



Ausarbeitung

Zur Vereinbarkeit der Richtlinie über die Vorratsspeicherung von Daten mit der Europäischen Grundrechtecharta

Roland Derksen

Zur Vereinbarkeit der Richtlinie über die Vorratsspeicherung von Daten mit der Europäischen Grundrechtecharta

Verfasser/in: MR Dr. Roland Derksen,
Aktenzeichen: WD 11 – 3000 – 18/11
Abschluss der Arbeit: 25. Februar 2011
Fachbereich: WD 11: Europa
Telefon: 030 227 33614

Inhaltsverzeichnis

1.	Einleitung	4
2.	Anwendungsbereich der Grundrechtecharta	6
3.	Eingriffe in Grundrechte der Charta	6
3.1.	Achtung des Privat- und Familienlebens (Art. 7 GRCh)	6
3.1.1.	Schutzbereich	6
3.1.2.	Eingriff	7
3.2.	Schutz personenbezogener Daten (Art. 8 GRCh)	8
3.2.1.	Schutzbereich	9
3.2.2.	Eingriff	9
3.3.	Berufs- und wirtschaftliche Betätigungsfreiheit (Art. 15 und 16 GRCh)	9
3.3.1.	Schutzbereich	10
3.3.1.1.	sachlicher Anwendungsbereich	10
3.3.1.2.	persönlicher Anwendungsbereich	10
3.3.2.	Eingriff	11
3.3.3.	Zwischenergebnis	12
4.	Rechtfertigung der Eingriffe	12
4.1.	Möglichkeit der Rechtfertigung	12
4.2.	Verhältnismäßigkeit	14
4.2.1.	legitimes Ziel	14
4.2.2.	Geeignetheit des Eingriffs	14
4.2.3.	Erforderlichkeit des Eingriffs	15
4.3.	Angemessenheit	17
5.	Ergebnis	21

1. Einleitung

Die „Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG“¹ (RL 2006/24/EG) musste von den Mitgliedstaaten bis zum 15. September 2007 in nationales Recht umgesetzt werden. Gegen Irland, Griechenland, Schweden und Österreich hat die Europäische Kommission jeweils wegen nicht rechtzeitiger bzw. mangelhafter Umsetzung ein Vertragsverletzungsverfahren eingeleitet.² Der Europäische Gerichtshof (EuGH) hat in jedem Verfahren die Position der Kommission bestätigt. In diesen Staaten liegen daher keine Umsetzungsgesetze vor. Gegen Luxemburg hat die Kommission Anfang August Klage wegen ungenügender Umsetzung eingereicht.³

In Deutschland wurde die Richtlinie mit dem „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ vom 21. Dezember 2007⁴ umgesetzt. Die Änderungen betrafen im Wesentlichen die Strafprozessordnung (StPO) und das Telekommunikationsgesetz (TKG).

Das **Bundesverfassungsgericht** (BVerfG) hat die deutschen Umsetzungsmaßnahmen in §§ 113a, 113b Telekommunikationsgesetz und § 100g Abs. 1 S. 1 Strafprozessordnung für verfassungswidrig erklärt.⁵ Die Speicherung der Daten sei zwar nicht von vorneherein mit Art. 10 Abs. 1 GG unvereinbar, jedoch sei die konkrete Ausgestaltung unverhältnismäßig, da weder Sicherheitsbedenken Rechnung getragen noch die Verwendungszwecke begrenzt worden seien.

Folgende **Anforderungen** hat das BVerfG für das deutsche Umsetzungsgesetz aufgestellt: Die Speicherung der Daten müsse durch private Unternehmen unter strenger Beachtung der Datensicherheit erfolgen und dürfe nur für einen engen zeitlichen Rahmen erlaubt sein. Die anlasslose Speicherung müsse eine Ausnahme bleiben und die gewonnenen Daten dürften nur aus einem wichtigen Grund verwendet werden. Es müsse ein wirksamer Rechtsschutz bestehen, unter anderem müsse dem Betroffenen grundsätzlich offengelegt werden, wenn Daten abgerufen würden. Demgegenüber hat es betont, dass die Richtlinie grundsätzlich grundrechtskonform umgesetzt werden könne.⁶

1 Amtsblatt L 105, S. 54, vom 13.04.2006.

2 Irland: C-202/09, 26.11.2009; Griechenland: C-211/09, 26.11.2009; Schweden: C-185/09, 04.02.2010; Österreich: C-189/09, 29.07.2010.

3 Rechtssache C-394/10.

4 BGBl. 2007 I S. 3198.

5 BVerfG, 1 BvR 256/08 u. a., 02.03.2010.

6 BVerfG, 1 BvR 256/08 u. a., 02.03.2010, Rn. 187.

Nach ähnlichen Entscheidungen von Verfassungsgerichten in anderen Mitgliedstaaten⁷, dass die Vorratsspeicherung gegen das nationale Verfassungsrecht verstoße, wird auf europäischer Ebene die Richtlinie kritisch betrachtet.⁸ Eine Nichtigkeitsklage Irlands wies der EuGH 2009 zwar ab.⁹ Irland hatte jedoch lediglich die Zuständigkeit der EU zur Harmonisierung des Rechtsgebiets gerügt. Eine inhaltliche Kontrolle durch den EuGH fand in diesem Verfahren nicht statt. Im Mai 2010 hat der irische High Court entschieden, dem EuGH nun die **Frage vorzulegen, ob die Richtlinie gegen Menschenrechte verstoße**.¹⁰

Auf Anfragen des Europäischen Parlaments antwortete die zuständige **Kommissarin Malmström**, dass die Richtlinie unter Berücksichtigung der Europäischen Grundrechtecharta (GRCh) verfasst worden und von den Mitgliedstaaten daher so lange zu beachten sei, bis sie zurückgenommen oder vom EuGH für nichtig erklärt würde.¹¹

Eine **Evaluation** der Richtlinie sollte nach Art. 14 RL 2006/24/EG von der Kommission bis zum 15. September 2010 vorgelegt werden.¹² In dem Bericht sollen die Auswirkungen der Richtlinie auf die Wirtschaftsbeteiligten und auf die Privatsphäre der Datennutzer geprüft werden. Er soll auf Informationen aller beteiligten relevanten Akteure beruhen. Die Kommission hat die Vorlage des Berichts auf die erste Jahreshälfte 2011 verschoben.

Nachfolgend wird geprüft, ob die RL 2006/24/EG in Grundrechte der Charta eingreift und ob, wenn dies der Fall ist, die Eingriffe gerechtfertigt sind. In diesem Zusammenhang findet auch das Urteil des EuGH vom 9.11.2010¹³ Berücksichtigung.

7 Schweden will trotz Verurteilung durch den EuGH keinen Gesetzentwurf erarbeiten. Rumäniens Verfassungsgericht sah einen Verstoß gegen die Verfassung: <http://www.mediafax.ro/english/romania-s-constitutional-court-rules-data-storage-law-unconstitutional-4972690/> (Stand: 20.01.2011).

8 Die Artikel 29-Datenschutzgruppe der Europäischen Union bemängelt eine inhomogene Umsetzung in den Mitgliedstaaten, insbesondere im Hinblick auf die Sicherheitsmaßnahmen der Telekommunikationsdienstleister (Bericht vom 13.07.2010, WP 172).

9 EuGH, Urteil vom 10.02.2009, C-301/06.

10 Vgl. <http://www.mcgarrosolicitors.ie/2010/05/05/digital-rights-ireland-update/> (Stand: 20.01.2011). In der Datenbank des EuGH findet sich allerdings noch kein diesbezüglicher Eintrag.

11 Anfrage vom 20. April 2010, E-2588/2010, und vom 16. Juni 2010, E-4328/2010.

12 Gemäß Art. 14 Abs. 1 RL 2006/24/EG hätte die Kommission dem Europäischen Parlament und dem Rat spätestens am 15.09.2010 eine Bewertung der Anwendung der Richtlinie sowie ihrer Auswirkungen auf die Wirtschaftsbeteiligten und die Verbraucher vorlegen müssen. Erklärtes Ziel ist es festzustellen, ob die Bestimmungen der Richtlinie, insbesondere die Liste von Daten in Artikel 5 und die in Artikel 6 vorgesehenen Speicherdauern, gegebenenfalls geändert werden müssen. Die Ergebnisse der Bewertung sind zu veröffentlichen.

13 C-92/09

2. Anwendungsbereich der Grundrechtecharta

Der Anwendungsbereich der Grundrechtecharta ist nur dann eröffnet, wenn Organe oder Einrichtungen der EU oder die Mitgliedstaaten EU-Recht, also Primär- und Sekundärrecht der EU, durchführen (Art. 51 GRCh). Was darunter genau zu verstehen ist, ist umstritten. Der Grundrechtekonvent hat sich gegen die Formulierung „bei Anwendung des Gemeinschaftsrechts“ entschieden und stattdessen den Ausdruck „bei der Durchführung des Rechts der Union“ bevorzugt.¹⁴ Mit dieser Formulierung sollte die vom EuGH vorgenommene bisherige weite Anwendung der Unionsgrundrechte auf alle unionsrelevanten Sachverhalte, insbesondere auf Bereiche, die die Grundfreiheiten betreffen, eingeschränkt werden.¹⁵ Die Grundrechtecharta findet also dann Anwendung, wenn die Mitgliedstaaten durch Erlass eines Rechtsaktes EU-Vorgaben umsetzen oder aufgrund von EU-Recht Verwaltungstätigkeiten vornehmen.¹⁶ Da es hier um einen Sekundärrechtsakt der EU, also das Handeln von EU-Organen, geht, kann die Prüfung unproblematisch am Maßstab der Grundrechtecharta erfolgen.

Die Grundrechtecharta ist in vielen Bereichen der Europäischen Menschenrechtskonvention (EMRK) nachgebildet. Nicht nur entsprechen viele Grundrechte der Charta im Wortlaut den von der EMRK gewährten Rechten, sondern nach dem Willen der Charta soll die EMRK einschließlich der Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte (EGMR) Auslegungshilfe für die Grundrechte der Charta sein, die auf die EMRK zurückgehen (Art. 52 Abs. 3 GRCh).

3. Eingriffe in Grundrechte der Charta

In Betracht kommt eine Verletzung der Rechte aus Art. 7, Art. 8 und Art. 15 und 16 GRCh.

3.1. Achtung des Privat- und Familienlebens (Art. 7 GRCh)

Die Richtlinie könnte insbesondere gegen das Recht auf Achtung des Privatlebens und der Kommunikation aus Art. 7 GRCh verstoßen. Recht auf Achtung bedeutet, dass der Staat einerseits Eingriffe zu unterlassen und andererseits den Schutz sicherzustellen hat.¹⁷

3.1.1. Schutzbereich

In den **Schutzbereich** des Grundrechts fällt sowohl das Privatleben als auch die Kommunikation. Das **Privatleben** erfasst allgemein die freie Entwicklung der Persönlichkeit¹⁸ sowie den Schutz

14 Siehe hierzu die Zusammenfassung der Diskussion im Konvent bei Borowsky, in: Meyer, Jürgen (Hrsg.), Charta der Grundrechte der Europäischen Union, Art. 51, Rn. 2 ff.

15 Borowsky, in: Meyer, Jürgen (Hrsg.), Charta der Grundrechte der Europäischen Union, Art. 51, Rn.24.

16 Jarass, Charta der Grundrechte der Europäischen Union, Art. 51, Rn. 16.

17 Bernsdorff, Norbert, in: Meyer, Jürgen (Hrsg.), Kommentar zur Charta der Grundrechte der Europäischen Union, 3. Auflage, Baden-Baden 2010, Art. 7 GRCh, Rn. 16.

der Privatsphäre¹⁹, die äußere Beziehung zu anderen Menschen²⁰ und die Bewegung im öffentlichen Raum, ohne vom Staat dabei überwacht zu werden²¹. Im Bereich der **Kommunikation** soll das Vertrauen des Bürgers geschützt werden, dass auch bei der Übertragung von Informationen über eine Distanz der zwischenmenschliche Austausch frei von Überwachung ist.²² Erfasst werden jedenfalls die modernen Kommunikationsformen, wie Telefon, E-Mail und Internettelefonie.²³

3.1.2. Eingriff

Ein **Eingriff** liegt beispielsweise vor, wenn Gesprächsdaten überwacht werden²⁴ oder, anhand dieser Daten oder durch Überwachung der Person, ein Bewegungsprofil erstellt wird.²⁵ Grundsätzlich schützt das Grundrecht nur gegen Eingriffe von Trägern öffentlicher Gewalt. Der EGMR hat aber aus der Schutzpflicht des Rechts die Verpflichtung eines Staates begründet, auch im Verhältnis von Privatpersonen untereinander Schutz zu gewähren.²⁶

Hier setzt der Staat durch die Verpflichtung der Telekommunikationsdienstleister eine unmittelbare Ursache dafür, dass Daten gespeichert werden. Ihm ist folglich das Verhalten der Unternehmen zurechenbar.

Es sind nach Art. 5 RL 2006/24/EG die Daten zu speichern, aus denen sich ergibt, von welchem Anschluss aus zu welchem Anschluss wann und wie lange telekommuniziert wurde. Dies umfasst:

-
- 18 Grabenwarter, Christoph, Europäische Menschenrechtskonvention, 4. Auflage, München 2009, S. 199; Schorkopf, Frank, in: Ehlers, Dirk (Hrsg.), Europäische Grundrechte und Grundfreiheiten, 3. Auflage, Berlin 2009, S. 512.
- 19 Grabenwarter, Christoph, Europäische Menschenrechtskonvention, 4. Auflage, München 2009, S. 201.
- 20 EGMR, 16.12.1992, Niemitz ./.. Deutschland, Rn. 29.
- 21 Dies sei bei der Überwachung des öffentlichen Raumes durch Kameras nicht auszuschließen, so EGMR, 28.01.2003, Peck ./.. Vereinigtes Königreich, Rn. 59. Siehe auch Schorkopf, Frank, in: Ehlers, Dirk (Hrsg.), Europäische Grundrechte und Grundfreiheiten, 3. Auflage, Berlin 2009, S. 512.
- 22 Schorkopf, Frank, in: Ehlers, Dirk (Hrsg.), Europäische Grundrechte und Grundfreiheiten, 3. Auflage, Berlin 2009, S. 514.
- 23 Grabenwarter, Christoph, Europäische Menschenrechtskonvention, 4. Auflage, München 2009, S. 209 mit Nachweisen auf die einschlägige Rechtsprechung des EGMR.
- 24 EGMR, 25.09.2001, P.G. und J.H. ./.. Vereinigtes Königreich, Rn. 42; Grabenwarter, Christoph, Europäische Menschenrechtskonvention, 4. Auflage, München 2009, S. 214.
- 25 Schorkopf, Frank, in: Ehlers, Dirk (Hrsg.), Europäische Grundrechte und Grundfreiheiten, 3. Auflage, Berlin 2009, S. 512.
- 26 Bernsdorff, Norbert, in: Meyer, Jürgen (Hrsg.), Kommentar zur Charta der Grundrechte der Europäischen Union, 3. Auflage, Baden-Baden 2010, Art. 7 GRCh, Rn. 17; Schorkopf, Frank, in: Ehlers, Dirk (Hrsg.), Europäische Grundrechte und Grundfreiheiten, 3. Auflage, Berlin 2009, S. 515.

- die genutzten Rufnummern und Kennungen,
- die Uhrzeit von Beginn und Ende der Verbindung,
- das Datum der Verbindungen,
- Angaben zu dem genutzten Dienst,
- bei der Mobilfunktelefonie die angewählte Funkzelle bei Beginn der Mobilfunkverbindung,
- die Internetprotokoll-Adresse (IP-Adresse) bei Internet-Kommunikation,
- den Zeitpunkt des Eingangs einer Nachricht und des Zugriffs auf ein elektronisches Postfach.

Die Pflicht zur Speicherung besteht auch dann, wenn ein Anruf unbeantwortet bleibt.

Zwar wird nicht unmittelbar in die Übermittlung der Nachricht eingegriffen, es besteht jedoch die Gefahr, dass die Bewegung der Person im öffentlichen Raum oder deren Gewohnheiten nachvollzogen werden kann, da bei Mobilkommunikation die Funkzellen bei Beginn und während der Kommunikation vermerkt werden. Auch ist möglich zu verfolgen, wer wann welche Person mit welchem Kommunikationsmittel kontaktiert. Zwar ist nach Art. 5 Abs. 2 RL 2006/24/EG verboten, Daten zu speichern, die Aufschluss über den Inhalt der Kommunikation geben können; anhand der Rahmendaten der Kommunikation ist aber die Erstellung eines Profils der Kommunikationsgewohnheiten einer Person möglich, das gewisse Teile des Privatlebens und der privaten Kommunikation dem vom Staat verpflichteten Unternehmen offen darlegt. Eine Person könnte durch dieses Wissen um die Speicherung der Daten und die Angst, dass dadurch seine Lebensweise überwacht wird, die Nutzung der Kommunikationsmittel einschränken. Ein Eingriff in den Schutzbereich des Art. 7 GRCh in seiner Gesamtschau ist daher zumindest mittelbar²⁷ zu bejahen.²⁸

3.2. Schutz personenbezogener Daten (Art. 8 GRCh)

Die RL 2006/24/EG berührt in jedem Fall das Recht auf Schutz personenbezogener Daten aus Art. 8 GRCh. Dieses Grundrecht beruht auf dem jetzigen Art. 16 AEUV (Art. 286 EGV a.F.),²⁹ der die EU-Organe und die Mitgliedstaaten bei der Ausführung von Tätigkeiten der EU auf den Datenschutz verpflichtet. Eine sekundärrechtliche Ausprägung hat das Recht in den Datenschutz-

27 Der EuGH erkennt auch nicht-finale Eingriffe in Rechte des Bürgers an: T-113/96, 29.01.1998, Rn. 75; C-84/95, 30.07.1996, Rn. 22 f.

28 Rusteberg, Benjamin, Die EG-Richtlinie zur Vorratsspeicherung von Verkehrsdaten im System des europäischen Grund- und Menschenrechtsschutzes, in: Verwaltungsblätter für Baden-Württemberg (VBlBW) 2007, S. 171 (S. 176); Klug, Christoph/Reif, Yvette, Vorratsdatenspeicherung in Unternehmen? – Gesetzeslage und Ausblick, in: Recht der Datenverarbeitung (RDV) 2008, S. 89 (S. 92); Kleszczewski, Diethelm, Kritik der Vorratsdatenspeicherung, in: Weßlau, Edda/Wohlers, Wolfgang (Hrsg.), Festschrift für Gerhard Fezer zum 70. Geburtstag, Berlin 2008, S. 19 (S. 24).

29 Bernsdorff, Norbert, in: Meyer, Jürgen (Hrsg.), Kommentar zur Charta der Grundrechte der Europäischen Union, 3. Auflage, Baden-Baden 2010, Art. 8 GRCh, Rn. 2; siehe auch die (nicht verbindlichen) Erläuterungen zur Charta der Grundrechte durch das Präsidium des Konvents, hier zu Art. 8 GRCh.

richtlinien, insbesondere die Richtlinie 95/46/EG³⁰, erfahren. Der Umfang des Grundrechts wird also durch das Gemeinschaftsrecht konkretisiert.³¹

3.2.1. Schutzbereich

Die RL 95/46/EG definiert personenbezogene Daten als alle Informationen über bestimmte oder bestimmbare natürliche Personen (Art. 2 lit. a RL 95/46/EG). Art. 5 RL 2006/24/EG verlangt insbesondere die Speicherung der Adressen und Namen sowie spezifischer Kennnummern (IP-Adresse, IMSI, IMEI) des Anrufers und der angerufenen Person.

3.2.2. Eingriff

Diese Daten dürfen nur unter den in Art. 8 Abs. 2 S. 1 GRCh genannten Voraussetzungen verarbeitet werden. Wiederum kann auf die Definition in Art. 2 lit. b RL 95/46/EG zurückgegriffen werden:³² Die **Verarbeitung** erfasst die gesamte Verwendung der Daten wie „das Erheben, das Speichern, die Organisation, die Aufbewahrung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Benutzung, die Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung“.

Da die RL 2006/24/EG sowohl die Erhebung und Speicherung der oben genannten Daten (Art. 3 RL 2006/24/EG) als auch deren Übermittlung an die zuständigen nationalen Behörden (Art. 4 RL 2006/24/EG) vorsieht, wird unproblematisch in den Schutzbereich von Art. 8 GRCh eingegriffen.³³

3.3. Berufs- und wirtschaftliche Betätigungsfreiheit (Art. 15 und 16 GRCh)

Die RL 2006/24/EG kann schließlich auch den gemeinschaftsrechtlichen Grundsatz der berufs- und wirtschaftlichen Betätigungsfreiheit berühren. Der EuGH erkennt in ständiger Rechtsprechung die Berufsfreiheit als „allgemeinen Grundsatz des Gemeinschaftsrechts an“.³⁴ Die **Berufsfreiheit in Art. 15 und die Unternehmerfreiheit in Art. 16 GRCh** gewährleisten sowohl die

30 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

31 Bernsdorff, Norbert, in: Meyer, Jürgen (Hrsg.), Kommentar zur Charta der Grundrechte der Europäischen Union, 3. Auflage, Baden-Baden 2010, Art. 8 GRCh, Rn. 14; Schorkopf, Frank, in: Ehlers, Dirk (Hrsg.), Europäische Grundrechte und Grundfreiheiten, 3. Auflage, Berlin 2009, S. 520. So auch die Erläuterungen des Präsidiums des Konvents.

32 Schorkopf, Frank, in: Ehlers, Dirk (Hrsg.), Europäische Grundrechte und Grundfreiheiten, 3. Auflage, Berlin 2009, S. 521; Bernsdorff, Norbert, in: Meyer, Jürgen (Hrsg.), Kommentar zur Charta der Grundrechte der Europäischen Union, 3. Auflage, Baden-Baden 2010, Art. 8 GRCh, Rn. 16.

33 Schorkopf spricht in diesem Zusammenhang von einer „bemerkenswerte(n) Beeinträchtigung des Grundrechts“, Schorkopf, Frank, in: Ehlers, Dirk (Hrsg.), Europäische Grundrechte und Grundfreiheiten, 3. Auflage, Berlin 2009, S. 521.

34 EuGH, Rs. 4/73, „Nold“, Slg. 1974, 491 ff.; EuGH, Rs. 44/79, „Hauer“, Slg. 1979, 3727 ff.; EuGH, Rs. C-280/93, „Deutschland/Rat“, Slg. 1994, I-4973 Tz. 78 ff.; EuGH, Rs. C-122/95 „Deutschland/Rat“, Slg. 1998, I-973 Tz. 74 ff.; EuGH, Rs. C-210/03, „Swedish Match AB/Secretary of State for Health“, Slg. 2004, I-11893 Tz. 72 ff.

selbständige als auch die unselbständige berufliche Tätigkeit im Sinne einer **umfassenden wirtschaftlichen Betätigungsfreiheit**.³⁵

3.3.1. Schutzbereich

Zunächst müsste die in der Richtlinie enthaltene Verpflichtung der Telekommunikationsunternehmen zur anlasslosen Speicherung von Telekommunikationsdaten in den **Schutzbereich** der wirtschaftlichen Betätigungsfreiheit fallen. Dies ist der Fall, wenn das Grundrecht sowohl in sachlicher als auch in persönlicher Hinsicht auf den vorliegenden Sachverhalt Anwendung findet.

3.3.1.1. sachlicher Anwendungsbereich

Der Begriff der wirtschaftlichen Betätigungsfreiheit wurde in der Rechtsprechung des EuGH bislang nicht eindeutig definiert. Aus den Erläuterungen des Präsidiums des Grundrechtekonvents ergibt sich jedoch, dass die unternehmerische Freiheit im Wesentlichen als Ausprägung der Berufsfreiheit zu verstehen ist.³⁶ Daher umfasst der Gewährleistungsbereich des Gemeinschaftsgrundrechts **jede Wirtschafts- oder Geschäftstätigkeit eines Unternehmens, mithin jede dem Erwerb dienende Tätigkeit, die auf Dauer angelegt ist**.³⁷

Da die Verpflichtung zur Vorratsdatenspeicherung **Einfluss auf die Speicherfristen der Telekommunikationsdaten** hat und die **Schaffung einer entsprechenden Infrastruktur** voraussetzt, ist der sachliche Anwendungsbereich vorliegend betroffen.³⁸

3.3.1.2. persönlicher Anwendungsbereich

Träger des Grundrechts sind alle natürlichen und juristische Personen, sowie Personenvereinigungen.³⁹ Die **europäischen Telekommunikationsunternehmen** gehören somit als potentielle Adressaten der RL 2006/24/EG zum geschützten Personenkreis des Art. 16 GRCh.

35 Ruffert, Matthias, in: Calliess, Christan/Ruffert, Matthias, Das Verfassungsrecht der Europäischen Union, 3. Auflage 2007, Art. 15 GRCh, Rn. 4 mit Hinweis auf EuGH, Verb. Rs. 63/84 und 147/84, Slg. 1985, 2857, Rn. 23 (Finsider).

36 Bernsdorff, Norbert, in: Meyer, Charta der Grundrechte der Europäischen Union, 3. Auflage 2011, Art. 16 GRCh, Rn. 1.

37 Vgl. Jarass, Hans, EU-Grundrechte, § 21 Rn. 6; Ruffert, Matthias, in: Ehlers, Dirk (Hrsg.), Europäische Grundrechte und Grundfreiheiten, § 16 Rn. 11.

38 Vgl. Vollmar, Tino J., Telefonüberwachung im Polizeirecht, Frankfurt a.M. 2008, S. 191.

39 Jarass, Hans, in: ders., Charta der Grundrechte der Europäischen Union, München 2010, Art. 16 GRCh, Rn. 11 mit dem Hinweis darauf, dass die Rechtslage bei öffentlichen Unternehmen, deren Anteile von Grundrechtsverpflichteten gehalten werden, umstritten ist.

3.3.2. Eingriff

Ein Grundrechtseingriff und damit eine Grundrechtseinschränkung liegt zunächst vor, wenn ein Grundrechtsverpflichteter eine Regelung trifft, die für den Grundrechtsinhaber im Hinblick auf die unternehmerischen Aktivitäten einen **Nachteil bezweckt oder unmittelbar bewirkt**.⁴⁰ Eine derartige unmittelbare Bewirkung kommt hier indes nicht in Betracht. Möglich erscheint aber eine **mittelbare, bzw. faktische Auswirkung** des Rechtsaktes; dies ist, vergleichbar mit dem modernen Eingriffsbegriff des deutschen Rechts, auf europäischer Ebene ebenfalls anerkannt.⁴¹ Dies ist hier der Fall. Durch die Vorgaben der RL 2006/24/EG wird der **Grundrechtsschutz** insofern **zurechenbar verkürzt**, als dass die Telekommunikationsunternehmen über ihren Eigenbedarf hinaus zur Speicherung der Nutzerdaten verpflichtet werden.

Allerdings kann nicht bereits jede Auferlegung einer Verhaltenspflicht einen Eingriff im o.g. Sinne darstellen. So sind zum Beispiel **allgemeine kaufmännische Interessen und Gewinnerwartungen** der Marktteilnehmer **nicht grundrechtlich geschützt**, jedenfalls sofern ihre Ungewissheit zum Wesen der wirtschaftlichen Betätigung gehört.⁴² Folglich wird dem Grundrechtsträger kein bestimmtes Geschäftsvolumen garantiert.

Die RL 2006/24/EG sieht in Art. 3 eine allgemeine Vorratsspeicherungspflicht vor; die **Kategorien der zu speichernden Daten** bestimmt Art. 5. Zu speichernde Daten sind danach Bestands- und Verkehrsdaten.

Bestandsdaten sind Daten eines Teilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden.⁴³ Dazu gehören etwa Name, Anschrift, Bankverbindung, die an den Kunden vergebene Anschlussnummer, eine fest an den Kunden vergebene statische IP-Adresse.

Im Gegensatz zu den gleichbleibenden Bestandsdaten sind die **Verkehrsdaten** Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden. Verkehrsdaten lassen erkennen, von welchem Anschluss wann mit wem wie lange kommuniziert wurde.⁴⁴ Dazu gehören Protokolle darüber, wer mit wem per Telefon, Handy oder E-Mail in Verbindung gestanden oder das Internet genutzt hat. Wann welcher Kunde online war und welche dynamische IP-Adresse ihm dabei zugewiesen war, ist ebenfalls eine Angabe über die näheren Umstände des Telekommunikationsverhaltens.

Die Verpflichtung zur Speicherung dieser Daten erstreckt sich dabei auf eine mindestens **sechsmonatige bis maximal zweijährige Speicherungspflicht** (Art. 6), wobei, wenn besondere

40 Jarass, Hans, in: ders., Charta der Grundrechte der Europäischen Union, München 2010, Art. 16 GRCh, Rn. 12 mit Hinweis auf EuGH, Rs. 200/96, Slg. 1998, I-1953 Rn. 28.

41 So z. B. EuGH, Rs. T-113/96 „Dubois et fils/Rat und Kommission“, Slg. 1998, II-125, Rn. 75; Rs. C-84/95 „Bosphorus“, Slg. 1996, I-3953, Rn. 22 f.

42 EuGH, Rs. C-104/97, „Atlanta“, Slg. 1999, I-6983 Tz. 12.

43 Büttgen, Peter, in: Beck'scher TKG-Kommentar, Bonn 2006, 3. Auflage, § 95 Rn 2.

44 Fezer, Karl-Heinz, in: ders., Markenrecht, München 2009, 4. Auflage, § 19 Rn 79.

Umstände vorliegen, auch eine längere Speicherung im Einzelfall gerechtfertigt sein kann (Art. 12 RL 2006/24/EG).

Aus den genannten Vorschriften ergibt sich, dass die Speicherungspflicht über die für die reine Entgeltabrechnung – als Eigenbedarf der Unternehmen – notwendigen Daten hinausgeht. Folge dessen ist ein **erhöhter Verwaltungsaufwand**, denn die Telekommunikationsunternehmen müssen die hierfür erforderliche **Infrastruktur anschaffen und bereithalten**. Sie werden mithin direkt aufgrund der Vorgaben der RL 2006/24/EG zu einem kostenintensiven Verhalten veranlasst.⁴⁵

3.3.3. Zwischenergebnis

Die Regelungen der RL 2006/24/EG führen bei den Telekommunikationsanbietern zu einem verwaltungs- und kostenrechtlichen Mehraufwand. In der Pflicht zur Speicherung der Daten kann somit eine **mittelbare Verkürzung des Schutzbereichs** gesehen werden. Damit ist das Vorliegen eines Eingriffs in das Grundrecht der wirtschaftlichen Betätigungsfreiheit zu bejahen.

4. Rechtfertigung der Eingriffe

4.1. Möglichkeit der Rechtfertigung

Die Grundrechte der Charta enthalten zwar nur in wenigen Fällen Rechtfertigungstatbestände für Eingriffe, sie sind aber bis auf wenige Ausnahmen (beispielsweise der Schutz der Menschenwürde in Art. 1 GRCh) nicht schrankenlos gewährt. Vielmehr findet sich die **allgemeine Schrankenbestimmung in Art. 52 GRCh**. Art. 52 GRCh enthält drei Einschränkungsklauseln: Die Verweisung auf die EMRK in Abs. 3 bewirkt, dass die Rechte der Charta, die der EMRK entlehnt sind, nur in dem Umfang gewährt werden, den ihnen die EMRK einräumt. Ähnlich sieht Abs. 2 vor, dass die Rechte, die den Verträgen entstammen, deren Grenzen unterliegen. Abs. 1 schließlich ist die Auffangvorschrift, die für alle anderen Rechte gilt.⁴⁶

Da Art. 7 GRCh auf Art. 8 EMRK zurückgeht, ist gemäß Art. 52 Abs. 3 GRCh die Schrankenbestimmung des Art. 8 Abs. 2 EMRK anwendbar.⁴⁷ Eine Rechtfertigung des Eingriffs kommt also in Betracht, wenn er gesetzlich vorgesehen ist und u. a. für die nationale oder öffentliche Sicherheit und zur Verhütung von Straftaten notwendig ist. Mit Blick auf den Schutz des Privatlebens hat der EuGH das Grundrecht „Beschränkungen unterworfen (...), sofern diese Beschränkungen tatsächlich dem Gemeinwohl dienenden Zielen der Gemeinschaft entsprechen und nicht einen im

45 Vgl. Vollmar, Tino J., Telefonüberwachung im Polizeirecht, Frankfurt a.M. 2008, S. 192.

46 Borowsky, Martin, in: Meyer, Jürgen (Hrsg.), Kommentar zur Charta der Grundrechte der Europäischen Union, 3. Auflage, Baden-Baden 2010, Art. 52 GRCh, Rn.13 ff.

47 Siehe die (nicht verbindlichen) Erläuterungen zur Charta der Grundrechte durch das Präsidium des Konvents, hier zu Art. 7 GRCh.

Hinblick auf den verfolgten Zweck unverhältnismäßigen, nicht tragbaren Eingriff darstellen, der die so gewährleisteten Rechte in ihrem Wesensgehalt antastet“.⁴⁸

Im Gegensatz zu Art. 7 GRCh gibt es in der EMRK keinen Art. 8 GRCh entsprechenden Artikel.⁴⁹ Daher findet nicht Art. 52 Abs. 3 GRCh, sondern der allgemeine Rechtfertigungstatbestand des Art. 52 Abs. 1 GRCh Anwendung.⁵⁰ Zusätzlich enthält Art. 8 Abs. 2 S. 1 GRCh eine eigene Grundrechtsschranke, indem er die Verarbeitung „nach Treu und Glauben für festgelegte Zwecke (...) auf einer sonstigen gesetzlich geregelten legitimen Grundlage“ erlaubt. Unklar ist, unter welchen Voraussetzungen nach einer jüngeren Entscheidung des EuGH⁵¹ ein Eingriff in Art. 8 GRCh durch eine **Einwilligung der betroffenen Grundrechtsträger** gerechtfertigt werden könnte⁵². Eine Einwilligung in die Verarbeitung personenbezogener Daten dürfte ausgehend vom Stand der Literatur als Rechtfertigungsgrund eine Zustimmung des Betroffenen in Kenntnis der Sachlage erfordern⁵³. Klärungsbedürftig wäre in diesem Zusammenhang, ob diesem Maßstab die Einholung einer vorformulierten Einverständniserklärung des Grundrechtsträgers bereits genüge und ob eine Rechtfertigung die Freiwilligkeit einer entsprechenden Erklärung voraussetzt⁵⁴. Die RL 95/46/EG kann fernerhin nicht als Schranke eines Grundrechts herangezogen werden, sie kann jedoch als Auslegungshilfe dienen.⁵⁵

Eingriffe und Einschränkungen der wirtschaftlichen Betätigungsfreiheit sind nach Art. 52 Abs. 1 GRCh möglich.⁵⁶

Die RL 2006/24/EG stellt zunächst als Unionsrechtsakt eine **taugliche Grundrechtsschranke** dar. Dabei muss die jeweilige Rechtsvorschrift, hier die RL 2006/24/EG, ausreichend bestimmt, also

48 EuGH, C-62/90, 08.04.1992, Rn. 23.

49 Allerdings hat der EGMR schon früh das Recht auf Datenschutz in den Schutz des Privatlebens aus Art. 8 EMRK hineingelesen.

50 Schorkopf, Frank, in: Ehlers, Dirk (Hrsg.), Europäische Grundrechte und Grundfreiheiten, 3. Auflage, Berlin 2009, S. 521.

51 EuGH, 9.11.2009, C-92/09

52 kritisch hierzu Brink/Wolff, JZ 2011, S. 206 (207); Art. 8 erlaubt die Verarbeitung personenbezogener Daten nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person. Der EuGH verweist in seiner Entscheidung vom 9.11.2010, C-92/09, darauf, dass „Unionsrechtsvorschriften, die lediglich vorsehen, dass die Mittlempfänger vorab über die Veröffentlichung ihrer Daten unterrichtet werden, ... die mit ihnen eingeführte Verarbeitung personenbezogener Daten nicht auf die Einwilligung der betroffenen Empfänger“ stützen.

53 Bernsdorff, Norbert, in: Meyer, Jürgen (Hrsg.), Kommentar zur Charta der Grundrechte der Europäischen Union, 3. Auflage, Baden-Baden 2010, Art. 8 GRCh, Rn. 21.

54 vgl. zu dieser Frage die Schlussanträge der Generalanwältin Sharpsson vom 17.06.2010 in der Rs. C-92/09; der EuGH folgert allerdings nicht aus dem Fehlen von freiwilliger Angaben zu personenbezogenen Daten die prinzipielle Umwirksamkeit einer Einwilligung i.S.d. Art. 8 Abs. 2 GRCh.

55 Dazu näher EuGH, 9.11.2010, C-92/09; Schorkopf, Frank, in: Ehlers, Dirk (Hrsg.), Europäische Grundrechte und Grundfreiheiten, 3. Auflage, Berlin 2009, S. 521.

56 Erläuterungen zur Charta der Grundrechte durch das Präsidium des Konvents, Art. 16 GRCh.

hinreichend genau formuliert sein. In diesem Zusammenhang wird kritisiert, dass insbesondere Art. 4 RL 2006/24/EG (Zugang zu Daten) zu unpräzise sei.⁵⁷ Es werde nicht ausgeführt, wer die „zuständigen nationalen Behörden“ seien. Die Kritik richtet sich aber hauptsächlich dagegen, dass durch diese Unbestimmtheit das Ziel der europaweiten Harmonisierung der Datenspeicherung kaum erreicht werden könne. Darüber hinaus darf nicht außer Acht gelassen werden, dass es sich bei dem Rechtsakt um eine Richtlinie handelt, die den Mitgliedstaaten zur Umsetzung einen Gestaltungsspielraum überlassen will und muss. Wie in den Erwägungspunkten an mehreren Stellen (beispielsweise Punkte 9, 17, 18) betont wird, soll die Richtlinie im Einklang mit den innerstaatlichen Rechtsvorschriften und den Grundrechten erfolgen. Je genauer aber die Vorgaben der Richtlinie sind, desto schwieriger und „gefährlicher“ gestaltet sich die Implementierung des Inhalts in das nationale Recht.

4.2. Verhältnismäßigkeit

Das bloße Vorliegen eines einschränkenden Gesetzes genügt dem Schrankenvorbehalt jedoch nicht. Wie die oben dargelegten Schrankenbestimmungen der betroffenen Grundrechte zeigen, muss das beschränkende Gesetz bestimmte inhaltliche Anforderungen erfüllen. Die Richtlinie muss insbesondere verhältnismäßig, also zur Erreichung eines legitimen Zwecks **geeignet, erforderlich und angemessen**, d.h. verhältnismäßig im engeren Sinne, sein und den **Wesensgehalt** der Grundrechte achten.

Der EuGH hatte jüngst in einer Grundsatzentscheidung zum europäischen Datenschutzrecht die Frage zu klären, ob eine im europäischen Sekundärrecht vorgesehene Veröffentlichungspflicht von Informationen über die Empfänger von Mitteln aus dem Europäischen Garantiefonds für die Landwirtschaft für die Entwicklung des ländlichen Raums mit der GRCh vereinbar ist⁵⁸. Diese Entscheidung wird in der folgenden Prüfung berücksichtigt.

4.2.1. legitimes Ziel

Als Ziel der RL 2006/24/EG wird in den Erwägungspunkten 4 und 9 die **Aufrechterhaltung der öffentlichen Ordnung**, die Verhütung, Ermittlung, Feststellung und **Verfolgung von Straftaten**, sowie der Schutz der Rechte und Freiheiten anderer genannt. Dies sind berechnete, da dem Gemeinwohl dienende Ziele, die auch dem Erfordernis des Art. 8 Abs. 2 EMRK genügen dürften.

4.2.2. Geeignetheit des Eingriffs

Der Eingriff in Form der Vorratsdatenspeicherungspflicht müsste des Weiteren geeignet sein, dieses legitime Ziel zumindest zu fördern. Maßgeblich ist insoweit die **abstrakte Eignung**.⁵⁹

57 Westphal, Dieter, Die Richtlinie zur Vorratsspeicherung von Verkehrsdaten – Brüsseler Stellungnahme zum Verhältnis von Freiheit und Sicherheit in der „Post-911-Informationsgesellschaft“, in: EuR 2006, S. 706 (S. 716).

58 EuGH, 9.11.2010, C-92/09

59 Inwiefern die Richtlinie konkrete Erfolge erzielt hat, kann an dieser Stelle nicht beurteilt werden. Dazu hätte die Kommission dem Europäischen Parlament und dem Rat spätestens am 15. September 2010 eine Bewertung der Anwendung dieser Richtlinie vorlegen müssen. Dies ist bislang nicht erfolgt.

Unter Außerachtlassung der technischen Einzelheiten, inwiefern die Erhebung der Daten im vorgesehenen Umfang möglich ist, erscheint dieses Mittel abstrakt geeignet, das beabsichtigte Ziel zu fördern. Es wird vorgebracht, dass Kriminelle oder Terroristen im Einzelfall in der Lage sind, durch verschiedene **technische Maßnahmen die Verfolgbarkeit ihrer Daten zu unterbinden**.⁶⁰ Im Bereich der Festnetz-, aber auch der Mobiltelefonie genügt etwa die Verwendung von öffentlichen Telefonzellen oder Wertkartenhandys bzw. von im (nicht EU-) Ausland angemeldeten Handys, um der Datenaufzeichnung mit der Möglichkeit der Rückführung auf die konkrete Person zu entgehen. Eine ähnliche Möglichkeit besteht auch bei der Kommunikation über das Internet, denn die Aufzeichnung von E-Mail-Daten kann durch die Verwendung außereuropäischer E-Mail-Provider umgangen werden.⁶¹ Diese Überlegungen wären allerdings Betrachtungen im konkreten Einzelfall, die für das Kriterium der Geeignetheit des Eingriffs nicht von Bedeutung sind.⁶²

Im Ergebnis ist daher unter Beachtung der **Einschätzungsprärogative des Richtliniengebers** davon auszugehen, dass die Vorratsdatenspeicherung generell geeignet ist, die o.g. Ziele⁶³ zu erreichen.

4.2.3. Erforderlichkeit des Eingriffs

Die Regelung zur Vorratsdatenspeicherung ist **erforderlich**, wenn es keine alternativen Maßnahmen gibt, mit denen das verfolgte Ziel ebenso gut erreicht werden kann und die in geringerem Umfang in Grundrechte eingreifen.⁶⁴ Der EuGH hat dies jüngst dahingehend präzisiert, „dass sich Ausnahmen und Einschränkungen in Bezug auf den Schutz der personenbezogenen Daten auf das absolut Notwendige beschränken müssen“. Der Grundsatz der Verhältnismäßigkeit ist nach dieser Entscheidung verletzt, soweit Maßnahmen vorstellbar sind, die das Grundrecht aus Art. 7 und 8 GRCh weniger stark beeinträchtigen, den Zielen der diese Grundrechte beeinträchtigen Unionsvorschriften jedoch in ebenso wirksamer Weise dienen.⁶⁵

60 Siehe die Nachweise bei Rusteberg, Benjamin, Die EG-Richtlinie zur Vorratsspeicherung von Verkehrsdaten im System des europäischen Grund- und Menschenrechtsschutzes, in: VBlBW 2007, S. 171 (S. 175); Klug, Christoph/Reif, Yvette, Vorratsdatenspeicherung in Unternehmen? – Gesetzeslage und Ausblick, in: RDV 2008, S. 89 (S. 92).

61 Rechtsvergleichende Analyse im Hinblick auf die Umsetzung der Richtlinie 2006/24/EG über die Vorratsdatenspeicherung im Auftrag des Bundesministeriums für Verkehr, Innovation und Technologie vorgelegt vom Ludwig Boltzmann Institut für Menschenrechte (BIM) in Kooperation mit dem Institut für Rechtsinformatik der Leibniz Universität Hannover (IRI), Österreich, Stand: 10. März 2008, online abrufbar unter http://www.bim.lbg.ac.at/files/sites/bim/Rechtsvergleich_Vorratsdatenspeicherung.pdf, zuletzt abgerufen am 03.02.2011.

62 Jarass, Hans, in: ders., Charta der Grundrechte der Europäischen Union, München 2010, Art. 52 GRCh, Rn. 37: „Dabei genügt es, wenn das angestrebte Ziel gefördert wird.“

63 Siehe Art. 4-11 der RL 2006/24/EG.

64 Jarass, Hans, in: ders., Charta der Grundrechte der Europäischen Union, München 2010, Art. 52 GRCh, Rn. 38.

65 EuGH, 9.11.2010, C-92/09

Als milderes Mittel käme das „**Quick-freeze-Verfahren**“⁶⁶ in Betracht: Bei diesem Verfahren werden im Normalfall die Daten, die das Telekommunikationsunternehmen zu Abrechnungszwecken erhoben hat, nach Gebrauch gelöscht. Besteht nun ein **Anfangsverdacht** gegen eine Person, so können die zuständigen Strafverfolgungsbehörden eine Speicheranordnung treffen, aufgrund derer die Daten nicht gelöscht, sondern **vorübergehend eingefroren** bzw. aufbewahrt werden („freeze“). Sobald der entsprechende **richterliche Beschluss** vorliegt, ist die Nutzung der Daten erlaubt, sie werden wieder aufgetaut („thaw“) und der Strafverfolgungsbehörde ausgehändigt. Diese Methode wird auch als „quick freeze, fast thaw“ bezeichnet.

Diese Methode ist weniger einschneidend als die in RL 2006/24/EG vorgesehene anlasslose Vorratsdatenspeicherung, da zur dauerhaften Speicherung bereits ein Anfangsverdacht gegen die Person, deren Daten eingesehen werden sollen, vorliegen muss. Folglich wäre ein milderes Mittel vorhanden. Ob dies allerdings **ebenso effektiv** wäre wie eine anlasslose Vorratsdatenspeicherung, kann bezweifelt werden. Denkbar ist durchaus, dass in einem Fall der Anfangsverdacht nicht gegeben ist und die Daten deshalb routinemäßig gelöscht werden und somit für die Strafverfolgungsbehörden verloren gehen. So wird beispielsweise vorgebracht, dass in Deutschland aufgrund des allgemein strengen Datenschutzes das „Quick-freeze-Verfahren“ leerlaufen würde, da die Speicherung von Daten die Ausnahme sei und somit auch keine Daten eingefroren werden könnten.⁶⁷

Es kann hier keine abschließende Beurteilung stattfinden, ob neben der anlasslosen Datenspeicherung ein milderes, in gleicher Weise geeignetes Mittel existiert. Die Meinungen darüber, ob etwa das „Quick-freeze-Verfahren“ ein gleichwertiger Ersatz wäre, weichen erheblich voneinander ab.⁶⁸ Das Gutachten muss sich darauf beschränken, auf die Möglichkeit des „Quick-freeze-Verfahrens“ hinzuweisen.

Fraglich ist des Weiteren im Hinblick auf die wirtschaftliche Betätigungsfreiheit die **Erforderlichkeit** der in Art. 6 RL 2006/24/EG vorgesehenen **Speicherfrist von sechs Monaten bis zu zwei Jahren**. Möglich wäre zum Beispiel eine kürzere Frist von etwa einem bis drei Monaten. Auch dies würde ein milderes Mittel darstellen, da die Menge der zu speichernden Daten verringert würde. Ob eine derart kürzere Frist ebenso effektiv wäre, wie die in der RL 2006/24/EG vorgese-

66 Deutsch: „Schockfrost“.

67 Vgl. Hans-Peter Uhl (CSU) in einem Interview in der Frankfurter Rundschau vom 04.02.2011, S. 3.

68 Vgl. für die Geeignetheit des „Quick-freeze-Verfahrens“: Westphal, Dieter, Die Richtlinie zur Vorratsspeicherung von Verkehrsdaten – Brüsseler Stellungnahme zum Verhältnis von Freiheit und Sicherheit in der „Post-911-Informationsgesellschaft“, in: EuR 2006, S. 706 (S. 715); Klug, Christoph/Reif, Yvette, Vorratsdatenspeicherung in Unternehmen? – Gesetzeslage und Ausblick, in: Recht der Datenverarbeitung (RDV) 2008, S. 89 (S. 93); „nicht vollkommen gleichwertig“; Leutheusser-Schnarrenberger, Sabine, PlPr. 16/19, S. 1419; Art. 29 Datenschutzgruppe, Stellungnahme 4/2005 zum Vorschlag 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 (KOM(2005) 438 endg. vom 21.9.2005), 21.10.2005, S. 7, abrufbar unter: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp113_de.pdf (Stand: 04.02.2011). Kritisch z. B. Hartenbach, PlPr. 16/19, S. 1426; Uhl, Hans-Peter, Frankfurter Rundschau vom 04.02.2011, S. 3. Rusteberg sieht die Entscheidung gegen das „Quick-freeze-Verfahren“ als noch in den gesetzgeberischen Prognosespielraum fallend an (Rusteberg, Benjamin, Die EG-Richtlinie zur Vorratsspeicherung von Verkehrsdaten im System des europäischen Grund- und Menschenrechtsschutzes, in: VBIBW 2007, S. 171 (S. 175)).

hene Frist, kann an dieser Stelle mangels entsprechender Erkenntnisquellen nicht abschließend beurteilt werden. Insbesondere der Bericht der Kommission, dessen Erscheinen zum Jahreswechsel 2010/11 angekündigt wurde, dürfte hier künftig Aufschluss geben. Aus Analysen schwedischer und britischer Stellen aus dem Jahr 2005 ergibt sich jedenfalls, dass sich die Datenabfragen der Behörden zu 80-85% auf den Zeitraum der letzten drei Monate beziehen.⁶⁹ Die Erforderlichkeit der vorgesehenen Speicherfristen von sechs Monaten bis zwei Jahren kann daher bezweifelt werden.

4.3. Angemessenheit

Schließlich müssen die die Grundrechte berührenden Regelungen der Richtlinie im engeren Sinne verhältnismäßig, d.h. angemessen, sein. Hier müssen die betroffenen Interessen gegeneinander abgewogen werden.

Nicht von der Hand zu weisen ist die Grundrechtsrelevanz der RL 2006/24/EG. Die Gefahr, dass in erheblicher Weise insbesondere der private Kommunikationsbereich einer Person dem Staat offengelegt wird, besteht. Allerdings ist fraglich, ob diese Gefahr unmittelbar von der RL 2006/24/EG ausgeht, d. h. ob die in ihr enthaltenen Bestimmungen bereits in einem deutlichen Widerspruch zur Grundrechtecharta stehen.

Die RL 2006/24/EG schreibt den Mitgliedstaaten lediglich vor, dafür Sorge zu tragen, dass die in Art. 5 RL 2006/24/EG aufgezählten Daten gespeichert werden (Art. 3 Abs. 1 RL 2006/24/EG). Darüber hinaus sollen die Mitgliedstaaten Maßnahmen erlassen, um sicherzustellen, dass diese Daten „nur in bestimmten Fällen und in Übereinstimmung mit dem innerstaatlichen Recht an die zuständigen nationalen Behörden weitergegeben werden“ (Art. 4 RL 2006/24/EG). Schließlich wird für die Dauer der Speicherung auf Vorrat eine Frist von sechs Monaten bis zwei Jahren vorgegeben (Art. 6 RL 2006/24/EG).

Die Richtlinie beschränkt sich also auf die Anordnung der Speicherungspflicht und gibt im Übrigen den Mitgliedstaaten nur besondere Rahmenbedingungen vor. Sie regelt gerade nicht, wann und unter welchen Voraussetzungen die gespeicherten Daten wem zur Verfügung zu stellen sind. Vielmehr stellt sie Mindestanforderungen auf, welche die Mitgliedstaaten zum Schutz der Daten vor Missbrauch beachten müssen (beispielsweise Art. 7, 8, 9 RL 2006/24/EG). Des Weiteren wird betont, dass die Mitgliedstaaten im Anwendungsbereich der Richtlinie das Recht der EU – was die Grundrechtecharta einschließt – sowie die EMRK zu beachten haben (vgl. Art. 4 S. 2, Erwägungspunkte 9 und 17 RL 2006/24/EG). Es obliegt also den Mitgliedstaaten, darauf zu achten, dass sie die Umsetzung der RL 2006/24/EG grundrechtskonform gestalten. Hierzu hatte der EuGH im Jahr 2003 zu der RL 95/46/EG entschieden, dass die Mitgliedstaaten die Richtlinie so auslegen müssen, dass diese nicht gegen das Gemeinschaftsrecht oder die allgemeinen Grundsätze verstößt.⁷⁰ Diese „salvatorische Klausel“ zugunsten des Richtliniengebers geht allerdings fehl, wenn die Richtlinie eklatant gegen Grundrechte verstieße, so dass auch eine grundrechtskonforme Umsetzung nicht möglich wäre. Eine solche hält aber das BVerfG, auch wenn es in seinem Urteil

69 Büllingen, Franz, Vorratsspeicherung von Telekommunikationsdaten im internationalen Vergleich, in: Datenschutz und Datensicherheit 2005, S. 349 (S. 350).

70 EuGH, C-101/01, 06.11.2003, Rn. 87.

nicht die Richtlinie selbst, sondern nur das deutsche Umsetzungsgesetz auf seine Verfassungsmäßigkeit geprüft hat, ausdrücklich für möglich.⁷¹ Es hat die anlasslose Speicherung der Daten durch private Unternehmen (für eine Dauer von sechs Monaten) gerade nicht für grundrechtswidrig gehalten. Genau dies sind aber die Vorgaben, welche die RL 2006/24/EG für die Mitgliedstaaten verbindlich aufstellt.

Die einzelnen Punkte, die besonders grundrechtsrelevant sind, sind folgende:

Verwendung der Daten:

Art. 4 RL 2006/24/EG eröffnet den Staaten die Möglichkeit, auf die gespeicherten Daten zuzugreifen. Die Voraussetzungen sowie die Bestimmung der zugangsberechtigten Behörden werden den Mitgliedstaaten überlassen. Aus den Erwägungspunkten geht hervor, dass sie zur Verfolgung bzw. Verhütung von Straftaten, insbesondere der organisierten Kriminalität und des Terrorismus verwendet werden sollen (Erwägungspunkte 7, 9, 11). Dies darf aber nach dem Willen der Richtlinie nur im Einklang mit den Grundrechten geschehen (Art. 4 S. 2 RL 2006/24/EG).

Gespeicherte Daten:

Zwar untersagt die RL 2006/24/EG ausdrücklich, dass Daten gespeichert werden, die Aufschluss auf den Inhalt der Kommunikation geben (Art. 5 Abs. 2 RL 2006/24/EG). Es ist aber nicht auszuschließen, dass insbesondere durch die Speicherung der IP-Adresse auch ein Rückschluss auf den Kommunikationsinhalt möglich wird.⁷² In diesem Bereich sind die Anforderungen an die nationalen Umsetzungsmaßnahmen entsprechend hoch.

Dauer der Speicherung:

Problematisch erscheint hier insbesondere die Regelung in Art. 12 RL 2006/24/EG, der die Verlängerung der Speicherhöchstfrist von zwei Jahren um einen „begrenzten Zeitraum“ ermöglicht, wenn „besondere Umstände“ dies rechtfertigen. Der Mitgliedstaat entscheidet dies zwar autonom, die Kommission kann die Entscheidung jedoch ablehnen. Für sich genommen erscheint die Regelung wegen ihres vagen Wortlauts bedenklich; aber auch hier muss die Verpflichtung der Mitgliedstaaten auf die Grundrechte hineingelesen werden.

Kostenlast für die Dienstleister:

Im Hinblick auf den Eingriff in die wirtschaftliche Betätigungsfreiheit erscheint die entstehende Kostenlast für die Speicherung des Datenvolumens, die zunächst die Telekommunikationsunternehmen und letztlich über Gebührenerhöhungen auch den Nutzer treffen, problematisch.

Die Schätzungen betreffend der Höhe der Kosten variieren je nach Quelle zwischen **150 Millionen Euro**⁷³, **241,8 Millionen Euro**⁷⁴ oder gar **336 Millionen Euro**⁷⁵. Die Mehrbelastungen entstün-

71 BVerfG, 1 BvR u. a., 02.03.2010, Rn. 187.

72 Rusteberg, Benjamin, Die EG-Richtlinie zur Vorratsspeicherung von Verkehrsdaten im System des europäischen Grund- und Menschenrechtsschutzes, in: VBIBW 2007, S. 171 (S. 175).

73 Berechnungen des Branchenverbandes BITKOM, (ohne genauere Quellenangabe) angegeben von Sierck/Schöning/Pöhl, Zulässigkeit der Vorratsdatenspeicherung nach europäischem und deutschem Recht, Wissenschaftliche Dienste des Deutschen Bundestages, WD 3 – 282/06 vom 3.8.2006, S. 14.

den durch die Anschaffung von Hard- und Software sowie durch Kosten für den Betrieb, zum Beispiel für Personal und Datensicherung.

Die RL 2006/24/EG trifft **keine ausdrückliche Regelung** zur Kostentragungspflicht. Der EuGH ist in dem Verfahren über die **Nichtigkeitsklage Irlands**, indem er lediglich kompetenzrechtliche Fragen geprüft und die Vereinbarkeit der RL 2006/24/EG mit den Gemeinschaftsgrundrechten ausdrücklich offen gelassen hat, deswegen zu seiner klagabweisenden Entscheidung gelangt, weil die Richtlinie nach seiner Auffassung in überwiegendem Maß das Funktionieren des Binnenmarktes betreffe und ihr Erlass insbesondere im Hinblick auf die **Harmonisierung** der unterschiedlichen nationalen Vorschriften zur Vorratsdatenspeicherung geboten gewesen sei. Was die Frage der Kostentragung betrifft, ist interessant, dass der EuGH im Zusammenhang mit **möglichen Wettbewerbsverzerrungen** infolge von Unterschieden zwischen den nationalen Regelungen darauf hinweist, dass die Verpflichtung zur Vorratsdatenspeicherung erhebliche wirtschaftliche Auswirkungen für die Dienstanbieter hätte, da sie hohe Investitionen und Betriebskosten nach sich ziehen könnte. Allerdings kann von einer Einheitlichkeit in dieser Hinsicht keine Rede sein. Gerade in den großen und daher im Hinblick auf mögliche Wettbewerbsverzerrungen besonders relevanten Mitgliedstaaten reichen die nationalen Entschädigungsregelungen von einer vollen Auferlegung bis hin zu einer weitgehenden Erstattung der Kosten.⁷⁶

Generell ist anzumerken, dass in den meisten Mitgliedstaaten, die die Speicherung von Daten auf Vorrat bereits praktizieren, keine expliziten Kostentragungsregelungen vorgesehen sind. Den Telekommunikationsdienstleistern in **Deutschland** werden die mit der Vorratsdatenspeicherung an sich verbundenen Kosten **ausdrücklich nicht ersetzt**, wobei aber ein Ersatz jener Kosten erfolgt, die im Zusammenhang mit der Beantwortung von Auskunftersuchen entstehen.⁷⁷ Auch in Spanien wurden keine Kostentragungsregeln in das Gesetz aufgenommen, hauptsächlich mit der Begründung, dass im Telekommunikationssektor ohnehin eine ausreichende Gewinnspanne vorläge, um die zusätzlichen Kosten abzudecken. Frankreich, Großbritannien und Tschechien hingegen sehen ausdrücklich vor, dass Telekommunikationsdienstleister für ihre Speicherpflichten ökonomisch zu entschädigen sind.

74 Schätzungen von Klaus Landefeld, Vorstand Infrastruktur und Netze des Verbandes der deutschen Internetwirtschaft (eco), online abrufbar unter http://www.eco.de/verband/202_2418.htm (Stand: 19.09.2007), zuletzt abgerufen am 01.02.2011.

75 In einem Argumentationspapier beruft sich die FDP ebenfalls auf den Branchenverband eco (ohne genauere Quellenangabe), online abrufbar unter: http://www.marco-buschmann.de/files/26949/10_12_13_Argumentationshilfe_VDS.pdf, zuletzt abgerufen am 01.02.2011.

76 Rechtsvergleichende Analyse im Hinblick auf die Umsetzung der Richtlinie 2006/24/EG über die Vorratsdatenspeicherung im Auftrag des Bundesministeriums für Verkehr, Innovation und Technologie vorgelegt vom Ludwig Boltzmann Institut für Menschenrechte (BIM) in Kooperation mit dem Institut für Rechtsinformatik der Leibniz Universität Hannover (IRI), Österreich.

77 Das Gesetz zur Neuordnung der Entschädigung von Telekommunikationsunternehmen für die Heranziehung im Rahmen der Strafverfolgung (TK-Entschädigungs-Neuordnungsgesetz – TKEntschNeuOG) vom 29. April 2009 sieht nur einen Ersatz von Aufwendungen für konkrete Anfragen, nicht aber den Ersatz von zuvor bereits erbrachten Implementierungs- und Betriebskosten vor.

Folge des Gestaltungsspielraums hinsichtlich der Kostentragung ist, dass die Ausgestaltung in den einzelnen Mitgliedstaaten variiert. Dementsprechend **mangelt es an einer Harmonisierung** durch die Richtlinie und es kommt stattdessen – gerade entgegen dem eigentlichen Ziel der Richtlinie – zu **Wettbewerbsverzerrungen**.

Überdies hat sich gezeigt, dass sich die Erfolge der Vorratsdatenspeicherung in einem sehr kleinen Rahmen halten. So hat zum Beispiel eine Studie des Bundeskriminalamts aus dem Jahr 2005⁷⁸ ergeben, dass lediglich 381 Straftaten aus dem Grund unaufgeklärt blieben, weil Ermittler nicht mehr auf bereits gelöschte Daten zugreifen konnten.⁷⁹ Die somit durch die Vorratsdatenspeicherung bislang nur marginal um 0,006 % verbesserte Aufklärungsquote⁸⁰ könnte daran zweifeln lassen, ob die Regelung in ihrer konkreten Ausgestaltung einer Überprüfung auf ihre Angemessenheit hin standhalten kann. **Zweck und Mittel** stehen hier zumindest **nicht in einem ausgewogenen Verhältnis**.

78 Tabellarische Übersicht der Kriminalstatistik des Bundeskriminalamts online abrufbar unter <http://www.vorratsdatenspeicherung.de/content/view/378/79/lang.de/> (Stand: 02.09.2010), zuletzt abgerufen am 03.02.11.

79 Das Max-Planck-Institut für ausländisches und internationales Strafrecht hat in einer Untersuchung aus dem Jahr 2007 für die ohne Vorratsspeicherung verfügbaren Kommunikationsdaten festgestellt: „Doch weist die Aktenanalyse selbst unter den heutigen rechtlichen Bedingungen nur für etwa 2 % der Abfragen nach, dass sie wegen Löschungen ins Leere gehen.“

80 Gietl, Andreas, Die Einführung der Vorratsdatenspeicherung, in: K&R 2007, S. 545-550 (S. 552).

5. Ergebnis

Die Richtlinie weist eine **erhebliche Grundrechtsrelevanz** auf. Da sie sich aber auf die Anordnung der Datenspeicherung auf Vorrat beschränkt und im Übrigen die wirklich sensiblen Bereiche, wie den Zugang zu und die Verwendung der Daten, den Mitgliedstaaten überlässt, liegt kein offensichtlicher Verstoß gegen die Grundrechtecharta vor. Vielmehr verpflichtet sie die Mitgliedstaaten, die Richtlinie grundrechtskonform umzusetzen. Die Mindestanforderungen an den Datenschutz in Art. 7 RL 2006/24/EG und die Einrichtung unabhängiger Kontrollstellen in den Mitgliedstaaten (Art. 9 RL 2006/24/EG) betonen die Verantwortung der Mitgliedstaaten, Missbrauch vorzubeugen.

An der Vereinbarkeit der RL 2006/24/EG mit der von ihr vorgesehenen Verpflichtung zur anlasslosen Vorratsdatenspeicherung mit dem gemeinschaftsrechtlichen Grundsatz der berufs- und wirtschaftlichen Betätigungsfreiheit bestehen **Zweifel**. Die Geeignetheit der Regelung lässt sich im Hinblick auf den abstrakt-generellen Beurteilungsmaßstab bejahen. Auch die Erforderlichkeit könnte man unter dem Aspekt, dass die anlasslose Speicherung umfangreicher und somit sicherer und effektiver ist als eine verdachtsbegründete Speicheranordnung im Einzelfall, bejahen. Problematisch dürfte indes die Angemessenheit der Regelung unter dem Gesichtspunkt der Zweck-Mittel-Relation sein. Vorbehaltlich der noch ausstehenden Bewertung der Kommission, die vermutlich tragfähige Daten über die Erfolgsaussichten der Vorratsspeicherung enthalten wird, könnte die Regelung in ihrer momentanen Ausgestaltung unangemessen in das Gemeinschaftsgrundrecht der berufs- und wirtschaftlichen Betätigungsfreiheit zu Lasten der Telekommunikationsanbieter eingreifen. Gemessen an dem derzeitigen Diskussionsstand zur Richtlinie 2006/24/EG und zur Auslegung der GRCh sowie der bestehenden Umsetzungsspielräume der Mitgliedstaaten lässt sich zweifelsfrei keine Ausgestaltung dieser Richtlinie umschreiben, die eine Vereinbarkeit mit der GRCh sicherstellte. Insb. kann nicht abschließend beurteilt werden, ob weniger eingriffsintensive Formen der Datenerhebung gegenüber der in der RL 2006/24/EG vorgesehenen anlasslosen Datenspeicherung in gleicher Weise geeignet sind, die mit dieser Richtlinie verfolgten Ziele zu verwirklichen.

(Dr. Derksen)