vereinbar ist – nicht umgekehrt.

cherung zum Zwecke der Strafverfolgung vorsieht. Der deutsche Gesetzgeber hatte sich im Rahmen der Novellierung des Telekommunikationsgesetzes (TKG) vom 26.06.2004 vielmehr ausdrücklich gegen die Einführung der Vorratsdatenspeicherung von Verkehrsdaten im Telekommunikationsbereich ausgesprochen (vgl. § 96 Abs. 2 TKG 2004).[23] Diese Entscheidung wird mit Inkrafttreten der Richtlinie überholt sein.[24]

b. Durch den nationalen Umsetzungsakt

In Bezug auf die Richtlinie zur Vorratsdatenspeicherung ist das deutsche Recht innerhalb von 18 Monaten nach Inkrafttreten der Richtlinie richtlinienkonform abzuändern. Problematisch erscheint hier vor allem die von den Mitgliedstaaten zwingend umzusetzende Speicherungspflicht der Diensteanbieter, die keinen Umsetzungsspielraum lässt. Einschränkungen der Datenspeicherung für bestimmte Personen- oder Berufsgruppen bzw. entsprechende Ausnahmemöglichkeiten sieht die Richtlinie nicht vor. Daher umfasst die Speicherungspflicht auch die Daten solcher Personen, deren Kommunikation mit Dritten durch eine **besondere Vertraulichkeit** gekennzeichnet ist und daher durch das deutsche Recht in spezifischer Weise geschützt wird. Zu diesen **sog. Berufsgeheimnisträgern/-innen** zählen neben **Abgeordneten** z. B. auch Rechtsanwälte/-innen, Ärzte/-innen oder Geistliche (vgl. § 97 Abs. 1, Abs. 3 i. V. m. § 53 Abs. 1 Nr. 1, 3 und 4 StPO). Anders als andere Personengruppen werden Abgeordnete durch das deutsche Recht aber nicht nur einfachgesetzlich, sondern **verfassungsrechtlich abgesichert:** Bundestagsabgeordneten stehen Art. 46 und Art. 47 GG zur Seite, Abgeordneten des Schleswig-Holsteinischen Landtags die verfassungsrechtlich verbürgten Schutzrechte des Art. 24 LV.

Es stellt sich mithin die Frage, ob die gemeinschaftsrechtlich vorgeschriebene Vorratsdatenspeicherung und die mögliche Weiterleitung der gespeicherten Daten an nationale Behörden die durch **Art. 24 LV** geschützte **Immunität (aa.)** oder das **Zeugnisverweigerungsrecht der Abgeordneten i. V. m. dem Beschlagnahmeverbot (bb.)** beeinträchtigt. Entsprechendes gilt ferner im Hinblick auf das Abgeordneten nach der Rechtsprechung gerade auch in ihrer spezifischen Eigenschaft als Abgeordnete zustehende **Recht auf informationelle Selbstbestimmung (cc.).**

---

[23] Vgl. BT-Drs. 15/4597 v. 22.12.2004.

[24] Bereits während der Umsetzungsfrist entfaltet die Richtlinie eine rechtliche Vorwirkung. Danach ist es den Mitgliedstaaten untersagt, die Verwirklichung der Ziele der Richtlinie durch nationale Maßnahmen ernstlich in Frage zu stellen, vgl. EuGH, Slg. 1997, I-7411 Rn. 40 ff. („Inter-Environment“)

aa. Immunität gem. Art. 24 Abs. 2 LV

Art. 24 Abs. 2 LV schützt Abgeordnete des Schleswig-Holsteinischen Landtags vor Strafverfolgung und Freiheitsbeschränkungen. Einbezogen ist auch das Verhalten der Abgeordneten außerhalb des Parlaments (vgl. Art. 46 Abs. 3 GG für Abgeordnete des Deutschen Bundestages). Sofern durch die gespeicherten Daten Rückschlüsse auf strafbare Tätigkeiten von Abgeordneten möglich werden, wirkt sich im Hinblick auf eine Strafverfolgung Art. 24 Abs. 2 LV grundsätzlich als persönliches Verfahrenshindernis für die Dauer des Mandats aus.[25] Durch die Umsetzung der Richtlinie ergeben sich keine Änderungen.

bb. Zeugnisverweigerungsrecht und Beschlagnahmeverbot gem. Art. 24 Abs. 3 LV

Fraglich erscheint, ob durch die Vorgaben der Richtlinie das durch Art. 24 Abs. 3 LV (entspricht Art. 47 GG) garantierte Zeugnisverweigerungsrecht von Abgeordneten sowie das mit diesem eng verbundene, akzessorische Beschlagnahmeverbot beeinträchtigt werden. Beide Rechte zielen darauf ab, neben der Funktionsfähigkeit des Parlaments vor allem die Unabhängigkeit der Abgeordneten zu sichern.

(1) Zeugnisverweigerungsrecht

Nach Art. 24 Abs. 3 LV bzw. Art. 47 S. 1 GG sind Abgeordnete berechtigt, über Personen, die ihnen in ihrer Eigenschaft als Abgeordnete oder denen sie in dieser Eigenschaft Tatsachen anvertraut haben, sowie über diese Tatsachen selbst das Zeugnis zu verweigern. Diese Bestimmungen schützen die **ungehinderte Kommunikation zwischen Abgeordneten und Bürgern bzw. Bürgerinnen** und ermöglichen damit ein **Vertrauensverhältnis**, das der Stärkung des freien Mandats, insbesondere der Unabhängigkeit und Entscheidungsfreiheit der Abgeordneten dient.[26] Mittelbar werden dadurch die Funktionsfähigkeit des Parlaments und die demokratische Willensbildung gestärkt.[27]

---

[25] *Pieroth*, in: Jarass/Pieroth, GG, 7. Aufl. Art. 46 Rn. 5f.
[26] BVerfGE 38, 312, 323; *Maunz*, in: Maunz/Dürig, GG IV, Art. 47 Rn. 2; *Pieroth*, a.a.O., Art. 47 Rn. 1; *Magiera* in: Sachs (Hrsg.), GG, 2003, Art. 47 Rn. 1; *Schulze-Fielitz*, a.a.O., Art. 47 Rn. 5; *Caspar*, a.a.O., Art. 24 Rn. 44.
[27] *Magiera*, a.a.O., Art. 47 Rn. 1; *Schulze-Fielitz*, in: Dreier (Hrsg.), GG II, 1998, Art. 47 Rn. 5; *Pieroth*, a.a.O., Art. 47 Rn. 1.

Geschützt ist das „**parlamentarische Berufsgeheimnis**“[28] von Abgeordneten und verleiht ihnen ein zeitlich unbegrenzt geltendes **individuelles subjektives Recht**, das nicht zur Disposition des Parlaments steht.[29] Die Verweigerung des Zeugnisses ist daher überall dort möglich, wo eine Zeugnispflicht von Abgeordneten besteht.[30] Umfasst werden alle Zeugnispflichten in gerichtlichen und behördlichen Verfahren. Dazu zählen neben Straf- und Zivilgerichtsverfahren auch Verwaltungsverfahren.[31] Der Sinn und Zweck des Zeugnisverweigerungsrechts liegt darin, Abgeordneten die Wahrung ihrer „**parlamentarischen Berufsgeheimnisse**“ gegenüber staatlichen Instanzen zu ermöglichen.[32]

Inhaltlich bezieht sich das Zeugnisverweigerungsrecht auf die Abgeordneten **anvertrauten Tatsachen** sowie die **Identität der Personen**, die mit Abgeordneten kommunizieren und Informationen austauschen. Geschützt ist demnach die Personen in ihrer Identität und die Mitteilung in ihrem Inhalt. Die näheren Umstände der Mitteilung wie etwa Ort, Zeit, Form etc. sind jedenfalls dann mitgeschützt, wenn diese Rückschlüsse auf die Person bzw. den Inhalt der betreffenden Mitteilung zulassen.[33] **Anvertraute Tatsachen** sind anzunehmen, wenn sie dem oder der Abgeordneten vertraulich mitgeteilt wurden. Maßgeblich ist insofern der **Modus der Mitteilung**, nicht hingegen die Vertraulichkeit der Tatsache selbst.[34] Vorausgesetzt wird aber der unmittelbare Zusammenhang der betreffenden Mitteilung mit der Abgeordnetentätigkeit.

Im Hinblick auf die Datenspeicherung nach Maßgabe der Richtlinie ergibt sich Folgende Überlegung:

Da die Vorratsdatenspeicherung ausdrücklich die Rückverfolgung und Identifizierung der Adressaten/-innen einer per Festnetztelefonie, Mobilfunk oder Email weitergegeben Nachricht ermöglichen soll bzw. ermöglicht, vgl. Art. 5 lit b), stellt sich die Frage, ob es zu einer Kollision mit dem Zeugnisverweigerungsrecht kommt, wenn Abgeordnete im Zusammenhang mit ihrer Abgeordnetentätigkeit Dritten per Telefon, Handy oder Email Informationen anvertrauen. Die bei diesem Kommunikationsakt außerhalb

---

[28] *Magiera*, a.a.O., Art. 47 Rn. 2; *Maunz*, a.a.O., Art. 47 Rn. 2.
[29] *Schulze-Fielitz*, in: Dreier (Hrsg.), GG, 1998, Art. 47 Rn. 7; *Trute*, in: von Münch, GG Bd. 2, 4./5. Aufl. 2001, Art. 47 Rn. 2; *Magiera*, a.a.O., Art. 47 Rn. 3.
[30] *Trute*, a.a.O., Art. 47 Rn. 9 m. w. N.
[31] *Caspar*, in: Caspar/Ewer/Nolte/Waack (Hrsg.), Landesverfassungsrecht, 2006 i. E., Art. 24 Rn. 43, 50; *Schulze-Fielitz*, a.a.O., Art. 47 Rn. 9.
[32] *Trute*, a.a.O., Art. 47 Rn. 2 m. w. N.
[33] *Trute*, a.a.O, Art. 47 Rn. 6 m. w. N.
[34] *Magiera*, a.a.O., Art. 47 Rn. 4 m. w. N.

des Parlaments bei einem (privaten) Dienstanbieter automatisch gespeicherten Daten (z. B. angewählte Nummer, Name und Anschrift der registrierten Benutzer, Benutzerkennung) lassen die Identifizierung der betreffenden Person bzw. des oder der Abgeordneten zu. Entsprechendes gilt, wenn Abgeordneten durch Dritte Tatsachen anvertraut werden, vgl. Art. 5 Abs. 1 lit. a). Die Identitätsfeststellung der an der vertraulichen Nachrichtenübermittlung beteiligten Person wird auf diese Weise jederzeit möglich. Die Vertraulichkeit der Information erscheint daher betroffen.

Gegen diese Annahme spricht auch nicht, dass die Daten durch private Diensteanbieter und nicht durch staatliche Instanzen gespeichert werden. Die Vorratsspeicherung erfolgt weder im Interesse der Diensteanbieter noch zum Zwecke der Nutzung durch dieselben, sondern im staatlichen Interesse zum Zwecke der Nutzung durch die nationalen Behörden im Rahmen der Strafverfolgung. Insofern wirkt sich lediglich aus, dass der Staat die entsprechenden technischen Einrichtungen nicht mehr selbst bereit hält, sondern die privaten Betreiber von Telekommunikationsdiensten für die Wahrnehmung ursprünglich staatlicher Aufgaben und der weiterhin bestehenden staatlichen Aufgabe der Strafverfolgung in die Pflicht nimmt.[35] Die Kombination aus staatlicher Inpflichtnahme mit dem Zugriffs- und alleinigen Verwendungsrecht staatlicher Behörden gefährdet damit die durch das Zeugnisverweigerungsrecht der Abgeordneten geschützte Vertraulichkeit der Kommunikation – lässt man an dieser Stelle den hinzutretenden Aspekt eines möglichen Missbrauchs der gespeicherten Daten durch die Diensteanbieter einmal außer Betracht.

(2) Beschlagnahmeverbot

Für diese Betrachtung spricht zudem der Schutzgedanke des in Art. 24 Abs. 3 S. 2 LV geregelten akzessorischen Beschlagnahmeverbots. Dieses steht in unmittelbarem Zusammenhang mit dem Zeugnisverweigerungsrecht und soll verhindern, dass dieses durch die Beschlagnahme von Schriftstücken unterlaufen wird (statt des Zeugenbeweises würde ansonsten Urkundenbeweis ermöglicht). Das Beschlagnahmeverbot ergänzt das Zeugnisverweigerungsrecht, indem es gegenständlich verfestigte Mitteilungen im funktionellen Herrschaftsbereich der Abgeordneten, die im Übrigen den An-

[35] Ebenso der Österr. VerfGH, Erkenntnis v. 27.02.2003, Az. G 37/02-16 G 118/02-14, G 122/02-19, G 156/02, V 42/02-17, G 157/02, V 43/02-17, G 195/02-16, DuD 2003, 440, 442. Danach ist die gesetzl. Verpflichtung der TK-Diensteanbieter, dem Staat eine Überwachung der Telekommunikation durch die Bereitstellung entspr. Anlagen nach dem Stand der Technik ohne eine Erstattung ihrer Kosten und ohne Festlegung einer Kostenbelastungsgrenze als unverhältnismäßig zu betrachten.

forderungen des Art. 24 Abs. 3 S. 1 LV bzw. Art. 47 S. 1 GG entsprechen, zusätzlich sichert.[36] Die Beschlagnahme ist daher in dem Umfang unzulässig, in dem das Zeugnisverweigerungsrecht besteht.[37] Zu den geschützten Objekten zählen vergegenständlichte Mitteilungen, d. h. Schriftstücke (schriftlich gefasste Informationen), nach neuerer Auffassung auch **digitalisierte elektronische Datenträger**[38] und **Email.**[39]. Letztgenannte werden in der Literatur als „elektronische Briefe" mit lesbaren Postkarten verglichen.[40]

Zwar werden durch die künftige Vorratsspeicherung keine Datenträger als körperliche Gegenstände beschlagnahmt. Dieses ist angesichts der automatischen, ohne Einwilligung der Abgeordneten in den Geschäftsräumen der Diensteanbieter außerhalb des Parlaments erfolgenden „Vorab"-Speicherung bestimmter Daten, die dem Zeugnisverweigerungsrecht unterliegenden, auch nicht mehr erforderlich. Es handelt sich gewissermaßen um eine automatisierte, **vorweggenommene „Beschlagnahme auf Vorrat"**. Dass es letztlich nicht auf den körperlichen Datenträger ankommt, sondern um den abgespeicherten Datenbestand, hat unlängst das *BVerfG* in der Entscheidung vom 12.04.2005[41] deutlich gemacht. Dazu das *BVerfG:*

> *„Den Beschwerdeführern geht es nicht um den Entzug des Eigentums an dem Datenträger als körperlichem Gegenstand. Die Verfassungsbeschwerde bezweckt, den umfassenden Zugriff auf alle Daten der Anwaltskanzlei und der Steuerberatungsgesellschaft durch die Strafverfolgungsbehörden zu verhindern."*[42]

Im Vordergrund stehen die auf dem Datenträger lesbaren Daten und der ermöglichte dauerhafte Zugriff auf den gesamten Datenbestand, einschließlich der automatischen Verarbeitung der erhobenen Daten.[43]

---

[36] *Caspar*, a.a.O., Art. 24 Rn. 55.
[37] *Schulze-Fielitz*, a.a.O., Art. 47 Rn. 10 m. w. N. Vom personellen Schutzbereich werden ebenfalls die engeren Mitarbeiter und Mitarbeiterinnen der Abgeordneten umfasst, *Trute*, a.a.O., Art. 47 Rn. 10.
[38] *Magiera*, a.a.O., Art. 47 Rn. 8*; Trute*, a.a.O., Art. 47 Rn. 12; *Pieroth*, in: Jarass/Pieroth, GG. 7. Aufl. 2004, Art. 47 Rn. 3; *Schulze-Fielitz*, a.a.O., Art. 47 Rn. 12; *Caspar*, a.a.O., Art. 24 Rn. 54.
[39] So ausdrücklich *Trute*, a.a.O., Art. 47 Rn. 12.
[40] *Krüger/Pagenkopf*, in: Sachs (Hrsg.), GG, 2003, Art. 10 Rn. 14 m. w. N.
[41] BVerfG, Beschl. v. 12.04.2005, Az. 2 BvR 1027/02, NJW 2005, 1917 zu den verfassungsrechtlichen Anforderungen an die Sicherstellung und Beschlagnahme von Datenträgern und darauf gespeicherten Daten einer Rechtsanwalts- und Steuerberatungskanzlei als Beweisgegenstände im Strafverfahren, vor dem Hintergrund des rechtlich geschützten Vertrauensverhältnisses zwischen Rechtsanwalt/-anwältin und Mandant/-in sowie dem Grundrecht auf informationelle Selbstbestimmung.
[42] BVerfG, NJW 2005, 1917, 1918.
[43] BVerfG, NJW 2005, 1917, 1918 f., 1921. Das *BVerfG* nimmt vor allem auf die aktuelle Gesetzgebung, insb. die Neufassung des § 110 Abs. 1 StPO Bezug, und schlussfolgert daraus, dass *„auch die auf einem Datenträger ver-*

Unter Berücksichtigung der Rechtsprechung des *BVerfG* und im Hinblick auf den Sinn und Zweck des Art. 24 Abs. 3 LV stellt sich die Frage, ob der Schutzgedanke der Norm möglicherweise auf die von der Richtlinie geforderten automatisierten Vorgänge außerhalb des Direktionsbereichs der Abgeordneten, welche durch Telekommunikationsakte der Abgeordneten *innerhalb* ihres Direktionsbereichs ausgelöst werden, zu übertragen ist – zumal der historische Verfassungsgesetzgeber die technische Entwicklung nicht vorhersehen konnte.

Gegen diese Betrachtung spricht das herkömmliche Verständnis des Beschlagnahmeverbots, das lediglich Schriftstücke bzw. Gegenstände, die sich tatsächlich im Gewahrsam der Abgeordneten befinden (oder im Mitarbeitergewahrsam unter dem Direktionsrecht der Abgeordneten in den Räumen des Parlaments), dem Anwendungsbereich des Beschlagnahmeverbots zurechnet.[44] Schriftstücke im Gewahrsam Dritter können hingegen grundsätzlich beschlagnahmt werden.[45]

Allerdings ist bereits seit langem umstritten, ob sich das Verbot der Beschlagnahme in einem engen, eher technischen Sinn nur auf die Beschlagnahme an sich bezieht (vgl. § 94 Abs. 2 StPO) oder aber in einem weiten Sinn auch auf andere, entsprechend zielgerichtete Hoheitsmaßnahmen, die eine zwangsweise Wegnahme intendieren – etwa Herausgabeerzwingungen (§ 95 StPO), Durchsuchungen (§§ 102 ff. StPO) oder aber Briefkontrollen. Die Befürworter[46] des weiten Verständnisses stellen auf die ratio des Beschlagnahmeverbots ab und halten eine Ausdehnung des Schutzbereichs über die Beschlagnahme im technischen Sinn hinaus für erforderlich, damit das Zeugnisverweigerungsrecht der Abgeordneten *„nicht illusorisch gemacht“* wird.[47]

Gerade unter dem Eindruck der rasant fortschreitenden technischen Entwicklungen im Bereich der Telekommunikation spricht sich auch eine Teilmeinung in der jüngeren Literatur dafür aus, diesen Entwicklungen im Hinblick auf den Schutzzweck des Art 47 GG stärker Rechnung zu tragen. So betont etwa *Schulze-Fielitz* im Rahmen der Aus-

---

körperten Daten sichergestellt und beschlagnahmt werden können (…) zumal der Begriff „Papiere“ alle Arten von Unterlagen, auch elektronische, umfasse.“ (S. 1920).

[44] BVerfGE 108, 251, 269; *Magiera*, a.a.O., Art. 47 Rn. 8 m. w. N.

[45] *Caspar*, a.a.O., Art. 24 Rn. 54; *Borchert*, DÖV 1992, 58, 61; *Dach*, ZRP 1992, 1.

[46] Für ein weites Verständnis bereits *Maunz*, a.a.O., 4. Lief. 1960 (gleichzeitig aktueller Stand), Art. 47 Rn. 16 („Die ratio des Art. 47 S. 2 verlangt aber eine Ausdehnung des Schutzbereiches über die Beschlagnahme im technischen Sinne des Strafprozessrechts hinaus.“); ebenso *Schulze-Fielitz*, a.a.O., Art. 47 Rn. 12; *Schneider*, in: AK-GG, 3. Aufl. Art. 47 Rn. 6 f.; *Magiera*, a.a.O., Art. 47 Rn. 7;

[47] *Maunz*, a.a.O., Art. 47 Rn. 16.

legung des Beschlagnahmeverbots gem. Art. 47 S. 2 GG, dass *„Art. 47 S. 2 GG angesichts gewandelter technischer Möglichkeiten analog auf Vorgänge anzuwenden (sei), die funktional äquivalent zur Beschlagnahme wirken“*. Beispielhaft nennt er in diesem Zusammenhang neben der Anfertigung von Kopien und der Erstellung von Duplikaten elektronischer Datenträger auch *„technische Überwachungsmaßnahmen*“.[48] Noch deutlicher die Kommentierung von *Trute,* der das herkömmliche Verständnis des Beschlagnahmeverbots gem. Art. 47 S. 2 GG *„angesichts heutiger technischer Möglichkeiten zur Ausforschung von Vertrauensverhältnissen als zu eng“* bezeichnet. Ausdrücklich kritisiert er in diesem Zusammenhang, dass von den technischen Überwachungsmaßnahmen nach der StPO nur das Abhören des nichtöffentlich gesprochenen Wortes in der Wohnung von Abgeordneten ausgeschlossen ist (vgl. § 100 c Abs. 1, Abs. 6 StPO)[49], sonstige Maßnahmen aber möglich bleiben, auch wenn sie letztlich dem gleichen Ziel dienen. Insoweit hält *Trute* – falls entsprechende einfachgesetzliche Regelungen fehlen oder lückenhaft sind – auch eine unmittelbare Anwendung des Art. 47 S. 2 GG zum Schutz der Abgeordneten für erforderlich.[50]

Für ein erweitertes Verständnis des Beschlagnahmeverbots gem. Art. 47 GG plädiert inzwischen wohl auch das *BVerwG.* In der Entscheidung vom 23.06.2004 („Stasi-Unterlagen“)[51] zieht es ausdrücklich in Erwägung, den Gewährleistungsinhalt des Art. 47 S. 2 GG auch *„auf andere Weisen hoheitlicher Kenntnisnahme gegen den Willen von Abgeordneten (z. B. Kopieren von Schriftstücken und Dateien) zu erstrecken“.*

Unter Berücksichtigung der skizzierten neueren Tendenzen in Literatur und Rechtsprechung erscheint es nicht ausgeschlossen, dass die Vorratsspeicherung von „Abgeordnetendaten“, welche das „parlamentarische Berufsgeheimnis“ betreffen, ebenso wie deren Weitergabe an nationale Behörden insgesamt dem **Schutzbereich des Art. 24 Abs. 3 LV** (bzw. des Art. 47 S. 2 GG) zugerechnet werden kann. Die automatische Sicherstellung der in der Richtlinie genannten Daten ermöglicht letztlich die staatliche Identifizierung aller Personen, die mit Abgeordneten per Telekommunikation i. S. der Richtlinie in Verbindung treten, auch wenn vertrauliche Informationen ausgetauscht werden und der oder die Abgeordnete sich dabei innerhalb des Parlaments aufhält. Das auf diese Weise im Auftrag des Staates bei den Diensteanbietern geschaffene

[48] *Schulze-Fielitz*, a.a.O., Art. 47 Rn. 12.
[49] *Trute*, a.a.O., Art. 47 Rn. 17 noch zu § 100d Abs. 3 S. 1 i. V. m. § 100c Abs. 1 Nr. 3 StPO a. F..
[50] *Trute*, a.a.O., Art. 47 Rn. 15, 17.
[51] BVerwGE 121, 115, 123.

„fremde Geheimwissen“[52], kann möglicherweise einen **abschreckenden Effekt auf die vertrauliche Kommunikation zwischen Abgeordneten und Bürgern/-innen** entfalten und das Vertrauensverhältnis beeinträchtigen.[53]

Folgt man hingegen der herkömmlichen Betrachtung, so lässt sich dem Zeugnisverweigerungsrecht im Rahmen der Umsetzung dadurch Rechnung tragen, dass jedenfalls ein **Verwertungsverbot der gespeicherten Daten** in Betracht kommt. Insofern lässt sich der Umsetzungsspielraum des deutschen Gesetzgebers realisieren.[54]

cc. Recht auf informationelle Selbstbestimmung von Abgeordneten

Darüber hinaus ist das Abgeordneten gerade auch in ihrer spezifischen Eigenschaft als Abgeordnete zustehende Recht auf informationelle Selbstbestimmung, welches aus dem allgemeinen Persönlichkeitsrecht gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG hergeleitet wird,[55] tangiert. Maßgeblich sind die Vorgaben des *BVerfG* in der Grundsatzentscheidung im Volkszählungsurteil, wonach die freie Entfaltung der Persönlichkeit unter den modernen Bedingungen der Datenverarbeitung den Schutz der Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe der persönlichen Daten voraussetze. Das Recht auf informationelle Selbstbestimmung gewährleistet den Einzelnen die **Befugnis, selbst über die Preisgabe und Verwendung persönlicher Daten zu bestimmen.**[56] Das Recht umfasst nicht nur elektronisch speicherbare, sondern sämtliche personenbezogenen Daten.[57] Dabei ist es grundsätzlich gleichgültig, wo diese Informationen gewonnen wurden oder welchen Inhalt sie haben.[58] Einschränkungen bedürfen eines Gesetzes und unterliegen einer strikten Prüfung der Verhältnismäßigkeit.

---

[52] Vgl. BVerfG NJW 2005, 1917, 1918.
[53] So das BVerfG, NJW 2005, 1917, 1919 f. in Bezug auf das Vertrauensverhältnis „Anwalt und Mandant“.
[54] Dies entspricht im Grundsatz der von der *Bundesregierung* i. Z. m. dem Schutz von Berufsgeheimnisträgern/-innen vertretenen Auffassung. Da sie Ausnahmeregelungen für die Speicherung von Telekommunikationsverkehrsdaten von Berufsgeheimnisträgern/-innen ebenso wie eine Begrenzung der Speicherungspflicht in der Richtlinie selbst für *„technisch und wirtschaftlich nicht leistbar“* hält, strebt sie entsprechende Schutzregelungen im Rahmen der Umsetzung durch die den Behördenzugang zu den gespeicherten Daten regelnden nationalen Bestimmungen an. Sie verweist insoweit beispielhaft auf § 100h Abs. 2 stopp, BT-Drs. 16/142, S. 3 zu Ziff. 4.
[55] Grundlegend BVerfGE 65, 1, 41 ff. Danach steht den Einzelnen das Recht zu, „selbst über die Preisgabe und Verwendung persönlicher Daten zu bestimmen“ (S. 43). Damit steht ihnen auch die Befugnis zu, „grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden, E 65, 1, 41 f.; vgl. auch E 78, 77, 84; E 84, 192, 194; E 103, 21, 33.
[56] BVerfG 65, 1, 43; E 84, 192, 194; E 103, 21, 32 f.
[57] BVerfGE 65, 1, 41 f.; E 103, 21, 32 f.
[58] BVerfG 101, 361, 381; E 106, 28, 40.

Sofern es um die unkörperliche Übermittlung von Informationen durch Telekommunikation geht, ist das speziellere, durch Art. 10 GG geschützte **Fernmeldegeheimnis** betroffen. Das Grundrecht ist entwicklungsoffen und umfasst beliebige elektromagnetische und andere unkörperliche Formen der Übermittlung (per Kabel oder Funk, analo oder digital, durch optische oder akustische Signale. Wesentlich ist, dass die Zeichen am Empfangsort wieder erzeugt werden. Geschützt wird sowohl der Inhalt als auch die Art und Weise der Kommunikation.[59] Da nach überwiegender Auffassung echte Privatpersonen bzw. Privatunternehmen nicht zu den Adressaten des Art. 10 GG gezählt werden und daher private Diensteanbieter nicht binden[60] – in privatrechtlichen Beziehungen ist die Ausstrahlungswirkung von Art. 10 GG zu beachten – , soll Art. 10 GG im Folgenden außer Betracht bleiben.

Das Grundrecht auf informationelle Selbstbestimmung schützt, wie das *BVerwG* 2004 („Herausgabe von Stasi-Unterlagen") hervorgehoben hat, auch Amtsträger/-innen als solche.[61] Damit bestätigte das *BVerwG* seine Rechtsprechung aus dem Jahre 2002, wonach *„amts- und funktionsbezogene Informationen – richtige und erst recht manipulierte – für einen Politiker in einem demokratischen Staat existenzvernichtende Folgen mit schwerwiegenden Auswirkungen auch auf die Privatsphäre haben können."*[62]

Ergänzend ist auf die Ausführungen des *BVerfG* in der o. g. Entscheidung aus dem Jahr 2005 Bezug zu nehmen. Darin führt es im Hinblick auf den von der Datenbeschlagnahme betroffenen Rechtsanwalt aus, das Recht auf informationelle Selbstbestimmung diene mittelbar, *„auch dem Schutz vor einem Einschüchterungseffekt, der entstehen und zu Beeinträchtigungen bei der Ausübung anderer Grundrechte führen kann, wenn für den Einzelnen nicht mehr erkennbar ist, wer was wann und bei welcher Gelegenheit über ihn weiß."* Der damit verbundene *„abschreckende Effekt fremden Geheimwissens"* müsse daher nicht nur im Interesse der betroffenen Einzelnen vermieden werden, sondern auch im Interesse des ebenfalls betroffenen Gemeinwohls, da die Selbstbestimmung als *„elementare Funktionsbedingung eines auf Hand-*

---

[59] *Jarass*, in: Jarass/Pieroth, GG, 7. Aufl. Art. 10 Rn. 9.
[60] *Jarass*, a.a.O., Art. 10 Rn. 16.
[61] BVerwGE 121, 115, 123: „Die Gefahr, dass das Erscheinungsbild eines Menschen in einer bestimmten Situation von diesem abgelöst und in anderen Zusammenhängen vor einem unüberschaubaren Personenkreis reproduziert, dabei verändert oder manipuliert wird, besteht bei Amtsträgern nicht anders als bei anderen, und sie besteht auch – und vielleicht gerade – hinsichtlich seines Erscheinungsbildes „im Amt". Die Folgen einer solchen beliebigen Darstellung treffen den Einzelnen nicht nur in seinem Amt – dessen Ausübung ja häufig zugleich sein Beruf ist –, sondern regelmäßig zugleich in seiner persönlichen und privaten Existenz."
[62] Vgl. BVerwGE 116, 104, 112.

lungs- und Mitwirkungsfähigkeit seiner Bürger gegründeten freiheitlichen Gemeinwesens" zu betrachten sei.[63]

Zwar fehlt es bislang noch an einer entsprechenden Rechtsprechung des *BVerfG* in Bezug auf Abgeordnete, angesichts der in beiden Fällen bestehenden Berufsgeheimnisträgerschaft, erscheinen die obigen Erwägungen aber auf Abgeordnete übertragbar. Es liegt nahe, dass der oben beschriebene Einschüchterungseffekt auch sie an der Ausübung ihres Amtes i. S. v. Art. 3 Abs. 1, Abs. 4, Art. 10, Art. 11 Abs. 1 LV bzw. Art. 38 GG (das durch die besonderen Rechte gem. Art. 47 GG bzw. Art. 24 Abs. 3 LV geschützt werden soll) hindern und damit in ihrer parlamentarischen Tätigkeit einschränken kann.

Im Hinblick darauf erscheint eine umfangreiche Speicherung personenbezogener Daten zu unbestimmten Zwecken, wie in der Richtlinie zur Vorratsdatenspeicherung vorgesehen, angesichts der besonderen verfassungsrechtlichen Bedeutung des Rechts auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG (allgemeines Persönlichkeitsrecht), nur schwer zu rechtfertigen. [64] Insofern hat das *BVerfG* in der o. g. Entscheidung aus dem Jahre 2005 ausdrücklich klargestellt, dass die gesetzliche Grundlage nur dann den Anforderungen des Recht auf informationelle Selbstbestimmung genügt, wenn der Gesetzgeber den **Verwendungszweck** der erhobenen Daten **bereichsspezifisch** und **präzise** bestimmt habe. Sofern es sich um Datenträger bzw. Daten von Berufsgeheimnisträgern/-innen handele, sei die besondere Schutzbedürftigkeit der von einem überschießenden Datenzugriff mitbetroffenen Vertrauensverhältnisse zu beachten. Der eingriffsintensive Zugriff auf Datenträger bedürfe daher im jeweiligen Einzelfall in besonderer Weise einer regulierenden Beschränkung.[65]

---

[63] BVerfG, NJW 2005, 1917, 1918.

[64] Instruktiv dazu die kritischen Ausführungen von *Ulmer/Schrief,* DuD 2004, 591 ff, die die Verfassungsmäßigkeit einer umfassenden Vorratsdatenspeicherung zu unbestimmten Zwecken verneinen; ebenso *Kühling,* K&R 2004, 105 ff.; i. E. ähnlich derzeit die Opposition im BT, vgl. den Antrag der *Fraktion der FDP* v. 01.12.2005, BT-Drs. 16/128 S. 2; Antrag der *Fraktion BÜNDNIS 90/DIE GRÜNEN* v. 14.12.2005, BT-Drs. 16/237, S. 1 f.; ebenso die Kleine Anfrage der *Fraktion DIE LINKE* v. 18.11.2005, BT-Drs. 16/72 S. 1 f.; vgl. auch die Entschließung der 70. Konferenz der *Datenschutzbeauftragten des Bundes und der Länder* am 27./28.10.2005, wonach die anlasslose Vorratsdatenspeicherung als verfassungswidrig eingestuft wird, www.datenschutzzentrum.de, download v. 06.02.2005; vgl auch die Stellungnahme des *Europäischen Datenschutzbeauftragten,* der die Verhältnismäßigkeit der Vorratsdatenspeicherung gem. KOM (2005) 438 endg. bezweifelt, ABL. EG Nr. C 298 v. 29.11.2005, S. 4 ff.). Das *BVerfG* hat erst unlängst in der Entscheidung zur vorbeugenden Überwachung der Telekommunikation vom 27.07.2005 hervorgehoben, dass insbesondere gesetzliche Vorkehrungen gegen Eingriffe in den absolut geschützten Kernbereich privater Lebensgestaltung notwendig sind, BVerfG, NJW 2005, 2603 ff.

[65] BVerfG, NJW 2005, 1917, 1920; vgl. auch BVerfG, Urt. v. 27.07.2005, Az. 1 BvR 668/04, NJW 2005, 2603, 2607 f.

Vor allem aber wird das staatliche Handeln durch den **Grundsatz der Verhältnismäßigkeit** begrenzt. Eingriffe in die Rechte Unverdächtiger, so das *BVerfG,* sind nach dem Grundsatz der Verhältnismäßigkeit in besonderer Weise rechtfertigungsbedürftig. In diesem Zusammenhang seien das Recht auf informationelle Selbstbestimmung sowie die Gefährdung des rechtlich geschützten Vertrauensverhältnisses zwischen den jeweiligen Berufsgeheimnisträgern/-innen und ihren Mandanten/-innen in den Blick zu nehmen. Bedeutung dürfte in Bezug auf Abgeordnete auch der objektivrechtliche Gehalt des „freien Mandats" gem. Art. 38 GG erlangen und das damit verbundene öffentliche Interesse an der besonders geschützten Vertraulichkeit der Kommunikation.[66]

Ob die Vorratsdatenspeicherung nach Maßgabe der Richtlinie diesem verfassungsrechtlichen Maßstab entspricht, erscheint insbesondere vor der aktuellen Entscheidung des *BVerfG* vom 28.07.2005[67] („Präventive Telekommunikationsüberwachung durch das Niedersächsische Polizeigesetz") äußerst fraglich. Die Verfassungsbeschwerde richtete sich gegen eine Norm des Niedersächsischen Polizeigesetzes, durch die personenbezogene Daten bereits im Vorfeld von Straftaten durch Überwachung der Telekommunikation von der Polizei erhoben werden durften, also in einer Phase, in der *„sich die Konturen des Straftatbestandes noch nicht abzeichneten".* Sofern der Gesetzgeber in solchen Situationen der Vorfeldermittlung Grundrechtseingriffe vorsehe, müsse er die den Anlass bildenden Straftaten sowie die Anforderungen an Tatsachen, die auf die künftige Begehung hindeuten, **so bestimmt umschreiben**, dass das Risiko einer Fehlprognose verfassungsrechtlich noch hinnehmbar sei. Andernfalls werde gegen das Bestimmtheitsgebot verstoßen. Im Hinblick auf den Verhältnismäßigkeitsgrundsatz sei im Rahmen der Verhältnismäßigkeit im engeren Sinn zu berücksichtigen, dass der Gesetzgeber zwischen den Allgemein- und Individualinteressen einen angemessenen Ausgleich herstellen müsse. Das Gericht bejahte hier einen schwerwiegenden Eingriff in das durch **Art. 10 GG geschützte Fernmeldegeheimnis**, da Kommunikationsinhalte, Verbindungsdaten und Standortkennung weite Einblicke in das Kommunikationsverhalten zuließen und eine unbefangene Telekommunikation verhinderten. Dies galt nach Auffassung des *BVerfG* ausdrücklich auch für Verbindungsdaten. Angesichts der großen Streubreite der Eingriffe nicht nur in Bezug

[66] Entsprechend zur Bedeutung der „freien Advokatur" BVerfG, NJW 2005, 1917, 1921.
[67] BVerfG NJW 2005, 2603 ff.

auf potentielle Straftäter, sondern auch auf völlig unbeteiligte Personen, bejahte das *BVerfG* letztlich einen unverhältnismäßigen Eingriff in das Fernmeldegeheimnis.

c. Schutzgewährleistung durch das BVerfG oder den EuGH?

Die Frage, ob die anlassunabhängige Vorratsdatenspeicherung nach Maßgabe der Richtlinie gegen das deutsche Verfassungsrecht verstößt – Abgeordnetenschutzrechte, Grundrecht auf informationelle Selbstbestimmung, das durch Art. 10 GG geschützte Fernmeldegeheimnis[68] (insoweit *lex specialis*) – wird künftig auf die EU-Ebene „verlagert" werden, denn er betrifft vorrangig Fragen zur Auslegung der Richtlinie und des gemeinschaftsrechtlichen Grundrechtsschutzes .

Seit der „Solange II"-Entscheidung (1986) prüft das *BVerfG* sekundäres Gemeinschaftsrecht nicht mehr am Maßstab des Grundgesetzes.[69] Nach Irritationen durch das teilweise anders interpretierte „Maastricht"-Urteil (1993)[70] stellte das *BVerfG* dann in dem „Bananenmarkt"-Beschluss[71] (2000) klar, dass insofern ein deckungsgleicher Grundrechtsschutz durch den *EuGH* nicht gefordert sei.

Dementsprechend wertet das *BVerfG* Verfassungsbeschwerden und Vorlagebeschlüsse, die die Grundrechtsverletzung durch abgeleitetes Gemeinschaftsrecht rügen, heute als „*von vornherein unzulässig"*, es sei denn in der Begründung ließe sich darlegen, dass die europäische Rechtsentwicklung einschließlich der Rechtsprechung des *EuGH* nach Ergehen der „Solange II"-Entscheidung unter den erforderlichen Grundrechtsstandard abgesunken ist.[72] Insoweit müsste im Einzelfall dargelegt wer-

---

[68] Zur teilweisen Verfassungswidrigkeit der verdachtslosen Rasterfahndung wegen unzureichender Zweckbindung der erhobenen Daten, unzureichender Sicherung des Verwendungszwecks bei der Weitergabe der Informationen aus der Fernmeldeüberwachung des BND an die Bundesregierung und andere Behörden sowie wegen Unausgewogenheit zwischen Schutzgut und Übermittlungsschwelle bei der Weitergabe von Daten an andere Behörden insb. zum Zwecke der Strafverfolgung, vgl. BVerfGE 100, 313, 385 ff.

[69] BVerfGE 73, 339. „Solange" der *EuGH* einen wirksamen Schutz der Grundrechte gegenüber der Hoheitsgewalt der Gemeinschaften *generell* gewährleistet, der dem vom Grundgesetz als unabdingbar gebotenen Grundrechtsschutz im Wesentlichen vergleichbar ist, beschränkt das *BVerfG* seine eigene Prüfungsbefugnis.

[70] BVerfGE 89, 155.

[71] BVerfG v. 07.06.2000, Az. 2 BvL 1/97, NJW 2000, 3124.

[72] In dem Verfahren wandte sich eine Hamburger Ärztin gegen ein Urteil des BVerwG und rügte u. a. eine Verletzung des Art. 12 Abs. 1 GG durch die Richtlinien 86/457/EWG und 93/16/EWG. Dazu heißt es:
„ Soweit sich die Beschwerdeführerin inhaltlich gegen die Richtlinie 86/457/EWG und die Richtlinie 93/16/EWG wendet und eine Verletzung ihrer Grundrechte aus Art. 12 Abs. 1 GG Art. 3 Abs. 3 GG geltend macht, sind ihre Rügen unzuläsig. Gemeinschaftsrecht wird grundsätzlich nicht mehr am Maßstab der Grundrechte durch das Bundesverfassungsgericht geprüft; Verfassungsbeschwerden und Vorlagen von Gerichten sind von vornherein unzulässig, wenn ihre Begründung nicht darlegt, dass die europäische Rechtsentwicklung einschließlich der Rechtsprechung des Europäischen Gerichtshofs unter die erforderlichen Gruundrechtsstandards abgesunken ist".

den, dass der jeweils als unabdingbar gebotene Grundrechtsschutz generell nicht gewährleistet wird, sodass eine Gegenüberstellung des Grundrechtsschutzes auf nationaler und auf Gemeinschaftsebene erforderlich wäre.[73] Dieser Maßstab gilt nach der Rechtsprechung des *BVerfG* (2001) auch für nationales Recht, soweit dieses zwingende Vorgaben des Gemeinschaftsrechts umsetzt:

> „*Soweit die Normsetzung zwingend dem Gemeinschaftsrecht folgt, ist sie ebenso wie das sekundäre Gemeinschaftsrecht selbst nicht mehr am Maßstab der deutschen Grundrechte durch das Bundesverfassungsgericht zu prüfen, sondern unterliegt dem auf Gemeinschaftsrechtsebene gewährleisteten Grundrechtsschutz".*[74]

Die Verzahnung der gemeinschaftsrechtlichen und nationalen Grundrechts- bzw. Verfassungsrechtskreise wird daher mangels Zuständigkeit des *BVerfG* regelmäßig auf ein Vorabentscheidungsersuchen gem. Art. 234 EG an den *EuGH* hinauslaufen, durch welches der *EuGH* die Möglichkeit erhält, sekundäres Gemeinschaftsrecht anhand der im Gemeinschaftsrecht entwickelten Grundrechtsverbürgungen zu überprüfen.

In Bezug auf die Richtlinie zur Vorratsdatenspeicherung besteht daher grundsätzlich keine Zuständigkeit des *BVerfG* zur materiellen Grundrechtsprüfung. Allenfalls in den Bereichen, in denen den Mitgliedstaaten ein Umsetzungsermessen im Einklang mit ihren nationalen Regelungen eingeräumt wird, bleibt Raum für die Prüfung des *BVerfG* anhand des Grundgesetzes. Dies kann etwa die Regelungen über die Konkretisierung der „schweren Straftaten" und die Weiterleitung der gespeicherten Daten an die zuständigen nationalen Behörden betreffen.[75]

Im Hinblick auf den Grundrechtsschutz kommt es daher maßgeblich auf die **Europäischen Grundrechte** in ihrer Ausprägung durch die Charta der Grundrechte der Europäischen Union (GRC)[76] und die Rechtsprechung des *EuGH* an. Berücksichtigung

---

Die Verfassungsbeschwerde hatte letztlich aus anderen Gründen Erfolg, da die Entscheidung des BVerwG, das seiner Pflicht zur Vorlage an den EuGH nicht nachgekommen war, die Beschwerdeführerin in ihrem Grundrecht aus Art. 101 Abs. 1 S. 2 GG verletzt hatte, vgl. BVerfG, NJW 2001, 1267, 1268.

[73] BVerfG, NJW 2000, 3124; vgl. auch BVerfGE 73, 339, 376 ff.

[74] BVerfG, NJW 2001, 1267, 1268.

[75] Vgl. dazu die Entscheidung des BVerfG zur Nichtigkeit des Europäischen Haftbefehlgesetzes v. 18.07.2005, Az. 2 BvR 2236/04 (LS 3), das den Rahmenbeschluss über den Europäischen Haftbefehl umgesetzt hat („Dritte Säule", GASP).

[76] ABl. C 364 v. 18.12.2000, S. 1. Es sprechen schon jetzt gute Gründe dafür, die GRC bereits heute als rechtserheblich zu betrachten. So haben sich zwischenzeitlich eine Reihe der *Generalanwälte* auf die GRC als Quelle der Identifikation von Gemeinschaftsrundrechten bezogen und auch das *Gericht Erster Instanz* hat bereits auf die GRC verwiesen, vgl. z. B. GA Alber, Rs. C-340/99 (TNT Traco), GA Tizzano, Rs. C-173/99 (BECTU); GA Stix-

erfahren insoweit auch die Menschenrechtsgewährleistungen der EMRK sowie die Rechtsprechung des EGMR.

aa. Keine Gewährleistung spezifischer Abgeordnetenschutzrechte durch die EMRK und GRC auf europäischer Ebene

Im internationalen wie auch europäischen Vergleich lässt sich ein ausdrücklich normiertes Zeugnisverweigerungsrecht für Abgeordnete nur selten feststellen. Die EMRK enthält kein entsprechendes Schutzrecht für Abgeordnete. Eine gewohnheitsrechtliche Ableitung auf europäischer Ebene dürfte daher an den unterschiedlichen Verfassungslagen der Mitgliedstaaten scheitern.[77] Anders als in Deutschland ist ein Zeugnisverweigerungsrecht für Abgeordnete auf verfassungsrechtlicher Ebene lediglich in einzelnen EU-Staaten normiert.[78] Auch die GRC sieht keine speziellen Schutzrechte für Abgeordnete vor. Ob auf gemeinschaftsrechtlicher Ebene ein dem deutschen Verfassungsrecht entsprechender Schutz von Abgeordneten gewährleistet wird, hängt daher davon ab, ob andere Gemeinschaftsgrundrechte einen äquivalenten Abgeordnetenschutz gewährleisten.

bb. Recht auf Schutz personenbezogener Daten gem. Art. 8 GRC

In den Blick rückt damit **Art. 8 GRC,** welcher das „Recht auf Schutz personenbezogener Daten“ in den Rang eines Grundrechts erhebt.[79] Art. 8 GRC stützt sich auf Art. 286 EG und die *Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr 95/46/EG* (EG-Datenschutzrichtlinie)[80] sowie auf Art. 8 EMRK („Achtung des Privatlebens“) und das von allen Mitgliedstaaten ratifizierte Übereinkommen des Europarates 1981 zum

---

Hackl, Rs. C 49/00 (Komm./Italien), Rs. C-131/00 (Nilsson), Rs. C-459/99 (MRAX); GA Geelhoed, Rs. C-413/99 (Baumbast und R), Rs. C-313/99 (Mulligan u. a.); GA Léger, Rs. C-353/99, (P Rat/ Hautala u. a.), Rs. C-309/99 (Wouters); vgl. auch EuG, Urt. v. 30.01.2002, T-54/99 (max-mobil) und Urt. v. 03.05.2002, T-177/01 (Jégo-Quéré). Jedenfalls aber kommt der Einbezug über Art. 6 Abs. 2 EU in Betracht. Danach achtet die Union die Grundrechte, wie sie in der EMRK gewährleistet sind und wie sie sich aus den gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten als allgemeine Grundsätze des Gemeinschaftsrechts ergeben, ebenso *Kingreen*, in *Calliess*/ *Ruffert* (Hrsg.), Kommentar zu EU-Vertrag und EG-Vertrag, 2. Aufl. 2002, Art. 6 EU Rn. 43; *Calliess*, EuZW 2001, S. 261, 267; *M. Schmidt*, Europäisches Arbeitsrecht, 2001, I Rn. 86; *Zuleeg*, EuGRZ 2000, S. 511, 514; *Laskowski*, KJ 2003, S. 421, 448.

[77] *Schulze-Fielitz*, a.a.O., Art. 47 Rn. 2

[78] *Schulze-Fielitz*, a.a.O., Art. 47 Rn. 3.

[79] *Bernsdorff*, in: Meyer (Hrsg.), Kommentar zur Charta der Grundrechte der Europäischen Union, 2003, Art. 8 Rn. 1.

[80] ABl. EG 1995 Nr. L 281, 31.

Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten.[81] Zudem wird in den Verfassungen der Mitgliedstaaten das Recht auf Schutz personenbezogener Daten ausdrücklich oder aber als Ausfluss anderer Rechte garantiert.[82] Das durch Art. 8 GRC geschützte Grundrecht soll nach Maßgabe der EG-Datenschutzrichtlinie ausgeübt werden. Einschränkungen sind unter den Voraussetzungen des Art. 52 GRC möglich.[83] Art. 8 GRC steht in einem engen Zusammenhang mit **Art. 7 GRC**, welcher das Recht jeder Person auf Achtung des Privat- und Familienlebens schützt und **Art. 8 EMRK** nachgebildet ist.[84] Damit regelt Art. 8 GRC einen speziellen Aspekt des Schutzes der Privatsphäre i. S. v. Art. 7 GRC. Aus der Zusammenschau dieser Regelungen wird das gemeinschaftsrechtliche **Recht auf informationelle Selbstbestimmung** hergeleitet, welches der EuGH bereits 1969 („Stauder") der Sache nach – jedoch ohne es zu benennen – anerkannt hat.[85]

Art. 8 Abs. 1 GRC übernimmt das Konzept der EG-Datenschutzrichtlinie[86], die heute durch die *Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation 2002/58/EG (*EG-Datenschutzrichtlinie für elektronische Kommunikation)[87] ergänzt wird. Art. 8 Abs. 2 GRC folgt dem in Art. 6 ff. EG-Datenschutzrichtlinie festgelegten Rahmen für die grds. den Mitgliedstaaten überlassene Festlegung rechtmäßiger Datenverarbeitung (vgl. Art. 5 RL 95/46/EG). [88] Die in die EG-Datenschutzrichtlinien vorgesehenen **Schranken zulässiger Datenverarbeitung** sind als sekundärrechtliche Regelungen **im Lichte der allgemeinen Grundrechtsschranke des Art. 52 Abs. 1 GRC** und unter Beachtung des **Art. 8 EMRK** zu interpretieren (Art. 52 Abs. 3 GRC).[89] Entsprechendes gilt im Hinblick auf die hier in Rede stehende EU-Richtlinie zur Vorratsdatenspeicherung.

---

[81] BGBl. 1985 II, 539.
[82] *Streinz*, in: Ders. (Hrsg.), EUV/EGV, 2003, Art. 8 GRC Rn. 2.; *Bernsdorff*, a.a.O., Art. 8 Rn. 3 m. w. N.
[83] *Streinz*, a.a.O., Art. 8 Rn. 1 unter Bezugnahme auf die Erläuterung des Präsidiums.
[84] *Bernsdorff*, a.a.O., Art. 7 Rn. 1.
[85] EuGH – C-29/69 –, Slg. 1969, 419 („Stauder") ; später EuGH – C-145/83 –, Slg. 1985, 3539 („Stanley George Adams"); EuGH – C-404/92 – Slg. 1994, 4780 („Aids-Test"); EuGH – C-465/00, C-138/01 und C-139/01 –, Slg. 2003, 4989 („Österreichischer Rundfunk" u. a.); zur Rspr. des EGMR vgl. Urt. v. 26.03.1987 („Leander/Schweden"), Nr. 10/1985/96/144, Serie A/116; dazu insgesamt *Bernsdorff*, a.a.O., Art. 8 Rn. 14.
[86] Der Konvent hat seinerzeit die in Richtlinie 95/46/EG aufgestellten Verarbeitungsanforderungen in Art. 8 Abs. 2 S. 1 GRC ohne Änderungen übernommen, dazu näher *Bernsdorff*, a.a.O., Art. 8 Rn. 22.
[87] ABl. EG 2002 Nr. L 201, 37.
[88] *Streinz*, a.a.O., Art. 8 Rn. 6.
[89] *Bernsdorff*, a.a.O., Art. 8 Rn. 17, 19; *Streinz*, a.a.O., Art. 8 Rn. 5; EuGH v. 20.05.2003, Az. C-465/00, Slg. 2003, I-4989 LS 2.

Zwar hat der *EuGH* – anders als die Generalanwälte/-innen und der EuG – bislang noch keine Veranlassung gesehen, sich zur Wirksamkeit der GRC zu äußern. Sinngemäß legt er den oben skizzierten Maßstab aber seiner aktuellen Rechtsprechung zum Schutz personenbezogener Daten zugrunde.

In dem Urteil des *EuGH* vom 20.05.2003[90], in der es zum Schutz natürlicher Personen bei der Speicherung und Verarbeitung personenbezogener Daten Stellung nahm, stellte es jedoch klar, dass die bloße Speicherung personenbezogener Daten als solche (im streitigen Fall: Daten über die an das Personal gezahlten Gehälter durch den Arbeitgeber) noch *keinen* Eingriff in die Privatsphäre begründet, sondern **erst die Weitergabe dieser Daten** an Dritte – in dem streitigen Fall an eine nationale Behörde – unabhängig von der späteren Verwendung der übermittelten Informationen eine Beeinträchtigung des Rechts der betroffenen auf Achtung ihres Privatlebens und damit einen Eingriff i. S. v. Art. 8 EMRK darstellt.

cc. Fazit

Als Fazit lässt sich vorläufig festhalten: Friktionen zwischen dem nationalen Recht auf informationelle Selbstbestimmung in der Rechtsprechung des *BVerfG,* das bereits vor Daten*speicherung* schützt und dem durch die Rechtsprechung des *EuGH* gewährten Schutz personenbezogener Daten, das erst die Daten*weiterleitung* betrifft, scheinen nicht ausgeschlossen. In Konsequenz dessen erscheinen künftige Einschränkungen der Abgeordnetenschutzrechte durchaus denkbar.

Diesbezüglich ist die Rechtsprechung des *EuGH* abzuwarten. Sollte sich in diesem Zusammenhang herausstellen, dass das durch den *EuGH* gewährte Schutzniveau zu einer Absenkung grundgesetzlich vorgegebenen Schutzniveaus führt, bleibt abzuwarten, ob das *BVerfG* vor diesem Hintergrund von seiner im „Maastricht"-Urteil 1993[91] formulierten „Reservebefugnis" zur Prüfung von Grundrechtsverletzungen durch Gemeinschaftsrecht künftig doch Gebrauch macht. Insoweit wird es auf die Beurteilung der Frage ankommen, ob *„die europäische Rechtsentwicklung (…) unter den erforderlichen Grundrechtsstandard abgesunken (…) und der jeweils als unabdingbar gebotene Grundrechtsschutz generell nicht mehr gewährleistet ist".*[92]

---

[90] EuGH v. 20.05.2003, Az. C-465/00, Slg. 2003, I-4989.
[91] BVerfGE 89, 155.
[92] BVerfGE 101, 147, 164.