Inhaltsverzeichnis

„Sicherheit und Rechtsstaat im Spannungsverhältnis“

Die Richtlinie 2006/24/EG zur Vorratsdatenspeicherung und die Erfolgsaussichten einer Klage im nationalen und europäischen Kontext

„Es nützt der Freiheit nichts, dass wir sie abschaffen, um sie zu schützen.“

Wolfgang Thierse, Deutscher Bundestagspräsident

A. Einleitung

I. Einleitende Gedanken zum Verhältnis von Freiheit und Sicherheit

„Im sogenannten „Dritten Reich“ hörten wir uns Feindsender nur mit einem Kristall-Detektor und Kopfhörern an – und sprachen mit niemandem darüber, buchstäblich mit keinem.

Wenn man es riskierte, jemandem etwas politisch vermutlich Missliebiges zu erzählen, dann sicherte man sich vorher mit dem sogenannten „deutschen Blick“ gegen unerwünschte Mithörer ab. Wer das einmal erlebt hat, vergisst es nie. Es ist das Gefühl der absoluten Isolierung, der Wehrlosigkeit und Einsamkeit, wenn jedes menschliche Vertrauen, zu wem auch immer, jedes Selbstgespräch, jede Tagebuchaufzeichnung zu einer wirklichen Gefahr für Freiheit, Leib und Leben wird.“[1]

Diese Gedanken des Ministers des Innern in Nordrhein-Westfalen a.D. und Vizepräsidenten des Deutschen Bundestages a.D. Burkhard Hirsch machen deutlich, welche Bedeutung Freiheit für jeden einzelnen Menschen hat, insbesondere dann, wenn man ihm diese genommen hat. Auch heute ist Freiheit lange keine Selbstverständlichkeit, denn auch Freiheitsrechte bedürfen zu ihrer Durchsetzung einer staatlichen Ordnung, die sich notfalls mit Hilfe des Zwangs Geltung verschaffen muss. Deshalb stehen Freiheits- und Sicherheitsrechte keineswegs in einem zwingenden Gegensatz zueinander, wie ab und an behauptet wird; tatsächlich bedingen sie sich

1 Hirsch, DuD 2008, 87.

sogar, auch wenn es immer wieder zu Zielkonflikten kommt.

Zwar lässt sich staatlicher Zwang auch ohne die Gewährung von Freiheitsrechten durchsetzen. Dies wäre mit dem Prinzip der Rechtsstaatlichkeit jedoch nicht vereinbar. Deshalb geht es gar nicht darum, dass sich das eine auf Kosten des anderen durchsetzen ließe. Vielmehr ist entscheidend, wie sich beides erreichen lässt, ohne dass es zu nicht hinnehmbaren Zugeständnissen an das eine oder das andere kommt.[2]

Wie elementar die Bedeutung von Freiheit ist, kommt bereits in der Bezeichnung der EU-Mitgliedstaaten als *freiheitliche demokratische Grundordnungen* zum Ausdruck, in denen sich die Staatsmacht auf der politischen Freiheit der Bürger gründet. Die Gewährleistung von Grundrechten, Rechtsstaatlichkeit und Demokratie ist es, die diese Grundordnung im Kern ausmacht.

Die Aufgabe des Rechtsstaats liegt darin, diese Freiheit, die in vielen verschiedenen Artikeln der nationalen Verfassungen, der Europäischen Menschenrechtskonvention und der Charta der Grundrechte der Europäischen Union, zum Ausdruck kommt, zu schützen und zu respektieren. Dabei geht es nicht darum, Freiheitsrechten grundsätzlich unbeschränkt Geltung zu verschaffen. Politische Erfordernisse bedingen vielmehr häufig einen Eingriff in gewisse Freiheitsrechte. Entscheidend ist jedoch, dass dieser nicht willkürlich vorgenommen wird und den Kern des entsprechenden Rechts nicht tangiert.[3]

Die Gewährleistung innerer und äußerer Sicherheit gehört zu den Herausforderungen, denen sich der Staat bei der Ausübung des Gewaltmonopols als Teil der staatlichen Gewaltenteilung zu stellen hat.[4] Eine glaubwürdige rechtsstaatliche Sicherheitspolitik kommt jedoch ohne die Gewährung von Freiheitsrechten nicht aus.

Dieses Spannungsverhältnis von der Gewährleistung von Sicherheit auf der einen Seite und rechtsstaatlich garantierter Freiheit des Einzelnen auf der anderen Seite vor dem Hintergrund der Richtlinie zur Vorratsdatenspeicherung im Rahmen der Erfolgsaussichten einer Klage vor dem deutschen Bundesverfassungsgericht, dem Europäischen Gerichtshof und dem Europäischen Gerichtshof für Menschenrechte näher zu bestimmen, die Konsequenzen einer Abwägung zu dieser oder jener Seite aufzuzeigen und letztlich zu einer begründeten Entscheidung zu gelangen, soll Aufgabe dieser Arbeit sein. Dabei soll es nicht darum gehen, die „Eine Lösung“ zu finden. Das würde der Komplexität dieses Themas und der auf beiden Seiten der Argumentation

2 Bielefeldt 2008, 11.
3 Bielefeld 2008, 12.
4 Glaeßner, Aus Politik und Zeitgeschichte 2002, 4.

stehenden jeweils ernstzunehmenden Ängste wohl kaum gerecht. Vielmehr sollen Sicherheits- und Freiheitsbedürfnisse möglichst umfassend miteinander abgewogen und den Erfolgsaussichten einer Klage vor den nationalen und europäischen Institutionen damit eine juristisch untermauerte Richtung gegeben werden. Letztlich ist es weniger von Bedeutung eine „Mitte“ zwischen Sicherheit auf der einen und Freiheit auf der anderen Seite zu finden. Vielmehr soll die Verhältnismäßigkeit der staatlichen Eingriffe in Freiheitsrechte in dem Sinne gewahrt sein, dass „die für das Selbstverständnis des freiheitlichen Rechtsstaats konstitutive Orientierung am Respekt der Rechtssubjektivität des Menschen auch in der Sicherheitspolitik maximal zum Tragen kommt.“[5]

Nach dem 11. September 2001 kam es in der Europäischen Union und in den einzelnen Mitgliedstaaten zur Verabschiedung zahlreicher neuer Sicherheitsgesetze, die auf eine Abwehr terroristischer Gefahren abzielten. Wie ernst diese auch in Europa zu nehmen sind, zeigten die Anschläge in Madrid und London. Die Terroristen intendieren eine Schwächung des Staates und bedienen sich dabei grausamer, menschenverachtender Instrumente, die sich jeglicher Nachvollziehbarkeit entziehen. Eine Handlungspflicht des Staates beziehungsweise der Europäischen Union steht deshalb außer Frage. Entscheidender Punkt ist jedoch, wie weit diese Handlungspflicht gehen darf und in welchem Umfang Terrorismus mit Mitteln bekämpft wird, die sich noch innerhalb des rechtsstaatlich vertretbaren Rahmens befinden beziehungsweise wann der Punkt erreicht ist, an dem andere Rechte so weit eingeschränkt werden, dass dieser Rahmen überschritten ist; zumal die Zielsetzung präventiver Sicherheit der bisherigen Strafrechtspraxis, wonach erst die bereits entstandene Verletzung eines Rechtsgut geahndet wird, widerspricht.[6] Dabei ist auch zu berücksichtigen, das absolute Sicherheit nicht erreichbar ist und eine Status-quo-Politik auch wenn sie im Hinblick auf den Wähler gelegentlich attraktiv erscheint, sich deshalb verbietet.[7] Die Abwägung zwischen Sicherheits- und Freiheitsrechten ist hochkomplex und muss mit äußerster Sensibilität und Sorgfalt für jeden Einzelfall vorgenommen werden. Diese Abwägung wird für die Richtlinie 2006/24/EG zur Vorratsdatenspeicherung und der Umsetzungsregelungen im Telekommunikationsgesetz in dieser Arbeit durchgeführt.

Das Hauptgewicht der Überprüfung liegt dabei auf dem Fernmeldegeheimnis aus Art.

5 Bielefeldt 2008, 14.
6 Bielefeldt 2008, 4.
7 Glaeßner, Aus Politik und Zeitgeschichte 2002, 5 f.

10 Abs. 1 Var. 3 GG, dem Recht auf den Schutz personenbezogener Daten aus Art. 8 Abs. 1 GRC und dem Recht auf Achtung des Privat- und Familienlebens aus Art. 8 Abs. 1 EMRK. Diese Rechte bilden den Schwerpunkt des grundrechtlichen Datenschutzes auf nationaler und europäischer Ebene. Eine abschließende Überprüfung weiterer möglicherweise einschlägiger Grundrechte wird im Hinblick auf den begrenzten Umfang dieser Arbeit nicht vorgenommen.

II. Aufbau der Arbeit

Die folgenden Ausführungen gliedern sich wie folgt: Ich werde zunächst die Richtlinie 2006/24/EG in ihren historischen Entstehungskontext einordnen. Danach erfolgt eine kurze inhaltliche Vorstellung. Im Anschluss werde ich die Kompetenz der EG zur Einführung der Vorratsdatenspeicherung näher beleuchten und in diesem Zusammenhang auch auf die Klage Irlands, die diese Problematik zum Inhalt hatte, eingehen.

Die rechtliche Prüfung wird zunächst anhand einer Auseinandersetzung mit der vor dem deutschen Bundesverfassungsgericht anhängigen Verfassungsklage gegen die Umsetzung der Richtlinie 2006/24/EG (§§ 113a, b TKG) vorgenommen. In diesem Rahmen wird auch die Stellungnahme der Bundesregierung diskutiert.

Im Anschluss erfolgt eine ausführliche Prüfung der Erfolgsaussichten einer Klage vor dem Europäischen Gerichtshof und vor dem Europäischen Gerichtshof für Menschenrechte unter Zuhilfenahme der Charta der Grundrechte der Europäischen Union und der Europäischen Menschenrechtskonvention. Da die diskursive Auseinandersetzung mit der Vorratsdatenspeicherung bereits in der Angemessenheitsprüfung zur Verfassungsbeschwerde vorgenommen wird, geht es im europäischen Kontext vor allem darum, anhand der bisherigen Entscheidungen der Gerichte eine mögliche Richtung auszumachen und die bereits ergangenen Urteile vor dem Hintergrund der Richtlinie 2006/24/EG zu diskutieren, um letztlich zu einer begründeten Beurteilung zu gelangen, wie sich die Erfolgsaussichten vor dem EuGH und dem EGMR darstellen.

Im Fazit werde ich die Erfolgsaussichten einer Klage vor den genannten Institutionen abschließend bewerten und die Konsequenzen aus dieser Bewertung aufzeigen.

Zunächst werde ich nachfolgend auf die Entstehung der Richtlinie 2006/24/EG eingehen.

III. Entstehungsgeschichte

Ursprünglich ist die Verkehrsdatenanalyse eine traditionell im Geheimdienst- und Militärbereich verwendete Methode, die ohne Kenntnis des Inhalts der Kommunikation Rückschlüsse auf den Gegner zulassen sollte. Die Möglichkeit Verbindungsdaten großflächig zu erfassen entstand aber erst mit der Digitalisierung der Telekommunikation seit den 1980er Jahren.[8] Auf EU-Ebene diskutiert und schließlich umgesetzt wurde diese Möglichkeit, als nach den Terroranschlägen in Madrid im März 2004 und im Juli 2005 in London einzelne Staaten eine gesetzliche Pflicht zur Speicherung von Daten auf Vorrat einführten, und damit eine Harmonisierung der unterschiedlichen Regelungen auf europäischer Ebene für notwendig erachtet wurde. Der Rat erhielt den Auftrag, entsprechende Rechtsvorschriften zu erarbeiten. Dem vorausgegangen war auch die steigende Besorgnis der nationalen Strafverfolgungsbehörden über die Zunahme der Nutzung von Neuerungen im Bereich der elektronischen Kommunikationsdienste für kriminelle Handlungen. Daraufhin hatten die Mitgliedstaaten Regelungen getroffen, um die Löschung dieser Daten zu verhindern und sicherzustellen, dass diese den Strafverfolgungsbehörden zur Verfügung stehen.[9]

Der auf Art. 31 Abs. 1 Buchstabe c und Art. 34 Abs. 2 Buchstabe 2 EUV gestützte Entwurf eines Rahmenbeschlusses, wonach innerhalb der 3. Säule über die Polizeiliche und Justitielle Zusammenarbeit in Strafsachen Einstimmigkeit erforderlich gewesen wäre, scheiterte jedoch an eben diesem Erfordernis.[10] Die Kommission legte darauf hin einen Entwurf für eine Richtlinie nach Art. 95 EGV vor. Dieser Entwurf führte zur Änderung der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation[11], welche wiederum die Richtlinie 95/46/EG ergänzt, die ebenfalls Regeln für die Verarbeitung personenbezogener Daten festlegt. Die Verpflichtung zur Löschung der Daten nach Art. 5, 6 und 9 der Richtlinie 2002/58/EG wurde darin aufgehoben und in Art. 5 der neuen Richtlinie bestimmt, dass diese Daten für einen bestimmten Zeitraum auf Vorrat

8 Kurz/Rieger 2009, 4.

9 Vorschlag für die 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, Brüssel 21.09.2005, 2 f.

10 Prof. Dr. Dietrich Murswiek in der Presseerklärung zum Urteil des Europäischen Gerichtshofs zur Vorratsdatenspeicherung, Karlsruhe, 10. Februar 2009.

11 EuGH, Rs. C-301/06, Slg. 2009, Rn. 19/20.

gespeichert werden sollen. Die Richtlinie wurde am 21. Februar 2006 vom Rat mit qualifizierter Mehrheit verabschiedet. Irland und die Slowakei stimmten dagegen.[12]

Um die rechtliche Diskussion auch inhaltlich entsprechend vorzubereiten, werde ich im folgenden Kapitel auf die wesentlichen Vorgaben der Richtlinie 2006/24/EG eingehen.

Die Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 weist in der entsprechenden Veröffentlichung im Amtsblatt der Europäischen Union vom 13.04.2006 unter (5) der in Erwägung nachstehenden Gründe darauf hin, dass einige Mitgliedstaaten unterschiedliche Regelungen zur Vorratsdatenspeicherung von Daten durch Diensteanbieter erlassen haben. Diese führten zu einer Beeinträchtigung des Binnenmarktes für elektronische Kommunikation, da die Anbieter mit unterschiedlichen Bedingungen konfrontiert seien. Nach Auffassung des Europäischen Parlaments und des Rates ist darin das vorherrschende Ziel der Richtlinie zu sehen.[13]

Die bei der Vorratsdatenspeicherung erhobenen Daten lassen sich verschiedenen Datentypen zuordnen: (1) Zum Einen werden Verkehrsdaten erfasst, die Informationen darüber enthalten, wer mit wem wie lange kommuniziert. Des Weiteren werden (2) die Begleitumstände der Kommunikation gespeichert (insbesondere der Ort des Kommunikationsvorgans) und (3) Bestandsdaten, welche Informationen über die Identität des Nutzers enthalten.[14]

Der Eingriff in Art. 8 der Europäischen Konvention zum Schutz der Menschenrechte (EMRK) wird in Erwägungsgrund (9) gerechtfertigt. Demnach wird die Notwendigkeit eines Eingriffs in das Recht auf Achtung des Privatlebens und der Korrespondenz jeder Person in der effektiven Einsetzung gespeicherter Daten für Zwecke der Strafverfolgung bei organisierter Kriminalität und Terrorismus gesehen. Auch Art. 7 und 8 der Charta der Grundrechte der Europäischen Union, worin es um die Wahrung der Rechte der Bürger auf Achtung des Privatlebens und der Kommunikation sowie den Schutz personenbezogener Daten geht, werden als mit der Richtlinie vereinbar angesehen.

Die Richtlinie bezieht sich nicht auf den Inhalt der übermittelten Informationen, sondern nur auf solche Daten, die als Folge einer Kommunikation entstanden sind. Das geht aus Art. 1 der Richtlinie hervor. Das Subsidiaritätsprinzip wird nach Erwägungsgrund (21) als gewahrt angesehen, weil der Umfang und die Wirkungen der Vorratsdatenspeicherung zum Zweck der Feststellung, Ermittlung und Verfolgung von

12 EuGH, Rs. C-301/06, Slg. 2009, Rn. 23.
13 EuGH, Rs. C-301/06, Slg. 2009, Rn. 36/37/40.
14 Kurz/Rieger 2009, 5.

schweren Straftaten besser auf Gemeinschaftsebene zu erreichen seien.

Die Kategorien von auf Vorrat zu speichernden Daten sind in Art. 5 der Richtlinie aufgeführt. Nach Abs. 1 müssen Telefonfestnetz und Mobilfunk betreffend die Rufnummer des anrufenden Anschlusses sowie Name und Anschrift des Teilnehmers oder registrierten Benutzers gespeichert werden. Bei Internetzugang, EMail und über das Internet geführten Telefonaten müssen die Benutzerkennung, die Rufnummer sowie Name und Anschrift des Teilnehmers oder registrierten Benutzers, dem eine IP-Adresse, Benutzerkennung oder Rufnummer zum Zeitpunkt der Nachricht zugewiesen war, gespeichert werden. Weitere Daten werden unter Art. 5 Abs. 1 Buchstabe b zur Identifizierung des Adressaten einer Nachricht benötigt sowie nach Buchstabe c zur Bestimmung von Datum, Uhrzeit und Dauer einer Nachrichtenübermittlung. Zur Bestimmung der Art einer Nachrichtenübermittlung werden nach Buchstabe d der in Anspruch genommene Telefon- und Internetdienst benötigt und nach Buchstabe e sind auch Daten zur Endeinrichtung in Form der entsprechenden Rufnummer und Geräte- und Teilnehmererkennung von Bedeutung. Nach Buchstabe f werden auch zur Bestimmung des Standorts mobiler Geräte benötige Daten gespeichert.

Der Speicherungszeitraum beträgt nach Art. 6 mindestens 6 Monate und höchstens 2 Jahre. Die Möglichkeit einer Verlängerung der maximalen Speicherfrist besteht bei Vorliegen besonderer Umstände unter den Voraussetzungen des Art. 12.

Spätestens bis zum Jahr 2010 soll eine Bewertung der Anwendung der Richtlinie und ihrer Auswirkungen auf Wirtschaftsbeteiligte und Verbraucher erfolgen (Art. 14 Abs. 1).

Die Umsetzungsfrist für die Mitgliedstaaten ist in Art. 15 Abs. 1 S. 1 auf dem 15. September 2007 festgelegt. Die Speicherung von Kommunikationsdaten betreffend Internetzugang, Internet-Telefonie und EMail kann nach Abs. 3 S. 1 bis zum 15. März 2009 aufgeschoben werden.[15]

B. Kompetenz der EG zur Einführung der Vorratsdatenspeicherung vor dem Hintergrund der Klage Irlands

Insbesondere Irland machte geltend, dass die Wahl von Art. 95 EG als Rechtsgrundlage für die Richtlinie 2006/24/EG fehlerhaft sei und die EG auf dieser Grundlage keine Kompetenz zur Einführung der Richtlinie gehabt habe. Unterstützt von der Slowakischen Republik als Streithelferin reichte Irland in der Rechtssache C-301/06 am

15 Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006.

6. Juli 2006 eine Nichtigkeitsklage nach Art. 230 EG ein, über die der Gerichtshof mit Urteil vom 10. Februar 2009 entschieden hat.

I. Die Position Irlands

Darin befand Irland, dass Art. 95 EG nicht als Rechtsgrundlage für die Richtlinie zur Vorratsdatenspeicherung in Frage kommt, da der Hauptzweck der Richtlinie auf die Strafverfolgung abziele und daher nur Art. 30, 31 Abs. 1 Buchstabe c und 34 Abs. 2 Buchstabe b EUV einschlägig seien. Auf Art. 95 EG gestützte Maßnahmen müssten dagegen das Funktionieren des Binnenmarktes fördern. Das vorliegend ein Mangel, betreffend den Binnenmarkt besteht, werde zwar hinsichtlich der Unterschiede der nationalen Rechtsvorschriften behauptet, sei aber nicht nachgewiesen. Hinzu komme, dass die in der 3. Säule geforderte Einstimmigkeit nicht umgangen werden könne, in dem in die Richtlinie 2002/58 Bestimmungen eingefügt würden, die nicht in die Zuständigkeit der Gemeinschaft nach der 1. Säule fielen.[16]

Stützen konnte sich Irland auf die Entscheidung des EuGH zur Fluggastdatenübermittlung in die USA. Auch in diesem Fall hat die Kommission die Datenübermittlung mit dem Argument, dass ein Funktionieren des Binnenmarktes nur dann sichergestellt werden könne, wenn die Regelungen zur Fluggastdatenübermittlung harmonisiert würden, auf der Grundlage von Art. 95 EG autorisiert. Der EuGH verwarf diese Argumentation, da die Datenverarbeitung vorrangig dem Schutz der öffentlichen Sicherheit und der Strafverfolgung diene.[17]

II. Die Position des Parlaments und des Rates

Das Parlament macht dagegen geltend, dass in den Erwägungsgründen das vorherrschende Ziel, die Beseitigung der Behinderungen für den Binnenmarkt aufgrund der bestehenden unterschiedlichen nationalen Regelungen ausdrücklich genannt sei. Der Kostenfaktor für die Anbieter elektronischer Kommunikation sei demzufolge nicht zu unterschätzen und könne zu erheblichen Verzerrungen des Binnenmarktes führen. Folgerichtig sei Art. 95 EG die korrekte Rechtsgrundlage. Das es dabei auch um die Bekämpfung von Kriminalität gehe, mache die Rechtsgrundlage des Art. 95 EG nicht ungültig.[18]

16 EuGH, Rs. C-301/06, Slg. 2009, Rn. 28-32.
17 EuGH, Rs. C-301/06, Slg. 2009, Rn. 64/65.
18 EuGH, Rs. C-301/06, Slg. 2009, Rn. 36/37.

Der Rat schließt sich dieser Argumentation an und betont insbesondere die zunehmende Besorgnis der Mitgliedstaaten bezüglich der Zunahme der Nutzungen von Neuerungen im Bereich der elektronischen Kommunikationsdienste für kriminelle Handlungen. Zudem stellt er fest, dass es vielmehr falsch gewesen wäre, den Rechtsakt auf Art. 30, 31 und 34 EU zu stützen, da der Gesetzgeber mit der Schaffung vereinheitlichter Bedingungen für die Diensteanbieter lediglich auf ein bereits bestehendes Ungleichgewicht im Binnenmarkt reagiert habe.[19]

III. Die Position des Gerichtshofs

Nach Ansicht des Gerichtshofs sind bei der Wahl der Rechtsgrundlage insbesondere das Ziel und der Inhalt des Rechtsaktes entscheidend. Art. 95 EG kann nach Auffassung des Gerichts dann als Rechtsgrundlage herangezogen werden, wenn Unterschiede zwischen nationalen Regeln bestehen, die (1) geeignet sind die Grundfreiheiten zu beeinträchtigen oder Wettbewerbsverzerrungen zu verursachen und sich (2) auf diese Weise unmittelbar auf das Funktionieren des Binnenmarktes auswirken. Das Entstehen von Hindernissen für den Handel muss (3) zudem wahrscheinlich sein und (4) die betreffende Maßnahme ihre Vermeidung bezwecken.[20] Im Hinblick auf die Erwägungsgründe 5 und 6 der Richtlinie sieht das Gericht es als erwiesen an, dass der Gemeinschaftsgesetzgeber aufgrund der unterschiedlichen nationalen Regelungen zur Vorratsdatenspeicherung tätig geworden ist, die mit erheblichen wirtschaftlichen Folgen für die Diensteanbieter einhergehen. Auch sei ein Erlass weiterer Regelungen durch die Mitgliedstaaten, die noch keine Vorkehrungen zur Vorratsdatenspeicherung getroffen haben, absehbar gewesen, so dass sich in der Konsequenz eine weitere Heterogenität in der Regelungsbreite hätte ergeben können.[21]

Im Hinblick auf diese Gründe seien die unterschiedlichen nationalen Regelungen zur Vorratsdatenspeicherung geeignet gewesen, sich unmittelbar auf das Funktionieren des Binnenmarktes auszuwirken. Daher war der Erlass von Harmonisierungsvorschriften mit dem Ziel eines Schutzes des Binnenmarktes gerechtfertigt. Das Gericht stellt außerdem fest, dass mit der Richtlinie 2006/24 die Richtlinie 2002/58 geändert wurde. Da nach Art. 47 EU der EG Vertrag den EU Vertrag unberührt lasse, könne die Richtlinie 2006/24 nicht auf eine Bestimmung des EU Vertrages gestützt werden, ohne

19 EuGH, Rs. C-301/06, Slg. 2009, Rn. 40.
20 EuGH, Rs. C-301/06, Slg. 2009, Rn. 63/64.
21 EuGH, Rs. C-301/06, Slg. 2009, Rn. 66-70.

gegen Art. 47 EU zu verstoßen.[22]

In einem dritten Punkt geht der Gerichtshof auch auf den materiellen Gehalt der Richtlinie ein. Nach Auffassung des Gerichtes beziehe sich die Richtlinie im Wesentlichen auf die Tätigkeiten der Diensteanbieter und regele nicht den Zugang zu Daten oder deren Nutzung. Auch brächten die in der Richtlinie vorgesehenen Maßnahmen selbst keine Strafverfolgungsregelungen mit sich. Damit regele die Richtlinie Tätigkeiten, welche die polizeiliche und justitielle Zusammenarbeit in Strafsachen gar nicht betreffen. Im Wesentlichen falle der materielle Gehalt daher unter die Tätigkeiten der Diensteanbieter und regele nicht staatliche Tätigkeiten, die unter den Titel VI des EU Vertrages fallen.[23] Diese Begründung wird auch durch den Schlussantrag des Generalanwalts gestützt. Yves Bot räumt zwar ein, dass die Richtlinie den Zweck einer Strafverfolgung fördere. Dieses sei jedoch nicht ausreichend, um die gesamte Richtlinie im Bereich der 3. Säule einzuordnen. Bot betont vielmehr die Ansiedlung der beschlossenen Maßnahmen vor der Durchführung der polizeilichen und justitiellen Zusammenarbeit. Da die Richtlinie nicht den Zugang und die Verwendung von Daten regele, könne sie auch nicht auf der Grundlage des EU Vertrages erlassen werden.[24]

Diese Begründungen führen zu der Entscheidung des Gerichtshofs, die Klage Irlands abzuweisen und Art. 95 EG als richtige Rechtsnorm für die Richtlinie 2006/24/EG festzustellen.[25]

IV. Stellungnahme

Der Auffassung des Gerichtshofs ist aus folgenden Gründen zu widersprechen: Zum Einen dient die Richtlinie 2006/54 entgegen der Meinung des Gerichtshofs nicht der Harmonisierung des Binnenmarktes, sondern im Hauptzweck der Strafverfolgung und damit der inneren Sicherheit.[26] Das wird auch deutlich, wenn man die Stellungnahme der Bundesregierung zur Verfassungsbeschwerde gegen §§ 113a, b TKG heranzieht, die sich auf den Entstehungskontext der Richtlinie 2006/24/EG in Reaktion auf die terroristischen Anschläge im März 2004 in Madrid und im Juli 2005 in London bezieht

22 EuGH, Rs. C-301/06, Slg. 2009, Rn. 66-70.
23 EuGH, Rs. C-301/06, Slg. 2009, Rn. 80-84.
24 GA *Yves Bot,* Schlussanträge in der Rs. C-301/06 vom 14.10.2008, Slg. 2009 Nr. 103.
25 EuGH, Rs. C-301/06, Slg. 2009, Rn. 93/94.
26 So auch Prof. Dr. Dietrich Murswiek in der Presseerklärung zum Urteil des Europäischen Gerichtshofs zur Vorratsdatenspeicherung, Karlsruhe, 10. Februar 2009.

und außerdem darauf hinweist, dass der Regelungskontext der Terrorismusbekämpfung in den Erwägungsgründen der Richtlinie 2006/24/EG gleich an mehreren Punkten ausdrücklich erwähnt wird.[27] Der erste Satz in Art. 1 macht deutlich, dass es der Richtlinie nicht nur um Wettbewerbsverzerrungen im Binnenmarkt geht, sondern „dass die Daten zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten, wie sie von jedem Mitgliedstaat in seinem nationalen Recht bestimmt werden, zur Verfügung stehen“. Eindringlicher hätte die Kommission, sich eine staatliche Aufgabe zu eigen zu machen, wohl kaum formulieren können.[28] Des Weiteren harmonisiert die Richtlinie nicht nur, sondern modifiziert dadurch, dass sie die Vorratsdatenspeicherung bis in alle Einzelheiten hinein regelt.[29] Das Urteil stellt hier lediglich fest, dass die Richtlinie die Harmonisierung nationaler Vorschriften bezweckt, ohne eine saubere Überprüfung durchzuführen, wo der Schwerpunkt der Richtlinie wirklich liegt. Die Erwägungsgründe 5 und 6, wonach die Richtlinie aufgrund der unterschiedlichen nationalen Vorschriften erlassen wurde, mögen zwar eine Rolle gespielt haben, können aber über den zugrunde liegenden Regelungsinhalt, dessen Kernzweck in der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten besteht nicht hinwegtäuschen. Nach geltendem Recht wäre ein Rahmenschluss innerhalb der 3. Säule notwendig gewesen. Da die Einstimmigkeit nicht zustande kam, musste der Gesetzgeber auf die 1. Säule „ausweichen“, um eine Entscheidung in dieser Sache treffen zu können. Nach Professor Dr. Dietrich Murswiek, Direktor des Instituts für Öffentliches Recht und Professor für Staats- und Völkerrecht an der Universität Freiburg ist darin ein „krasser Rechtsmißbrauch“ zu sehen.[30] Das die Richtlinie in der Hauptsache nicht der Harmonisierung dient, zeigt sich bereits darin, dass sie weder hinsichtlich der Speicherdauer, noch hinsichtlich der Datentypen, noch hinsichtlich der Datenverwendung harmonisiert, sondern in allen Punkten nur Mindestvorgaben macht. Die Vorgaben der Mitgliedstaaten fallen damit dementsprechend weit auseinander. Die Anbieter sind im Ergebnis dadurch dass alle Mitgliedstaaten ein Gesetz zur Vorratsdatenspeicherung haben müssen, viel unterschiedlicheren Anforderungen ausgesetzt als vor Erlass der Richtlinie, als nur wenige Staaten entsprechende Regelungsvorschriften hatten. So erscheint es beispielsweise verwunderlich, dass eine Richtlinie, die aufgrund der erheblichen Kosten, welche den Diensteanbietern im

27 Stellungnahme der Bundesregierung vom 28. November 2008, 27.
28 Simitis, NJW 2009, 1784.
29 Simitis, NJW 2009, 1784.
30 Prof. Dr. Dietrich Murswiek in der Presseerklärung zum Urteil des Europäischen Gerichtshofs zur Vorratsdatenspeicherung, Karlsruhe, 10. Februar 2009.

Rahmen der Vorratsdatenspeicherung entstehen und die angeblich mit dem Ziel einer Harmonisierung und damit auch einer Angleichung dieser Kosten verabschiedet wurde, in Art. 6 einen Zeitraum für Speicherfristen von 6 Monaten bis 2 Jahren einräumt und in dieser angeblich so wichtigen Kostenfrage den Mitgliedstaaten einen so großen Spielraum belässt. Das der Zeitraum der Speicherung für die Kostenfrage von entscheidender Bedeutung ist, da diese nicht nur Anschaffungskosten für die entsprechende Technik beinhaltet, sondern ebenfalls laufende Kosten der Speicherung bestehen, zeigt eine Stellungnahme des Bundesverbandes Informationswirtschaft, Telekommunikation und neue Medien e.V. vom 22. Mai 2007, welche den deutschen Regierungsentwurf deshalb positiv bewertet, weil dieser lediglich die minimale Frist von 6 Monaten regelt und den Diensteanbietern damit die Kosten für eine weitergehende Speicherung erspart.[31] Vor dem Hintergrund der Entscheidung das es den Mitgliedstaaten freisteht, ob sie den Diensteanbietern die erheblichen mit der Einführung der Vorratsdatenspeicherung entstehenden Kosten erstatten[32], erscheint das vorgegebene Ziel der Entstehung von Wettbewerbsverzerrungen vorzubeugen wie eine Farce und dürfte bei der zu erwartenden unterschiedlichen Regelung in den Mitgliedstaaten zu weiteren Verzerrungen des Wettbewerbs führen. Entgegen der Argumentation des Gerichtshofs bezweckt die Richtlinie 2006/54/EG damit nicht die Vermeidung von Wettbewerbsverzerrungen, sondern fördert diese noch.

Zudem ist es schlicht und ergreifend nicht richtig, dass die Richtlinie 2006/54/EG nach Art. 47 EUV auf Art. 95 EG gestützt werden musste, weil diese die Richtlinie 2002/58/EG ändert. Der Grund liegt in der Öffnungsklausel des Art. 15 Abs. 1 der Richtlinie 2002/58/EG, der einen Rahmenbeschluss zur Vorratsdatenspeicherung ermöglicht hätte.[33]

Letztlich muss auch die Konsequenz dieses Urteils berücksichtigt werden. Schließlich muss es dazu führen, dass jede Inpflichtnahme Privater zu staatlichen Zwecken die mit Kostennachteilen verbunden ist, durch die EG harmonisiert werden kann. Dadurch wird das Subsidiaritätsprinzip gem. Art. 5 EG-Vertrag ad absurdum geführt. Die EG kann

---

31 Stellungnahme des Bundesverbandes Informationswirtschaft, Telekommunikation und neue Medien e.V. zum Regierungsentwurf für ein Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 22.05.2007, http://www.bitkom.org/files/documents/Stellungnahme_BITKOM_RegE_Neuregelung_TKUe_22_05_07.pdf (10.06.09)

32 http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+IM-PRESS+20051215IPR03785+0+DOC+XML+V0//DE (Zugriff: 27.06.09).

33 Breyer, 06.06.2009.

damit auch in Bereichen der 3. Säule tätig werden, in denen sich die Mitgliedstaaten aufgrund der Sensibilität dieser Politikfelder Einstimmigkeit vorbehalten hatten. Die extensive Auslegung des Art. 95 EG ist auch dann nicht nachvollziehbar, wenn man bedenkt, dass dieser bei Wettbewerbsverzerrungen beziehungsweise dem Abbau von Handelshemmnissen und nicht bei jeder geringfügigen Wirkung auf den Wettbewerb einschlägig sein sollte.[34] Gerade diese wesentliche Unterscheidung nimmt der Gerichtshof jedoch nicht vor. Die Argumentation bleibt in diesem Punkt schwach und weist lediglich darauf hin, dass es zu Wettbewerbsverzerrungen kommt, ohne auf die Folgen näher einzugehen. Professor Dr. Dietrich Murswiek äußert sich dazu wie folgt:“ Mit seinem Urteil zur Vorratsdatenspeicherung hat der EuGH erneut unter Beweis gestellt, dass er sich als „Motor der Integration“ versteht und die binnenmarktbezogenen Kompetenzen der Union in extremer Weise ausdehnt, um auf diese Weise die Machtpositionen der Europäischen Union zu stärken und die Entscheidungsfreiheit der Mitgliedstaaten und ihrer nationalen Parlamente zu schwächen.“[35]

Ein weiteres Prinzip, das durch das Urteil des EuGH unterlaufen wird, ist das der begrenzten Einzelermächtigung, wonach die Europäische Union nur in den Bereichen tätig werden kann, die ihr durch die Verträge ausdrücklich zugewiesen worden sind und wonach die Organe der EU die ihnen zustehenden Kompetenzen nicht überschreiten dürfen.[36] Der EuGH unterstützt mit diesem Urteil die Tendenz der europäischen Organe, sich immer neue Kompetenzen zuzuschreiben, die ihnen im Rahmen der Verträge gar nicht zugestanden worden sind und hat damit die Chance vertan als kontrollierendes Organ dem für das Funktionieren der Gemeinschaft so wichtigem Prinzip der begrenzten Einzelermächtigung Geltung zu verschaffen.[37]

Insgesamt gesehen erscheint die Kürze des Urteils im Gegensatz zur Bedeutung der zu klärenden Rechtsfrage unproportional. Die Argumentation muss sich den Vorwurf der Vordergründigkeit gefallen lassen, da sie häufig nicht den Kern des Problems trifft und die zugrunde liegenden Konsequenzen außer acht lässt. Zudem steht das Urteil im offensichtlichen Kontrast zur Rechtsprechung im Falle der Fluggastdaten. Die

34 Rzeniecki, http://www.rewi.euv-frankfurt-o.de/de/profil/Projekte/deluxe/aktueller_fall/fall_vorratsdatenspeicherung.html (Zugriff: 07.06.09).

35 Prof. Dr. Dietrich Murswiek in der Presseerklärung zum Urteil des Europäischen Gerichtshofs zur Vorratsdatenspeicherung, Karlsruhe, 10. Februar 2009.

36 http://www.cep.eu/index.php?id=68&no_cache=1&L=0&tx_sgglossary_pi1%5Bsearchmode%5D=1&tx_sgglossary_pi1%5Bsearch%5D%5Babc%5D=Prinzip+der+begrenzten+Einzelermächtigung (Zugriff: 07.06.09).

37 Prof. Dr. Dietrich Murswiek in der Presseerklärung zum Urteil des Europäischen Gerichtshofs zur Vorratsdatenspeicherung, Karlsruhe, 10. Februar 2009.

Abgrenzung, dass die Passagierdaten ausschließlich zum Schutz der öffentlichen Sicherheit und zu Strafverfolgungszwecken verarbeitet werden, während es bei der Vorratsdatenspeicherung darum gehe, Tätigkeiten bestimmter Diensteanbieter im Binnenmarkt und gerade nicht das Handeln staatlicher Stellen zu Strafverfolgungszwecken zu regeln,[38] ist nicht nachzuvollziehen und hätte weiterer Ausführungen bedurft, gerade weil der Gerichtshof hätte wissen müssen, dass das Urteil zur Vorratsdatenspeicherung daran gemessen wird. Schließlich sind die Speichertätigkeiten der Diensteanbieter auf einen ganz bestimmten Zweck hingerichtet für das, ebenso wie bei der Übermittlung der Flugpassagierdaten, die Kommission nicht zuständig ist.[39]

Die weitere Auseinandersetzung mit Grundrechten des Grundgesetzes, der Grundrechtecharta der EU und der EMRK wird nun zeigen, inwieweit die Richtlinie 2006/24/EG einer inhaltlichen Überprüfung standhalten kann.

C. Erfolgsaussichten einer Verfassungsbeschwerde in Deutschland

I. Zulässigkeit

Die Zulässigkeit werde ich im Folgenden nicht anhand einer Abarbeitung der einzelnen Zulässigkeitsvoraussetzungen prüfen, zumal dieses aufgrund der Tatsache das es sich um einen Vorgang handelt, der die Umsetzung einer Richtlinie der EG zum Inhalt hat, zumindest im klassischen Sinne problematisch wäre. Ich möchte vielmehr auf die Probleme, die sich gerade aufgrund dieser Verknüpfung von europäischem Recht und nationalem Verfassungsgericht ergeben, eingehen und damit eine kurze Einschätzung der rechtlichen Situation in dieser Frage wiedergeben.

Eine wichtige Orientierung bietet der Antrag zur Aussetzung des Umsetzungsgesetzes im Verfahren der einstweiligen Anordnung nach § 32 BVerfGG, der im Rahmen der am 31.12.2007 eingereichten Verfassungsbeschwerde von der Bürgerinitiative des Arbeitskreises Vorratsdatenspeicherung gestellt wurde.[40] Darüber entschied das Bundesverfassungsgericht am 11.03.2008.[41]

Soweit sich die Zulässigkeit auf Teile des Umsetzungsgesetzes, die über die Vorgaben

38 EuGH, Rs. C-301/06, Slg. 2009, Rn. 88/91.
39 Simitis, NJW 2009, 1785.
40 http://wiki.vorratsdatenspeicherung.de/images/Verfassungsbeschwerde_Vorratsdatenspeicherung.pdf (Zugriff: 08.06.09).
41 BVerfGE 256.

der Richtlinie hinausgehen, bezieht, ist diese zu bejahen. Zweifel ergeben sich jedoch an der Zulässigkeit der Verfassungsbeschwerde gegen jene Regeln, die aufgrund nicht zur Disposition stehender Vorgaben der Richtlinie 2006/24/EG umgesetzt wurden. Auch die Bundesregierung äußert in ihrer Stellungnahme zur Verfassungsbeschwerde gegen die §§ 113a, b TKG erhebliche Zweifel und schätzt diese mangels Prüfungskompetenz des Bundesverfassungsgerichts als unzulässig ein. Da die §§ 113a, b TKG im Wesentlichen den Vorgaben der Richtlinie 2006/24/EG entsprächen, sei die Prüfung durch das Bundesverfassungsgericht ausgeschlossen. Insbesondere sei auch die Regelung zu Anonymisierungsdiensten nach § 113a Abs. 6 TKG von den Regelungen der Richtlinie gedeckt, da andernfalls keine vollständige Speicherung der Verkehrsdaten erreicht werden könne und dieses zudem auch Art. 5 Abs. 1 Buchstabe a der Richtlinie 2006/24/EG widerspräche, wonach es zur ausdrücklichen Pflicht der Mitgliedstaaten gehört die für die Rückverfolgung und Identifizierung der Quelle einer Nachricht benötigten Daten zu speichern.[42] Der Beschwerdegegenstand sei insgesamt der Prüfung durch das Bundesverfassungsgericht entzogen. Insbesondere sei auch nicht vom Ausbleiben eines vergleichenden Rechtsschutzes im Sinne der „Solange“ Rechtsprechung auszugehen.[43]

Daran, dass das Bundesverfassungsgericht im Verfahren der einstweiligen Anordnung keinen Grund sieht, die Verfassungsbeschwerde von vornherein als unzulässig anzusehen,[44] kann jedoch abgesehen werden, dass es auch inhaltlich die Möglichkeit in Betracht zieht, dass der erforderliche Grundrechtsstandard durch die Umsetzung der Richtlinie 2006/24/EG nicht mehr gewahrt sein könnte. Grund für diese Schlussfolgerung ist die Entscheidung zur Bananenmarktordnung,[45] wonach das Gericht Verfassungsbeschwerden als von vornherein unzulässig ablehnt, wenn in der Begründung nicht dargelegt wird, „dass die europäische Rechtsentwicklung einschließlich der Rechtsprechung des Europäischen Gerichtshofs […] unter den erforderlichen Grundrechtsstandard abgesunken sind.“[46] Darauf berufen sich auch die Beschwerdeführer der Verfassungsbeschwerde und sehen zudem die angegriffenen Regelungen als nicht zwingend europarechtlich vorgegeben an.[47] Die Bundesregierung führt in ihrer Stellungnahme dazu lediglich an, dass nach dem erreichten Stand der

42 Stellungnahme der Bundesregierung vom 28. November 2008,10.
43 Stellungnahme der Bundesregierung vom 28. November 2008,13.
44 BVerfGE 256, 134.
45 BVerfGE 102, 147.
46 BVerfGE 102, 147.
47 Verfassungsbeschwerde Vorratsdatenspeicherung vom 31.12.2007, 20.

Integration von einem dem Grundgesetz vergleichbaren Grundrechtsschutz ausgegangen werden muss und auch aus diesem Grund keine Prüfungskompetenz des Bundesverfassungsgerichts bestehe.[48] Diese Annahme muss einer Prüfung im Einzelfall jedoch nicht zwingend entbehren, zumal die Grundrechtecharta bis heute nicht rechtsverbindlich ist und damit wenn überhaupt nur faktisch von einem vergleichbaren Grundrechtsschutz die Rede sein kann.

Eine Zulässigkeitsprüfung unter diesen Voraussetzungen beinhaltet die Gefahr eines Kompetenzkonfliktes im Verhältnis zum EuGH. Bezüglich der Aussetzung des Umsetzungsgesetzes stellt das Bundesverfassungsgericht deshalb fest, dass diese nur unter der drohenden Gefahr eines schweren und irreparablen Schadens unter dem hinnehmbaren Risiko des Überschreitens der eigenen Entscheidungskompetenz und einer möglichen schwerwiegenden Beeinträchtigung des effektiven Vollzugs des Gemeinschaftsrechts möglich sei.[49]

II. Prüfung der möglichen Grundrechtsverletzungen

Die am 31.12.2007 vor dem deutschen Bundesverfassungsgericht eingelegte Verfassungsbeschwerde zielt darauf ab, die §§ 113a, b des Telekommunikationsgesetzes in der Fassung des Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG für unvereinbar mit Art. 10, Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1, Art. 5, Art. 12, Art. 14 und Art. 3 Abs. 1 GG zu erklären und den Europäischen Gerichtshof im Rahmen des Vorabentscheidungsverfahrens nach Art. 234 EG die Frage der Gültigkeit der Richtlinie 2006/24/EG zur Klärung vorzulegen.[50]

Wie bereits in der Einleitung erläutert, wird nachfolgend nur Art. 10 Abs. 1 Var. 3 GG und das Verhältnis zum Recht auf informationelle Selbstbestimmung geprüft.

Das Fernmeldegeheimnis aus Art. 10 Abs. 1 Var. 3 GG und das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG

Das Fernmeldegeheimnis

1. Schutzbereich

In Betracht kommt ein Verstoß gegen das Fernmeldegeheimnis aus Art. 10 Abs. 1 Var. 3

48 Stellungnahme der Bundesregierung vom 28. November 2008, 14.
49 BVerfGE 102, 147.
50 Verfassungsbeschwerde Vorratsdatenspeicherung vom 31.12.2007, 6.

GG. Der Schutzbereich umfasst sowohl die Vertraulichkeit von Inhalt und näheren Umständen eines Telekommunikationsvorganges,[51] als auch jede Form „staatlicher Einschaltung“, die nicht im Einverständnis mit beiden Kommunikationspartnern erfolgt.[52] Zu den „näheren Umständen“ gehört etwa die Information ob und wann zwischen welchen Personen Fernmeldeverkehr stattgefunden hat.[53] Es soll vermieden werden, dass der Meinungs- und Informationsaustausch mittels Telekommunikationsanlagen deswegen unterbleibt oder nach Form und Inhalt verändert verläuft, weil die Beteiligten mit Überwachung rechnen müssen.[54] Geschützt ist nicht nur der Austausch von Gedanken und Meinungen, sondern auch von anderen Informationen[55], wie Bildern, Musik, Zeichen und sonstige Daten. Außerdem sind auch neue Kommunikationsformen wie EMail und Internet geschützt. Eröffnet ist der Schutzbereich bereits dann, wenn der Wille der Teilnehmer darauf gerichtet ist, ein regelmäßig übertragungssicheres Medium in Anspruch zu nehmen.[56] Hinzu kommt, dass nicht nur die staatliche Kenntnisnahme von Fernmeldekommunikation geschützt ist, sondern auch der Informations- und Datenverarbeitungsprozess, der sich daran anschließt und durch den Gebrauch von den erlangten Kenntnissen in Gang gesetzt wird.[57]

Da die Aufzeichnung im Rahmen der Vorratsdatenspeicherung durch private Diensteanbieter und nicht durch den Staat selber erfolgt, ist außerdem zu klären, ob auch durch Private erfasste Telekommunikationsdaten vom Schutzbereich des Art. 10 Abs. 1 Var. 3 GG erfasst sind. Weil der Staat letztlich das Zugriffsrecht auf die gespeicherten Daten hat, kann jedoch nichts anderes gelten, als wenn dieser direkt die Aufzeichnung vornehmen würde.[58]

Nach § 113a Abs. 2-4 TKG speichern die Diensteanbieter das und auch zu welchem Zeitpunkt Fernmeldeverkehr zwischen Personen stattgefunden hat. Nach Abs. 9 können berechtigte Stellen Auskünfte über diese Daten einholen und diese damit auch für eine Weiterverarbeitung zu Strafverfolgungszwecken nutzen. Beide Elemente des § 113a TKG unterliegen folglich dem Schutzbereich des Art. 10 Abs. 1 Var. 3 GG. Gleiches gilt für § 113 b TKG, der die Verwendung der nach § 113 a TKG gespeicherten Daten

51 BVerfGE 67, 157, 172.
52 BVerfGE 85, 386, 399.
53 BVerfGE 67, 157, 172.
54 Korn, HRRS 2009, 114.
55 BVerfGE 100, 313, 358 f.
56 Breyer 2005, 82.
57 Münch/Kunig 2001, 701.
58 Duden Recht A-Z. 2007.

regelt.

Das Recht auf informationelle Selbstbestimmung

2. Schutzbereich

Das Recht auf informationelle Selbstbestimmung ist eine Ausprägung des allgemeinen Persönlichkeitsrechts und damit mit Verfassungsrang ausgestattet.[59] Es gibt dem Einzelnen die Befugnis selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte erhoben, verwendet gespeichert oder weitergegeben werden dürfen.[60] Ein persönlicher Lebenssachverhalt liegt dann vor, wenn die Verknüpfung des Lebenssachverhalts mit der Person möglich ist.[61] Anonymisierte Daten fallen somit nicht in den Schutzbereich des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG.[62] Die Erhebung und Verarbeitung personenbezogener Daten durch Private und durch staatliche Institutionen kann grds. eine pflichtwidrige Verletzung des Persönlichkeitsrechts des Betroffenen darstellen.[63] In § 3 des Bundesdatenschutzgesetzes (BDSG) findet sich eine Legaldefinition der „personenbezogenen Daten“. Danach versteht man unter personenbezogenen Daten nicht nur Name und Anschrift, sondern alle Angaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Das Recht auf informationelle Selbstbestimmung ist aufgrund der Multipolarität von Kommunikationsbeziehungen nicht nur als subjektives Recht zu begreifen, sondern bringt auch die Machtteilhabe durch Informationszugang zum Ausdruck.[64]

Die nach § 113 a Abs. 1-4 TKG zu speichernden Daten sind personenbezogen. Da eine Erhebung durch Private und ggf. auch spätere staatliche Weiterverarbeitung (§ 113b TKG) nicht ausgeschlossen werden kann, ist der Schutzbereich tangiert. Eine weitere Überprüfung erfolgt nur insoweit als das Fernmeldegeheimnis als lex specialis[65] vorliegend nicht einschlägig ist.

3. Eingriff

Einen Eingriff in Art. 10 Abs. 1 Var. 3 GG stellt jede staatliche Erhebung, Speicherung,

59 Petersen 2000, 19.
60 BVrfGE 103, 21, 32 f.
61 BVerfGE 103, 21, 33.
62 Petersen 2000, 14.
63 Brüggemeier 2006, 326.
64 Petersen 2000,19.
65 BverfGE 100, 313, 359.

Verarbeitung, Verwendung und Weitergabe von personenbezogenen Daten dar.[66] Bei Eingriffen in das Fernmeldegeheimnis ist auch die Gefahr des Missbrauchs von Daten zu berücksichtigen.[67] Die Grundrechte schützen den Einzelnen nämlich auch vor „fehlerhafter, missbräuchlicher oder exzessiver Verwertung von Kommunikationsdaten durch […] staatliche Stellen“.[68]

Es ist jedoch fraglich, ob ein Eingriff bereits dann vorliegt, wenn der Gesetzgeber die Diensteanbieter dazu verpflichtet, Daten auf Vorrat zu speichern und für den Abruf durch staatliche Behörden verfügbar zu halten. Nach dem modernen Eingriffsbegriff, wonach ein Eingriff bei jedem staatlichen Handeln, „das dem Einzelnen ein Verhalten, das in den Schutzbereich eines Grundrechts fällt, ganz oder teilweise unmöglich macht“,[69] vorliegt, schützen die Grundrechte auch vor mittelbaren Eingriffen, die durch typische beziehungsweise in Kauf genommene Nebenfolgen die Gefahr einer Beeinträchtigung beinhalten.[70] Die Gefahr einer Beeinträchtigung ist im Falle der Vorratsdatenspeicherung bereits durch die Aufzeichnung der Daten gegeben, da diese typischerweise eine staatliche Kenntnisnahme zur Folge haben kann und der Staat damit weiterhin das Zugriffsrecht auf die Daten hat. Da sich durch jede Verwendung zusätzliche nachteilige Folgen für den Betroffenen ergeben können, stellt auch die weitere Verarbeitung, Verwendung oder Weitergabe von Daten , die bereits zuvor durch einen Eingriff (Speicherung) in Art. 10 Abs. 1 Var. 3 GG erlangt worden sind, einen eigenständigen Eingriff in das Fernmeldegeheimnis dar.[71] Ein Eingriff in das Fernmeldegeheimnis aus Art. 10 Abs. 1 Var. 3 GG ist somit sowohl für die Speicherung, als auch für die weitere Verwendung der Daten zu bejahen.

4. Verfassungsmäßige Rechtfertigung und Auseinandersetzung mit der Stellungnahme der Bundesregierung vom 28. November 2008

a) Formelle Verfassungsmäßigkeit

In formeller Hinsicht bestehen gegen die §§ 113a, b TKG keine Bedenken. Die Gesetzgebungskompetenz des Bundes folgt aus Art. 73 Abs. 1 Nr. 7 GG. Dem Zitiergebot ist mit Art. 15 zur Änderung des Telekommunikationsgesetzes Genüge getan.

66 BVerfGE 85, 386, 398.
67 BVerfGE 65, 1, 46.
68 BVerfGE 85, 386, 397.
69 BVerfGE 105, 279, 299 ff.
70 Gröpl, http://www.groepl.uni-saarland.de/lehre/lehre07/GR04.pdf (Zugriff: 26.07.09).
71 Vgl. BVerfGE 100, 313, 360.

b) Materielle Verfassungsmäßigkeit

aa) Bestimmtheitsgebot

Beschränkungen des Fernmeldegeheimnisses können nach Art. 10 Abs. 2 S. 1 GG auf Grund eines Gesetzes angeordnet werden. Das Bundesverfassungsgericht hat wiederholt festgestellt, dass eine Vorratsdatenspeicherung von Daten, wenn sie „zu unbestimmten oder noch nicht bestimmbaren Zwecken“ erfolgt, verfassungswidrig sei.[72] Das Bundesverfassungsgericht sieht eine Vorratsdatenspeicherung damit nicht generell als verfassungswidrig an, sondern unter anderem dann, wenn der Verwendungszweck nicht hinreichend bestimmt ist. Dies folgt zusammen mit einer klaren Ermächtigung zu dem Eingriff auch aus dem Bestimmtheitsgebot, welches sich aus dem Rechtsstaatsprinzip ergibt. An dieses sind umso höhere Anforderungen zu stellen, je schwerwiegender die Auswirkungen der Regelungen sind.[73] § 113b TKG bestimmt für die auf Vorrat gespeicherten Daten, nur pauschal, dass sie „zur Verfolgung von Straftaten“ (Nr. 1), zur „Abwehr von erheblichen Gefahren für die öffentliche Sicherheit“ (Nr. 2) oder „zur Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes und des militärischen Abschirmdienstes“ (Nr. 3) verwendet werden dürfen. Diese Regelung zur Vorratsdatenspeicherung wird dem Bestimmtheitserfordernis damit nicht gerecht.[74] Vielmehr wäre eine Umschreibung notwendig, anhand derer sich eindeutig und unzweifelhaft die Straftatbestände ableiten lassen, die einen Datenzugriff rechtfertigen. Nach § 100g StPO werden die Verkehrsdaten durch die Strafverfolgungsbehörden nur erhoben, wenn bestimmte Tatsachen den Verdacht begründen, dass eine Straftat von erheblicher Bedeutung bzw. eine Straftat mittels Telekommunikation begangen wurde. § 100g StPO bestimmt damit die Voraussetzungen und den Zweck, zu dem Eingriffe in Art. 10 Abs. 1 Var. 3 GG vorgenommen werden hinreichend.[75]

bb) Verhältnismäßigkeit

Eine Klage vor dem Bundesverfassungsgericht hätte dann Aussicht auf Erfolg, wenn die §§ 113a, b TKG in Art. 10 Abs. 1 Var. 3 GG eingreifen und der Eingriff verfassungsmäßig nicht gerechtfertigt ist. Nach dem Verhältnismäßigkeitsprinzip dürfen Grundrechte nur insoweit eingeschränkt werden, wie die Maßnahme zur Erreichung des

72 BVerfGE 100, 313,359 f.; BVerfGE 65, 1, 46.
73 BVerfGE 62, 203 (210).
74 Puschke/Singelnstein, NJW 2008, 113, 118.
75 Korn, HRRS 2009, 122.

angestrebten Zwecks geeignet, erforderlich und angemessen ist und ein legitimes Ziel verfolgt wird.[76]

(1) Legitimer Zweck

Ziel der Umsetzung der Richtlinie 2006/24/EG ist die Verfolgung von schweren Straftaten und die Abwehr von Gefahren für die öffentliche Sicherheit (§ 113b Nr. 1, 2 TKG i.V.m. § 100g Abs. 1 S. 1 StPO).[77] An der Legitimität dieses Ziels bestehen keine Zweifel.

(2) Geeignetheit

Die Geeignetheit der Erhebung der auf Vorrat gespeicherten Verkehrsdaten zur Verfolgung dieses Ziels erscheint dagegen schon fraglicher. Zum Einen wird durch das Datenvolumen, welches bei der Speicherung sämtlicher Verkehrs- und Standortdaten entsteht, die Dauer des für die Erhebung notwendigen Suchlaufs stark erhöht bzw. eine angemessene Analyse unmöglich gemacht. Zum Anderen haben Straftäter zahlreiche Möglichkeiten, einer Entdeckung durch Erhebung ihrer Verkehrsdaten z.B. durch den Erwerb von Telefonkarten oder die Nutzung von Internetcafes zu entgehen.[78] Nicht unerwähnt bleiben sollte auch, dass 80 bis 90 Prozent aller Emails Spam sind, womit fast 60 Prozent des gesamten Speicherbedarfs im Rahmen der Vorratsdatenspeicherung nur für Daten über Spam verbraucht werden.[79]

Für die Eignung im Rahmen der Verhältnismäßigkeitsprüfung genügt es jedoch zunächst, wenn die Möglichkeit der Zweckerreichung besteht. Die Maßnahme darf nicht von vornherein untauglich erscheinen.[80] Die Umsetzung der Richtlinie 2006/24/EG lässt eine abstrakte Eignung zur Förderung des angestrebten Zwecks nicht bestreiten. Es kann nicht von vornherein ausgeschlossen werden, dass diese nicht in einzelnen Fällen zur Strafverfolgung geeignet ist.

(3) Erforderlichkeit

Bedenken bestehen auch hinsichtlich der Erforderlichkeit eines Zugriffs auf die nach § 113a TKG gespeicherten Verkehrsdaten. Nicht erforderlich ist eine Regelung, wenn der Zweck durch ein gleich wirksames, aber weniger belastendes Mittel erreicht werden

76 Calliess 2001, 570.
77 Siehe auch B.IV.
78 Breyer, StV 2007, 214.
79 http://www.heise.de/newsticker/Oesterreichs-IT-Branche-gegen-Vorratsdatenspeicherung-und-Bundestrojaner--/meldung/105029 (Zugriff: 13.06.09).
80 BVerfGE 67, 157, 175.

kann.[81] Die Strafverfolgungsbehörden hatten jedoch schon nach § 100g StPO a.F. Zugriff auf die Verbindungsdaten, die die Diensteanbieter zu Abrechnungszwecken speichern. Wie sich aus einer Studie des BKA ergibt, waren fehlende Verkehrsdaten nur in 0,01 % der Fälle, von jährlich 2,8 Mio. unaufgeklärten Straftaten, die Ursache.[82] Die Erhebung der auf Vorrat gespeicherten Daten wird den Ermittlungsbehörden daher nur in einzelnen Fällen nützlich sein. Zudem haben Untersuchungen ergeben, dass sich behördliche Datenabfragen in Großbritannien und Schweden zu mehr als 80 % nur auf die letzten drei Monate beziehen[83], während § 113a Abs. 1 S. 1 TKG nach Maßgabe der Richtlinie 2006/24/EG eine sechsmonatige Speicherungspflicht vorsieht, die folglich nicht als erforderlich angesehen werden kann. Die Bundesregierung vertritt in ihrer Stellungnahme zur Verfassungsbeschwerde gegen die §§ 113a, b TKG dagegen die Auffassung, dass die Speicherfrist von sechs Monaten eine absolute Untergrenze darstelle, da die Auswahl von Datenspuren eine Ermittlungsleistung der Sicherheitsbedürfnisse voraussetze, die einige Zeit in Anspruch nehme, so dass eine kürzere Phase nicht sinnvoll sei. Auf empirische Erkenntnisse kann sie sich dabei allerdings nicht stützen. Stattdessen werden Einzelfälle angeführt, welche die Untersuchungen zu Datenabfragen in Großbritannien und Schweden nicht zu widerlegen vermögen.[84]

Ein milderes Mittel ist das in den USA bereits seit längerem praktizierte „Quick-Freeze“ Verfahren, bei dem die Daten nur bei dringendem Verdacht gespeichert werden. Über die gleiche Eignung kann allerdings noch keine zutreffende Aussage gemacht werden, da es an einer verlässlichen Datenbasis fehlt.[85] Auch die Stellungnahme der Bundesregierung spricht dieses Verfahren als mögliche Alternative an, verneint jedoch die gleiche Eignung, da die nicht zu Abrechnungszwecken benötigte Daten wieder gelöscht werden und dann nicht mehr eingefroren werden können, und weil die „Quick-Freeze“ Anordnungen in der Regel nur den Geschäftszeiten der Unternehmen und damit weder nachts noch am Wochenende erfolgen.[86]

Da eine klare Aussage zur Erforderlichkeit nach dem derzeitigen Stand somit nicht klar getätigt werden kann, wird diese zusammen mit der ebenfalls in Zweifel stehenden Geeignetheit im Rahmen der sich anschließenden Angemessenheitsprüfung weitere

81 Pieroth/Schlink 2008, Rn 285.
82 Breyer, StV 2007, 214, 218.
83 Westphal, EuR 2006, 706, 715.
84 Stellungnahme der Bundesregierung vom 28. November 2008, 53.
85 https://www.datenschutzzentrum.de/material/tb/tb27/kap04_2.htm (Zugriff: 28.06.09).
86 Stellungnahme der Bundesregierung vom 28. November 2008, 56.

Berücksichtigung finden.

(4) Angemessenheit

Die Angemessenheit wird anhand des Verhältnismäßigkeitsgrundsatzes geprüft, wonach Eingriff und verfolgter Zweck nicht außer Verhältnis zueinander stehen dürfen.[87] Gegenüber stehen sich das öffentliche Interesse an einer wirksamen Strafverfolgung und der Eingriff in das Fernmeldegeheimnis. Zwar hat das Bundesverfassungsgericht Sicherheit bereits als ein Gut mit Verfassungsrang bezeichnet und dessen Bedeutung besonders hervorgehoben[88], es hat aber auch die freie Kommunikation einer Gesellschaft „als elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens“ bezeichnet.[89] Die Bundesregierung nennt in ihrer Stellungnahme einige vom Bundesverfassungsgericht entwickelte Indikatoren, anhand derer die Angemessenheit bewertet werden kann: dazu gehören unter anderem (1) die „Streubreite“ der Maßnahme, (2) die Zulässigkeit einer Vorratsdatenspeicherung, (3) der Umfang und die Sensibilität der erfassten Informationen, (4) die Heimlichkeit der Maßnahme und (5) die verfassungsrechtlichen Grenzen einer solchen Speicherung.[90] Diese sollen hier nicht den ausschließlichen Maßstab der Verhältnismäßigkeitsprüfung bilden; sie stellen aber eine wichtige Orientierung dar, anhand derer die Abwägung vorgenommen werden kann.

(a) Möglichkeiten der Umgehung

Das ein öffentliches Interesse an einer wirksamen Strafverfolgung besteht ist sicherlich unbestritten. Es ist jedoch zu prüfen, wie gut dieses Ziel anhand der Vorratsdatenspeicherung zu erreichen ist, denn es müssen daran zumindest insoweit ernsthafte Zweifel bestehen, als das die Gefahr besteht, dass die Datenspeicherung gerade von denen umgangen wird, deren kriminelles Vorgehen sie aufzudecken bezweckt. Nach Oliver Sürne, Vorstand Recht und Regulierung des Verbandes der deutschen Internetwirtschaft ist die Vorratsdatenspeicherung „leicht zu umgehen“[91] und betrifft damit gerade diejenigen, die nicht das technische Know-how haben, um sich dieser zu entziehen. Die Menschen dagegen, die es darauf anlegen, nicht entdeckt zu

87 BVerfGE 100, 313, 375 f.
88 BVerfGE 49, 24, 56 f.
89 BVerfGE 65, 1, 43.
90 Stellungnahme der Bundesregierung vom 28. November 2008, 57.
91 http://www.pcpraxis.de/index.php?option=com_content&view=article&id=2275&catid=178 (Zugriff: 12.06.09).

werden, werden alle zur Verfügung stehenden technischen Maßnahmen einsetzen, so dass die Vorratsdatenspeicherung wenn überhaupt nur begrenzten Nutzen für die Strafverfolgung haben kann. Sich der Möglichkeiten zur Anonymisierung nicht zu bedienen wäre für Terroristen so offensichtlich leichtsinnig, dass es kaum als realistische Option in Betracht kommen dürfte. Zumal organisierte Täter grundsätzlich sehr viel professioneller vorgehen und bereit sind, höheren Aufwand zu betreiben, um ihr Ziel zu erreichen. Deshalb ist anzunehmen, dass sich diese einer Identifizierung entziehen werde und das die Vorratsdatenspeicherung kein geeignetes Mittel ist, um dagegen vorzugehen. Wahrscheinlich ist folglich, dass sich ein Nutzen vor allem bei Fällen der kleineren und mittleren Kriminalität ergibt und gerade das ist eben nicht das vorgegebene Ziel der Vorratsdatenspeicherung. Das diese Argumentation nicht nur reine Spekulation ist, zeigt der Fall der sog. „Sauerland Terroristen“, die den Kontakt zum Terrornetzwerk *Islamische Dschihad Union* über identifizierungsfreie Internetverbindungen aufgenommen haben.[92]

Die Möglichkeiten, die Datenspeicherung zu umgehen, sind zahlreich, so kann man etwa Proxy-Server oder Anonymisierungsdienste nutzen. Bei der Versendung von EMails besteht die Möglichkeit auf EMail-Server im außereuropäischen Ausland zurück zu greifen und mit diesen über TLS oder SSL verschlüsselt kommunizieren, ohne das EMail-Verbindungsdaten beim jeweiligen europäischen Internet Service Provider gespeichert werden können. Auch die IP-Telefonie kann durch das Einrichten eigener Telefonanlagen mit bestimmter Software der Speicherung von Verbindungsdaten entgehen.[93] Für das Mobiltelefon reicht es, eine Telefonkarte zu benutzen. Anrufe vom Hoteltelefon oder anderen externen Telefonen können ebenfalls nicht zugewiesen werden. So müssen beim Kauf von SIM-Karten häufig keine Personalien angegeben werden.

Die Bundesregierung verweist hinsichtlich dieser Problematik darauf, dass die Argumentation der Beschwerdeführer widersprüchlich sei, weil diese einerseits die Eignung der Vorratsdatenspeicherung aufgrund der Möglichkeiten zur Anonymisierung in Frage stellten, andererseits aber die Anwendung der gesetzlichen Regelung auf Anonymisierungsdienste kritisierten.[94] Damit verbunden ist jedoch die Befürchtung eines deutlichen Rückgangs von Anonymisierungsdiensten aufgrund der erheblichen zu

92 http://www.stern.de/politik/deutschland/:Anti-Terror-Kampf-BKA-Gro%DFen-Sp%E4hangriff/604785.html (Zugriff: 11.06.09).
93 http://de.indymedia.org/2007/01/165957.shtml (Zugriff: 11.06.09).
94 Stellungnahme der Bundesregierung vom 28. November 2008, 50.

speichernden Datenmengen[95] und des in der Folge erschwerten Zugangs. Grundsätzlich ist es als problematisch anzusehen, wenn der Bürger, gerade wenn es um besonders vertrauliche Daten geht, diese auf Vorrat speichern lassen muss und wenn ihm vordergründig gesetzlich dann auch noch die Möglichkeit genommen wird, sein Kommunikationsverhalten zu anonymisieren. Das tatsächlich auch weiterhin noch die Möglichkeit einer Anonymisierung besteht, ist von der Kritik am Gesetzgeber ganz klar zu trennen. Denn Möglichkeiten die Vorratsdatenspeicherung zu umgehen gibt es trotzdem genügend, so dass an den Zweifeln zur Eignung dieser Maßnahme auch weiterhin festzuhalten ist. Tatsächlich besteht damit kein Widerspruch, wenn man die Kritik an der Anwendung der gesetzlichen Regelung auch auf Anonymisierungsdienste von der Eignung der Vorratsdatenspeicherung zur Zielerreichung trennt.

Als weiteres Argument führt die Bundesregierung an, dass das Bundesverfassungsgericht in seiner Entscheidung vom 14. Juli 1999 die Geeignetheit strategischer Überwachung bejaht hat, weil die Möglichkeit der Verschlüsselung nach Angaben der Bundesregierung nur relativ wenig genutzt wird.[96] Auf empirische Daten wird dabei jedoch nicht verwiesen, so dass unklar bleibt, in welchem Umfang die Nutzung tatsächlich erfolgt ist. Dieser Argumentation kann zudem schon deshalb nicht gefolgt werden, weil die Nutzung des Internets ebenso wie das Angebot an Anonymisierungsdiensten in den neunziger Jahren noch vollkommen anders war und nicht mit der heutigen Situation vergleichbar ist. So funktionierten die zur Anonymisierung genutzten Tools Ende der neunziger Jahre noch nur dienstespezifisch, z.B. für EMails, ohne dass nach außen hin eine Möglichkeit der anonymisierten Identifikation mit dem tatsächlich ablaufenden Dienst möglich war.[97] Die Möglichkeiten zur Anonymisierung haben sich seitdem ständig erweitert, auch weil der Bedarf danach stetig gewachsen ist, so dass sich daraus ergebende Zweifel an der Geeignetheit der Vorratsdatenspeicherung auch weiterhin in jedem Fall berechtigt sind.

(b) Notwendigkeit der Vorratsdatenspeicherung

Ein weiterer Grund der zu Zweifeln an der Vorratsdatenspeicherung berechtigt, ist die Tatsache, dass empirisch bisher noch nicht belegt ist, dass geringere Eingriffsbefugnisse auch eine höhere Kriminalitätsrate nach sich ziehen. Im Umkehrschluss kann auch keine Senkung des Kriminalitätsniveaus erwartet werden, soweit weitergehende

95 http://www.heise.de/newsticker/TOR-Server-durch-Vorratsdatenspeicherung-von-Schliessung-bedroht--/meldung/100649 (Zugriff: 15.06.09).
96 BVerfGE 100, 313, 374 f.
97 https://www.datenschutzzentrum.de/projekte/anon/1zwwau.htm (Zugriff: 02.07.09).

Ermittlungsbefugnisse zugestanden werden, obwohl gerade dies von Politikern behauptet wird. Verschiedene Beispiele zeigen, dass auch wenn die Telekommunikationsüberwachung erheblich seltener zum Einsatz kommt, kein erkennbarer Rückgang der Sicherheit zu verzeichnen ist.[98] Dabei muss auch beachtet werden, dass eine präventive Durchsuchung der Datenbestände auf bestimmte Merkmale hin, die geeignet sind das Vorliegen einer Gefahr zu indizieren, wenig erfolgversprechend ist, weil sich Terroristen meistens gerade dadurch auszeichnen, dass sie vollständig integriert leben[99] und damit häufig gar nicht anhand äußerer Merkmale identifizierbar sind. Von Bedeutung kann eine Vorratsdatenspeicherung deshalb nur dann sein, wenn bereits eine Straftat vorliegt. Sie hilft dabei, Kommunikationsvorgänge nachvollziehbar zu machen. Dabei muss sie sich allerdings die Frage gefallen lassen, wie häufig ein Zugriff auf diese Daten überhaupt notwendig ist. Da es in der Praxis zudem nur wenig Fälle gibt, in denen ein Auskunftsverlangen daran scheiterte, dass die Daten bereits gelöscht wurden, muss generell bezweifelt werden, ob eine Vorratsdatenspeicherung nennenswerten Nutzen für die staatliche Aufgabenerfüllung entfalten kann.[100] Repräsentative wissenschaftliche Studien zur Abfrage von Telekommunikationsdaten liegen bisher kaum vor, was angesichts der sicherheitspolitischen Einschätzung verwunderlich erscheint.[101] Untersuchungen haben jedoch ergeben, dass die Art der Daten, die von den Diensteanbietern für eigene Zwecke gespeichert werden, auch für Zwecke der Strafverfolgung ausreichend sind. So hätten zwei Drittel der dort untersuchten Fälle auch ohne die Abfrage der Verkehrsdaten aufgeklärt werden können.[102] Das sich die Abfrage der Strafverfolgungseinrichtungen in Schweden und England überwiegend auf einen Zeitraum von nur drei Monaten konzentrieren, wurde bereits bei der Geeignetheit angeführt. In Deutschland nennt das Bundeskriminalamt 381 Ermittlungsverfahren, in denen Behörden Verbindungsdaten fehlten,[103] was gemessen an der Anzahl der Gesamtstraftaten ein verschwindend geringer Anteil ist. Das Gutachten des Max-Planck-Instituts für ausländisches und internationales Strafrecht kommt letztlich zu dem Schluss, dass „der Bedarf zur Einführung einer Vorratsdatenspeicherung auf der Grundlage der beobachteten

98 Breyer 2005, 23.
99 Follath, Der Spiegel 2006, 94.
100 Verfassungsbeschwerde Vorratsdatenspeicherung vom 31.12.2007, 15.
101 Albrecht/Grafe/Kilchling 2008, 80.
102 Albrecht/Grafe/Kilchling 2008, 83.
103 Mahnken, http://www.vorratsdatenspeicherung.de/images/bka_vorratsdatenspeicherung.pdf. (Zugriff: 05.06.09).

Praktiken bezweifelt“ werden muss.[104]

Die in der Stellungnahme der Bundesregierung aufgeführten Einzelfälle, bei denen die Speicherung von Daten auf Vorrat notwendig war,[105] können eine Aufzeichnung der Kommunikationsdaten aller am Fernmeldeverkehr teilnehmenden nicht rechtfertigen. Begründet dargelegt werden könnte der Eingriff in das Fernmeldegeheimnis nur dann, wenn sich aus repräsentativen Studien wirklich ergeben würde, dass die flächendeckende Speicherung von Kommunikationsdaten zu einer wesentlichen Verbesserung der öffentlichen Sicherheit führen würde. Einen solchen Nachweis bleibt die Bundesregierung jedoch schuldig. Die Aufzählung von Einzelfällen kann hierfür kein Ersatz sein. Zu diesem Ergebnis kommt auch das Gutachten des Max-Planck Instituts, wenn es feststellt: “Weit verbreitet ist im Kontext des Gesetzgebungsprozesses die Einzelfallanalyse, die freilich Grundlagen für eine begründete Entscheidung nicht liefern kann.“[106]

Soweit es speziell um den Zugriff auf Daten nach § 113a TKG geht, verweist die Bundesregierung darauf, dass in 43 % der Strafverfahren auf solche Daten zurückgegriffen wurde und dabei 7,5 % der Anordnungen erfolglos blieben, weil die Diensteanbieter die Speicherungspflichten nach § 113a TKG zu diesem Zeitpunkt noch nicht erfüllten.[107] Das Gutachten des Max-Planck Instituts stellt hierzu jedoch zutreffend fest, dass repräsentative wissenschaftliche Studien zu Ergebnissen der Abfragen und Auskünfte von Telekommunikationsdaten sowie zu den Folgen der Abfrage bisher noch nicht vorliegen.[108] Zwar sei es richtig, dass die quantitative Bedeutung der Verkehrsdatenabfrage erheblich ist, die empirischen Befunde verwiesen jedoch darauf, dass die Nutzung von Telekommunikationsverkehrsdaten auf kurze Zeiträume konzentriert ist.[109]

Auch der Umfang der Datenspeicherung erscheint nicht angemessen. So betreffen die meisten Auskunftsersuchen Telefonverbindungsdaten, während Internetdaten nur zu einem sehr geringen Teil abgefragt werden, der in keinem Verhältnis zu den Kosten der Diensteanbieter steht.[110] Sieht man sich die Zahlen der Zugriffe von Strafverfolgungsbehörden auf gespeicherte Daten an, so zeigt sich, dass im

104 Albrecht/Grafe/Kilchling 2008, S. 84.
105 Stellungnahme der Bundesregierung vom 28. November 2008, 43 ff.
106 Albrecht/Grafe/Kilchling 2008, 400.
107 Stellungnahme der Bundesregierung vom 28. November 2008, 52.
108 Albrecht/Grafe/Kilchling 2008, 80.
109 Albrecht/Grafe/Kilchling 2008, 400.
110 Verfassungsbeschwerde Vorratsdatenspeicherung vom 31.12.2007, 68.

Internetbereich von T-Online nur 0,0004 % der dort insgesamt anfallenden Telekommunikationsdaten abgefragt werden.[111]

Insgesamt gesehen bestehen an dem verfolgten Zweck, der Strafverfolgung an sich, damit bereits erhebliche Zweifel, was die Eignung und Wirksamkeit der Maßnahme angeht. Dem ist im Folgenden der Eingriff in das Fernmeldegeheimnis gegenüber zu stellen und die Gewichtung zu prüfen.

(c) Umfang der Vorratsdatenspeicherung

Ein Indikator an dem sich die Schwere des Eingriffs festmachen lässt, ist die „Streubreite" einer Maßnahme. Dieses Kriterium fällt danach häufig mit dem Kriterium der Anlasslosigkeit zusammen, da diese in der Regel einen großen Adressatenkreis zur Folge hat.[112] Bei der Vorratsdatenspeicherung handelt es sich um eine verdachtslose Maßnahme, von der alle Personen betroffen sind, die sich der Fernmeldetechnik bedienen, ohne dass diese den Eingriff in ihre subjektiven Rechte durch ihr Verhalten in irgendeiner Weise veranlasst haben.[113] Damit ist quasi jede Telekommunikation beeinträchtigt. Der Umstand, dass zum größten Teil Personen betroffen sind, die sich nichts haben zu Schulden kommen lassen dürfte hinsichtlich der Eingriffsintensität besonders schwer wiegen.[114]

Auch die Bundesregierung bestätigt zunächst die größere Eingriffstiefe durch die umfassende Streubreite[115], sieht aber gleichzeitig auch die Möglichkeit, dass eine gesetzliche Maßnahme die viele Personen ohne Rücksicht auf individuelles Verhalten betrifft, auch für eine geringere Eingriffsintensität sprechen kann, weil dieses indiziere, dass der Gesetzgeber gerade nicht die individuelle Freiheitswahrnehmung in einer besonders intensiven Art und Weise einschränke.[116] Dem ist zu entgegnen, dass die Intensität einer Maßnahme schließlich nicht von der Anzahl der Betroffenen abhängt. Nur weil die Freiheitswahrnehmung nicht individuell, sondern kollektiv eingeschränkt wird, wiegt dieses für jeden Einzelnen nicht weniger schwer. Die Annahme der Bundesregierung ist folglich im Falle der Vorratsdatenspeicherung nicht zutreffend.

(d) Rechtsprechung des Bundesverfassungsgerichts

Was das Kriterium der verfassungsrechtlichen Zulässigkeit angeht, stellt die

111 Uhe/Herrmann 2003, 161.
112 BVerfGE 100, 313, 376, 392.
113 Korn HRRS 2009, 123.
114 Verfassungsbeschwerde Vorratsdatenspeicherung vom 31.12.2007, 73.
115 Stellungnahme der Bundesregierung vom 28. November 2008, 59 f.
116 Stellungnahme der Bundesregierung vom 28. November 2008, 60.

Bundesregierung die Unterschiede der Vorratsdatenspeicherung zu früheren Entscheidungen des Bundesverfassungsgerichts zum Datenschutz, zum Beispiel die Entscheidung zur Rasterfahndung in Nordrhein-Westfalen oder das Urteil zur Volkszählung, heraus. Das wesentliche Argument dabei ist, dass dem Staat die Daten bei diesen Fällen ohne das Dazwischentreten weiterer rechtlicher Anforderungen zur Verfügung standen, während die Speicherungspflichten durch § 113b TKG mit einer Zweckbestimmung versehen worden seien und zudem stets mit einer weiteren Befugnisnorm verknüpft werden müssten, die erst die staatliche Kenntnisnahme gestatte. Auch könne aus den bisherigen Äußerungen des Bundesverfassungsgerichts zur Vorratsdatenspeicherung nicht automatisch auf die Verfassungswidrigkeit der zu prüfenden Normen geschlossen werden.[117] Diese Feststellung ist hier genau so zutreffend wie die Tatsache, dass aus der Zweckbindung des § 113b TKG genau so wenig auf eine automatische Verfassungskonformität geschlossen werden kann. Die bisherige Rechtsprechung des Bundesverfassungsgerichts soll schließlich lediglich dazu dienen, die Argumentation zu stützen und im besten Falle eine mögliche Richtung in dieser Entscheidung vorzugeben. Ein endgültiges Urteil kann damit ebenso wenig vorweggenommen werden, wie eine für ewig geltende Festlegung.

Insbesondere das Volkszählungsurteil vom 15. Dezember 1983 lässt jedoch grundsätzliche Leitlinien des Bundesverfassungsgerichts erkennen. Darin heißt es: “Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet und weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, dass etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und dass ihm dadurch Risiken entstehen können, wird möglicherweise auf die Ausübung seiner entsprechenden Grundrechte verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.“[118] Diese Grundsätze sind unabhängig von weiteren rechtlichen Anforderungen auch auf die Vorratsdatenspeicherung anwendbar, da sich damit die Gefahr einer Speicherung von Daten, die auf solche Handlungsweisen und Ereignisse schließen lassen, die vor diesem Hintergrund möglicherweise eher einen Verzicht auf

117 Stellungnahme der Bundesregierung vom 28. November 2008, 61 f.
118 BVerfGE 6, 1 ff.; NJW 1984, 419 ff.

die Grundrechtsausübung zur Folge haben, konkretisiert. Die Folgen für eine demokratische Gesellschaft dürften daher erheblich sein.

(e) Das Kriterium der Heimlichkeit und die Betroffenheit der Menschenwürde

Hinsichtlich der Heimlichkeit der Maßnahme ist die Bundesregierung der Meinung der Eingriff sei abgeschwächt, weil die Speicherung als solche nicht heimlich erfolge.[119] Das ist zwar richtig, vor dem Hintergrund einer gesetzlich angeordneten Speicherung der Daten all jener, die sich der Telekommunikation bedienen, aber auch offensichtlich. Schließlich stellt die pauschale Speicherung gerade das Problem dar und ist ein Kernaspekt der Verfassungsbeschwerde. Folgt man der Auffassung der Bundesregierung, so wäre eine tägliche, anlasslose und offene Hausdurchsuchung bei der gesamten Bevölkerung weniger eingriffsintensiv als die Gefahr einer heimlichen Wohnungsdurchsuchung in besonderen Verdachtsfällen.[120] Auch unter dem Gesichtspunkt der Zumutbarkeit erscheint die Speicherung problematisch. Die Frage, ob es Menschen zugemutet werden darf, ihr Verhalten auf staatliche Überwachung auszurichten, lässt erhebliche rechtsstaatliche Bedenken aufkommen.

Ein weiterer Punkt, der die Schwere des Eingriffs betrifft ist die Tatsache, dass alle Betroffenen identifizierbar sind, da die gespeicherten Daten personenbezogen sein müssen, um für die Strafverfolgung genutzt werden zu können. Wenn in dieser Weise Menschen zum bloßen Objekt staatlicher Sicherheitsbedürfnisse herabgewürdigt werden, dürfte auch eine Verletzung der grundrechtlich geschützten Menschenwürde (Art. 1 Abs. 1 GG) gegeben sein.[121] Auch diesbezüglich ist die Bundesregierung anderer Meinung. Diese sieht den „Kernbereich privater Lebensgestaltung“[122] nicht berührt. Die bloße Abfrage von Verkehrsdaten sei nicht ausreichend, um an derart sensible Informationen für die Persönlichkeit zu kommen. Auch im Falle einer möglichen Profilerstellung des Kommunikations- und Bewegungsverhaltens könne unter Verzicht auf die Inhalte der Kommunikation der Kernbereich der persönlichen Lebensgestaltung nicht betroffen und eine Verletzung der Menschenwürde nicht erfolgt sein.[123] Die nachfolgenden Ausführungen zeigen jedoch, dass von Kommunikationsdaten häufig auch auf deren Inhalt geschlossen werden kann, so dass Verkehrsdaten nicht zwingend weniger aussagekräftig sind als die Inhalte einer Kommunikation.[124] Es erscheint

119 Stellungnahme der Bundesregierung vom 28. November 2008, 40.
120 Starostik, Meinhard: Schriftsatz vom 23. Februar 2009, 20.
121 Vgl. dazu BVerfGE 87, 209 ff.
122 BVerfGE 109, 279, 313 ff.
123 Stellungnahme der Bundesregierung vom 28. November 2008, 110 f.
124 Korn, HRRS 2009, 123.

demnach zu einfach, eine Berührung des Kernbereichs generell auszuschließen, nur weil keine Inhalte gespeichert werden. So ist beispielsweise ein Anruf bei einer Drogenberatungsstelle ohne Zweifel eine hochsensible Angelegenheit, die nicht einfach mit dem Verweis auf fehlende Inhaltsdaten abgetan werden kann.

Grundsätzlich steht bei der heimlichen Verwendung die Wahrscheinlichkeit, dass ein Missbrauch erkannt wird, in keinem Verhältnis zum potenziellen Schaden. Missbrauchsfälle sind bei heimlich operierenden Systemen nicht überraschend, da für denjenigen, der Entdeckung oder Strafe nicht zu befürchten hat, die Schwelle Verbindungsdaten auch zu anderen, als den rechtlich vorgesehenen Zwecken zu nutzen, ungleich niedriger ist. Außerdem wissen die Betroffenen bei geheim konzipierten Systemen nicht, wie ihre Daten abgerufen werden, so dass sie sich gegen einen Missbrauch zunächst gar nicht zur Wehr setzen könnten.

(f) Fehlende Gefahrennähe

Bei der Schwere des Eingriffs ist auch auf die Gefahrennähe abzustellen. Der Freiheitsanspruch des Einzelnen verlangt dabei, dass er von solchen Maßnahmen verschont bleibt, die keine hinreichende Beziehung zwischen ihm und dem zu schützenden Rechtsgut aufweisen.[125] Eine solche Gefahrennähe ist bei der Vorratsdatenspeicherung nicht erkennbar. Stattdessen wird ein Generalverdacht statuiert, der keinen Bezug mehr zur strafprozessualen Unschuldsvermutung als Ausprägung des Rechtsstaatsprinzips hat.[126] So hat das Bundesverfassungsgericht bereits festgestellt, dass ein konkreter Tatverdacht Voraussetzung für die Erhebung von Verbindungsdaten ist. [127] Ein solcher fehlt bei der Vorratsdatenspeicherung aber genauso wie jeder sonstige Bezug zu einer Gefahrenquelle. Damit liegt auch ein Verstoß gegen das aus dem Rechtsstaatsprinzip resultierende Verbot unnötiger Eingriffe vor.[128]

Es ist folglich anzunehmen, dass ein Eingriff, der eine so große Anzahl von Personen ohne konkreten Tatverdacht betrifft, ohne dass zudem noch eine Gefahrennähe vorliegt, eine hohe Eingriffsintensität aufweist. Zumal die Telekommunikation im Gegensatz zu anderen Überwachungsmaßnahmen, die häufig in öffentlichen Räumen stattfinden gerade im geschützten Raum stattfindet, in dem eigentlich von der Vertraulichkeit der Transaktionen ausgegangen wird.

---

125 So auch LT-Drs. Mecklenburg-Vorpommern 4/2116, 37.
126 BVerfGE 74, 370 .
127 BVerfGE 107, 299, 322.
128 BVerfGE 17, 306, 313 f.; BVerfGE 30, 250, 263.

(g) Die strafrechtliche Problematik der Generalprävention

Ein weiterer ganz wesentlicher Punkt ist die Bedeutung, die eine präventive Speicherung von Daten für das Strafrecht hat. Obwohl bereits der Ausdruck „Strafverfolgung“ ein nachträgliches Moment enthält, wird die Speicherung ohne konkreten Verdacht vorgenommen. Das widerspricht auch dem klassischen Verständnis des Strafrechts, wonach „sich die Strafe aus sich selbst, aus ihrem Gleichmaß mit dem Verbrechen auf das sie Antwort war“ rechtfertigt „und sich nicht aus ihren heilenden Wirkungen auf [...] die möglichen Verbrecher von morgen (Generalprävention, Abschreckung)“ bemisst.[129] Vor dem Hintergrund der Terrorismusbekämpfung soll dem Strafrecht heute eine immer stärker präventive Funktion zukommen und es soll damit als Agent für die bürgerliche Sicherheit dienen. Eine klassische Anschauung des Strafrechts hätte dagegen keine strafrechtlichen Maßnahmen in das Vorfeld eines Tatverdachts verlängert und damit auch auf ganz unbeteiligte Personen erstreckt, wie es durch die alle Personen unter einen Generalverdacht stellende Vorratsdatenspeicherung der Fall ist. Es hätte auch nicht mit dem Paradigma der Sicherheit operiert und sich nicht grundrechtsorientierter Kritik aussetzen müssen.[130] Das Ziel polizeilicher Arbeit wandelt sich von der Straftatenverfolgung zur vorbeugenden Risikobekämpfung.[131] Es stellt sich letztlich auch in Verbindung mit der Vorratsdatenspeicherung die Frage, ob langfristig die hohen Erwartungen an die Wirksamkeit der präventiven Maßnahmen zur Erfüllung von Sicherheitsinteressen überhaupt erfüllt werden können.

(h) Mögliche gesellschaftliche Folgen eines veränderten Kommunikationsverhaltens

Im Rahmen der Abwägung müssen auch die Ängste der Bürger mit einbezogen werden, da diese schon im Vorfeld zu einer „Befangenheit in der Kommunikation, zu Kommunikationsstörungen und Verhaltensanpassungen […] führen“.[132] Aufgrund des Risikos ständig auch mit missbräuchlichem Umgang der Daten durch die Diensteanbieter, aber auch den Staat rechnen zu müssen, geht die Unbefangenheit der Kommunikation automatisch verloren.[133] Eine solche Entwicklung wäre jedoch kontraproduktiv für eine demokratische Gesellschaft, die auf eine offene Kommunikation und den Austausch von Meinungen angewiesen ist.[134] Zumal es unbeobachtete Telekommunikation praktisch nicht mehr gäbe. Auch in diesem Punkt ist

129 Hassemer, HRRS 2006, 131 f.
130 Hassemer, HRRS 2006, 133.
131 Hirsch, DuD 2008, 89.
132 BVerfGE 100, 313, 376.
133 https://www.datenschutzzentrum.de/allgemein/061004_vdspeicherung.htm (Zugriff: 13.06.09).
134 Birnbaum, FS Iring Fetscher (2002), 156.

die Vorratsdatenspeicherung damit als eher belastungsintensiv einzustufen.

Die Bundesregierung sieht die Gefahr einer Einschüchterung dagegen nicht. Zudem könne bei der rechtlichen Einordnung einer solchen Wirkung nicht allein auf das subjektive Empfinden der Adressaten abgestellt werden. Des Weiteren könne nur dann eine abschreckende Wirkung als Eingriff erzeugt werden, wenn diese dem Gesetzgeber zuzurechnen wäre.[135] In ihren Ausführungen führt die Bundesregierung ausschließlich Beispiele der Kritiker der Vorratsdatenspeicherung an und macht deutlich, dass sie zumindest vom Gesetz her, keine abschreckende Wirkung erkennen kann. Wirkungen die aus politischen Kampagnen resultieren seien dagegen von vornherein nicht relevant. Sie unterstellt den Beschwerdeführern selber zu der Einschüchterung beizutragen, die diese durch das Gesetz realisiert sehen, um seine Aufhebung zu erwirken. Die Bundesregierung führt weiter aus, dass die angegriffene Regelung gar keinen staatlichen Zugriff auf die gespeicherten Daten gestatte, da es hierzu einer weiteren Zugriffsnorm bedürfe. Auch bestehe bei einer Speicherpflicht von sechs Monaten keine Gefahr, dass die gespeicherten Daten in einer nicht voraussehbaren Art und Weise verwendet werden. Sowieso könnten sich die Kommunikationsteilnehmer schließlich darauf einrichten, unter welchen Bedingungen eine Datenabfrage rechtlich möglich sei. Der Zugriff auf alle Daten sei damit weit davon entfernt, eine abschreckende Wirkung auf das Kommunikationsverhalten zu entfalten. Auch die berufliche Kommunikation sei nicht gefährdet, da die Möglichkeit der offenen Kommunikation nicht durch eine Regelung beschränkt werde, die lediglich eine Speicherung von Daten vorsehe, ohne den Zugriff zu regeln.[136]

Es stellt sich die Frage, auf wen bzgl. des Einschüchterungseffektes abgestellt werden soll, wenn nicht auf den Adressaten. Das dieser vor allem aus politischen Kampagnen resultiere ist zudem nicht richtig. Denn dort geht es lediglich darum, über mögliche Gefahren aufzuklären. Diese haben kein Motiv noch zusätzliche Ängste zu schüren. Dafür ist die Masse derjenigen, die im Zusammenhang mit der Vorratsdatenspeicherung auf mögliche Folgen für eine freie Kommunikation aufmerksam machen, auch viel zu breit gestreut und nicht auf politische Organisationen beschränkt. Das die Speicherung und eventuelle spätere Verwendung von Daten das Kommunikationsverhalten, gerade soweit es um besonders vertrauliche Daten geht, beeinflussen kann, liegt schließlich auf der Hand. Hätte dieses keine abschreckende Wirkung auf die Betroffenen, so könnte

135 Stellungnahme der Bundesregierung vom 28. November 2008, 69 f.
136 Stellungnahme der Bundesregierung vom 28. November 2008, 69 ff.

man sich letztlich auch die Debatte um Anonymisierungsdienste sparen, weil darin schlicht und ergreifend keine Notwendigkeit gesehen würde. Ein weiterer Punkt ist außerdem, dass die Globalisierung dazu führt, dass Menschen an verschiedenen Orten auf der Welt arbeiten und darauf angewiesen sind, enge persönliche Gespräche über das Telefon oder das Internet zu führen. Das Fernmeldegeheimnis wird damit immer wichtiger, gleichzeitig findet jedoch eine zunehmende Eingriffsdichte statt.
Das die Kommunikationsteilnehmer sich darauf einrichten können, wann rechtlich eine Datenabfrage vorgenommen werden kann, ist zwar richtig, das Paradoxon liegt jedoch darin, dass sie nur anhand von Anonymisierungsmaßnahmen dagegen vorgehen können, was dem Ziel der Vorratsdatenspeicherung wiederum zuwider laufen würde. Insgesamt erscheint es nicht unwahrscheinlich, dass eine Vorratsdatenspeicherung zu Kommunikationsanpassungen führen könnte.[137] Der Schaden der dadurch für eine freie demokratische Gesellschaft entsteht, dürfte damit größer sein als der Effizienzgewinn infolge einer zunehmenden Überwachung. Und auch wenn es einer weiteren Zugriffsnorm bedarf, ergibt sich aus § 113b TKG doch klar, dass die gespeicherten Daten unter den in Nr. 1-3 genannten Voraussetzungen an die zuständigen Stellen übermittelt werden können, soweit es in den gesetzlichen Bestimmungen vorgesehen und im Einzelfall angeordnet ist. Das dieses auch Auswirkungen auf die Kommunikation zumindest in Berufsgruppen haben kann, die mit besonders sensiblen Daten zu tun haben, kann nicht von der Hand gewiesen werden, da die Speicherung gerade eine effektivere Strafverfolgung und damit einen Zugriff auf Daten zum Zweck hat. Genauso wenig richtig ist, dass bei einer Speicherpflicht von sechs Monaten keine Gefahr besteht, dass die Daten in einer nicht vorhersehbaren Art und Weise verwendet werden. In sechs Monaten kann genauso eine missbräuchliche Verwendung stattfinden, wie in einem längeren Zeitraum.

(i) Gefahr einer missbräuchlichen Verwendung der gespeicherten Daten

Auf die Gefahr einer missbräuchlichen Verwendung, auch zu kommerziellen Zwecken, geht die Bundesregierung dagegen nicht weiter ein, obwohl die Datenskandale der letzten Zeit haben deutlich werden lassen, dass es sich hierbei nicht um eine abstrakte Gefahr handelt und schon gar nicht um eine Angst, die nur von politischen Kampagnen geschürt wird, sondern dass diese ganz real ist und jederzeit Wirklichkeit werden kann. Gerade kleinere Provider sind in der Regel mit weniger geschulten Fachkräften

137 http://www.vorratsdatenspeicherung.de/content/view/29/79/lang,de/ (Zugriff: 13.06.09).

ausgestattet, so dass es noch schwieriger ist, eine entsprechende Datensicherheit zu gewährleisten. Diese sind zudem auch noch unverhältnismäßig hoch von der finanziellen Belastung betroffen.

Die erhebliche Menge an zu speichernden Daten wird es nach Einschätzung der Diensteanbieter zudem extrem schwierig machen, die entsprechende Datensicherheit zu gewährleisten. Das Wissen um die gespeicherten Daten weckt mit großer Wahrscheinlichkeit Begehrlichkeiten der Wirtschaft, gerade aufgrund des hohen kommerziellen Werts, den diese Daten haben können, insbesondere wenn es um das Erstellen von Persönlichkeitsprofilen geht. Mit einem missbräuchlichen Umgang der Daten ist aber nicht nur zu rechnen, soweit es um Werbemaßnahme geht. Wirtschaftlich könnten diese beispielsweise für ein Unternehmen, dass gentechnisch veränderte Futtermittel anbietet interessant sein, wenn es um Personen geht, die in einer Umweltschutzgruppe von zentraler Bedeutung sind.[138] Gerade für kleinere Unternehmen könnten sich lukrative Geschäfte ergeben, aber auch bzgl. größerer Unternehmen sind solche Bedenken ernst zu nehmen. Es besteht damit die Gefahr, dass Daten vorsätzlich oder unbeabsichtigterweise in die falschen Hände geraten. Selbst unter der Annahme, dass die Verbindungsdaten bei den Providern – auch vor Kriminellen – sicher gespeichert sind, müssen sich deutsche Behörden die Frage gefallen lassen, ob sie überhaupt zu einer sicheren Verwahrung der Daten in der Lage sind.[139] Der Verlust einer erheblichen Menge von Daten im Bundesinnenministerium 2008 legt zumindest einen anderen Schluss nahe.[140] Leider besteht diese Gefahr nicht nur bei Behörden, sondern auch in der Wirtschaft. Im Oktober 2008 publizierte zum Beispiel T-Mobile siebzehn Millionen Kundendatensätze versehentlich im Internet.[141] Ein wirklich effektiver Schutz vor Missbräuchen wäre demnach nur gegeben, wenn es zur Speicherung der Daten gar nicht erst käme.

Die Bundesregierung erwähnt in diesem Zusammenhang einzig die Missbrauchsfälle bei der Deutsche Telekom AG, allerdings mit dem Argument, dass die Missbrauchsgefahr nicht durch die §§ 113a, b TKG ermöglicht oder erleichtert würde.[142] Belegt wird damit jedoch, dass eine Missbrauchsgefahr überhaupt besteht und das diese umso größer ist, desto besser Rückschlüsse auf den Inhalt möglich sind. Im Übrigen ist davon auszugehen, dass nur ein Bruchteil aller Datenschutzverletzungen öffentlich wird

138 Kurz/Rieger 2009, 11.
139 Kurz/Rieger 2009, 40 ff.
140 http://computer.t-online.de/c/14/84/66/82/14846682.html (Zugriff: 02.07.09).
141 http://www.spiegel.de/wirtschaft/0,1518,581938,00.html (Zugriff: 02.07.09).
142 Stellungnahme der Bundesregierung vom 28. November 2008, 87 f.

und die Dunkelziffer sehr viel höher liegt.

Da die Ausübung der meisten Grundrechte einen Informationsaustausch notwendig machen, ist die Vorratsdatenspeicherung außerdem nicht mit dem Grundsatz vereinbar, dass die Grundrechte grds. ungestört von staatlichen Eingriffen ausgeübt werden sollten. So ist der Mensch von Natur aus auf Kommunikation angewiesen[143] und auch die Meinungs- und Pressefreiheit, um nur zwei Beispiele zu nennen, wären ohne den Austausch von Informationen undenkbar, so dass sich hieraus ein besonderer Schutz ergeben muss. Dieser Konzeption würde es zudem widersprechen, wenn man bereits in dem Austausch von Informationen eine abstrakte Gefahr sehen würde, die den Staat zu Eingriffen berechtigt.[144]

(j) Aussagekraft der gespeicherten Daten

Was Art und Umfang der gespeicherten Daten betrifft, so räumt die Bundesregierung in ihrer Stellungnahme zunächst einmal ein, dass die gespeicherten Daten Rückschlüsse auf die Persönlichkeit von Betroffenen zulassen.[145] Die Daten seien aber trotzdem nur „begrenzt sensibel“, weil das Bundesverfassungsgericht die verfassungsrechtliche Einordnung auch von der Betroffenheit derer abhängig gemacht hat, deren Rechte durch das Sammeln von Daten geschützt werden sollen und weil die Verkehrsdaten nicht den Inhalt der Kommunikation beträfen.[146] Es kann jedoch nicht sein, dass die Sensibilität von Daten von der Betroffenheit Dritter abhängig gemacht wird. Vielmehr handelt es sich hier um zwei zunächst getrennt voneinander zu bewertende Aspekte, die in ihrer Eigenständigkeit miteinander abgewogen werden sollen. Die Sensibilität ist vielmehr anhand des Persönlichkeitsbezuges und der Vertraulichkeit der Information zu prüfen. Dieser Punkt deutet nämlich gerade auf die besondere Schwere des Eingriffs in Art. 10 Abs. 1 Var. 3 GG hin, weil nicht nur Einzeldaten gespeichert werden, sondern der Informationstechnologie besondere Verknüpfungsmöglichkeiten zur Verfügung stehen, die das Entstehen von Bewegungs- und Kommunikationsprofilen ermöglichen. „ A complete communication profile can be build from the recorded data […] to draw conclusions about a user's so called „social network“. […] While email addressees in the form of e.g. cancer.treatment@hospital or even gaylover@freemailer give strong hints on the actual content of an email.“[147] Diese Daten sind damit nicht zwingend

143 BVerfGE 65, 1, 44.
144 Verfassungsbeschwerde Vorratsdatenspeicherung vom 31.12.2007, 79.
145 Stellungnahme der Bundesregierung vom 28. November 2008, 62.
146 Stellungnahme der Bundesregierung vom 28. November 2008, 63.
147 Pimenidis/Kosta, DuD 2008, 95.

weniger aussagekräftig als die Inhalte einer Kommunikation.[148] Dadurch das diese automatisiert analysierbar sind, können sie sogar aussagekräftiger als Inhaltsdaten sein.[149] In diesem Zusammenhang besonders prekär ist die sogenannte „Stille SMS“, die nach § 113a Abs. 2 S. 2 TKG ebenfalls von der Speicherpflicht erfasst ist. Darunter versteht man einen bestimmten Typ von Kurznachrichten, die nicht auf dem Bildschirm des Empfängertelefons angezeigt werden und die ursprünglich für die netzinterne Verwendung vorgesehen waren. Zu jeder verschickten „Stillen SMS“ wird auch die Position des Betroffenen gespeichert. Durch das regelmäßige Aussenden kann ein Bewegungsprofil erstellt werden. Die heute erhältlichen Mobiltelefone weisen den Nutzer nicht auf den Eingang einer solchen SMS hin, so dass er von dieser Art der Speicherung seines persönlichen Bewegungsablaufs gar nichts mitbekommt. Der Einsatz „Stiller SMS“ beim Bundeskriminalamt, Bundesgrenzschutz und beim Zoll wurde bereits bestätigt.[150] Außerdem kann häufig von den Kommunikationsdaten auch auf deren Inhalt geschlossen werden. Gerade im Bereich des Internets ist eine strikte Trennung in der Regel gar nicht möglich. Der Besuch von bestimmten Diskussionsforen oder Beratungsangeboten lässt immer auch gewisse Rückschlüsse auf den Inhalt zu. Auch Gesprächspartner am Telefon erlauben Rückschlüsse auf den Kommunikationsinhalt,[151] so zum Beispiel, wenn es um Anrufe bei einer Eheberatungsstelle geht. Das Bundesverfassungsgericht hat in einem Urteil zur Wohnungsdurchsuchung zudem festgestellt, dass Verbindungsdaten auch Rückschlüsse über das soziale Umfeld einer Person erlauben.[152] So impliziert beispielsweise eine häufige und lange Kommunikation eine engere soziale Bindung als nur gelegentliche kurze Kommunikation.[153] Einer Studie des US-amerikanischen Forschungszentrums MIT zufolge kann selbst die Zufriedenheit am Arbeitsplatz anhand von Telekommunikationsdaten ermittelt werden.[154] Die heutige Informationstechnologie macht es möglich, ganze Persönlichkeitsprofile zu erstellen.[155] Auch durch die Verbreitung des mobilen Internets lassen sich sehr präzise Bewegungsprofile herausarbeiten. So ist vorgesehen, dass der Access-Provider den Zugriff auf

148 Korn, HRRS 2009, 123.
149 Biermann, http://www.zeit.de/online/2009/28/vorratsdaten-ccc-verfassungsgericht?page=1 (Zugriff: 14.07.09).
150 Kurz/Rieger 2009, 36 f.
151 Arbeitskreis Vorratsdatenspeicherung/Netzwerk Neue Medien e.V./Neue Richtervereinigung e.V. 2007, 4.
152 BVerfGE 107, 299, 320.
153 Kurz/Rieger 2009, 8.
154 Eagle/Pentland/Lazer, http://reality.media.mit.edu/-pdfs/network_structure.pdf. (Zugriff: 28.06.09).
155 BVerfGE 65, 1, 42.

bereitsgestellte Email-Accounts protokolliert. Die dabei erfassten Daten enthalten auch Informationen darüber, an welchem Ort und zu welcher Zeit der Nutzer EMails abruft und sendet. Die dadurch anfallenden ortsabhängigen Daten erlauben die Erstellung eines Bewegungsprofils.[156] Kommunikationsdaten eignen sich auch zur politischen Kontrolle, weil sie es erlauben, soziale Netzwerke wie zum Beispiel Globalisierungskritiker zu identifizieren.[157] Auch die Begleitumstände der Kommunikation sollen im Rahmen der Vorratsdatenspeicherung erfasst werden. Dabei handelt es sich um Standortdaten, die Aufschluss darüber geben, in welche Mobilfunkzelle sich welches Endgerät eingewählt hat.[158] Nach einer Änderung des Sicherheitspolizeigesetzes zeigte sich in Österreich bereits ein starker Anstieg der dort vereinfacht möglichen Standortabfragen bei Mobiltelefonen. So war die Anzahl der Ortungen in nur zwei Monaten um siebzig Prozent gegenüber dem Vorjahr gestiegen.[159] Bei Tatorten die auf dem Land liegen, wo eine einzige Funkzelle ein viele Quadratkilometer großes Gebiet umfasst, ist die Wahrscheinlichkeit in einen Verdächtigenkreis zu geraten noch größer. Dagegen ist die Erfolgsquote der Ermittlungsbehörden eher gering, da die Wahrscheinlichkeit, dass ein Straftäter in unmittelbarer Tatortnähe telefoniert eher kaum beseht. Derartige Massenabfragen, bei denen die Ermittlungsbehörden bei allen Netzanbietern alle Verkehrs- und Standortdaten in Erfahrung bringen, werden jedoch immer häufiger.[160] Mögliche Rückschlüsse auf das Privatleben von Personen sind vielfältig. Der Chaos Computer Club bringt in seiner Stellungnahme zur Verfassungsbeschwerde das Beispiel eines Kontakts mit einem auf Familienrecht spezialisierten Anwalt an, der im Anschluss eine telefonische Anfrage bei Wohnungsmaklern vornimmt, woraus unschwer eine Scheidungsabsicht prognostiziert werden kann.[161] Insofern ist die Annahme der Bundesregierung falsch, wenn diese in ihrer Stellungnahme einen abgeschwächten Eingriff annimmt, weil nach § 113a Abs. 8 TKG keine Speicherung von Kommunikationsinhalten vorgesehen ist.[162] Das die Speicherung eine Verflechtung und Zusammenhänge bei Organisationsstrukturen erkennen lässt, wird in der

156 Kurz/Rieger 2009, 25.
157 http://www.daten-speicherung.de/index.php/pressemitteilung-us-abhoerskandal-erfordert-umdenken-auch-in-europa/ (Zugriff: 13.06.09).
158 Kurz/Rieger 2009, 19.
159 Vgl. http://help.orf.at/?story=7497 (Zugriff: 15.07.09).
160 Kurz/Rieger 2009, 21 f.
161 Kurz/Rieger 2009, 10.
162 Stellungnahme der Bundesregierung vom 28. November 2008, 40.

Stellungnahme sogar dargestellt.[163] Das der Rückschluss auf Inhalte damit nur noch ein formaler Schritt ist, dürfte daraus klar erkennbar sein. Kommunikationsdaten dürfen nicht weniger schutzbedürftig sein als Inhaltsdaten. Eine staatliche Überwachung greift letztlich tief in das Persönlichkeitsrecht ein und tangiert auch besondere Vertrauensverhältnisse wie das Arztgeheimnis.

Bei der nächsten Generation von Auswertungssoftware für Verbindungsdaten besteht bereits die Möglichkeit, aus der graphischen Analysesoftware die Übermittlung der Daten einer interessierenden Person direkt zu beantragen. In Ländern in denen kein Richtervorbehalt existiert, kommuniziert die Analysesoftware direkt mit den Datenbanken der Netzanbieter.[164]

Die Vorratsdatenspeicherung von Telekommunikationsdaten bringt immer auch die Gefahr falscher Verdächtigungen mit sich, weil Internet- oder Telefonanschlüsse nicht zwingend vom Inhaber selber genutzt werden, sondern diese ggf. auch ohne sein Wissen anderen Personen zur Verfügung stehen. Selbst wenn sich nachher die Unschuld einer Person herausstellt, kann ein falscher Verdacht ausreichen, um zu Hausdurchsuchungen, Untersuchungshaft etc. zu führen, was mit erheblichen Belastungen für den Betroffenen verbunden ist.[165] Die Argumentation der Bundesregierung ist an dieser Stelle viel zu kurz gedacht, da sie eine Notwendigkeit zur Vorratsdatenspeicherung gerade deshalb sieht, weil „in kriminellen Kreisen so gut wie immer – Nutzer und Anschlussinhaber nicht identisch sind […].[166] Gerade in diesem Fall kann jedoch keine Ermittlung des Nutzers und keine Speicherung von Daten des eigentlich Kriminellen erfolgen.

(k) Zwischenergebnis

Wägt man den Eingriff in das Fernmeldegeheimnis und das verfolgte Ziel einer Verbesserung der Strafverfolgungsmöglichkeiten miteinander ab, so muss man zu dem Ergebnis kommen, dass das öffentliche Interesse an einer effektiven Strafverfolgung zwar berechtigt und ernst zu nehmen ist, unter Berücksichtigung der fraglichen Eignung und im Hinblick auf die Schwere des Eingriffs aber eindeutig unverhältnismäßig ist. So wurde zum Einen die Möglichkeit der Umgehung der Datenspeicherung durch Anonymisierung genannt, die jeder, der ein Interesse daran hat, mit relativ einfachen Mitteln nutzen kann. Zudem ist die Anzahl der Straftaten, bei denen tatsächlich auf die Daten zurück gegriffen werden müsste, verschwindend gering, so dass auch angesichts

163 Stellungnahme der Bundesregierung vom 28. November 2008, 48.
164 Kurz/Rieger 2009, 12.
165 Verfassungsbeschwerde Vorratsdatenspeicherung vom 31.12.2007, 85.
166 Stellungnahme der Bundesregierung vom 28. November 2008, 49.

der immensen Kosten, die durch die Speicherung entstehen, die Notwendigkeit stark angezweifelt werden muss.

Der Eingriff in das Fernmeldegeheimnis wiegt demgegenüber schwerer, insbesondere die Betroffenheit jedes Telekommunikationsnutzers ohne Vorliegen eines konkreten Tatverdachts indiziert erhebliche Folgen für das Kommunikationsverhalten, zumal eine Einzelfallprüfung mit Verhältnismäßigkeitsprüfung nicht stattfindet. Eine zunehmende Verhaltensanpassung, besonders auf Seiten regierungskritischer Personen oder Gruppierungen, wäre die wahrscheinliche Folge, mit unabsehbaren Konsequenzen für den Meinungsaustausch in einer freien, demokratischen Gesellschaft. Die Aussagekraft der Daten ist aufgrund der Verknüpfungsmöglichkeiten zum Erstellen von Persönlichkeitsprofilen immens. Damit steigt auch das Missbrauchsrisiko der Daten, wenn diese in die falschen Hände geraten oder gezielt verkauft werden.

Insgesamt gesehen ist der Schaden für eine demokratische Gesellschaft unabsehbar groß, während der Nutzen einer Vorratsdatenspeicherung nur für wenige Einzelfälle zu erwarten ist und damit in deutlichem Missverhältnis zu den beeinträchtigen Rechtsgütern steht. Die Vorratsdatenspeicherung von Telekommunikationsdaten stellt einen Eingriff in das Fernmeldegeheimnis aus Art. 10 Abs. 1 Var. 3 GG dar, der verfassungsmäßig nicht gerechtfertigt ist.

Die Stellungnahme der Bundesregierung kommt in ihrer Gesamtabwägung zu dem Ergebnis, dass das Bundesverfassungsgericht unter bestimmten Bedingungen auch die eingriffsintensivere anlasslose Überwachung von Kommunikationsinhalten verfassungsrechtlich für zulässig erachtet hat. Zudem müsse man bedenken, dass bestimmte Kommunikationsformen in denen sich Kriminalität abspielt nur durch Rückgriff auf die Verkehrsdaten erfasst werden könnten. Die Regelung sei außerdem schon deshalb angemessen, weil der Schutz von Spuren in Kommunikationsformen in denen diese besonders flüchtig seien, besonders wichtig sei. Daraus schließt die Bundesregierung, dass es sich dabei wohl deshalb nicht um die „globale und pauschale Überwachung“[167] handele, in der das Bundesverfassungsgericht einen Verfassungsverstoß gesehen hat. Auch wird die Speicherfrist von sechs Monaten noch einmal erwähnt, die sich auf konkrete kriminelle Ereignisse beziehe und nicht geeignet sei, eine flächendeckende Überwachung der Bevölkerung zu gestatten. Der Eingriff in den Schutzbereich von Art. 10 GG sei damit verfassungsrechtlich gerechtfertigt.[168]

167 BVerfGE 100, 313, 376.
168 Stellungnahme der Bundesregierung vom 28. November 2008, 67 ff.

Argumentation und Schlussfolgerung passen hier nicht zusammen und eine überzeugende Darlegung, weshalb es sich hier nicht um die vom Bundesverfassungsgericht abgelehnte pauschale Überwachung handelt, bleibt aus. Auch dem Einwand das sich die sechsmonatige Speicherfrist auf konkrete kriminelle Ereignisse bezieht, kann nicht gefolgt werden, vielmehr wird sich die Vorratsdatenspeicherung den Vorwurf der Pauschalität auch weiterhin gefallen lassen müssen. Zwar können anhand der gespeicherten Daten konkrete kriminelle Ereignisse ermittelt werden, die Formulierung geht jedoch fehl soweit es darum geht, dass sich die sechsmonatige Speicherfrist darauf bezieht, weil von der Speicherfrist alle Kommunikationsteilnehmer und nicht nur diejenigen, deren Kommunikation auf kriminelle Ereignisse abzielt, betroffen sind. Ebenso wenig schlüssig ist das Argument, dass mit der sechsmonatigen Speicherfrist eine flächendeckende Überwachung der Bevölkerung verhindert werde, da die Speicherdauer völlig unabhängig von der Streubreite ist und weil trotzdem jeder, der sich der Telekommunikation bedient, von der Vorratsdatenspeicherung erfasst ist.

Die Stellungnahme der Bundesregierung kann im Ergebnis nicht überzeugen, da sie oft nicht zu Ende gedacht wirkt und den Eindruck der Vordergründigkeit erweckt. Die Aussichten der Verfassungsbeschwerde erscheinen dagegen, folgt man der dargestellten Argumentationslogik, durchaus erfolgreich.

Für den Erfolg der Verfassungsbeschwerde ist Art. 10 Abs. 1 Var. 3 GG als lex specialis zu Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG zunächst maßgeblich. Auch von einer Überprüfung weiterer Grundrechte wird aufgrund des begrenzten Umfangs vorerst abgesehen. Im Folgenden werde ich die Vereinbarkeit der Richtlinie zur Vorratsdatenspeicherung mit den auf EU-Ebene geschaffenen Grundrechten prüfen.

D. Vereinbarkeit der Richtlinie 2006/24/EG mit den im Gemeinschaftsrecht anerkannten Grundrechten

Nachdem auch die Generalanwältin Juliane Kokott in den Schlussanträgen im Fall *Promusicae* gegen *Telefónica* die Grundrechtskonformität der Richtlinie 2006/24/EG in Frage gestellt hat: „Man kann daran zweifeln, ob die Speicherung von Verkehrsdaten aller Nutzer – gewissermaßen auf Vorrat – mit Grundrechten vereinbar ist, insbesondere da dies ohne konkreten Verdacht geschieht […] Möglicherweise ist diese Frage eines Tages aus Anlass der Richtlinie 2006/24 zu prüfen, die eine gemeinschaftsrechtliche

Verpflichtung zur Vorratsdatenspeicherung einführt."[169], erscheint die Prüfung einer möglichen Entscheidung durch den EuGH berechtigt. Diesbezüglich sind zunächst die möglichen Klageoptionen aus deutscher Sicht zu beschreiben.

I. Klagemöglichkeiten für eine Überprüfung durch den EuGH

Rechtsschutz gegen die Richtlinie 2006/24/EG kann vor dem EuGH erlangt werden. Gegen das Umsetzungsgesetz ist vor dem Bundesverfassungsgericht die bereits geprüfte Klage vor dem Bundesverfassungsgericht anhängig. Sollten sich Zweifel an der Richtlinie ergeben, ist die entsprechende Frage nach Art. 234 EG, wie von den Beschwerdeführern beantragt,[170] dem EuGH zur Vorabentscheidung vorzulegen. Dieses wurde durch das Verwaltungsgericht Wiesbaden mit Beschluss vom 27.02.2009 (Az. 6 K 1045/08.WI) unter Annahme der Unverhältnismäßigkeit der Richtlinie bereits vorgenommen.[171] Und auch der Europäische Gerichtshof selber hat eine eventuelle Verletzung der Grundrechte durch die Richtlinie in Erwägung gezogen.[172]

Erklärt nur das Bundesverfassungsgericht das Umsetzungsgesetz dagegen für verfassungswidrig, so könnte die Nichtigkeit zwar festgestellt werden, die Umsetzungspflicht auf europäischer Ebene bliebe aber bestehen, da Maßstab allein Gemeinschaftsrecht ist und die alleinige Verwerfungskompetenz von EU-Richtlinien beim EuGH liegt.[173] Die Folge wäre ein gemeinschaftsrechtswidriges Verhalten des Mitgliedstaats und mögliche Sanktionen im Rahmen eines Vertragsverletzungsverfahrens. Um dem zu entgehen, könnte eine Nichtigkeitsklage vor dem EuGH nach Art. 230 EGV angestrengt werden, antragsberechtigt wären jedoch nur die Mitgliedstaaten, das Europäische Parlament, der Rat oder die Kommission. Die Rücknahme könnte auch auf politischem Wege in den Gremien der Gemeinschaft erfolgen. Eine nationale Verfassungsänderung wäre ebenfalls eine Option.[174]

Aufgrund des Anwendungsvorrangs des EU-Rechts hat das Bundesverfassungsgericht in der Solange II-Entscheidung jedoch festgestellt, dass es seine eigene Rechtsprechungskompetenz nicht ausübt, soweit der Grundrechteschutz auf EU-Ebene

169 GA *Juliane Kokott,* Schlussanträge in der Rs. C-275/06 vom 18. Juli 2007, Slg. 2008, I-271, Nr. 82.
170 Verfassungsbeschwerde Vorratsdatenspeicherung vom 31.12.2007, 18.
171 http://www.heise.de/newsticker/Verwaltungsgericht-bezeichnet-Vorratsdatenspeicherung-als-ungueltig--/meldung/134616 (Zugriff: 05.07.09).
172 EuGH, Rs. C-301/06, Slg. 2009, Rn. 57.
173 Kahler, DuD 2008, 452.
174 Sierck/Schöning/Pöhl, http://webarchiv.bundestag.de/archive/2006/1206/bic/analysen/2006/Zulaessigkeit_der_Vorratsdatenspeicherung_nach_europaeischem_und_deutschem_Recht.pdf (Zugriff: 07.07.09) 6 f.

den Grundrechtsgarantien des Grundgesetzes im Wesentlichen entspricht.[175] Das Bundesverfassungsgericht hat damit weniger einzelne Entscheidungen im Blick, sondern stellt vielmehr auf die generelle Rechtsentwicklung der EU ab.

Für den Fall einer Vorlage durch das Bundesverfassungsgericht im Vorabentscheidungsverfahren nach Art. 234 EG, ist im Folgenden die Vereinbarkeit der Richtlinie mit Gemeinschaftsgrundrechten zu prüfen.

II. Prüfung eines Verstoßes gegen Art. 8 Charta der Grundrechte der Europäischen Union

Der EuGH müsste prüfen, ob die Speicherung der in der Richtlinie genannten Verbindungsdaten mit seiner Rechtsprechung zu den Grundrechten im Einklang steht. Der EuGH zieht als Prüfungsmaßstab drei Rechtsquellen heran: Die Europäische Menschenrechtskonvention, die gemeinsamen Verfassungsgrundsätze der Mitgliedstaaten sowie die Europäische Grundrechtecharta.[176] Da die Grundrechte der EMRK bereits im Rahmen der Erfolgsaussichten einer Klage vor dem EGMR zum Tragen kommen, findet vorliegend zunächst eine Prüfung der Grundrechtecharta statt. Dabei muss der EuGH die Rechte aus der Europäischen Menschenrechtskonvention jedoch als Prüfungsmaßstab heranziehen und dafür Sorge tragen, dass ein gleiches Schutzniveau gewährleistet ist. Es ist zu berücksichtigen, dass die Bestimmungen der Richtlinie 2006/24, soweit sie die Verarbeitung personenbezogener Daten betreffen, die zu Beeinträchtigungen des Rechts auf Achtung des Privatlebens führen kann, im Licht der Grundrechte auszulegen sind, die nach ständiger Rechtsprechung zu den allgemeinen Rechtsgrundsätzen gehören, deren Wahrung der Gerichtshof zu sichern hat.[177] Die Ansätze in der Rechtsprechung des EuGH zum Datenschutz sind allerdings wenig ausgeprägt und geben kein Bild einer kohärenten Dogmatik des grundrechtlichen Datenschutzes. In der Folge lassen sich aus den ohnehin vergleichsweise wenigen bisher ergangenen Urteilen nur recht isolierte Hinweise auf die Erfolgsaussichten einer Klage entnehmen. Zudem sind bisher in nur wenigen Fällen Akte der Gemeinschaft für grundrechtswidrig erklärt worden, wofür der EuGH vielfach kritisiert worden ist.[178] Dennoch ist auch in der Judikatur des EuGH im Prinzip anerkannt, dass der Einzelne von einer unfreiwilligen Preisgabe und einem widerrechtlichen Gebrauch seiner Daten

175 BVerfGE 73, 339 ff.
176 Kahler, DuD 2008, 451.
177 Vgl. u. a. EuGH, Rs. C-274/99, Slg. 2001, I-1611, Rn. 37.
178 Weber, NJW 2000, 543.

grundrechtlich geschützt ist.[179] Das Recht auf den Schutz personenbezogener Daten ist in der Charta der Grundrechte in Art. 8 verankert. Komplementiert wird der Datenschutz mit der Datenschutzrichtlinie[180], der Datenschutzverordnung[181] und der Datenschutzrichtlinie für elektronische Kommunikation[182] Auch dem Übereinkommen des Europarates zum Schutz der Menschen bei der automatischen Verarbeitung personenbezogener Daten (Konvention Nr. 108) vom 28. Januar 1981 kommt, wenn es um Datenschutzmaßstäbe der EU geht, eine große Bedeutung zu.[183] Schließlich wird mit der Einführung eines speziellen Grundrechts auf Schutz personenbezogener Daten der besonderen Bedeutung Rechnung getragen, die dem Datenschutz in der Gemeinschaft zukommt.[184] Das Grundrecht auf den Schutz personenbezogener Daten aus Art. 8 geht Art. 7 GRC (Achtung des Privat- und Familienlebens) als lex specialis vor.[185]

1. Schutzbereich

Geschützt sind personenbezogene Daten. Darunter fallen alle Informationen über eine bestimmte oder bestimmbare natürliche Person, unabhängig davon, ob sie deren Privat- oder Intimsphäre oder andere Bereiche betreffen. Voraussetzung dürfte ein ausreichender personaler Bezug sein.[186] Als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind.[187] Das Vorliegen personenbezogener Daten wurde für die § 113 a Abs. 1-

179 Mehde, in: Hesselhaus/Nowak 2006, 613.
180 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, ABl. L 281 vom 23.11.1995.
181 Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, ABl. L 8/1 vom 12.1.2001.
182 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, ABl. L 201, 37 vom 31.7.2002.
183 Mehde, in: Nowak/Hesselhaus, 2006, 615.
184 Craig/de Burca 2003 EU, 359.
185 Mehde, in: Nowak/Hesselhaus, 2006, 614.
186 Jarass 2005, 171.
187 Art. 2 der 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

4 TKG bereits bei der Prüfung des Schutzbereichs der informationellen Selbstbestimmung bejaht. Dieses entspricht auch dem Verständnis des Art. 8 der Grundrechtecharta. Der Schutzbereich ist damit berührt.

2. Eingriff

Ein Eingriff in Art. 8 GRC liegt dann vor, wenn Grundrechtsadressaten persönliche Daten i.S.d. Art. 8 Abs. 2 „verarbeiten". Darunter ist jede Erhebung, Speicherung oder Verwendung von Daten zu verstehen.[188] Auch die bloße Weitergabe persönlicher Daten stellt einen Eingriff dar,[189] weil diese, unabhängig von der späteren Verwendung der übermittelten Information, eine Beeinträchtigung des Rechts auf Achtung des Privatlebens begründet. Für die Feststellung eines solchen Eingriffs kommt es auch nicht darauf an, ob die übermittelten Informationen als sensibel anzusehen sind oder ob die Betroffenen durch den Vorgang irgendwelche Nachteile erlitten haben.[190] Wie bereits bei Prüfung des Fernmeldegeheimnisses bestätigt, werden Daten gespeichert und ggf. auch später verwendet. Damit stellt sowohl die Speicherung, als auch die Weitergabe, die typischerweise eine staatliche Kenntnisnahme zur Folge haben kann, einen Eingriff in Art. 8 Abs. 1 GRC dar.

3. Verfassungsmäßige Rechtfertigung

a) Schrankenregelung des Art. 8 GRC

Des Weiteren ist zu prüfen, inwieweit Art. 8 GRC überhaupt einer Schrankenregelung unterliegt. Art. 8 GRC ist eines der wenigen Rechte aus der Charta, das einen eigenen Schrankenkatalog aufweist. Anders als in der EMRK wurde bei den meisten Rechte bewusst auf die Schranken verzichtet. Art. 52 GRC enthält dafür eine allgemeine Schrankenbestimmung, die grundsätzlich für alle Rechte der Charta gilt.[191] Zusätzlich zu den in Art. 8 GRC festgelegten Schranken, ist das Recht auf Datenschutz damit auch den allgemeinen Schrankenregelungen des Art. 52 GRC unterworfen. Die in Art. 8 Abs. 2 aufgeführten Schrankenbestimmungen entsprechen weitgehend den in Art. 6 und 7 der Datenschutzrichtlinie geregelten Zulässigkeitsvoraussetzungen für die Verarbeitung personenbezogener Daten. Bisher lässt sich in der Rechtsprechung des EuGH zu den Grundrechtsschranken keine einheitliche Linie erkennen. Teilweise greift der EuGH auf

Datenverkehr , ABl. L 281, 31.
188 Jarass 2005, 172.
189 EuGH, Rs. C-465/00, Slg. 2003, I-4989, Rn. 74.
190 EuGH, Rs. C-138/01, Slg. 2003, I-4989, Rn. 74.
191 Siemen 2006, 283.

die Schranken der EMRK Rechte zurück.[192]

Das im Allgemeininteresse liegende Ziel der öffentlichen Sicherheit könnte einen Eingriff in Art. 8 Abs. 1 GRC daher dann rechtfertigen, wenn dieser der Schrankenregelung der Art. 8 Abs. 2 S. 1 und Art. 52 Abs. 1 der Grundrechtecharta genügt. Zudem wären die Vorgaben der EMRK bei Beschränkungen im Interesse der öffentlichen Sicherheit und Ordnung hier vorzusehen, wonach diese nur soweit gehen dürfen, wie es in einer demokratischen Gesellschaft notwendig ist. Dabei handelt es sich um eine Konkretisierung des Gesichtspunktes der Angemessenheit.[193] Da eine Überprüfung der EMRK im Rahmen der Begutachtung der Klagemöglichkeiten vor dem EGMR erfolgt, ist an dieser Stelle auf das Erfordernis der Notwendigkeit in einer demokratischen Gesellschaft jedoch nicht weiter einzugehen.

Grundsätzlich bedarf jede Einschränkung einer gesetzlichen Grundlage. Dabei ist die in Art. 8 Abs. 2 S. 1 GRC hervorgehobene Gesetzesbindung nicht Teil der Einschränkung wie die des Art. 52 GRC, sondern elementarer Bestandteil des Garantiegehalts des Grundrechts.[194] Die gesetzliche Grundlage muss hinreichend bestimmt sein, weil auf diese Weise die Vorhersehbarkeit der zu erwartenden Beeinträchtigung für die Betroffenen sichergestellt werden soll. Dies ist vor dem Hintergrund der Schutzrichtung des Grundrechts auch deswegen unverzichtbar, weil ansonsten trotz der gesetzlichen Ermächtigung jene Unsicherheit in der persönlichen Lebensgestaltung eintritt, vor der die Gewährleistung gerade schützen will. Des Weiteren muss der Eingriff an „festgelegte Zwecke“ gebunden sein, d.h. er muss rechtlich normiert sein und ein legitimes Ziel verfolgen. Die Zweckbindung gehört dabei zum unzweifelhaften Kernbestand datenschutzrechtlicher Gewährleistungen. Art. 8 Abs. 2 S. 1 GRC legt damit fest, dass Daten nur zu dem Zweck verarbeitet werden dürfen, zu dem sie auch erhoben wurden. Das dabei auf die Gefährdungslage des Grundrechtsträgers abzustellen ist, spricht für eine möglichst restriktive Definition des jeweiligen Zwecks.[195] Die Verknüpfung von Zweck und Erforderlichkeit erlaubt es dabei, die von der Datenschutzrichtlinie und den Datenschutzgesetzen postulierte Datensparsamkeit zu realisieren.[196] Die Bindung an „Treu und Glauben“ legt zum Einen die Bindung an festgelegte Zwecke fest und beinhaltet zum Anderen ein Missbrauchsverbot dieser Zwecke. Nach Abs. 3 ist eine Beschränkung zudem nur dann gerechtfertigt, wenn die

192 Siemen 2006, 227.
193 Mehde, in: Nowak/Hesselhaus 2006, 626 f.
194 Mehde in: Nowak/Hesselhaus 2006, 614.
195 Mehde, in: Nowak/Hesselhaus 2006, 620.
196 Simitis, NJW 2009, 1785.

Einhaltung der Vorschrift von einer unabhängigen Stelle überwacht wird. Daraus folgt auch ein Beschwerderecht gegenüber dieser Stelle. Mit dieser Norm wird nicht nur der Datenschutzbeauftragte als Institution abgesichert, sondern auch seine Unabhängigkeit gefordert. Damit ist auch der Gesichtspunkt der Vorsorge gegenüber Grundrechtsverletzungen gefordert. Das Datenschutzrecht ist ein Regelungsbereich, bei dem der effektive Grundrechtsschutz nicht darauf beschränkt werden darf, dass den Rechtsträgern entsprechende Abwehrrechte eingeräumt werden. Vielmehr geht es um die kontinuierliche, auch von eigens geschaffenen Institutionen wahrgenommene Pflege des Raums individueller Freiheit.[197]

Im Zusammenhang mit Art. 8 GRC ist der allgemeine Schrankenvorbehalt des Art. 51 Abs. 1 GRC anwendbar. Die Einschränkung des Rechts auf Schutz personenbezogener Daten muss also gesetzlich vorgesehen sein und dessen Wesensgehalt achten. Nach Art. 52 Abs. 1 S. 2 müssen Einschränkungen notwendig sein und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer entsprechen. Außerdem muss der Grundsatz der Verhältnismäßigkeit gewahrt sein, d.h. die durch die Datenverarbeitung verursachte Belastung, darf dem verfolgten Zweck nicht unverhältnismäßig gegenüberstehen. Das Recht auf den Schutz personenbezogener Daten dürfte die Grundrechtsadressaten dazu verpflichten, im Rahmen ihrer Zuständigkeit für einen Schutz personenbezogener Daten auch ggü. Privaten zu sorgen. Insbesondere die Vorgaben des Art. 8 Abs. 2 S. 1 sind auch auf die Verarbeitung von Daten durch Private zu erstrecken.

Berücksichtigt man das Erfordernis der Vorhersehbarkeit, müssen die Adressaten ihr Verhalten nach dem Eingriff ausrichten können. Das Erfordernis der Vorhersehbarkeit hat im Datenschutzrecht mit der in Art. 8 Abs. 2 S. 1 GRC ausdrücklich genannten Zweckbindung eine besondere Ausprägung erfahren. Der Eingriff erfolgt durch die Richtlinie 2006/24/EG und beruht damit auf einer gesetzlichen Grundlage. Es stellt sich die Frage, ob diese Bestimmung so genau formuliert ist, dass die Adressaten ihr Verhalten danach einrichten können und diese damit dem Erfordernis der Vorhersehbarkeit genügt, welches in der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte entwickelt worden ist.[198] Die Richtlinie nennt sowohl die Speicherung als solche (Art. 3), als auch den Zeitraum der Speicherung (Art. 6) und die Kategorien der zu speichernden Daten (Art. 5). Auch § 113a TKG nennt diese

197 Mehde, in: Nowak/Hesselhaus 2006, 614.
198 Vgl. u. a. EGMR, Urt. vom 20. Mai 1999, *Rekvényi v. Ungarn*, (Rs. 25390/94), Rn. 34.

Bestimmungen, so dass die Regelungen insgesamt so genau sind, dass die Adressaten ihr Verhalten danach ausrichten können und dem Erfordernis der Vorhersehbarkeit damit Genüge getan ist. Praktisch läuft dieses Erfordernis vorliegend jedoch ins Leere, weil eine Ausrichtung des Verhaltens dazu führen würde, dass es im Grunde keine freie Kommunikation mehr geben würde, weil alle Daten gespeichert werden, nicht nur die für die Strafverfolgung benötigten – und ggf. auch ohne das Wissen der Betroffenen an die Strafverfolgungsbehörden weitergegeben werden. Das Erfordernis der Vorhersehbarkeit, mit dem Ziel das die Bürger ihr Verhalten darauf einstellen können, verdeutlicht im Fall der Richtlinie 2006/24/EG erst, als wie gefährlich diese in ihren Folgen einzuordnen ist. Die Vorratsdatenspeicherung führt dazu, dass eine anonyme Kommunikation kaum noch möglich ist und man sich stets der Nachvollziehbarkeit von Telekommunikation bewusst sein muss. Dadurch sinkt die Bereitschaft zur Nutzung der Telekommunikation in bestimmten Situationen erheblich. Will man das Risiko von Ermittlungsmaßnahmen gänzlich ausschließen, muss man auf die Post oder den persönlichen Kontakt ausweichen oder Kommunikation generell vermeiden.[199] Die zusätzliche Anfälligkeit dieser Daten für den Missbrauch zu kommerziellen Zwecken wurde bereits erwähnt. Auch die Generalanwältin befürchtet bei einer Speicherung der gesamten Kommunikation als Folge den „gläsernen Bürger“.[200]

Die Zweckbindung stellt sich genau dort als fraglich dar, wo die Speicherung von Daten auf „Vorrat“ Verarbeitungsmaßstab ist, da diese zu dem Zeitpunkt nicht in die Behandlung eines konkret anstehenden Vorgangs eingebracht werden. Sie stellen lediglich die Grundlage für derzeit nicht erforderliche und zu einem späteren Zeitpunkt nur in seltenen Fällen benötigte Informationen dar[201] und laufen damit dem Grundsatz der Datensparsamkeit[202] zuwider. Vor dem Hintergrund, dass die Zweckbindung als der wohl wichtigste Datenschutzgrundsatz bezeichnet werden muss[203] kann die Richtlinie 2006/24/EG der Schrankenregelung des Art. 8 Abs. 2 GRC kaum gerecht werden.

b) Verhältnismäßigkeit

Eine Klage vor dem EuGH hätte dann Aussicht auf Erfolg, wenn die Richtlinie

199 Starostik, Meinhard: Stellungnahme vom 23. März 2007 zum Schriftsatz des Bevollmächtigten der Bundesregierung vom 22. Januar 2007, 15.
200 GA *Juliane Kokott,* Schlussanträge in der Rs. C-275/06 vom 18. Juli 2007, Slg. 2008, I-271, Nr. 97.
201 Simitis, NJW 2009, 1785.
202 Schwenke, DuD 2006, 250.
203 So auch Simitis, NJW 2009, 1786.

2006/24/EG in Art. 8 Abs. 1 GRC eingreift und der Eingriff verfassungsmäßig nicht gerechtfertigt ist. Nach dem Verhältnismäßigkeitsprinzip dürfen Grundrechte nur insoweit eingeschränkt werden, wie die Maßnahme zur Erreichung des angestrebten Zwecks geeignet, erforderlich und angemessen ist und ein legitimer Zweck verfolgt wird. Als weitere Schranken-Schranke fordert der Gerichtshof, dass die Grundrechte nicht in ihrem Wesensgehalt angetastet werden. Nach überwiegender Auffassung geht man jedoch davon aus, dass nur unverhältnismäßige Eingriffe den Wesensgehalt eines Grundrechts beeinträchtigen.[204]

aa) Legitimes Ziel

Die Verhältnismäßigkeitsprüfung erfordert zunächst das Vorliegen eines legitimen Ziels. In den Erwägungsgründen der Richtlinie 2006/24/EG werden die Bekämpfung von Straftaten, Organisierter Kriminalität und Terrorismus genannt.[205] Die öffentliche Sicherheit ist ein legitimes Ziel,[206] welches auch der Zweckbindung des Art. 8 Abs. 2 S. 1 GRC genügt; insbesondere die spezifische Gefährdungslage, der mit dem Eingriff entgegengewirkt werden soll, lässt einen solchen Schluss zu.

bb) Geeignetheit

Im Anschluss ist die Eignung der Maßnahme zu prüfen, d.h. es muss zumindest die Möglichkeit der Zweckerreichung bestehen. An der Geeignetheit wurden bereits bei der Prüfung der Verfassungsbeschwerde Zweifel geäußert, weil die Möglichkeit besteht, dass Kriminelle über Dritte entsprechende Kommunikationsgeräte erwerben oder zu Anonymisierungsmaßnahmen greifen, um die Verfolgbarkeit ihrer Daten zu verhindern. Es kann jedoch nicht generell ausgeschlossen werden, dass die Vorratsdatenspeicherung dazu beitragen kann, dass Bedrohungspotenzial zu vermindern.[207]

cc) Erforderlichkeit

Die Richtlinie ist erforderlich, wenn kein milderes, gleich geeignetes Mittel existiert. Als ein solches wurde bereits das „Quick-Freeze“ Verfahren geprüft, das sich als ein milderes Mittel darstellt, zu dem aber noch keine verlässlichen Daten vorliegen.[208]

---

204 Siemen 2006, 229.
205 Erwägungsgründe 4-11 der Richtlinie 2006/24/EG.
206 Siehe auch B.IV.
207 Sierck/Schöning/Pöhl, http://webarchiv.bundestag.de/archive/2006/1206/bic/analysen/2006/Zulaessigkeit_der_Vorratsdatenspeicherung_nach_europaeischem_und_deutschem_Recht.pdf (Zugriff: 07.07.09), 13.
208 Siehe auch C.II.4.b)bb)(3).

Dieses Verfahren erfüllt allerdings nur dann in gleichem Maße den angestrebtem Zweck, wenn es um eine Ermittlung permanenten kriminellen Verhaltens geht, die fraglichen Verbindungsdaten sich also auf die Gegenwart oder Zukunft beziehen. Für einen Zugriff auf in der Vergangenheit angefallene Daten ist das Verfahren dagegen nutzlos und nicht in gleichem Maße förderlich, wie die Vorratsdatenspeicherung. Von der Erforderlichkeit ist also auch bei der Richtlinie 2006/24/EG zunächst einmal auszugehen.

dd) Angemessenheit

Des Weiteren ist zu prüfen, ob die Richtlinie 2006/24/EG angemessen ist und ob der Eingriff in Art. 8 Abs. 1 der Grundrechtecharta in gewichtetem Verhältnis zum Ziel einer effektiven Strafverfolgung steht. Da die Hauptargumentationslinien bereits bei der Angemessenheitsprüfung der vor dem Bundesverfassungsgericht anhängigen Klage aufgezeigt wurden, soll Gegenstand der folgenden Prüfung vor allem EU-Recht (speziell Art. 8 GRC) und die bisherigen Entscheidungen des EuGH sein, sowie Erfahrungen mit dieser Thematik in anderen europäischen Ländern, um die Erfolgsaussichten einer Entscheidung abschätzen zu können.
Eine Orientierung bietet der Fall *Promusicae gegen Telefonica* in der Rechtssache C-275/06. Die Generalanwältin Juliane Kokott beginnt ihren Schlussantrag mit den Worten " Der vorliegende Fall veranschaulicht, dass die Speicherung von Daten für bestimmte Zwecke den Wunsch weckt, diese Daten umfassender zu nutzen."[209] und verdeutlicht damit zugleich die bei der Richtlinie 2006/24/EG bestehende Gefahr, dass die Speicherung von Daten auf Vorrat Begehrlichkeiten wecken kann, deren Folgen nicht abzusehen sind. Die Generalanwältin äußert in ihrem Schlussantrag zudem ganz offen Zweifel an der Vereinbarkeit der Vorratsdatenspeicherung mit den Grundrechten, insbesondere, weil die Speicherung ohne konkreten Verdacht vorgenommen wird.[210] Diese Ausführungen könnten bereits Anhaltspunkte für eine Entscheidung des Gerichtshofs darstellen.

Zunächst einmal ist im europäischen Kontext auffällig, dass nur der deutsche Text mit seiner Wortwahl die eigentliche Verwendungsabsicht und damit zugleich den Konflikt mit den Grundvoraussetzungen des Datenschutzes preisgibt, während in der französischen Fassung der Richtlinie von „rétention" und in der englischen von

209 GA *Juliane Kokott*, Schlussanträge in der Rs. C-275/06 vom 18.07.2007, Slg. 2008, I-271, Nr. 1.
210 GA Juliane Kokott, Rs. C-275/06 vom 18.07.2007, Slg. 2008, I-271, Nr. 82.

„retention“, also von „Zurückbehaltung“ die Rede ist.

(1) Der Umgang mit gespeicherten Daten am Beispiel der Niederlande

Nach der Stellungnahme des Chaos Computer Clubs resultiert die Intensität des Eingriffs aus der Kombination der Verbindungsdatensätze und deren automatisierter Auswertungsmöglichkeit.[211] Ein einfaches Beispiel kann zeigen, wie gefährlich der Umgang mit gespeicherten Daten für den Betroffenen, aber auch für das Kommunikationsverhalten einer ganzen Gesellschaft sein kann. So führt die Vorratsdatenspeicherung zu einer Verbreiterung der Basis der zu analysierenden Daten. In den Niederlanden gibt es bereits ein Projekt, bei dem Personen die zwar verdächtigt werden, denen aber keine konkreten kriminellen Vorgehensweisen nachgewiesen werden können, mit einer Vielzahl an sich legaler Einzelmaßnahmen, wie Steuerprüfungen, Kontrollen durch die Gewerbeaufsicht etc. konfrontiert werden, die über das normale Maß hinausgehen, bei den Betroffenen aber einen erheblichen Leidensdruck erzeugen können und diese in ihrem gesellschaftlichen und politischen Engagement stark beeinträchtigen können. Die Betroffenen haben keine rechtliche Handhabe dagegen und sind über das Vorliegen von Verdächtigungen ihnen gegenüber nicht informiert.[212]

(2) Die Bedeutung des Informationszugangs unter Berücksichtigung der Datenschutzrichtlinie

Bei der Prüfung der Erfolgsaussichten einer Klage muss soweit es um die Schwere des Eingriffs geht, auch die überragende Bedeutung, die dem Gut der Information in der heutigen Gesellschaft zukommt, berücksichtigt werden. So stellt der Datenschutz, zusammen mit dem Informationszugang eine der tragenden Säulen der Informationsgesellschaft dar. Daraus ergeben sich besondere Gefahren, wenn der Einzelne nicht sicher sein kann, welche personenbezogenen Daten über ihn an welcher Stelle vorhanden sind, aber auch, wenn ihm wesentliche Daten vorenthalten werden.[213] Ein umfassender Schutz kann daher heute nicht mehr gewährleistet werden, wenn man den Gewährleistungsgehalt auf die abwehrrechtliche Dimension des Schutzes in der Privatsphäre beschränkt.[214] Dabei ist von Bedeutung, dass die legal gesammelten Daten

211 Kurz/Rieger 2009, 3.
212 Kurz/Rieger 2009, 14 f.
213 Trute, JZ 1998, 822 f.
214 Hatje, in: Magiera/Sommermann, 193, 207.

von staatlicher Seite stets so aufzubereiten und zu pflegen sind, dass einerseits die grundrechtlichen Gefährdungen auf ein Mindestmaß reduziert werden, gleichzeitig aber auch die Aufgaben unter den Bedingungen optimal erfüllbar sind. Vor diesem Hintergrund ist die allgemeine Informationsvorsorge nicht vertretbar. Soweit es nämlich um personenbezogene Daten geht, verbietet das Grundrecht auf Datenschutz eine gleichsam präventive Datensammlung oder auch Datendepots, deren Zweckrichtung erst anlässlich eines sich später entwickelnden Bedarfs festgelegt wird.[215]

Verstärkt wird diese Argumentation durch den Umstand der entstehenden Kostenlast für die Speicherung des Datenvolumens, die zunächst die Telekommunikationsunternehmen und über die Gebühren letztlich den Telekommunikationsnutzer treffen. Nach Berechnungen des Branchenverbandes BITKOM handelt es sich dabei um Anlaufinvestitionen in Höhe von 150 Mio. Euro ohne Berücksichtigung der Kosten für den laufenden Betrieb. Die anlassbezogene Speicherung der Daten würde dagegen zu einem geringeren Aufwand für die privaten Anbieter führen und diese weniger in ihrer wirtschaftlichen Betätigungsfreiheit belasten.

Zwar ist die Heranziehung privater Unternehmen zur Verbrechensbekämpfung nicht grundsätzlich unzulässig, sondern wird im Gegenteil bereits nach geltendem Recht praktiziert. Allerdings können öffentliche Aufgaben, wie die Wahrung der Sicherheit und Ordnung, nicht in beliebigem Maße auf Private übergewälzt werden, ohne dass diese eine Entschädigung erhalten. Angesichts der Höhe der notwendigen Investitionen und der bereits angesprochenen zweifelhaften Erfolgsaussicht der Maßnahmen erscheint die Vorratsdatenspeicherung auch im Hinblick auf den Kostenpunkt als höchst zweifelhaft.[216]

(3) Zwischenergebnis

Zusammenfassend lässt sich feststellen, dass die Richtlinie 2006/24/EG einen Eingriff in Art. 8 Abs. 1 GRC darstellt, der verfassungsmäßig nicht gerechtfertigt ist. Zwar ist die Zweckbindung nach Treu und Glauben i.S.v. Art. 8 Abs. 2 S. 1 GRC erfüllt und die Richtlinie stellt eine legitime gesetzliche Grundlage dar;[217] das verfolgte Ziel einer effektiven Strafverfolgung steht dem Eingriff in den Schutz personenbezogener Daten jedoch unverhältnismäßig gegenüber. Die Tatsache, dass der Datenschutz zur Wahrung der Selbstbestimmung der privatautonomen Staatsbürger unabdingbar ist, begrenzt die

215 Mit Blick auf die Datenschutzrichtlinie vgl. Jacob, DuD 2000, 5 f.; Simitis, NJW 1997, 281, 285.
216 Büllingen, DuD 2005, 349 f.
217 Die nach Urteil des Gerichtshofs vom 10. Februar 2009 ebenfalls auf einer legitimen Rechtsgrundlage (Art. 95 EG) beruht.

Möglichkeiten seiner Einschränkung von vornherein. Die Schwere des Eingriffs ist aufgrund der Missbrauchsanfälligkeit enorm. Auch die unter dem Erfordernis der Vorhersehbarkeit erläuterten Konsequenzen für eine demokratische Gesellschaft, aber auch für eine Gesellschaft, die auf Informationen angewiesen ist, implizieren die Schwere des Grundrechtseingriffs. Die erheblichen Kosten für die Diensteanbieter, die in keinem Verhältnis zur tatsächlichen Verwendung der Daten stehen, sind ein weiteres Argument, weshalb die Richtlinie nicht angemessen ist. Der zu erwartende geringe Gewinn für die öffentliche Sicherheit, der bereits bei der Prüfung des Fernmeldegeheimnisses anhand der vorhandenen Daten belegt wurde, steht diesem schweren Grundrechtseingriff unverhältnismäßig gegenüber. Sollte daher eine Klärung der Verfassungsmäßigkeit im Rahmen des Vorabentscheidungsverfahrens angestrengt werden, muss damit gerechnet werden, dass der Gerichtshof die Richtlinie 2006/24/EG für verfassungswidrig und damit für nichtig erklärt.

III. Wären die Mitgliedstaaten der EU unter diesen Voraussetzungen zur Umsetzung der Richtlinie 2006/24/EG verpflichtet gewesen?

Eine Pflicht zur Umsetzung gilt jedenfalls insoweit nicht, als dass Vorgaben über die Richtlinie hinausgehen. Eine solche besteht jedoch auch für Rechtsakte nicht, die mit einem Fehler behaftet sind, dessen Schwere so offensichtlich ist, dass er von der Gemeinschaftsrechtsordnung nicht geduldet werden kann.[218] In einem solchen Fall ist der Rechtsakt von vornherein inexistent. Obwohl der Europäische Gerichtshof grundsätzlich von der Vermutung der Rechtmäßigkeit ausgeht,[219] wiegt der bereits geprüfte Verstoß gegen Gemeinschaftsgrundrechte jedoch so schwer, dass eine Umsetzungspflicht entfällt. Die formelle Rechtmäßigkeit zur Kompetenz der Gemeinschaft zum Erlass der Richtlinie hat der Gerichtshof in seinem Urteil vom 10. Februar 2009 zwar bereits bestätigt,[220] in materieller Hinsicht liegt jedoch ein offensichtlicher Verstoß gegen Art. 8 Abs. 1 GRC vor.[221]

Die Richtlinie 2006/24/EG ist grob unverhältnismäßig, weil dadurch das Regelungssystem der Grundrechte in das Gegenteil verkehrt wird. Den Grundrechten zufolge ist das grundrechtlich geschützte Verhalten grundsätzlich frei und Einschränkungen sind nur zulässig, soweit diese erforderlich sind. Die

218 EuGH, Rs. C-475/01, Slg. 2004, I-8923, Rn. 19; st. Rspr.
219 EuGH, Rs. C-475/01, Slg. 2004, I-8923, Rn. 18.
220 EuGH, Rs. C-301/06, Slg. 2009, Rn. 93.
221 Siehe auch D.II.3.b)dd)(3).

Vorratsdatenspeicherung erklärt den Eingriff dagegen zum Normalfall und setzt keine Erforderlichkeit voraus.[222]

Zur Umsetzung der Richtlinie 2006/24/EG wäre Deutschland aber auch dann nicht verpflichtet gewesen, wenn nach dem Europäischen Gerichtshof eine Umsetzungspflicht bestanden hätte, da Normen die gegen primäres Gemeinschaftsrecht verstoßen vom deutschen Zustimmungsgesetz zum EG-Vertrag nicht gedeckt sind.[223] Die Bundesregierung sieht in ihrer Stellungnahme zur Verfassungsbeschwerde gegen §§ 113a, b TKG nur dann keine ausreichende Deckung mehr, wenn die Europäische Gemeinschaft ohne jede rechtliche Grundlage gehandelt hat und es ihr damit an einer völkerrechtlichen Ermächtigung für den erlassenen Rechtsakt fehlt.[224] Die Voraussetzung einer mangelnden Deckung kann jedoch ausschließlich nicht ausreichen, da damit auch Rechtsakte gedeckt wären, die Primärrecht in seinem Kern verletzen, und die zusätzlich auf einer falschen Rechtsgrundlage beruhen. Das kann jedoch nicht Ziel eines völkerrechtlichen Ansatzes sein. Vielmehr muss davon ausgegangen werden, dass ein Verstoß gegen primäres Gemeinschaftsrecht und damit eine Überschreitung der im EG-Vertrag übertragenen Hoheitsbefugnisse eine Umsetzung der Richtlinie 2006/24/EG entbehrlich gemacht hätte.[225]

E. Erfolgsaussichten einer Klage vor dem Europäischen Gerichtshof für Menschenrechte

I. Prüfung der Klagemöglichkeiten

Nach Art. 34 EMRK kann jede natürliche Person, nichtstaatliche Organisation oder Personengruppe, eine Individualbeschwerde zum EGMR mit der Behauptung in ihren durch die EMRK oder in einem ihrer Zusatzprotokolle zugesicherten Rechte verletzt zu sein, erheben. Die Zulässigkeit der Individualbeschwerde setzt gem. Art. 35 EMRK die Erschöpfung des innerstaatlichen Rechtswegs voraus. Dabei gehört die Verfassungsbeschwerde zum Bundesverfassungsgericht nach gefestigter Rechtsprechung des EGMR zum vorab zu durchlaufenden Rechtsweg im Sinne des Art.

222 Arbeitskreis Vorratsdatenspeicherung/Netzwerk Neue Medien e.V./Neue Richtervereinigung e.V. 2007, 8.
223 BVerfGE 89, 155, 188.
224 Stellungnahme der Bundesregierung vom 28. November 2008, 18.
225 Arbeitskreis Vorratsdatenspeicherung/Netzwerk Neue Medien e.V./Neue Richtervereinigung e.V. 2007, 9.

35 EMRK.[226]

Der EGMR hat einen Weg gefunden die Einhaltung der EMRK-Gewährleistungen auch auf Ebene des Gemeinschaftsrechts zu überprüfen. Alle Mitgliedstaaten der EU sind Vertragsparteien der EMRK.[227] Selber ist die EU der EMRK bisher allerdings noch nicht beigetreten. Der EGMR hat entschieden, dass die Konvention die Übertragung von Hoheitsgewalt auf eine internationale Organisation nicht ausschließt, solange gewährleistet ist, dass der Schutz der Konventionsrechte weiterhin sichergestellt ist. Die Vertragsparteien können sich ihrer Verpflichtung aus der EMRK nicht dadurch entledigen, dass sie Hoheitsbefugnisse auf eine supranationale Organisation übertragen, sie bleiben der EMRK daher auch im Rahmen des Gemeinschaftsrechts verantwortlich.[228] Es ist dem EGMR deshalb grundsätzlich möglich, eine nationale Umsetzungsmaßnahme eines Mitgliedsstaates auf deren Vereinbarkeit mit den Konventionsgewährleistungen zu überprüfen. Der EGMR hat die Einlegung einer Beschwerde somit für unzulässig erachtet, solange auf der Ebene des Gemeinschaftsrechts ein effektiver und der EMRK vergleichbarer Grundrechtsschutz besteht. Eine Klage vor dem Europäischen Gerichtshof für Menschenrechte (EGMR) hat deshalb nur dann Aussicht auf Erfolg, wenn der Grundrechtsschutz der EU gemessen am Standard der Europäischen Menschenrechtskonvention (EMRK) „offensichtlich unzulänglich“ wäre. Das hat der EGMR in seiner „Bosporus-Entscheidung“[229] neu geregelt. Damit nimmt der EGMR wie das Bundesverfassungsgericht ein Letztentscheidungsrecht für sich in Anspruch. Im Gegensatz zum Bundesverfassungsgericht, geht es dem EGMR dabei weniger um eine Korrektur der Entscheidungen des EuGH, er behält sich aber eine Überprüfung im Einzelfall vor.[230]

Die Bundesrepublik Deutschland ist auch der EMRK beigetreten. Die Umsetzung der EMRK erfolgte wie bei anderen völkerrechtlichen Verträgen in Form eines Bundesgesetzes gem. Art. 59 Abs. 2 GG. Bei der Auslegung des Grundgesetzes sollen Inhalt und Entwicklung der EMRK sowie die Rechtsprechung des EGMR berücksichtigt werden. Der Grundrechtsschutz der EMRK kann dabei über den des GG

226 Breuer, JZ 2003, 433, 440 m. w. N.
227 Vormbaum 2005, 160.
228 EGMR Urt. vom 18. Februar 1999, *Matthews v. Vereinigtes Königreich,* (Rs. 24833/94), Rn. 200 201.
229 EGMR, Urt. vom 30. Juni 2005, *Bosphorus Hava Yollari Turizm Ticaret Anonim Sireketi v. Irland*, (Rs. 45036/98), Rn. 155.
230 Kahler, DuD 2008, 453.

hinausgehen. Erreicht also der AK Vorratsdatenspeicherung sein Ziel durch die Verfassungsbeschwerde nicht, kann eine Individualklage vor dem EGMR Aussicht auf Erfolg haben. Sollte der EGMR in diesem Fall ein Urteil fällen, das inhaltlich einen weitergehenden Grundrechtsschutz gewährleistet als das Bundesverfassungsgericht, sind die innerstaatlichen Organe gleichwohl durch den völkerrechtlichen Vertrag an dieses Urteil gebunden. Der deutsche Gesetzgeber müsste dann die notwendigen Anpassungen vornehmen.[231]

Für den vorliegenden Fall der Vorratsdatenspeicherung bedeutet dies, dass den Klägern die Möglichkeit einer Individualbeschwerde vor dem EGMR nach Art. 34 EMRK offenstehen würde, wenn das Bundesverfassungsgericht kein Vorabentscheidungsverfahren vor dem EuGH anstreben würde und die Umsetzung der Vorratsdatenspeicherung in Deutschland für verfassungsgemäß erklären würde. Würde das Bundesverfassungsgericht dagegen die Frage der Grundrechtskonformität zur Vorabentscheidung dem EuGH vorlegen und dieser würde die Richtlinie 2006/24/EG für verfassungskonform erklären, so wäre das Bundesverfassungsgericht an diese Entscheidung gebunden und eine Klage vor dem EGMR hätte Aussicht auf Erfolg, wenn dieser den Grundrechtsschutz auf Gemeinschaftsebene nicht als effektiv und mit der EMRK vergleichbar ansieht.

Unabhängig davon, ob eine Klage vor dem EGMR überhaupt erhoben werden muss, sind im Folgenden die Voraussetzungen zu prüfen, soweit es zu einer Überprüfung der EMRK kommt. In Betracht kommt das Recht auf Achtung des Privatlebens und der Korrespondenz aus Art. 8 EMRK.

II. Recht auf Achtung des Privatlebens und der Korrespondenz (Art. 8 EMRK)

1. Schutzbereich

Der Datenschutz ist hauptsächlich über das Recht auf Achtung des Privatlebens aus Art. 8 Abs. 1 EMRK erfasst.[232] Auf die Definition des Privatlebens hat der EGMR ausdrücklich verzichtet.[233] Der Begriff des Privatlebens dürfte jedoch im Zusammenhang mit den Ausführungen des EGMR zur Korrespondenz eher weit zu

231 Kahler, DuD 2008, 453.
232 Siemen 2006, 57.
233 Uerpmann-Wittzack, in: Becker/Ehlers 2005, 64.

verstehen sein und über den inneren Bereich menschlichen Daseins auch den Kontakt zur Außenwelt erfassen. Er ist damit vom öffentlich-staatlichen Bereich abzugrenzen.[234] Bestandteil des Rechts auf Privatleben ist auch das Recht auf Privatsphäre, welches als negativer Abwehranspruch gegen staatliche Übergriffe dient.[235] Der Schutzbereich umfasst neben einem aktiven Element, welches sich auf die Selbstbestimmung des Einzelnen bezieht, auch ein passives Element, das sich am Schutz vor Öffentlichkeit orientiert.[236] Auch das Herstellen und Entfalten von Beziehungen zu anderen Menschen ist vom Recht auf Achtung des Privatlebens erfasst.[237] Der EGMR hat zudem wiederholt entschieden, dass auch Telefongespräche als Korrespondenz i.S.d. Art. 8 EMRK gelten.[238] Die näheren Umstände der Telekommunikation fallen ebenfalls unter den Schutzbereich.[239] Grund ist das eine vergleichbare Gefährdungslage hinsichtlich der räumlich distanzierten Kommunikation besteht. Der EGMR hat auch die Sammlung und Speicherung von Daten als in den Schutzbereich von Art. 8 EMRK fallend anerkannt. Da die Richtlinie 2006/24/EG eine Speicherung von Daten auf Vorrat vorsieht, ist der Schutzbereich des Art. 8 EMRK tangiert.

2. Eingriff

Art. 8 Abs. 2 EMRK lässt sich entnehmen, dass ein Eingriff eine Maßnahme voraussetzt, die die Ausübung des Rechts auf Achtung des Privatlebens einschränkt.[240] Eine systematische Eingriffsdogmatik zur EMRK wurde bislang jedoch nicht entwickelt. Das Vorgehen ist vielmehr kasuistisch.[241] So stellt der EGMR vielfach gar nicht darauf ab, ob die Nachteilszufügung final oder unbeabsichtigt, unmittelbar oder mittelbar erfolgt ist. In Einzelfällen kann sich die Lage anders darstellen, weil zum Beispiel eine gewisse Intensität der Beeinträchtigung verlangt wird, grundsätzlich herrscht jedoch die Tendenz vor, keine besonderen Anforderungen an den Eingriff zu stellen.[242] Der Gerichtshof erkennt aber allgemein an, dass die Sammlung und Speicherung personenbezogener Daten einen Eingriff in das Privatleben des Einzelnen

234 Uerpmann-Wittzack, in: Becker/Ehlers 2005, 64.
235 Siemen, 2006, 71.
236 Siemen 2006, 63.
237 Siemen 2006, 72.
238 EGMR, Urt. vom 27. Mai 2003, *Craxi v. Italien,* (Rs. 25337/94), Rn. 57; EGMR, Urt. vom 27. April 2004, *Doerga v. Niederlande,* (Rs. 50210/99), Rn. 43.
239 EGMR, Urt. vom 3. April 2007, *Copland v. UK,* (Rs. 62617/00), Rn. 41 ff.
240 Siemen, 2006, 133.
241 Vgl. Schilling, 2004, 21.
242 Vgl. Roth 1994, 58 ff.

darstellt, ebenso wie die Verwendung und Verweigerung der Löschung.[243] Dabei handelt es sich bei der Speicherung und der Weitergabe der Informationen jeweils um eigenständige Eingriffe.[244] In der Vergangenheit hat der EGMR entschieden, dass die Erhebung von Verbindungsdaten ohne Einwilligung des Betroffenen einen Eingriff in dessen Rechte auf Achtung der Korrespondenz und des Privatlebens darstellt, weil Verbindungsdaten, „besonders die gewählten Nummern […] integraler Bestandteil der Kommunikation" seien.[245] Dies gilt auch für die E-Mail und Internetnutzung.[246] Ein Eingriff in Art. 8 Abs. 1 EMRK liegt damit vor.

3. Verfassungsmäßige Rechtfertigung

Verhältnismäßigkeit

Im Vergleich zur Verhältnismäßigkeitsprüfung im deutschen Recht weist die Vorgehensweise des Gerichtshofs einige Besonderheiten auf. So wird die Eignung der Maßnahme schon bei der Prüfung des legitimen Ziels untersucht. Auch die Erforderlichkeit wird nicht gesondert geprüft. Die Prüfung ob ein milderes, gleich geeignetes Mittel zur Verfügung steht, wird aber in der Abwägung vorgenommen.[247] Diesbezüglich ist vorliegend jedoch auf die Ausführungen ab S. 23 verwiesen.

Zu detaillierteren Verhältnismäßigkeitsprüfungen und damit einer Beschränkung des Beurteilungsspielraums der Mitgliedstaaten kommt es vor allem bei Maßnahmen, denen ein besonders schwerwiegender Eingriff zugrunde liegt, oder die besonders sensible Bereiche betreffen.[248]

aa) Legitimes Ziel

Die zulässigen Ziele werden in Art. 8 Abs. 2 EMRK abschließend aufgezählt. Vorliegend kommt die öffentliche Sicherheit sowie die Verhütung von Straftaten in Betracht. Die Geeignetheit der Richtlinie für die Erreichung dieser Ziele wurde bereits auf S. 51 geprüft und zunächst bejaht.

---

243 EGMR, Urt. vom 26. März 1987, *Leander v. Schweden*, (Rs. 9248/81), Rn. 48.
244 Siemen, 2006, 135.
245 EGMR, Urt. vom 2. August 1984, *Malone v. GB*, (Rs. 8691/79), Rn. 84.
246 EGMR, Urt. vom 3. April 2007, *Copland v. UK*, (Rs. 62617/00), Rn. 41.
247 So etwa in EGMR Urt. vom 28. Januar 2003, *Peck v. UK,* (Rs. 44647/98), Rn. 80.
248 Siemen 2006, 157.

bb) Angemessenheit

Eingriffe in den Schutzbereich des Art. 8 EMRK bedürfen der Rechtfertigung. Wie die Mehrzahl der Konventionsrechte gewährt Art. 8 EMRK kein absolutes Recht, sondern enthält in seinem Abs. 2 Möglichkeiten der Einschränkung. Die durch Art. 8 Abs. 1 EMRK gewährten Rechte werden also nicht schrankenlos gewährleistet. Damit wird dem Gedanken Rechnung getragen, dass jeder menschliche Freiheitsanspruch schon wegen der gleichen Freiheitsrechte der Mitmenschen, Grenzen in sich trägt.[249] Nach Art. 8 Abs. 2 EMRK ist zunächst eine gesetzliche Grundlage erforderlich. Diesem Erfordernis genügen nicht nur verbindliche Rechtsnormen, sondern auch eine gefestigte innerstaatliche Rechtsprechung.[250] Aus dem Erfordernis einer gesetzlichen Grundlage in Verbindung mit dem Rechtsstaatsprinzip leitet der EGMR zudem ab, dass das innerstaatliche Recht hinreichend bestimmt und für den Bürger zugänglich sein muss.[251] Die Anforderungen an die Vorhersehbarkeit hängen im Einzelnen von der Eingriffstiefe der jeweiligen Maßnahme ab.[252]

Des Weiteren muss das nationale Recht einen hinreichenden und effektiven Schutz vor willkürlichen Eingriffen und vor Missbrauch der eingeräumten Befugnisse gewährleisten. Der Gerichtshof betont, dass dieses Risiko gerade bei Maßnahmen ohne Wissen der Betroffenen evident sei.[253] Welche rechtsstaatlichen Sicherungen gefordert werden hängt vom Einzelfall ab, insbesondere von der Art, dem Umfang und der Dauer möglicher Maßnahmen.[254]

(1) Der Schutz vor Missbrauch der gespeicherten Daten

An der hinreichenden Bestimmung der gesetzlichen Grundlage bestehen bei der Richtlinie 2006/24/EG keine Zweifel. Es ist jedoch fraglich, ob ein ausreichender Schutz vor Missbrauch gewährleistet ist. Nach § 113 a Abs. 10 TKG muss der Diensteanbieter die im Bereich der Telekommunikation erforderliche Sorgfalt beachten. Vor diesem Hintergrund hat er durch technische und organisatorische Maßnahmen sicherzustellen, dass der Zugang zu den gespeicherten Daten ausschließlich von ihm hierzu ermächtigten Personen möglich ist. Die Richtlinie führt dazu in Art. 7 aus, dass

249 Siemen, 2006, 138.
250 EGMR, Urt. vom 24. April 1990, *Huvig v. Frankreich*, (Rs. 11105/84), Rn. 28.
251 EGMR, Urt. vom 26. April 1979, *Sunday Times v. GB*, (Rs. 6538/74), Rn. 49.
252 EGMR, Urt. vom 25. März 1998, *Kopp v. Schweiz*, (Rs. 13/1997/797/1000), Rn. 72.
253 EGMR, Urt. vom 2. August 1984, *Malone v. GB*, (Rs. 8691/79), Rn. 67, 81.
254 EGMR, Urt. vom 6. September 1978, *Klass u.a. v. Deutschland,* (Rs. 5029/71), Rn. 50.

geeignete technische und organisatorische Maßnahmen getroffen werden müssen, um die Daten gegen Zerstörung, Verlust oder Änderung, unberechtigte oder unrechtmäßige Speicherung, Verarbeitung, Zugänglichmachung oder Verbreitung zu schützen. Angesichts der kommerziellen Interessen, die mit den gespeicherten Daten verbunden sein dürften, besteht dennoch eine große Gefahr des Missbrauchs. Dieser wird jedoch gesetzlich kaum hundertprozentig effektiv begegnet werden können.

(2) Das Kriterium der „Notwendigkeit“

Die Maßnahme muss außerdem in einer demokratischen Gesellschaft notwendig für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer sein. Dabei hat sich nach und nach durchgesetzt, dass der Terminus Notwendigkeit nicht mit Erforderlichkeit, sondern mit Verhältnismäßigkeit gleichzusetzen ist.[255] Bei der gesellschaftlichen Notwendigkeit handelt es sich um eine Konkretisierung des Gesichtspunktes der Angemessenheit.[256] Dieses Kriterium stellt das Herzstück des durch Art. 8 EMRK vorgesehenen Schutzmechanismus dar.[257]

Es ist also zu prüfen, ob der fragliche Eingriff in einer demokratischen Gesellschaft für die Erreichung des mit ihm verfolgten berechtigten Zweckes notwendig ist. In Betracht kommt vorliegend die Notwendigkeit für die öffentliche Sicherheit. Nach der Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte bedeutet das Eigenschaftswort „notwendig“ in Artikel 8 Absatz 2 EMRK, dass ein „zwingendes gesellschaftliches Bedürfnis“ bestehen und die Maßnahme „in einem angemessenen Verhältnis zu dem verfolgten berechtigten Zweck“ stehen muss.[258] Die nationalen Behörden verfügen zudem über ein Ermessen, „dessen Umfang nicht nur von der Zielsetzung, sondern auch vom Wesen des Eingriffs abhängig ist“.[259] In diesem Sinne ist das Interesse an der öffentlichen Sicherheit durch eine effektivere Strafverfolgung mit der Beeinträchtigung des Rechts der Betroffenen auf Achtung ihres Privatlebens abzuwägen. Diese Abwägung wurde bereits im Rahmen der Angemessenheitsprüfung der Verfassungsbeschwerde mit dem Ergebnis, dass die Maßnahme der Speicherung von

255 Vgl. EGMR, EuGRZ 1990, 255, Rn. 70 – Groppera Radio AG.
256 Mehde, in: Nowak/Hesselhaus 2006, 626 f.
257 Siemen, 2006, 153.
258 Vgl. u. a. EGMR, Urt. vom 24. November 1986, *Gillow v. GB*, (Rs. 9063/80), Rn. 55.
259 Vgl. EGMR, Urt. vom 26. März 1987, *Leander v. Schweden*, (Rs. 9248/81), Rn. 59.

Daten auf Vorrat zur Gewährleistung der öffentlichen Sicherheit der Schwere des Eingriffs in das Privatleben unverhältnismäßig gegenübersteht, vorgenommen. Die Ausführungen zu Art. 10 Abs. 1 GG und zu Art. 8 Abs. 1 GRC haben letztlich gezeigt, dass eine Abwägung im Rahmen des Verhältnismäßigkeitsgebots zu dem Ergebnis kommt, dass der Eingriff unverhältnismäßig ist. Die Unverhältnismäßigkeit ergibt sich insbesondere daraus, dass einem Bruchteil tatsächlich nachgefragter Daten (etwa 0,0004 %)[260] ein erheblicher Anteil von Betroffenen gegenübersteht, deren Daten ohne jedes Verdachtsmoment gespeichert werden.

Es bleibt aber noch zu prüfen, ob dem Erfordernis der Notwendigkeit im Sinne eines zwingenden gesellschaftlichen Bedürfnisses Genüge getan ist. Das Verwaltungsgericht Wiesbaden hat in seinem Beschluss vom 27.02.2009 eine solche Notwendigkeit in einer demokratischen Gesellschaft nicht gesehen. So gebe der Einzelne keine Veranlassung für einen Eingriff, kann aber bei legalem Verhalten wegen der Risiken des Missbrauchs und des Gefühls der Überwachung eingeschüchtert werden.[261] Bereits 1981 hat es das Kommissionsmitglied Klecker als nicht notwendig und damit nicht gerechtfertigt angesehen, dass Daten von Personen weiter aufbewahrt werden, von denen sich herausgestellt hat, dass diese zu Unrecht verdächtigt werden.[262] Erst Recht darf eine Notwendigkeit doch dann nicht bestehen, wenn Daten von Personen gespeichert werden, die noch nicht mal einen Anlass dazu gegeben haben. Das Vorliegen eines zwingenden gesellschaftlichen Bedürfnisses kann auch vor dem Hintergrund angezweifelt werden, der die mangelnde Eignung der Vorratsdatenspeicherung zur Erreichung des Ziels einer effektiven Strafverfolgung betrifft.[263] So kann das Ziel der öffentlichen Sicherheit zwar als ein zwingendes Bedürfnis angesehen werden, das Mittel, welches vorliegend dafür eingesetzt werden soll dieses Ziel zu erreichen, entbehrt jedoch jeder Notwendigkeit.

In der Rechtssache *Klass* haben die Strassburger Organe der Abwehr und Bedeutung terroristischer Akte eine große Bedeutung beigemessen und sie letztendlich zu dem Schluss veranlasst, dass gesetzliche Bestimmungen, die zur geheimen Überwachung der

260 Uhe/Herrmann, http://ig.cs.tu-berlin.de/oldstatic/da/2003-08/UheHerrmann-Diplomarbeit-082003.pdf, (11.06.09), 161.
261 VG Wiesbaden, Beschluss vom 27. Februar 2009, AZ 6 K 1045/08.WI, Rn. 28. (http://www.jurpc.de/rechtspr/20090114.htm).
262 Abweichende Meinung des Kommissionsmitglieds Klecker im Fall EKMR, Urt. vom 18. März 1981, *Mc Veigh u.a. v. GB,* (Rs. 8022/77), DR 25, S. 56.
263 Siehe auch C.II.4.b)bb)(2).

Kommunikation ermächtigen, in einer demokratischen Gesellschaft „bei einer außergewöhnlichen Situation zum Schutz der nationalen Sicherheit notwendig sind." Die Rechtsprechung des EGMR zeigt damit, dass die Bedrohung des Staates durch Terroristen als sehr ernste Gefahr betrachtet wird. In der Folge können zur Bekämpfung des Terrorismus relativ schwerwiegende Eingriffe in das Recht auf Achtung des Privatlebens als verhältnismäßig beurteilt werden. Trotzdem stellt dies nur eines der zu berücksichtigenden Interessen dar.[264] So legt der Gerichtshof gleichzeitig einen strengen Maßstab zugrunde, wenn er angibt: „Powers of secret surveillance of citizens, characterising as they do the police state, are tolerable under the Convention only insofar as *strictly necessary for safeguarding the democratic institutions.* "[265]

Die Bedrohung der nationalen Sicherheit durch terroristische Akte hat sich zudem inzwischen gewandelt, aber nicht unbedingt verringert. Die genannten Entscheidungen beziehen sich in erster Linie auf den Terrorismus der 70er Jahre, dürften aber trotzdem auch heute noch Geltung beanspruchen.[266]

Insgesamt lässt der Gerichtshof Maßnahmen, die dem Schutz der nationalen Sicherheit dienen, eine große Bedeutung zukommen. Er hat allerdings auch darauf hingewiesen, dass die Daten der damaligen Entscheidungen nicht der elektronischen Datenverarbeitung zugeführt wurden.[267] Heute muss davon ausgegangen werden, dass Daten grundsätzlich der elektronischen Datenverarbeitung zugeführt werden und die technischen Möglichkeiten immer ausgereifter werden. Damit kommt dem Schutz personenbezogener Daten eine ganz andere Bedeutung zu. Es ist daher davon auszugehen, dass der Gerichtshof den Interessen des Individuums heute mehr Gewicht zumessen wird. Das wird auch deutlich, wenn man sich die letzten beiden Entscheidungen des EGMR zum Datenschutz ansieht, deren Prüfung soweit es um die Abschätzung der Erfolgsaussichten einer Klage geht, unerlässlich ist.

(3) Rechtsprechung des EGMR zur Speicherung von Fingerabdrücken und DNA-Proben

In seinem Urteil vom 4. Dezember 2008 zur Speicherung von Fingerabdrücken und DNA Proben hat der EGMR die Bedeutung des Datenschutzes für das Privatleben, wie

264 Siemen 2006, 161.
265 EGMR, Urt. vom 6. September 1978, *Klass u.a. v. Deutschland,* (Rs. 5029/71), Rn. 48.
266 Siemen 2006, 164.
267 EGMR, Urt. vom 19. Mai 1994, *Ludwig Friedl v. Österreich,* (Rs. 15225/89).

es in Art. 8 der Konvention gewährleistet ist, noch einmal ausdrücklich betont und auf die Notwendigkeit des Schutzes dieser Daten durch das nationale Recht für jede Verwendung die gegen die Garantien aus Art. 8 verstoßen, hingewiesen. Des Weiteren stellt der EGMR ganz klar fest:“ The domestic law should notably ensure that such data are relevant and not excessive in relation to the purposes for which they are stored; and preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.“[268] Damit gibt er deutlich zu verstehen, dass die gespeicherten Daten eine Relevanz haben müssen, die im Falle der Vorratsdatenspeicherung für den Großteil jedoch gar nicht vorliegt, da dieser keiner weiteren Verwendung dient und damit nicht von Bedeutung ist. Außerdem betont der EGMR, dass die Daten nicht länger gespeichert werden dürfen, als es zur Erreichung des verfolgten Zwecks notwendig ist. Zu diesem Punkt liegen bereits Erkenntnisse vor, die belegen, dass eine Abfrage durch die Strafverfolgungsbehörden in der Regel einen Zeitraum von drei Monaten betrifft[269], die Richtlinie 2006/24/EG sieht jedoch einen Zeitraum von mindestens 6 Monaten vor.

Der Gerichtshof bezeichnet die Speicherung der Fingerabdrücke als rücksichtslos, auch weil die Speicherung unabhängig von der tatsächlichen Schuld vorgenommen wird.[270] Unschuldige Personen werden damit genauso behandelt, wie solche die einer Straftat verdächtigt werden.[271] Bei der Vorratsdatenspeicherung werden Daten sogar ohne einen konkreten Verdacht gespeichert, so dass unabhängig von der Aussagekraft des jeweils zu speichernden Materials zunächst von einem noch schwererer wiegenden Eingriff ausgegangen werden muss. Dafür spricht außerdem, dass in der englischen Datensammlung bis zu drei Angaben, nämlich Fingerabdruck, Gewebeprobe und DNA-Profil gespeichert wurden, während die Vorratsdatenspeicherung das gesamte Kommunikations- und Bewegungsverhalten erfasst. Da die auf Vorrat gespeicherten Daten Rückschlüsse auf die Persönlichkeit und das private und berufliche Leben zulassen, haben sie zudem einen wesentlich höheren Aussagegehalt als biometrische Merkmale, wie sie in England erfasst wurden. Soweit der Europäische Gerichtshof für Menschenrechte in der Sammlung biometrischer Daten aller Verdächtigen eine Verletzung des Verhältnismäßigkeitsgebots sieht, muss dieses folglich erst Recht für die

268 EGMR, Urt. vom 4. Dezember 2008, *S. und Marper v. GB,* (Rs. 30562/04 und 30566/04), Rn. 103.
269 Westphal, EuR 2006, 706, 715.
270 EGMR, Urt. vom 4. Dezember 2008, *S. und Marper v. GB,* (Rs. 30562/04 und 30566/04), Rn. 119.
271 EGMR, Urt. vom 4. Dezember 2008, *S. und Marper v. GB,* (Rs. 30562/04 und 30566/04), Rn. 122.

Vorratsdatenspeicherung gelten.[272]

(4) Urteil des EGMR gegen Finnland

Im Urteil gegen Finnland vom 02.12.2008 kommt der EGMR allerdings zu einem anderen Schluss. Darin hat er entschieden, dass eine positive Verpflichtung des Staates besteht, Straftaten auch zu sanktionieren und die abschreckende Wirkung der Kriminalisierung durch eine wirksame Ermittlung und Strafverfolgung zu verstärken, insbesondere dann, wenn gravierende Eingriffe in grundlegende Aspekte des Privatlebens vorliegen, die das physische und moralische Wohlergehen eines Kindes beeinträchtigen.[273] Danach müssen die Vertraulichkeit der Kommunikation und die Privatsphäre hinter der Verhütung von Straftaten zurücktreten soweit es der effektiven Strafverfolgung im Fall schwerer Beeinträchtigungen dient.[274] In diesem Fall scheint vor allem die Sensibilität des verletzten Rechtsguts und die Tatsache das es sich um den Schutz eines Kindes handelt für die Entscheidung ausschlaggebend gewesen zu sein. Es erscheint insgesamt jedoch schwierig, daran eine grundsätzliche Richtung des EGMR auszumachen, insbesondere deshalb, weil hier der Eindruck entsteht, dass es sich um einen besonders gelagerten Einzelfall handelt, der einer ungleich höheren Anzahl von Fällen gegenübersteht, die von der Vorratsdatenspeicherung betroffen wären. Auch im Falle von Foltermethoden mag es einzelne Fälle geben, bei denen diese zum Erfolg führen und zum Schutz elementarer Rechtsgüter verwendet werden könnten, letztlich darf aber auch dabei kein Zweifel an dem Verbot von Folter bestehen. Zwar gehört das Folterverbot zu den Menschenrechten, die absolute, ausnahmslose Rechtsgeltung haben und ist, wie es sich aus Art. 3 EMRK ergibt, nicht beschränkbar. Es stellt sich aber trotzdem ganz generell als problematisch dar, anhand einzelner Beispiele einen so elementaren Grundrechtseingriff zu rechtfertigen. Die Aufklärung einzelner Verbrechen kann damit insgesamt nicht gerechtfertigt werden, insbesondere dann nict, wenn die Maßnahme Gefahr läuft den Wesensgehalt von Grundrechten anzutasten. Schließlich ist eine demokratische Gesellschaft in der freie Kommunikation und der offene Austausch von Meinungen möglich ist, wichtiger als der Versuch jede Straftat aufzuklären.

Die Entscheidung steht auch deshalb nicht der Unverhältnismäßigkeit der Vorratsdatenspeicherung entgegen, da diesem Fall ein anderer Sachverhalt zugrunde

272 Starostik, Meinhard: Schriftsatz vom 23. Februar 2009, 4.
273 EGMR, Urt. vom 2. Dezember 2008, *K.U. v. Finnland,* (Rs. 2872/02), Rn. 46.
274 EGMR, Urt. vom 2. Dezember 2008, *K.U. v. Finnland,* (Rs. 2872/02), Rn. 49.

lag. Entscheidend ist hier, dass die Daten ohnehin vorhanden waren und das finnische Recht die Herausgabe nicht erlaubte.[275] Das gesetzlich zur Aufklärung schwerer Straftaten auf ohnehin zu betrieblichen Zwecken gespeicherte Daten zurückgegriffen werde darf, ist gar nicht in Frage gestellt. Auch hat der EGMR in dieser Entscheidung eine präventive Erfassung des gesamten Kommunikationsverhaltens der Bevölkerung nicht gefordert.[276] Daraus eine Konformität der Richtlinie 2006/24/EG mit den Rechten aus der EMRK abzuleiten, wäre also verfehlt.

(5) Zwischenergebnis

Insgesamt gesehen fällt es vor dem Hintergrund dieses Urteils und der Rechtsprechung in vergangenen Jahren relativ schwer zu beurteilen, wie der Gerichtshof entscheiden würde. Einerseits betont er die Bedeutung von Art. 8 EMRK für den Datenschutz und die Sensibilität mit der eine Abwägung erfolgen muss und andererseits hört für ihn der Datenschutz dort auf, wo er eine effektive Strafverfolgung bei schweren Beeinträchtigungen behindert und er erachtet gesetzliche Bestimmungen, die zur geheimen Überwachung der Kommunikation ermächtigen, in einer demokratischen Gesellschaft in außergewöhnlichen Situationen für notwendig, soweit sie dem Schutz der nationalen Sicherheit dienen.[277] Es ist jedoch sehr zweifelhaft, ob eine solch „außergewöhnliche Situation“, die eine Vorratsdatenspeicherung rechtfertigen könnte, derzeit besteht. Zumindest gibt es wenig Anhaltspunkte, die dafür sprechen. Entscheidendes Argument, die Richtlinie in Gegenüberstellung früherer Urteile, als einen Verstoß gegen Art. 8 EMRK zu werten, dürfte jedoch sein, dass die Daten heute der elektronischen Datenspeicherung zugeführt werden und sich damit eine deutlich andere Situation ergibt, als noch vor wenigen Jahren. Wie weit die technischen Möglichkeiten heute sind, wurde bereits bei Prüfung der Aussagekraft deutlich.[278] Zudem muss auch bei einer Entscheidung des EGMR berücksichtigt werden, dass es sich um eine anlasslose, flächendeckende Speicherung von Daten handelt, die diese rechtliche Vorschrift von allen anderen unterscheidet und die deshalb besonders tief in die Privatsphäre eines jeden Menschen eingreift. Ob der EGMR dieser Argumentation ein entsprechendes Gewicht einräumt, kann nicht abschließend geklärt werden.

275 EGMR, Urt. vom 2. Dezember 2008, *K.U. v. Finnland,* (Rs. 2872/02), Rn. 40.
276 Starostik, Meinhard: Schriftsatz vom 23. Februar 2009, 6.
277 EGMR, Urt. vom 6. September 1978, *Klass u.a. v. Deutschland,* (Rs 5029/71), Rn. 48.
278 Siehe auch C.II.4.b)bb))(4)(j).

F. Fazit

I. Zusammenfassung

Das Spannungsverhältnis zwischen Sicherheit und Rechtsstaat zieht sich durch die gesamte Arbeit und wird bei der Prüfung der Richtlinie 2006/24/EG immer wieder deutlich. Die Richtlinie zur Vorratsdatenspeicherung muss sich dabei durchgängig den Vorwurf gefallen lassen, dass sie den Erwartungen an Sicherheit, die sie erbringen soll, wegen erheblicher Zweifel an der Eignung der beschlossenen Maßnahmen, nicht gerecht werden kann. Demgegenüber scheint der Rechtsstaat unverhältnismäßig in Mitleidenschaft gezogen zu sein, betrachtet man die Schwere des Eingriffs in Datenschutzrechte, die sowohl auf nationaler, als auch auf europäischer Ebene zum Kernbestand des Menschenrechtsschutzes gehören. Als ganz entscheidendes Argument, weshalb der Eingriff durch die Richtlinie und das deutsche Umsetzungsgesetz dem angestrebten Ziel der öffentlichen Sicherheit unverhältnismäßig gegenüber stehen, ist die verdachtsunabhängige Speicherung von Daten aller am Fernmeldeverkehr Beteiligten anzusehen, die damit auch vor dem Hintergrund der bisher zur Terrorbekämpfung ergangenen Regelungen, eine neue Dimension des Eingriffs in den Datenschutz darstellt, die in dieser Form zu keiner Verfassungskonformität führen kann.

Ein Grund, der zu dieser im Ergebnis doch recht deutlichen verfassungsrechtlichen Einordnung führt, ist die fehlende Gefahrennähe zwischen den Betroffenen und dem zu schützenden Rechtsgut. Der statuierte Generalverdacht weist keinen Bezug mehr zur strafprozessualen Unschuldsvermutung als Ausprägung des Rechtsstaatsprinzips auf[279], und lässt das Spannungsverhältnis klar zum Vorschein treten. Im damit einhergehenden präventiven Charakter des Strafrechts sieht Rainer Wolf ein „Recht, das präventiv wirken, regeln und steuern soll, dies aber nicht leisten kann.[...] das Recht müsse akzeptieren, dass es keine Sicherheit geben kann.“[280]

Die Stellungnahme der Bundesregierung vom 28. November 2008 vermag in ihrer Gänze nicht zu überzeugen. Besonders kritisch ist dabei zu sehen, dass sie sich zur Unterstützung ihrer Argumentation immer wieder auf Einzelfälle beruft, die für sich genommen zwar stimmig sind, bei einem so schweren Eingriff in elementare Grundrechte eine empirische Datengrundlage aber nicht ersetzen können. Auch die

279 BVerfGE 74, 370
280 Wolf, 1991, 386.

Beschwerdeführer haben zwar nur wenige abgesicherte wissenschaftliche Erkenntnisse zur Hand, bemühen sich jedoch um eine sachgerechte Auswertung und Interpretation. Insgesamt ist diese eigentlich entscheidende Problematik schwierig, weil, wie auch das Gutachten des Max-Planck Instituts festgestellt hat, dass repräsentative wissenschaftliche Studien zu Ergebnissen der Abfragen und Auskünfte von Telekommunikationsdaten sowie zu den Folgen der Abfrage bisher noch nicht vorliegen.[281] Daher sollten weder vorschnelle Schlüsse zur einen, noch zur anderen Seite gezogen werden, soweit es um Argumentationen geht, die solcher Studien bedürften.

Was mögliche Gefahren für eine freie Kommunikation in einer demokratischen Gesellschaft angeht, muss dagegen sehr deutlich auf die nicht abzusehenden Folgen hingewiesen werden. Eine Veränderung des Kommunikationsverhaltens erscheint angesichts des Umfangs der gespeicherten Daten nicht unwahrscheinlich. Denn die Vorratsdatenspeicherung nimmt letztlich jedem Telekommunikationsnutzer die Freiheit, unbeobachtet zu kommunizieren. In einer Zeit, in der man auf Informationen angewiesen ist, in der aber auch immer mehr Lebensbereiche von dieser Art der Kommunikation erfasst werden, muss es den Menschen jedoch unbenommen bleiben, frei kommunizieren zu können. Die zunehmende Häufigkeit mobiler Kommunikation wird außerdem zu einem enormen Anwachsen der Verkehrsdaten führen. Dabei geht es nicht um von Kritikern geschürte Ängste, sondern um ganz reale Gefahren, die der Betroffene zu befürchten hat. Die Datenskandale der letzten Zeit haben die großen kommerziellen Interessen, die mit Daten verbunden sind, offen zutage treten lassen.[282] Die Gefahr von Missbrauch sowie die Möglichkeit Rückschlüsse auf die Persönlichkeit der Menschen zu ziehen, stehen deshalb in einem unangemessenen Verhältnis zu einzelnen Erfolgen bei der Strafverfolgung. Die Vorratsdatenspeicherung potenziert diese Risiken, mit unabsehbaren Folgen für eine digitalisierte Gesellschaft.[283] Vor dem Hintergrund dieser Entwicklungen sowie dem hohen kommerziellen Wert, den diese Daten haben, muss man keine hellseherischen Fähigkeiten besitzen, um sich die zukünftigen Datenskandale auszumalen. Die Datenschutzgesetzgebung hat schließlich nicht ohne Grund das Ziel einer Datenvermeidung. Je weniger Daten gespeichert werden, desto geringer ist schließlich auch das Missbrauchsrisiko.[284]

281 Albrecht/Grafe/Kilchling 2008, 80.
282 So z.B. der Datenskandal bei der Deutschen Bahn: Bauchmüller/Ott, http://www.sueddeutsche.de/wirtschaft/386/457048/text/ (Zugriff: 11.07.09).
283 Kurz/Rieger 2009, 51 f.
284 Kurz/Rieger 2009, 50.

Die Aussagekraft der gespeicherten Daten wird von den Befürwortern einer Vorratsdatenspeicherung häufig unterschätzt, da keine Inhalte aufgezeichnet werden dürfen. Dabei darf aber nicht vergessen werden, welche Möglichkeiten der Informationstechnologie heute zur Verfügung stehen, um entsprechende Verknüpfungen und letztlich ganze Bewegungsprofile zu erstellen. Die gespeicherten Daten haben ein erhebliches Potenzial auch auf die Inhalte von Kommunikation zu schließen, so dass der Eingriff in datenschutzbegründende Rechte erheblich ist.

Sollte das Bundesverfassungsgerichts die Frage der Grundrechtskonformität dem Europäischen Gerichtshof vorlegen, so erscheint eine Feststellung der Grundrechtswidrigkeit, insbesondere aufgrund der bereits in diese Richtung gehenden Äußerungen der Generalanwältin Juliane Kokott[285] nicht unwahrscheinlich. Die bisherige Rechtsprechung des Gerichtshofs selber lässt allerdings keine klare Tendenz erkennen, da die Ansätze zum Datenschutz bisher eher wenig ausgeprägt sind. Das Urteil zur Klage Irlands, die richtige Kompetenzgrundlage betreffend, entzieht sich jeglicher Bemerkungen zu den Grundbedingungen des Datenschutzes und verfestigt nur die Funktion von Art. 95 EG „die Funktionsfähigkeit des Binnenmarktes als Einfallstor einer systematisch betriebenen strukturellen Veränderung der Gemeinschaft zu nutzen.“[286] Die Tatsache, dass der Datenschutz in einer Gesellschaft, die auf Information angewiesen ist, unabdingbar ist, begrenzt die Möglichkeiten der Einschränkung von Art. 8 Abs. 1 GRC jedoch von vornherein und lässt auch auf der Ebene der Europäischen Union auf einen Eingriff in das Grundrecht auf den Schutz personenbezogener Daten schließen, der verfassungsrechtlich nicht gerechtfertigt ist. Soweit ein Verstoß gegen Grundrechte aus der Grundrechtecharta bejaht würde, hätte jedoch von vornherein keine Umsetzungspflicht der Richtlinie bestanden, da Deutschland zur Umsetzung der Richtlinie 2006/24/EG dann nicht verpflichtet ist, wenn diese gegen primäres Gemeinschaftsrecht verstößt. [287] Aus der Rechtsprechung des EuGH geht zudem hervor, dass auch dann keine Umsetzungspflicht für Rechtsakte besteht, wenn diese mit einem Fehler behaftet sind und dessen Schwere so offensichtlich ist, dass er von der Gemeinschaftsrechtsordnung nicht geduldet werden kann.[288]

Eine Klage vor dem EGMR kann nach Art. 34 EMRK im Rahmen der

285 GA *Juliane Kokott,* Schlussanträge in der Rs. C-275/06 vom 18. Juli 2007, Slg. 2008, I-271, Nr. 82.
286 Simitis, NJW 2009, 1784.
287 BVerfGE 89, 155, 188.
288 EuGH, Rs. C-475/01, Slg. 2004, I-8923, Rn. 19. st. Rspr.

Individualbeschwerde nach Erschöpfung des innerstaatlichen Rechtswegs erfolgen. Was das Verhältnis der Mitgliedstaaten zur Übertragung von Hoheitsgewalt auf eine internationale Organisation betrifft, hat der EGMR entschieden, dass dieses möglich ist, solange gewährleistet ist, dass der Schutz der Konventionsrechte weiterhin sichergestellt ist.[289] Eine Klage vor dem EGMR hätte folglich dann Aussicht auf Erfolg, wenn der EuGH die Grundrechtskonformität der Richtlinie 2006/24/EG feststellen würde und der EGMR den Grundrechtsschutz auf Gemeinschaftsebene nicht ausreichend sichergestellt sieht. Maßgeblich ist Art. 8 Abs. 1 EMRK. Wesentliche Rechtfertigung ist dabei das Erfordernis der Maßnahme in einer demokratischen Gesellschaft nach Art. 8 Abs. 2 EMRK. Das Verwaltungsgericht Wiesbaden hat eine solche Notwendigkeit nicht gesehen.[290]

Die Rechtsprechung des EGMR ist hinsichtlich des Datenschutzes schwer einzuordnen. In seinem Urteil zur Speicherung von Fingerabdrücken und DNA-Proben bezeichnet er diese als rücksichtslos, auch weil die Speicherung unabhängig von der tatsächlichen Schuld vorgenommen wird.[291] In seinem Urteil gegen Finnland hat er dagegen entschieden, dass die Vertraulichkeit der Kommunikation und die Privatsphäre hinter der Verhütung von Straftaten zurücktreten soweit es der effektiven Strafverfolgung im Fall schwerer Beeinträchtigungen dient.[292] Die Erfolgsaussichten einer Klage vor dem EGMR sind daher schwer einzuschätzen, müssen aber im Ergebnis, insbesondere im Hinblick auf die neue Dimension dieser rechtlichen Regelung als verdachtsunabhängige flächendeckende Datenspeicherung als gut beurteilt werden.

II. Abschließende Gedanken zum Verhältnis von Sicherheit und Freiheit

Bei aller Kritik an der Vorratsdatenspeicherung verwundert es schon, wie wenig gesellschaftlicher Widerstand sich dagegen formiert hat. Obwohl dieses Thema in den letzten Wochen und Monaten immer wieder in der öffentlichen Diskussion stand und auch Gegenstand medialer Kritik war, scheint ein Großteil der Bevölkerung staatliche Zugriffe auf den privaten Lebensbereich weitgehend hinzunehmen. Wenn man sich anschaut mit welcher Freude viele ihre personenbezogenen Daten nur für eine entfernte Gewinnchance oder für Rabatte an Privatunternehmen herausgeben, lässt sich eine

289 EGMR, EuGRZ 1999, 200 f.
290 VG Wiesbaden, Beschluss vom 27. Februar 2009, AZ 6 K 1045/08.WI, Rn. 28. (http://www.jurpc.de/rechtspr/20090114.htm).
291 EGMR, Urt. vom 4. Dezember 2008, *S. und Marper v. GB,* (Rs. 30562/04 und 30566/04), Rn. 119.
292 EGMR, Urt. vom 2. Dezember 2008, *K.U. v. Finnland,* (Rs. 2872/02), Rn. 49.

Erklärung erahnen. Der entscheidende Unterschied zur gesetzlich vorgesehenen Speicherung besteht jedoch auch darin, dass es sich hierbei um eine freiwillige Herausgabe handelt.

Der Argumentation derer sich viele Menschen, darauf angesprochen bedienen, nämlich selber nichts zu verbergen zu haben, liegt der Gedanke zugrunde, die eigene Sicherheit erhöhen zu wollen, auf Kosten der Freiheit der anderen. Das geht jedoch nicht, in einem Rechtsstaat, der allen Menschen die gleichen Rechte verleiht. Denkt man diesen Gedanken bis zum Ende, so wird deutlich, dass es ohne individuelle Freiheit auch keine allgemeine gesellschaftliche Freiheit geben kann. In einer Demokratie darf es nicht die Effektivität sein die staatliches Handeln bestimmt, sondern das Recht.[293] Trotz der Datenskandale der letzten Zeit scheint sich eine Sensibilität für diese Thematik nur langsam herauszubilden. Der Politik lässt dieser Vorsprung die Möglichkeit, Maßnahmen zur Kriminalitätsbekämpfung voranzutreiben, ohne auf nennenswerten gesellschaftlichen Widerstand zu stoßen. Das Tempo das sie dabei häufig vorlegt, macht sowohl eine ausgereifte Entscheidung, als auch eine breite öffentliche Diskussion im Vorfeld unmöglich. Welche Normalität dieses Vorgehen inzwischen erlangt hat, zeigen die zahlreichen Gesetze zur Kriminalitätsbekämpfung, die das Bundesverfassungsgericht für ganz oder teilweise verfassungswidrig erklärt hat.[294] Auf europäischer Ebene ist dieses Vorgehen noch nicht in dem Maße in Erscheinung getreten, was jedoch dem Umstand geschuldet ist, dass es sich in der Regel um einen Bereich der 3. Säule handelt, in dem die Mitgliedstaaten aufgrund der Sensibilität dieses Politikbereichs lieber eigene Entscheidungen treffen. Das dieses nicht zwingend so sein muss und auch eine gerichtliche Korrektur nicht immer erwartet werden kann, zeigt die Entscheidung des EuGH zur richtigen Kompetenzgrundlage der Richtlinie 2006/24/EG.[295]

Zusammenfassend muss davon ausgegangen werden, dass sowohl die Richtlinie 2006/24/EG, als auch das innerstaatliche Umsetzungsgesetz einer verfassungsrechtlichen Prüfung nicht standhalten können. Die wahrscheinlichste und wohl auch sauberste Lösung bestände darin, dass der EuGH die Richtlinie zur Vorratsdatenspeicherung für nicht vereinbar mit dem Grundrechtsschutz der

293 Hirsch, DuD 2008, 88.
294 So z.B. Gesetz zur Neuregelung der Luftsicherheitsaufgaben BvR 357/05 2006; Gesetz zur Förderung der Steuerehrlichkeit BvR 1550/03 2007.
295 EuGH, Rs. C-301/06, Slg. 2009.

Gemeinschaft befindet. Nach dem derzeitigen Stand kann dieses die einzige Lösung sein, die aufgrund der aufgeführten Argumente gegen eine Speicherung von Daten auf Vorrat befriedigen kann. Niemand stellt dabei in Frage, dass die öffentliche Sicherheit und die Bekämpfung von Terrorismus und Kriminalität wichtige Ziele sind, deren Bekämpfung von staatlicher Seite natürlich auch erwartet werden darf. Gerade die neue, global vernetzte Dimension des Terrorismus macht vielen Mensch Angst. Einer Demokratie darf es aber nicht geschuldet werden, wenn Politiker mit diesen Ängsten spielen und vorschnelle Reaktionen folgen lassen, die wenig geeignet sind, zur Problemlösung tatsächlich beizutragen, wie die Vorratsdatenspeicherung. Vielmehr muss realisiert werden, dass die Pflicht des Staates zur Gefahrenabwehr auf die Anwendung der Mittel beschränkt ist, die ihm die Verfassung einräumt. Er darf sich von keiner Bedrohung dazu verleiten lassen, seine eigenen Rechtstraditionen in Frage zu stellen. Kein Bürger darf ohne Verdacht zum Objekt polizeilicher oder strafrechtlicher Ermittlungen werden. Eine Speicherung von Daten auf Vorrat darf daher nur dann zulässig sein, wenn sie auf einem konkreten Tatverdacht beruht.[296] Alles andere schränkt den Rechtsstaat zugunsten von Sicherheitsbedürfnissen in einer Art und Weise ein, die demokratischem Maßstäben zuwiderläuft und die Ausgewogenheit des Spannungsverhältnisses von Sicherheit und Rechtsstaat unmöglich macht. Durch die Analysierung der gespeicherten Daten ist es möglich, ein nahezu vollständiges Persönlichkeitsprofil zu erstellen und über die Zeit fort zu entwickeln. Bei der gerichtlichen Beurteilung der Verfassungsbeschwerde darf deshalb nicht nur vom heutigen Stand der Technik ausgegangen werden, sondern es müssen auch zukünftige technologische Entwicklungsmöglichkeiten mit einbezogen werden.

Auch müssen wir uns letztlich ganz einfach damit abfinden, dass es niemals eine hundertprozentige Sicherheit geben kann. Das menschliche Leben wird immer so verletzlich, wie die Menschen selbst. Gleichzeitig ist der Staat keine unfehlbare Macht, die den Anspruch vor allem schützen zu können, gar nicht haben darf. Dieser defizitäre Zustand wird immer ein Teil der Gesellschaft sein. Eine andere Erwartungshaltung darf sich weder auf staatlicher, noch auf gesellschaftlicher Seite herausbilden. Das Ergebnis wäre ein Minimum an der Freiheit, die jedem menschlichen Leben als ureigenstem Bedürfnis zugrunde liegt.

296 Hirsch, DuD 2008, 91.