Verfassungsbeschwerde

1. der HUMANISTISCHEN UNION e.V.,
   ...

2. des Herrn Dr. Fredrik Roggan,
   Rechtsanwalt und stellvertretender Bundesvorsitzender der HUMANISTISCHEN UNION e.V.,
   ...

3. des Prof. Dr. ...

4. des Herrn ..., Pfarrer und kirchlicher Beauftragter für Kriegsdienstverweigerer,

5. des Herrn ..., Rechtsanwalt und Abgeordneter a.D.,

6. der Frau ..., Freie Journalistin,

7. des Herrn ..., Steuerberater,

   des Herrn ..., Arzt,

8. der ... [Telekommunikationsdienstleister]

9. der Frau ..., Dipl.-Psychologin und Psychotherateutin,

gegen das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG, sowie Art 34b Abs. 2 i. V. m. Art. 34a Abs. 1 Satz 1, Abs. 3 S. 1 Bayerisches Polizeiaufgabengesetz (BayPAG), Art. 6c Bayerisches Verfassungsschutzgesetz (BayVSG) und § 34 a Thüringisches Poizeiaufgabengesetz (ThürPAG)

Inhaltsverzeichnis

A. Tatbestand

Die Beschwerdeführerin zu 1) wurde 1961 gegründet und ist die älteste Bürgerrechtsorganisation der Bundesrepublik Deutschland. Die Humanistische Union (HU) kämpft seither für die Achtung und Durchsetzung der Grundrechte und die Aufrechterhaltung der Verfassung. Ein Arbeitsschwerpunkt der HU besteht seit langem im Einsatz für das Grundrecht auf informationelle Selbstbestimmung, den Datenschutz, das Fernmeldegeheimnis und das Recht auf Informationsfreiheit. Der Ausbau eines umfassenden staatlichen Überwachungsapparates wird zur zunehmenden Bedrohung bürgerlicher Freiheitsrechte. In diesem Zusammenhang steht die Auseinandersetzung um die sogenannte Vorratsdatenspeicherung von Telekommunikationsverbindungsdaten, bei der die HU eine Vorreiterrolle übernommen hat. Seit dem 21. Januar 2008 betreibt die HU einen Anonymisierungsserver, mit dem interessierte Bürger ohne zusätzliche Kosten anonym das Internet nutzen können. Darüber hinaus ermöglicht der Dienst Menschen aus anderen Ländern die Umgehung staatlicher Zugangssperren zu bestimmten Internetinhalten. Die Beschwerdeführerin finanziert den Dienst aus Beiträgen und Spenden ihrer Mitglieder, die Wartung des Servers wird ehrenamtlich erbracht. Sollte die Speicher- und Auskunftsverpflichtung für die Betreiber von Anonymisierungsdiensten aufrecht erhalten bleiben, sähe sich die Beschwerdeführerin u.U. gezwungen, diesen Dienst aufgrund des damit verbundenen Aufwands und der anfallenden Kosten einstellen zu müssen.

Der Beschwerdeführer zu 2) ist Rechtsanwalt in Berlin und seit 2005 stellvertretender Bundesvorsitzender der HUMANISTISCHEN UNION e.V. Im Rahmen seiner Tätigkeit als Rechtsanwalt ist er vor allem als Strafverteidiger tätig. Er nutzt Telekommunikationsmittel zu beruflichen Zwecken u.a. für den Kontakt zu seinen Mandanten und Recherchen zu seinen aktuellen Mandaten.

Der Beschwerdeführer zu 3) ist Hochschullehrer für Staats- und Verwaltungsrecht mit dem Schwerpunkt Polizei- und Ordnungsrecht in Berlin.

Der Beschwerdeführer zu 4) ist Pfarrer und kirchlicher Beauftragter für Kriegsdienstverweigerer.

Der Beschwerdeführer zu 5) ist Rechtsanwalt und Abgeordneter a.D. des Bayerischen Landtags.

Die Beschwerdeführerin zu 6) ist Redakteurin einer Tageszeitung und darüber hinaus als freie Journalistin tätig. Sie nutzt Telekommunikationsmittel beruflich unter anderem für Recherchen zu geplanten Artikeln und den Kontakt zu Informanten, von denen sie regelmäßig Dokumente in elektronischer Form übermittelt bekommt (per E-Mail oder Fax).

Der Beschwerdeführer zu 7) ist freiberuflicher Steuerberater.

Der Beschwerdeführer zu 8) ist praktizierender Arzt in Guissau.

Der Beschwerdeführer zu 9) ist ein Anbieter von Telekommunikationsdiensten mit Sitz in Berlin. Es handelt sich um einen kleinen mittelständigen Dienstleister für Hosting-Dienste.

Die Beschwerdeführerin zu 10) ist Dipl.-Psychologin und Psychotherapeutin in Berlin. Es werden von ihr im Durchschnitt vier bis sechs Telefongespräche täglich aus beruflichen Gründen geführt. Dies sind Terminvereinbarungen aber auch beratende Gespräche mit Patienten, Rücksprachen mit Ärzten, Sozialarbeitern, Angehörigen, Krankenkassen, Beihilfestelle und Kassenärztliche Vereinigung. Darüber hinaus werden Gespräche mit Kollegen zur Abstimmung von Inter- und Supervision bzw. zur gegenseitigen kollegialen Beratung geführt.

B. Zulässigkeit der Verfassungsbeschwerde

Die Verfassungsbeschwerden sind zulässig. Die Beschwerdeführer sind beschwerdefähig. Sie werden durch die angegriffenen gesetzlichen Regelungen unmittelbar, gegenwärtig und selbst in ihren Grundrechten verletzt. Die angegriffenen Regelungen des Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG sind in wesentlichen Teilen seit dem 1. Januar 2008 in Kraft getreten. Dies gilt auch hinsichtlich der Internet-Dienste, obwohl sie ihre Verpflichtungen gem. § 150 Abs. 1 b TKG erst spätestens ab dem 1. Januar 2009 erfüllen müssen.
Die Regelungen des Bayerischen Polizeiaufgabengesetzes, des bayerischen Verfassungsschutzgesetzes und des Thüringischen Polizeiaufgabengesetzes sind seit dem 1. August 2008 in Kraft.

I. Beschwerdefähigkeit

Der Beschwerdeführer zu 2) bis 8) und zu 10) sind als natürliche Person Grundrechtsträger und damit beschwerdefähig gemäß § 90 Abs. 1 BVerfGG.

Die Beschwerdeführerin zu 1) ist ein eingetragener Verein mit Sitz in der Bundesrepublik Deutschland. Die Beschwerdeführerin zu 9) ist als GmbH eine juristische Person des Privatrechts eingetragen im Handelsregister Amtsgericht Berlin Charlottenburg, HRB 56627. Damit sind sie inländische juristische Personen des Privatrechts und nach Art. 19 Abs. 3 GG im vorliegenden Fall grundrechts- und beschwerdefähig, weil das hier in Betracht kommende Grundrecht der

Telekommunikationsfreiheit aus Art. 10 GG auf inländische juristische Personen anwendbar ist. Zudem findet in Bildung und Betätigung der Beschwerdeführerin zu 1) die freie Entfaltung der hinter ihr stehenden natürlichen Personen ihren Ausdruck (BVerfGE 21, 362, 369; 68, 193, 205f.). Die Beschwerdeführerin zu 9) ist zudem in Art. 12 I GG betroffen, welches seinem Wesen nach umfassend auf juristische Personen des Privatrechts anwendbar ist (BVerfGE 21, 261, 266; 65, 196, 210; 97, 228, 253).

II. Beschwerdebefugnis

Die Beschwerdeführer sind auch beschwerdebefugt. Es besteht die Möglichkeit einer Verletzung von Grundrechten der Beschwerdeführer durch die öffentliche Gewalt. Von der Grundrechtsverletzung geht eine gegenwärtige, eigene und unmittelbare Beschwer für die Beschwerdeführer aus.

1. Möglichkeit einer Grundrechtsverletzung

Die Beschwerdeführer machen mit ihren Verfassungsbeschwerden eine Verletzung durch die öffentliche Gewalt in ihrem Grundrecht aus Art. 10 Abs.1 (und Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1) GG geltend. Sie sind damit im Sinne von § 90 Abs. 1 BVerfGG beschwerdebefugt, da eine Grundrechtsverletzung der Beschwerdeführer durch das angegriffene Gesetz möglich erscheint. Alle Beschwerdeführer nutzen regelmäßig und dauerfhaft verschiedene von der gesetzlichen Regelung betroffene Telekommunikationseinrichtungen, wie Mobiltelefone, Telefone, Internet u. a.
Der Schutzbereich des Art. 10 Abs. 1 GG ist betroffen, da die angegriffenen Normen Befugnisse der Telekommunikationsanbieter sowie der Strafverfolgungsbehörden regeln, die in die Telekommunikationsfreiheit eingreifen.
Das Fernmeldegeheimnis als besonderer Schutzgehalt der in Art. 10 Abs. 1 GG geschützten Telekommunikationsfreiheit schützt die durch unkörperliche Signale transportierte, räumlich distanzierte individuelle Kommunikation. Der Schutzbereich umfasst nicht nur die Inhalte der Telekommunikation, sondern auch alle mit dem Fernmeldevorgang zusammenhängenden näheren Umstände des Fernmeldeverhältnisses (BVerfGE 85, 386, 396;67, 157, 172, OVG Münster NJW 1975, 1335.). Zu diesen Kommunikationsumständen gehören das Zustandekommen eines Telekommunikationsvorgangs, die Identität der Beteiligten sowie Art, Zeitpunkt, Dauer und Ort der Verbindung (BVerfGE 100, 313, 358;113, 348, 365). Die nach dem angegriffenen Gesetz auf Vorrat zu speichernden Verbindungs- und Standortdaten geben genau Aufschluss über die Telekommunikationsumstände. Die Schutzwirkung des Fernmeldegeheimnisses erstreckt sich aber auch auf den Informations- und Datenverarbeitungsprozess, der sich an die Kenntnisnahme von geschützten Kommunikationsvorgängen anschließt und auf den Gebrauch, der von den erlangten Kenntnissen gemacht wird (BVerfGE 100, 313, 359; 113, 348, 365). Die gesetzliche Anordnung des Staates entsprechende Daten zu speichern und sie zu verwerten, ist daher ein Eingriff in den Schutzbereich des Grundrechts aus Art. 10 Abs. 1 GG . Es besteht vor allem wegen der flächendeckenden Möglichkeit einer anlasslosen Speicherung auf Vorrat und der vorgesehenen

Zugriffsbefugnisse der Strafverfolgungsbehörden auf die gespeicherten Telekommunikationsdaten die Möglichkeit, dass Art. 10 Abs. 1 GG verletzt wird.

Die Beschwerdeführerin zu 9) rügt zudem einen Verstoß gegen Art. 12 Abs. 1 GG. Dieses Grundrecht gewährleistet jedem Deutschen das Recht, seinen Beruf grundsätzlich frei wählen und ausüben zu dürfen. Gemäß Art. 19 Abs. 3 GG ist es auf inländische juristische Personen anwendbar. Beruf im Sinne des Art. 12 Abs. 1 GG ist jede Tätigkeit, die der Schaffung und Erhaltung einer Lebensgrundlage dient. Das Erbringen von Telekommunikationsdiensten ist zur dauerhaften Erzielung von Gewinnen geeignet und ist daher als berufliche Tätigkeit anzusehen. Diese Tätigkeit wird typischerweise von kommerziellen Anbieter vorgenommen. Die anlasslose Speicherverpflichtung für Telekommunikationsbetreiber weist einen spezifischen Bezug zur Tätigkeit des kommerziellen Erbringens von Telekommunikationsdiensten auf. Sie besitzt damit eine berufsregelnde Tendenz, die möglicherweise Art.12 Abs.1 GG verletzt.

Die Beschwerdeführer zu 2) bis 8) und zu 10) rügen wegen der Ausübung von Vertrauensberufen (Geistliche, Rechtsanwälte, Steuerberater, Ärzte, psychologische Psychotherapeuten, Journalisten) ebenfalls einen Verstoß gegen Art. 12 Abs. 1 GG. Die Kontaktaufnahme der Klienten erfolgt üblicherweise via Telefon. Allein aus der Kontaktaufnahme selbst lassen sich bereits Schlüsse ziehen, aus denen ein geschütztes Geheimnis offenbart werden kann. Insbesondere sind das anwaltliche Mandatsverhältnis oder das Vorliegen einer psychischen Störung als geschütztes Geheimnis, allein aus dem Telekommunikationsvorgang zu entschlüsseln. Allein durch die Tatsache der Vorratsdatenspeicherung wird das Vertrauensverhältnis belastet. Potentielle Klienten werden abgehalten, Rat und Hilfe beim Berufsgeheimnisträger einzuholen oder Informationen an die Presse weiterzugeben. Dies gilt besonders, da sich den unter Speicherpflicht fallenden Verkehrsdaten beim Berufsgeheimnisträger nicht ansehen lässt, ob sie als zu schützendes Geheimnis anzusehen sind.

Die Beschwerdeführerin zu 6) macht als Journalistin zudem einen Verstoß gegen das Grundrecht auf Pressefreiheit aus Art. 5 Abs. 1 S.2 GG geltend. Pressefreiheit reicht von der Beschaffung der Information bis zur Verbreitung der Nachrichten und Meinungen (BVerfGE 20, 162, 176) und umfasst auch den Informations- und Informantenschutz, d.h. die Geheimhaltung von Informationsquellen und das Vertrauensverhältnis zu privaten Informanten (BVerfGE 36, 193, 204; 107, 299, 329). Der Informations- und Informantenschutz wird durch die angegriffenen Regelungen beeinträchtigt, da aufgrund der Speicherung die Geheimheit der Informationsquellen nicht garantiert werden kann.

Zudem rügt der Beschwerdeführer zu 4) die Verletzung des Art. 4 Abs. 1 GG. Die Glaubens- und Gewissensfreiheit schützen die Kernelemente der Persönlichkeit. Den unmittelbaren Gegenstand der Grundrechtsgarantie bilden diejenigen Elemente, mit denen sich der Grundrechtsträger für seine Existenz als moralisches Wesen maßgebend identifiziert. Die Freiheit der Bildung von Glaubensvorstellungen oder Gewissensentscheidungen ist ebenso geschützt wie die der individuellen Religionsentwicklung dienenden Kontakte mit dem Beichtvater bzw. Geistlichen. Die Geheimheit dieser Kontakte wird aufgrund der Vorratsdatenspeicherung nicht mehr gewährleistet.

2. Eigene Beschwer

Die Beschwerdeführer sind durch die Regelungen der neueingefügten §§ 113a und 113b TKG und der geänderten §§ 111 TKG und 100g StPO sowie Art 34b Abs. 2 i. V. m. Art. 34a Abs. 1 Satz 1, Abs. 3 S. 1 BayPAG, Art. 6c BayVSG und § 34 a ThürPAG selbst betroffen. Für die eigene Betroffenheit genügt es, „wenn ein Gesetz die Normadressaten bereits gegenwärtig zu später nicht mehr korrigierbaren Entscheidungen zwingt, oder schon jetzt zu Dispositionen veranlasst, die sie nach dem späteren Gesetzesvollzug nicht mehr nachholen können" (BVerfGE 65, 1, 37; 75, 78, 95). Ein entsprechender Fall liegt hier vor.

Für die Beschwerdeführer müssen sich aus den angegriffenen Regelungen Rechtswirkungen ergeben, die die Rechtspositionen der Beschwerdeführer zu ihrem Nachteil verändern (BVerfGE 60, 360, 371). Dies ist bei §§ 113a und 113b TKG gegeben. Seit dem Inkrafttreten der angegriffenen Regelungen können die Beschwerdeführer kein Medium der Telekommunikation mehr nutzen, ohne dass sie befürchten müssen, dass sie und die anderen Beteiligten des jeweiligen Telekommunikationsvorgangs registriert, identifiziert und geortet werden, dass die anfallenden Verbindungs- und Standortdaten gespeichert, zu einem späteren Zeitpunkt von staatlicher Seite ausgewertet und benutzt werden. Eine eigene Betroffenheit besteht auch hinsichtlich des Eingriffs in das Grundrecht aus Art. 10 Abs. 1 GG durch die Speicherung der Daten auf Vorrat und den späteren Zugriff der staatlichen Behörden auf die vorrätig gespeicherten Daten für alle Beschwerdeführer.

Bezüglich der landesrechtlichen Regelungen sind die Beschwerdeführer auch selbst betroffen. Zwar haben die Beschwerdeführer ihren Lebensmittelpunkt außerhalb der Länder Bayern und Thüringen. Jedoch müssen die Beschwerdeführer, die sich aus den landesrechtlichen Regelungen für sie ergebenden Rechtswirkungen im Verfahren der Verfassungsbeschwerde vor dem Bundesverfassungsgericht geltend machen können. Die Regelungen ermächtigen jeweils die Landespolizeibehörden von Bayern und Thüringen, beziehungsweise den Verfassungschutz des Freistaates Bayern zum Zugriff auf die nach § 113a TKG gespeicherten Daten. Aus den Abrufmöglichkeiten ergeben sich jedoch Folgen, die ihre Grundlage unmittelbar in den bundesrechtlichen Eingriffsmöglichkeiten der §§ 113a, 113b TKG finden. Mithin stehen den Landesbehörden aus Bayern und Thüringen auch Zugriffsmöglichkeiten auf die Daten der Kommunikationsteilnehmer aller Bundesländer zu[1]

Die Beschwerdeführer zu 2) bis 8) und zu 10) sind ebenfalls selbst in ihren Grundrecht aus Art. 12 Abs. 1 GG durch die Regelungen betroffen. Durch die Ausübung von Vertrauensberufen und die übliche Kontaktaufnahme mittels eines Telekommunikationsvorgangs sind sie selbst beschwert.

Der Beschwerdeführer zu 4) wird durch die angeordnete Speicherung der Telekommunikationsverbindungsdaten auf Vorrat selbst und gegenwärtig in seinem Grundrecht aus Art. 4 Abs. 1 GG betroffen.

Die Beschwerdeführerin zu 6) ist selbst in ihrem Grundrecht aus Art. 5 Abs. 1 GG betroffen. Die Freiheit der Presse als ein wesentlicher Schutzgehalt des Art. 5 Abs. 1 GG wird durch die

[1] So auch BVerfG, Beschluss vom 28. November – 1 BvR 256/08, Rn. 71

Speicherung der Verbindungsdaten auf Vorrat eingeschränkt. Insoweit ist die Beschwerdeführerin zu 6) selbst betroffen.

Für die Beschwerdeführerin zu 9) kommt es durch die Möglichkeit des staatlichen Zugriffes der auf Vorrat gespeicherten Telekommunikationsverbindungsdaten auch zu einer eigenen Beschwer für das Grundrecht der Berufsausübungsfreiheit aus Art. 12 Abs. 1 GG. Die durch die Regelungen angeordnete Speicherpflicht verpflichtet den Telekommunikationsanbieter zur Vorhaltung der Daten über Telekommunikationsverbindungsvorgänge innerhalb eines Zeitraums von sechs Monaten.

Sollte das Gericht weiteren Sachvortrag zur eigenen Beschwer der jeweiligen Beschwerdeführer für notwendig erachten, so bitte ich um einen entsprechenden Hinweis.

3. Gegenwärtige Beschwer

Die Beschwerdeführer sind auch gegenwärtig betroffen.

Das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG ist am 01. Januar 2008 in Kraft getreten. Seitdem werden die Daten auf Vorrat erhoben. An dieser Betrachtung ändert sich auch dadurch nichts, dass Bußgeldvorschriften erst ab 01.01.2009 angewendet werden, gem. Art. 2 Nr. 9 des Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG, denn die gesetzliche Verpflichtung zur Speicherung für Anbieter von Telekommunikationsdiensten gilt bereits seit 01. Januar diesen Jahres.

Gleiches gilt hinsichtlich der Internetzugangsdienste, elektronischer Post und Internettelefonie. Die Verpflichtung zur Speicherung ist bereits in Kraft und bis spätestens zum 01.01.2009 zu erfüllen, wie sich ebenfalls aus Art. 2 Nr. 9 ergibt. Die Gegenwärtigkeit liegt bereits dann vor, wenn bereits jetzt eindeutig abzusehen ist, dass und wie der Beschwerdeführer in der Zukunft von der Regelung betroffen sein wird (BVerfGE 97, 157, 164), die Betroffenheit also klar abzusehen und gewiss ist (BVerfGE 101, 54, 74). Aufgrund der eindeutigen Regelung des Gesetzgebers ist die Betroffenheit nach Zeitpunkt und Auswirkung genau bestimmt, der Eingriff somit nicht lediglich „virtuell". Für die Beschwerdeführer, die als Nutzer diese Dienste in Anspruch nehmen, ist zudem nicht erkennbar, welche Anbieter bereits derzeit die Daten speichern.

Die Regelungen der Ländern Bayern und Thüringen sind am 1. 8. 2008 in Kraft getreten.

4. Unmittelbare Beschwer

Die Vorratsspeicherung der Telekommunikationsverbindungsdaten durch die Telekommunikationsunternehmen erfolgt gemäß den angegriffenen Gesetzen automatisch, d.h. für die Durchführung des Gesetzes ist kein weiterer Vollzugsakt notwendig. Alle Beschwerdeführer

sind deshalb von der Speicherung ihrer Telekommunikationsverbindungsdaten unmittelbar betroffen.

Nach der Rechtsprechung des Bundesverfassungsgerichts kann sich eine Verfassungsbeschwerde aber auch gegen ein vollziehungsbedürftiges Gesetz richten, wenn der Beschwerdeführer den Rechtsweg nicht bestreiten kann, weil er keine Kenntnis von der Maßnahme erlangt (BVerfGE 67, 157, 169; 100, 313, 354; 109, 279, 306f.). Gleiches gilt, soweit eine nachträgliche Bekanntgabe zwar vorgesehen ist, von ihr aber aufgrund weitreichender Ausnahmetatbestände auch langfristig abgesehen werden kann (BVerfGE 113, 348, 362). So liegt es bei den im Gesetz geregelten Zugriffsmöglichkeiten staatlicher Behörden auf die gespeicherten Telekommunikationsmöglichkeiten.

Für die Möglichkeit der eigenen und gegenwärtigen Betroffenheit reicht es aus, wenn ein Beschwerdeführer darlegt, dass er mit einiger Wahrscheinlichkeit durch die auf den angegriffenen Rechtsnormen beruhenden Maßnahmen in seinen Grundrechten berührt wird (BVerfGE 67, 157, 169f.; 100, 313, 354). Bei der Bestimmung des Grades der Wahrscheinlichkeit ist zu berücksichtigen, welche Möglichkeiten der Beschwerdeführer hat, seine Betroffenheit darzulegen. Dabei ist die Streubreite der Maßnahme sowie die Tatsache, ob sie auch Dritte zufällig erfassen kann, bedeutsam (BVerfGE 113, 348, 363). Diese Bedingungen für die eigene und gegenwärtige Betroffenheit sind für alle Beschwerdeführer erfüllt. Sowohl der Zugriff der Strafverfolgungsbehörden auf die vorrätig gespeicherten Daten als auch die Datenerhebung durch die Behörden selbst erfolgen heimlich. Die Betroffenen erfahren davon weder vor noch während der Durchführung der Maßnahme, so dass zu diesem Zeitpunkt kein fachgerichtlicher Rechtsschutz in Anspruch genommen werden kann (BVerfGE 113, 348, 362). Die Tatsache, dass § 101 Abs. 4 und 5 StPO eine nachträgliche Benachrichtigung regeln, sobald dies ohne Gefährdung der Maßnahme möglich ist, steht der Zulässigkeit der Verfassungsbeschwerde nicht entgegen (vgl. BVerfGE 113, 348, 362). Wegen der zahlreichen Ausnahmetatbestände sind eine zeitnahe Kenntnis von der Maßnahme und eine entsprechende Möglichkeit eines gerichtlichen Rechtsschutzes nicht gesichert. Nach § 101 Abs. 5 StPO unterbleibt die Unterrichtung, solange der Untersuchungszweck, das Leben oder die körperliche Unversehrtheit und der persönlichen Freiheit einer Person gefährdet sind. Außerdem kann es gemäß § 101 Abs. 7 StPO u.U. von einer Benachrichtigung völlig abgesehen werden. Eine kürzlich vorgelegte Studie zur Rechtswirklichkeit der TK-Verbindungsdatenabfrage [2] belegt, dass die Benachrichtigung der Betroffenen die Ausnahme darstellt: In 1257 untersuchten Beschlüssen fanden sich lediglich 40 aktenkundige Benachrichtigungen.

Die Eintrittswahrscheinlichkeit der Gefahr für die Beschwerdeführer ist ebenfalls gegeben. Diesbezüglich ist ausreichend, wenn ein Gesetz eine ernsthaft zu besorgende Grundrechtsgefährdung mit sich bringt (BVerfGE 49, 89, 141; 51, 324, 347). Dies ist hier der Fall. Bereits das Bewusstsein, dass anhand der zahlreichen gespeicherten Telekommunikationsdaten

---

[2] Hans-Jörg Albrecht, Adina Grafe und Michael Kilchling: Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO. Forschungsbericht im Auftrag des Bundesministeriums der Justiz. Forschungsgruppe Kriminologie des Max-Planck-Institut für ausländisches und internationales Strafrecht. Freiburg, Februar 2008.

die Verortung und die Identifizierbarkeit der Betroffenen sowie die Erstellung von Bewegungs- und Kommunikationsprofilen bei der Auswertung der Daten möglich ist, zwingt die Betroffenen mit großer Wahrscheinlichkeit zu Kommunikationsanpassungen und anderen Maßnahmen, die ihre Telekommunikationsfreiheit beeinträchtigen würden. Die Beschwerdeführer müssen auch mit einer zufälligen Erfassung ihrer Daten rechnen. Die Möglichkeit, Objekt einer Maßnahme der Erhebung und Auswertung von personenbezogenen Verkehrsdaten aufgrund der angegriffenen Regelungen zu sein, kann trotz der Regelung des § 100g Abs. 2 S. 1 i.V.m. 100a Abs. 3 StPO praktisch nicht nur den möglichen Straftäter oder dessen Nachrichtenmittler erfassen, sondern auch Personen, die mit den Adressaten der Maßnahme über Telekommunikationseinrichtungen in Verbindung stehen (vgl. BVerfGE 113, 348, 364). Die Beschwerdeführer zu 2) bis 8) und zu 10) müssen außerdem mit einer berufsbedingt gesteigerten Wahrscheinlichkeit der Betroffenheit ihrer Telekommunikationsfreiheit rechnen.

Aus den bisherigen Ausführungen ergibt sich, dass die Voraussetzung der Unmittelbarkeit der Beschwer gegeben ist. Die Beschwerdeführer sind durch die bloße Existenz der angegriffenen Regelungen unmittelbar betroffen. Die Speicherung ihrer Verbindungsdaten können sie durch eigene Handlungen nicht verhindern. Außerdem besteht für die Beschwerdeführer keine Möglichkeit, sich gegen den Zugriff der Strafverfolgungsbehörden zu wehren, weil es an einer zeitnahen Benachrichtigung über die Durchführung der Maßnahme fehlt.
Alle Beschwerdeführer sind durch die angeordnete Speicherung der Telekommunikationsverbindungsdaten unmittelbar in ihren jeweils gerügten Grundrechtspositionen betroffen.
Die Beschwerdeführer dürfen nicht darauf verwiesen werden, dass der Staat die Daten nicht selbst speichert, sondern die Speicherung durch Private durchführen lässt (vgl. BVerfGE 107, 299, 313). Die Speicherung aller Daten erfolgt ausschließlich aufgrund der mit der Verfassungsbeschwerde angegriffenen Regelungen.

III. Frist

Die Verfassungsbeschwerde ist fristgemäß erhoben. Da sich die Verfassungsbeschwerde gegen ein Gesetz richtet, gilt hier die einjährige Frist des § 93 Abs. 3 BVerfGG. Diese Frist beginnt mit dem Inkrafttreten des Gesetzes und ist hier offensichtlich gewahrt.

IV. Subsidarität der Verfassungsbeschwerde

Die Beschwerdeführer können nicht darauf verwiesen werden, vorab den ordentlichen Rechtsweg zu beschreiten. Eine Unterlassungsklage gegen die Anbieter der Telekommunikationsdienste, die von den angegriffenen Regelungen zur Speicherung verpflichtet werden, ist nicht möglich. Jeder Beschwerdeführer nimmt eine Vielzahl von verschiedenen Telekommunikationsdiensten bei verschiedenen Anbietern in Anspruch.

Die möglichen Gegner einer Unterlassungsklage haben kein eigenes Interesse an der Speicherung der Telekommunikationsverbindungsdaten auf Vorrat. Eine Unterlassungsklage gegen die Anbieter könnte sodann nur die Frage betreffen, ob das die Speicherung anordnende Gesetz selbst verfassungsgemäß und mit europäischen Recht vereinbar ist. Jede dieser Klagen würde spätestens nach der Rechtswegerschöpfung oder durch Vorlage nach Art. 100 Abs. 1 GG dem BVerfG vorlegt werden. Mit Blick darauf und auf die unmittelbare Verletzung elementarer Grundrechte durch die angegriffenen Regelungen kann es den Beschwerdeführern nicht zugemutet werden, eine Klärung durch die ordentlichen Gerichte abzuwarten. Dies wäre auch der weitreichenden Bedeutung des angegriffenen Gesetzes nicht angemessen.

Darüberhinaus ist die Verfassungbeschwerde von allgemeiner Bedeutung gemäß § 90 Abs. 2 S. 2 BVerfGG. Die angegriffenen Regelungen betreffen die Bundesbürger in ihrer Gesamtheit. Nur eine verfassungsgerichtliche Entscheidung kann die erforderliche Klarheit über die Vielzahl der durch das Gesetz herbeigeführten Grundrechtseingriffe treffen (vgl. BVerfG NJW 93, 2367).

Die Voraussetzungen des § 93a BVerfGG für die Zulässigkeit der Verfassungsbeschwerde liegen somit vor.

V. Europarechtliche Zulässigkeitsfragen

Das BVerfG ist im vollen Umfang befugt, die von den Beschwerdeführern gerügten Grundrechtsverstöße am Maßstab des nationalen Rechts zu überprüfen.

1. Uneingeschränkte Prüfung der Regelungen des Umsetzungsgesetzes, die über die Vorgaben der Vorratsdatenspeicherungsrichtlinie hinaus gehen, durch das Bundesverfassungsgericht

Soweit die Beschwerdeführer die Verfassungswidrigkeit der in Art. 1 des Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG rügen, ist das BVerfG in vollem Umfang zur Prüfung befugt. Unabhängig von der Rechtmäßigkeit der Richtlinie 2006/24/EG, der Solange-Rechtsprechung des BVerfG und einer etwaigen Vorlage beim EuGH ist die Verfassungsbeschwerde in diesem Teil zulässig. Gleiches gilt für die Regelung des Art. 2 Nr. 6 des Gesetzes soweit er die Einfügung des § 113b Satz 1 Nr. 2 und 3 TKG betrifft.

Die Verfassungsbeschwerde betrifft insoweit Regelungen, die über die Vorgaben der Richtlinie hinausgehen. Art. 1 des Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG regelt Änderungen der Strafprozessordnung, also zum Abruf der nach dem TKG auf Vorrat zu speichernden Daten. Die Richtlinie 2006/24/EG gab dazu keine Vorgaben. Ebenso enthält die Richtlinie 2006/24/EG keine Vorgaben zur Weitergabe der gespeicherten Verbindungsdaten zur Gefahrenabwehr und an die Nachrichtendienste.

Darüberhinaus erfolgten die gesetzlichen Regelungen in Art. 1 des Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur

Umsetzung der Richtlinie 2006/24/EG, um die Ratifikation des Übereinkommens des Europarates über Computerkriminalität (sog. Cybercrime-Konvention) zu ermöglichen.

Die Solange-Rechtsprechung des BVerfG ist folglich nicht anwendbar. Die Solange-Rechtsprechung bezieht sich nicht auf Normen des nationalen Rechts, die über die Vorgaben des umzusetzenden europäischen Rechtsaktes hinaus gehen. Diese Normen des nationalen Umsetzungsgesetzes können vom Bundesverfassungsgericht vorbehaltlos und uneingeschränkt geprüft werden.

Soweit die Beschwerdeführer die Verfassungsmäßigkeit von Art 34b Abs. 2 i. V. m. Art. 34a Abs. 1 Satz 1, Abs. 3 S. 1 BayPAG, Art. 6c BayVSG und § 34 a ThürPAG rügen, sind europarechtliche Bezüge ebenso nicht erkennbar.

2. Uneingeschränkte Prüfung der Regelungen des Umsetzungsgesetzes, bei denen die Richtlinie 2026/24/EG dem nationalen Gesetzgeber einen Umsetzungsspielraum überließ, durch das Bundesverfassungsgericht

Die Richtlinie 2006/24/EG sieht in Art. 6 Fristen für die auf Vorrat zu speichernden Daten von 6 bis 24 Monaten vor. Die genaue Wahl des Zeitraumes innerhalb dieser Frist war dem nationalen Gesetzgeber überlassen.

Hierzu hat das BVerfG in seiner einstweiligen Anordnung vom 11. März 2008 zutreffend ausgeführt, dass die Richtlinie den nationalen Gesetzgebern einen Umsetzungsspielraum gewährt und dieser vom deutschen Gesetzgeber ausgeschöpft wurde[3]. Zum Prüfungsumfang des BVerfG hat das Gericht in der Teilzeitarbeit-Entscheidung ausdrücklich betont: „Wenn der nationale Gesetzgeber Spielraum bei der Umsetzung von sekundärem Gemeinschaftsrecht hat, ist er zwar an die Vorgaben des Grundgesetzes gebunden und unterliegt insoweit in vollem Umfang der verfassungsrechtlichen Überprüfung. Soweit im Übrigen die Normsetzung zwingend dem Gemeinschaftsrecht folgt, ist sie ebenso wie das sekundäre Gemeinschaftsrecht selbst nicht am Maßstab der deutschen Grundrechte durch das Bundesverfassungsgericht zu prüfen, sondern unterliegt dem auf Gemeinschaftsrechtsebene gewährleisteten Grundrechtsschutz“ [4] . Diese Rechtsprechung wurde auch hinsichtlich der sogenannten 3. Säule der EU durch das Haftbefehl-Urteil bestätigt[5]. Das Bundesverfassungsgericht hat das Europäische Haftbefehlgesetz[6] wegen Verletzung der Auslieferungsfreiheit (Art. 16 Abs. 2 GG) für nichtig erklärt, da der Gesetzgeber die ihm durch den Rahmenbeschluss zum Europäischen Haftbefehl eröffneten Spielräume nicht für eine möglichst grundrechtsschonende Umsetzung des Rahmenbeschlusses ins deutsche Recht ausgeschöpft habe. Es wurde außerdem betont, dass die politische Gestaltungsmacht bei der

---

[3] BVerfG, einstweilige Anordnung vom 11. März 2008, 1 BvR 256/08, Rn. 136.
[4] BVerfG, BvR 1036/99 vom 9.1.2001 – Teilzeitarbeit, II.1.b; BVerfGE, NJW 2001, S. 1267f.
[5] 2 BvR 2236/04=NJW 2005, S. 2289f.
[6] BGBl. 2004 I S. 1748.

Umsetzung von Rahmenbeschlüssen bei den nationalen Parlamenten liegt, die notfalls die Umsetzung auch verweigern können[7].

Daraus folgt, dass bei einer Verfassungsbeschwerde gegen ein Umsetzungsgesetz stets zu prüfen ist, inwieweit der eventuell vorliegende Grundrechtsverstoß durch gemeinschaftsrechtliche Vorgaben bedingt ist. Bei Verstößen, die nicht durch den umsetzungsbedürftigen gemeinschaftlichen Rechtsakt determiniert sind, muss das jeweilige Gesetz vom Bundesverfassungsgericht uneingeschränkt an den Maßstäben des Grundgesetzes geprüft werden. Hinsichtlich Grundrechtseingriffe, die durch gemeinschaftsrechtliche Regelungen bedingt sind, ist es gemeinschaftsrechtlich, aber auch verfassungsrechtlich verpflichtet, gemäß Art. 234 Abs. 2 bzw. 3 EGV den EuGH anzurufen [8] . (Wegen der „normativen Verklammerung des Gemeinschaftsrechts mit den Verfassungen der Mitgliedsstaaten" und der „funktionellen Verschränkung der Gerichtsbarkeit der Europäischen Gemeinschaft mit der Gerichtsbarkeit der Mitgliedsstaaten" erkennt das Bundesverfassungsgericht den EuGH als gesetzlichen Richter im Sinne des Art. 101 Abs. 1 S. 2 GG[9].) Wenn das vom Grundgesetz unabdingbar gebotene Grundrechtsschutzniveau auf diese Weise nicht erreicht werden kann, entsteht eine „Reserveprüfungskompetenz" des Bundesverfassungsgerichts. „Prüfungsgegenstand ist dann das deutsche Zustimmungsgesetz zu dem Gründungsvertrag, der dem konkreten Rechtsakt zu Grunde liegt, Prüfungsmaßstab der relativierte Standart des Grundgesetzes"[10].

3. Die Vorratsdatenspeicherungsrichtlinie als ein „ausbrechender Akt" (Prüfungsmaßstab Integrationsgrenzen)

Das BVerfG ist auch zur Prüfung der weiteren angegriffenen Regelungen befugt. Nach dem Urteil des BVerfG zum Vetrag von Maastricht prüft das Gericht auch, „ob Rechtsakte der europäischen Einrichtungen und Organe sich in den Grenzen der ihnen eingeräumten Hoheitsrechte halten oder aus ihnen ausbrechen"[11]

Bezogen auf die Vorratsdatenspeicherungsrichtlinie bedeutet dies, dass das Bundesverfassungsgericht die Rechtmäßigkeit der Vorratsdatenspeicherungsrichtlinie jedenfalls dahingehend prüfen kann und muss, ob sich der Gemeinschaftsgesetzgeber bei ihrem Erlass im Rahmen der Integrationsermächtigung gehalten hat. Dies ist bei der Vorratsdatenspeicherungsrichtlinie gerade nicht der Fall, weil sie sowohl formell- als auch materiellrechtlich offenkundig gegen das primäre Gemeinschaftsrecht verstößt[12].

Das Instrument der Richtlinie wurde in Zusammenhang mit der Einführung der Vorratsdatenspeicherung nur deswegen eingesetzt, weil es für den Erlass eines entsprechenden Rahmenbeschlusses an der notwendigen Einstimmigkeit im Rat gefehlt hat. Somit liegt ein Fall der

---

[7] 2 BvR 2236/04, Rn. 85.

[8] Das Bundesverfassungsgericht sollte dazu aber auf jeden Fall eine unmittelbare Verfassungsbeschwerde zur Prüfung annehmen, wenn die Zuständigkeit des EuGH gegeben ist, aber eines Vorlagebeschlusses bedarf. Vgl. Burkhard Hirsch, Raum der Freiheit, der Sicherheit und des Rechts, S. 323.

[9] BVerfGE 73, 339 (367f., 385).

[10] Streinz, Europarecht, S. 89.

[11] BVerfGE 89, 155, 188.

[12] Vgl. dazu unten B.V.5.c) und B.V.5.d).

evidenten Umgehung der Kompetenzordnung der EU vor. Maßnahmen, die die Kompetenzaufteilung zwischen der EG, der EU und den Mitgliedsstaaten evident missachten, sind aber vom deutschen Zustimmungsgesetz nicht gedeckt.

Daraus folgt, dass das Handeln der EG-Organe beim Erlass der RL 24/2006/EG vom deutschen Zustimmungsgesetz nicht gedeckt ist und somit innerhalb Deutschlands rechtlich unverbindlich ist[13]. Daher kann die RL 24/2006/EG in Deutschland keine Anwendung finden. Die deutschen Staatsorgane sind verfassungsrechtlich gehindert, sie ins deutsche Recht umzusetzen und zu vollziehen. Dies ist vom Bundesverfassungsgericht festzustellen[14].

4. Die Solange-Rechtsprechung des Bundesverfassungsgerichts

Sollte das BVerfG die Richtlinie 2006/24/EG für anwendbar halten, so können die Beschwerdeführer jedenfalls auch nicht darauf verwiesen werden, dass das BVerfG entsprechend der Solange II-Entscheidung[15] für die Verfassungsbeschwerde unzuständig sei.

In seinem sogenannten Solange II-Beschluss hat das Bundesverfassungsgericht postuliert: „Solange die Europäischen Gemeinschaften, insbesondere die Rechtsprechung des Gerichtshofs der Gemeinschaften einen wirksamen Schutz der Grundrechte gegenüber der Hoheitsgewalt der Gemeinschaften generell gewährleisten, der dem vom Grundgesetz als unabdingbar gebotenen Grundrechtsschutz im wesentlichen gleich zu achten ist, zumal den Wesensgehalt der Grundrechte generell verbürgt, wird das Bundesverfassungsgericht seine Gerichtsbarkeit über die Anwendbarkeit von abgeleitetem Gemeinschaftsrecht, das als Rechtsgrundlage für ein Verhalten deutscher Gerichte und Behörden im Hoheitsbereich der Bundesrepublik Deutschland in Anspruch genommen wird, nicht mehr ausüben und dieses Recht mithin nicht mehr am Maßstab der Grundrechte des Grundgesetzes überprüfen; entsprechende Vorlagen nach Art. 100 Abs. 1 GG sind somit unzulässig“ [16] . An dieser Rechtsprechung hält das Bundesverfassungsgericht grundsätzlich immer noch fest.

Allerdings behält sich das Bundesverfassungsgericht in seinem Maastricht-Urteil ausdrücklich das Recht vor, Gemeinschaftsrecht für nicht anwendbar in Deutschland zu erklären, wenn es gegen den Wesensgehalt der Grundrechte des Grundgesetzes verstößt oder sich nicht im Rahmen der der EG übertragenen Kompetenzen hält[17]. Dabei bleibt unklar, ob das Bundesverfassungsgericht sich berechtigt sieht, Gemeinschaftsrechtsakte direkt auf ihre Vereinbarkeit mit dem Grundgesetz zu prüfen. Jedenfalls besteht eine Pflicht des Bundesverfassungsgerichts „zur Wahrung des

---

[13] Vgl. BVerfGE 89, 155, 195.

[14] S. dazu Hirsch, Bemerkungen zum Schutz der Grundrechte im "Raum der Freiheit, der Sicherheit und des Rechts" der Europäischen Gemeinschaft, KritV 2006, S. 307, 320: „Das BVerfG hat das ständige Recht und die Pflicht, darüber materiell selbst zu entscheiden, ob eine Handlung oder ein Rechtsakt der Gemeinschaft, die ihr nach Art. 23 GG übertragenen Rechte überschreitet, also ultra vires, ohne eigene Rechtsgrundlage vorgenommen wird.“

[15] BVerfGE 73, 339 (387) – Solange II.

[16] BVerfGE 73, 339 (387) – Solange II.

[17] BVerfGE 89, 155 (175): „Das Bundesverfassungsgericht sichert so diesen Wesensgehalt auch gegenüber der Hoheitsgewalt der Gemeinschaft (vgl. BVerfGE 73, 339, 386). Auch Akte einer besonderen, von der Staatsgewalt der Mitgliedsstaaten geschiedenen öffentlichen Gewalt einer supranationalen Organisation betreffen die Grundrechtsberechtigten in Deutschland. Sie berühren damit die Gewährleistungen des Grundgesetzes und die Aufgaben des Bundesverfassungsgerichts, die den Grundrechtsschutz in Deutschland und insoweit nicht nur gegenüber deutschen Staatsorganen zum Gegenstand haben (Abweichung von BVerfGE 58, 1, 27)“.

Grundgesetzes gegenüber allen Akten deutscher Staatsgewalt, auch solchen, die Gemeinschaftsrecht begründen oder vollziehen“ [18] . Ein Prüfungsvorbehalt behält sich das Bundesverfassungsgericht nicht nur im Bereich des Grundrechtsschutzes, sondern auch hinsichtlich Gemeinschaftsakte, die ultra vires ergangen sind, d.h. durch die Kompetenzübertragungen des deutschen Zustimmungsgesetzes, das den Anwendungsbefehl bezüglich des Gemeinschaftsrechts enthält (Vorrang des Gemeinschaftsrechts kraft verfassungsrechtlicher Ermächtigung), nicht gedeckt sind [19] . Bemerkenswert ist in diesem Zusammenhang, dass das Bundesverfassungsgericht die Ausübung seiner Rechtsprechung anhand einer Kooperation mit dem EuGH lediglich im Bereich des Grundrechtsschutzes sieht. „Dagegen ist auf dem Feld der Kompetenzbegrenzung das Konfliktpotential noch nicht gleichermaßen entschärft. Insoweit fehlt noch eine Solange III-Entscheidung des Bundesverfassungsgerichts“[20].

Für die Feststellung, dass der gebotene Grundrechtsschutz auf EU-Ebene generell nicht gewährleistet ist, bedarf es nach der Rechtsprechung des Bundesverfassungsgerichts einer Gegenüberstellung des Grundrechtsschutzes auf nationaler und auf Gemeinschaftsebene, wie sie vom Bundesverfassungsgericht in BVerfGE 73, 339 (378 bis 381) vorgenommen wurde[21]. Im Solange II-Beschluss stellte das Bundesverfassungsgericht fest, dass „mittlerweile im Hoheitsbereich der Europäischen Gemeinschaften ein Maß an Grundrechtsschutz erwachsen (sei), das nach Konzeption, Inhalt und Wirkungsweise dem Grundrechtsstandart des Grundgesetzes im wesentlichen gleichzuachten ist“[22]. Diese Feststellung stützt sich auf eine Übersicht einzelner Entscheidungen des EuGH, wodurch einzelne Grundrechte anerkannt werden. Dabei sei die prinzipielle Haltung des EuGH gegenüber Grundrechtsgebundenheit der Gemeinschaft und der normativen Verankerung der Grundrechte im Gemeinschaftsrecht sowie die tatsächliche Bedeutung, die der Grundrechtsschutz in der Handhabung des Gerichtshofs gewonnen hat, entscheidend [23] . Allerdings stellt das Bundesverfassungsgericht ebenfalls fest, dass der Grundrechtsstandard auf der Gemeinschaftsebene im Vergleich zu diesem des Grundgesetzes noch Lücken aufweist[24]. Weitere Ausführungen dazu blieb das Bundesverfassungsgericht aber schuldig, sodass es unklar blieb, wie es um die Grundrechte bestellt ist, wenn auf der Gemeinschaftsebene generell ein Grundrechtsschutz besteht, aber in bestimmten Bereichen kein ausreichender Grundrechtsschutz vorhanden ist.

Dazu nimmt das Bundesverfassungsgericht im späteren Bananenmarkt-Beschluss in einem obiter dictum Stellung. Dort behält das Gericht grundsätzlich die Solange-Rechtsprechung bei, modifiziert sie aber teilweise: „Verfassungsbeschwerden und Vorlagen von Gerichten, die eine Verletzung in Grundrechten des Grundgesetzes durch sekundäres Gemeinschaftsrecht geltend

---

[18] Streinz, Europarecht, S. 87.
[19] BVerfGE 89, 155 (195, 210).
[20] Hirsch, EuR, Beiheft 1, 2006, S. 10.
[21] BVerfGE 102, 147, 2. LS – Bananenmarktordnung.
[22] BVerfGE 73, 339 (378).
[23] Warum dies so sein soll, also warum lediglich eine grundsätzliche positive Haltung des EuGH zum Grundrechtsschutz ausreichend zur Feststellung ist, dass ein genügender Grundrechtsschutz auf Gemeinschaftsebene gegeben, hat das Bundesverfassungsgericht nicht begründet.
[24] BVerfGE 73, 339, 383.

machen, sind von vornherein unzulässig, wenn ihre Begründung nicht darlegt, dass die europäische Rechtsentwicklung einschließlich der Rechtssprechung des Europäischen Gerichtshofs nach Ergehen der Solange II-Entscheidung (BVerfGE 73, 339, 378-381) unter den erforderlichen Grundrechtsstandart abgesunken sei"[25]. Deshalb muss die Begründung der Vorlage oder einer Verfassungsbeschwerde im Einzelnen darlegen, dass der jeweils als unabdingbar gebotene Grundrechtsschutz generell nicht gewährleistet ist[26]. Der Gebrauch des Wortes „jeweils" deutet darauf hin, dass der gebotene Grundrechtsschutz in jedem Lebensbereich vorhanden sein soll, damit angenommen werden kann, dass er auch generell gewährleistet ist. Dies wird auch durch die europabezogenen Normen des Grundgesetzes bekräftigt. Art. 23 Abs. 1 S. 1 GG verlangt zwar lediglich eine Vergleichbarkeit und keine Identität des Grundrechtsschutzes auf nationaler und europäischer Ebene. Das Gebot der Vergleichbarkeit verlangt jedoch, dass die eventuellen Abweichungen grundsätzlich in ihrer Reichweite begrenzt bleiben müssen, sodass der Kernbereich der durch die einzelnen Grundrechte geschützten Rechtsgüter und Tätigkeiten generell nicht unterbunden wird[27].

a) Kein ausreichender Grundrechtsschutz bezüglich des Datenschutzes im Telekommunikationsbereich auf EU-Ebene

Auf europäischer Ebene besteht kein dem Grundgesetz im wesentlichen vergleichbarer Grundrechtsschutz im Bereich (des Datenschutzes in) der individuellen Telekommunikation. Ein möglicherweise vorhandener Grundrechtsschutz im Bereich der individuellen Telekommunikation durch die Rechtsetzung und die Rechtsprechung auf europäischer Ebene, wird durch den Erlass der Vorratsdatenspeicherungsrichtlinie völlig ausgehöhlt. Somit sind die durch die Solange-Rechtsprechung des Bundesverfassungsgerichts aufgestellten Voraussetzungen für die Zulässigkeit einer Verfassungsbeschwerde, die sich gegen ein Gesetz richtet, das EG-Rechtsakte in nationales Recht umsetzt, gegeben.

b) Primäres und sekundäres Gemeinschaftsrecht zum Datenschutz im Telekommunikationsbereich

Der Datenschutz wurde relativ spät zum Objekt gesetzgeberischen Handelns auf europäischer Ebene. Erst mit der technischen Entwicklung und der massenhaften Einführung von Datenverarbeitungssystemen in den 80er Jahren wurden datenschutzrechtliche Regelungen einerseits für die Errichtung und für das Funktionieren des Binnenmarktes sowie zur Gewährleistung des freien Verkehrs von Waren, Personen, Dienstleistungen und Kapital und andererseits zur Wahrung der Grundrechte erforderlich[28]. Zur Erleichterung des wirtschaftlich notwendig gewordenen grenzüberschreitenden Verkehrs personenbezogener Daten, aber auch zur Gewährleistung des „in den allgemeinen Grundsätzen des Gemeinschaftsrechts anerkannten

---

[25] BVerfGE 102, 147, 1. LS – Bananenmarktordnung.
[26] BVerfGE 102, 147, 2. LS – Bananenmarktordnung.
[27] Vgl. von Mangoldt/Klein/Starck, Kommentar zum Grundgesetz, Art. 23 Abs. 1, Rn. 49.
[28] Vgl. Erwägungsgrund Nr. 3 RL 95/46/EG.

Rechts auf die Privatsphäre"[29] wurde die Schaffung eines gleichwertigen Schutzniveaus hinsichtlich der Rechte von Personen bei der Verarbeitung solcher Daten in allen Mitgliedsstaaten unerlässlich. Der europäische Gesetzgeber hat dann durch eine Reihe von Richtlinien reagiert, die auf die Angleichung der relevanten innerstaatlichen Vorschriften abzielten.

Schon im Jahre 1981 wurde das Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Konvention Nr. 108) verabschiedet. Seine Bedeutung ist u.a. deswegen hoch einzuschätzen, weil es den Stand der damaligen datenschutzrechtlichen Diskussion wiedergibt und die tragenden Prinzipien des Datenschutzrechts enthält. Geregelt wurden insbesondere die Notwendigkeit der unbedingten Zweckbindung der Speicherung und Verarbeitung von Daten (Art. 5 lit. b und c), der Auskunfts- und Löschungsanspruch (Art. 8), der qualifizierte Gesetzesvorbehalt für Grundrechtseingriffe (Art. 9).

1990 hat die Europäische Kommission ein Maßnahmenpaket zum Datenschutz vorgelegt[30]. Darauf folgend wurden die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutzrichtlinie) und die Richtlinie 97/66/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation (Telekommunikationsrichtlinie) verabschiedet. Die RL 97/66/EG wurde 2002 durch die RL 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) ersetzt. Der Erlass der RL 2002/58/EG wurde notwendig, damit die Regelungen an die Entwicklungen der Märkte und Technologien für elektronische Kommunikationsdienste angepasst werden. Die Richtlinie transponiert die Grundsätze der RL 95/46/EG in besondere Vorschriften für den Bereich der elektronischen Telekommunikation. Als Ziel der Richtlinie wird die Achtung der Grundrechte, insbesondere der in den Art. 7 und 8 GRCh niedergelegten, erklärt (Erwägungsgrund Nr. 2).

Die genannten Richtlinien etablieren die tragenden Prinzipien des europäischen Datenschutzrechts, die den Grundsätzen des deutschen Datenschutzrechts weitgehend entsprechen. Diese sind das Prinzip der Zweckbindung, der Grundsatz der Datensparsamkeit, die Löschungspflicht, das Anonymisierungsgebot etc. Insbesondere hinsichtlich der Verkehrsdaten sieht Art. 6 Abs. 1 RL 2002/58/EG vor, dass sie zu löschen oder zu anonymisieren sind, sobald sie für die Übertragung einer Nachricht nicht mehr benötigt werden. Die Verarbeitung von Verkehrsdaten, die zum Zwecke der Gebührenabrechnung und der Bezahlung von Zusammenschaltungen erforderlich sind, ist nur bis zum Ablauf der Frist zulässig, innerhalb derer die Rechnung rechtlich angefochten oder der Anspruch auf Zahlung geltend gemacht werden kann (Art. 6 Abs. 2 RL 2002/58/EG). Eine Verwendung der Verkehrsdaten zum Zwecke der Vermarktung elektronischer Telekommunikationsdienste ist nur bei Einwilligung des jeweiligen Nutzers gestattet (Art. 6 Abs. 3 RL 2002/58/EG). Allerdings ist in den genannten Richtlinien die Möglichkeit zur gesetzlichen Einschränkung der gewährleisteten Rechte vorgesehen, wenn dies für die nationale Sicherheit, die

---

[29] Erwägungsgrund Nr. 10 RL 95/46/EG.

[30] Mitteilung der Kommission zum Schutz von Personen bei der Verarbeitung personenbezogener Daten in der Gemeinschaft und zur Sicherheit der Informationssysteme vom 13. September 1990 (zitiert nach Rusteberg, VB-BW 2007, S. 171).

Landesverteidigung, und die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten notwendig, angemessen und verhältnismäßig ist (Art. 13 RL 95/46/EG und Art. 15 Abs. 1 RL 2002/58/EG). Zu bemerken ist aber, dass die Kompetenzmäßigkeit dieser Regelung zweifelhaft ist[31] sowie dass sie lediglich eine Befugnis, aber keine Pflicht für die Mitgliedsstaaten vorsieht, die Einschränkungen einzuführen. Gerade darin unterscheidet sich die Vorratsdatenspeicherungsrichtlinie von den bisherigen Regelungen. Sie verpflichtet nämlich die Mitgliedsstaaten, Telekommunikationsunternehmen zur vorrätigen Speicherung von nahezu allen anfallenden Verkehrsdaten (unabhängig davon, ob die jeweiligen Daten für die Erbringung der Telekommunikationsdienste notwendig sind).

Datenschutzrechtliche Normen wurden auch auf primärrechtlicher Ebene geschaffen. Mit dem durch den Vertrag vom Amsterdam eingeführten Art. 286 EGV wurden die gemeinschaftlichen Organe und Einrichtungen an den durch sekundärrechtliche Regelungen geschaffenen Datenschutzstandard gebunden sowie die Errichtung einer Kontrollinstanz vorgesehen, die für die Überwachung der Anwendung dieser Regelungen auf die Organe und Einrichtungen der Gemeinschaft verantwortlich ist. Zur Umsetzung dieser Vorschrift wurde die VO 45/2001 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr" verabschiedet, wodurch auch der Europäische Datenschutzbeauftragte als unabhängige Kontrollinstanz eingerichtet wurde[32].
Im Art. 8 der feierlich proklamierten Charta der Grundrechte der Europäischen Union (GRC) wird das Grundrecht auf Datenschutz ausdrücklich anerkannt: „Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten". Im Art. 7 GRC wurde auch ein Grundrecht auf Achtung des Privat- und Familienlebens, der Wohnung und der Telekommunikation verbürgt. Bekanntlich ist aber die Charta der Grundrechte der Europäischen Union rechtlich nicht bindend. Der EuGH hat sich bisher auf die Charta der Grundrechte, soweit ersichtlich, noch nicht berufen.

Die mühsam erreichten datenschutzrechtlichen Standards im Bereich der Telekommunikation auf europäischer Ebene werden durch den Erlass der Vorratsdatenspeicherungsrichtlinie völlig unterminiert. Die durch die bisher verabschiedeten Datenschutzrichtlinien etablierten Grundsätze werden durch die Vorratsdatenspeicherungsrichtlinie auf den Kopf gestellt. Im Widerspruch zum bisher geltenden Prinzip der Datensparsamkeit werden nunmehr praktisch alle anfallenden Verkehrsdaten gespeichert. Auch das Prinzip der konkreten Zweckbindung der Datenerhebung und Datenverwendung wird ausgehöhlt. Die Speicherung der Verkehrsdaten soll nach der Richtlinie anlasslos und verdachtsunabhängig, also vorrätig, erfolgen. Betroffen sind alle europäischen Bürger, die sich Telekommunikationsdienste bedienen, und zwar unabhängig davon, ob sie in irgendeiner Beziehung zu einer Straftat oder anderem Fehlverhalten stehen. „Die mit Hilfe der Vorratsdatenspeicherung abzuwehrenden Bedrohungen oder Gefahren für die Sicherheit spezieller

---

[31] Vgl. dazu Rusteberg, VBlBW 2007, S. 172 und Schild, EuZW 1996, S. 549f.

[32] Die Erwägungsgründe dieser Verordnung werden im Schrifttum als „Bekenntnis zum gemeinschaftsrechtlichen Grundrecht auf Datenschutz" angesehen. S. Mehde, in: Heselhaus/Nowak (Hrsg.), Handbuch der Europäischen Grundrechte, S. 617.

oder allgemeiner Rechtsgüter sind weder konkretisierbar, noch können Wahrscheinlichkeiten für deren tatsächliches Eintreffen angegeben werden. Das heißt, dass der Verwendungszweck der gespeicherten Daten weder bereichsspezifisch noch präzise bestimmbar ist". [33] Die Richtlinie überlässt den Mitgliedsstaaten weitreichende Umsetzungsspielräume, sodass sie die Voraussetzungen für den Zugriff auf die gespeicherten Daten frei bestimmen können (Art. 4 RL 2006/24/EG). Der datenschutzrechtliche Grundsatz der Anonymität wird, da die Richtlinie gerade auf die Identifizierbarkeit aller Telekommunikationsnutzer abzielt, vollständig abgeschafft. Vor diesem Hindergrund kann vom Datenschutz als Verbraucherschutz und als Grundrechtsschutz auf europäischer Ebene nicht mehr die Rede sein.

Der Regelungsinhalt der Vorratsdatenspeicherungsrichtlinie widerspricht somit dem in Art. 23 Abs. 1 S. 1 GG enthaltenen Gebot der Vergleichbarkeit des Grundrechtsschutzes auf nationaler und europäischer Ebene. Hoheitsrechte können auf die Europäische Union übertragen werden, wenn sie (die Europäische Union) einen dem Grundgesetz im wesentlichen vergleichbaren Grundrechtsschutz gewährleistet. Es wird zwar eine Vergleichbarkeit und keine Identität gefordert. Der Wesensgehalt der Grundrechte nach dem Grundgesetz muss allerdings auf jeden Fall gewährleistet sein[34]. Die Umsetzung der Richtlinie verlangt vom nationalen Gesetzgeber intensive Grundrechtseingriffe. Dadurch wurde der Wesensgehalt des Grundrechts auf informationelle Selbstbestimmung und des Fernmeldegeheimnisses tangiert.
Gemäß Art. 6 Abs. 3 EUV achtet die Union die nationale Identität der Mitgliederstaaten. Zur nationalen Identität gehören auch die Rechtstraditionen im Bereich des Grundrechtsschutzes. Mit der Vorratsdatenspeicherungsrichtlinie und dem Umsetzungsgesetz wird ein Paradigmenwechsel herbeigeführt, wobei die Grundrechte auf informationelle Selbstbestimmung und auf vertrauliche Kommunikation im Bereich der Telekommunikation praktisch aufgehoben werden. Damit verstößt die Richtlinie auch gegen Art. 6 Abs. 3 EUV.
Die Richtlinie 2006/24/EG widerspricht auch der Norm des Art. 6 Abs. 2 EUV, wonach die Union die Grundrechte achtet, wie sie sich aus der EKMR und den gemeinsamen Verfassungsüberlieferungen der Mitgliedsstaaten als allgemeine Grundsätze des Gemeinschaftsrechts ergeben.

Im Ergebnis kann festgehalten werden, dass mit dem Erlass der Vorratsdatenspeicherungsrichtlinie der unabdingbare Grundrechtsschutz auf europäischer Rechtsetzungsebene nicht mehr gegeben ist.

c) Der Schutz der personenbezogenen Daten im Bereich der Telekommunikation in der Rechtsprechung des EuGH

Bei der Herleitung eines Rechts auf Achtung der Privatsphäre beruft sich der EuGH auf die gemeinsamen Verfassungstraditionen der Mitgliedsstaaten sowie auf dessen Verankerung in Art. 8

[33] Leutheusser-Schnarrenberger, ZRP 2007, S. 9 (11).

EMRK. Ein ausdrückliches Grundrecht auf informationelle Selbstbestimmung hat der EuGH bislang allerdings nicht ausdrücklich anerkannt[35]. Trotzdem ist der Rechtsprechung des EuGH der Gedanke zu entnehmen, dass der Einzelne vor einer unfreiwilligen Preisgabe und einem widerrechtlichen Gebrauch seiner persönlichen Daten grundrechtlich geschützt sein soll[36]. Den Grundsatz der Vertraulichkeit des Schriftverkehrs zwischen Anwalt und Mandanten hat der EuGH durch eine rechtsvergleichende Abstraktion der relevanten nationalen Vorschriften etabliert[37].

Der EuGH hat sich aber bisher auf Art. 7 GRC, der das Recht auf Achtung der Kommunikation verbürgt, und auf Art. 8 Abs. 1 GRC, der ein Recht auf Datenschutz gewährt, mangels Rechtsverbindlichkeit der GRC nicht gestützt[38]. Soweit ersichtlich hat der EuGH bisher auch keinen europäischen Rechtsetzungsakt wegen Verletzung von europäischen Grundrechten für rechtswidrig erklärt.

5. Hilfsantrag auf Vorlage beim EuGH bezüglich der Regelungen, die lediglich die Richtlinie umsetzen und nicht über die Vorgaben der Richtlinie hinaus gehen

Dieser Antrag gilt nur für den Fall, dass sich das Bundesverfassungsgericht weiterhin an den Zulässigkeitsanforderungen der Solange-Rechtsprechung hält und sich dabei nicht der Auffassung anschließt, dass die Richtlinie als EU-Rechtssetzungsakt einen „ausbrechender Akt" darstellt bzw. dass mit der Richtlinie der Grundrechtsschutz hinsichtlich des Datenschutzes im Telekommunikationsbereich auf EU-Ebene unterminiert wird.

Das Bundesverfassungsgericht ist verpflichtet, das Vorlageverfahren nach Art. 234 EG in Gang zu setzen. Es muss die Prüfung der Vorratsdatenspeicherungsrichtlinie durch den EuGH sowohl aus formell- als auch aus materiellrechtlicher Sicht beantragen.

a) Das „Kooperationsverhältnis" zwischen dem EuGH und den nationalen (Verfassungs)gerichten beim Grundrechtsschutz

Es ist Aufgabe des EuGH das Letztentscheidungsrecht für die Interpretation des Gemeinschaftsrechts auszuüben[39].

Nach der Rechtsprechung des EuGH zum Vorrang des Gemeinschaftsrechts unterliegt das gemeinschaftliche Sekundärrecht nicht der Gültigkeitskontrolle anhand des nationalen (Verfassungs-)rechts[40]. Begründet wird das mit der Notwendigkeit der Einheitlichkeit des Gemeinschaftsrechts. Diese könnte nicht gewährleistet werden, wenn den nationalen Gerichten eine eigene Verwerfungskompetenz bezüglich EG-Rechtsnormen zuerkannt würde. Daraus ergibt

---

[34] Vgl. von Mangoldt/Klein/Starck, Kommentar zum Grundgesetz, Art. 23 Abs. 1, Rn. 48f.

[35] Vgl. dazu Rusteberg, VBBW 2007, S. 171 (176), dort auch Nachweise über relevante Gerichtsentscheidungen.

[36] Mehde, in: Heselhaus/Nowak (Hrsg.), Handbuch der Europäischen Grundrechte, S. 613. Vgl. EuGH, Rs. „Stauder" und „Panasonic.

37 Marauhn, in: Heselhaus/Nowak (Hrsg.), Handbuch der Europäischen Grundrechte, S. 578.
Ausführlicher zum grundrechtlichen Schutz der Individualkommunikation auf europäischer Ebene Marauhn, S. 585.

[38] Vgl. aber die Urteile „Österreichischer Rundfunk" und „Lindqvist", bei denen das Gemeinschaftsrecht am gemeinschaftsrechtlich rezipierten Maßstab des Art. 8 EMRK gemessen wird.

[39] EuGH, Slg. 1987, 4199, 4231, Rs. 314/85 – Foto Frost.

sich die (gemeinschaftsrechtlich in Art. 234 Abs. 2 EGV verbürgte) Vorlagepflicht der nationalen Gerichte, falls sie bei der Rechtsanwendung zu einem Auslegungsergebnis kommen, dass ein Gemeinschaftsrechtsakt gegen höherrangiges Gemeinschaftsrecht verstößt[41]. Dies gilt erst recht für das Bundesverfassungsgericht, wenn es über die Verfassungsmäßigkeit von deutschen Gesetzen zu entscheiden hat, die der Umsetzung von EG-Richtlinien dienen und Grundrechtseingriffe regeln.

Aus dem funktionellen Nebeneinander des supranationalen Rechtssystems der EG und den Rechtordnungen der Mitgliederstaaten ergibt sich für das Verhältnis zwischen dem EuGH und den nationalen Gerichten, dass es keinen hierarchischen, sondern einen kooperativen Charakter aufweist[42]. Dieses Kooperationsverhältnis zwischen den nationalen (Verfassungs)gerichten und dem EuGH ist in Zusammenhang mit der Gewährleistung eines ausreichenden Grundrechtsschutzes auf nationaler und europäischer Ebene von besonderer Bedeutung[43]. Das Vorlageverfahren gemäß Art. 234 EGV stellt in diesem Sinne ein wichtiges Instrument für die Kooperation zwischen dem EuGH und dem Bundesverfassungsgericht sowie für das Funktionieren der Gemeinschaftsordnung dar.

b) Vorlagepflicht des Bundesverfassungsgerichts

Gemäß Art. 234 Abs. 1 lit. B EGV entscheidet der EuGH im Wege der Vorabentscheidung über die Gültigkeit und die Handlungen der Organe der Gemeinschaft. Wird eine derartige Frage in einem schwebenden Verfahren bei einem einzelstaatlichen Gericht gestellt, dessen Entscheidungen selbst nicht mehr mit Rechtsmitteln des innerstaatlichen Rechts angefochten werden können, so ist dieses Gericht zur Anrufung des Gerichtshofes verpflichtet (Art. 234 Abs. 3 EGV). Das Bundesverfassungsgericht sieht sich selbst als letztinstanzielles Gericht im Sinne des Art. 234 Abs. 3 EGV, hat allerdings bisher, soweit ersichtlich, noch nie eine Rechtssache dem EuGH vorgelegt[44].

Die Vorlagepflicht des Bundesverfassungsgerichts der nationalen letztinstanziellen Gerichte ist sowohl gemeinschafts- als auch verfassungsrechtlich begründet. Die Feststellung der Ungültigkeit des sekundären Gemeinschaftsrechts ist nach anerkannter Auffassung ausschließlich dem EuGH vorbehalten[45]. Die gebotene einheitliche Geltung des Gemeinschaftsrechts sowie die Gleichheit vor dem europäischen Gesetz wäre beeinträchtigt, wenn bei der Entscheidung über die Gültigkeit von Handlungen der Gemeinschaftsorgane Normen des nationalen Rechts herangezogen werden oder wenn nationale Gerichte diesbezüglich „das letzte Wort" hätten[46].

Daher muss das Bundesverfassungsgericht bei entsprechenden Verfahren zur Vereinbarkeit des jeweiligen Gesetzes mit einem europäischen Rechtsakt und zur Vereinbarkeit dieses Rechtsakts mit dem primären Gemeinschaftsrecht Stellung nehmen. Käme es dabei zu dem Ergebnis, dass der europäische Rechtsakt aus formellen oder materiellen Gründen rechtswidrig ist, wäre es

---

[40] EuGHE 1970, 1125, Rn. 3 – Internationale Handelsgesellschaft; EuGHE 1987, 4199, Rn. 14f. – Foto-Frost.
[41] Streinz, Europarecht, S. 235.
[42] Rodriguez Iglesias, NJW 2000, 1889 (1890).
[43] Vgl. Pernice, EuR, 1996, S. 33.
[44] BVerfGE 37, 271, 282; 52, 187, 201; siehe dazu Feige, AöR 100 (1975), 530 (531).
[45] EuGH, Urteil vom 22. Oktober 1987, Rs. 314/85, Foto-Frost, Slg. 1987, 4199.

verpflichtet, den Gerichtshof der Europäischen Gemeinschaften im Wege der Vorabentscheidung nach Art. 234 EGV anzurufen[47].

Verletzt das Bundesverfassungsgericht die Vorlagepflicht nach Art. 234 EG, kann der Betroffene eine Verfassungsbeschwerde nach Art. 101 Abs. 1 S. 2 GG erheben, da der EuGH als gesetzlicher Richter im Sinne dieser Norm vom Bundesverfassungsgericht anerkannt ist[48]. Dabei braucht er keinen Willkür nachzuweisen, da die Vorlage beim EuGH oft die einzige Möglichkeit ist, Grundrechtsschutz gegen Akte der EG zu erlangen[49]. Dies wird vom Bundesverfassungsgericht im „Teilzeitarbeit-Urteil" ausdrücklich anerkannt: „Denn der Grundrechtsschutz der Beschwerdeführerin liefe ins Leere, wenn das Bundesverfassungsgericht mangels Zuständigkeit keine materielle Prüfung anhand der Grundrechte vornehmen kann und der Europäische Gerichtshof mangels Vorabentscheidungsersuchens nicht die Möglichkeit erhält, sekundäres Gemeinschaftsrecht anhand der für die Gemeinschaft entwickelten Grundrechtsverbürgungen zu überprüfen"[50].

Im Zusammenhang mit der Prüfung des Umsetzungsgesetzes zur Vorratsdatenspeicherungsrichtlinie spricht für eine Vorlage auch die Tatsache, dass die Frage des „Ob" einer Vorratsdatenspeicherung bereits durch die Richtlinie entschieden ist. Falls das BVerfG an der Solange-Rechtsprechung festhält, kann es (soweit sich das Umsetzungsgesetz im Rahmen der Richtlinie hält) über die Verfassungsmäßigkeit der Speicherungspflicht nicht urteilen. Dadurch wäre eine Klärung seitens des EuGH im Sinne der Kooperation im Bereich des Grundrechtsschutzes unentbehrlich[51].

Da die Feststellung der Ungültigkeit sekundären Gemeinschaftsrechts dem EuGH vorbehalten ist, ist das Bundesverfassungsgericht zur Vorlage verpflichtet, wenn es die Richtlinie 2006/24/EG aus formellen oder materiellen Gründen für rechtswidrig hält (wenn an der Rechtmäßigkeit der Richtlinie Zweifel bestehen) oder wenn es bei ihrer Auslegung auf Schwierigkeiten stößt. Die Voraussetzungen für die Entstehung der Vorlagepflicht des Bundesverfassungsgerichts sind bezüglich der Vorratsdatenspeicherungsrichtlinie bzw. des Umsetzungsgesetzes gegeben. Die Vorratsdatenspeicherungsrichtlinie ist sowohl formellrechtlich wegen der Wahl eines falschen Kompetenztitels als auch materiellrechtlich wegen Grundrechtsverletzungen rechtswidrig.

---

[46] Vgl. EuGHE 1970, 1125, Rn. 3 – Internationale Handelsgesellschaft; EuGHE 1964, 1141, Rn. 9 – Costa/ENEL.

[47] In der Entscheidung zur Rechtssache Union de Pequenos Agricultores betont der EuGH, dass „die nationalen Gerichte gemäß dem in Art. 5 EGV aufgestellten Grundsatz der loyalen Zusammenarbeit die nationalen Verfahrensvorschriften über die Einlegung von Rechtsbehelfen möglichst so auszulegen und anzuwenden (haben), dass natürliche und juristische Personen die Rechtmäßigkeit jeder nationalen Entscheidung oder Maßnahme, mit der eine Gemeinschaftshandlung allgemeiner Geltung auf sie angewandt wird, gerichtlich anfechten und sich dabei auf die Ungültigkeit dieser Handlung berufen können" (EuGHE, Rs. C-50/00 P, Union de Pequenos Agricultores, Slg. 2002, I-6677, Rn. 42).

[48] Streinz, S. 240; BVerfGE 73, 339 (385).

[49] Pernice, S. 31.

[50] BVerfGE, NJW 2001, S. 1267(1268) – Teilzeitarbeit. (Vgl. auch Handbuch der Europäischen Grundrechte, S. 321)

[51] Dem steht die CILFIT-Rechtsprechung des EuGH nicht entgegen. Danach ist ein mitgliedsstaatliches Gericht zur Einleitung eines Vorabentscheidungsverfahrens nicht verpflichtet, wenn eine gesicherte gemeinschaftsrechtliche Rechtsprechung vorliegt, durch welche die betreffende Rechtsfrage geklärt ist oder wenn die richtige Auslegung des Gemeinschaftsrechts offensichtlich ist („acte claire-Doktrin). Vgl. EuGHE 1982, I-3415, Rn. 14 und 16 – CILFIT. Beides ist im vorliegenden Fall nicht gegeben.

c) Formelle Rechtswidrigkeit der Vorratsdatenspeicherungsrichtlinie

An der formellen Rechtmäßigkeit der Vorratsdatenspeicherungsrichtlinie bestehen erhebliche Zweifel. Die Richtlinie wird auf Art. 95 Abs. 1 EGV gestützt. Diese Norm bietet eine Rechtsgrundlage für Maßnahmen zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedsstaaten, welche die Errichtung und das Funktionieren des Binnenmarktes zum Gegenstand haben. In seiner Rechtsprechung verlangt der EuGH, dass eine auf der Grundlage von Art. 95 Abs. 1 EGV erlassene Richtlinie tatsächlich den primären Zweck haben soll, die Voraussetzungen für die Errichtung und das Funktionieren des Binnenmarktes zu verbessern[52]. Dabei hat der EuGH strenge Maßstäbe entwickelt: Eine bloße Feststellung von Unterschieden zwischen den nationalen Vorschriften und eine abstrakte Gefahr der Entstehung von Wettbewerbsverzerrungen rechtfertigen demnach nicht die Berufung auf Art. 95 EGV als Rechtsgrundlage einer Richtlinie[53].

Die politische Auseinandersetzung um die Vorratsspeicherung von Verkehrsdaten erfolgte auf europäischer Ebene stets im Kontext der polizeilichen und justiziellen Zusammenarbeit in Strafsachen. Der Wechsel zur Handlungsform der Richtlinie wurde erst vollzogen, nachdem die für den ursprünglich vorgelegten Entwurf eines Rahmenbeschlusses nach Art. 31 und 34 EUV erforderliche Einstimmigkeit nicht erreicht werden konnte[54]. Die Wahl des Regelungsinstruments der „Rechtsangleichungsrichtlinie" nach Art. 95 EGV wurde mit der vermeintlichen Notwendigkeit einheitlicher Regelungen bezüglich der Speicherungspflichten der Telekommunikationsunternehmen in allen Mitgliedsstaaten zur Gewährleistung eines funktionierenden Binnenmarktes begründet. Die Unterschiede zwischen den nationalen Vorschriften zur Speicherung von Telekommunikationsdaten beeinträchtigten den Binnenmarkt für elektronische Kommunikation, da die Dienstanbieter in den einzelnen Mitgliedsstaaten divergierende Anforderungen hinsichtlich der zu speichernden Arten von Verkehrs- und Standortdaten, der Voraussetzungen und der Dauer der Vorratsdatenspeicherung unterliegen[55].

Nach ständiger Rechtsprechung des EuGH muss sich die Wahl der Rechtsgrundlage eines gemeinschaftlichen Rechtsaktes generell auf objektive, gerichtlich nachprüfbare Umstände stützen. Dazu gehören insbesondere das Ziel und der Inhalt des jeweiligen Rechtsaktes[56].

Ergibt die Prüfung eines gemeinschaftlichen Rechtsakts, dass er zwei Zielsetzungen verfolgt oder zwei Komponenten hat, und lässt sich eine davon als wesentliche oder überwiegende ausmachen, während die andere nur von untergeordneter Bedeutung ist, so ist der Rechtsakt nur auf eine Rechtsgrundlage zu stützen, und zwar auf diejenige, die die wesentliche oder überwiegende Zielsetzung oder Komponente erfordert[57]. Lediglich dann, wenn mit dem Rechtsakt gleichzeitig

---

[52] EuGH, Urteil vom 5. Oktober 2000, Rs. C-376/98, Deutschland/EP und Rat („Tabakwerbeverbotsrichtlinie"), Slg. 2000, I-8419, Rn. 86.

[53] Streinz, Europarecht, 7. Aufl., Heidelberg 2005, S. 361.

[54] Ratsdokument 8958/04 vom 28. April 2004.

[55] Vgl. Erwägungsgründe 5 und 6 der Richtlinie 2006/24/EG.

[56] Vgl. EuGH, Rs. C-176/03, Kommission/Rat, Rn. 45; Rs. C-300/89, Kommission/Rat („Titandioxid"), Slg. 1991, I-2867, Rn. 10; Rs. C-336/00, Huber, Slg. 2002, I-7699, Rn. 30.

[57] Vgl. Urteile vom 17. März 1993, Rs. C-155/91, Kommission/Rat, Slg. 1993, I-939, Rn. 19 und 21, vom 23. Februar 1999, Rs. C-42/97, Parlament/Rat, Slg. 1999, I-869, Rn. 39 und 40, vom 30. Januar 2001, Rs. C-36/98, Spanien/Rat, Slg. 2001, I-779, Rn. 59 und vom 19. September 2002, Rs. C-336/00, Huber, Slg. 2002, I-7699, Rn. 31.

mehrere Ziele verfolgt werden, die untrennbar miteinander verbunden sind, ohne dass das eine im Verhältnis zum anderen zweitrangig ist und mittelbaren Charakter hat, kann ein solcher Rechtsakt ausnahmsweise auf die verschiedenen einschlägigen Rechtsgrundlagen gestützt werden [58]. Voraussetzung ist allerdings, dass die einschlägigen Gesetzgebungsverfahren miteinander vereinbar sind[59].

Das Ziel und der Inhalt der Vorratsdatenspeicherungsrichtlinie betreffen aber in erster Linie die Vorsorge zur Strafverfolgung. So heißt es im Art. 1 Abs. 1 RL 2006/24/EG: „Mit dieser Richtlinie sollen die Vorschriften der Mitgliederstaaten über die Pflichten von Anbietern öffentlich zugänglicher Telekommunikationsdienste oder Betreiber eines öffentlichen Kommunikationsnetzes im Zusammenhang mit der Vorratsdatenspeicherung bestimmter Daten, die von ihnen erzeugt oder verarbeitet werden, harmonisiert werden, um sicherzustellen, dass die Daten zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten, wie sie von jedem Mitgliedsstaat in seinem nationalen Recht bestimmt werden, zur Verfügung stehen"[60]. Somit ist das Primärziel der Richtlinie eindeutig die Verbesserung der Strafverfolgung. Die Angleichung nationaler Rechtsvorschriften zwecks Verbesserung des Binnenmarktes kann bei der Vorratsdatenspeicherung, wenn überhaupt, lediglich als sekundärer Zweck bezeichnet werden[61].

Zu bemerken ist diesbezüglich noch, dass lediglich mittelbare Auswirkungen, die ein Rechtsakt im Bereich des Binnenmarkts herbeiführen kann, die Berufung auf Art. 95 EGV bei seinem Erlass nicht rechtfertigt[62]. Vielmehr ist es notwendig, dass ein auf Art. 95 EGV beruhender Rechtsakt tatsächlich den Zweck haben muss, die Errichtung und das Funktionieren des Binnenmarkts zu erleichtern[63]. Art. 95 EGV darf auch wegen des in Art. 5 Abs. 1 EGV verankerten Prinzips der begrenzten Einzelermächtigung nicht als eine allgemeine Kompetenz zur Regelung des Binnenmarktes interpretiert werden[64]. Dies widerspräche auch dem Wortlaut des Art. 95 Abs. 1 EGV.

Betreffend den Inhalt der Richtlinie verpflichtet Art. 3 Abs. 1 RL 2006/24/EG die Mitgliedsstaaten, sicherzustellen, dass die in Art. 5 genannten Daten auf Vorrat gespeichert werden. Den Mitgliedsstaaten steht es frei, die zugriffberechtigten Strafverfolgungsbehörden und die Voraussetzungen (Katalog der Straftaten, Zugriffsverfahren etc.) für den Zugriff auf die gespeicherten Daten zu regeln (Art. 4). Hinsichtlich der Speicherungsfristen sieht die Richtlinie

---

[58] Vgl. die Urteile Titandioxid, a.a.O., Rn. 13 und 17, Parlament/Rat, a.a.O., Rn. 38, Gutachten 2/00 vom 6. Dezember 2001, Slg. 2001, I-9713, Rn. 23, Huber, a.a.O., Rn. 31 und Urteil vom 10. Januar 2006, Kommission/Parlament und Rat, C-178/03, Rn. 43.

[59] Vgl. Urteil vom 29. April 2004, Rs. C-338/01, Kommission/Rat, Slg. 2004, I-4829: Artikel 95 (Mitentscheidung) ist subsidiär zu Artikeln 93 und 94 EG (Anhörung und Einstimmigkeit).

[60] Vgl. auch Erwägungsgründe Nr. 7 und 21 RL2006/24/EG.

[61] Wenn die Zielsetzung eines gemeinschaftlichen Rechtsaktes zwei Komponente hat und eine davon als überwiegende erscheint, dann ist der Rechtsakt auf die Rechtsgrundlage zu stützen, die die wesentliche Zielsetzung erfordert: Vgl. EuGH, Urteil vom 30. Januar, Rs. C-36/98, Spanien/Rat, Slg. 2001, I-779, Rn. 59.

[62] Vgl. Urteil vom 10. Dezember 2002, Rs. C-491/01, British American Tobacco, Slg. 2002, I-11453, Rn. 61; Urteil vom 14. Dezember 2004, Rs. C-434/02, Arnold Andrè, Slg. 2004, I-11825, Rn. 30.

[63] Zwar kann der Zweck einer Harmonisierungsmaßnahme nach Art. 95 EGV auch darin bestehen, neue Hindernisse für den freien Handel infolge der uneinheitlichen Entwicklung der nationalen Rechtsvorschriften zu verhindern. Das Entstehen solcher Hindernisse muss aber wahrscheinlich sein und die Maßnahme muss ihr Auftreten tatsächlich bezwecken (Vgl. Urteil 13. Juli 1995, Rs. C-350/92, Spanien/Rat, Slg. 1995, I-1985, Rn. 35; Urteil vom 5. Oktober 2000, Rs. C-376/98, Deutschland/Parlament und Rat, Slg. 2000, I-8419, Rn. 86). Diese Voraussetzungen liegen im Fall der geplanten Vorratsdatenspeicherung offensichtlich nicht vor.

eine Mindestspeicherungsfrist von sechs Monaten und eine maximale Speicherungsfrist von höchstens zwei Jahren vor (Art. 6). Da die Richtlinie die Regelung zahlreicher essentieller Bereiche dem freien Ermessen der Mitgliedsstaaten überlässt, kann sie keine Harmonisierung der relevanten Vorschriften in den Mitgliedsstaaten herbeiführen. Wenn die Vorratsdatenspeicherungsrichtlinie in Wirklichkeit nicht geeignet ist, eine Harmonisierung zu fördern, darf sie auf Art. 95 EGV auch nicht gestützt werden.

Die Auffassung, dass die Vorratsdatenspeicherungsrichtlinie als formell nichtig anzusehen ist, wird auch durch die neuere Rechtsprechung des EuGH bekräftigt. Im Urteil vom 30. Mai 2006 zur Übermittlung von Flugpassagierdaten in die USA erklärte der EuGH in ähnlicher Konstellation den ebenfalls auf Art. 95 EGV gestützten Beschluss des Rates 2004/496/EG zum Abschluss eines Abkommens zwischen der EG und den USA über die Verarbeitung und Übermittlung von Fluggastdatensätzen sowie die nach Art. 25 Abs. 6 S. 1 der aufgrund des Art. 95 EGV erlassenen Richtlinie 95/46/EG (Datenschutzrichtlinie) getroffene Angemessenheitsentscheidung der Kommission über die Angemessenheit des Schutzes der in den Passagierdaten enthaltenen personenbezogenen Daten, die übermittelt werden sollen, mangels Rechtsgrundlage für nichtig[65]. Die Europäische Kommission vertrat die Auffassung, dass die Tätigkeit der Fluggesellschaften bei der Erhebung und der Übermittlung der Passagierdaten in den Anwendungsbereich des Gemeinschaftsrechts falle, unter anderem auch, weil es sich dabei um Tätigkeiten von Privatpersonen und nicht von staatlichen Behörden handele[66]. Der EuGH hat sich dieser Ansicht nicht angeschlossen. Er hat zwar akzeptiert, dass die Fluggastdaten ursprünglich im Rahmen einer unter das Gemeinschaftsrecht fallenden Tätigkeit erhoben worden sind, nämlich beim Verkauf von Flugtickets, der eine Dienstleistung darstelle. Die Übermittlung der Passagierdaten sei aber „eine Datenverarbeitung, die nicht für die Erbringung einer Dienstleistung erforderlich ist, sondern zum Schutz der öffentlichen Sicherheit und zu Strafverfolgungszwecken als erforderlich angesehen wird"[67]. Da dieser Zweck aber durch Art. 3 Abs. 2 RL 95/46/EG aus dem Anwendungsbereich der Richtlinie ausdrücklich ausgenommen ist, durfte die Angemessenheitsentscheidung der Kommission nicht erlassen werden. Die Tatsache, dass die Datenübermittlung durch die Fluggesellschaften als private Wirtschaftsteilnehmer erfolgt, sei nicht von Belang, weil sie in einem staatlich geschaffenen Rahmen durchgeführt werde und der öffentlichen Sicherheit diene[68]. Der Ratsbeschluss zum Abschluss des Passagierdaten-Abkommens durfte nach Ansicht des EuGH ebenfalls nicht auf der Grundlage des Art. 95 EGV erlassen werden, weil das Abkommen eine Verarbeitung von Daten betrifft, die nicht in den Anwendungsbereich des Gemeinschaftsrechts fiele[69].

---

[64] Vgl. EuGH, Urteil vom 5. Oktober 2000, Rs. C-376/98, Tabakwerberichtlinie, Slg. 2000, I-8419 (EuZW 2000, 694, Rn. 83).
[65] EuGH, Urteil vom 30. Mai 2006, Rs. C 317/04 und C-318/04, EP/Rat = NJW 2006, S. 2029f.
[66] EuGH, Urteil vom 30. Mai 2006, Rs. C 317/04 und C-318/04, EP/Rat, Abs. 53.
[67] EuGH, Urteil vom 30. Mai 2006, Rs. C 317/04 und C-318/04, EP/Rat, Abs. 57.
[68] EuGH, Urteil vom 30. Mai 2006, Rs. C 317/04 und C-318/04, EP/Rat, Abs. 58.
[69] EuGH, Urteil vom 30. Mai 2006, Rs. C 317/04 und C-318/04, EP/Rat, Abs. 68.

Auch die vorrätige Speicherung von Verkehrsdaten ist für die Erbringung der jeweiligen Telekommunikationsdienstleistungen nicht erforderlich, bezweckt primär die Verbesserung der Strafverfolgung und fällt daher nicht in den Anwendungsbereich des Gemeinschaftsrechts[70].

Dem 2005 ergangenen Urteil des EuGH[71] über den Rahmenbeschluss des Rates zum Schutz der Umwelt durch das Strafrecht[72] sind ebenfalls keine Argumente gegen die hier angenommene formelle Rechtswidrigkeit der Vorratsdatenspeicherungsrichtlinie zu entnehmen. Der auf Titel VI des Vertrags über die Europäische Union gestützte Rahmenbeschluss definiert eine Reihe von Umweltstraftaten und verpflichtet die Mitgliedsstaaten, entsprechende strafrechtliche Sanktionen vorzusehen. Die Europäische Kommission und das Europäische Parlament vertraten die Auffassung, dass für dieses Vorhaben Art. 175 Abs. 1 EG die richtige Rechtsgrundlage sei[73]. Der EuGH entschied, dass Art. 1 bis 7 des Rahmenbeschlusses die Zuständigkeit der Gemeinschaft nach Art. 175 EG (Umweltschutz) insoweit berühren, als sie auf der Grundlage dieser Bestimmung hätten erlassen werden können und erklärte den Rahmenbeschluss für nichtig. Seinem Zweck und Inhalt nach verfolge der Rahmenbeschluss das Ziel des Umweltschutzes. Seine Art. 2 bis 7 enthielten zwar eine begrenzte Teilharmonisierung der strafrechtlichen Vorschriften der Mitgliedsstaaten, insbesondere im Bezug auf die Tatbestandsmerkmale verschiedener Umweltstraftaten. Dies führe aber nicht dazu, dass die Rechtsform des Rahmenbeschlusses hätte gewählt werden müssen. Grundsätzlich fielen das Straf- und das Strafprozessrecht nicht in die Zuständigkeit der Gemeinschaft. Dies könne „den Gemeinschaftsgesetzgeber jedoch nicht daran hindern, Maßnahmen in Bezug auf das Strafrecht der Mitgliedsstaaten zu ergreifen, die seiner Meinung nach erforderlich sind, um die volle Wirksamkeit der von ihm zum Schutz der Umwelt erlassenen Rechtsnormen zu gewährleisten, wenn die Anwendung wirksamer, verhältnismäßiger und abschreckender Sanktionen durch die zuständigen nationalen Behörde eine zur Bekämpfung schwerer Beeinträchtigungen der Umwelt unerlässliche Maßnahme darstellt"[74]. Begründet wurde dies mit der überragenden Bedeutung des Umweltschutzes im Gemeinschaftsrecht und mit der Unerlässlichkeit wirksamer Sanktionen gegen Umweltverstöße[75]. Der Umweltschutz sei eines der wesentlichen Ziele der Gemeinschaft und seine Erfordernisse müssten nach Art. 6 EG bei der Festlegung und Durchführung der Gemeinschaftspolitiken einbezogen werden. Der Querschnittscharakter und die herausragende Bedeutung dieses Zieles rechtfertigen den Vorzug des Art. 175 EG (vor dem Art. 34 EU) als Rechtsgrundlage[76]. Der Rahmenbeschluss verstöße

---

[70] In seinen Schlussanträgen zum Flugpassagierdaten-Urteil weist der Generalanwalt Lèger ausdrücklich auf die Vorratsdatenspeicherung hin und nimmt eine fehlende Regelungskompetenz der EG für alle Fälle an, bei denen eine juristische Person zur Verarbeitung und Weitergabe von personenbezogenen Daten an staatliche Stellen zu Sicherheits- und Strafverfolgungszwecken verpflichtet ist. Vgl. Schlussanträge des Generalanwalts Philippe Lèger vom 22.11.2005 zur Rs. C-317/04, Abs. 160.

[71] Urteil vom 13. September 2005, Rs. C-176/03 (= EuZW 2005, 632).

[72] ABl. L 29, 55 vom 5. Februar 2003.

[73] Urteil vom 13. September 2005, Rs. C-176/03, Rn. 11.

[74] Urteil vom 13. September 2005, Rs. C-176/03, Rn. 48.

[75] Urteil vom 13. September 2005, Rs. C-176/03, Rn. 41.

[76] Urteil vom 13. September 2005, Rs. C-176/03, Rn. 42.

dadurch, dass er in die nach Art. 175 EG der Gemeinschaft übertragene Kompetenzen übergreife, aufgrund seiner Unteilbarkeit gegen Art. 47 EU[77].

Im Unterschied zur Konstellation dieser Rechtssache wirft die Vorratsdatenspeicherungsrichtlinie bereits Probleme bei der Suche nach einer möglichen Rechtsgrundlage im Gemeinschaftsrecht auf. Denn Art. 95 EG erlaubt eine Harmonisierung nur in Bereichen, die in die Zuständigkeit der Gemeinschaft fallen. Um die Lösung aus dem Urteil zum Umweltstrafrecht auf die Problematik der Vorratsdatenspeicherung übertragen zu können, müsste zunächst eine Verbandskompetenz für die zu regelnde Sachmaterie begründet werden. Hieran fehlt es der Gemeinschaft aber.

Die Umweltstrafrechtsentscheidung stellt auch deswegen keine Vorentscheidung für die Kompetenz bezüglich der Richtlinie 2006/24/EG dar, weil es sich bei der Vorratsdatenspeicherung nicht primär um eine strafrechtliche Absicherung des Gemeinschaftsrechts, wie etwa bei der strafrechtlichen Sanktionierung von Verstößen gegen das Datenschutzrecht, handelt. Die Vorratsdatenspeicherungsrichtlinie bezweckt von Anfang an, dass die Telekommunikationsverkehrsdaten zum Zwecke der Bekämpfung von Straftaten zur Verfügung stehen (vgl. Art. 1 Abs. 1 RL 2006/24/EG)[78].

Zwischenergebnis: Die Vorratsdatenspeicherungsrichtlinie ist wegen ihrer fehlenden Rechtsgrundlage deshalb als formell nichtig anzusehen. Die richtige Rechtsgrundlage für den Erlass einer Regelung, die die EU-Mitgliedsstaaten zur Einführung der Vorratsdatenspeicherung verpflichtet, wäre ein Rahmenbeschluss im Bereich der dritten Säule der Europäischen Union. Es ist zu erwarten, dass die von der Republik Irland erhobene Nichtigkeitsklage gegen die Richtlinie Erfolg haben wird[79]. Diese Prognose wird durch die neuere Rechtsprechung des EuGH bekräftigt.

d) Materiellrechtliche Rechtswidrigkeit der Vorratsdatenspeicherungsrichtlinie

Es bestehen erhebliche Zweifel, ob der Inhalt der Richtlinie dem Maßstab von Art. 8 EMRK standhält. Bei der Prüfung der Eingriffe in das durch Art. 8 EMRK gewährleistete Grundrecht auf Privatsphäre und private Telekommunikation orientiert sich der EuGH an der Rechtsprechung des EMGR[80]. Eingriffe in dieses Grundrecht sind zulässig, insoweit sie gesetzlich vorgesehen sind und Maßnahmen darstellen, die in einer demokratischen Gesellschaft zum Schutz der nationalen Sicherheit, der öffentlichen Ordnung sowie zur Verhütung von Straftaten und zum Schutz der Rechte und Freiheiten anderer notwendig sind (Art. 8 Abs. 2 EMRK). Durch die Verpflichtung zur vorrätigen Speicherung der Kommunikationsdaten sämtlicher Nutzer greift die Richtlinie in das Gemeinschaftsgrundrecht auf Achtung des Privatlebens und der Korrespondenz aus Art. 8 EMRK unverhältnismäßig ein. Eine Erfassung sämtlicher Telekommunikation aller EU-Bürger ohne konkreten Anlass und ohne jeglichen Tatverdacht kann in einer demokratischen Rechtsordnung nicht als notwendig angesehen werden.

---

[77] Urteil vom 13. September 2005, Rs. C-176/03, Rn. 53.
[78] Rusteberg, VBlBW 2007, S. 171 (174).
[79] EuGH, Rs. C-301/06.
[80] Vgl. EuGH, Rs. 136/79, „National Panasonic", Slg. 1980, S. 2033; EuGH, Rs. 46/87 und 227/88, "Hoechst", Slg. 1989, 2859f.

e) Keine prozessualen Hindernisse für die Vorlage durch das Bundesverfassungsgericht

Der Vorlage durch das Bundesverfassungsgericht stehen keine Hindernisse prozessualrechtlichen Charakters im Wege.

Die Tatsache, dass eine Klage gegen die Vorratsdatenspeicherungsrichtlinie beim EuGH bereits anhängig ist (Nichtigkeitsklage von Irland, EuGH, Rs. 301/06), stellt kein prozessuales Hindernis dar. Soweit bekannt, bezieht sich die Klage Irlands lediglich auf die formelle Rechtsmäßigkeit der Richtlinie. Mit der hier beantragten Vorlage wird auch die materiellrechtliche Prüfung der Vereinbarkeit der Richtlinie mit den Europäischen Grundrechten durch den EuGH angestrebt.

Die Vorlage ist auch deswegen zulässig, weil auf EU-Ebene keine gesicherte Rechtsprechung im Bereich des Datenschutzes in der Telekommunikation gegeben ist bzw. weil keine Auslegung der in Betracht kommenden Vorschriften offenkundig ist[81]

[81] Zur CILFIT-Rechtsprechung (EuGHE 1982, I-3415, Rn. 16) vgl. Pernice, Europäische und nationale Gerichte, S. 22f.).

C. Begründetheit

Die Verfassungsbeschwerde ist begründet, weil die Beschwerdeführer durch das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG und Art 34b Abs. 2 i. V. m. Art. 34a Abs. 1 Satz 1, Abs. 3 S. 1 BayPAG, Art. 6c BayVSG und § 34 a ThürPAG in ihren Grundrechten aus Art. 10 Abs. 1, aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1, Art. 5 Abs. 1 Satz 2, Art. 4 Abs. 1, Art. 12 Abs. 1 GG, Art. 19 Abs. 4 und Art. 103 Abs. 1 GG verletzt sind. Die §§ 113a und 113b TKG sowie § 100g StPO, Art 34b Abs. 2 i. V. m. Art. 34a Abs. 1 Satz 1, Abs. 3 S. 1 BayPAG, Art. 6c BayVSG und § 34 a ThürPAG stellen ungerechtfertigte Grundrechtseingriffe dar.

I. Verletzung des Fernmeldegeheimnisses, Art. 10 Abs. 1 GG

1. Betroffenheit des Schutzbereichs des Fernmeldegeheimnisses

Die angegriffenen Rechtsnormen berühren den Schutzbereich des Grundrechts aus Art. 10 Abs. 1 GG der Beschwerdeführer. Der Schutzbereich des Fernmeldegeheimnisses erstreckt sich auf jede Übermittlung von Informationen mit Hilfe der verfügbaren Telekommunikationsmittel und umfasst sowohl den Inhalt der Telekommunikation als auch die näheren Umstände des Fernmeldeverhältnisses[82]. Dazu gehört insbesondere, ob, wann und wie oft zwischen Personen oder Endeinrichtungen Telekommunikationsverkehr stattgefunden hat oder versucht worden ist. Anderenfalls wäre der grundrechtliche Schutz unvollständig, denn die Verbindungsdaten haben einen eigenen Aussagegehalt. Sie können im Einzelfall erhebliche Rückschlüsse auf das Kommunikations- und Bewegungsverhalten zulassen. Häufigkeit, Dauer und Zeitpunkt von Kommunikationsverbindungen geben Hinweise auf Art und Intensität von Beziehungen und ermöglichen auf den Inhalt bezogene Schlussfolgerungen[83]. Daher soll die Nutzung jedes Kommunikationsmediums in allem vertraulich möglich sein[84].

Der Schutz des Art. 10 Abs. 1 GG erstreckt sich auch auf den Informations- und Datenverarbeitungsprozess, der sich an zulässige Kenntnisnahmen anschließt und den Gebrauch, der von den erlangten Kenntnissen gemacht wird[85].

---

[82] BVerfGE 67, 157 (172).
[83] BVerfG, NJW 2006, 976 (978). Vgl. auch BVerfGE 107, 299 (320); 113, 348 (365).
[84] BVerfGE 100, 313 (358).
[85] BVerfGE 100, 313 (359).

2. Zweistufiger Eingriff in das Fernmeldegeheimnis

Ein Eingriff in das Fernmeldegeheimnis liegt vor, wenn staatliche Stellen sich ohne Zustimmung der Betroffenen Kenntnis von dem Inhalt oder den Umständen eines fernmeldetechnisch vermittelten Kommunikationsvorgangs verschaffen [86] . Die vorgesehenen Regelungen zur Umsetzung der Richtlinie 2006/24/EG greifen zweistufig in das Fernmeldegeheimnis der Beschwerdeführer ein. Auf der ersten Stufe erfolgt der Eingriff in das Kommunikationsgeheimnis mit der gesetzlich angeordneten Verpflichtung der Anbieter öffentlicher Telekommunikationsdienste, die anfallenden Verbindungsdaten für 6 Monate zu speichern (vgl. § 113a Abs. 1 bis 5 TKG). Die Tatsache, dass die Erhebung und Speicherung der Daten durch die Telekommunikationsunternehmen und nicht direkt durch staatliche Stellen erfolgt, ändert an ihrer Qualität als staatlichem Eingriff in das Fernmeldegeheimnis nichts. Die vorgesehene Erfassung und Speicherung ist hoheitlich angeordnet, die Unternehmen verfügen dabei über keinen Handlungsspielraum [87] . Diese Konstellation als Nichteingriff zu bewerten würde die bisherige Rechtsprechung des Bundesverfassungsgerichts ändern.

Auf der zweiten Stufe erfolgt der Eingriff in das Grundrecht aus Art. 10 Abs. 1 GG durch die Regelungen, die einen staatlichen Zugriff auf die auf Vorrat gespeicherten Verkehrsdaten und ihre Verwendung ermöglichen. Die Telekommunikationsunternehmen werden ausdrücklich verpflichtet, die erfassten und gespeicherten Daten den zuständigen staatlichen Stellen auf Ersuchen unverzüglich zur Verfügung zu stellen (§ 113b S. 1 TKG). Aufgrund der §§ 100g, 100a StPO, Art 34b Abs. 2 i. V. m. Art. 34a Abs. 1 Satz 1, Abs. 3 S. 1 BayPAG, Art. 6c BayVSG und § 34 a ThürPAG sowie 113b S. 1 TKG können sich dann zahlreiche staatliche Stellen ohne Wissen und Zustimmung der Beteiligten von den Umständen aller Telekommunikationsvorgänge ein genaues Bild machen.

Der Zugriff auf die umfangreichen Verbindungsdaten erlaubt einen umfassenden Einblick in das Kommunikationsverhalten der Betroffenen, deren Identität feststellbar ist. Auf beiden Stufen greift das Gesetz intensiv in Art. 10 Abs. 1 GG ein. Dabei ermöglicht die Vielzahl der erfassten Daten Rückschlüsse auf Kommunikationsstrukturen, z. T. auch auf den Inhalt der Telekommunikation[88]. Die Bewertung der zahlreichen Standortdaten erlaubt außerdem die Erstellung genauer Bewegungsprofile der Betroffenen.

Damit wird sowohl auf der ersten als auch auf der zweiten Stufe gegen das Fernmeldegeheimnis verstoßen. Wegen der eigenständigen Eingriffsqualität von Speicherung und staatlichem Abruf wird ihre Verfassungswidrigkeit einzeln gerügt.

---

[86] BVerfGE 107, 299 (313).
[87] Vgl. BVerfGE 107, 299 (313).
[88] Vgl. BVerfGE 113, 348 (365).

3. Die anlasslose Erhebung und Speicherung sämtlicher Verbindungsdaten als genereller Verstoß gegen das Fernmeldegeheimnis

Die Regelungen des § 113a TKG verstoßen gegen die Anforderungen, die Art. 10 GG an die Bestimmtheit und Normenklarheit von Eingriffsbefugnissen in den Fernmeldeverkehr stellt.
Des Weiteren sind die Bestimmungen des § 113a TKG unverhältnismäßig und überschreiten die Grenzen der Grundrechtsschranke des Art. 10 GG. Nach dem Grundsatz der Verhältnismäßigkeit müssen Grundrechtseingriffe einen legitimen Zweck verfolgen und geeignet, erforderlich und angemessen sein.

a) Mangelnde Bestimmtheit, Normenklarheit und Verstoß gegen das Gebot der Zweckbindung erhobener Daten

Art. 10 GG verlangt, dass „der Zweck, zu dem Eingriffe in das Fernmeldegeheimnis vorgenommen werden dürfen, bereichsspezifisch und präzise bestimmt werden muss. Eine Sammlung nicht anonymisierter Daten auf Vorrat zu unbestimmten oder nicht bestimmbaren Zwecken wäre damit unvereinbar“ [89] . Diese zur Rechtfertigung eines Eingriffs in das Recht auf informationelle Selbstbestimmung entwickelten Anforderungen, sind bei der Bestimmung des Umfangs des Grundrechtsschutzes durch Art. 10 Abs. 1 GG zu berücksichtigen. Das Bundesverfassungsgericht hat ausdrücklich festgestellt, dass, soweit der Eingriff in das Fernmeldegeheimnis die Erlangung personenbezogener Daten betrifft, die Maßgaben des Volkszählungsurteils grundsätzlich auch auf die spezielle Garantie in Art. 10 Abs. 1 GG zu übertragen sind [90] . Zu den besonderen Anforderungen an den Gesetzgeber, die die Erhebung, Nutzung und Verarbeitung personenbezogener Daten betreffen, gehört u.a., dass die Einschränkungen einer verfassungsmäßigen gesetzlichen Grundlage bedürfen, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muss. Insbesondere muss der Zweck, zu dem Eingriffe in das Fernmeldegeheimnis vorgenommen werden dürfen, bereichsspezifisch und präzise bestimmt werden[91]. Ferner ist das Verhältnismäßigkeitsprinzip besonders zu beachten. Des Weiteren hat das Bundesverfassungsgericht ausdrücklich festgestellt, dass das Grundgesetz eine „globale und pauschale Überwachung“ zu Zwecken der Auslandsaufklärung nicht zulässt [92] . Bei der Strafverfolgungsvorsorge, bei der Gefahrenabwehr und bei der Aufgabenerfüllung der Verfassungsschutzbehörden, des Auslandsnachrichtendienstes und des Militärischen Abschirmdienstes kann dies nicht anders sein.

---

[89] BVerfGE 100, 313 (360).
[90] Vgl. BVerfGE 100, 313 (359); BVerfG, NJW 2006, 976 (980).
[91] BVerfGE 100, 313 (360).
[92] BVerfGE 100, 313 (376).

Die im Gesetz formulierte allgemeine Zweckbestimmung des Gesetz, wonach die Speicherung und die weitere Verarbeitung der Verbindungsdaten der Strafverfolgung, der Gefahrenabwehr und der Aufgabenerfüllung der Nachrichtendienste diene (vgl. § 113b TKG), genügt in dieser Allgemeinheit nicht den verfassungsrechtlichen Anforderungen. Vielmehr wird eine Sammlung personenbezogener Daten auf Vorrat zu noch nicht bestimmbaren Zwecken angelegt. Der damit einhergehende Grundrechtseingriff kann nicht mit dem Verweis gerechtfertigt werden, dass die später zu schaffenden Zugriffsnormen hinreichend präzise Vorgaben enthalten. Diese können allein für die Beurteilung des eigenständigen Grundrechtseingriffs „Abruf der Datensätze" von Bedeutung sein.

Das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG muss daher selbst hinreichend umreißen, unter welchen Voraussetzungen die Informationen verwendet werden dürfen. Die Schaffung eines Datenpools, ohne gleichzeitig Anforderungen bezüglich der Verwendung der Daten aufzustellen, ist unzulässig. Fehlt eine derartige Begrenzung, ließe sich der Verwendungszweck in den jeweiligen Zugriffsnormen der Fachgesetze beliebig bestimmen. Aufgrund dieser Unsicherheit über einen möglicherweise sehr weit gefassten Verwendungszweck wiegt die Eingriffsintensität der Speicherung schwer. Ohne umgrenzende Vorgaben für die Verwendung der Informationen sind die Regelungen nicht verfassungskonform.

Ein Verfassungsverstoß liegt zudem darin, dass ein bestimmter Grad von Tatverdacht nicht gefordert wird. In einer freiheitlichen Demokratie darf eine umfangreiche Datenerfassung nur im Verdachtsfall erfolgen. Der Staat darf nicht jeden Bürger vorsorglich als potenziellen Verbrecher behandeln. Eine vorsorgliche Überwachung für künftige Strafverfolgungsmaßnahmen ist bisher an das Vorhandensein einer konkreten Gefahrenlage oder einer negativen Kriminalprognose der betroffenen Personen gebunden[93]. Grundrechtseingreifende Maßnahmen „ins Blaue hinein" sind unzulässig[94]. Mit einer anlass- und verdachtslosen Speicherung sämtlicher Verbindungsdaten würde praktisch allen Benutzerinnen und Benutzern elektronischer Telekommunikationsmittel unterstellt, sie könnten in der Zukunft zum Objekt staatlicher Strafverfolgung werden. Vor diesem Hintergrund erscheint es aus verfassungsrechtlicher Sicht äußerst bedenklich, dass Daten, die ansonsten nicht vorliegen würden, zu allgemeinen Sicherheitszwecken gespeichert werden sollen. Eine derartige umfassende Speicherung zur verdachtslosen „vorbeugenden Verbrechensbekämpfung" bzw. „Strafverfolgungsvorsorge" verstößt gegen die Anforderungen an die Bestimmtheit. Die vollumfängliche Speicherung aller Telekommunikationsvorgänge ist aufgrund ihrer Streubreite und Verdachtsunabhängigkeit verfassungskonformer Auslegung aus ihrer Natur heraus nicht zugänglich.

---

[93] BVerwGE 1 C 57.66 vom 09.02.1967.
[94] BVerfGE 112, 284 (297).

b) Mangelnde Geeignetheit der angegriffenen Rechtsnormen

Unabhängig von der Frage nach der Legitimität des Zwecks der Regelungen zur Speicherungspflicht fehlt es an ihrer Geeignetheit zur Erreichung der genannten Ziele. Zweifel an der Geeignetheit ergeben sich schon daraus, dass Kriminelle oder Terroristen mit relativ einfachen Mitteln die Überwachungsmaßnahmen unterlaufen können. Dazu bräuchten die Betroffenen lediglich ihre Kommunikationsgeräte über Dritte erwerben oder auf öffentliche Kommunikationsmittel – wie Internetcafés, Straßentelefonzellen, Mailkonten außerhalb der EU und den USA oder vorausbezahlte international einsetzbare SIM-Karten – zurückgreifen[95]. Darüber hinaus muss auch die Möglichkeit berücksichtigt werden, Anonymisierungsdienste einzusetzen. Die Methoden einer anonymen Nutzung der Telekommunikation werden eher besonders gefährliche Straftäter als Kleinkriminelle oder gar Unbeteiligte gebrauchen. Für die Verfolgung besonders schwerer Straftaten erscheint die Speicherung von Vorratsdaten daher wenig geeignet, da die eigentliche „Zielgruppe" der Maßnahme sich ihr entziehen wird. Wenn die vorhandenen Verbindungsdaten keiner Person eindeutig zugeordnet werden können, dann ist ihre Verwertbarkeit bei einer strafrechtlichen Ermittlung oder bei Maßnahmen zur Gefahrenabwehr sehr gering. Auch eine erhebliche gesetzliche Beschränkung oder ein Verbot von Anonymisierungsdiensten, worauf das Umsetzungsgesetz praktisch abzielt, könnte daran nichts ändern, da sich die anonyme Nutzung von Telekommunikationsnetzen technisch kaum verhindern lässt[96].

Die mangelnde Geeignetheit der Vorratsdatenspeicherung zeigt sich besonders deutlich im Internetbereich. So ist es beispielsweise möglich, mit Einsatz von sogenannten Proxy-Servern mit einem geringen Aufwand „die tatsächliche IP-Adresse schon während der Telekommunikation mit der Folge zu ändern, dass an einer IP-Adresse ansetzende Ermittlungsmaßnahmen ins Leere gingen"[97].

Die vorhandenen empirischen Angaben lassen ebenfalls Zweifel daran entstehen, ob die Vorratsdatenspeicherung in einem großen Maße zur Verbesserung der Strafverfolgung beitragen kann. In der Praxis scheitern demnach nur wenige Ermittlungsverfahren an Telekommunikationsverkehrsdaten, zumal die Strafverfolgungsbehörden oft nur an den Bestandsdaten interessiert sind[98]. Nach einem Gutachten des Freiburger Max-Planck-Institutes für ausländisches und internationales Strafrecht kann eine über die heutigen rechtlichen Bedingungen

---

[95] Vgl. *Wissenschaftliche Dienste des Deutschen Bundestages*, Gutachten 282/06, S. 13. Ausführlich zu den technischen Umgehungsmöglichkeiten bei den verschiedenen Telekommunikationsdiensten *Breyer*, Die systematische Aufzeichnung und Vorhaltung von Telekommunikations-Verkehrsdaten für staatliche Zwecke in Deutschland, Berlin 2005, S. 14f.

[96] Vgl. dazu *Breyer*, Die systematische Aufzeichnung und Vorhaltung von Telekommunikations-Verkehrsdaten für staatliche Zwecke in Deutschland, Berlin 2005, S. 189.

[97] Stellungnahme von BITKOM, Rechtsausschuss des Deutschen Bundestages, Zusammenfassung der Stellungnahmen zur öffentlichen Anhörung am 21. September 2007, S. 117.

[98] Ausführlich dazu *Breyer*, Die systematische Aufzeichnung und Vorhaltung von Telekommunikations-Verkehrsdaten für staatliche Zwecke in Deutschland, Berlin 2005, S. 188f. und *Büllingen*, DuD 2005, S. 349 (351, 353).

hinaus gehende gesetzliche Regelung der Speicherung von Verbindungsdaten die Aufklärungsquote bei der Strafverfolgung nicht erhöhen[99].

Äußerst zweifelhaft ist außerdem, ob die bezweckte Vorratsdatenspeicherung sowie die Auswertung der zu speichernden Daten wegen des enormen Volumens der zu speichernden Daten technisch durchführbar ist. Zahlreiche Daten aus dem Katalog von § 133a Abs. 1 bis 5 TKG sind technisch gar nicht erfassbar[100]. Dazu kommt, dass viele von den geplanten Maßnahmen bzw. der zu speichernden Daten wie etwa die IMEI-Speicherung oder die Protokollierung der IP-Adressen leicht zu unterlaufen bzw. manipulierbar sind[101]. Es ist außerdem allgemein bekannt, dass sich viele elektronische Spuren ohne großen Aufwand fälschen lassen. Dabei besteht eine erhöhte Gefahr, dass Unschuldige in Verdacht geraten. Die Speicherungsmaßnahmen sind daher hinsichtlich der Strafverfolgung sogar kontraproduktiv.

All dies lässt die in § 113a Abs. 1 bis 5 TKG geregelte Vorratsdatenspeicherung ungeeignet erscheinen, die Strafverfolgung sowie die Aufgabenerfüllung der Verfassungsschutzämter und der Nachrichtendienste zu fördern.

c) Mangelnde Erforderlichkeit der angegriffenen Rechtsnormen

Erhebliche Bedenken bestehen auch hinsichtlich der Erforderlichkeit der vorgesehenen Vorratsdatenspeicherung zur Terrorismus- und Verbrechensbekämpfung. Mit dem sogenannten „Quick-freeze-Verfahren" oder „Data Preservation", das u.a. in den USA praktiziert wird, steht ein milderes Mittel zur Verfügung, durch das die Ziele des Gesetzgebers zu erreichen wären[102]. Dabei werden die Daten einer verdächtigen Person nach der Aufforderung durch die Strafverfolgungsorgane ab sofort gespeichert, der Zugriff auf diese Daten ist dann nach Erlass einer richterlichen Anordnung möglich. Damit wäre die Speicherung von Verbindungsdaten auf konkrete Verdachtsfälle beschränkt, ohne die Wirksamkeit der Strafverfolgung zu beeinträchtigen.

Erhebliche Zweifel bestehen insbesondere an der Notwendigkeit der Speicherungsdauer von sechs Monaten. Erfahrungsgemäß betreffen die Zugriffe der berechtigten Behörden in ähnlichen Konstellationen fast ausschließlich die ersten drei Monate der Speicherung[103]. Unter dem Gesichtspunkt der Erforderlichkeit wäre daher eine dreimonatige Speicherfrist hinreichend[104]. Laut eines Gutachtens des Freiburger Max-Planck-Instituts für ausländisches und internationales Strafrecht zur „Rechtswirklichkeit der Auskunftserteilung über

---

[99] Albrecht, Hans-Jörg; Grafe, Adina; Kilchling, Michael, „Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO", Freiburg i.Br, Februar 2008.

[100] Stellungnahme des VATM, Rechtsausschuss des Deutschen Bundestages, Zusammenfassung der Stellungnahmen zur öffentlichen Anhörung am 21. September 2007, S. 81 und 83.

[101] Stellungnahme von BITKOM, Rechtsausschuss des Deutschen Bundestages, Zusammenfassung der Stellungnahmen zur öffentlichen Anhörung am 21. September 2007, S. 105 und 120.

[102] Zum sogenannten „Quick-freeze-Verfahren" vgl. *Büllingen*, DuD 2005, S. 349 (350).

[103] Vgl. dazu *Westphal*, EuZW 2006, S. 555 (558).

Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO" gehen unter den heutigen rechtlichen Bedingungen nur etwa 2% der Abfragen wegen Löschungen ins Leere[105].

d) Mangelnde Angemessenheit der Regelungen zur Vorratsdatenspeicherung

Es fehlt schließlich auch an der Angemessenheit der angegriffenen Regelungen. Grundrechtseingriffe dürfen die Betroffenen nicht übermäßig belasten, d.h. bei einer Gesamtabwägung zwischen der Schwere des Eingriffs und dem Gewicht der ihn rechtfertigenden Gründe muss die Grenze der Zumutbarkeit gewahrt bleiben. Dies ist weder bezüglich der von der Vorratsdatenspeicherung betroffenen Personen noch hinsichtlich des Katalogs der zu speichernden Daten der Fall. Die Vorratsspeicherung der Telekommunikationsverbindungsdaten sämtlicher Nutzer bringt zudem erhebliche Missbrauchsgefahren mit sich. Ebenfalls zu berücksichtigen sind die negativen gesamtgesellschaftlichen Auswirkungen der Einführung der Vorratsdatenspeicherung.

(1) Die von der Vorratsdatenspeicherung erfassten Personen

Eine Unterscheidung der betroffenen Personen, deren Daten auf Vorrat gespeichert werden sollen, ist im Gesetz nicht enthalten. Es fehlt jegliche Differenzierung nach fahndungsrelevanten Personengruppen, vielmehr sollen die Daten aller Telekommunikationsteilnehmer gleichermaßen gespeichert werden. Das gesamte Kommunikationsverhalten der Beschwerdeführer wird aufgezeichnet, ohne dass hierfür ein gesetzwidriges Verhalten vorausgesetzt wird.

Dass jegliche Unterscheidung zwischen Tatverdächtigen, Kontaktpersonen und völlig unbeteiligten Bürgern unterbleibt ist nicht angemessen. Im Ergebnis wird damit pauschal die gesamte Ebene der Speicherung bzw. Nichtspeicherung einer zukünftigen rechtsstaatlichen Gestaltung entzogen. Es zeichnet sich ein überwachungsstaatliches Szenario ab, bei dem zukünftig über einzelne Zugriffe seitens bestimmter Institutionen verhandelt werden wird. Die grundlegende Frage der staatlichen Verfügbarkeit der Daten ist dann dem Streit entzogen. Eine derartige Regelung ist mit den verfassungsfesten Schutzkonzeptionen von Art. 10 GG unvereinbar.

---

[104] Allerdings würde die Umsetzung sich damit gegen die minimale Speicherungsfrist aus Art. 6 der Richtlinie 2006/24/EG wenden.

[105] Gutachten des Max-Planck-Instituts für ausländisches und internationales Strafrecht zur „Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO", S. 407. Im Rahmen der 2005 erfolgten Verabschiedung des Gesetzes zur Verlängerung der Geltungsdauer der §§ 110g, 100h StPO hatte der Deutsche Bundestag die Bundesregierung zur Vorlage eines entsprechendes Berichts aufgefordert. Das BMJ hatte das MPI mit der Erstellung des Gutachtens beauftragt. Obwohl das Gutachten der Bundesregierung vorlag, wurde dem Bundestag vor der Verabschiedung des hiermit angegriffenen Gesetzes lediglich eine vierseitige Zusammenfassung der Ergebnisse des Gutachtens zur Verfügung gestellt.

Die Regelungen des § 113a TKG stehen damit im Gegensatz zu wichtigen verfassungsrechtlichen Grundsätzen des Datenschutzes[106]. Durch die Vorratsdatenspeicherung werden Strukturprinzipien wie Datensparsamkeit, Datenvermeidung und Zweckbindungsgebot als Ausfluss des Verhältnismäßigkeitsprinzips ausgehöhlt. Die Erhebung, die Aufzeichnung und die Aufbewahrung der Telekommunikationsverbindungsdaten erfolgen unabhängig von einem im Einzelfall bestehenden Tatverdacht. Es werden alle Kommunikationsvorgänge sämtlicher Kommunikationsteilnehmer auf Vorrat gespeichert. Wenn es einerseits „kein belangloses Datum"[107] mehr gibt und die Vorratsdatenspeicherung andererseits ermöglicht, dass praktisch alle Verkehrs- und Standortdaten von allen Telekommunikationsteilnehmern gespeichert werden, dann liegt die Verfassungswidrigkeit der jeweiligen Vorschriften auf der Hand.

Im „IMSI-Catcher"-Beschluss hat das Bundesverfassungsgericht in Zusammenhang mit der bevorstehenden Gesamtregelung der strafprozessualen heimlichen Ermittlungsmaßnahmen darauf hingewiesen, dass zu prüfen ist, „ob und in welchem Umfang von einer neuerlichen Ausdehnung heimlicher Ermittlungsmethoden im Hinblick auf Grundrechtspositionen unbeteiligter Dritter Abstand zu nehmen ist"[108]. Die hiermit angegriffenen Regelungen berücksichtigen diese Forderung nicht.

(2) Liste der zu speichernden Daten: erhebliche Beeinträchtigung der individuellen Kommunikationsfreiheit und geringer praktischer Nutzwert

Eng mit den Vorschriften, die den Adressatenkreis der Speicherungspflicht regeln, sind die Normen verbunden, die die zu speichernden Daten festlegen. Der Umfang der zu speichernden Daten (§ 113a Abs. 2 bis 5 TKG) ist im Verhältnis zu dem Nutzen dieser Daten für die Strafverfolgung und Gefahrenabwehr nicht angemessen. Dies betrifft beispielsweise die Pflicht zur Speicherung der ersten Aktivierung des jeweiligen Dienstes bei vorausbezahlten Diensten wie beispielsweise Prepaid-SIM-Karten oder Flatrate-Tarifen für den Internetzugang (§ 113a Abs. 2 Nr. 4 d) TKG), die Pflicht zur Speicherung erfolgloser Anrufsversuche (§ 113a Abs. 5 TKG)[109], die Speicherung aller zur Identifizierung erforderlichen feststehenden sowie dynamischen Kennungen der Geräte sowie Verbindungsvorgänge, die Speicherungspflicht der Anbieter von E-Mail-Diensten bezüglich jedes Zugriffs auf das elektronische Postfach oder jedes Versands oder Empfangens von E-Mail (§ 113a Abs. 3 Nr. 3 TKG), die vollständige Verknüpfung der eben genannten Daten mit Datum und Uhrzeit der Verbindung sowie den Aufenthaltsorten der Teilnehmer (Standortdaten), das

---

[106] BVerfGE, 65, 1 (44, 46).
[107] BVerfGE, 65, 1 (45).
[108] BVerfGE 2 BvR 1345/03 („IMSI-Catcher"), Rn. 84.
[109] Daten in Zusammenhang mit erfolglosen Anrufversuchen (vgl. Art. 2 Abs. 2 f RL 2006/24/EG) müssen gespeichert werden, wenn sie von den Anbietern im Zuge der Bereitstellung von Kommunikationsdiensten oder zu Rechnungszwecken erzeugt und verarbeitet werden (vgl. Art. 3 Abs. 2 und Erwägungsgrund 12 der RL 2006/24/EG; § 113a Abs. 5 TKG). Zu kritisieren ist dabei, dass auf diese Weise dem Angerufenen erschwert wird, sich einer Speicherung zu entziehen, auch

praktische Verbot der Anonymisierungsdienste[110] sowie die Angaben über die Hauptstrahlrichtung der Funkantennen beim Mobilfunk (§ 113a Abs. 7 TKG). Damit wird jede elektronische Kommunikation – sei sie auch bloß versucht – erfasst und jede Bewegung mit Datum, Uhrzeit, Ort, Ortsveränderung und Teilnehmern nachvollziehbar. Der geringe praktische Nutzwert all dieser Daten kann den Grundrechtseingriff durch ihre vorrätige Speicherung nicht rechtfertigen. Mit der Speicherung der Kennung eines ankommenden Anrufs (§ 113a Abs. 2 Nr. 1 TKG) wird die bisherige, umstrittene „Zielwahlsuche" teilweise entbehrlich. Für jedes Benutzerkonto werden künftig nicht nur alle ausgehenden, sondern auch alle ankommenden Verbindungen gespeichert. Die Speicherung aller Verbindungsdaten sowohl beim Sender als auch beim Empfänger zeigt einmal mehr, wie umfassend die Vorratsdatenspeicherung von Verkehrsdaten ist und mit welcher Intensität sie in die Grundrechte eingreift[111].

Nach § 113a Abs. 2 Nr. 4 Buchst. c TKG sind die Standortdaten des anrufenden und des angerufenen Anschlusses bei Beginn der Verbindung zu speichern. Da ein betriebsbereites Mobiltelefon in geringen zeitlichen Abständen Signale an die nächststehende Funkzelle sendet, kann der Standort des Apparats bzw. seines Nutzers relativ genau bestimmt werden[112]. Durch die Möglichkeit der Ortung eines eingeschalteten Mobiltelefons können genaue Bewegungsprofile erstellt werden. Die Tatsache, dass die Speicherung der Standortdaten durch die Telekommunikationsunternehmen nur beim Beginn der Verbindung erfolgt, ändert daran nichts, denn § 100g Abs. 1 S. 3 StPO soll künftig die Erhebung von Standortdaten durch die Strafverfolgungsbehörden in Echtzeit ermöglichen, auch wenn das Mobiltelefon gerade nicht genutzt wird[113]. Damit würde das eingeschaltete Mobiltelefon „zu einer Art ungewolltem Peilsender"[114], der die Bewegung seines Nutzers meldet. Somit wird auch die aus verfassungsrechtlicher Sicht äußerst bedenkliche Ermittlungsmethode des so genannten „stillen SMS" de facto legalisiert[115].

Diese Maßnahmen beeinträchtigen die individuelle Kommunikationsfreiheit der Beschwerdeführer erheblich, da sie zwangsläufig zu Anpassungen ihres Kommunikationsverhaltens führen. Sie sind auch deswegen nicht angemessen, weil der Aufwand für ihre Erfassung und ihr Nutzen für die Strafverfolgung in keinem Verhältnis stehen. Nach einer offiziell nicht veröffentlichten Studie des BKA blieben 2005 nur 381 Fälle wegen fehlender Kommunikationsdaten ungeklärt. Dabei betrafen lediglich zwei Fälle den Bereich der organisierten Kriminalität[116].

---

wenn er absichtlich einen Kommunikationsvorgang ablehnt und z. B. nicht ans Telefon geht. Dass dies das Risiko stark erhöht, in unbegründeten Verdacht zu geraten, liegt auf der Hand.

[110] Vgl. dazu die Ausführungen unter C. 2. c).

[111] Die Ausführungen in der Begründung des Gesetzentwurfs, wonach die Zielwahlsuche „entfällt" (BTDrs. 16/5846, Begründung zum Regierungsentwurf, S. 54), sind hier irreführend. Kritisch dazu Zoller, Goltdammer's Archiv für Strafrecht (GA) 2007, S. 393 (397f.).

[112] Um eine genauere Ermittlung des Standortes eines Mobiltelefons zu ermöglichen, verpflichtet § 113a Abs. 7 TKG die Anbieter zur Angabe der geografischen Lage der jeweiligen Funkzelle sowie der Hauptstrahlrichtung der Funkantennen.

[113] BTDrs. 16/5846, Begründung zum Regierungsentwurf, S. 51.

[114] Zöller, CILIP 85 (3/2006), S. 21 (26).

[115] BTDrs. 16/5846, Begründung zum Regierungsentwurf, S. 51.

[116] BKA, Mindestspeicherungsfristen für Telekommunikationsverkehrsdaten, 15.11.2005.

Entsprechend den Vorgaben der Richtlinie (Art. 5 Abs. 2 RL) sieht § 113a Abs. 8 TKG generell vor, dass keine Daten über aufgerufene Internetseiten sowie keine Daten gespeichert werden dürfen, die Aufschluss über den Inhalt der Kommunikation geben[117]. Hierzu ist aber zum einen zu bemerken, dass eine Trennung zwischen Inhaltsdaten und „reinen" Verbindungsdaten in vielen Fällen technisch kaum erfolgreich vorgenommen werden kann. Insbesondere bei E-Mail und SMS wird diese Trennung sehr schwierig sein, weil beide Dienste diese Daten auf Protokollebene vermischen[118].

Zum anderen können auf Grund einer umfangreichen Sammlung von Verkehrs-, Standort- und Bestandsdaten Kommunikationsinhalte durchaus nachgebildet werden. Nach § 113a Abs. 4 Nr. 1 TKG werden die den Nutzern für jede Internetsitzung zugewiesenen dynamischen und statischen IP-Adressen gespeichert. Bei entsprechenden Auswertungen auf Grund beschlagnahmter Webserver könnten die darauf erfassten URLs mit den IP-Adressen abgeglichen werden und Kenntnisse über die Kommunikationsinhalte einzelner Nutzer gewonnen werden. Mit Hilfe technischer Analysen der Verkehrsdaten lassen sich daraus detaillierte Informationen über soziale Netzwerke, Freundeskreise, persönliche Präferenzen etc. gewinnen sowie speziell im Internetbereich Profile über einzelne Nutzer erstellen. Aus der Dauer eines http-Aufrufs eines Webservers kann geschlossen werden, welche Teile einer Internetseite bzw. eines Online-Angebotes die Nutzerin oder der Nutzer in Anspruch genommen hat[119]. Studien von Forschern des Massachusetts Institute of Technology (MIT)[120] sowie der Erasmus-Universität Rotterdam[121] weisen nach, dass allein die Analyse der äußeren Umstände der Kommunikation bereits weitgehende Erkenntnisse über dessen Inhalte liefern. Die so zu gewinnenden Erkenntnisse gehen weit über das Sichtbarmachen von Strukturen hinaus. Sie betreffen persönliche Aktivitäten des Einzelnen bis hin zu seinen Empfindungen.[122] Die Verbindungsdaten lassen damit die Inhalte der Verbindung gleichsam „durchscheinen". Damit behindert eine Speicherung sämtlicher Daten erheblich die unbefangene Nutzung des Internets. Die Beschwerdeführer haben zu befürchten, dass ihr Nutzungsverhalten aufgezeichnet und später in einer möglicherweise völlig anderen Konstellation ausgewertet wird.

Dabei ist insbesondere zu berücksichtigen, dass die weitgehenden technischen Möglichkeiten einer automatischen Verarbeitung von Verkehrsdaten deren längerfristige Speicherung und Auswertung zu einem ähnlich intensiven Grundrechtseingriff werden lassen, wie die Speicherung von Kommunikationsinhalten. Das Bundesverfassungsgericht hat schon im Volkszählungsurteil betont, dass es bei der Bemessung der Intensität eines Grundrechtseingriffs nicht allein auf die Art der

---

[117] Für den Internetbereich dürfte dies bedeuten, dass z.B. URLs, FTP-Transfers sowie Chats nicht gespeichert werden müssen, da es sich dabei um Inhaltsdaten handelt.

[118] Vgl. www.heise.de/ct/hintergrund/meldung/69995.

[119] Vgl. www.heise.de/newsticker/meldung/83054.

[120] Eagle, Nathan; Pentland, Lazer, Alex; Lazer David (2007): Inferring Social Network Structure using Mobile Phone Data. Science Report. Online: http://www.socialsciences.cornell.edu/0508/sciencereport_formatted_10.12.pdf. Ausführliche Informationen zur Arbeit der Human Dynamics Group am MIT unter: http://reality.media.mit.edu/.

[121] Danezis, George und Wittneben, Bettina (2006): The Economics of Mass Surveillance and the Questionable Value of Anonymous Communications. K.U. Leuven, ESAT/COSIC, RSM Erasmus University, Rotterdam. Online: http://weis2006.econinfosec.org/docs/36.pdf.

Angaben, sondern auf ihre Nutzbarkeit und Verwendungsmöglichkeit ankommt [123] . Indem Verkehrsdaten in digitalisierter, standardisierter Form erfasst werden, bestehen für sie ungleich mehr Möglichkeiten ihrer automatisierten Auswertung und Verarbeitung als bei Inhaltsdaten. Der Nutzen von Inhaltsdaten ist zudem sehr eingeschränkt, wenn sie keiner konkreten Person zugeordnet werden können, was aber auf Grund der Verkehrsdaten möglich wird. Daher ist die Behauptung, der durch die Vorratsdatenspeicherung erfolgende Grundrechtseingriff sei geringer einzustufen, weil es sich dabei „nur" um Verkehrsdaten handele, in ihrer Pauschalität irreführend[124].

Nach alledem ist festzuhalten, dass die Pflicht zur Speicherung und Aufbewahrung der in § 113a Abs. 2 bis 5 TKG aufgelisteten Daten zu einer sehr umfangreichen Sammlung von sensiblen personenbezogenen Daten führt.

Die Beschwerdeführer haben zu befürchten, dass auf deren Grundlage umfassende Kommunikations- und Bewegungsprofile jedes Nutzers von Telekommunikationsdiensten erstellt werden können. Der erwartete Nutzen für die Verbesserung der Strafverfolgung ist im Vergleich zur Intensität der Beeinträchtigung der Kommunikationsfreiheit und der Privatsphäre der Beschwerdeführer, aber auch sämtlicher Kommunikationsnutzer, verhältnismäßig gering. Die entsprechenden Regelungen im angegriffenen Gesetz verstoßen daher gegen den Verhältnismäßigkeitsgrundsatz und verletzen das Grundrecht der Beschwerdeführer auf vertrauliche Telekommunikation.

(3) Missbrauchsgefahr durch Private

Die massenhafte Speicherung von Verkehrs- und Standortdaten erhöht das Risiko eines Datenmissbrauchs. Sobald die Datensammlungen einmal vorhanden sind, werden staatlicherseits als auch von Privaten zunehmende Versuchungen bestehen, diese Daten für andere Zwecke zu nutzen oder die Daten an andere Interessenten zu übermitteln. Die im § 113a Abs. 10 S. 2 TKG vorgesehene Verpflichtung für die Telekommunikationsanbieter, durch technische und organisatorische Maßnahmen sicherzustellen, dass der Zugang zu den gespeicherten Daten ausschließlich hierzu besonders ermächtigten Personen möglich ist, kann den Missbrauchsgefahren nicht erfolgreich begegnen. Wie diese Maßnahmen konkret aussehen sollen und welche diese „besonders ermächtigten" Personen sein sollen, wird nicht geregelt und bleibt offensichtlich im freien Ermessen der verpflichteten Telekommunikationsdiensteanbieter. Für die Benutzerinnen und Benutzer der Dienste bleibt ein nicht geringes Risiko eines unberechtigten Zugriffs durch die

---

[122] Vgl. Eagle, Nathan; Pentland, Lazer, Alex; Lazer David (2007): Inferring Social Network Structure using Mobile Phone Data. Science Report.

[123] BVerfGE 65, 1 (45).

[124] Ausführlich dazu *Breyer*, Die systematische Aufzeichnung und Vorhaltung von Telekommunikations-Verkehrsdaten für staatliche Zwecke in Deutschland, Berlin 2005, S. 213f.

Mitarbeiter der Telekommunikationsunternehmen bestehen[125]. Die Tatsache, dass die Speicherung automatisch, also ohne jede Kenntnisnahme durch Personen erfolgen soll, kann dieses Risiko nicht mindern. Technische Fehler führten bereits mehrfach zur Offenlegung von zahlreichen Kundendaten, die plötzlich im Internet zugänglich waren. Wenn aber sensible personenbezogene Daten auch nur für kurze Zeit allgemein zugänglich sind, können sich die Betroffenen gegen einen potenziellen Missbrauch ihrer Verbindungsdaten kaum mehr schützen. Dafür, dass ein solcher Missbrauch keinesfalls nur theoretisch denkbar ist, existieren zahlreiche Beispiele, etwa für den unberechtigten Zugriff auf Telekommunikationsdaten von unbefugten Hackern und einzelnen Unternehmensmitarbeitern oder für den Verkauf solcher Daten an andere Unternehmen. Die sogenannte „Telefonüberwachungsaffäre", die 2006 in Italien für Schlagzeilen sorgte, und das im November 2007 bekannt gewordene Verschwinden von Datenträgern mit den personenbezogenen Daten von Millionen Menschen in England sind markante Beispiele solcher Missbrauchsgefahren.

Wegen des hohen kommerziellen Werts der Verkehrsdaten ist auch nicht auszuschließen, dass die zur Speicherung Verpflichteten selbst gern die gesammelten Daten anderweitig als im Gesetz vorgesehen nutzen würden [126]. Auf diese Weise könnte die Vorratsdatenspeicherung zu kontraproduktiven Effekten bei der Verbrechensbekämpfung führen, weil sie das Begehen bestimmter Straftaten erleichtern würde[127]. Ein wirksames präventives Datenschutzmanagement erscheint daher im behandelten Zusammenhang zwingend geboten. Das hiermit angegriffene Gesetz enthält allerdings keine Vorkehrungen, die dieses gewährleisten können. Es müsste als Mindestanforderungen die Einrichtung unabhängiger Kontrollstellen vorsehen. Diese müssten befugt sein regelmäßig die Datensicherheit bei der „Lagerung", Zugriff und Weitergabe vor Ort zu überprüfen. Zu ihrer Wirksamkeit bedürfen diese Stellen eines eigenen Sanktionsrechts. Die Aufsicht über das Datenschutzmanagement allein einer vom Telekommunikationsdiensteanbieter zu bestimmenden Person zu überlassen ist nicht ausreichend. Die Aufgabe des Schutzes der sensiblen Daten, die nur um des Staates Willen erhoben werden, kann nicht allein Privaten übertragen werden sondern bleibt in der Verantwortung des Staates. Um diese Sicherheit gewährleisten zu können, muss er substantiellen Einfluss behalten.

(4) Antastung des Wesensgehalts des Grundrechts auf vertrauliche Telekommunikation

---

[125] Zur ähnlichen Problematik der derzeit nach § 110 TKG einzurichtenden Überwachungsschnittstellen vgl. *Breyer*, Die systematische Aufzeichnung und Vorhaltung von Telekommunikations-Verkehrsdaten für staatliche Zwecke in Deutschland, Berlin 2005, S. 228.

[126] Vgl. für entsprechende Beispiele *Breyer*, Die systematische Aufzeichnung und Vorhaltung von Telekommunikations-Verkehrsdaten für staatliche Zwecke in Deutschland, Berlin 2005, S. 231.

[127] Diesbezüglich ist zu bemerken, dass dem Grundgesetz eine Schutzpflicht des Staates zu entnehmen ist, in solchen sensiblen Bereichen wie dem Umgang mit personenbezogenen Daten vor Beeinträchtigungen durch Private zu schützen oder sie mindestens nicht zu erleichtern. Dementsprechend bestehen Regelungen, die die Erfüllung dieser Schutzpflicht sichern (vgl. z. B. § 88 Abs. 2 TKG, wonach die Telekommunikationsdiensteanbieter zum Schutz des Fernmeldegeheimnisses verpflichtet sind). Mit dem vorliegenden Gesetz wird aber dieser Schutzpflicht keinesfalls Genüge getan.

Mit der umfangreichen anlasslosen Speicherung sensibler Verkehrs- und Standortdaten und den damit verbundenen Gefahren kommt es dazu, dass kaum ein Telekommunikationsvorgang bleibt, der dem staatlichen Zugriff entzogen ist. Eine freie und unbefangene Telekommunikation ist unter diesen Umständen nicht mehr möglich. In der Phase der Datenspeicherung wird die Aufzeichnung des Fernmeldeverkehrs weder rechtlich noch tatsächlich begrenzt. Die Tatsache, dass „nur" Verbindungsdaten gespeichert und verwendet werden, ändert daran nichts. Denn zum einen ist die Trennung zwischen Verkehrs- und Inhaltsdaten, insbesondere bei der Internetnutzung, schwer vorzunehmen. Zum anderen ist die Zahl und die Art der zu erhebenden Daten so umfangreich, dass es leicht möglich ist, durch ihren Abgleich und ihre Bewertung Schlüsse auch über den Inhalt der einzelnen Kommunikationsvorgänge bzw. des gesamten Kommunikationsverhaltens jeder Person zu ziehen. Der einzige Ausweg der Beschwerdeführer als Betroffene wäre es, auf die Nutzung von modernen Kommunikationsmitteln überhaupt zu verzichten.

Die Vielzahl der erfassten Daten und der betroffenen Personen sowie das hohe Missbrauchsrisiko führen zu einer besonderen Intensität des Eingriffs in das Fernmeldegeheimnis, sodass auch der Wesensgehalt des Grundrechts angetastet wird (Art. 19 Abs. 2 GG)[128]. Daher erscheinen die Gesetzesnormen, die die Vorratsdatenspeicherung regeln, auch unter diesem Gesichtspunkt, verfassungswidrig.

(5) Berührung des Kernbereichs der privaten Lebensgestaltung

Das Bundesverfassungsgericht hat anerkannt, dass zur Unantastbarkeit der Menschenwürde gemäß Art. 1 Abs. 1 GG die Anerkennung eines absolut geschützten Kernbereichs privater Lebensgestaltung gehört[129]. Auch im Telekommunikationsbereich fordert es einen ausreichenden einfachgesetzlichen Schutz des Kernbereichs[130]. Diese Forderung bezieht sich zwar im konkreten Fall auf den Kommunikationsinhalt.

Kommunikationsmittel dienen der Nutzung von Beratungsangeboten um anonym Verständnis und Hilfe in schwierigen Lebenssituationen zu erhalten. Dazu tragen nicht allein die telefonische Beratung und Seelsorge, beispielsweise im kirchlichen Bereich, des Kindernotdienstes, der Sucht- und Schuldnerberatung, bei. Auch Internetforen bieten Plattformen des Austauschs und der Hilfe zu den intimsten Lebensbereichen, wie z.B. der sexuellen Orientierung, der politischen Einstellung aber auch aller denkbaren anderen Themenbereiche. Die Beschäftigung mit diesen Inhalten würde durch die Speicherung der Zugriffe offenbar werden. Aus der Dauer und Häufigkeit und der Natur der Verbindung, aus der Tageszeit und dem Ort der Anwahl lassen sich Ansichten und Empfindungen höchstpersönlicher Art sowie intimste Beziehungen leicht rekonstruieren.

---

[128] Vgl. BVerfGE 100, 313 (376).

[129] BVerfGE 109, 279.

[130] Vgl. BVerfGE, NJW 2005, S. 2603 (2611). Mehr dazu, dass die Schaffung kernbereichsschützender Vorschriften auch für Eingriffe in Art. 10 Abs. 1 GG vor dem Hintergrund der neuen Rechtsprechung des Bundesverfassungsgerichts unabweisbar ist, vgl. Kutscha, NJW 2005, S. 20f.

Die Gefahr, dass derartige höchstpersönliche Angelegenheiten sichtbar werden, steigt durch die völlige Durchleuchtung des gesamten Kommunikationsverhaltens einer unbegrenzten Personenzahl. So können Daten aus den verschiedensten Lebensbereichen eines Menschen zusammengeführt werden. Dies ergibt zumindest in der Gesamtheit ein Bild des Einzelnen, das geeignet ist, seine Persönlichkeit zu erfassen.

Die so erfolgende Verletzung des Kernbereichs der Privatheit kann durch die Regelungen des § 113a Abs. 8 TKG nicht vermieden werden. Demnach dürfen Daten, die Aufschluss über den Inhalt der Kommunikation geben, nicht gespeichert werden. Diese Norm hat lediglich deklarativen Charakter und sie ist technisch kaum durchführbar.

Durch das Anhäufen umfangreicher Kommunikationsdaten (vgl. § 113a Abs. 2 bis 5 TKG) werden Schlüsse über den Kommunikationsinhalt ermöglicht. Die Speicherung der Daten soll automatisch erfolgen, sodass eine entsprechende Einschätzung, welche Informationen erlangt werden, im Voraus nicht möglich ist.

Vor diesem Hintergrund erscheint die Schaffung besonderer Regelungen für einen wirkungsvollen Schutz des unantastbaren Kernbereichs persönlicher Lebensgestaltung bei der Speicherung und Verwendung von Verkehrsdaten geboten. Entsprechende Normen fehlen aber im verabschiedeten Gesetz[131].

(6) Gesamtgesellschaftliche Auswirkungen: Vorratsdatenspeicherung und Freiheit der öffentlichen Meinungsbildung

Die Problematik der Vorratsdatenspeicherung hat auch eine gesamtgesellschaftliche Dimension, die im Rahmen der Verhältnismäßigkeitsprüfung zu berücksichtigen ist. In diesem Zusammenhang führt das Bundesverfassungsgericht treffend aus: „Ein von der Grundrechtsausübung abschreckender Effekt fremden (Geheim)wissens muss nicht nur im Interesse der betroffenen Einzelnen vermieden werden. Auch das Gemeinwohl wird hierdurch beeinträchtigt, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger gegründeten freiheitlichen demokratischen Gemeinwesens ist“[132]. Die Mitwirkung möglichst vieler Teilnehmer an der öffentlichen Auseinandersetzung ist also ein Wesenselement der modernen Demokratie. In der Mediengesellschaft erfolgt diese Auseinandersetzung in immer größerem Maße über verschiedene Kommunikationsmittel. Wenn der Einzelne weiß, dass jeder Kommunikationsvorgang beobachtet und gespeichert wird, entstehen psychische Hemmungen, die zwangsläufig zu einer erheblichen Verengung des öffentlichen Diskurses und somit zu einem immensen Freiheitsverlust führen. In diesem Sinne

---

[131] § 100a Abs. 4 S. 1 StPO, wonach beim Vorliegen tatsächlicher Anhaltspunkte für die Annahme, dass allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden, die entsprechende Maßnahme unzulässig ist, ist lediglich auf die Telekommunikationsüberwachung nach § 100a StPO und nicht auf die Erhebung von Verkehrsdaten nach § 100g StPO anwendbar. Diesbezüglich ist zu bemerken, dass eine Feststellung, dass bei einer Telekommunikationsüberwachung allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt werden, praktisch kaum möglich sein würde.

[132] BVerfGE, NJW 2006, S. 976 (979); Vgl. auch BVerfGE 65, 1 (43).

erscheint die Gewährleistung einer freien und möglichst ungestörten individuellen Kommunikation als eine Bedingung für die Freiheit der öffentlichen Meinungsbildung. Eine Totalüberwachung des Kommunikationsverhaltens der Bürger, wie sie durch die vorgesehene Vorratsdatenspeicherung ermöglicht wird, hindert die Kommunikationsfreiheit in einem erheblichen Maße. Sie ist geeignet, insbesondere die Aktivitäten von kritischen Personen und Organisationen wie Journalisten, Menschenrechtsorganisationen, Oppositions- und außerparlamentarischen Parteien etc. zu beeinträchtigen, die für das Funktionieren der modernen Demokratie unentbehrlich sind. Bei einzelnen Bürgern ist außerdem ein Verzicht der Nutzung von Telekommunikationsmitteln zu befürchten. Dies würde ebenfalls zur Beeinträchtigung der für die Demokratie unabdingbaren Freiheit der gesamtgesellschaftlichen geistigen Auseinandersetzung führen.

Das Bundesverfassungsgericht hat bei Maßnahmen mit einer hohen Streubreite die gesamtgesellschaftliche Bedeutung des Schutzes der Vertraulichkeit der Telekommunikation hervorgehoben: „Es gefährdet die Unbefangenheit der Nutzung der Telekommunikation und in der Folge die Qualität der Kommunikation einer Gesellschaft, wenn die Maßnahmen dazu beitragen, dass die Risiken des Missbrauchs und ein Gefühl des Überwachtwerdens entstehen“[133]. Für die Vorratsdatenspeicherung gilt dies erst recht, weil es sich um einen Grundrechtseingriff mit maximaler Streubreite handelt, der alle Teilnehmer und Nutzer der elektronischen Kommunikation betrifft.

Die Vorratsspeicherung von umfangreichen Kommunikationsdaten führt also zwangsläufig zu Kommunikationsanpassungen bei den einzelnen Bürgern. Auf diese Weise gefährdet sie wichtige Grundwerte der Demokratie des Grundgesetzes. Die Rechtsnormen, die sie regeln, sind daher mit dem Grundgesetz unvereinbar.

(7) Zwischenergebnis

Die durch § 113a TKG vorgesehene Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten stellt wegen der pauschalen Erfassung umfangreicher Telekommunikationsdaten einer Vielzahl von Personen ohne jeglichen Verdacht einen unverhältnismäßigen Eingriff in das Grundrecht auf Fernmeldegeheimnis aus Art. 10 Abs. 1 GG dar. Mit der umfangreichen anlasslosen Speicherung sensibler Verkehrs- und Standortdaten und den damit verbundenen Gefahren würde es in einem gewissen Sinne keine unbeobachtete Telekommunikation mehr geben. Die Beschwerdeführer sind in ihrem Grundrecht aus Art. 10 Abs. 1 GG verletzt.

---

[133] BVerfGE 107, 299 (328).

4. Der Zugriff auf die Vorratsdaten als Verletzung des Fernmeldegeheimnisses aus Art. 10 Abs. 1 GG

Auch wenn anzunehmen wäre, dass die anlasslose Erhebung und Speicherung sämtlicher Verbindungsdaten aller Kommunikationsteilnehmer generell nicht gegen das durch Art. 10 Abs. 1 GG gewährleistete Fernmeldegeheimnis verstößt, sind die Zugriffs- und Verwendungsmöglichkeiten der auf Vorrat gespeicherten Daten selbständige unverhältnismäßige Eingriffe in das Fernmeldegeheimnis der Beschwerdeführer aus Art. 10 Abs. 1 GG.

Das Bundesverfassungsgericht hat in ständiger Rechtsprechung besondere Anforderungen an den staatlichen Informationszugriff auf personenbezogene Telekommunikationsdaten gestellt. Bei der Bemessung der Intensität des Grundrechtseingriffs sind danach die Gestaltung der Eingriffsschwellen, die Bestimmung der zugriffsberechtigten Behörden, die Zahl der Betroffenen und ihre Identifizierbarkeit, die Intensität der Beeinträchtigungen, die Missbrauchsgefahren sowie die aus dem Bestimmtheitsgebot folgende Notwendigkeit einer hinreichenden und normenklaren Bestimmung des Zwecks der Datenerhebung und -verwendung zu berücksichtigen[134].

a) Art der Informationszugriffe

Die Vorratsdatenspeicherungsrichtlinie eröffnet den Mitgliedsstaaten Ermessensspielräume, was die Bestimmung der zugriffsberechtigten Behörden und der Zugriffsvoraussetzungen und -verfahren betrifft (Art. 4 RL 2006/24/EG). Damit wird den Unterschieden in den jeweiligen mitgliedsstaatlichen Rechtsordnungen, die die Struktur und die Kompetenzen der nationalen Strafverfolgungsbehörden regeln, Rechnung getragen. Eine Möglichkeit zur Verwendung der Vorratsdaten von anderen Behörden und zu anderen Zwecken als der Strafverfolgung, sieht die Richtlinie nicht vor (vgl. Art. 4 und Art. 11 RL 2006/24/EG i.V.m. Art. 15 Abs. 1 der Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG).

Demgegenüber regelt das neue TKG Zugriffsmöglichkeiten auf die vorrätig gespeicherten Daten nicht nur für die Strafverfolgungsbehörden, sondern auch für die Verfassungsschutzbehörden des Bundes und der Länder sowie die Nachrichtendienste und die übrigen mit der Abwehr von erheblichen Gefahren beauftragten Behörden (§ 113b TKG). Die entsprechenden Regelungen in den jeweiligen Gesetzen sollen zusätzlich geändert werden und eine Bezugnahme auf § 113a TKG enthalten (§ 113b TKG)[135]. Damit geht der deutsche Gesetzgeber auch in diesem Punkt eindeutig über die Vorgaben der Richtlinie deutlich hinaus und erhöht erheblich die Intensität des mit der Vorratsdatenspeicherung herbeigeführten Grundrechtseingriffs. Insbesondere die Befugnisse der

---

[134] Vgl. BVerfGE 100, 313 (376); 107, 299 (320); 113, 348 (282).

[135] Nach der geltenden Rechtslage dürfen die Nachrichtendienste sowie die Verfassungsschutzämter auf bestimmte Verkehrsdaten zugreifen. Vgl. § 100g StPO, § 3 Nr. 3 TKG, §§ 112, 113 TKG, § 8a Abs. 2 Nr. 4 BVerfSchG, § 2a S. 1 BNDG, § 4a S. 1 MADG.

Nachrichtendienste, auf die vorrätig gespeicherten Daten zuzugreifen, sind wegen der diesbezüglichen geringen Rechtsschutzmöglichkeiten der Betroffenen mit dem Grundgesetz nicht vereinbar.

In der Begründung zum ursprünglichen Gesetzesentwurf des Bundesjustizministeriums wurde versucht, die Verhältnismäßigmäßigkeit der Gesamtregelung gerade mit dem Argument zu retten, dass die Geheimdienste keinen Zugriff auf die Vorratsdaten erhalten. Danach sollte eine Übermittlung der gespeicherten Vorratsdaten für andere Zwecke als zur Verfolgung von Straftaten nicht zulässig sein. Damit sei – so die Begründung zum Referentenentwurf – „insbesondere eine Übermittlung der allein auf der Grundlage des § 113a TKG gespeicherten Daten für Zwecke der Gefahrenabwehr, der Aufgabenerfüllung der Dienste oder auch zur Erfüllung zivilrechtlicher Ansprüche" ausgeschlossen [136]. Die Gründe für die Änderung dieser Rechtsauffassung beim Verfassen des Regierungsentwurfs sind nicht ersichtlich[137].

Bei der Umsetzung der Vorratsdatenspeicherungsrichtlinie werden grundlegende Änderungen bezüglich der Art des staatlichen Zugriffs auf Verkehrsdaten eingeführt. Durch die Neufassung des § 100g Abs. 1 StPO soll der bisherige Auskunftsanspruch der Strafverfolgungsbehörden gegenüber den Telekommunikationsunternehmen in eine umfassende Erhebungsbefugnis für Verkehrsdaten umgewandelt werden [138]. So würde es ihnen künftig ermöglicht, selbst und in Echtzeit Verkehrsdaten sowie Standortdaten zu erheben und zu verwerten. Dies ermöglicht, die Bewegungen einer Person ohne Zeitverzögerung im Moment der jeweiligen Ortswechsel mitzuverfolgen, und damit jeweils im Zeitpunkt des tatsächlichen Geschehens lückenlos über Aufenthaltsorte und elektronische Kontaktaufnahmen informiert zu sein. Die Auskunftsverpflichtung der Dienstanbieter bleibt davon unberührt[139]. Mit dem Verzicht auf das Tatbestandsmerkmal „im Falle einer Verbindung" und mit der Zulassung der Echtzeiterhebung von Standort- und Verbindungsdaten bei der mobilen Telefonie wird künftig die Erstellung von Bewegungsprofilen einzelner Personen möglich sein. Dies stellt einen tiefgehenden Eingriff in das Grundrecht auf vertrauliche Telekommunikation dar, für dessen Rechtfertigung keine Gründe ersichtlich sind. Zu bemerken ist dazu, dass auch in diesem Punkt eine Verschärfung der Regelung im Vergleich zum ersten Referentenentwurf besteht. Ursprünglich war die Verkehrsdatenabfrage in Echtzeit nur bei in § 100a Abs. 2 StPO bezeichneten Straftaten vorgesehen. Die Regelung des § 100g Abs. 1 S. 3 StPO weitet die Echtzeitabfrage auf alle im § 100g Abs. 1 S. 1 Nr. 1 StPO bezeichneten Straftaten aus.

Zu bemerken ist außerdem, dass § 113b die Verwendung der gespeicherten Daten lediglich seitens der Dienstanbieter und nicht seitens der Behörden, die zur Anordnung der Weitergabe der Daten befugt sind, einschränkt. Dies kann u.U. dazu führen, dass diese Behörden dann die Daten

---

[136] Begründung zum Referentenentwurf des BMJ, S. 151.

[137] Gleichwohl werden die Verhältnismäßigkeitsprobleme in der Begründung zum Regierungsentwurf erkannt (vgl. BTDrs. 16/5846, Begründung zum Regierungsentwurf, S. 74).

[138] BTDrs. 16/5846, Begründung zum Regierungsentwurf, S. 50.

[139] § 100g Abs. 2 S. 1 StPO i.V.m. § 100b Abs. 3 StPO.

anderen Interessierten zur Verfügung stellen. Das Fehlen einer präzisen Bestimmung der Übermittlung und des Verwendungszwecks macht die Regelung unverhältnismäßig.

Schwerwiegende verfassungsrechtliche Bedenken bestehen auch hinsichtlich des staatlichen Zugriffs auf die dynamischen IP-Adressen im Internetbereich[140]. De lege lata ist diesbezüglich die Norm des § 113 Abs. 1 TKG relevant. Danach sind die Anbieter von Telekommunikationsdiensten verpflichtet, den zuständigen Stellen Auskunft über die nach den §§ 95 und 111 TKG erhobenen Bestandsdaten zu erteilen, soweit dies für die Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder für die Erfüllung der Aufgaben der Verfassungsschutzbehörden, des Bundesnachrichtendienstes oder des Militärischen Abschirmdienstes erforderlich ist. Nach allgemeiner Auffassung ist die Norm bei Auskunftsersuchen bezüglich statischer IP-Adressen einschlägig, weil diese Adressen als Bestandsdaten im Sinne von § 3 Nr. 3 TKG anzusehen sind[141]. Demgegenüber stellen die dynamischen IP-Adressen aber Verkehrsdaten dar, u.a. weil sie in keinem unmittelbaren Zusammenhang mit dem jeweiligen Vertragsverhältnis stehen. Dementsprechend dürfen derzeit Auskunftsersuchen bezüglich dynamischer IP-Adressen nach Maßgabe der §§ 100g und 100h StPO angeordnet werden. Die relevante Rechtsprechung ist allerdings uneinheitlich[142]. Eine gesetzliche Klarstellung, dass der Zugriff auf die dynamischen IP-Adressen nur unter den Voraussetzungen des § 110g StPO zulässig ist, erscheint wegen ihrer hohen Aussagekraft daher notwendig[143]. Darauf hat aber der Gesetzgeber verzichtet, was der Sensibilität der aufgrund der dynamischen IP-Adressen zu erlangenden Informationen nicht gerecht wird[144]. Eine uneinheitliche Rechtspraxis, bei der es unter Umständen auch zur inhaltlichen Überwachung der Internetnutzung kommen kann, erscheint somit vorprogrammiert[145].

b) Voraussetzungen für den Zugriff auf die vorrätig gespeicherten Verkehrsdaten

(1) Straftatenkatalog für den staatlichen Zugriff auf die Vorratsdaten (§ 100g Abs. 1 StPO)

---

[140] § 113a Abs. 2 Nr. 5, Abs. 3 Nr. 1-3 und Abs. 4 Nr. 1, 3 TKG ordnen die Vorratsspeicherung der IP-Adressen bei den verschiedenen Internetkommunikationsvorgängen an, ohne dabei nach statischen und dynamischen IP-Adressen zu differenzieren.

[141] *Gercke*, in: F. Roggan/M. Kutscha (Hrsg.), Handbuch zum Recht der inneren Sicherheit, 2. Aufl., Berlin 2006, S. 170.

[142] Vgl. einerseits *LG Bonn*, DuD 2004, S. 628 und andererseits *LG Hamburg*, MMR 2005, S. 711, LG Stuttgart, NJW 2005, S. 614.

[143] Diesbezüglich heißt es in der Stellungnahme des Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein zum Regierungsentwurf vom 27.06.2007, S. 14: „Die IP-Adresse wird in der Praxis von vielen Internetanbietern – entgegen der Gesetzeslage – mitgelogt. Erhalten die Behörden Zugriff auf Log-Dateien, so lassen sich umfassende Interessenprofile des Betroffenen abbilden. So lässt sich etwa bei einem Besuch einer Online-Zeitung genau nachvollziehen, für welche Zeitungsartikel er sich interessiert hat. Verknüpft man die Log-Dateien verschiedener Anbieter, lässt sich mit Hilfe der Vorratsdatenspeicherung ein umfassendes Persönlichkeitsbild erstellen". Die Stellungnahme ist abrufbar unter www.datenschutzzentrum.de.

[144] Die Begründung zum Regierungsentwurf betrachtet die dynamischen IP-Adressen pauschal als Bestandsdaten und verweist auf eine angeblich gefestigte Rechtsprechung, die richtigerweise zur Anwendbarkeit des § 113 TKG führte. Vgl. BTDrs. 16/5846, S. 26-27.

Gemäß Art. 1 Abs. 1 Richtlinie 2006/24/EG bezweckt die verbindliche Speicherung und Sicherung der Verfügbarkeit der Verkehrsdaten die Ermittlung, Feststellung und Verfolgung von schweren Straftaten. Es wird nicht ausdrücklich festgelegt, was unter „schwere Straftaten" zu verstehen ist[146]. Vielmehr überlässt die Richtlinie die konkrete Bestimmung der Straftaten zu deren Verfolgung die Daten verwendet werden dürfen ausdrücklich den Mitgliedstaaten.[147] Damit lässt sie dem nationalen Gesetzgeber einen Entscheidungsspielraum bei der Bestimmung des Straftatenkatalogs. Die darauf gründende Auswahl ist vom Bundesverfassungsgericht vollständig überprüfbar.

Sollte es sich bei der Regelung der Richtlinie, wonach schwere Straftaten zu speichern sind, um inhaltliche Vorgaben handeln, so geht das Umsetzungsgesetz zumindest über diese Vorgaben hinaus. Die Richtlinie stellt auf „schwere Straftaten" ab (Art. 1 Abs. 1 RL 2006/24/EG).

Die Begründung des Entwurfs zum Umsetzungsgesetz betont zu Recht die inhaltlichen Unterschiede bei den Begriffen „schwere Straftat", „Straftat von erheblichen Bedeutung" und „besonders schwere Straftat". Der Begriff der „schweren Straftat" nähme eine Zwischenstellung zwischen den anderen zwei Begriffen ein. Hierunter könnten solche Straftaten verstanden werden, die eine Mindesthöchststrafe / Mindeststrafandrohung von fünf Jahren Freiheitsstrafe aufweisen, in Einzelfällen aufgrund der besonderen Bedeutung des geschützten Rechtsgutes oder des besonderen öffentlichen Interesses an der Strafverfolgung aber auch eine geringere Freiheitsstrafe. 100g Abs. 1 StPO lässt jedoch einen Zugriff auf die gespeicherten Verbindungsdaten schon bei „Straftaten von erheblicher Bedeutung" zu, und nicht erst bei „schweren Straftaten". Die Begründung versucht dies mit einer wenig überzeugenden Sprachequilibristik zu rechtfertigen, indem der in der Richtlinie verwendete Begriff der „schweren Straftat" mit dem Begriff der „Straftat von erheblicher Bedeutung" nach der StPO gleichgesetzt wird. Die deutsche Übersetzung des englischen Begriffs „serious crime" sei unglücklich gewählt worden. Dieser Begriff diene in europäischen Rechtsinstrumenten dazu, Tatbestände auszugrenzen, die lediglich die Schwere von Ordnungswidrigkeiten oder Bagatellkriminalität erreichen, und sei im europäischen Kontext im Sinne einer „ernsthaften Straftat" zu übersetzen als mit schwerer Kriminalität zu assoziieren.

Dabei wird erstens verkannt, dass die europäischen Rechtsakte in allen sprachlichen Fassungen gleich verbindlich sind. Zweitens ist zu bemerken, dass eine etablierte europarechtliche Terminologie im Bereich des Strafrechts wegen der geringen Kompetenzen der EU in diesem Bereich kaum existiert. Vielmehr ist üblich, in den jeweiligen Regelungsinstrumenten entsprechende Begriffsbestimmungen aufzunehmen. Diese Auffassung kann drittens auch angesichts der Entstehungsgeschichte der Richtlinie nicht überzeugen – während des

---

[145] Vgl. dazu Zöller, GA 2007, S. 393 (407).

[146] Vgl. auch die Erklärung des Europarates zum Begriff der „schweren Straftat", Ratsdokument 5777/06 ADD 1 REV 1 vom 17.02.2006, http://register.consilium.europa.eu/pdf/de/06/st05/st05777-ad01re01.de06.pdf. Diese Erklärung kann allerdings die fehlende Definition in der Richtlinie nicht ersetzen, da der Rat nicht befugt ist, durch einen eigenen Beschluss eine Richtlinie zu ergänzen.

[147] RL 24 2006/24/EG, Art. 1 Abs. 1.

Rechtsetzungsprozesses hatte das Europäische Parlament die Begrenzung auf „schwere Straftaten" mühsam erreicht. Indem das Umsetzungsgesetz einen Zugriff auf die Verbindungsdaten bereits beim Verdacht auf „Straftaten von erheblicher Bedeutung" zulässt, geht es über die Vorgaben – sollten sie als solche zu verstehen sein – des Art. 1 Abs. 1 der Richtlinie 2006/24/EG hinaus.

(a) Verweis über die in Art. 100a Abs. 2 StPO genannten Straftaten hinaus in seiner Weite verfassungswidrig

Nach § 100g Abs. 1 StPO darf Auskunft über die gespeicherten Verkehrsdaten zur Verfolgung von Straftaten von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Abs. 2 StPO bezeichnete Straftat, sowie zur Verfolgung mittels Telekommunikation begangener Straftaten verlangt werden. Der Verweis auf § 100a Abs. 2 StPO ist also nur beispielhaft, d.h. es kann auch andere Straftaten von „erheblicher Bedeutung" geben, zu deren Verfolgung ein Zugriff auf die gespeicherten Daten möglich sein soll[148]. Kriterien für die Bestimmung dieser weiteren Straftaten sind im Gesetz nicht enthalten. Hierunter könnten solche Straftaten verstanden werden, die eine Mindeststrafandrohung von fünf Jahren Freiheitsstrafe aufweisen, in Einzelfällen aufgrund der besonderen Bedeutung des geschützten Rechtsgutes oder des besonderen öffentlichen Interesses an der Strafverfolgung aber auch eine geringere Freiheitsstrafe[149].

Außerdem genügt der interpretationsbedürftige Bezug auf eine „Straftat von erheblicher Bedeutung" in § 100g Abs. 1 Nr. 1 StPO dem verfassungsrechtlichen Bestimmtheitserfordernis nicht. Entsprechend dem aus dem Rechtsstaatsprinzip ableitbaren Bestimmtheitsgebot müssen sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Einzelnen erkennbar aus dem Gesetz ergeben[150]. Die Begründung zum Gesetzes geht davon aus, dass eine solche Straftat mindestens dem Bereich der mittleren Kriminalität zuzurechnen sein soll, den Rechtsfrieden empfindlich stören und dazu geeignet sein müsse, das Gefühl der Rechtssicherheit der Bevölkerung zu beeinträchtigen[151]. Sowohl der Normtext als auch die Begründung enthalten unbestimmte Begriffe, die eine sehr weite Auslegung erlauben und damit für die Rechtsanwendung keine feste Grundlage bieten. Dem Gebot der Normenklarheit, das bei Eingriffen in das Fernmeldegeheimnis besonders zu berücksichtigen ist, wird somit nicht Genüge getan. Vielmehr erscheint es wegen der hohen Intensität des Grundrechtseingriffs verfassungsrechtlich geboten, die betreffenden Straftaten in einem enger gefassten abschließenden Katalog aufzulisten. Indem die Regelungen einen Zugriff schon bei „Straftaten von erheblicher Bedeutung" zulassen und die relevanten Straftaten nicht klar definieren, verstoßen sie

---

[148] Zu bemerken ist außerdem, dass in der Norm des § 113b TKG, die laut Begründung den Zweck der Datenspeicherung und Datenverwendung regeln soll, lediglich von „Verfolgung von Straftaten" die Rede ist.

[149] BTDrs. 16/5846, Begründung zum Regierungsentwurf, S. 40.

[150] Zu den verfassungsrechtlichen Bedenken bezüglich des Begriffs „Straftat von erheblicher Bedeutung" vgl. *Gercke*, in: F. Roggan/M. Kutscha (Hrsg.), Handbuch zum Recht der inneren Sicherheit, 2. Aufl., Berlin 2006, S. 159f. Das Bundesverfassungsgericht hat allerdings den Begriff im Hinblick auf § 110g StPO als hinreichend bestimmt angesehen (BVerfGE 107, 299, 322).

[151] BTDrs. 16/5846, Begründung zum Regierungsentwurf, S. 40.

sowohl gegen das Prinzip der Verhältnismäßigkeit staatlicher Maßnahmen als auch gegen den Grundsatz der konkreten Zweckbestimmung bei Zugriffen auf personenbezogene Daten.

(b) Verweis auf Art. 100a Abs. 2 StPO und fehlende Subsidiaritätsklausel verfassungswidrig

Der generelle Verweis auf den umfangreichen Straftatenkatalog des § 100a Abs. 2 StPO ist angesichts der „Streubreite" und der Intensität der Vorratsdatenspeicherung nicht angemessen. Der Gesetzgeber müsste prüfen und begründen, ob die Verwendung der durch die Vorratsdatenspeicherung gewonnenen Daten bei der Verfolgung aller im § 100a Abs. 2 StPO aufgezählten Straftaten dem Verhältnismäßigkeitsgrundsatz entspricht. Dies ist im Rahmen des Gesetzgebungsprozesses nicht geschehen. Außerdem ist im Rahmen der Novellierung des § 100a StPO eine Ausweitung der Straftatbestände erfolgt, deren Verdacht eine Telekommunikationsüberwachung rechtfertigen soll.

Zu bemerken ist ferner, dass die Subsidiaritätsklausel des § 100g Abs. 1 S. 2 StPO nur die Kategorie der mittels Telekommunikation begangenen Straftaten betrifft. Der Zugriff auf die gespeicherten Verkehrsdaten ist also im Fall einer der im § 100a Abs. 2 StPO genannten Straftaten nicht an die Voraussetzung gebunden, dass die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos wäre und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht. Ist schon die praktische Bedeutung dieser Subsidiaritätsklausel in § 100g Abs. 1 S. 2 StPO zweifelhaft, so wird bei der Verfolgung von Straftaten von erheblicher Bedeutung gänzlich auf den Vorrang offener Ermittlungsmethoden verzichtet. Eine solche Regelung ist nicht angemessen.

(c) Regelung über Abruf bei mittels Telekommunikation begangener Straftaten, § 100g Abs. 1 Nr. 2 StPO verfassungswidrig

Bezüglich der mittels Telekommunikationsmittel begangenen Straftaten ist nicht vorgesehen, dass es sich bei ihnen auch um „schwere Straftaten" bzw. „Straftaten von erheblicher Bedeutung" handeln muss. Diese Regelung gründet nicht auf der Richtlinie 2006/24/EG sondern auf der Cybercrime - Konvention[152], die Umsetzung ist in vollem Umfang überprüfbar. Der Mangel an einschränkenden Merkmalen im Hinblick auf die Schwere oder Erheblichkeit der Anlasstat bei mittels Telekommunikation begangener Straftaten kann dazu führen, dass ein Zugriff auf die umfangreichen und aussagekräftigen Verkehrsdaten auch bei Bagatellstraftaten, etwa bei einer Beleidigung per Telefon, erfolgt. Dies führt zur Unverhältnismäßigkeit des § 100g Abs. 1 S. 1 Nr. 2 StPO.

---

[152] ETS 185 – Convention on Cybercrime, 23.XI.2001.

Dieser Wertung steht auch der Beschluss des Bundesverfassungsgerichts zur Nichtannahme einer Verfassungsbeschwerde [153] , nach dem die Erhebung von Verkehrsdaten bei mittels Telekommunikation begangener Straftaten von nicht erheblicher Bedeutung verfassungsgemäß ist, nicht entgegen. [154] Der erwähnte Beschluss bezieht sich konkret auf die bisher geltende Rechtslage und ist auf die Vorratsdatenspeicherung wegen ihrer neuartigen grundrechtseingreifenden Intensität nicht übertragbar[155].

(2) Zugriff durch Verfassungsschutz und Geheimdienste nach landesrechtlichen Vorschriften

Noch weniger hinreichend bestimmt ist der Zweck des staatlichen Zugriffs seitens der Verfassungsschutzämter, der Geheimdienste und der anderen zugriffsberechtigten Behörden in § 113b S. 1 Nr. 2 u. 3. TKG. An diese Vorschrift im TKG knüpfen die gerügten landesrechtlichen Regelungen an. Art 34b Abs. 2 i. V. m. Art. 34a Abs. 1 Satz 1, Abs. 3 S. 1 BayPAG, Art. 6c BayVSG und § 34 a ThürPAG an.

An einem Katalog von Straftaten bzw. Gefahren, die den Informationseingriff rechfertigen sollen, fehlt es hier. Nach geltender Rechtslage sind diese Behörden bei Ausübung ihrer Befugnisse in Zusammenhang mit dem Zugriff auf Verkehrsdaten an keinen konkreten Tatverdacht bzw. an keine konkrete Gefahrenlage gebunden. Die allgemeine polizeirechtliche Eingriffsschwelle der Gefahr für die öffentliche Sicherheit wird in § 113b S. 1 Nr. 2 TKG nur durch den unbestimmten Rechtsbegriff der „Erheblichkeit" eingeschränkt. Damit werden den Polizeibehörden weitreichende Erkenntnisse über das Kommunikationsverhalten und die sozialen Kontakte der Betroffenen erlangen können. Die Zugriffsmöglichkeiten der Nachrichtendienste intensivieren den Grundrechtseingriff in besonderem Maße, weil sie keine richterliche Anordnung voraussetzen.

Art 34b Abs. 2 i. V. m. Art. 34a Abs. 1 Satz 1, Abs. 3 S. 1 BayPAG ermöglicht es den Polizeibehörden im Freistaat Bayern auch die sensiblen Telekommunikationsdaten von unbeteiligten Dritten einsehen zu können. Zwar verschärft die Norm die Eingriffsschwelle gegenüber § 113b S. 2 Nr. 2 TKG. Dies führt jedoch nicht dazu, die grundsätzlichen verfassungsrechtlichen Bedenken an der Norm fallen zu lassen. Die Normen sehen weder die Eingriffsermächtigung durch einen Richter noch die ordnungsgemäße Dokumentation der Eingriffe vor.

Art. 34a ThürPAG verzichtet ebenfalls auf einen Richtervorbehalt.

Art. 6c BayVSG ist ebenso verfassungswidrig. Die bereits in § 113b TKG vorgesehene Möglichkeit zum Abruf der Vorratsdaten durch die Nachrichtendienste ist zu weit gefasst. Die Begrenzung auf

---

[153] Vgl. BVerfG, 2 BvR 1085/05 vom 17.06.2006, Absatz Nr. 17-18.

[154] Anders BTDrs. 16/5846, Begründung zum Regierungsentwurf, S. 52.

[155] Außerdem fordert das Bundesverfassungsgericht auch in diesem Fall die Einhaltung des Verhältnismäßigkeitsgrundsatzes. Zu bemerken ist auch, dass die nicht näher begründete Aussage, wonach sich der Anspruch eines Beschuldigten auf vertrauliche Telekommunikation beim Einsatz einer Telekommunikationsanlage als Tatmittel mindern soll, wenig überzeugend ist (vgl. BVerfG, 2 BvR 1085/05 vom 17.06.2006, Absatz Nr. 17).

die gesetzlichen Aufgaben der Nachrichtendienste kommt einer Pauschalermächtigung gleich und kann nicht ausreichen den erheblichen Grundrechtseingriff zu rechtfertigen. Mit dem Tatbestand des Art. 6c BayVSG übernimmt der bayerische Gesetzgeber dieses Regelungskonzept. Zwar reichert er dieses mit der weiteren Eingriffsschwelle, der sich aus tatsächlichen Anhaltspunkten ergebenden schwerwiegenden Gefahr für die Schutzgüter des Art. 3 Abs. 1 BAyVSG an. Jedoch fehlt es auch hier im Bereich der sogenannten Vorfeldgefahren an einer ordentlichen (gesetzlichen) Dokumentationspflicht und einem Richtervorbehalt.

Zusammenfassend ist festzustellen, dass mit der Verwendung der gesammelten Daten zur Aufklärung mittelschwerer und mittels Telekommunikationseinrichtungen begangener Straftaten eine unverhältnismäßige Lösung vorgeschlagen wurde, die über die Vorgaben der Vorratsdatenspeicherungsrichtlinie hinaus geht.

(3) Zusammenfassung: Zu niedrige Eingriffsschwelle

Für den Zugriff auf die von den Telekommunikationsanbietern gespeicherten Daten zu Zwecken der Strafverfolgung ist lediglich ein Anfangsverdacht vorgesehen (§ 100g Abs. 1 S. 1 StPO). Die Praxis zeigt, dass es nicht selten vorkommt, dass ein Anfangsverdacht allein auf Grund der Tatsache, dass jemand auf einer E-Mail-Userliste steht, angenommen wird. Diese niedrige Eingriffsschwelle ist angesichts des breiten Betroffenenkreises, der Vielzahl der gespeicherten Daten und des damit verbundenen erhöhten Risikos falscher Verdächtigung unangemessen. Das damit einhergehende Ausmaß der vorgesehenen Zugriffsbefugnisse steht in keinem angemessenen Verhältnis zu ihrem tatsächlichen Nutzen[156].

Beim Zugriff auf die vorrätigen Verkehrsdaten zu Zwecken der Abwehr von erheblichen Gefahren und zur Aufgabenerfüllung der Verfassungsschutzämter und der Geheimdienste sind die Eingriffsschwellen ebenfalls niedrig angesetzt bzw. sehr allgemein formuliert. Die Begriffe „erhebliche Gefahr" (§113b TKG), „schwerwiegende Gefahr" (§ 8a Abs. 2 BVerfSchG, § 2a S. 2 BNDG) und „schwerwiegende Gefährdung" (§ 4a S. 1 MADG) sind ungeeignet, zu bestimmen, wann der Zugriff auf die Daten zulässig sein soll.

c) Unzureichende Differenzierung nach betroffenen Personen

Nach § 100a Abs. 3 StPO darf sich die Anordnung auch gegen eine Person richten, von der auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Beschuldigten bestimmte oder von

---

[156] Mehr dazu bei *Breyer*, Die systematische Aufzeichnung und Vorhaltung von Telekommunikations-Verkehrsdaten für staatliche Zwecke in Deutschland, Berlin 2005, S. 178f., 265f.

ihm herrührende Mitteilungen entgegennimmt oder weitergibt oder dass der Beschuldigte ihren Anschluss benutzt. Diese Vorschrift bezieht sich auf die Telekommunikationsüberwachung, soll aber auf die Erhebung von Verkehrsdaten entsprechend angewandt werden (§ 100g Abs. 2 S. 1 StPO). Diese Beschränkung der Maßnahme auf den Beschuldigten und auf seine Nachrichtenmittler kann praktisch nicht erfolgen. Technisch bedingt betrifft die Maßnahme immer auch ihre übrigen Telekommunikationspartner, die bezüglich der jeweiligen Straftat gänzlich unbeteiligt sind. Aufgrund dieser Streubreite ist die Regelung unangemessen. Außerdem erscheint sie angesichts der Intensität des Grundrechtseingriffs, den sie herbeiführt, nicht ausreichend bestimmt. Es fehlt ein handhabbarer Maßstab für die Prüfung, bei Vorliegen welcher konkreten Tatsachen eine Unterstützung des Beschuldigten durch eine Drittperson mittels Kommunikationsmittel anzunehmen ist. Eine restriktive Auslegung könnte das Bestimmtheitsdefizit nicht beseitigen.

Dasselbe gilt für die Normen, die die entsprechenden Befugnisse zur Erhebung und Verwertung von Verkehrsdaten durch die Verfassungsschutzämter, die Nachrichtendienste und die übrigen zugriffsberechtigten Behörden regeln (vgl. beispielsweise § 8a Abs. 3 i.V.m. Abs. 2 Nr. 4 BVerfSchG, § 4a MADG, § 2a S. 3 BNDG[157]).

d) Zwischenergebnis

Die Zugriffsmöglichkeiten auf Vorratsdaten zur Verfolgung mittelschwerer und aller mit Telekommunikationsmitteln begangener Straftaten sowie zur Gefahrenabwehr und der Aufgabenerfüllung der Geheimdienste ist unverhältnismäßig und geht über die Vorgaben der Vorratsdatenspeicherungsrichtlinie hinaus. Dies wird noch dadurch verstärkt, dass für die Verwendung von Vorratsdaten bereits ein Anfangsverdacht ausreicht und die Differenzierung bezüglich der Kontaktpersonen unzureichend ist.

Die Zugriffsmöglichkeiten zahlreicher staatlicher Stellen weisen eine besonders hohe Eingriffsintensität auf und verletzen das Fernmeldegeheimnis der Beschwerdeführer.

II. Verletzung des Rechts auf informationelle Selbstbestimmung, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG

Das Recht auf informationelle Selbstbestimmung und das Fernmeldegeheimnis stehen, soweit es um den Schutz der technischen Kommunikationsdaten geht, in einem Ergänzungsverhältnis[158].

---

[157] Diese Regelungen sollen entsprechend § 113b TKG, der eine ausdrückliche Bezugnahme auf den künftigen § 113a TKG fordert, geändert werden.

[158] BVerfGE, 2 BvR 1345/03 („IMSI-Catcher"), Rn. 66.

Das Fernmeldegeheimnis ist ein Spezialfall des Rechts auf informationelle Selbstbestimmung und enthält, bezogen auf den Fernmeldeverkehr, eine spezielle Garantie. Greift Art. 10 Abs. 1 GG nicht, werden die Daten technischer Kommunikation durch das Recht auf informationelle Selbstbestimmung geschützt.

Im Zusammenhang mit den Regelungen des Umsetzungsgesetzes stellt sich die Frage, ob konkrete Datenarten (z.B. Bestandsdaten oder Standortdaten), zu deren Erhebung und Speicherung das Umsetzungsgesetz ermächtigt, den Schutz des Art. 10 Abs. 1 GG genießen oder lediglich vom Grundrecht auf informationelle Selbstbestimmung umfasst sind. Nach einer stark werdenden Auffassung sind die Bestandsdaten jedenfalls durch das Recht der informationellen Selbstbestimmung geschützt. Die Bestandsdaten über das Vertragsverhältnis mit Kommunikationsmittlern seien auch durch das Fernmeldegeheimnis geschützt [159]. Vorliegend spricht vieles dafür, auch die Bestandsdaten in den Schutz des Art. 10 Abs. 1 GG einzubeziehen. Sie werden zusammen mit den Verkehrsdaten und den Standortdaten erhoben, gespeichert und ausgewertet und bilden somit eine Einheit. Auf diese Weise entsteht die Möglichkeit zur Erstellung umfassender Bewegungs- und Kommunikationsprofile der Kommunikationsnutzer.

Auch wenn die Bestands- und Standortdaten nicht als vom Schutzbereich des Fernmeldegeheimnisses umfasst angesehen werden, sind sie als personenbezogene Daten durch das Grundrecht auf informationelle Selbstbestimmung geschützt. Dasselbe gilt auch für andere zu speichernde Daten, hinsichtlich deren das Gericht Art. 10 Abs. 1 GG nicht für einschlägig halten sollte. Insoweit rügen die Beschwerdeführer subsidiär eine Verletzung des Grundrechts auf informationelle Selbstbestimmung. Gerügt wird die mangelnde Geeignetheit, Erforderlichkeit und Angemessenheit der Regelungen. Dazu wird auf die obigen Ausführungen zur Verletzung des Art. 10 Abs. 1 GG entsprechend verwiesen.

III. Verstoß gegen die Berufsfreiheit, Art. 12 Abs. 1 GG

Die Beschwerdeführer zu 2), 5), 7), 8), 9), 10) machen eine Verletzung ihrer Berufsfreiheit aus Art. 12 Abs. 1 GG geltend.

§ 113a Abs. 1 bis 6 TKG verletzt die Berufsfreiheit der Beschwerdeführerin zu 9), indem er ihnen die Verpflichtung zur Speicherung sämtlicher Telekommunikationsverbindungsdaten ihrer Kunden ohne jegliche Entschädigung für die entstehenden Kosten auferlegt.

Die Berufsfreiheit der Beschwerdeführer zu 2), 5), 7), 8) und 10) wird dadurch verletzt, dass die Kommunikation und das Vertrauensverhältnis zwischen ihnen und ihren Mandanten bzw. Patienten angesichts der eingeführten Vorratsdatenspeicherung ungerechtfertigt beeinträchtigt wird.

---

[159] Vgl. Breyer, RDV 2003, S. 219.

1. Schutzbereich und Eingriff

a) Telekommunikationsunternehmen

Das Grundgesetz sieht ein Grundrecht auf Unternehmensfreiheit nicht ausdrücklich vor. Rechtsprechung und Lehre sind sich jedoch einig, dass das Grundrecht der Berufsfreiheit aus Art. 12 Abs. 1 S. 1 GG auch die Unternehmensfreiheit, also das Recht auf freie Gründung und Führung von Unternehmen und auf eigene wirtschaftliche Betätigung umfasst[160]. Art. 12 Abs. 1 S. 1 GG, dessen persönlicher Schutzbereich auch Handelsgesellschaften einschließt, umfasst in sachlicher Hinsicht auch die Investitions-, Preisbindungs- und Wettbewerbsfreiheit eines jeden Unternehmers[161].

§ 113a TKG berührt den Schutzbereich des Grundrechts aus Art. 12 Abs. 1 GG der Beschwerdeführerin zu 9). Die neu geschaffene Pflicht zur Vorratsdatenspeicherung stellt einen Eingriff in Form einer Berufsausübungsregelung dar. Die Verknüpfung zusätzlicher Pflichten mit der Ausübung eines Berufs ist regelmäßig ein Eingriff in das Grundrecht aus Art. 12 Abs. 1 S. 1 GG[162].

Mit der Verpflichtung der Beschwerdeführerin zu 9) zur Speicherung der in § 113a Abs. 2 bis 6 TKG aufgeführten Daten sowie zur Schaffung der in § 113a Abs. 10 und 11 TKG Maßnahmen wird in ihre Unternehmensfreiheit als Unterfall der Berufsfreiheit (Art. 12 Abs. 1 GG) eingegriffen. Die Beschwerdeführerin zu 9) wird durch die genannten Regelungen gezwungen, die Struktur und die Geschäftsplanung ihrer Unternehmen grundlegend zu verändern. Um die staatlich auferlegten Speicherungspflichten zu erfüllen, müssten sie erhebliche Investitionen vornehmen und neues Personal anstellen[163]. Außerdem werden für sie in Zukunft zusätzliche laufende Betriebskosten in beträchtlicher Höhe entstehen. Erhebliche Kosten werden auch die Bereitstellung von zusätzlichen Speicherungskapazitäten und der Kauf von neuen Geräten verursachen. Als kleine Telekommunikationsunternehmen wird die Beschwerdeführerin zu 9) besonders hart betroffen, weil die notwendigen zusätzlichen Investitionen ihre Wettbewerbsfähigkeit auf dem Telekommunikationsmarkt erheblich beeinträchtigen und von ihnen einen unverhältnismäßig höheren finanziellen und organisatorischen Aufwand verlangen als von den großen Telekommunikationskonzernen. Die Beschwerdeführerin sieht sich gezwungen, die Preise für die von ihr erbrachten Dienste zu erhöhen. Dies wird zu einem Kundenverlust führen, was wiederum die Insolvenz als Folge der neuen Gesetzeslage für die Beschwerdeführerin zu 9) bedeuten könnte.

Ein weiterer Eingriff in die Unternehmensfreiheit der Beschwerdeführerin zu 9) ist das in § 113a Abs. 6 TKG enthaltene praktische Verbot von Anonymisierungsdiensten. Die Beschwerdeführerin

---

[160] Vgl. Jarass, in: Jarass/Pieroth, Art. 12, Rn. 8; BVerfGE 50, 290 (363).

[161] BVerfGE 46, 120 (137f.); 50, 290 (363).

[162] Jarass, in: Jarass/Pieroth, Art. 12, Rn. 11; BVerfGE 68, 155 (170).

[163] Nach Berechnungen des BITKOM würde die Vorratsdatenspeicherung für die Industrie Anfangsinvestitionen für die notwendige neue Technik in Höhe von ca. 50 - 75 Mio. Euro verursachen (Stellungnahme von BITKOM, Rechtsausschuss des Deutschen Bundestages, Zusammenfassung der Stellungnahmen zur öffentlichen Anhörung am 21. September 2007, S. 119). Die Begründung des Gesetzesentwurfs geht hingegen aufgrund der Angaben eines großen Telekommunikationsanbieters davon aus, dass der zusätzliche Investitionsaufwand nicht erheblich sein wird (*vgl. Begründung zum Referentenentwurf, S. 71*).

zu 9) werden durch die neue Gesetzeslage gezwungen, das Betreiben ihrer Anonymisierungsdienste aufzugeben.

Die im § 113b TKG und den jeweiligen speziellen Gesetzen vorgesehene Pflicht zur Weiterleitung der gespeicherten Daten ist ebenfalls als Eingriff in die Unternehmensfreiheit der Beschwerdeführerin zu 9) zu qualifizieren.

Der Eingriff in die Unternehmensfreiheit der Beschwerdeführerin zu 9) wird besonders dadurch intensiviert, dass das Gesetz keine Entschädigung für die entstehenden hohen Kosten vorsieht[164]. Dabei ist zu berücksichtigen, dass der Deutsche Bundestag die Bundesregierung ausdrücklich aufgefordert hat, zeitnah einen Gesetzesentwurf für eine angemessene Entschädigung der Telekommunikationsunternehmen für die Inanspruchnahme im Rahmen der Erfüllung hoheitlicher Ermittlungsmaßnahmen im Bereich der Telekommunikation vorzulegen[165]. Dies ist bis heute nicht geschehen.

b) Ausübende von Vertrauensberufen wie Rechtsanwalt, Arzt, Psychotherapeutin, Steuerberater

Eine vollständige Speicherung und Weitergabe der elektronischen Kontakte beeinträchtigt die Beschwerdeführer zu 2), 5), 7), 8) und 10) in ihrer Berufsausübung.
Zwischen Rechtsanwälten, Ärzten, Psychotherapeuten, Steuerberatern und ihren jeweiligen Mandanten bzw. Patienten besteht ein besonderes Vertrauensverhältnis. Dieses entsteht bereits mit der Anbahnung des Erstkontaktes und besteht während der gesamten Zeit der Beratung und Begleitung. Gegenstand der Arbeit sind sensible persönliche Lebensumstände. Dabei geht es um die finanzielle Situation des Mandanten bzw. Patienten, um seine sozialen Kontakte und (Rechts-)Beziehungen zu anderen Personen, seine Krankheiten körperlicher oder seelischer Art, mithin einen wesentlichen Teil seiner Persönlichkeit. Die Offenlegung dieser Daten kann zu gesellschaftlicher Ausgrenzung führen. Sie werden mit Dritten ausschließlich unter der Voraussetzung absoluter Vertraulichkeit sowohl des Kontaktes als auch des Inhaltes der Kontakte besprochen. Bereits aus dem Kontakt mit einem der Beschwerdeführer lassen sich Rückschlüsse auf den Inhalt des Kontaktes ziehen. Dadurch wird sowohl die Gewinnung von Mandanten bzw. Patienten als auch deren Betreuung schwerwiegend beeinträchtigt. Somit sind die Beschwerdeführer zu 2), 5), 7), 8) und 10) in ihrer Berufsfreiheit betroffen.

---

[164] Bemerkenswert ist diesbezüglich, dass der ursprüngliche Richtlinienentwurf eine Entschädigung vorsah, die bei den späteren Beratungen entfallen ist. Vgl. dazu *Köcher/Kaufmann*, DuD 2006, S. 360 (364).
[165] Vgl. BT-Drs. 16/545, S. 4.

2. Unverhältnismäßigkeit der Speicherungs- und Weiterleitungspflicht

a) Verfassungswidrigkeit des § 113a Abs. 1 bis 5, 10 und 11 TKG sowie des § 113b TKG wegen mangelnder Entschädigung für die zur Speicherung und Weitergabe verpflichteten Telekommunikationsdienstanbieter

Die Regelungen des § 113a Abs. 1 bis 5, 10 und 11 TKG sind unverhältnismäßig. Die darin vorgesehene Speicherungs- und Weiterleitungspflicht belastet die Beschwerdeführerin zu 9) übermäßig. Durch die angegriffenen Normen wird sie vom Staat zur Erfüllung von öffentlichen Aufgaben in Dienst genommen, ohne dass sie einen Ausgleich für die erlittenen wirtschaftlichen Nachteile erhalten. Als Telekommunikationsdiensteanbieter benötigen sie die zu speichernden Daten nicht für eigene Zwecke, sondern sind in der Regel bemüht, die Daten zur Entlastung schnellstmöglich zulöschen.

Der Begründung zum Gesetzes sowie den Protokollen der Debatten im Deutschen Bundestag ist nicht zu entnehmen, dass sich der Gesetzgeber ernsthaft mit der Entschädigungsfrage beschäftigt hat. In der Begründung wird pauschal davon ausgegangen, dass die entstehenden Investitionskosten „voraussichtlich nicht so erheblich sein" werden [166]. Diese unrealistische Vermutung wird allerdings weder belegt noch begründet. Der Verzicht auf eine Entschädigungsregelung wird mit praktischen Problemen bei der Ermittlung der entstehenden Kosten, mit der Überwälzbarkeit der Zusatzkosten auf die Telekommunikationsnutzer sowie mit dem Verweis auf ähnliche verfassungsrechtlich nicht unbedenkliche Konstellationen (§ 9 Geldwäschegesetz), bei denen Aufwendungen für Speicherungspflichten nicht erstattet werden, begründet[167]. Dies kann nicht überzeugen.

Die eventuellen Probleme bei der Feststellung der durch die Speicherungspflicht entstehenden Kosten können den Gesetzgeber nicht von seiner rechtstaatlichen Verpflichtung befreien, bei Schaffung von Regelungen, die intensive Grundrechtseingriffe darstellen, die zugänglichen Informationsquellen zur Einschätzung der Belastung der Betroffenen hinzuziehen. Das Argument der Überwälzbarkeit der Kosten auf die Kunden ist ebenfalls nicht stichhaltig, weil die erhöhten Entgelte für die Nutzung der jeweiligen Telekommunikationsdienste zum Kundenverlust führen könnten und daher den Anbietern nicht zumutbar sind[168]. Der Verweis auf § 9 Geldwäschegesetz ist auch nicht tauglich, die fehlende Entschädigungsregel bezüglich der staatlich angeordneten Vorratsdatenspeicherung zu rechtfertigen. Diese Rechtsnorm ist eher als eine bedenkliche

---

[166] Begründung zum Gesetzesentwurf, S. 62.
[167] Begründung zum Gesetzesentwurf, S. 62.
[168] *Zur Untauglichkeit des Argument der Überwälzbarkeit vgl. BVerfGE 58, 137 (151f.).*

Ausnahme vom Prinzip einer Vollentschädigung bei Indienstnahme Privater zur Erfüllung öffentlichen Aufgaben zu qualifizieren[169].

Zu bemerken ist auch, dass die umfassende Vorratsspeicherungspflicht möglicherweise bedeutende negative Auswirkungen auf die gesamte deutsche Telekommunikationswirtschaft haben wird, da sie ihre Wettbewerbsfähigkeit im Vergleich zu Ländern, in denen keine solche Pflicht besteht bzw. eine Entschädigung vorgesehen ist, erheblich schwächt.

Jedenfalls stellt die Verpflichtung der Beschwerdeführerin zu 9) zur Speicherung und Weitergabe von Verkehrsdaten ohne eine Entschädigung für die daraus entstehenden Zusatzkosten und für die sonstigen wirtschaftlichen Nachteile eine unverhältnismäßige Einschränkung ihrer Unternehmensfreiheit dar und ist somit verfassungswidrig. Ein Blick ins Ausland zeigt, dass die Verfassungsgerichte von Österreich und Frankreich schon in diesem Sinne entschieden haben[170].

b) Verstoß gegen Bestimmtheitsgebot bei der Regelung über die Adressaten der speicherungspflichtigen Anbieter, § 113a Abs. 1 Satz 1 TKG

In § 113a Abs. 1 Satz 1 TKG wird der Kreis der zur Speicherung Verpflichteten festgelegt. Danach sind zur Speicherung im Inland oder in einem anderen Mitgliedsstaat der Europäischen Union diejenigen verpflichtet, die Telekommunikationsdienste für Endnutzer erbringen. Gespeichert werden müssen nur Verkehrsdaten, die vom jeweiligen Dienstanbieter bei der Nutzung seines Dienstes erzeugt oder verarbeitet werden. Für die Anbieter, die Telekommunikationsdienste erbringen, ohne selbst Verkehrsdaten zu erzeugen oder zu verarbeiten, besteht die Pflicht, die Speicherung sicherzustellen (§ 113a Abs. 1 S. 2 TKG). Bei der Festlegung der Adressaten der Speicherungspflicht werden zahlreiche unbestimmte Begriffe verwendet. Damit wird dem Bestimmtheitsgebot nicht ausreichend Rechnung getragen.

Bei der Rechtsanwendung können durchaus Zweifel entstehen, ab wann von einer „Erzeugung" und „Verarbeitung" von Daten ausgegangen wird. Vergleichbare Anwendungsschwierigkeiten gab es beispielsweise beim Streit darum, ob der Mautsystembetreiber Toll Collect GmbH Telekommunikationsdienste im Sinne des TKG erbringt und dementsprechend Normadressat des §100g StPO wäre[171]. Vergleichbare Streitfälle werden mit dem novellierten TKG nicht beseitigt, sondern eher noch verstärkt.

In der Begründung zu den hiermit angegriffenen Regelungen wird zum Begriff des „Verarbeitens" erklärt, dass er weit zu verstehen sei und etwa auch die Fälle erfasse, in denen ein Mobilfunknetzbetreiber die von einem Teilnehmer eines anderen Netzbetreibers initiierte

---

[169] Kirchner, Stellungnahme, Rechtsausschuss des Deutschen Bundestages, Zusammenfassung der Stellungnahmen zur öffentlichen Anhörung am 21. September 2007, S. 100.

[170] *Conseil constitutionnel*, DC 2000-441 vom 28.12.2000; *Österreichischer Verfassungsgerichtshof*, G 37/02-16 vom 27.02.2003.

[171] Vgl. *Fraenkel/Hammer*, DuD 2006, S. 499f.

Verbindung „übernimmt" und die Verbindung zu seinem eigenen Endnutzer herstellt[172]. Welche anderen Leistungen noch unter dem Begriff des „Verarbeitens" in Zusammenhang mit der Vorratsdatenspeicherung zu subsumieren wären, ist offen. Die Beschwerdeführer zu 9) und 12) können den genauen Umfang ihrer Speicherungspflicht dem Gesetz nicht entnehmen. Das Rechtsklarheitsprinzip wird hiermit verletzt.

Zu bemerken ist außerdem, dass die geplante Regelung keine Begrenzung der Speicherungspflicht auf solche Betreiber vorsieht, die Telekommunikationsdienste geschäftsmäßig erbringen oder daran mitwirken. Dabei bleibt unklar, ob auch Privatpersonen zur Speicherung verpflichtet sind, wenn sie kostenlos einen öffentlichen WLAN-Zugang, einen E-Mail-Dienst oder Ähnliches anbieten.

Vor diesem Hintergrund ist anzunehmen, dass es in der Praxis zu zahlreichen Anwendungsproblemen kommen wird, da die Adressaten der Speicherungspflicht nicht hinreichend bestimmt sind. Die Anforderungen des rechtstaatlichen Bestimmtheitsgebots, wonach der Umfang und die Voraussetzungen der Einschränkungen sich klar aus dem Gesetz ergeben müssen, werden durch die Normen über die Festlegung der Adressaten der Speicherungspflicht nicht eingehalten.

c) Verstoß gegen Art. 12 Abs. 1 S. 1 GG wegen des praktischen Verbots der Anonymisierungsdienste

Das Gesetz regelt eine Speicherungspflicht auch derjenigen, die so genannte Anonymisierungsdienste betreiben und anbieten (vgl. § 113a Abs. 6 TKG)[173]. Darunter werden Programme verstanden, die Internetverbindungen durch ein verteiltes Netz von Servern leiten. Durch die Nutzung von mehreren Servern kann die Quelle einer Nachricht derart verschleiert werden, dass die Identität des Nutzers nicht mehr feststellbar ist[174]. Ist sowohl die Eingabe vor Anonymisierung als auch das Ergebnis der Anonymisierung zu speichern, können die anonymisierten Daten anhand der Originaleingaben jederzeit rekonstruiert und bestimmten Personen zugeordnet werden. Von einer Anonymisierung der Daten kann dann nicht mehr gesprochen werden. Damit werden die bisher zulässigen Anonymisierungsdienste faktisch verboten.

Dem Wortlaut des relevanten § 113a Abs. 6 TKG ist allerdings nicht direkt zu entnehmen, dass die Anonymisierungsdienste darunter zu subsumieren sind. In der Begründung zu dieser Regelung im Gesetzes wird ausgeführt, dass die Anbieter von Anonymisierungsdiensten öffentlich zugängliche Telekommunikationsdienste im Sinne von § 3 Nr. 24 TKG erbringen und daher von der Speicherungspflicht betroffen seien. Die Anonymisierungsdienste wiesen eine Doppelnatur auf, da ihre Tätigkeit sowohl in der Durchleitung der Nachricht als auch in der Ersetzung der Ausgangskennung des Telekommunikationsnutzers besteht. Diese Dienste seien daher sowohl

---

[172] BTDrs. 16/5846, Begründung zum Regierungsentwurf, S. 69.
[173] Vgl. BTDrs. 16/5846, Begründung zum Regierungsentwurf, S. 71.
[174] Vgl. Spindler/ Schmitz/ Geis, TDG-Kommentar, München 2004, S. 292f.

Telemedien als auch Telekommunikationsdienste[175]. Die Rechtsfolge wäre, dass mit § 113a Abs. 6 TKG die Anonymisierungsdienste praktisch verboten werden. Wenn die Anbieter von Internetanonymisierungsdiensten die entsprechenden in § 113a TKG aufgelisteten Daten, also auch alle in der Kette der Anonymisierung vergebenen IP-Adressen, speichern sollen, bedeutet dies praktisch, dass eine „Re-Anonymisierung" möglich sein soll.

Dazu ist zu bemerken, dass eine Speicherungspflicht für Betreiber von Anonymisierungsdiensten sich nicht unmittelbar aus der Richtlinie 2006/24/EG ergibt. Die Richtlinie bezieht sich lediglich auf elektronische Telekommunikationsdienste, nicht aber auf Teledienste, wozu Anonymisierungsdienste bisher gezählt werden. Sie gilt für Verkehrs- und Standortdaten sowie für alle damit in Zusammenhang stehenden Daten, die zur Feststellung der Benutzer erforderlich sind (Art. 1 Abs. 2 RL). Art. 5 RL regelt die Daten, die vorrätig gespeichert werden müssen und unterteilt sie in die Kategorien Telefonnetz, Mobilfunk, Internetzugang, Internet-E-Mail und Internet-Telefonie. Die Anonymisierungsdienste können ihrer Natur nach von keiner dieser Datenkategorien erfasst sein. Insoweit geht eine Verpflichtung zur Vorratsdatenspeicherung für die Anbieter solcher Dienste über die Anforderungen der Richtlinie hinaus.

Außerdem stellen die Anonymisierungsdienste keine Telekommunikationsdienste, sondern Telemedien dar. Gemäß § 1 Abs. 1 TMG sind die Telemedien „alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht Telekommunikationsdienste nach § 3 Nr. 24 des Telekommunikationsgesetzes, die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen, telekommunikationsgestützte Dienste nach § 3 Nr. 25 des Telekommunikationsgesetzes oder Rundfunk nach § 2 des Rundfunkstaatsvertrages sind". Die Zuordnung der Anonymisierungsdienste zu den Telemedien ist dadurch begründet, dass bei Ihnen die Umschreibung der IP-Adressen auf der Anwendungsebene und nicht auf der Ebene des Transportprotokolls stattfindet. Da die Verschlüsselung der Inhalte und die Tarnung der IP-Adressen auf der Inhaltsebene erfolgt, entsteht die Gefahr, dass Telekommunikationsinhalte bekannt werden, was der Intention des Richtlinien- und des Gesetzgebers widerspricht[176].

Auch wenn man sich der Begründung des Gesetzes anschließt und die Anonymisierungsdienste auch als Telekommunikationsdienste einstuft, stellt sich erneut die Frage nach der Geeignetheit und Verhältnismäßigkeit des § 113 Abs. 6 TKG zur Erreichung der angestrebten Ziele. Da bei der Anonymisierung eine Kaskade von zahlreichen Telekommunikationsvorgängen entsteht, an der viele selbständige Betreiber beteiligt sind, wäre eine Prüfung der bei jedem einzelnen Teilnehmer gespeicherten Daten notwendig. Der für diese Datensammlung und -auswertung erforderliche Aufwand würde enorm groß sein. Zudem wiegt die Beeinträchtigung des Art- 12 Abs. 1 GG relativ schwer. Das faktische Verbot der Anonymisierung führt dazu, dass die Nutzung dieses Dienstes stark zurückgehen wird. Dies führt zu einer erheblichen und dauerhaften Beeinträchtigung der Berufsfreiheit. Zudem werden Berufsgruppen, die ausschließlich Anonymisierungsdienste anbieten unangemessen betroffen. Für sie kommt die Belastung einem Berufsverbot nahe. Dazu kommt,

---

[175] BTDrs. 16/5846, Begründung zum Regierungsentwurf, S. 72.

[176] Vgl. Stellungnahme des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein vom 27.06.2007, S. 22.

dass Anonymisierungsdienste eine gesellschaftlich wünschenswerte Funktion erfüllen. Der einzelne Nutzer kann sich ohne Angst vor staatlicher Beobachtung politisch und gesellschaftlich betätigen.

Außerdem steht das Gesetz nicht im Einklang mit der geltenden Rechtslage, wonach die Anbieter von Telemedien verpflichtet sind, den Nutzern die Inanspruchnahme sowie die Bezahlung von Diensten anonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist (vgl. § 13 Abs. 6 Telemediengesetz (TMG), früher § 4 Abs. 6 TDDSG).

d) Unverhältnismäßigkeit der Regelungen für Berufsgeheimnisträger

Die Regelungen des § 113a Abs. 1 bis 5, 10 und 11 TKG sind unverhältnismäßig. Sie belasten die Beschwerdeführer zu 2), 5), 7), 8) und 10) übermäßig.

Die vollumfängliche Speicherung führt zur Erfassung jeder Kontaktaufnahme via elektronischer Kommunikationsmittel. Diese Art der Kommunikation ist für die wirksame Arbeit der Beschwerdeführer nicht durchgängig durch persönliche Treffen ersetzbar. In der Arbeit mit Mandanten bzw. Patienten geht es oftmals um akute Situationen, die eine Hilfeleistung erforderlich machen. Diese Hilfe kann nur durch die schnelle Erreichbarkeit der Beschwerdeführer via elektronischer Kommunikationsmittel geleistet werden.

Des Weiteren erfolgt auch die Terminvergabe zum größten Teil mittels elektronischer Kommunikationsmittel. Dass Mandanten bzw. Patienten in der Folge von einer Kontaktaufnahme gänzlich absehen, erscheint mehr als wahrscheinlich. Dadurch, dass der Sensibilität der Daten keine Rechnung getragen wird, geht ein Verlust an Mandaten bzw. Patienten einher. Die Arbeit von Berufsgeheimnisträgern ist gerade darauf angelegt, Menschen zu unterstützen, die mit gesellschaftlich nicht akzeptierten Problemen kämpfen. Berufsgeheimnisträger können ihnen z.B. ein rechtsstaatliches Verfahren garantieren bzw. ihnen zur Linderung körperlicher und seelischer Schmerzen verhelfen. Können Berufsgeheimnisträger diese Funktion nicht garantieren, verlieren sie ein bestimmendes Merkmal ihrer Arbeit. In Konsequenz werden sie auch Mandanten bzw. Patienten verlieren, die auf diesen Faktor angewiesen sind. Zumindest wird deren Betreuung mit hoher Intensität gestört.

Daher ist es nicht angemessen, dass § 113a Abs. 1 bis 5, 10 und 11 TKG keine Ausnahmeregelung für Berufsgeheimnisträger vorsieht. Die dadurch bewirkte Beeinträchtigung der Berufsfreiheit der Beschwerdeführer zu 2), 5), 7), 8), zu 10) ist unverhältnismäßig.

3. Ergebnis

Eine Verletzung der Berufsfreiheit der Beschwerdeführer zu 2), 5), 7), 8), 9), 10) liegt vor.

IV. Verletzung der Pressefreiheit, Art. 5 Abs. 1 S. 2 GG

Die Beschwerdeführerin zu 6) rügt eine Verletzung der Pressefreiheit (Art. 5 Abs. 1 S. 1 GG). §§ 113a, 113b TKG und 100g StPO verletzen ihre Pressefreiheit, da sie ihre Tätigkeit als Pressejournalistin durch die Aushebelung des Informantenschutzes unangemessen beeinträchtigt. (Im vorliegenden Fall wird die Berufsfreiheit durch die Pressefreiheit als spezielleres Grundrecht verdrängt. Die Pressefreiheit schützt vor allem die Voraussetzungen, die gegeben sein müssen, damit die Presse ihre Aufgabe im Kommunikationsprozess erfüllen kann[177].) Für den Fall, dass das Gericht die Pressefreiheit als nicht einschlägig ansieht, macht die Beschwerdeführerin zu 6) hilfsweise eine Verletzung ihrer Berufsfreiheit geltend.

1. Schutzbereich und Eingriff

Gegenstand der Pressefreiheit des Art. 5 Abs. 1 S. 2 Alt. 1 GG ist jede Tätigkeit, die darin besteht, Nachrichten zu beschaffen und zu sammeln, um Druckwerke herzustellen und zu veröffentlichen. Sie ist ein Recht des Einzelnen, Pressetätigkeit ohne staatliche Einflussnahme auszuüben[178]. Die Reichweite der Pressefreiheit reicht von der Beschaffung der Informationen bis zur Verbreitung der Nachrichten und Meinungen[179]. Geschützt ist insbesondere die Vertraulichkeit der Redaktionsarbeit sowie das Vertrauensverhältnis zwischen den Pressejournalisten und ihren Informanten[180]. Art. 5 Abs. 1 S. 2 GG enthält auch eine objektive Einrichtungsgarantie und gewährleistet das Institut der freien Presse[181].

Träger der Pressefreiheit sind alle Personen und Unternehmen, die produktiv an der geistig-inhaltlichen Pressearbeit teilnehmen[182]. Dazu gehören Verleger, Redakteure, Herausgeber, Journalisten, also auch der Beschwerdeführerin zu 6).

Mit dem Inkrafttreten des Gesetzes zur Umsetzung der Vorratsdatenspeicherungsrichtlinie erhalten die staatlichen Stellen potentielle Zugriffsmöglichkeit auf alle telekommunikationsbezogenen Kontakte eines jeden Journalisten. „So könnte in Zukunft praktisch jede Veröffentlichung von Insiderinformationen zur Überprüfung der kompletten elektronischen Kontakte des Autors für das jeweils vergangene halbe Jahr führen. Die Abschreckungswirkung für potentielle Informanten ist offensichtlich. Ihnen bliebe kaum noch eine Möglichkeit vertraulicher Kontaktaufnahme mit Journalisten. Das Vertrauensverhältnis zwischen Informanten und Presse, ohne das die Pressefreiheit in einer Vielzahl für die Demokratie äußerst bedeutsamer Fälle

---

[177] Bethge, in: M. Sachs (Hrsg.), Grundgesetz-Kommentar, Art. 5, Rn. 89.
[178] Fechner, Medienrecht, S. 154.
[179] BVerfGE 20, 162 (176).
[180] BVerfGE 36, 193 (204); 66, 116 (133).
[181] BVerfGE 20, 162 (175); 80, 124 (133).
[182] BVerfGE 21, 271 (277f.).

weitgehend leer läuft, wird so strukturell und flächendeckend beschädigt"[183]. Somit wird in die Pressefreiheit der Beschwerdeführerin zu 6) eingegriffen.

2. Unverhältnismäßigkeit der angegriffenen Normen

Der Eingriff in die Pressefreiheit der Beschwerdeführerin zu 6) ist nicht angemessen. Schon der Eingriff durch die in § 113a TKG vorgesehene Erhebung und vorrätige Speicherung der Verbindungsdaten der Journalisten beeinträchtigt die Pressefreiheit unverhältnismäßig stark.

Das Demokratieverständnis des Grundgesetzes beruht auf der Anerkennung des politischen Gewichts der Meinung des Einzelnen. Der freie Meinungskampf ist ein „konstituierendes Element" der freiheitlich-demokratischen Staatsform [184]. Dafür ist die Existenz einer freien Presse unentbehrlich. Das Bundesverfassungsgericht betont in seiner Rechtsprechung die Bedeutung der freien Wahrnehmung der politischen Grundrechte, insbesondere der Meinungs- und Pressefreiheit für das Funktionieren des demokratischen Staates. Ohne die Gewährleistung des Informantenschutzes ist diese freie Wahrnehmung praktisch unmöglich. Das Wissen, dass jede Kontaktaufnahme zu einem Journalisten zurückverfolgt und bewertet werden kann, führt zwangsläufig zu psychologischen Hemmungen bei den potentiellen Informanten. Die vorrätige Speicherung aller Verbindungsdaten beschädigt daher dauerhaft das Vertrauensverhältnis zwischen Informanten und Journalisten. Dafür gibt es zahlreiche Beispiele aus Ländern (wie z.B. Belgien), die die Vorratsdatenspeicherung bereits eingeführt haben. Dort hat der Abschreckungseffekt der Vorratsdatenspeicherung zum Verlust zahlreicher Informationsquellen geführt, was die freie Pressebetätigung erheblich beeinträchtigt.

Die Speicherung der Verbindungsdaten schafft Möglichkeiten zur Identifikation des Informanten und zur Ausforschung der Inhalte seiner Mitteilungen. Die Journalisten und ihre Informanten sind gezwungen, elektronische Kommunikation zu vermeiden, was die Kontaktaufnahme zwischen ihnen sehr aufwendig macht. Auf diese Weise wird die Aufdeckung von Fehlentwicklungen in Staat und Gesellschaft sowie der öffentliche Diskurs insgesamt eingeschränkt.

Die Zugriffsmöglichkeiten seitens zahlreicher staatlicher Stellen intensivieren den Eingriff in die Pressefreiheit der Beschwerdeführerin zu 6) immens. Insbesondere die unzureichende Begrenzung der Verwendung der gespeicherten Daten und die Befugnis der Nachrichtendienste darauf zuzugreifen, zwingen sie einerseits zu Autozensur und erschweren andererseits die Möglichkeiten zur vertraulichen Kontaktaufnahme zu verlässlichen Informanten.

Der zweifelhafte Nutzen der vorrätig gespeicherten Verbindungsdaten für die Zwecke der Strafverfolgung und der Aufgabenerfüllung der Nachrichtendienste können den intensiven Eingriff in die Pressefreiheit der Beschwerdeführerin zu 6) nicht rechtfertigen. Die Regelungen über die Benachrichtigung von Journalisten, auf deren elektronische Kommunikation zugegriffen wurde,

---

[183] ARD/BDZV/DJV/Deutscher Presserat/VDZ/Ver.di/VPRT/ZDF, Stellungnahme, Rechtsausschuss des Deutschen Bundestages, Zusammenfassung der Stellungnahmen zur öffentlichen Anhörung am 21. September 2007, S. 51.

[184] BVerfGE 7, 198 (208).

sind ebenfalls unzureichend, um die intensive Beeinträchtigung der Pressefreiheit durch die Vorratsdatenspeicherung auszugleichen.

V. Verletzung der Religionsfreiheit, Art. 4 Abs. 1 GG

Der Beschwerdeführer zu 4) rügt die Verletzung der Glaubens- und Gewissensfreiheit gemäß Art. 4 Abs. 1 GG. §§ 113a, 113b TKG und 100g StPO verletzen seine Glaubens- und Gewissensfreiheit, da seine Tätigkeit als Geistlicher sowie als kirchlicher Beauftragter für Kriegsdienstverweigerer durch die Aushebelung der Anonymität seiner Kontakte unangemessen beeinträchtigt wird.

1. Schutzbereich und Eingriff

Den unmittelbaren Gegenstand der Grundrechtsgarantie bilden diejenigen Elemente, mit denen sich der Grundrechtsträger für seine Existenz als moralisches Wesen maßgebend identifiziert. Die Freiheit der Bildung von Glaubensvorstellungen oder Gewissensentscheidungen ist ebenso geschützt wie die der individuellen Religionsentwicklung dienenden Kontakte mit dem Beichtvater bzw. Geistlichen. Die Geheimheit dieser Kontakte wird aufgrund der Vorratsdatenspeicherung nicht mehr gewährleistet.
Werden die Kommunikationsdaten des Geistlichen staatlich erfasst, wird damit die Möglichkeit anonymer Kontaktaufnahme vereitelt. Soll dieser Kontakt wirksam geschützt sein, muss er auch die Vertraulichkeit auf der Seite des Beichtvaters gewährleisten können. Anderenfalls liefe diese Schutzdimension leer. Zudem wird die Verkündung des Glaubens und den daraus persönlich für richtig erkannten Verhaltensweisen sowie die daraus folgende Hilfestellung und Unterstützung für Hilfesuchende erheblich erschwert. Indem der Staat diese Tätigkeiten beobachtet, greift er in die Schutzdimension des Art. 4 Abs. 1 GG ein.

2. Unverhältnismäßigkeit der angegriffenen Normen

Die Schwere dieses Eingriffs steht außer Verhältnis zu dem mit ihm verfolgten Zweck. In Frage stehen hier zwei betroffene Dimensionen des Art. 4 Abs. 1 GG. Einerseits das Recht des Geistlichen auf ungestörte Ausübung seiner aus dem Glauben folgenden Handlungen, kirchenintern und kirchenextern. Zudem ist das Recht des Einzelnen betroffen, einen Glauben bzw. Weltanschauung zu bilden und auszuüben. Zur Glaubensbildung notwendig sind Anlaufstellen, die dem Einzelnen Hilfestellung geben. Der erste Kontakt erfolgt dabei meist telefonisch – gerade weil ein hohes Maß an Anonymität gesichert bleiben soll. Dies ist dem Umstand geschuldet, dass vor dem Moment des Bekenntnisses zu einer bestimmten Weltanschauung eine hohe Hemmschwelle besteht. Möglicherweise wäre ein offenes Bekenntnis

sogar mit negativen Folgen verbunden. Aus der negativen Religionsfreiheit folgt daher, dass der Einzelne seine Sympathien zu bestimmten Weltanschauungen nicht offen legen muss. Sind die Kontaktaufnahmen nun aber nachvollziehbar, wird dieser Schutz ausgehöhlt. Dabei ist insbesondere die hohe Schutzwürdigkeit von Daten aus dem Bereich des genuin privaten zu beachten. Dazu gehört, das Haben einer Weltanschauung für sich und geheim zu (be)halten.
Ebenso schwer wiegt die Behinderung der Pflege und Förderung des Bekenntnisses und Glaubens, also die Behinderung der Organisationen und Institutionen in denen der Einzelne glaubt. Die Tätigkeit als Geistlicher, die Betreuung von Gemeindegliedern wie auch Bekannten setzt den Einsatz eines elektronischen Kommunikationsmittels voraus. Die Organisation des Gemeindelebens und die Betreuung der Mitglieder allein durch Hausbesuche ist nicht nur bei großen Kirchen faktisch nicht möglich. Kann eine derart wesentliche Tätigkeit nicht mehr unbeobachtet durchgeführt werden, verliert die in Art. 4 Abs. 1 GG verbürgte Ausübungsfreiheit ihren Wert. Aufgrund der großen Sensibilität der Daten und der schwer wiegenden Auswirkungen ihrer Offenlegung für die persönliche Lebensgestaltung des Betroffenen ist die Speicherung der Kommunikationsdaten Geistlicher unverhältnismäßig.

VI. Verletzung des Gebots effektiven Rechtsschutzes, Art. 19 Abs. 4 GG und des Anspruchs auf rechtliches Gehör, Art. 103 Abs. 1 GG

Die Regelung über die Benachrichtigung, § 101 Abs. 1, Abs. 4 S. 1 Nr. 6, S. 3 StPO, verstößt gegen Art. 19 Abs. 4 GG und Art. 103 Abs. 1 GG. Sie nimmt den Betroffenen die Möglichkeit, über eine Rechtsverletzung durch die öffentliche Gewalt eine Entscheidung durch ein deutsches Gericht herbeizuführen. Nach § 101 Abs. 4 S. 1 StPO kann die Benachrichtigung ohne richterliche Zustimmung vollständig unterbleiben, wenn ein Beteiligter der betroffenen Kommunikation (vgl. § 101 Abs. 4 S. 1 StPO) „nur unerheblich betroffen wurde und anzunehmen ist, dass [er] kein Interesse an einer Benachrichtigung hat". Eine Regelung, die dem Betroffenen die Kenntnis eines Grundrechtseingriffs vorenthält, sorgt dafür, dass die Beschreitung des Rechtswegs faktisch nicht möglich ist. Gleichzeitig besteht an der Feststellung, dass ein Grundrechtseingriff stattgefunden hat immer ein berechtigtes Interesse. Voraussetzung für diese Feststellung ist aber zwingend die Kenntnis der Maßnahme. Das Unterbleiben der Benachrichtigung ist daher verfassungswidrig. Zumindest ist es nicht hinnehmbar, dass die zu treffende Einschätzung ohne richterliche Überprüfung bleibt, sondern allein von der Exekutive angeordnet wird. Zudem genügt die Vorschrift mit den entscheidenden Formulierungen „unerheblich" und „anzunehmen" nicht dem Bestimmtheitsgebot.

VII. Verletzung der Allgemeinen Handlungsfreiheit, Art. 2 Abs. 1 GG

Die Beschwerdeführerin zu 1) rügt eine Verletzung ihrer Allgemeinen Handlungsfreiheit, Art. 2 Abs. 1 GG. Sie ist durch §§ 113a, 113b TKG und 100g StPO in ihrem Grundrecht verletzt, da sie in ihrer Vereinstätigkeit unangemessen beeinträchtigt wird. Diese besteht allgemein darin, politische Partizipation zu fördern, staatliche Betätigungen zu hinterfragen, gesellschaftliche Phänomene kritisch zu begleiten sowie Minderheiten eine Stimme zu verleihen. Zweck der Tätigkeiten ist die Stärkung demokratischer Prozesse und das Fördern des für die Demokratie konstituierenden Wettbewerbs konkurrierender Meinungen. Diese Betätigung bedarf der elektronischen Kommunikation, da sie auf Hinweise von Informationsgebern angewiesen ist. Dabei besteht die Gefahr, dass die Identität der Kommunikationsteilnehmer von staatlichen Organen aufgedeckt wird. Dies führt zu einem Rückgang dieser Informationen. Aufgrund der Notwendigkeit der Informationsgewinnung für seine Tätigkeit wird der Verein schwerwiegend beeinträchtigt.

Daraus folgt zugleich auch, dass die Humanistische Union e.V. selbst nicht mehr zeitnah auf gesellschaftliche Ereignisse reagieren kann. Diese Beeinträchtigung wiegt angesichts des Vereinszwecks und der fehlenden Ausweichmöglichkeiten zu seiner Erreichung schwer.

Des Weiteren betreibt die Humanistische Union e.V. selbst einen kostenfrei zugänglichen Anonymisierungsserver. Damit soll ein Mittel zu unbefangener Kommunikation bereitgestellt werden, dessen Gebrauch jedem offen steht. Dies unterstützt die Arbeit der Humanistischen Union e.V., die Mitwirkung eines möglichst großen Teilnehmerkreises an der öffentlichen Auseinandersetzung zu erreichen. Die dabei anfallenden Daten sind nun zu speichern. Zusätzlich zur damit einhergehenden Beeinträchtigung des Vereinszwecks bindet die Speicherung Finanzmittel und Personal eines Vereins ohne kommerzielle Struktur übermäßig. Somit sind die Eingriffe in die allgemeine Handlungsfreiheit, Art. 2 Abs. 1 GG nicht zumutbar.

Prof. Dr. Rosemarie Will
– Bevollmächtigte –