cylaw tu-darmstadt

TECHNISCHE UNIVERSITÄT DARMSTADT

(Cyber)Law – Klausurhilfsmittel

KW 5/2018

Jean Monnet Centre of Excellence
EU IN GLOBAL DIALOGUE (CEDI)

Co-funded by the Erasmus+ Programme of the European Union

JOHANNES GUTENBERG UNIVERSITÄT MAINZ

JG|U

Technische Universität Darmstadt
Fachgebiet Öffentliches Recht
Prof. Dr. Viola Schmid, LL.M. (Harvard)
Hochschulstraße 1
64289 Darmstadt
schmid@cylaw.tu-darmstadt.de

Stand: Wintersemester 2017/2018

Inhaltsverzeichnis

Diese Edition des Cyberlaw-Texts (Edition X-Klausurhilfsmittel) ist das Ergebnis eines engagierten Time-Managements. Auf das Geleit zur Edition X der KW 51/2017 wird vollinhaltlich Bezug genommen. Erstmals wird für die Klausur eine eigene Klausurhilfsmittelversion erstellt und angeboten, die alleine zugelassen wird. Die allgemeinen Hinweise zum Umgang mit Klausurhilfsmitteln werden als bekannt vorausgesetzt. Der Ausdruck erfolgt – wie bekannt gegeben – durch die Studierenden.

Die Gesetzestexte sind eigenständig kompiliert. Gekürzte Passagen sind mit [...] gekennzeichnet.

Teil 1: Normgebung

I. Nationales Primärrecht – Grundgesetz (GG)[1]

Art. 1 – Schutz der Menschenwürde, Menschenrechte, Grundrechtsbindung

(1) Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.

(2) Das Deutsche Volk bekennt sich darum zu unverletzlichen und unveräußerlichen Menschenrechten als Grundlage jeder menschlichen Gemeinschaft, des Friedens und der Gerechtigkeit in der Welt.

(3) Die nachfolgenden Grundrechte binden Gesetzgebung, vollziehende Gewalt und Rechtsprechung als unmittelbar geltendes Recht.

Art. 2 – Freie Entfaltung der Persönlichkeit, Recht auf Leben, körperliche Unversehrtheit, Freiheit der Person

(1) Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.

(2) Jeder hat das Recht auf Leben und körperliche Unversehrtheit. Die Freiheit der Person ist unverletzlich. In diese Rechte darf nur auf Grund eines Gesetzes eingegriffen werden.

Art. 3 – Gleichheit vor dem Gesetz

(1) Alle Menschen sind vor dem Gesetz gleich.

[...]

Art. 10 – Brief-, Post- und Fernmeldegeheimnis

(1) Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich.

(2) Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden. Dient die Beschränkung dem Schutze der freiheitlichen demokratischen Grundordnung oder des Bestandes oder der Sicherung des Bundes oder eines Landes, so kann das Gesetz bestimmen, daß sie dem Betroffenen nicht mitgeteilt wird und daß an die Stelle des Rechtsweges die Nachprüfung durch von der Volksvertretung bestellte Organe und Hilfsorgane tritt.

Art. 13 – Unverletzlichkeit der Wohnung

(1) Die Wohnung ist unverletzlich.

[1] Grundgesetz für die Bundesrepublik Deutschland in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, das zuletzt durch Art. 1 des Gesetzes vom 13. Juli 2017 (BGBl. I S. 2347) geändert worden ist; http://www.gesetze-im-internet.de/gg/index.html#BJNR000010949BJNE010200314 (08.11.2017).

(2) Durchsuchungen dürfen nur durch den Richter, bei Gefahr im Verzuge auch durch die in den Gesetzen vorgesehenen anderen Organe angeordnet und nur in der dort vorgeschriebenen Form durchgeführt werden.

(3) Begründen bestimmte Tatsachen den Verdacht, daß jemand eine durch Gesetz einzeln bestimmte besonders schwere Straftat begangen hat, so dürfen zur Verfolgung der Tat auf Grund richterlicher Anordnung technische Mittel zur akustischen Überwachung von Wohnungen, in denen der Beschuldigte sich vermutlich aufhält, eingesetzt werden, wenn die Erforschung des Sachverhalts auf andere Weise unverhältnismäßig erschwert oder aussichtslos wäre. Die Maßnahme ist zu befristen. Die Anordnung erfolgt durch einen mit drei Richtern besetzten Spruchkörper. Bei Gefahr im Verzuge kann sie auch durch einen einzelnen Richter getroffen werden.

(4) Zur Abwehr dringender Gefahren für die öffentliche Sicherheit, insbesondere einer gemeinen Gefahr oder einer Lebensgefahr, dürfen technische Mittel zur Überwachung von Wohnungen nur auf Grund richterlicher Anordnung eingesetzt werden. Bei Gefahr im Verzuge kann die Maßnahme auch durch eine andere gesetzlich bestimmte Stelle angeordnet werden; eine richterliche Entscheidung ist unverzüglich nachzuholen.

(5) Sind technische Mittel ausschließlich zum Schutze der bei einem Einsatz in Wohnungen tätigen Personen vorgesehen, kann die Maßnahme durch eine gesetzlich bestimmte Stelle angeordnet werden. Eine anderweitige Verwertung der hierbei erlangten Erkenntnisse ist nur zum Zwecke der Strafverfolgung oder der Gefahrenabwehr und nur zulässig, wenn zuvor die Rechtmäßigkeit der Maßnahme richterlich festgestellt ist; bei Gefahr im Verzuge ist die richterliche Entscheidung unverzüglich nachzuholen.

(6) Die Bundesregierung unterrichtet den Bundestag jährlich über den nach Absatz 3 sowie über den im Zuständigkeitsbereich des Bundes nach Absatz 4 und, soweit richterlich überprüfungsbedürftig, nach Absatz 5 erfolgten Einsatz technischer Mittel. Ein vom Bundestag gewähltes Gremium übt auf der Grundlage dieses Berichts die parlamentarische Kontrolle aus. Die Länder gewährleisten eine gleichwertige parlamentarische Kontrolle.

(7) Eingriffe und Beschränkungen dürfen im übrigen nur zur Abwehr einer gemeinen Gefahr oder einer Lebensgefahr für einzelne Personen, auf Grund eines Gesetzes auch zur Verhütung dringender Gefahren für die öffentliche Sicherheit und Ordnung, insbesondere zur Behebung der Raumnot, zur Bekämpfung von Seuchengefahr oder zum Schutze gefährdeter Jugendlicher vorgenommen werden.

Art. 20 – Bundesstaatliche Verfassung; Widerstandsrecht

(1) Die Bundesrepublik Deutschland ist ein demokratischer und sozialer Bundesstaat.

(2) Alle Staatsgewalt geht vom Volke aus. Sie wird vom Volke in Wahlen und Abstimmungen und durch besondere Organe der Gesetzgebung, der vollziehenden Gewalt und der Rechtsprechung ausgeübt.

(3) Die Gesetzgebung ist an die verfassungsmäßige Ordnung, die vollziehende Gewalt und die Rechtsprechung sind an Gesetz und Recht gebunden.

(4) Gegen jeden, der es unternimmt, diese Ordnung zu beseitigen, haben alle Deutschen das Recht zum Widerstand, wenn andere Abhilfe nicht möglich ist.

Art. 23 – Verwirklichung der Europäischen Union; Beteiligung des Bundesrates, der Bundesregierung

(1) Zur Verwirklichung eines vereinten Europas wirkt die Bundesrepublik Deutschland bei der Entwicklung der Europäischen Union mit, die demokratischen, rechtsstaatlichen, sozialen und föderativen Grundsätzen und dem Grundsatz der Subsidiarität verpflichtet ist und einen diesem Grundgesetz im wesentlichen vergleichbaren Grundrechtsschutz gewährleistet. Der Bund kann hierzu durch Gesetz mit Zustimmung des Bundesrates Hoheitsrechte übertragen. Für die Begründung der Europäischen Union sowie für Änderungen ihrer vertraglichen Grundlagen und vergleichbare Regelungen, durch die dieses Grundgesetz seinem Inhalt nach geändert oder ergänzt wird oder solche Änderungen oder Ergänzungen ermöglicht werden, gilt Artikel 79 Abs. 2 und 3.

[...]

Art. 73 – Gegenstände der ausschließlichen Gesetzgebung

(1) Der Bund hat die ausschließliche Gesetzgebung über:

[...]

7. das Postwesen und die Telekommunikation;

[...]

Art. 79 – Deutsche Verfassungsidentität (e.T.)

(1) [...]

(2) Ein solches Gesetz bedarf der Zustimmung von zwei Dritteln der Mitglieder des Bundestages und zwei Dritteln der Stimmen des Bundesrates.

(3) Eine Änderung dieses Grundgesetzes, durch welche die Gliederung des Bundes in Länder, die grundsätzliche Mitwirkung der Länder bei der Gesetzgebung oder die in den Artikeln 1 und 20 niedergelegten Grundsätze berührt werden, ist unzulässig.

II. Nationales Sekundärrecht

1. Bundeskriminalamtgesetz (BKAG) in der Fassung ab 25.05.2018[2]

§ 46 – Besondere Bestimmungen über den Einsatz technischer Mittel in oder aus Wohnungen

(1) Das Bundeskriminalamt kann zur Abwehr einer dringenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, durch den verdeckten Einsatz technischer Mittel in oder aus Wohnungen

1. das nichtöffentlich gesprochene Wort einer Person abhören und aufzeichnen,

a) die entsprechend § 17 oder § 18 des Bundespolizeigesetzes verantwortlich ist oder

b) bei der konkrete Vorbereitungshandlungen für sich oder zusammen mit weiteren bestimmten Tatsachen die begründete Annahme rechtfertigen, dass sie Straftaten nach § 5 Absatz 1 Satz 2 begehen wird, und

2. Lichtbilder und Bildaufzeichnungen über diese Person herstellen, wenn die Abwehr der Gefahr auf andere Weise aussichtslos oder wesentlich erschwert wäre.

[...]

(6) Die Maßnahme nach Absatz 1 darf nur angeordnet und durchgeführt werden, soweit aufgrund tat-sächlicher Anhaltspunkte, insbesondere zu der Art der zu überwachenden Räumlichkeiten und dem Verhältnis der zu überwachenden Personen zueinander, anzunehmen ist, dass durch die Überwachung Äußerungen, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, nicht erfasst werden. Das Abhören und Beobachten nach Satz 1 ist unverzüglich zu unterbrechen, soweit sich während der Überwachung tatsächliche Anhaltspunkte dafür ergeben, dass Inhalte, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, erfasst werden. Sind das Abhören und Beobachten nach Satz 2 unterbrochen worden, so darf es unter den in Satz 1 genannten Voraussetzungen fortgeführt werden.

(7) Erkenntnisse, die durch Maßnahmen nach Absatz 1 erlangt worden sind, sind dem anordnenden Gericht unverzüglich vorzulegen. Das Gericht entscheidet unverzüglich über die Verwertbarkeit oder Löschung. Erkenntnisse aus dem Kernbereich privater Lebensgestaltung, die durch eine Maßnahme nach Absatz 1 erlangt worden sind, dürfen nicht verwertet werden. Aufzeichnungen hierüber sind unverzüglich zu löschen. Die Tatsachen der Erfassung der Daten und der Löschung sind zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist sechs Monate nach der Benachrichtigung nach § 74 oder sechs Monate nach Erteilung der gerichtlichen Zustimmung über das endgültige Absehen von der Benachrichtigung zu löschen. Ist die Datenschutzkontrolle nach

[2] Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Bundeskriminalamtgesetz – BKAG), das in dieser Fassung am 25.05.2018 in Kraft tritt (Art. 13 Abs. 1 Gesetz zur Neustrukturierung des Bundeskriminalamtgesetzes vom 1. Juni 2017, BGBl. 2017 Teil I Nr. 33, S. 1354 ff.

§ 69 Absatz 1 noch nicht beendet, ist die Dokumentation bis zu ihrem Abschluss aufzubewahren.

[...]

2. Hessisches Gesetz über die öffentliche Sicherheit und Ordnung (HSOG)[3]

§ 26 – Besondere Formen des Datenabgleichs

(1) 1Die Polizeibehörden können von öffentlichen Stellen oder Stellen außerhalb des öffentlichen Bereichs zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leben, Gesundheit oder Freiheit oder wenn gleichgewichtige Schäden für die Umwelt zu er-warten sind, die Übermittlung von personenbezogenen Daten bestimmter Personengruppen zum Zwecke des automatisierten Abgleichs mit anderen Datenbeständen verlangen, wenn dies zur Abwehr der Gefahr erforderlich ist. 2Rechtsvorschriften über ein Berufs- oder besonderes Amtsgeheimnis bleiben unberührt.

(2) 1Das Übermittlungsersuchen ist auf Namen, Anschriften, Tag und Ort der Geburt sowie auf im einzelnen Falle festzulegende Merkmale zu beschränken. 2Werden wegen technischer Schwierigkeiten, die mit angemessenem Zeit- oder Kostenaufwand nicht beseitigt werden können, weitere Daten übermittelt, dürfen diese nicht verwertet werden.

(3) 1Ist der Zweck der Maßnahme erreicht oder zeigt sich, dass er nicht erreicht werden kann, sind die übermittelten und im Zusammenhang mit der Maßnahme zusätzlich angefallenen Daten auf dem Datenträger zu löschen und die Unterlagen, soweit sie nicht für ein mit dem Sachverhalt zusammenhängendes Verfahren erforderlich sind, unverzüglich zu vernichten. 2Über die getroffenen Maßnahmen ist eine Niederschrift anzufertigen. 3Diese Niederschrift ist gesondert aufzubewahren, durch technische und organisatorische Maßnahmen zu sichern und am Ende des Kalenderjahres, das dem Jahr der Vernichtung der Unterlagen nach Satz 1 folgt, zu vernichten.

(4) 1Die Maßnahme nach Abs. 1 bedarf der schriftlich begründeten Anordnung durch die Behördenleitung und der Zustimmung des Landespolizeipräsidiums. 2Von der Maßnahme ist die oder der Hessische Datenschutzbeauftragte unverzüglich zu unterrichten.

(5) 1Personen, gegen die nach Abschluss einer Maßnahme nach Abs. 1 weitere Maßnahmen durchgeführt werden, sind hierüber durch die Polizei zu unterrichten, sobald dies ohne Gefährdung des Zweckes der weiteren Datennutzung erfolgen kann. 2§ 29 Abs. 6 Satz 4 und 5 und Abs. 7 gilt entsprechend.

[3] Hessisches Gesetz über die öffentliche Sicherheit und Ordnung (HSOG) in der Fassung der Bekanntmachung vom 14. Januar 2005 (GVBl. I S. 14), zuletzt geändert durch Artikel 2 des Gesetzes vom 4. Mai 2017 (GVBl. S. 66), http://www.rv.hessenrecht.hessen.de/lexsoft/default/hessenrecht_rv.html#docid:169564,1,20170801 (02.02.2018).

Teil 2: Rechtsprechung: Eine (IT-)(Un-)Sicherheitscharta für die BRD seit 2010 – Urteil des Bundesverfassungsgerichts zur Vorratsdaten“organisation“ (eigene Terminologie) vom 02.03.2010

A. Zum Geleit

I. Historie und Relation von „Verarbeitung“, „Datensammlungen“ und „Datenorganisation“

In einer globalen Perspektive ist das Urteil des Bundesverfassungsgerichts (BVerfG) vom 02.03.2010, Az. 1 BvR 256/08 u.a.[4], – soweit ersichtlich – eine der ersten judikativen Grundlegungen für das IT-Sicherheitsrecht wie auch die Vorratsdatenorganisation (eigene Terminologie), die der Cyberspace – die fünfte Dimension des Seins (über die m³ der Realworld und die Zeit hinaus) – ermöglicht.

Artikel 4 EU-DSGVO[5] (ab 25.05.2018 – Art. 99 Abs. 2) - Begriffsbestimmungen

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

[...]

2. „Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

[...]

Die Terminologie des Fachgebiets Öffentliches Recht (Autorin: Viola Schmid) lehnt den aus der Anthropologie und Geschichte stammenden Begriff/die Metapher des „Sammelns“ im Kontext von Informationstechnologie seit mehr als einem Jahrzehnt ab und legt als Oberbegriff für sämtliche Umgangsformen (in der Vergangenheit bis 24.05.2018 legaldefiniert in § 3 Abs. 2-5 BDSG) mit Daten die Terminologie „Organisation“ zugrunde.[6] Mit der ab 25.05.2018 geltenden

[4] Deutsch: http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2010/03/rs20100302_1bvr025608.html; englisch: http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016R0679 (Stand: 29.01.2018).

[5] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016R0679 (Stand: 29.01.2018).

[6] Vgl. Schmid, Cyberlaw – Eine neue Disziplin im Recht? in: Hendler/Marburger/Reinhardt/Schröder (Hrsg.), Jahrbuch des Umwelt- und Technikrechts 2003, S. 449-480, 455.

europäischen Datenschutz-Grundverordnung, die allein die Qualität der Informationstechnologie definiert, ergibt sich ein Terminologieunterschied zwischen Legaldefinition und wissenschaftlicher Meinung. In der Datenschutz-Grundverordnung handelt es sich um einen Unterbegriff zur „Verarbeitung“, während es sich in der hier vertretenen wissenschaftlichen Meinung um einen Oberbegriff handelt, der auch Verarbeitung umfasst. Die Rechtfertigung bleibt hier noch einer weiteren Veröffentlichung vorbehalten.

II. Zur Bedeutung des Urteils für die Vorlesung und Klausur

Die (rechts-)historische wie informationstechnologische und ökonomische Bedeutung des Urteils ist Grund für die didaktische Neuformatierung im folgenden Text. Dabei erfolgt im Rahmen des Konzepts „so wenig Recht wie möglich, so viel recht wie nötig“ keine vollständige Wiedergabe des ausgewählten Urteils. Gekürzte Passagen sind mit [...] gekennzeichnet. Es sei außerdem darauf hingewiesen, dass es sich bei den Ziffern am linken Rand, zu Beginn der einzelnen Absätze, um die Randnummern des Urteils handelt.

Eine weitere Konsequenz der informationstechnologischen und ökonomischen Bedeutung des Urteils ist die Zulassung dieses Texts als Hilfsmittel in der Cyberlaw I Klausur ab dem Wintersemester 2017/2018.

B. Bundesverfassungsgericht, Urteil vom 02.03.2010, Az. 1 BvR 256/08 u.a. (abgekürzt)

Leitsätze [...]

Im Namen des Volkes

In dem Verfahren über die Verfassungsbeschwerden

I.

[...]
gegen Telekommunikationsgesetzes in der Fassung des Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21. Dezember 2007 (BGBl I S. 3198)

- 1 BvR 256/08 -,

II.

[...]
gegen Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21. Dezember 2007 (BGBl I S. 3198)

- 1 BvR 263/08 -,

III.

[...]
gegen die Regelungen zur Vorratsdatenspeicherung im Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21. Dezember 2007 (BGBl I S. 3198)

- 1 BvR 586/08 -

FÖR-Hinweis: Es handelt sich um drei Verfassungsbeschwerden, die unterschiedliche Aktenzeichen tragen, aber zur gemeinsamen Verhandlung und Entscheidung verbunden wurden.

hat das Bundesverfassungsgericht - Erster Senat [...] aufgrund der mündlichen Verhandlung vom 15. Dezember 2009 durch

Urteil

für Recht erkannt:

1. **Die §§ 113a und 113b des Telekommunikationsgesetzes in der Fassung des Artikel 2 Nummer 6 des Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21. Dezember 2007 (Bundesgesetzblatt Teil I Seite 3198) verstoßen gegen Artikel 10 Absatz 1 des Grundgesetzes und sind nichtig.**
2. **§ 100g Absatz 1 Satz 1 der Strafprozessordnung in der Fassung des Artikel 1 Nummer 11 des Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter**

Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21. Dezember 2007 (Bundesgesetzblatt Teil I Seite 3198) verstößt, soweit danach Verkehrsdaten nach § 113a des Telekommunikationsgesetzes erhoben werden dürfen, gegen Artikel 10 Absatz 1 des Grundgesetzes und ist insoweit nichtig.

3. **Die aufgrund der einstweiligen Anordnung vom 11. März 2008 im Verfahren 1 BvR 256/08 (Bundesgesetzblatt Teil I Seite 659), wiederholt und erweitert mit Beschluss vom 28. Oktober 2008 (Bundesgesetzblatt Teil I Seite 2239), zuletzt wiederholt mit Beschluss vom 15. Oktober 2009 (Bundesgesetzblatt Teil I Seite 3704), von Anbietern öffentlich zugänglicher Telekommunikationsdienste im Rahmen von behördlichen Auskunftsersuchen erhobenen, aber einstweilen nicht nach § 113b Satz 1 Halbsatz 1 des Telekommunikationsgesetzes an die ersuchenden Behörden übermittelten, sondern gespeicherten Telekommunikationsverkehrsdaten sind unverzüglich zu löschen. Sie dürfen nicht an die ersuchenden Stellen übermittelt werden.**

4. **Die Bundesrepublik Deutschland hat den Beschwerdeführern ihre notwendigen Auslagen aus den Verfassungsbeschwerdeverfahren zu erstatten.**

Gründe

A. FÖR-Systematik: Beschwerdegegenstand

1 Gegenstand der Verfassungsbeschwerden sind Vorschriften des Telekommunikationsgesetzes (im Folgenden: TKG) und der Strafprozessordnung (im Folgenden: StPO), die eine vorsorgliche Speicherung von Telekommunikationsverkehrsdaten seitens der Anbieter öffentlich zugänglicher Telekommunikationsdienste für sechs Monate sowie die Verwendung dieser Daten regeln.

I. FÖR-Systematik: Historische Informationen

2 Die angegriffenen Vorschriften wurden durch das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21. Dezember 2007 (BGBl I S. 3198; im Folgenden: Gesetz zur Neuregelung der Telekommunikationsüberwachung) eingefügt oder geändert und sind nach dessen Art. 16 Abs. 1 am 1. Januar 2008 in Kraft getreten. Sie dienen der Umsetzung der Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunika-tionsnetze erzeugt und verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (ABl L 105 vom 13. April 2006, S. 54; im Folgenden: Richtlinie 2006/24/EG).

3 1. Alle Verfassungsbeschwerden richten sich unmittelbar gegen die §§ 113a und 113b TKG, die durch Art. 2 Nr. 6 des Gesetzes zur Neuregelung der Telekommunikationsüberwachung in das Telekommunikationsgesetz eingefügt worden sind. Die Verfassungsbeschwerden in den Verfahren 1 BvR 263/08 und 1 BvR 586/08 wenden sich darüber hinaus unmittelbar gegen § 100g StPO in der Fassung des Art. 1 Nr. 11 des Gesetzes zur Neuregelung der Telekommunikationsüberwachung, soweit er die Erhebung von nach § 113a TKG gespeicherten Daten zulässt.

4 a) § 113a TKG zielt darauf ab, hinsichtlich aller öffentlich zugänglichen Telekommunikationsdienste Verkehrsdaten, die Auskunft geben über die an einer Telekommunikationsverbindung beteiligten Anschlüsse, über die Zeit, zu der die Telekommunikation stattgefunden hat, und über die Orte, von denen aus kommuniziert worden ist, für sechs Monate zu speichern und für die staatliche Aufgabenwahrnehmung verfügbar zu halten. Das Gesetz greift damit seit längerem erhobene Forderungen des Bundesrates auf (vgl. BTDrucks 14/9801, S. 8; BRDrucks 755/03 <Beschluss>, S. 33 ff.; BRDrucks 406/1/04; BRDrucks 406/04 <Beschluss>; BRDrucks 723/05 <Beschluss>, S. 1), denen sich im Jahr 2006, bezugnehmend auf die diesbezüglichen Vorstöße auf europäischer Ebene, auch der Deutsche Bundestag anschloss. Er forderte die Bundesregierung auf, dem Entwurf der Richtlinie 2006/24/EG zuzustimmen und alsbald den Entwurf eines Umsetzungsgesetzes vorzulegen (vgl. BTDrucks 16/545, S. 4; 16/690, S. 2; BTPlenarprotokoll 16/19, S. 1430). Dem kam die

Bundesregierung mit dem Entwurf des Gesetzes zur Neuregelung der Telekommunikationsüberwachung nach (vgl. BTDrucks 16/5846).

5 § 113a Abs. 1 Satz 1 TKG verpflichtet die Betreiber öffentlich zugänglicher Telekommunikationsdienste, die in § 113a Abs. 2 bis 5 TKG einzeln aufgeführten Telekommunikationsverkehrsdaten zu Festnetz-, Internet- und Mobilfunktelefonaten, zum Versand von SMS-, MMS- und ähnlichen Nachrichten, zu E-Mail-Verbindungen und zum Internetzugang für einen Zeitraum von sechs Monaten zu speichern. Derjenige, der solche Dienste erbringt, ohne selbst Verkehrsdaten zu erzeugen, hat nach § 113a Abs. 1 Satz 2 TKG sicherzustellen, dass die Daten gespeichert werden, und der Bundesnetzagentur mitzuteilen, wer die Daten speichert. Wer Telekommunikationsdienste erbringt und dabei nach § 113a TKG zu speichernde Daten verändert, ist darüber hinaus gemäß § 113a Abs. 6 TKG zur Speicherung der ursprünglichen und der veränderten Angaben verpflichtet. Nach Ablauf der Speicherungsfrist sind die Daten gemäß § 113a Abs. 11 TKG binnen eines Monats zu löschen. Der Inhalt der Kommunikation und Daten über aufgerufene Internetseiten dürfen nach § 113a Abs. 8 TKG nicht gespeichert werden. Für die Datensicherheit verweist § 113a Abs. 10 TKG auf die im Bereich der Telekommunikation erforderliche Sorgfalt und verlangt, dass der Zugang zu den Daten nur hierzu besonders ermächtigten Personen vorbehalten bleibt.

6 Neben der Speicherung nach § 113a TKG besteht für die Anbieter von Telekommunikationsdiensten nach Maßgabe von § 96 TKG auch weiterhin die Möglichkeit, Telekommunikationsverkehrsdaten zu speichern und zu verwenden, soweit dies zu den dort genannten Zwecken erforderlich ist. Nach dem Ende einer Telekommunikationsverbindung dürfen diese Daten dabei nach § 96 Abs. 2 Satz 1 TKG im Wesentlichen verwendet werden, soweit sie zur Ermittlung des Entgelts und zur Abrechnung mit den Teilnehmern benötigt werden (§ 97 Abs. 1 Satz 1 TKG), zur Erstellung eines Einzelverbindungsnachweises (§ 99 Abs. 1 Satz 1 TKG), soweit dies zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen erforderlich ist (§ 100 Abs. 1 TKG), und zur Erteilung von Auskünften über die Inhaber von Anschlüssen, von denen bedrohende oder belästigende Anrufe ausgingen (§ 101 Abs. 1 Satz 1 TKG).

7 FÖR-Systematik: Rechtsverhalt

§ 113a TKG lautet:

8 § 113a

9 Speicherungspflichten für Daten

10 (1) Wer öffentlich zugängliche Telekommunikationsdienste für Endnutzer erbringt, ist verpflichtet, von ihm bei der Nutzung seines Dienstes erzeugte oder verarbeitete Verkehrsdaten nach Maßgabe der Absätze 2 bis 5 sechs Monate im Inland oder in einem anderen Mitgliedstaat der Europäischen Union zu speichern. Wer öffentlich zugängliche Telekommunikationsdienste für Endnutzer erbringt, ohne selbst Verkehrsdaten zu erzeugen oder zu verarbeiten, hat sicherzustellen, dass die Daten gemäß Satz 1 gespeichert werden, und der Bundesnetzagentur auf deren Verlangen mitzuteilen, wer diese Daten speichert.

11 (2) Die Anbieter von öffentlich zugänglichen Telefondiensten speichern:

12 1. die Rufnummer oder andere Kennung des anrufenden und des angerufenen Anschlusses sowie im Falle von Um- oder Weiterschaltungen jedes weiteren beteiligten Anschlusses,

13 2. den Beginn und das Ende der Verbindung nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone,

14 3. in Fällen, in denen im Rahmen des Telefondienstes unterschiedliche Dienste genutzt werden können, Angaben zu dem genutzten Dienst,

15 4. im Fall mobiler Telefondienste ferner:

16 a) die internationale Kennung für mobile Teilnehmer für den anrufenden und den angerufenen Anschluss,

b) die internationale Kennung des anrufenden und des angerufenen Endgerätes,

c) die Bezeichnung der durch den anrufenden und den angerufenen Anschluss bei Beginn der Verbindung genutzten Funkzellen,

d) im Fall im Voraus bezahlter anonymer Dienste auch die erste Aktivierung des Dienstes nach Datum, Uhrzeit und Bezeichnung der Funkzelle,

5. im Fall von Internet-Telefondiensten auch die Internetprotokoll-Adresse des anrufenden und des angerufenen Anschlusses.

Satz 1 gilt entsprechend bei der Übermittlung einer Kurz-, Multimedia- oder ähnlichen Nachricht; hierbei sind anstelle der Angaben nach Satz 1 Nr. 2 die Zeitpunkte der Versendung und des Empfangs der Nachricht zu speichern.

(3) Die Anbieter von Diensten der elektronischen Post speichern:

1. bei Versendung einer Nachricht die Kennung des elektronischen Postfachs und die Internetprotokoll-Adresse des Absenders sowie die Kennung des elektronischen Postfachs jedes Empfängers der Nachricht,

2. bei Eingang einer Nachricht in einem elektronischen Postfach die Kennung des elektronischen Postfachs des Absenders und des Empfängers der Nachricht sowie die Internetprotokoll-Adresse der absendenden Telekommunikationsanlage,

3. bei Zugriff auf das elektronische Postfach dessen Kennung und die Internetprotokoll-Adresse des Abrufenden,

4. die Zeitpunkte der in den Nummern 1 bis 3 genannten Nutzungen des Dienstes nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone.

(4) Die Anbieter von Internetzugangsdiensten speichern:

1. die dem Teilnehmer für eine Internetnutzung zugewiesene Internetprotokoll-Adresse,

2. eine eindeutige Kennung des Anschlusses, über den die Internetnutzung erfolgt,

3. den Beginn und das Ende der Internetnutzung unter der zugewiesenen Internetprotokoll-Adresse nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone.

(5) Soweit Anbieter von Telefondiensten die in dieser Vorschrift genannten Verkehrsdaten für die in § 96 Abs. 2 genannten Zwecke auch dann speichern oder protokollieren, wenn der Anruf unbeantwortet bleibt oder wegen eines Eingriffs des Netzwerkmanagements erfolglos ist, sind die Verkehrsdaten auch nach Maßgabe dieser Vorschrift zu speichern.

(6) Wer Telekommunikationsdienste erbringt und hierbei die nach Maßgabe dieser Vorschrift zu speichernden Angaben verändert, ist zur Speicherung der ursprünglichen und der neuen Angabe sowie des Zeitpunktes der Umschreibung dieser Angaben nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone verpflichtet.

(7) Wer ein Mobilfunknetz für die Öffentlichkeit betreibt, ist verpflichtet, zu den nach Maßgabe dieser Vorschrift gespeicherten Bezeichnungen der Funkzellen auch Daten vorzuhalten, aus denen sich die geografischen Lagen der die jeweilige Funkzelle versorgenden Funkantennen sowie deren Hauptstrahlrichtungen ergeben.

(8) Der Inhalt der Kommunikation und Daten über aufgerufene Internetseiten dürfen auf Grund dieser Vorschrift nicht gespeichert werden.

(9) Die Speicherung der Daten nach den Absätzen 1 bis 7 hat so zu erfolgen, dass Auskunftsersuchen der berechtigten Stellen unverzüglich beantwortet werden können.

(10) Der nach dieser Vorschrift Verpflichtete hat betreffend die Qualität und den Schutz der gespeicherten Verkehrsdaten die im Bereich der Telekommunikation erforderliche Sorgfalt zu beachten. Im Rahmen dessen hat er durch technische und organisatorische Maßnahmen

sicherzustellen, dass der Zugang zu den gespeicherten Daten ausschließlich hierzu von ihm besonders ermächtigten Personen möglich ist.

37 (11) Der nach dieser Vorschrift Verpflichtete hat die allein auf Grund dieser Vorschrift gespeicherten Daten innerhalb eines Monats nach Ablauf der in Absatz 1 genannten Frist zu löschen oder die Löschung sicherzustellen.

38 b) § 113b TKG regelt die Zwecke, zu denen die nach § 113a TKG gespeicherten Daten verwendet werden dürfen. Er unterscheidet dabei zwischen der Übermittlung an Behörden, um diesen eine Verwendung zur Erfüllung ihrer Aufgaben zu ermöglichen, und einer Verwendung durch die Telekommunikationsdiensteanbieter selbst zur Erteilung von Auskünften nach § 113 TKG, insbesondere über die Inhaber von Internetanschlüssen.

39 aa) § 113b Satz 1 Halbsatz 1 TKG regelt die Zwecke, zu denen die Telekommunikationsunternehmen die Daten an Behörden übermitteln dürfen. Die Voraussetzungen, unter denen diese ihrerseits die Daten nutzen dürfen, sollen durch bundes- oder landesrechtliche Bestimmungen des jeweiligen Fachrechts geregelt werden. § 113b Satz 1 Halbsatz 1 TKG sieht vor, dass der zur Speicherung Verpflichtete diejenigen Daten, die allein aufgrund der Speicherungsverpflichtung nach § 113a TKG gespeichert werden, ausschließlich zur Verfolgung von Straftaten (Nr. 1), zur Abwehr erheblicher Gefahren für die öffentliche Sicherheit (Nr. 2) und zur Erfüllung nachrichtendienstlicher Aufgaben (Nr. 3) an die zuständigen Stellen übermitteln darf.

40 Die Übermittlung der Daten an die jeweils zuständige Stelle darf auf deren Verlangen nach § 113b Satz 1 Halbsatz 1 TKG nur erfolgen, soweit dies in den einschlägigen gesetzlichen Bestimmungen des Fachrechts unter Bezugnahme auf § 113a TKG ausdrücklich vorgesehen und im Einzelfall angeordnet ist.

41 Die fachrechtliche Ermächtigungsgrundlage zur Nutzung der nach § 113a TKG gespeicherten Daten zur Strafverfolgung ist der von den Beschwerdeführern in den Verfahren 1 BvR 263/08 und 1 BvR 586/08 angegriffene § 100g StPO. Für die Gefahrenabwehr und die Aufgabenwahrnehmung der Nachrichtendienste verweisen mittlerweile § 20m des Bundeskriminalamtgesetzes (im Folgenden: BKAG) in der Fassung des Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt vom 25. Dezember 2008 (BGBl I S. 3083) sowie verschiedene landesrechtliche Bestimmungen auf § 113a TKG und ermöglichen so den behördlichen Rückgriff auf die nach dieser Bestimmung gespeicherten Daten.

42 In zulässiger Weise gespeicherte Telekommunikationsverkehrsdaten konnten allerdings auch vor Inkrafttreten von § 113a TKG schon zur Strafverfolgung, zur Gefahrenabwehr oder zur Erfüllung nachrichtendienstlicher Aufgaben herangezogen werden. So sah § 100g Abs. 1 StPO in der Fassung des Art. 1 des Gesetzes zur Änderung der Strafprozessordnung vom 20. Dezember 2001 (BGBl I S. 3879; im Folgenden: § 100g StPO a.F.) bei Verdacht einer Straftat von erheblicher Bedeutung oder einer mittels einer Endeinrichtung der Telekommunikation begangenen Straftat auf der Grundlage richterlicher Anordnung eine Verpflichtung der Diensteanbieter zur Erteilung von Auskünften über Telekommunikationsverbindungsdaten vor. Ebenso ermächtigten etwa Art. 34b Abs. 2 Nr. 1 des Gesetzes über die Aufgaben und Befugnisse der Bayerischen Staatlichen Polizei (Polizeiaufgabengesetz; im Folgenden: BayPAG) in der Fassung des Gesetzes zur Änderung des Polizeiaufgabengesetzes und des Parlamentarischen Kontrollgremium-Gesetzes vom 24. Dezember 2005 (GVBl S. 641) oder § 8a Abs. 1 Satz 1 Nr. 4 des Gesetzes über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (Bundesverfassungsschutzgesetz; im Folgenden: BVerfSchG) in der Fassung des Gesetzes zur Ergänzung des Terrorismusbekämpfungsgesetzes vom 5. Januar 2007 (BGBl I S. 2) dazu, zur Gefahrenabwehr oder zur Erfüllung von Verfassungsschutzaufgaben Auskünfte über vorhandene Telekommunikationsverbindungsdaten einzuholen.

43 bb) § 113b Satz 1 Halbsatz 2 TKG schließt die Verwendung der nach § 113a TKG gespeicherten Daten zu anderen als den in § 113b Satz 1 Halbsatz 1 TKG genannten Zwecken zwar grundsätzlich aus. Er lässt aber eine Ausnahme in der Weise zu, dass sie von den Diensteanbietern auch zur Erteilung von Auskünften nach § 113 TKG verwendet werden dürfen.

44 § 113 Abs. 1 TKG erlaubt Behörden die Abfrage von sogenannten Kunden- und Bestandsdaten gemäß §§ 95 und 111 TKG, insbesondere von Rufnummern, Anschlusskennungen sowie Namen und Anschriften von Anschlussinhabern. § 113b Satz 1 Halbsatz 2 TKG ermöglicht es damit den Diensteanbietern, Auskünfte über die Inhaber von sogenannten „dynamischen“ Internetprotokolladressen (im Folgenden: IP-Adressen) zu erteilen. IP-Adressen werden nach dem derzeitigen Stand der Entwicklung einem Anschluss in der Regel nicht als sogenannte „statische“ IP-Adressen fest zugeordnet, sondern dem Internetnutzer jeweils nur für die Dauer des jeweiligen Zugangs zum Internet als dynamische IP-Adressen zugewiesen. Über den Inhaber des Anschlusses, von dem aus eine bestimmte dynamische IP-Adresse zu einer bestimmten Zeit genutzt worden ist, kann deshalb nur Auskunft erteilt werden, wenn die Verkehrsdaten ausgewertet werden können, die Aufschluss darüber geben, welchem Anschluss die betreffende IP-Adresse zur maßgeblichen Zeit zugewiesen war. Dies ermöglicht § 113b Satz 1 Halbsatz 2 TKG für die nach § 113a TKG gespeicherten Daten.

45 Nach überwiegender Auffassung durften Verkehrsdaten zur Erteilung von Auskünften über Inhaber von dynamischen IP-Adressen nach §113 Abs. 1 TKG auch schon vor Inkrafttreten der §§ 113a und 113b TKG verwendet werden (vgl. etwa LG Stuttgart, Beschluss vom 4. Januar 2005 - 13 Qs 89/04 -, NJW 2005, S. 614 <614 f.>; LG Hamburg, Beschluss vom 23. Juni 2005 - 1 Qs 43/05 -, MMR 2005, S. 711 <712 f.>; Sankol, MMR 2006, S. 361 <365>; a.A. LG Bonn, Beschluss vom 21. Mai 2004 - 31 Qs 65/04 -, DuD 2004, S. 628 <628 f.>; OLG Karlsruhe, Urteil vom 4. Dezember 2008 - 4 U 86/07 -, MMR 2009, S. 412 <413 f.>; Bär, Handbuch zur EDV-Beweissicherung, 2007, S. 148, Rn. 212; Bock, in: Geppert/Piepenbrock/Schütz/Schuster, Beck’scher Kommentar zum TKG, 3. Aufl. 2006, § 113 Rn. 23 f.). Zurückgegriffen werden konnte dabei allerdings nur auf nach Maßgabe von § 96 TKG gespeicherte Verkehrsdaten. Die Möglichkeit einer Identifizierung des Inhabers einer dynamischen IP-Adresse über eine Auskunft nach § 113 Abs. 1 TKG war daher davon abhängig, ob solche Daten zum Zeitpunkt des Auskunftsersuchens noch gespeichert waren.

46 Bedeutung hat die Identifizierung des Inhabers von IP-Adressen etwa für den Urheberrechtsschutz. Gelingt es den Rechteinhabern, die IP-Adressen festzuhalten, unter denen Urheberrechtsverletzungen im Internet begangen werden, können die Strafverfolgungsbehörden durch Auskunftsersuchen nach § 113 Abs. 1 TKG die jeweiligen Anschlussinhaber ermitteln, gegen die die Rechteinhaber nach Einsicht in die Strafakten dann zivilrechtlich vorgehen können. Zwar räumt § 101 Abs. 2 Satz 1 Nr. 3 des Urheberrechtsgesetzes (im Folgenden: UrhG) in der Fassung des Art. 6 Nr. 10 des Gesetzes zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums vom 7. Juli 2008 (BGBl I S. 1191) den in ihren Urheberrechten Verletzten inzwischen unter bestimmten Voraussetzungen auch einen zivilrechtlichen Auskunftsanspruch gegenüber den Telekommunikationsdiensteanbietern ein. Diese dürfen die Auskunft nach § 101 Abs. 9 UrhG auf der Grundlage einer richterlichen Anordnung auch unter Verwendung von Telekommunikationsverkehrsdaten erteilen. Jedoch ist dabei ein Rückgriff auf die nach § 113a TKG gespeicherten Daten ausgeschlossen (vgl. OLG Frankfurt am Main, Beschluss vom 12. Mai 2009 - 11 W 21/09 -, MMR 2009, S. 542 <544> m.w.N.; Hoeren, NJW 2008, S. 3099 <3101>; Bäcker, in: Rensen/Brink, Linien der Rechtsprechung des Bundesverfassungsgerichts, 2009, S. 99 <111 f.>, Fn. 49).

47 Auskünfte nach § 113 Abs. 1 Satz 1 TKG sind zu erteilen, soweit dies für die Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung nachrichtendienstlicher Aufgaben erforderlich ist.

48 cc) § 113b TKG lautet:

49 § 113b

50 Verwendung der nach § 113a gespeicherten Daten

51 Der nach § 113a Verpflichtete darf die allein auf Grund der Speicherungsverpflichtung nach § 113a gespeicherten Daten

52 1. zur Verfolgung von Straftaten,

53 2. zur Abwehr von erheblichen Gefahren für die öffentliche Sicherheit oder

54 3. zur Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes und des Militärischen Abschirmdienstes

55 an die zuständigen Stellen auf deren Verlangen übermitteln, soweit dies in den jeweiligen gesetzlichen Bestimmungen unter Bezugnahme auf § 113a vorgesehen und die Übermittlung im Einzelfall angeordnet ist; für andere Zwecke mit Ausnahme einer Auskunftserteilung nach § 113 darf er die Daten nicht verwenden. § 113 Abs. 1 Satz 4 gilt entsprechend.

56 Die von § 113b TKG in Bezug genommene Regelung des § 113 TKG lautet auszugsweise:

57 § 113

58 Manuelles Auskunftsverfahren

59 (1) Wer geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, hat im Einzelfall den zuständigen Stellen auf deren Verlangen unverzüglich Auskünfte über die nach den §§ 95 und 111 erhobenen Daten zu erteilen, soweit dies für die Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes oder des Militärischen Abschirmdienstes erforderlich ist. Auskünfte über Daten, mittels derer der Zugriff auf Endgeräte oder in diesen oder im Netz eingesetzte Speichereinrichtungen geschützt wird, insbesondere PIN oder PUK, hat der nach Satz 1 Verpflichtete auf Grund eines Auskunftsersuchens nach § 161 Abs. 1 Satz 1, § 163 Abs. 1 der Strafprozessordnung, der Datenerhebungsvorschriften der Polizeigesetze des Bundes oder der Länder zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung, § 8 Abs. 1 des Bundesverfassungsschutzgesetzes, der entsprechenden Bestimmungen der Landesverfassungsschutzgesetze, § 2 Abs. 1 des BND-Gesetzes oder § 4 Abs. 1 des MAD-Gesetzes zu erteilen; an andere öffentliche oder nicht öffentliche Stellen dürfen diese Daten nicht übermittelt werden. Ein Zugriff auf Daten, die dem Fernmeldegeheimnis unterliegen, ist nur unter den Voraussetzungen der hierfür einschlägigen gesetzlichen Vorschriften zulässig. Über die Auskunftserteilung hat der Verpflichtete gegenüber seinen Kundinnen und Kunden sowie Dritten gegenüber Stillschweigen zu wahren.

60 (2) […]

61 c) § 100g Abs. 1 Satz 1 StPO regelt die Erhebung der Telekommunikationsverkehrsdaten zu Zwecken der Strafverfolgung. Die Strafverfolgungsbehörden können danach zunächst wie schon nach § 100g StPO a.F. auf Verkehrsdaten zugreifen, die die Telekommunikationsunternehmen auf der Grundlage von § 96 TKG gespeichert haben. Darüber hinaus gestattet § 100g StPO nun auch die Erhebung der nach § 113a TKG vorsorglich gespeicherten Daten. Hiergegen richten sich die Verfassungsbeschwerden in den Verfahren 1 BvR 263/08 und 1 BvR 586/08.

62 Im Einzelnen gestattet es § 100g Abs. 1 Satz 1 StPO unter Bezugnahme auf § 113a TKG den Strafverfolgungsbehörden, ohne Wissen des Betroffenen Verkehrsdaten zu erheben, soweit dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsorts des Beschuldigten erforderlich ist. Dies gilt allerdings nur, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Abs. 2 StPO bezeichnete Straftat, begangen hat, zu begehen versucht hat oder durch eine Straftat vorbereitet hat oder dass jemand als Täter oder Teilnehmer eine Straftat mittels Telekommunikation begangen hat.

63 Die Datenerhebungen dürfen nach § 100g Abs. 2 Satz 1 in Verbindung mit § 100b Abs. 1 Satz 1 und 2 StPO außer bei Gefahr im Verzug nur durch den Richter angeordnet werden. Die Anordnung darf sich gemäß § 100g Abs. 2 Satz 1 in Verbindung mit § 100a Abs. 3 StPO nur gegen den Beschuldigten oder gegen Personen richten, von denen aufgrund bestimmter Tatsachen anzunehmen ist, dass sie für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Beschuldigte ihren Anschluss benutzt.

64 Bei mittels Telekommunikation begangenen Straftaten ist die Verkehrsdatenerhebung nach § 100g Abs. 1 Satz 3 StPO nur zulässig, wenn die Erforschung des Sachverhalts oder die Ermittlung des

Aufenthaltsorts des Beschuldigten auf andere Weise aussichtslos wäre und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht. Diese Einschränkung hielt der Gesetzgeber aus Gründen der Verhältnismäßigkeit für erforderlich, weil die Verkehrsdatenerhebung durch die mit der Speicherungspflicht nach § 113a TKG verbundene Ausweitung des Datenvolumens insgesamt an Eingriffsintensität gewonnen habe (vgl. BTDrucks 16/5846, S. 52).

65 Von den Maßnahmen nach § 100g Abs. 1 Satz 1 StPO ist der Betroffene gemäß § 101 Abs. 4 Satz 1 StPO zu benachrichtigen. Ihre gerichtliche Überprüfung kann er innerhalb von zwei Wochen nach der Benachrichtigung beantragen (§ 101 Abs. 7 Satz 2 StPO). In bestimmten Fällen kann eine Benachrichtigung unterbleiben (§ 101 Abs. 4 StPO), in anderen Fällen kann sie zurückgestellt werden (§ 101 Abs. 5 StPO). Eine langfristige Zurückstellung nach § 101 Abs. 5 StPO bedarf anders als das Absehen von einer Benachrichtigung nach § 101 Abs. 4 StPO der gerichtlichen Bestätigung.

66 § 100g StPO lautet:

67 § 100g

68 (1) Begründen bestimmte Tatsachen den Verdacht, dass jemand als Täter oder Teilnehmer

69 1. eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Abs. 2 bezeichnete Straftat, begangen hat, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat oder durch eine Straftat vorbereitet hat oder

70 2. eine Straftat mittels Telekommunikation begangen hat,

71 so dürfen auch ohne Wissen des Betroffenen Verkehrsdaten (§ 96 Abs. 1, § 113a des Telekommunikationsgesetzes) erhoben werden, soweit dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich ist. Im Falle des Satzes 1 Nr. 2 ist die Maßnahme nur zulässig, wenn 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. Die Erhebung von Standortdaten in Echtzeit ist nur im Falle des Satzes 1 Nr. 1 zulässig.

72 (2) § 100a Abs. 3 und § 100b Abs. 1 bis 4 Satz 1 gelten entsprechend. Abweichend von § 100b Abs. 2 Satz 2 Nr. 2 genügt im Falle einer Straftat von erheblicher Bedeutung eine räumlich und zeitlich hinreichend bestimmte Bezeichnung der Telekommunikation, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wäre.

73 (3) Erfolgt die Erhebung von Verkehrsdaten nicht beim Telekommunikationsdiensteanbieter, bestimmt sie sich nach Abschluss des Kommunikationsvorgangs nach den allgemeinen Vorschriften.

74 (4) Über Maßnahmen nach Absatz 1 ist entsprechend § 100b Abs. 5 jährlich eine Übersicht zu erstellen, in der anzugeben sind:

75 1. die Anzahl der Verfahren, in denen Maßnahmen nach Absatz 1 durchgeführt worden sind;

76 2. die Anzahl der Anordnungen von Maßnahmen nach Absatz 1, unterschieden nach Erst- und Verlängerungsanordnungen;

77 3. die jeweils zugrunde liegende Anlassstraftat, unterschieden nach Absatz 1 Satz 1 Nr. 1 und 2;

78 4. die Anzahl der zurückliegenden Monate, für die Verkehrsdaten nach Absatz 1 abgefragt wurden, bemessen ab dem Zeitpunkt der Anordnung;

79 5. die Anzahl der Maßnahmen, die ergebnislos geblieben sind, weil die abgefragten Daten ganz oder teilweise nicht verfügbar waren.

80 2. Die Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates, deren Umsetzung die angegriffenen Regelungen, soweit sie die Strafverfolgung betreffen, dienen, wurde vom Rat auf der Grundlage von Art. 95 EGV gegen die Stimmen Irlands und der Slowakei angenommen (vgl.

Ratsdokument 6598/06 ADD 1 vom 27. Februar 2006, S. 4), nachdem das Europäische Parlament einen von Frankreich, Irland, Schweden und Großbritannien vorgelegten Entwurf eines auf Art. 31 Abs. 1 Buchstabe c und Art. 34 Abs. 2 Buchstabe b EUV - in der bis zum Inkrafttreten des Vertrages von Lissabon gültigen Fassung (im Folgenden: EUV a.F.) - gestützten Rahmenbeschlusses über die Vorratsspeicherung von Telekommunikationsdaten (vgl. Ratsdokument 8958/04 vom 28. April 2004) abgelehnt hatte (vgl. Parlamentsdokument P 6 TA[2005]0348).

81 a) Die Richtlinie knüpft daran an, dass Telekommunikationsverkehrsdaten ein wertvolles Instrument bei der Verfolgung von Straftaten insbesondere in den Bereichen der organisierten Kriminalität und des Terrorismus seien (vgl. Erwägungsgründe 7 bis 10 der Richtlinie 2006/24/EG) und dass einige Mitgliedstaaten Regelungen über die Vorratsdatenspeicherung von solchen Daten erlassen hätten, die stark voneinander abwichen (vgl. Erwägungsgrund 5 der Richtlinie 2006/24/EG). Die dadurch geschaffenen rechtlichen und technischen Unterschiede beeinträchtigten den Binnenmarkt für die elektronische Telekommunikation, weil die Anbieter von Telekommunikationsdiensten mit unterschiedlichen Anforderungen hinsichtlich der zu speichernden Daten und der Speicherungsdauer konfrontiert seien (vgl. Erwägungsgrund 6 der Richtlinie 2006/24/EG).

82 b) Die Gültigkeit der Richtlinie 2006/24/EG wird sowohl hinsichtlich ihrer Vereinbarkeit mit den Gemeinschaftsgrundrechten (vgl. Klesczewski, in: Festschrift für Gerhard Fezer zum 70. Geburtstag, 2008, S. 19 <24 f.>; Klug/Reif, RDV 2008, S. 89 <91 ff.>; Rusteberg, VBlBW 2007, S. 171 <176>; Westphal, EuZW 2006, S. 555 <558 f.>; Zöller, GA 2007, S. 393 <410 ff.>; Generalanwältin Kokott, Schlussanträge vom 18. Juli 2007 - Rs. C-275/06 -, Slg. 2008, I-271 <276>, Rn. 82 - Promusicae -) als auch in Bezug auf die in Anspruch genommene Kompetenzgrundlage der Europäischen Gemeinschaft in Zweifel gezogen (vgl. Gitter/Schnabel, MMR 2007, S. 411 <412 f.>; Jenny, CR 2008, S. 282 <285>; Klesczewski, in: Festschrift für Gerhard Fezer zum 70. Geburtstag, 2008, S. 19 <22 ff.>; Klug/Reif, RDV 2008, S. 89 <91>; Leutheusser-Schnarrenberger, ZRP 2007, S. 9 <11 ff.>; Rusteberg, VBlBW 2007, S. 171 <173 f.>; Westphal, EuZW 2006, S. 555 <557 f.>; Zöller, GA 2007, S. 393 <407 ff.>).

83 Mit Urteil vom 10. Februar 2009 wies der Europäische Gerichtshof eine Nichtigkeitsklage Irlands gemäß Art. 230 EGV ab (vgl. EuGH, Urteil vom 10. Februar 2009 - Rs. C-301/06 -), die sich darauf stützte, dass vorherrschender Zweck der Richtlinie die Erleichterung der Verfolgung von Straftaten sei und deshalb als Rechtsgrundlagen nur die Einstimmigkeit voraussetzenden Regelungen des EU-Vertrages alte Fassung über die polizeiliche und justizielle Zusammenarbeit, insbesondere Art. 30, Art. 31 Abs. 1 Buchstabe c und Art. 34 Abs. 2 Buchstabe b EUV a.F. in Betracht kämen (vgl. Klage vom 6. Juli 2006 - Rs. C-301/06 -, ABl C 237 vom 30. September 2006, S. 5). Dabei stellte der Gerichtshof ausdrücklich klar, dass die Entscheidung nicht eine etwaige Verletzung von Gemeinschaftsgrundrechten zum Gegenstand habe (vgl. EuGH, Urteil vom 10. Februar 2009 - Rs. C-301/06 -, Rn. 57).

84 c) Nach Art. 1 Abs. 1 Richtlinie 2006/24/EG zielt die Richtlinie auf die Harmonisierung der Vorschriften der Mitgliedstaaten über die Pflichten der Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste oder von Betreibern eines öffentlichen Telekommunikationsnetzes zur Vorratsspeicherung von Telekommunikationsdaten, um sicherzustellen, dass die Daten zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten, wie sie von jedem Mitgliedstaat in seinem nationalen Recht bestimmt werden, zur Verfügung stehen. Anlässlich der Annahme der Richtlinie erklärte der Rat dazu, die Mitgliedstaaten hätten bei der Definition des Begriffs „schwere Straftat“ die in Art. 2 Abs. 2 des Rahmenbeschlusses des Rates über den Europäischen Haftbefehl und die Übergabeverfahren zwischen den Mitgliedstaaten (2002/584/JI) vom 13. Juni 2002 (ABl L 190 vom 18. Juli 2002, S. 1) genannten Straftaten sowie Straftaten unter Einsatz von Telekommunikationseinrichtungen angemessen zu berücksichtigen (vgl. Ratsdokument 6598/06 ADD 1, S. 4). Eine Verwendung der Daten für Aufgaben der Gefahrenabwehr oder der Nachrichtendienste regelt die Richtlinie nicht.

85 Gemäß Art. 3 Abs. 1 Richtlinie 2006/24/EG haben die Mitgliedstaaten dafür Sorge zu tragen, dass die in Art. 5 Richtlinie 2006/24/EG im Einzelnen aufgeführten Daten auf Vorrat gespeichert werden, wobei nach Art. 6 Richtlinie 2006/24/EG ein Zeitraum von mindestens sechs Monaten und höchstens zwei Jahren vom Zeitpunkt der Kommunikation an festzulegen ist. Nach Art. 4 Richtlinie 2006/24/EG müssen die Mitgliedstaaten sicherstellen, dass die auf Vorrat gespeicherten Daten nur in bestimmten

Fällen und in Übereinstimmung mit dem innerstaatlichen Recht an die zuständigen nationalen Behörden weitergegeben werden. Jeder Mitgliedstaat legt dabei das Verfahren und die Bedingungen fest, die für den Zugang zu den Daten nach den Anforderungen der Notwendigkeit und der Verhältnismäßigkeit einzuhalten sind.

86 Art. 7 Richtlinie 2006/24/EG verpflichtet die Mitgliedstaaten sicherzustellen, dass in Bezug auf die auf Vorrat zu speichernden Daten bestimmte Mindestanforderungen der Datensicherheit eingehalten werden. Daneben bleiben die Regelungen der Richtlinien 95/46/EG und 2002/58/EG anwendbar (vgl. Erwägungsgründe 15 und 16 der Richtlinie 2006/24/EG). Nach Art. 8 Richtlinie 2006/24/EG gewährleisten die Mitgliedstaaten, dass die gespeicherten Daten und alle sonstigen erforderlichen Informationen unverzüglich auf Anfrage an die zuständigen Behörden weitergeleitet werden können. Gemäß Art. 13 Richtlinie 2006/24/EG stellen die Mitgliedstaaten außerdem sicher, dass die Maßnahmen zur Umsetzung der Regelungen von Kapitel III der Richtlinie 95/46/EG über Rechtsbehelfe, Haftung und Sanktionen auch im Hinblick auf die Datenverarbeitung nach der Richtlinie 2006/24/EG vollständig umgesetzt werden. Keine Regelung trifft die Richtlinie darüber, wer die Kosten der Datenspeicherung zu tragen hat.

87 3. § 100g StPO hat darüber hinaus für das Übereinkommen des Europarats über Computerkriminalität (BGBl II S. 1242; im Folgenden: Übereinkommen über Computerkriminalität) Bedeutung (vgl. BTDrucks 16/5846, S. 27 f. und 50). Das Übereinkommen verpflichtet nicht nur zur Schaffung materiellen Strafrechts zur Bekämpfung der Computerkriminalität, sondern auch zu bestimmten strafverfahrensrechtlichen Regelungen. Insbesondere sind nach Art. 16 des Übereinkommens die zuständigen Behörden zu ermächtigen, die umgehende Sicherung von Verkehrsdaten anzuordnen. Personen, in deren Kontrolle sich solche Daten befinden, müssen verpflichtet werden können, diese kurzfristig und unversehrt zu sichern, um den zuständigen Behörden zu ermöglichen, deren Weitergabe zu erwirken (sogenanntes Quick Freezing). Eine entsprechende Regelung hielt der Gesetzgeber allerdings für entbehrlich, weil die einzufrierenden Daten aufgrund der umfassenden Speicherung nach § 113a TKG ohnehin aufbewahrt werden müssten (vgl. BTDrucks 16/5846, S. 53).

88 4. Auf Antrag der Beschwerdeführer im Verfahren 1 BvR 256/08 hat das Bundesverfassungsgericht mit Beschluss vom 11. März 2008 eine einstweilige Anordnung erlassen, nach der § 113b Satz 1 Nr. 1 TKG bis zur Entscheidung in der Hauptsache nur eingeschränkt angewendet werden durfte (vgl. BVerfGE 121, 1). Mit Beschluss vom 28. Oktober 2008 hat es diese einstweilige Anordnung dahingehend erweitert, dass auch von § 113b Satz 1 Nr. 2 und 3 TKG bis zur Hauptsacheentscheidung nur mit Einschränkungen Gebrauch gemacht werden konnte (vgl. BVerfGE 122, 120). Außerdem wurde der Bundesregierung aufgegeben, jeweils für aufeinanderfolgende mehrmonatige Zeiträume über die praktischen Auswirkungen der in § 113a TKG vorgesehenen Datenspeicherungen und der einstweiligen Anordnung für die Strafverfolgung zu berichten. Die Bundesregierung ist dem für die Zeiträume vom 1. Mai 2008 bis 31. Juli 2008, vom 1. August 2008 bis 1. März 2009 und vom 1. März 2009 bis 1. September 2009 nachgekommen.

II. FÖR-Systematik: Informationen der Rechtsmittelführer zur Zulässigkeit und zu „Recht und Eingriff“ im Verfahren 1 BvR 256/08

89 1. Die Beschwerdeführer im Verfahren 1 BvR 256/08 wenden sich gegen die §§ 113a und 113b TKG. Sie rügen die Verletzung von Art. 10 Abs. 1, Art. 12 Abs. 1, Art. 14 Abs. 1, Art. 5 Abs. 1 und Art. 3 Abs. 1 GG. Dem haben sich mit gleichem Vorbringen in dem unter dem Aktenzeichen 1 BvR 508/08 geführten Verfahren rund 34.000 weitere Beschwerdeführer angeschlossen.

90 a) Die Verfassungsbeschwerden seien zulässig.

91 aa) **Die Beschwerdeführer zu 1) bis 3) und zu 5) bis 8) nutzten als Hochschullehrer, Rechtsanwälte, Geschäftsführer, Steuerberater und vereidigter Buchprüfer sowie investigativ tätiger Journalist privat und geschäftlich verschiedene Telekommunikationsdienste wie Festnetzanschlüsse, Mobiltelefone, Internetzugangsdienste und E-Mail-Postfächer.** Es sei ihnen nicht zumutbar, zunächst vor den Fachgerichten gegen die Telekommunikationsunternehmen zu klagen.

92 Die Beschwerdeführerin zu 4) entwickle und vertreibe die Software für einen kommerziellen Internet-Anonymisierungsdienst. Der Dienst werde im Zusammenwirken mit anderen unabhängigen Betreibern erbracht, auf deren Servern ihre Software genutzt werde. Dabei betreibe die Beschwerdeführerin auch selbst einen öffentlich zugänglichen Anonymisierungsserver. Der Anonymisierungsdienst sei infolge der angegriffenen Normen nicht mehr wirtschaftlich zu erbringen. Auch drohe ihr der Verlust ihrer Kunden, weil diese wegen der Vorratsdatenspeicherung nicht mehr darauf vertrauen könnten, anonym zu bleiben. Faktisch komme die Speicherungspflicht einem Berufsverbot gleich. Die Speicherungspflicht betreffe sie selbst, gegenwärtig und unmittelbar, da ihr nicht zugemutet werden könne, durch deren Nichtbeachtung das Risiko eines Bußgeld- oder Strafverfahrens einzugehen. […]

113 Auch verletze es Art. 3 Abs. 1 GG, dass zwar die Nutzung von Informationsangeboten im Internet, nicht aber diejenige traditioneller Massenmedien wie Zeitschriften, Bücher und Fernsehen festgehalten werde. Dafür, dass Massenkommunikation über die Telekommunikationsnetze besonders schadensträchtig sei, gebe es keine stichhaltigen Anhaltspunkte. Eine ungerechtfertigte Ungleichbehandlung sei auch, dass die Vorratsdatenspeicherung die nicht telekommunikative Computerbenutzung nicht erfasse. Gleichfalls sei Art. 3 Abs. 1 GG verletzt, weil der Gesetzgeber ungerechtfertigt von der Wahl milderer Mittel wie technischer, struktureller und aufklärender Präventionsmaßnahmen oder des Quick-Freezing-Verfahrens abgesehen habe.

114 Ebenso wenig seien die Ungleichbehandlung zwischen der Telekommunikation als elektronischem Informationsaustausch und dem Postwesen als distanziertem Austausch verkörperter Informationen, die Ungleichbehandlung von Telekommunikationsunternehmen gegenüber Postunternehmen, die Ungleichbehandlung der Inanspruchnahme von Telekommunikationsdiensten gegenüber der Inanspruchnahme sonstiger Leistungen und die Ungleichbehandlung von Telekommunikationsunternehmen gegenüber anderen Unternehmen wie Banken und Fluggesellschaften verfassungsrechtlich gerechtfertigt.

115 Ferner verletze die Gleichbehandlung kleiner Telekommunikationsunternehmen den allgemeinen Gleichheitssatz, weil dadurch eine Gruppe typischer Fälle ohne ausreichende Gründe wesentlich stärker belastet werde.

116 Vor Art. 3 Abs. 1 GG nicht zu rechtfertigen sei schließlich die entschädigungslose Indienstnahme privater Telekommunikationsunternehmen zu öffentlichen Zwecken. Die Kriterien für die Zulässigkeit einer Sonderabgabe mit Finanzierungsfunktion seien nicht erfüllt. Die Abwehr von Gefahren und die Ahndung von Straftaten seien Aufgaben der Allgemeinheit, die aus Steuermitteln finanziert werden müssten und nicht den betroffenen Unternehmen und ihren Kunden auferlegt werden dürften.

117 FÖR-Systematik: Beschwerdegegenstand § 100 g StPO – Informationen der Rechtsmittelführer zur Zulässigkeit und zu „Recht und Eingriff“ im Verfahren 1 BvR 263/08

2. Die Beschwerdeführer im Verfahren 1 BvR 263/08 wenden sich außer gegen die §§ 113a und 113b TKG auch gegen § 100g StPO, soweit er die Erhebung der nach § 113a TKG gespeicherten Daten betrifft. Sie rügen eine Verletzung von Art. 1 Abs. 1, Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1, Art. 10 Abs. 1 und Art. 19 Abs. 2 GG. […]

133 ee) Die Entscheidungsspielräume, die die Richtlinie 2006/24/EG lasse, seien nicht verfassungskonform ausgefüllt. § 113b TKG gehe über die Zweckbestimmung der Richtlinie hinaus, soweit die gespeicherten Daten zu sämtlichen nachrichtendienstlichen Zwecken zur Verfügung gestellt würden. § 100g StPO definiere den Kreis der Straftaten, die den Abruf von Vorratsdaten rechtfertigen könnten, nicht eindeutig. Es bleibe offen, wann eine Straftat auch im Einzelfall von erheblicher Bedeutung sei. Demgegenüber komme es - sofern man das Gemeinschaftsrecht überhaupt für maßgeblich halte - darauf an und sei für jede künftige Befugnisnorm gesondert zu klären, ob ihre Zweckbestimmung europarechtlich zwingend vorgegeben sei und ob sie dem nationalen Verfassungsrecht entspreche. § 100g StPO lasse den Abruf von Verbindungsdaten für jede mittels Telekommunikation begangene Straftat zu und gehe damit weit über die Zweckbestimmung der Richtlinie hinaus, terroristische Straftaten abzuwehren.

134 FÖR-Systematik: Informationen der Rechtsmittelführer zur Zulässigkeit und zu „Recht und Eingriff“ im Verfahren 1 BvR 586/08

3. Auch die Beschwerdeführer im Verfahren 1 BvR 586/08 wenden sich gegen die §§ 113a und 113b TKG und § 100g StPO. Sie rügen die Verletzung von Art. 10 Abs. 1 und Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG.

135 a) Die Verfassungsbeschwerden seien zulässig. Die Beschwerdeführer - Abgeordnete des Deutschen Bundestages und Mitglieder der Fraktion von Bündnis 90/Die Grünen, die teilweise außerdem nebenberuflich als Rechtsanwalt oder Arzt tätig sind - seien selbst, unmittelbar und gegenwärtig in ihrem Recht aus Art. 10 Abs. 1 GG sowie ihrem Recht auf informationelle Selbstbestimmung betroffen.

136 Auch könne die Regelung, da die Richtlinie 2006/24/EG erhebliche Umsetzungsspielräume belasse, in großem Umfang anhand der deutschen Grundrechte überprüft werden. Zwingend festgelegt seien lediglich die zu speichernden Datenkategorien und -typen sowie die Mindestspeicherungsdauer von sechs Monaten. Umsetzungsspielräume bestünden bezüglich der Speicher- und Verwendungszwecke, der zugriffsberechtigten Stellen, der Zugriffsvoraussetzungen und -verfahren, der Zweckbindung sowie der Anforderungen an die Datensicherheit. Soweit die Mitgliedstaaten in den Grenzen von Art. 15 Abs. 1 Richtlinie 2002/58/EG mit der Gefahrenabwehr und der Erfüllung der Aufgaben der Nachrichtendienste andere Verwendungszwecke als den der Strafverfolgung vorsähen, unterlägen sie uneingeschränkter verfassungsrechtlicher Kontrolle. Die Bestimmung der schweren Straftaten, zu deren Verfolgung die Vorratsdatenspeicherung erfolge, liege in der Hand der Mitgliedstaaten. Art. 7 der Richtlinie 2006/24/EG lege Mindestanforderungen fest, die weiterreichende datenschutzrechtliche Anforderungen im nationalen Verfassungsrecht nicht blockierten. Schließlich sei auch die Finanzierung der Vorratsdatenspeicherung in der Richtlinie nicht geregelt.

137 Eine vollständige verfassungsrechtliche Prüfung der Regelungen über die Vorratsdatenspeicherung sei außerdem möglich, wenn die Richtlinie 2006/24/EG nichtig sei, der Europäische Gerichtshof die Ungültigkeit der Richtlinie feststelle oder wenn man eine Überprüfung der Kompetenz der Europäischen Gemeinschaft zum Erlass der Richtlinie ausnahmsweise durch das Bundesverfassungsgericht selbst in Betracht ziehe. Eine Gültigkeitsvorlage könne insbesondere auf einen Verstoß gegen Gemeinschaftsgrundrechte gestützt werden.

138 b) Die Verfassungsbeschwerden seien auch begründet. Die angegriffenen Vorschriften verletzten Art. 10 Abs. 1 GG. Dieser schütze die Vertraulichkeit der näheren Umstände des Kommunikationsvorgangs. In seinen Schutzbereich fielen deshalb die nach § 113a Abs. 2 TKG zu speichernden Telefonverkehrsdaten und die nach § 113a Abs. 3 und 4 TKG zu speichernden E-Mail-Verkehrs- und Internetzugangsdaten. Dass im Internet auch Massenkommunikation stattfinde, die herkömmlich der Rundfunkfreiheit zugeordnet worden sei, stehe dem nicht entgegen. Dass auch Individualkommunikation vermittelt werden könne, reiche aus, um den Grundrechtsschutz auszulösen.

139 Die Regelungen zur Vorratsdatenspeicherung griffen in den Schutzbereich von Art. 10 GG ein. Der staatliche Eingriff beginne mit der Verkehrsdatenspeicherungspflicht gemäß § 113a TKG. Er setze sich fort mit der in § 113b TKG zugelassenen Übermittlung von Verkehrsdaten an staatliche Behörden. Weitere Eingriffsakte seien die Auswertung und Verwendung der Daten durch die auskunftsberechtigten Behörden und die Weitergabe der Daten an andere Behörden oder Private.

140 Hinreichend bestimmt sei § 100g Abs. 1 Nr. 1 StPO, weil er auf Straftaten von auch im Einzelfall erheblicher Bedeutung abstelle und konkretisierend auf die in § 100a Abs. 2 StPO bezeichneten Straftaten verweise. Kritischer zu beurteilen sei § 100g Abs. 1 Nr. 2 StPO im Hinblick auf § 100g Abs. 1 Satz 2 StPO. Wann die Datenerhebung in einem angemessenen Verhältnis zur Bedeutung der Sache stehe, sei für den Bürger nicht in der gebotenen Klarheit erkennbar. Problematisch sei auch die Bestimmtheit von § 113b TKG. Für den Bereich der Gefahrenabwehr und der Nachrichtendienste sei nicht absehbar, in welchem Umfang die ermächtigten Behörden auf die Vorratsdaten zugreifen dürften.

141 Die Vorratsdatenspeicherung verstoße außerdem gegen den Grundsatz der Verhältnismäßigkeit. Eine wirksame Strafverfolgung sei zwar ein legitimer Zweck. Auch ließen sich die Eignung und

Erforderlichkeit der Vorratsdatenspeicherung nicht verneinen. Das Quick-Freezing-Verfahren sei nicht gleich gut geeignet, weil es ins Leere gehe, wenn Verkehrsdaten nicht oder nicht mehr vorhanden seien. Die Vorratsdatenspeicherung sei allerdings unangemessen. Verkehrsdaten ließen erhebliche Rückschlüsse auf das Kommunikations- oder Bewegungsverhalten zu. Aufgrund ihrer automatischen Auswertbarkeit seien sie für Rasterfahndungsmethoden und strategische Überwachungen durch die Nachrichtendienste besonders geeignet. Sie lieferten Ermittlungsansätze und erlaubten, soziale, politische oder wirtschaftliche Beziehungsnetzwerke zu rekonstruieren. Umfassende Persönlichkeitsprofile könnten erstellt werden. Besonders belastend wirkten die Verdachtslosigkeit der Speicherung und ihre außergewöhnliche Streubreite. Zu berücksichtigen seien darüber hinaus die Rückwirkung auf gesamtgesellschaftliche Verhaltensmuster und den demokratischen Diskurs sowie Missbrauchsbefürchtungen.

142 § 100g StPO gehe über das zur Umsetzung der Richtlinie 2006/24/EG erforderliche Maß hinaus, weil der Abruf der nach § 113a TKG gespeicherten Daten generell auch wegen mittels Telekommunikation begangener Straftaten erfolgen könne. Bereits mittlere Kriminalität reiche für den Zugriff auf die Vorratsdaten aus. Dies steigere das Risiko, einem unberechtigten Verdacht ausgesetzt und dadurch zum Gegenstand belastender Ermittlungsmaßnahmen zu werden. Die Datenerhebungen erfolgten heimlich. § 100g Abs. 2 in Verbindung mit § 100b und § 101 StPO gewähre nur nachträglichen, durch eine restriktive Benachrichtigungspraxis geschwächten Rechtsschutz. Die Effektivität des Richtervorbehalts sei umstritten. Die bisherigen Zugriffsmöglichkeiten seien meist ausreichend gewesen. Bei Berücksichtigung alternativer Ermittlungsmethoden wie des Quick-Freezing-Verfahrens falle die Angemessenheitsprüfung negativ aus.

143 § 113b Satz 1 Nr. 2 TKG eröffne den Zugriff auf die anlasslos gespeicherten Daten bereits für erhebliche Gefahren für die öffentliche Sicherheit. Nachrichtendienstliche Überwachungsmaßnahmen erfolgten im Vorfeld konkreter Gefahren bei deutlich reduzierten Rechtsschutzmöglichkeiten. Beschränkungen für die Telekommunikationsüberwachung von Abgeordneten gebe es nicht. Angesichts ihrer Vorwirkungen auf das Verhalten der Bürger und den demokratischen Diskurs seien die Regelungen in § 113b Satz 1 Nr. 2 und 3 TKG unangemessen.

144 Berufsgeheimnisträger seien nicht gesondert geschützt. Besonders beeinträchtigend wirke sich dies bei Ärzten und nicht ausschließlich als Strafverteidiger tätigen Anwälten aus. Es fehlten außerdem hinreichende Datensicherungsstrukturvorgaben für die Diensteanbieter. Dies berge erhebliche Missbrauchsgefahren. Erst recht unangemessen sei die Nutzung der Daten durch Private zur Durchsetzung zivilrechtlicher Ansprüche, wie sie § 113b Satz 1 Halbsatz 2 TKG ermögliche. Da auf diese Weise nur die Inhaber von Anschlüssen ermittelt werden könnten, der Anschlussinhaber aber nicht zwangsläufig mit dem Internetnutzer übereinstimme, sei in erheblichem Umfang mit einer Verfolgung Unbeteiligter zu rechnen.

145 Die Verpflichtungen nach § 113a Abs. 10 TKG, die in der Telekommunikation erforderliche Sorgfalt zu beachten und durch technische und organisatorische Maßnahmen sicherzustellen, dass die gespeicherten Daten nur besonders ermächtigten Personen zugänglich seien, werde nicht näher konkretisiert. Die Datensicherheit werde so nicht hinreichend gewährleistet. Das Gewicht des Eingriffs werde nicht durch seinen Mehrwert aufgewogen. Gerade bei der organisierten Kriminalität und dem Terrorismus sei er am geringsten, da hier die Täter die Energie aufbrächten, die Speicherung zu unterlaufen, was ohne weiteres möglich sei. Die Rückwirkungen der Speicherung auf den demokratischen Diskurs und die Gefahren des Datenmissbrauchs könnten nicht hinreichend durch eine Begrenzung der Verwendungszwecke verringert werden.

III. FÖR-Systematik: Stellungnahmen […]

IV. FÖR-Systematik: Mündliche Verhandlung

174 In der mündlichen Verhandlung haben sich geäußert: die Beschwerdeführer, die Bundesregierung, das Bundeskriminalamt, die Bundesnetzagentur, die Bayerische Staatsregierung, der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, der Berliner Beauftragte für Datenschutz und Informationsfreiheit, als sachkundige Auskunftspersonen Prof. Dr. Dr. h.c. Hans-Jörg Albrecht, Constanze Kurz, Prof. Dr. Felix Freiling, Prof. Dr. Andreas Pfitzmann, Prof. Dr. Alexander Roßnagel,

Prof. Dr. Christoph Ruland, der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM), der Verband der deutschen Internetwirtschaft e.V. (eco), der Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e.V. (VATM), der Börsenverein des Deutschen Buchhandels e.V. und der Bundesverband Musikindustrie e.V.

B. FÖR-Systematik: Zulässigkeit […]

II.

180 Die Verfassungsbeschwerden sind nicht unzulässig, soweit die angegriffenen Vorschriften in Umsetzung der Richtlinie 2006/24/EG ergangen sind.

181 Allerdings übt das Bundesverfassungsgericht seine Gerichtsbarkeit über die Anwendbarkeit von Gemeinschafts- oder nunmehr Unionsrecht, das als Grundlage für ein Verhalten deutscher Gerichte und Behörden im Hoheitsbereich der Bundesrepublik Deutschland in Anspruch genommen wird, grundsätzlich nicht aus und überprüft dieses Recht nicht am Maßstab der Grundrechte des Grundgesetzes, solange die Europäischen Gemeinschaften (beziehungsweise heute die Europäische Union), insbesondere die Rechtsprechung des Europäischen Gerichtshofs, einen wirksamen Schutz der Grundrechte generell gewährleisten, der dem vom Grundgesetz jeweils als unabdingbar gebotenen Grundrechtsschutz im Wesentlichen gleich zu achten ist, zumal den Wesensgehalt der Grundrechte generell verbürgt (vgl. BVerfGE 73, 339 <387>; 102, 147 <162 f.>). Diese Grundsätze gelten auch für innerstaatliche Rechtsvorschriften, die zwingende Vorgaben einer Richtlinie in deutsches Recht umsetzen. Verfassungsbeschwerden, die sich gegen die Anwendung von in diesem Sinne verbindlichem Recht der Europäischen Union richten, sind grundsätzlich unzulässig (vgl. BVerfGE 118, 79 <95>; 121, 1 <15>).

182 Die Beschwerdeführer können sich auf die Grundrechte des Grundgesetzes jedoch insoweit berufen, als der Gesetzgeber bei der Umsetzung von Unionsrecht Gestaltungsfreiheit hat, das heißt durch das Unionsrecht nicht determiniert ist (vgl. BVerfGE 121, 1 <15>). Darüber hinaus sind die Verfassungsbeschwerden vorliegend aber auch insoweit zulässig, als die angegriffenen Vorschriften auf Richtlinienbestimmungen beruhen, die einen zwingenden Inhalt haben. Die Beschwerdeführer machen geltend, dass es der Richtlinie 2006/24/EG an einer gemeinschaftsrechtlichen Kompetenzgrundlage fehle und sie gegen europäische Grundrechtsverbürgungen verstoße. Sie erstreben deshalb unter anderem, ohne dass sie dies angesichts ihrer unmittelbar gegen das Umsetzungsgesetz gerichteten Verfassungsbeschwerden vor den Fachgerichten geltend machen konnten, eine Vorlage durch das Bundesverfassungsgericht an den Europäischen Gerichtshof, damit dieser im Wege der Vorabentscheidung nach Art. 267 AEUV (vormals Art. 234 EGV) die Richtlinie für nichtig erkläre und so den Weg frei mache für eine Überprüfung der angegriffenen Vorschriften am Maßstab der deutschen Grundrechte. Jedenfalls ist auf diesem Weg eine Prüfung der angegriffenen Vorschriften am Maßstab der Grundrechte des Grundgesetzes nach dem Begehren der Beschwerdeführer nicht von vornherein ausgeschlossen.

C. FÖR-Systematik: Begründetheit

183 Die Verfassungsbeschwerden sind im Wesentlichen begründet. Die angegriffenen Vorschriften verletzen die Beschwerdeführer in ihrem Grundrecht aus Art. 10 Abs. 1 GG. Eine Vorlage an den Europäischen Gerichtshof kommt nicht in Betracht, da es auf einen möglichen Vorrang des Gemeinschaftsrechts nicht ankommt. Die grundrechtlichen Gewährleistungen des Grundgesetzes stehen einer - anders gestalteten - Umsetzung der Richtlinie 2006/24/EG nicht entgegen. 184

Unbegründet ist die Verfassungsbeschwerde der Beschwerdeführerin zu 4) im Verfahren 1 BvR 256/08, soweit diese eine Verletzung von Art. 12 Abs. 1 GG rügt.

I. FÖR-Systematik: (Internationales) Recht – hier EU-Recht

185 Die Verfassungsbeschwerden geben keinen Anlass für ein Vorabentscheidungsverfahren vor dem Europäischen Gerichtshof gemäß Art. 267 AEUV. Zwar könnte eine entsprechende Vorlage durch das Bundesverfassungsgericht (vgl. BVerfGE 37, 271 <282>) insbesondere in Betracht kommen, wenn die Auslegung oder die Wirksamkeit von Gemeinschafts- beziehungsweise Unionsrecht in Frage stehen,

das Vorrang vor innerstaatlichem Recht beansprucht und dessen Umsetzung vom Bundesverfassungsgericht grundsätzlich nicht am Maßstab der Grundrechte des Grundgesetzes geprüft wird. Jedoch kann eine solche Vorlage nur dann zulässig und geboten sein, wenn es auf die Auslegung beziehungsweise Wirksamkeit des Unionsrechts ankommt. Dies ist vorliegend nicht der Fall.

186 Die Wirksamkeit der Richtlinie 2006/24/EG und ein sich hieraus möglicherweise ergebender Vorrang des Gemeinschaftsrechts vor deutschen Grundrechten sind nicht entscheidungserheblich. Der Inhalt der Richtlinie belässt der Bundesrepublik Deutschland für die Gestaltung der in ihr vorgeschriebenen Speicherung von Telekommunikationsverkehrsdaten einen weiten Entscheidungsspielraum. Die Richtlinie verpflichtet die Mitgliedstaaten zwar dazu, Betreibern von öffentlich zugänglichen elektronischen Kommunikationsnetzen und Kommunikationsdiensten die Speicherung von praktisch allen Telekommunikationsverkehrsdaten für eine Dauer von mindestens sechs Monaten vorzuschreiben (Art. 1, 3, 5 und 6 Richtlinie 2006/24/EG). Ihre Regelungen sind dabei aber im Wesentlichen auf die Speicherungspflichten selbst beschränkt und regeln nicht den Zugang zu den Daten oder deren Verwendung durch die Behörden der Mitgliedstaaten. Insbesondere harmonisieren sie weder die Frage des Zugangs zu den Daten durch die zuständigen nationalen Strafverfolgungsbehörden noch die Frage der Verwendung und des Austausches dieser Daten zwischen diesen Behörden (vgl. EuGH, Urteil vom 10. Februar 2009 - Rs. C-301/06 -, Rn. 83). Ausgehend von den Mindestanforderungen der Richtlinie (Art. 7 und 13 Richtlinie 2006/24/EG) liegt es ebenfalls bei den Mitgliedstaaten, die erforderlichen Maßnahmen zur Gewährleistung von Datensicherheit, Transparenz und Rechtsschutz zu ergreifen.

187 Mit diesem Inhalt kann die Richtlinie ohne Verstoß gegen die Grundrechte des Grundgesetzes umgesetzt werden. Das Grundgesetz verbietet eine solche Speicherung nicht unter allen Umständen. Vielmehr kann sie auch unabhängig von einem etwaigen Vorrang des Gemeinschaftsrechts nach den Maßgaben der Grundrechte des Grundgesetzes zulässig angeordnet werden (siehe unten IV). Eine Prüfung der angegriffenen Vorschriften insgesamt am Maßstab der deutschen Grundrechte gerät damit nicht in Konflikt mit der Richtlinie 2006/24/EG, so dass es auf deren Wirksamkeit und Vorrang nicht ankommt.

II. FÖR-Systematik: RER-Prüfung – Recht und Eingriff

188 Die angegriffenen Vorschriften greifen in Art. 10 Abs. 1 GG ein.

189 1. Art. 10 Abs. 1 GG gewährleistet das Telekommunikationsgeheimnis, welches die unkörperliche Übermittlung von Informationen an individuelle Empfänger mit Hilfe des Telekommunikationsverkehrs (vgl. BVerfGE 106, 28 <35 f.>; 120, 274 <306 f.>) vor einer Kenntnisnahme durch die öffentliche Gewalt schützt (vgl. BVerfGE 100, 313 <358>; 106, 28 <37>). Dieser Schutz erfasst dabei nicht nur die Inhalte der Kommunikation. Geschützt ist vielmehr auch die Vertraulichkeit der näheren Umstände des Kommunikationsvorgangs, zu denen insbesondere gehört, ob, wann und wie oft zwischen welchen Personen oder Telekommunikationseinrichtungen Telekommunikationsverkehr stattgefunden hat oder versucht worden ist (vgl. BVerfGE 67, 157 <172>; 85, 386 <396>; 100, 313 <358>; 107, 299 <312 f.>; 115, 166 <183>; 120, 274 <307>).

190 Der Schutz durch Art. 10 Abs. 1 GG gilt nicht nur dem ersten Zugriff, mit dem die öffentliche Gewalt von Telekommunikationsvorgängen und -inhalten Kenntnis nimmt. Seine Schutzwirkung erstreckt sich auch auf die Informations- und Datenverarbeitungsprozesse, die sich an die Kenntnisnahme von geschützten Kommunikationsvorgängen anschließen, und auf den Gebrauch, der von den erlangten Kenntnissen gemacht wird (vgl. BVerfGE 100, 313 <359>). Ein Grundrechtseingriff ist jede Kenntnisnahme, Aufzeichnung und Verwertung von Kommunikationsdaten sowie jede Auswertung ihres Inhalts oder sonstige Verwendung durch die öffentliche Gewalt (vgl. BVerfGE 85, 386 <398>; 100, 313 <366>; 110, 33 <52 f.>). In der Erfassung von Telekommunikationsdaten, ihrer Speicherung, ihrem Abgleich mit anderen Daten, ihrer Auswertung, ihrer Selektierung zur weiteren Verwendung oder ihrer Übermittlung an Dritte liegen damit je eigene Eingriffe in das Telekommunikationsgeheimnis (vgl. BVerfGE 100, 313 <366 f.>). Folglich liegt in der Anordnung gegenüber Kommunikationsunternehmen, Telekommunikationsdaten zu erheben, zu speichern und an staatliche Stellen zu übermitteln, jeweils ein Eingriff in Art. 10 Abs. 1 GG (vgl. BVerfGE 107, 299 <313>).

191 Das aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG folgende Recht auf informationelle Selbstbestimmung kommt neben Art. 10 GG nicht zur Anwendung. Bezogen auf die Telekommunikation enthält Art. 10 GG eine spezielle Garantie, die die allgemeine Vorschrift verdrängt und aus der sich besondere Anforderungen für die Daten ergeben, die durch Eingriffe in das Fernmeldegeheimnis erlangt werden. Insoweit lassen sich allerdings die Maßgaben, die das Bundesverfassungsgericht aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG entwickelt hat, weitgehend auf die speziellere Garantie des Art. 10 GG übertragen (vgl. BVerfGE 100, 313 <358 f.>).

192 2. a) Die in § 113a Abs. 1 TKG den Diensteanbietern auferlegte Speicherung der Telekommunikationsverkehrsdaten greift in das Telekommunikationsgeheimnis ein. Dies gilt zunächst für die Speicherungspflichten bezüglich der Telekommunikationsdienste gemäß § 113a Abs. 2 bis 5 TKG und in Verbindung hiermit gemäß § 113a Abs. 6 und 7 TKG. Die insoweit zu speichernden Angaben geben Auskunft darüber, ob, wann, wo und wie oft zwischen welchen Telekommunikationseinrichtungen Verbindungen aufgenommen oder aufzunehmen versucht wurden. Insbesondere gilt dies auch für die Speicherung der Daten zu Diensten der elektronischen Post gemäß § 113a Abs. 3 TKG, deren Vertraulichkeit gleichfalls durch Art. 10 Abs. 1 GG geschützt wird (vgl. BVerfGE 113, 348 <383>; 120, 274 <307>). Dass sich E-Mails technisch leicht abfangen lassen, ändert an deren vertraulichem Charakter und ihrer Schutzwürdigkeit nichts. Einen Eingriff in Art. 10 Abs. 1 GG begründet dabei auch die Speicherung der den Internetzugang betreffenden Daten gemäß § 113a Abs. 4 TKG. Zwar ermöglicht der Internetzugang nicht nur die Aufnahme von Individualkommunikation, die dem Schutz des Telekommunikationsgeheimnisses unterfällt, sondern auch die Teilnahme an Massenkommunikation. Da eine Unterscheidung zwischen Individual- und Massenkommunikation ohne eine der Schutzfunktion des Grundrechts zuwiderlaufende Anknüpfung an den Inhalt der jeweils übermittelten Information nicht möglich ist, ist bereits in der Speicherung der den Internetzugang als solchen betreffenden Daten ein Eingriff zu sehen, auch wenn sie Angaben über die aufgerufenen Internetseiten nicht enthalten (vgl. Gusy, in: v. Mangoldt/Klein/Starck, GG, Bd. 1, 5. Aufl. 2005, Art. 10 Rn. 44; Hermes, in: Dreier, GG, Bd. 1, 2. Aufl. 2004, Art. 10 Rn. 39).

193 Die Eingriffsqualität des § 113a TKG wird auch nicht dadurch in Frage gestellt, dass die in dieser Vorschrift vorgeschriebene Speicherung nicht durch den Staat selbst, sondern durch private Diensteanbieter erfolgt. Denn diese werden allein als Hilfspersonen für die Aufgabenerfüllung durch staatliche Behörden in Anspruch genommen. § 113a TKG verpflichtet die privaten Telekommunikationsunternehmen zur Datenspeicherung allein für die Aufgabenerfüllung durch staatliche Behörden zu Zwecken der Strafverfolgung, der Gefahrenabwehr und der Erfüllung nachrichtendienstlicher Aufgaben gemäß § 113b TKG. Dabei ordnet der Staat die mit der Speicherung verbundene Grundrechtsbeeinträchtigung unmittelbar an, ohne dass den speicherungspflichtigen Unternehmen insoweit ein Handlungsspielraum verbleibt; die Daten sind so zu speichern, dass Auskunftsersuchen der berechtigten öffentlichen Stellen nach § 113a Abs. 9 TKG unverzüglich erfüllt werden können. Unter diesen Voraussetzungen ist die Speicherung der Daten rechtlich dem Gesetzgeber als unmittelbarer Eingriff in Art. 10 Abs. 1 GG zuzurechnen (vgl. BVerfGE 107, 299 <313 f.>).

194 b) Grundrechtseingriffe in Art. 10 Abs. 1 GG liegen auch in den Regelungen zur Datenübermittlung in § 113b Satz 1 Halbsatz 1 TKG. Zwar eröffnet diese Vorschrift für sich genommen noch keine Verwendung der nach § 113a TKG gespeicherten Daten, sondern verweist auf weitere gesetzlich eigens zu schaffende Abrufnormen. Jedoch liegt in ihr die grundlegende Bestimmung, für welche Zwecke die Daten verwendet werden dürfen. Sie befreit diesbezüglich die Telekommunikationsunternehmen von ihrer im Übrigen geltenden Geheimhaltungspflicht. Dass die Datenverwendung letztlich endgültig erst im gestuften Ineinandergreifen von Vorschriften auf verschiedenen Normebenen ihre Gesamtregelung findet, ändert nichts daran, dass die Definition der Verwendungszwecke und die Erlaubnis zur Datenübermittlung Teil der Verwendungsregelung sind und insoweit Eingriffscharakter haben. Auch hier ist es unerheblich, dass § 113b TKG eine Übermittlung der Daten seitens privater Diensteanbieter betrifft. Die vorgesehene Übermittlung beruht auf einer gesetzlichen Regelung und damit unmittelbar auf einem Akt der nach Art. 1 Abs. 3 GG grundrechtsgebundenen öffentlichen Gewalt, setzt eine hoheitliche Anordnung im Einzelfall voraus und erfolgt an Behörden. Sie ist damit rechtlich als Eingriff des Staates anzusehen.

195 c) Einen Eingriff in Art. 10 Abs. 1 GG begründet auch § 113b Satz 1 Halbsatz 2 in Verbindung mit § 113 Abs. 1 TKG. Danach können Behörden von den Diensteanbietern Auskünfte über Bestands- und Kundendaten gemäß §§ 95, 111 TKG verlangen, die die Diensteanbieter nur unter Nutzung der nach § 113a Abs. 4 TKG gespeicherten Daten ermitteln können. Unabhängig von der Frage, ob und wieweit in Auskünften gemäß § 113 TKG allgemein ein Eingriff in Art. 10 Abs. 1 GG liegt beziehungsweise ob insoweit grundsätzlich allein das Recht auf informationelle Selbstbestimmung gemäß Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG einschlägig ist, ist jedenfalls für Auskünfte gemäß § 113b Satz 1 Halbsatz 2, § 113 Abs. 1 TKG ein Eingriff in das Telekommunikationsgeheimnis des Art. 10 Abs. 1 GG zu bejahen. Denn es wird hier die Nutzung der gemäß § 113a TKG gespeicherten und damit durch einen Eingriff in Art. 10 Abs. 1 GG gewonnenen Daten geregelt. Jede Folgeverwendung von Daten, die einmal in Form eines Eingriffs in Art. 10 Abs. 1 GG erhoben worden sind, bleibt stets an diesem Grundrecht zu messen (vgl. BVerfGE 100, 313 <359>; 110, 33 <68 f.>; 113, 348 <365>). Auch hier kann es nicht darauf ankommen, dass diese gesetzlich vorgeschriebene Nutzung nicht durch die öffentliche Hand selbst, sondern - in Erfüllung des Auskunftsverlangens - durch private Anbieter erfolgt.

196 d) Einen Eingriff in Art. 10 Abs. 1 GG begründet schließlich auch § 100g StPO. Er ermöglicht den Strafverfolgungsbehörden, sich die nach § 113a TKG gespeicherten Daten von den zur Speicherung Verpflichteten übermitteln zu lassen und zu nutzen. § 100g Abs. 1 Satz 1 StPO selbst sowie das Gebrauchmachen von dieser Ermächtigung greifen als Akte der öffentlichen Gewalt daher gleichfalls in den Schutzbereich von Art. 10 Abs. 1 GG ein.

III. FÖR-Systematik: Formelle Rechtmäßigkeit der Eingriffsermächtigungen

197 In formeller Hinsicht begegnen die angegriffenen Vorschriften keinen Bedenken. Sie genügen dem Gesetzesvorbehalt des Art. 10 Abs. 2 Satz 1 GG und sind durch eine Kompetenz des Bundes gedeckt.

198 1. Beschränkungen des Telekommunikationsgeheimnisses dürfen gemäß Art. 10 Abs. 2 Satz 1 GG nur aufgrund eines Gesetzes angeordnet werden. Keinen Zweifeln unterliegen insoweit zunächst § 113b TKG und § 100g StPO, die - gegebenenfalls im Zusammenwirken mit weiteren Vorschriften - eine gesetzliche Grundlage für den Erlass einzelfallbezogener Anordnungen darstellen, aufgrund deren der Zugriff auf die Daten erfolgt. Verfassungsrechtlich unbedenklich ist insoweit auch § 113a TKG, der für die Speicherung der Daten nicht auf einzelfallbezogene Anordnungen verweist, sondern diese unmittelbar selbst vorschreibt. Art. 10 Abs. 2 Satz 1 GG steht Beschränkungen des Telekommunikationsgeheimnisses auch unmittelbar durch Gesetz nicht entgegen (vgl. BVerfGE 85, 386 <396 ff.>).

199 2. Dem Bund fehlt es nicht an einer Gesetzgebungskompetenz. Die §§ 113a, 113b TKG finden ihre Kompetenzgrundlage in Art. 73 Abs. 1 Nr. 7 GG, § 100g StPO findet sie in Art. 74 Abs. 1 Nr. 1, Art. 72 Abs. 1 GG.

200 Art. 73 Abs. 1 Nr. 7 GG berechtigt unmittelbar allerdings nur zur Regelung der technischen Seite der Errichtung einer Telekommunikationsinfrastruktur und der Informationsübermittlung mit Hilfe von Telekommunikationsanlagen. Von der Norm nicht umfasst sind Regelungen, die auf die übermittelten Inhalte oder die Art der Nutzung der Telekommunikation gerichtet sind (vgl. BVerfGE 113, 348 <368>; 114, 371 <385>) und etwa eine Telekommunikationsüberwachung zum Zwecke der Erlangung von Informationen für Aufgaben der Strafverfolgung oder der Gefahrenabwehr vorsehen. Solche Regelungen sind im Hinblick auf die Gesetzgebungskompetenz jeweils dem Rechtsbereich zuzuordnen, für dessen Zwecke die Überwachung erfolgt (vgl. BVerfGE 113, 348 <368>).

201 Die §§ 113a und 113b TKG sind von der Kompetenz zur Regelung des Telekommunikationsrechts jedoch als Bestandteil der hiermit zu verbindenden datenschutzrechtlichen Bestimmungen kraft Sachzusammenhangs miterfasst. Mangels ausdrücklicher Kompetenzzuweisung fällt das Recht des Datenschutzes zwar grundsätzlich in die Zuständigkeit der Länder. Eine bundesgesetzliche Zuständigkeit für dessen Regelung besteht kraft Sachzusammenhangs jedoch insoweit, als der Bund eine ihm zur Gesetzgebung zugewiesene Materie verständigerweise nicht regeln kann, ohne dass die datenschutzrechtlichen Bestimmungen mitgeregelt werden (vgl. BVerfGE 3, 407 <421>; 98, 265 <299>; 106, 62 <115>; 110, 33 <48>; stRspr; zum Datenschutzrecht vgl. Simitis, in: Simitis, BDSG, 6. Aufl. 2006, § 1 Rn. 4). Dies ist für die §§ 113a, 113b TKG der Fall. Diese stehen im Zusammenhang mit den Bestimmungen des Telekommunikationsgesetzes zum Datenschutz und normieren in Anknüpfung an

die Regelung der technischen Bedingungen der Informationsübermittlung die jeweils zu beachtenden Anforderungen an den Umgang mit den bei der Erbringung von Telekommunikationsdiensten erzeugten oder verarbeiteten Daten. Sie knüpfen damit unmittelbar an Sachverhalte an, die in den Bereich der Gesetzgebungsmaterie der Telekommunikation fallen. Wegen dieses engen Zusammenhangs zwischen technischem Übermittlungsvorgang und den dabei anfallenden Daten kann die erforderliche datenschutzrechtliche Regelung ihrer Verwendung nur einheitlich durch den Bundesgesetzgeber erfolgen, der über die Kompetenz zur Regelung des Übermittlungsvorgangs verfügt. Andernfalls bestünde die Gefahr eines Inkongruenzen verursachenden Auseinanderfallens der technischen und datenschutzrechtlichen Regelungen der Datenverarbeitung. Dementsprechend enthält das Telekommunikationsgesetz neben den Regelungen der §§ 113a und 113b TKG und über das Fernmeldegeheimnis in den §§ 88 ff. TKG auch in den §§ 91 bis 107 TKG umfangreiche bereichsspezifische Regelungen zum Datenschutz, deren kompetenzielle Rechtmäßigkeit bisher - soweit ersichtlich - nicht ernsthaft in Zweifel gezogen wurde.

202 Der Reichweite nach kann der Bund auf dieser Kompetenzgrundlage diejenigen Regelungen treffen, die zu einer grundrechtskonformen Regelung der Datenverwendung erforderlich sind. Insbesondere kann er die Bestimmungen vorsehen, die notwendig sind, damit die in § 113a TKG vorgesehene Datenspeicherung und die Übermittlung der Daten an Strafverfolgungs- und Gefahrenabwehrbehörden sowie Nachrichtendienste und ihre Verwendung zur Erteilung von Auskünften nach § 113 TKG den grundrechtlichen Anforderungen von Art. 10 Abs. 1 GG genügen. Da Eingriffe in Art. 10 Abs. 1 GG voraussetzen, dass ihr Zweck bereichsspezifisch, präzise und normenklar bestimmt ist (vgl. BVerfGE 100, 313 <359 f.>; 110, 33 <53>; 115, 320 <365>; 118, 168 <187 f.>), beinhaltet dies die Kompetenz zur bereichsspezifischen, präzisen und normenklaren Regelung des Zwecks der Speicherung. Die Gesetzgebungskompetenz des Bundes reicht diesbezüglich freilich nur so weit, wie dies nach datenschutzrechtlichen Gesichtspunkten und den hiermit verbundenen verfassungsrechtlichen Anforderungen geboten ist. Die Ermächtigungen zum Datenabruf selbst kann der Bund deshalb nicht auf Art. 73 Abs. 1 Nr. 7 GG stützen. Er bedarf dafür eines eigenen Kompetenztitels oder muss die Entscheidung hierüber den Ländern überlassen.

203 §§ 113a, 113b TKG tragen dem vom Grundsatz her Rechnung. Sie beschränken sich allein darauf, durch Speicherungspflichten und Übermittlungsregelungen die Voraussetzungen für einen staatlichen Zugriff auf die Daten zu schaffen. Deren Ausfüllung bleibt demgegenüber eigenen Regelungen zum Datenabruf überlassen. Unbeschadet der materiellrechtlichen Frage, ob der Bund die Verwendungszwecke hierbei sachlich hinreichend begrenzt hat (siehe unten C V 5 und VI 3 b), sind hiergegen kompetenzrechtlich keine Einwände zu erheben.

IV. FÖR-Systematik: Materielle Rechtmäßigkeit – Verhältnismäßigkeit (im engeren Sinne)

204 Materiell verfassungsgemäß sind die Eingriffe in das Telekommunikationsgeheimnis, wenn sie legitimen Gemeinwohlzwecken dienen und im Übrigen dem Grundsatz der Verhältnismäßigkeit genügen (vgl. BVerfGE 100, 313 <359>), das heißt zur Erreichung der Zwecke geeignet, erforderlich und angemessen sind (vgl. BVerfGE 109, 279 <335 ff.>; 115, 320 <345>; 118, 168 <193>; 120, 274 <318 f.>; stRspr).

205 Eine sechsmonatige anlasslose Speicherung von Telekommunikationsverkehrsdaten für qualifizierte Verwendungen im Rahmen der Strafverfolgung, der Gefahrenabwehr und der Aufgaben der Nachrichtendienste, wie sie die §§ 113a, 113b TKG anordnen, ist danach mit Art. 10 GG nicht schlechthin unvereinbar. Der Gesetzgeber kann mit einer solchen Regelung legitime Zwecke verfolgen, für deren Erreichung eine solche Speicherung im Sinne des Verhältnismäßigkeitsgrundsatzes geeignet und erforderlich ist. Einer solchen Speicherung fehlt es auch in Bezug auf die Verhältnismäßigkeit im engeren Sinne nicht von vornherein an einer Rechtfertigungsfähigkeit. Bei einer Ausgestaltung, die dem besonderen Gewicht des hierin liegenden Eingriffs hinreichend Rechnung trägt, unterfällt eine anlasslose Speicherung der Telekommunikationsverkehrsdaten nicht schon als solche dem strikten Verbot einer Speicherung von Daten auf Vorrat im Sinne der Rechtsprechung des Bundesverfassungsgerichts (vgl. BVerfGE 65, 1 <46 f.>; 115, 320 <350>; 118, 168 <187>).

206 1. Die Effektivierung der Strafverfolgung, der Gefahrenabwehr und der Erfüllung der Aufgaben der Nachrichtendienste sind legitime Zwecke, die einen Eingriff in das Telekommunikationsgeheimnis grundsätzlich rechtfertigen können (vgl. BVerfGE 100, 313 <373, 383 f.>; 107, 299 <316>; 109, 279 <336>; 115, 320 <345>). Dabei liegt eine illegitime, das Freiheitsprinzip des Art. 10 Abs. 1 GG selbst aufhebende Zielsetzung nicht schon darin, dass die Telekommunikationsverkehrsdaten anlasslos vorsorglich gesichert werden sollen. Art. 10 Abs. 1 GG verbietet nicht jede vorsorgliche Erhebung und Speicherung von Daten überhaupt, sondern schützt vor einer unverhältnismäßigen Gestaltung solcher Datensammlungen und hierbei insbesondere vor entgrenzenden Zwecksetzungen. Strikt verboten ist lediglich die Speicherung von personenbezogenen Daten auf Vorrat zu unbestimmten und noch nicht bestimmbaren Zwecken (vgl. BVerfGE 65, 1 <46>; 100, 313 <360>). Eine vorsorglich anlasslose Datenspeicherung ist allerdings nur ausnahmsweise zulässig. Sie unterliegt sowohl hinsichtlich ihrer Begründung als auch hinsichtlich ihrer Ausgestaltung, insbesondere auch in Bezug auf die vorgesehenen Verwendungszwecke, besonders strengen Anforderungen.

207 2. Eine vorsorglich anlasslose Speicherung von Telekommunikationsverkehrsdaten zur späteren anlassbezogenen Übermittlung an die für die Strafverfolgung oder Gefahrenabwehr zuständigen Behörden beziehungsweise an die Nachrichtendienste darf der Gesetzgeber zur Erreichung seiner Ziele als geeignet ansehen. Es werden hierdurch Aufklärungsmöglichkeiten geschaffen, die sonst nicht bestünden und angesichts der zunehmenden Bedeutung der Telekommunikation auch für die Vorbereitung und Begehung von Straftaten in vielen Fällen erfolgversprechend sind. Unerheblich ist, ob die vom Gesetzgeber geschaffenen Regelungen in der Lage sind, lückenlos alle Telekommunikationsverbindungen zu rekonstruieren. Auch wenn eine solche Datenspeicherung nicht sicherstellen kann, dass alle Telekommunikationsverbindungen verlässlich bestimmten Anschlussnehmern zugeordnet werden können, und etwa Kriminelle die Speicherung durch die Nutzung von Hotspots, Internetcafés, ausländischen Internettelefondiensten oder unter falschen Namen angemeldeten Prepaid-Handys unterlaufen können, kann dies der Geeignetheit einer solchen Regelung nicht entgegenhalten werden. Diese erfordert nicht, dass das Regelungsziel in jedem Einzelfall tatsächlich erreicht wird, sondern verlangt lediglich, dass die Zweckerreichung gefördert wird (vgl. BVerfGE 63, 88 <115>; 67, 157 <175>; 96, 10 <23>; 103, 293 <307>).

208 3. Der Gesetzgeber darf eine sechsmonatige Speicherung der Telekommunikationsverkehrsdaten auch als erforderlich beurteilen. Weniger einschneidende Mittel, die ebenso weitreichende Aufklärungsmaßnahmen ermöglichen, sind nicht ersichtlich. Eine vergleichbar effektive Aufklärungsmöglichkeit liegt insbesondere nicht im sogenannten Quick-Freezing-Verfahren, bei dem an die Stelle der anlasslos-generellen Speicherung der Telekommunikationsdaten eine Speicherung nur im Einzelfall und erst zu dem Zeitpunkt angeordnet wird, zu dem dazu etwa wegen eines bestimmten Tatverdachts konkreter Anlass besteht. Ein solches Verfahren, das Daten aus der Zeit vor der Anordnung ihrer Speicherung nur erfassen kann, soweit sie noch vorhanden sind, ist nicht ebenso wirksam wie eine kontinuierliche Speicherung, die das Vorhandensein eines vollständigen Datenbestandes für die letzten sechs Monate gewährleistet.

209 4. Eine sechsmonatige Speicherung von Telekommunikationsverkehrsdaten in einem wie in § 113a TKG vorgesehenen Umfang ist auch nicht von vornherein unverhältnismäßig im engeren Sinne.

210 a) Allerdings handelt es sich bei einer solchen Speicherung um einen besonders schweren Eingriff mit einer Streubreite, wie sie die Rechtsordnung bisher nicht kennt: Erfasst werden über den gesamten Zeitraum von sechs Monaten praktisch sämtliche Telekommunikationsverkehrsdaten aller Bürger ohne Anknüpfung an ein zurechenbar vorwerfbares Verhalten, eine - auch nur abstrakte - Gefährlichkeit oder sonst eine qualifizierte Situation. Die Speicherung bezieht sich dabei auf Alltagshandeln, das im täglichen Miteinander elementar und für die Teilnahme am sozialen Leben in der modernen Welt nicht mehr verzichtbar ist. Grundsätzlich ist keine Form der Telekommunikation prinzipiell von der Speicherung ausgenommen. Zwar lässt die Regelung im Ergebnis vereinzelt Lücken, die verhindern, dass ausnahmslos jede Telekommunikationsverbindung individualisierend rekonstruiert werden kann, wie unter Umständen bei Nutzung von Hotspots, unübersichtlichen privaten Netzwerken oder Diensteanbietern im nichteuropäischen Ausland. Eine reguläre Ausweichmöglichkeit für den Bürger eröffnet dies jedoch nicht. Der Gesetzgeber versucht vielmehr, grundsätzlich alle Telekommuni-

kationsverbindungen so zu erfassen, dass die Nutzer möglichst flächendeckend ermittelt werden können.

211 Die Aussagekraft dieser Daten ist weitreichend. Je nach Nutzung von Telekommunikationsdiensten seitens der Betroffenen lassen sich schon aus den Daten selbst - und erst recht, wenn diese als Anknüpfungspunkte für weitere Ermittlungen dienen - tiefe Einblicke in das soziale Umfeld und die individuellen Aktivitäten eines jeden Bürgers gewinnen. Zwar werden mit einer Telekommunikationsverkehrsdatenspeicherung, wie in § 113a TKG vorgesehen, nur die Verbindungsdaten (Zeitpunkt, Dauer, beteiligte Anschlüsse sowie - bei der Mobiltelefonie - der Standort) festgehalten, nicht aber auch der Inhalt der Kommunikation. Auch aus diesen Daten lassen sich jedoch bei umfassender und automatisierter Auswertung bis in die Intimsphäre hineinreichende inhaltliche Rückschlüsse ziehen. Adressaten (deren Zugehörigkeit zu bestimmten Berufsgruppen, Institutionen oder Interessenverbänden oder die von ihnen angebotenen Leistungen), Daten, Uhrzeit und Ort von Telefongesprächen erlauben, wenn sie über einen längeren Zeitraum beobachtet werden, in ihrer Kombination detaillierte Aussagen zu gesellschaftlichen oder politischen Zugehörigkeiten sowie persönlichen Vorlieben, Neigungen und Schwächen derjenigen, deren Verbindungsdaten ausgewertet werden. Einen Vertraulichkeitsschutz gibt es insoweit nicht. Je nach Nutzung der Telekommunikation und künftig in zunehmender Dichte kann eine solche Speicherung die Erstellung aussagekräftiger Persönlichkeits- und Bewegungsprofile praktisch jeden Bürgers ermöglichen. Bezogen auf Gruppen und Verbände erlauben die Daten überdies unter Umständen die Aufdeckung von internen Einflussstrukturen und Entscheidungsabläufen.

212 Eine Speicherung, die solche Verwendungen grundsätzlich ermöglicht und in bestimmten Fällen ermöglichen soll, begründet einen schwerwiegenden Eingriff. Von Gewicht ist hierbei auch, dass unabhängig von einer wie auch immer geregelten Ausgestaltung der Datenverwendung das Risiko von Bürgern erheblich steigt, weiteren Ermittlungen ausgesetzt zu werden, ohne selbst Anlass dazu gegeben zu haben. Es reicht etwa aus, zu einem ungünstigen Zeitpunkt in einer bestimmten Funkzelle gewesen oder von einer bestimmten Person kontaktiert worden zu sein, um in weitem Umfang Ermittlungen ausgesetzt zu werden und unter Erklärungsdruck zu geraten. Auch die Missbrauchsmöglichkeiten, die mit einer solchen Datensammlung verbunden sind, verschärfen deren belastende Wirkung. Das gilt insbesondere wegen der Vielzahl verschiedener privater Anbieter, bei denen die Telekommunikationsdaten gespeichert werden. Schon angesichts der Anzahl der Speicherungsverpflichteten ist die Zahl derjenigen groß, die Zugriff auf solche Daten haben und haben müssen. Da die Speicherungspflicht kleinere Diensteanbieter mitbetrifft, stößt die Sicherung vor Missbrauch ungeachtet aller möglichen und erforderlichen Anstrengungen des Gesetzgebers auch in Blick auf deren Leistungsfähigkeit auf strukturelle Grenzen. Verstärkt wird dies dadurch, dass die Anforderungen an die Datenverwaltung und die Übermittlung der Daten an die Behörden ein hohes Maß an Technikbeherrschung sowie anspruchsvolle Software voraussetzen, womit sich zwangsläufig die Gefahr von Schwachstellen und das Risiko von Manipulationen durch interessierte Dritte verbinden. Besonderes Gewicht bekommt die Speicherung der Telekommunikationsdaten weiterhin dadurch, dass sie selbst und die vorgesehene Verwendung der gespeicherten Daten von den Betroffenen unmittelbar nicht bemerkt werden, zugleich aber Verbindungen erfassen, die unter Vertraulichkeitserwartungen aufgenommen werden. Hierdurch ist die anlasslose Speicherung von Telekommunikationsverkehrsdaten geeignet, ein diffus bedrohliches Gefühl des Beobachtetseins hervorzurufen, das eine unbefangene Wahrnehmung der Grundrechte in vielen Bereichen beeinträchtigen kann.

213 b) Trotz der außerordentlichen Streubreite und des mit ihr verbundenen Eingriffsgewichts ist dem Gesetzgeber die Einführung einer sechsmonatigen Speicherungspflicht, wie in § 113a TKG vorgesehen, verfassungsrechtlich nicht schlechthin verboten. Allerdings entspricht es der ständigen Rechtsprechung des Bundesverfassungsgerichts, dass dem Staat eine Sammlung von personenbezogenen Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken verfassungsrechtlich strikt untersagt ist (vgl. BVerfGE 65, 1 <46>; 100, 313 <360>; 115, 320 <350>; 118, 168 <187>). Um eine solche von vornherein verbotene Form der Datensammlung handelt es sich bei einer vorsorglich anlasslosen Speicherung der Telekommunikationsverbindungsdaten nicht in jedem Fall. Erfolgt sie zu bestimmten Zwecken, kann eine solche Speicherung eingebunden in eine dem Eingriff adäquate gesetzliche

Ausgestaltung (siehe unten V) vielmehr auch den Verhältnismäßigkeitsanforderungen im engeren Sinne genügen.

214 aa) Maßgeblich ist hierfür zunächst, dass die vorgesehene Speicherung der Telekommunikationsverkehrsdaten nicht direkt durch den Staat, sondern durch eine Verpflichtung der privaten Diensteanbieter verwirklicht wird. Die Daten werden damit bei der Speicherung selbst noch nicht zusammengeführt, sondern bleiben verteilt auf viele Einzelunternehmen und stehen dem Staat unmittelbar als Gesamtheit nicht zur Verfügung. Dieser hat insbesondere, was durch entsprechende Regelungen und technische Vorkehrungen sicherzustellen ist, keinen direkten Zugriff auf die Daten. Der Abruf der Daten seitens staatlicher Stellen erfolgt erst in einem zweiten Schritt und nunmehr anlassbezogen nach rechtlich näher festgelegten Kriterien. Die Ausgestaltung der zum Abruf und zur weiteren Verwendung der gespeicherten Daten ermächtigenden Bestimmungen kann dabei sicherstellen, dass die Speicherung nicht zu unbestimmten oder noch nicht bestimmbaren Zwecken erfolgt. So kann und muss bei Anordnung einer solchen Speicherungspflicht gewährleistet werden, dass eine tatsächliche Kenntnisnahme und Verwendung der Daten in normenklarer Form in einer Weise begrenzt bleibt, die dem Gewicht der weitreichenden Datenerfassung Rechnung trägt und den Abruf sowie die tatsächliche Verwendung der Daten auf den unbedingt erforderlichen Teil der Datensammlung beschränkt. Die Trennung von Speicherung und Abruf fördert strukturell zugleich die - durch gesetzliche Ausgestaltung näher zu gewährleistende - Transparenz und Kontrolle der Datenverwendung.

215 bb) Eine sechsmonatige Speicherung der Telekommunikationsverkehrsdaten hebt auch nicht bereits aus sich heraus das Prinzip des Art. 10 Abs. 1 GG als solches auf; sie verletzt weder dessen Menschenwürdekern (Art. 1 Abs. 1 GG) noch dessen Wesensgehalt (Art. 19 Abs. 2 GG). Sie bleibt trotz ihrer außerordentlichen Weite noch wirksam begrenzt. So wird der Inhalt der Telekommunikation von der auf die Verkehrsdaten beschränkten Speicherung ausgespart. Auch bleibt die Speicherungsdauer zeitlich begrenzt. Zwar ist eine Speicherungsdauer von sechs Monaten angesichts des Umfangs und der Aussagekraft der gespeicherten Daten sehr lang und liegt an der Obergrenze dessen, was unter Verhältnismäßigkeitserwägungen rechtfertigungsfähig ist. Nach ihrem Ablauf kann sich der Bürger jedoch darauf verlassen, dass seine Daten - sofern sie nicht aus gewichtigem Anlass ausnahmsweise abgerufen wurden - gelöscht werden und für niemanden mehr rekonstruierbar sind.

216 cc) Eine Speicherung der Telekommunikationsverkehrsdaten für sechs Monate stellt sich auch nicht als eine Maßnahme dar, die auf eine Totalerfassung der Kommunikation oder Aktivitäten der Bürger insgesamt angelegt wäre. Sie knüpft vielmehr in noch begrenzt bleibender Weise an die besondere Bedeutung der Telekommunikation in der modernen Welt an und reagiert auf das spezifische Gefahrenpotential, das sich mit dieser verbindet. Die neuen Telekommunikationsmittel überwinden Zeit und Raum in einer mit anderen Kommunikationsformen unvergleichbaren Weise und grundsätzlich unter Ausschluss öffentlicher Wahrnehmung. Sie erleichtern damit zugleich die verdeckte Kommunikation und Aktion von Straftätern und ermöglichen es auch verstreuten Gruppen von wenigen Personen, sich zusammenzufinden und effektiv zusammenzuarbeiten. Durch die praktisch widerstandsfreie Kommunikation wird eine Bündelung von Wissen, Handlungsbereitschaft und krimineller Energie möglich, die die Gefahrenabwehr und Strafverfolgung vor neuartige Aufgaben stellt. Manche Straftaten erfolgen unmittelbar mit Hilfe der neuen Technik. Eingebunden in ein Konglomerat von nurmehr technisch miteinander kommunizierenden Rechnern und Rechnernetzen entziehen sich solche Aktivitäten weithin der Beobachtung. Zugleich können sie - etwa durch Angriffe auf die Telekommunikation Dritter - auch neuartige Gefahren begründen. Eine Rekonstruktion gerade der Telekommunikationsverbindungen ist daher für eine effektive Strafverfolgung und Gefahrenabwehr von besonderer Bedeutung.

217 Hinzu kommt, dass es hinsichtlich der Telekommunikationsdaten mangels öffentlicher Wahrnehmbarkeit auch kein gesellschaftliches Gedächtnis gibt, das es wie in anderen Bereichen erlaubte, zurückliegende Vorgänge auf der Grundlage zufälliger Erinnerung zu rekonstruieren: Telekommunikationsdaten werden entweder gelöscht und sind dann ganz verloren oder werden gespeichert und sind damit voll verfügbar. Daher darf der Gesetzgeber bei der Entscheidung, wie weit solche Daten zu löschen oder zu speichern sind, einen Interessenausgleich vornehmen und die Belange staatlicher Aufgabenwahrnehmung berücksichtigen. Hierbei kann er auch in seine Erwägungen einbeziehen, dass die Verbreitung bestimmter Vertragsgestaltungen der Telekommunikationsdienste-

anbieter (wie die Zunahme von Flatrates) bei Geltung einer strikten Löschungspflicht für Telekommunikationsverkehrsdaten, die für die Vertragsabwicklung nicht benötigt werden, die Verfügbarkeit solcher Daten reduziert. Auch insoweit kann sich die vorsorgliche Speicherung der Telekommunikationsverkehrsdaten auf Gesichtspunkte stützen, die in Besonderheiten der modernen Telekommunikation einen spezifischen Grund haben.

218 Umgekehrt darf die Speicherung der Telekommunikationsverkehrsdaten nicht als Schritt hin zu einer Gesetzgebung verstanden werden, die auf eine möglichst flächendeckende vorsorgliche Speicherung aller für die Strafverfolgung oder Gefahrenprävention nützlichen Daten zielte. Eine solche Gesetzgebung wäre, unabhängig von der Gestaltung der Verwendungsregelungen, von vornherein mit der Verfassung unvereinbar. Die verfassungsrechtliche Unbedenklichkeit einer vorsorglich anlasslosen Speicherung der Telekommunikationsverkehrsdaten setzt vielmehr voraus, dass diese eine Ausnahme bleibt. Sie darf auch nicht im Zusammenspiel mit anderen vorhandenen Dateien zur Rekonstruierbarkeit praktisch aller Aktivitäten der Bürger führen. Maßgeblich für die Rechtfertigungsfähigkeit einer solchen Speicherung ist deshalb insbesondere, dass sie nicht direkt durch staatliche Stellen erfolgt, dass sie nicht auch die Kommunikationsinhalte erfasst und dass auch die Speicherung der von ihren Kunden aufgerufenen Internetseiten durch kommerzielle Diensteanbieter grundsätzlich untersagt ist. Die Einführung der Telekommunikationsverkehrsdatenspeicherung kann damit nicht als Vorbild für die Schaffung weiterer vorsorglich anlassloser Datensammlungen dienen, sondern zwingt den Gesetzgeber bei der Erwägung neuer Speicherungspflichten oder -berechtigungen in Blick auf die Gesamtheit der verschiedenen schon vorhandenen Datensammlungen zu größerer Zurückhaltung. Dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf, gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland (vgl. zum grundgesetzlichen Identitätsvorbehalt BVerfG, Urteil des Zweiten Senats vom 30. Juni 2009 - 2 BvE 2/08 u.a. -, juris, Rn. 240), für deren Wahrung sich die Bundesrepublik in europäischen und internationalen Zusammenhängen einsetzen muss. Durch eine vorsorgliche Speicherung der Telekommunikationsverkehrsdaten wird der Spielraum für weitere anlasslose Datensammlungen auch über den Weg der Europäischen Union erheblich geringer.

219 dd) Zusammenfassend ist eine sechsmonatige Speicherung der Telekommunikationsverkehrsdaten in dem vom Gesetzgeber in § 113a Abs. 1 bis 8 TKG vorgesehenen Umfang unter den gegenwärtigen Umständen nicht von vornherein unverhältnismäßig. Für ihre verfassungsrechtliche Unbedenklichkeit ist allerdings Voraussetzung, dass die Ausgestaltung der Speicherung und der Verwendung der Daten dem besonderen Gewicht einer solchen Speicherung angemessen Rechnung trägt.

V.

220 FÖR-Systematik: Cyberlaw-Highlight – BVerfG „Reserve- und Zukunftsgesetzgebung“

Die Ausgestaltung einer vorsorglichen Telekommunikationsverkehrsdatenspeicherung, wie sie in § 113a TKG vorgesehen ist, unterliegt besonderen verfassungsrechtlichen Anforderungen insbesondere hinsichtlich der Datensicherheit, des Umfangs der Datenverwendung, der Transparenz und des Rechtsschutzes. Nur wenn diesbezüglich hinreichend anspruchsvolle und normenklare Regelungen getroffen sind, ist der in einer solchen Speicherung liegende Eingriff verhältnismäßig im engeren Sinne.

221 FÖR-Systematik: Cyberlaw-Highlight – Zweistufiges Schutzkonzept (rechtlich und/oder technisch)

1. Eine Speicherung der Telekommunikationsverkehrsdaten im Umfang des § 113a TKG bedarf der **gesetzlichen Gewährleistung eines besonders hohen Standards der Datensicherheit.**

222 Angesichts des Umfangs und der potentiellen Aussagekraft der mit einer solchen Speicherung geschaffenen Datenbestände ist die Datensicherheit für die Verhältnismäßigkeit der angegriffenen Vorschriften von großer Bedeutung. Dieses gilt besonders, weil die Daten bei privaten Diensteanbietern gespeichert werden, die unter den Bedingungen von Wirtschaftlichkeit und Kostendruck handeln und dabei nur begrenzte Anreize zur Gewährleistung von Datensicherheit haben. Sie handeln grundsätzlich

privatnützig und sind nicht durch spezifische Amtspflichten gebunden. Zugleich ist die Gefahr eines illegalen Zugriffs auf die Daten groß, denn angesichts ihrer vielseitigen Aussagekraft können diese für verschiedenste Akteure attraktiv sein. Geboten ist daher ein besonders hoher Sicherheitsstandard, der über das allgemein verfassungsrechtlich gebotene Maß für die Aufbewahrung von Daten der Telekommunikation hinausgeht. Solche Anforderungen der Datensicherheit gelten dabei sowohl für die Aufbewahrung der Daten als auch für deren Übermittlung; ebenso bedarf es effektiver Sicherungen zur Gewährleistung der Löschung der Daten.

223 In den Äußerungen in der mündlichen Verhandlung sowie in den schriftlichen Stellungnahmen zu diesem Verfahren wurde von sachverständiger Seite ein weites Spektrum von Instrumenten zur Erhöhung der Datensicherheit aufgezeigt. Genannt wurden etwa eine getrennte Speicherung der nach § 113a TKG zu speichernden Daten auf auch physisch getrennten und vom Internet entkoppelten Rechnern, eine asymmetrische kryptografische Verschlüsselung unter getrennter Verwahrung der Schlüssel, die Vorgabe des Vier-Augen-Prinzips für den Zugriff auf die Daten verbunden mit fortschrittlichen Verfahren zur Authentifizierung für den Zugang zu den Schlüsseln, die revisionssichere Protokollierung des Zugriffs auf die Daten und deren Löschung sowie der Einsatz von automatisierten Fehlerkorrektur- und Plausibilitäts-verfahren. Ergänzend zu solch technisch orientierten Instrumenten ist auch die Schaffung von Informations-pflichten bei Datenschutzverletzungen, die Einführung einer verschuldensunabhängigen Haftung oder eine Stärkung der Ausgleichsansprüche für immaterielle Schäden genannt worden, um so Anreiz für die Imple-mentierung eines wirksamen Datenschutzes zu schaffen.

224 Die Verfassung gibt nicht detailgenau vor, welche Sicherheitsmaßgaben im Einzelnen geboten sind. Im Ergebnis muss jedoch ein Standard gewährleistet werden, der unter spezifischer Berücksichtigung der Besonderheiten der durch eine vorsorgliche Telekommunikationsverkehrsdatenspeicherung geschaffenen Datenbestände ein besonders hohes Maß an Sicherheit gewährleistet. Dabei ist sicherzustellen, dass sich dieser Standard - etwa unter Rückgriff auf einfachgesetzliche Rechtsfiguren wie den Stand der Technik (vgl. Heibey, in: Roßnagel, Handbuch Datenschutzrecht, 2003, S. 575, Rn. 19, S. 598, Rn. 145; Tinnefeld/ Ehrmann/Gerling, Einführung in das Datenschutzrecht, 4. Aufl. 2005, S. 628) - an dem Entwicklungsstand der Fachdiskussion orientiert und neue Erkenntnisse und Einsichten fortlaufend aufnimmt. Entsprechend ist vorzusehen, dass die speicherpflichtigen Unternehmen - zum Beispiel auf der Grundlage von in regelmäßigen Abständen zu erneuernden Sicherheitskonzepten - ihre Maßnahmen hieran nachprüfbar anpassen müssen. Das Gefährdungspotential, das sich aus den in Frage stehenden Datenbeständen ergibt, erlaubt es nicht, die beschriebenen Sicherheitsanforderungen einer freien Abwägung mit allgemeinen wirtschaftlichen Gesichtspunkten zu unterwerfen. Wenn der Gesetzgeber eine flächendeckende Speicherung der Telekommunikationsverkehrsdaten ausnahmslos vorschreibt, gehört es zu den erforderlichen Voraussetzungen, dass die betroffenen Anbieter nicht nur ihre Pflicht zur Speicherung, sondern auch die korrespondierenden Anforderungen zur Datensicherheit erfüllen können. Anknüpfend an die sachver-ständigen Stellungnahmen liegt es nahe, dass nach dem gegenwärtigen Stand der Diskussion grundsätzlich eine getrennte Speicherung der Daten, eine anspruchsvolle Verschlüsselung, ein gesichertes Zugriffsregime unter Nutzung etwa des Vier-Augen-Prinzips sowie eine revisionssichere Protokollierung sichergestellt sein müssen, um die Sicherheit der Daten verfassungsrechtlich hinreichend zu gewährleisten.

225 **Erforderlich sind gesetzliche Regelungen, die einen solchen besonders hohen Sicherheitsstandard in qualifizierter Weise jedenfalls dem Grunde nach normenklar und verbindlich vorgeben. Dabei steht es dem Gesetzgeber frei, die technische Konkretisierung des vorgegebenen Maßstabs einer Aufsichtsbehörde anzuvertrauen. Der Gesetzgeber hat dabei jedoch sicherzustellen, dass die Entscheidung über Art und Maß der zu treffenden Schutzvorkehrungen nicht letztlich unkontrolliert in den Händen der jeweiligen Telekommunikationsanbieter liegt.** Die zu stellenden Anforderungen sind entweder durch differenzierte technische Vorschriften - möglicherweise gestuft auf verschiedenen Normebenen - oder in allgemein-genereller Weise vorzugeben und dann in transparenter Weise durch verbindliche Einzelentscheidung der Aufsichtsbehörden gegenüber den einzelnen Unternehmen zu konkretisieren. Verfassungsrechtlich geboten sind weiterhin eine für die Öffentlichkeit transparente Kontrolle unter

Einbeziehung des unabhängigen Datenschutzbeauftragten (vgl. BVerfGE 65, 1 <46>) sowie ein ausgeglichenes Sanktionensystem, das auch Verstößen gegen die Datensicherheit ein angemessenes Gewicht beimisst.

226 2. Eine Speicherung von Telekommunikationsverkehrsdaten, wie in § 113a TKG vorgesehen, setzt weiterhin gesetzliche Regelungen zur Verwendung dieser Daten voraus. Die verhältnismäßige Ausgestaltung dieser Verwendungsregeln entscheidet damit nicht nur über die Verfassungsmäßigkeit dieser einen eigenen Eingriff begründenden Bestimmungen selbst, sondern wirkt auf die Verfassungsmäßigkeit schon der Speicherung als solcher zurück. Nach der Rechtsprechung des Bundesverfassungsgerichts müssen die Voraussetzungen für die Datenverwendung und deren Umfang in den betreffenden Rechtsgrundlagen umso enger begrenzt werden, je schwerer der in der Speicherung liegende Eingriff wiegt. Anlass, Zweck und Umfang des jeweiligen Eingriffs sowie die entsprechenden Eingriffsschwellen sind dabei durch den Gesetzgeber bereichsspezifisch, präzise und normenklar zu regeln (vgl. BVerfGE 100, 313 <359 f.>; 110, 33 <53>; 113, 29 <51>; 113, 348 <375>; 115, 166 <191>; 115, 320 <365>; 118, 168 <186 f.>).

227 Die Verwendung der durch eine anlasslos systematische Speicherung praktisch aller Telekommunikationsverkehrsdaten gewonnenen Datenbestände unterliegt dementsprechend besonders hohen Anforderungen. Insbesondere ist diese nicht in gleichem Umfang verfassungsrechtlich zulässig wie die Verwendung von Telekommunikationsverkehrsdaten, die die Diensteanbieter in Abhängigkeit von den jeweiligen betrieblichen und vertraglichen Umständen - von den Kunden teilweise beeinflussbar - nach § 96 TKG speichern dürfen. Angesichts der Unausweichlichkeit, Vollständigkeit und damit gesteigerten Aussagekraft der über sechs Monate systematisch vorsorglich erhobenen Verkehrsdaten hat ihr Abruf ein ungleich größeres Gewicht. Da eine Auswertung dieser Daten tief in das Privatleben eindringende Rückschlüsse und unter Umständen detaillierte Persönlichkeits- und Bewegungsprofile ermöglicht, kann insoweit nicht ohne weiteres davon ausgegangen werden, dass der Rückgriff auf diese Daten grundsätzlich geringer wiegt als eine inhaltsbezogene Telekommunikationsüberwachung (zur Abfrage nach altem Recht vgl. BVerfGE 107, 299 <322>). Vielmehr kann auch die Verwendung solcher Daten nur dann als verhältnismäßig angesehen werden, wenn sie besonders hochrangigen Gemeinwohlbelangen dient. Eine Verwendung der Daten kommt deshalb nur für überragend wichtige Aufgaben des Rechtsgüterschutzes in Betracht, das heißt zur Ahndung von Straftaten, die überragend wichtige Rechtsgüter bedrohen oder zur Abwehr von Gefahren für solche Rechtsgüter.

228 a) Für die Strafverfolgung folgt hieraus, dass ein Abruf der Daten zumindest den durch bestimmte Tatsachen begründeten Verdacht einer schweren Straftat voraussetzt. Welche Straftatbestände hiervon umfasst sein sollen, hat der Gesetzgeber abschließend mit der Verpflichtung zur Datenspeicherung festzulegen. Ihm kommt hierbei ein Beurteilungsspielraum zu. Er kann dabei entweder auf bestehende Kataloge zurückgreifen oder einen eigenen Katalog schaffen, etwa um Straftaten, für die die Telekommunikationsverkehrsdaten besondere Bedeutung haben, zu erfassen. Die Qualifizierung einer Straftat als schwer muss aber in der Strafnorm - insbesondere etwa durch deren Strafrahmen - einen objektivierten Ausdruck finden (vgl. BVerfGE 109, 279 <343 ff., insbesondere 347 f.>). Eine Generalklausel oder lediglich die Verweisung auf Straftaten von erheblicher Bedeutung reichen hingegen nicht aus.

229 Über die abstrakte Festlegung eines entsprechenden Straftatenkatalogs hinaus hat der Gesetzgeber sicherzustellen, dass ein Rückgriff auf die vorsorglich gespeicherten Telekommunikationsverkehrsdaten nur dann zulässig ist, wenn auch im Einzelfall die verfolgte Straftat schwer wiegt (vgl. BVerfGE 121, 1 <26>; zu Straftaten von erheblicher Bedeutung vgl. BVerfGE 107, 299 <322>; zu besonders schweren Straftaten im Sinne von Art. 13 Abs. 3 GG vgl. BVerfGE 109, 279 <346>) und die Verwendung der Daten verhältnismäßig ist.

230 b) Für die Gefahrenabwehr ist die Verwendung der in Frage stehenden Daten gleichermaßen wirksam zu begrenzen. Den Datenzugriff unter Bezugnahme auf Kataloge von bestimmten Straftaten zu eröffnen, deren Verhinderung die Datenverwendung dienen soll (vgl. BVerfGE 122, 120 <142>), ist hier keine geeignete Regelungstechnik. Sie nimmt den Anforderungen an den Grad der Rechtsgutgefährdung ihre Klarheit und führt zu Unsicherheiten, wenn schon die Straftatbestände selbst

Vorbereitungshandlungen und bloße Rechtsgutgefährdungen unter Strafe stellen. Stattdessen bietet sich an, gesetzlich unmittelbar die Rechtsgüter in Bezug zu nehmen, deren Schutz eine Verwendung der Daten rechtfertigen soll, sowie die Intensität der Gefährdung dieser Rechtsgüter, die als Eingriffsschwelle hierfür erreicht sein muss. Eine solche Regelung entspricht dem Charakter der Gefahrenabwehr als Rechtsgüterschutz und gewährleistet eine unmittelbare Anknüpfung an das maßgebliche Ziel, das den Grundrechtseingriff rechtfertigen soll.

231 Die Abwägung zwischen dem Gewicht des in der Datenspeicherung und Datenverwendung liegenden Eingriffs und der Bedeutung einer wirksamen Gefahrenabwehr führt dazu, dass ein Abruf der vorsorglich gespeicherten Telekommunikationsverkehrsdaten nur zur Abwehr von Gefahren für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder zur Abwehr einer gemeinen Gefahr zugelassen werden darf (vgl. BVerfGE 122, 120 <141 ff.>). Die gesetzliche Ermächtigungsgrundlage muss diesbezüglich zumindest tatsächliche Anhaltspunkte einer konkreten Gefahr für die zu schützenden Rechtsgüter verlangen. Dieses Erfordernis führt dazu, dass Vermutungen oder allgemeine Erfahrungssätze nicht ausreichen, um den Zugriff auf die Daten zu rechtfertigen. Vielmehr müssen bestimmte Tatsachen festgestellt sein, die die Prognose einer konkreten Gefahr tragen. Es bedarf insoweit einer Sachlage, bei der im Einzelfall die hinreichende Wahrscheinlichkeit besteht, dass in absehbarer Zeit ohne Eingreifen des Staates ein Schaden für die Schutzgüter der Norm durch bestimmte Personen verursacht wird. Die diesbezüglichen Ausführungen des Senats zu den Anforderungen an Online-Durchsuchungen gelten hier entsprechend (vgl. BVerfGE 120, 274 <328 f.>). Die konkrete Gefahr wird durch drei Kriterien bestimmt: den Einzelfall, die zeitliche Nähe des Umschlagens einer Gefahr in einen Schaden und den Bezug auf individuelle Personen als Verursacher. Die Abfrage der vorsorglich gespeicherten Daten kann allerdings schon gerechtfertigt sein, wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr schon in näherer Zukunft eintritt, sofern bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen. Die Tatsachen müssen zum einen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, zum anderen darauf, dass bestimmte Personen beteiligt sein werden, über deren Identität zumindest so viel bekannt ist, dass die Maßnahme gezielt gegen sie eingesetzt und auf sie konzentriert werden kann. Dagegen wird dem Gewicht des Grundrechtseingriffs nicht hinreichend Rechnung getragen, wenn der tatsächliche Eingriffsanlass noch weitgehend in das Vorfeld einer im Einzelnen noch nicht absehbaren konkreten Gefahr für die Schutzgüter der Norm verlegt wird.

232 c) Die verfassungsrechtlichen Anforderungen für die Verwendung der Daten zur Gefahrenabwehr gelten für alle Eingriffsermächtigungen mit präventiver Zielsetzung. Sie gelten damit auch für die Verwendung der Daten durch die Nachrichtendienste. Da die Beeinträchtigung durch den Eingriff in allen diesen Fällen für die Betroffenen die gleiche ist, besteht hinsichtlich dieser Anforderungen kein Anlass zu behördenbezogenen Differenzierungen, etwa zwischen Polizeibehörden und anderen mit präventiven Aufgaben betrauten Behörden wie Verfassungsschutzbehörden. Dass Polizei- und Verfassungsschutzbehörden unterschiedliche Aufgaben und Befugnisse haben und in der Folge Maßnahmen mit unterschiedlicher Eingriffstiefe vornehmen können, ist für die Gewichtung einer Verwendung von vorsorglich flächendeckend und langfristig gespeicherten Telekommunikations-verkehrsdaten grundsätzlich ohne Belang (vgl. BVerfGE 120, 274 <329 f.>). Zwar können Differenzierungen zwischen den Ermächtigungen der verschiedenen Behörden mit präventiven Aufgaben vor der Verfassung Bestand haben (vgl. BVerfGE 100, 313 <383>; 120, 274 <330>). Jedoch ist der Gesetzgeber auch bei der Regelung der einzelnen Befugnisse von Sicherheitsbehörden, deren Aufgabe in der Vorfeldaufklärung besteht, an die verfassungsrechtlichen Vorgaben gebunden, die sich aus dem Verhältnismäßigkeitsgrundsatz ergeben (vgl. BVerfGE 120, 274 <330 f.>). Diese führen vorliegend dazu, dass sowohl hinsichtlich der zu schützenden Rechtsgüter als auch hinsichtlich der hierbei zu beachtenden Eingriffsschwelle besondere Anforderungen an die Datenverwendung zu stellen sind.

233 Es gibt keinen Grund, warum diese Anforderungen für die Aufgabenerfüllung der Nachrichtendienste nicht gelten sollten. Zwar beschränken sich die Aufgaben der Nachrichtendienste grundsätzlich auf die Sammlung von Informationen zur Unterrichtung der Regierung. Das vermindert das Gewicht des Eingriffs insoweit, als sich damit für den einzelnen Bürger über die Gefahr des

Beobachtetwerdens hinaus nicht auch die Gefahr von hieran anknüpfenden weiteren Maßnahmen verbindet. Zugleich verringert sich hierdurch aber auch das Gewicht zur Rechtfertigung solcher Eingriffe, denn durch bloße Informationen der Regierung können Rechtsgutverletzungen nicht verhindert werden. Dies ist erst möglich durch Folgemaßnahmen der für die Gefahrenabwehr zuständigen Behörden, deren verfassungsrechtliche Begrenzungen bei der Datenverwendung nicht durch weitergehende Verwendungsbefugnisse im Vorfeld unterlaufen werden dürfen. Eine besondere Belastungswirkung solcher Eingriffe gegenüber den Bürgern liegt im Übrigen darin, dass nicht nur der jeweilige Eingriff in das Telekommunikationsgeheimnis als solcher in der Regel verdeckt geschieht, sondern praktisch die gesamten Aktivitäten der Nachrichtendienste geheim erfolgen. Befugnisse dieser Dienste zur Verwendung der vorsorglich flächendeckend gespeicherten Telekommunikationsverkehrsdaten befördern damit das Gefühl des unkontrollierbaren Beobachtetwerdens in besonderer Weise und entfalten nachhaltige Einschüchterungseffekte auf die Freiheitswahrnehmung.

234 Der Senat verkennt nicht, dass damit eine Verwendung der vorsorglich gespeicherten Telekommunikationsverkehrsdaten von Seiten der Nachrichtendienste in vielen Fällen ausscheiden dürfte. Dies liegt jedoch in der Art ihrer Aufgaben als Vorfeldaufklärung und begründet keinen verfassungsrechtlich hinnehm-baren Anlass, die sich aus dem Verhältnismäßigkeitsgrundsatz ergebenden Voraussetzungen für einen Eingriff der hier vorliegenden Art abzumildern (vgl. BVerfGE 120, 274 <331>).

235 d) Die Begrenzung der Datenverwendung auf bestimmte Zwecke muss auch für die Verwendung der Daten nach deren Abruf und Übermittlung an die abrufenden Behörden sichergestellt und verfahrensmäßig flankiert werden. Insoweit ist gesetzlich zu gewährleisten, dass die Daten nach Übermittlung unverzüglich ausgewertet werden und, sofern sie für die Erhebungszwecke unerheblich sind, gelöscht werden (vgl. BVerfGE 100, 313 <387 f.>). Im Übrigen ist vorzusehen, dass die Daten vernichtet werden, sobald sie für die festgelegten Zwecke nicht mehr erforderlich sind, und dass hierüber ein Protokoll gefertigt wird (vgl. BVerfGE 100, 313 <362>; 113, 29 <58>).

236 Die Telekommunikationsverkehrsdaten verlieren ihren durch Art. 10 GG vermittelten Schutz nicht dadurch, dass bereits eine staatliche Stelle von ihnen Kenntnis erlangt hat. Die Anforderungen des Grundrechts an eine klare Zweckbindung beziehen sich deshalb auch auf die Weitergabe der Daten und Informationen an weitere Stellen. Dies schließt Zweckänderungen indes nicht aus. Sie bedürfen jedoch einer eigenen gesetzlichen Grundlage, die ihrerseits verfassungsrechtlichen Ansprüchen genügt (vgl. BVerfGE 100, 313 <360>; 109, 279 <375 f.>). Eine Weitergabe der übermittelten Telekommunikationsverkehrsdaten an andere Stellen darf gesetzlich dementsprechend nur vorgesehen werden, soweit sie zur Wahrnehmung von Aufgaben erfolgt, deretwegen ein Zugriff auf diese Daten auch unmittelbar zulässig wäre (vgl. BVerfGE 100, 313 <389 f.>; 109, 279 <375 f.>; 110, 33 <73>). Dies ist von der weiterleitenden Stelle zu protokollieren (vgl. BVerfGE 100, 313 <395 f.>). Dabei lässt sich die Zweckbindung nur gewährleisten, wenn auch nach der Erfassung erkennbar bleibt, dass es sich um Daten handelt, die vorsorglich anlasslos gespeichert wurden. Der Gesetzgeber hat dementsprechend für diese Daten eine Kennzeichnungspflicht anzuordnen (vgl. BVerfGE 100, 313 <360 f.>).

237 e) Verfassungsrechtliche Grenzen können sich schließlich auch hinsichtlich des Umfangs der abzurufenden Daten ergeben. So lassen sich unter Verhältnismäßigkeitsgesichtspunkten vielfältige Abstufungen zwischen den verschiedenen Auskunftsbegehren ausmachen, etwa danach, ob sie nur eine einzelne Telekommunikationsverbindung betreffen, sie auf die Übermittlung der Daten aus allein einer Funkzelle zu einem bestimmten Zeitpunkt zielen, sie bezogen sind nur auf die Kommunikation zwischen einzelnen Personen - begrenzt möglicherweise auf einen bestimmten Zeitraum oder eine bestimmte Form der Kommunikation - und hierbei auch die Standortdaten ein- oder ausschließen beziehungsweise ob sie auf eine vollständige Übermittlung der Daten einer Person zur Erstellung eines möglichst detaillierten Bewegungs- oder Persönlichkeitsprofils zielen. Auch kann es in Blick auf das Eingriffsgewicht einen Unterschied machen, ob bei der Datenübermittlung Filter zwischengeschaltet werden, mit denen bestimmte Telekommunikationsverbindungen zum Schutz von besonderen Vertrauensbeziehungen ausgesondert werden.

238 Angesichts der hohen Schwellen, die nach den vorstehenden Maßgaben schon grundsätzlich für die Verwendung vorsorglich gespeicherter Telekommunikationsverkehrsdaten gelten, hat der Gesetzgeber bei der näheren Regelung des Umfangs der Datenverwendung allerdings einen

Gestaltungsspielraum. Insbesondere steht es ihm grundsätzlich auch frei, solche Verhältnismäßigkeitserwägungen dem zur Entscheidung über die Anordnung eines Datenabrufs berufenen Richter bei der Prüfung im Einzelfall zu überlassen. Verfassungsrechtlich geboten ist als Ausfluss des Verhältnismäßigkeitsgrundsatzes jedoch, zumindest für einen engen Kreis von auf besondere Vertraulichkeit angewiesenen Telekommunikations-verbindungen ein grundsätzliches Übermittlungsverbot vorzusehen. Zu denken ist hier etwa an Verbin-dungen zu Anschlüssen von Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen, die grundsätzlich anonym bleibenden Anrufern ganz oder überwiegend telefonische Beratung in seelischen oder sozialen Notlagen anbieten und die selbst oder deren Mitarbeiter insoweit anderen Verschwiegenheits-verpflichtungen unterliegen (vgl. § 99 Abs. 2 TKG).

239 3. Verhältnismäßig ist eine vorsorglich anlasslose Speicherung von Telekommunikationsver-kehrsdaten und deren Verwendung weiterhin nur, wenn der Gesetzgeber hinreichende Vorkehrungen zur Transparenz der Datenverwendung sowie zur Gewährleistung eines effektiven Rechtsschutzes und effektiver Sanktionen trifft.

240 a) Zu den Voraussetzungen der verfassungsrechtlich unbedenklichen Verwendung von durch eine solche Speicherung gewonnenen Daten gehören Anforderungen an die Transparenz. Soweit möglich muss die Verwendung der Daten offen erfolgen. Ansonsten bedarf es grundsätzlich zumindest nachträglich einer Benachrichtigung der Betroffenen. Unterbleibt ausnahmsweise auch diese, bedarf die Nichtbenachrichtigung einer richterlichen Entscheidung.

241 aa) Eine vorsorglich anlasslose Speicherung aller Telekommunikationsverkehrsdaten über sechs Monate ist unter anderem deshalb ein so schwerwiegender Eingriff, weil sie ein Gefühl des ständigen Überwachtwerdens hervorrufen kann; sie erlaubt in unvorhersehbarer Weise tiefe Einblicke in das Privatleben, ohne dass der Rückgriff auf die Daten für den Bürger unmittelbar spürbar oder ersichtlich ist. Der Einzelne weiß nicht, was welche staatliche Behörde über ihn weiß, weiß aber, dass die Behörden vieles, auch Höchstpersönliches über ihn wissen können.

242 Der Gesetzgeber muss die diffuse Bedrohlichkeit, die die Datenspeicherung hierdurch erhalten kann, durch wirksame Transparenzregeln auffangen. Regelungen zur Information der von Datenerhebungen oder -nutzungen Betroffenen gehören allgemein zu den elementaren Instrumenten des grundrechtlichen Datenschutzes (vgl. BVerfGE 100, 313 <361>; 109, 279 <363 f.>; 118, 168 <207 f.>; 120, 351 <361 f.>). Für die Verwendung der umfangreichen und vielfältig aussagekräftigen Datenbestände einer vorsorglich anlasslosen Telekommunikationsverkehrsdatenspeicherung sind insoweit hohe Anforderungen zu stellen. Sie haben zum einen die Aufgabe, eine sich aus dem Nichtwissen um die tatsächliche Relevanz der Daten ergebende Bedrohlichkeit zu mindern, verunsichernden Spekulationen entgegenzuwirken und den Betroffenen die Möglichkeit zu schaffen, solche Maßnahmen in die öffentliche Diskussion zu stellen. Zum anderen sind solche Anforderungen auch aus dem Gebot des effektiven Rechtsschutzes gemäß Art. 10 Abs. 1 GG in Verbindung mit Art. 19 Abs. 4 GG herzuleiten. Ohne Kenntnis können die Betroffenen weder eine Unrechtmäßigkeit der behördlichen Datenverwendung noch etwaige Rechte auf Löschung, Berichtigung oder Genugtuung geltend machen (vgl. BVerfGE 100, 313 <361>; 109, 279 <363>; 118, 168 <207 f.>; 120, 351 <361>).

243 bb) Zu den Transparenzanforderungen zählt der Grundsatz der Offenheit der Erhebung und Nutzung von personenbezogenen Daten. Eine Verwendung der Daten ohne Wissen des Betroffenen ist verfassungsrechtlich nur dann zulässig, wenn andernfalls der Zweck der Untersuchung, dem der Datenabruf dient, vereitelt wird. Für die Gefahrenabwehr und die Wahrnehmung der Aufgaben der Nachrichtendienste darf der Gesetzgeber dies grundsätzlich annehmen. Demgegenüber kommt im Rahmen der Strafverfolgung auch eine offene Erhebung und Nutzung der Daten in Betracht (vgl. § 33 Abs. 3 und 4 StPO). Ermittlungsmaßnahmen werden hier zum Teil auch sonst mit Kenntnis des Beschuldigten und in seiner Gegenwart durchgeführt (vgl. zum Beispiel §§ 102, 103, 106 StPO). Dementsprechend ist der Betroffene vor der Abfrage beziehungsweise Übermittlung seiner Daten grundsätzlich zu benachrichtigen. Eine heimliche Verwendung der Daten darf nur vorgesehen werden, wenn sie im Einzelfall erforderlich und richterlich angeordnet ist.

244 FÖR-Systematik: Cyberlaw Highlight – Reaktiver Rechtsschutz – Benachrichtigung

Soweit die Verwendung der Daten heimlich erfolgt, hat der Gesetzgeber die Pflicht einer zumindest nachträglichen Benachrichtigung vorzusehen. Diese muss gewährleisten, dass diejenigen, auf die sich eine Datenabfrage - sei es als Beschuldigte, Polizeipflichtige oder Dritte - unmittelbar bezogen hat, wenigstens im Nachhinein grundsätzlich in Kenntnis zu setzen sind. Ausnahmen kann der Gesetzgeber in Abwägung mit verfassungsrechtlich geschützten Rechtsgütern Dritter vorsehen. Sie sind jedoch auf das unbedingt Erforderliche zu beschränken (vgl. BVerfGE 109, 279 <364>). Denkbar sind Ausnahmen von den Benachrichtigungspflichten im Zusammenhang mit der Strafverfolgung etwa, wenn die Kenntnis des Eingriffs in das Telekommunikationsgeheimnis dazu führen würde, dass dieser seinen Zweck verfehlt, wenn die Benachrichtigung nicht ohne Gefährdung von Leib und Leben einer Person geschehen kann oder wenn ihr überwiegende Belange einer betroffenen Person entgegenstehen, etwa weil durch die Benachrichtigung von einer Maßnahme, die keine weiteren Folgen gehabt hat, der Grundrechtseingriff noch vertieft würde (vgl. BVerfGE 100, 313 <361>; 109, 279 <364 ff.>). Liegen zwingende Gründe vor, die auch eine nachträgliche Benachrichtigung ausschließen, ist dieses richterlich zu bestätigen und in regelmäßigen Abständen zu prüfen (vgl. BVerfGE 109, 279 <367 f.>). In entsprechender Weise bedarf es einer Ausgestaltung der Benachrichtigungspflichten auch hinsichtlich der Verwendung der Daten für Zwecke der Gefahrenabwehr oder der Aufgaben der Nachrichtendienste.

245 Verfassungsrechtlich nicht geboten sind demgegenüber vergleichbar strenge Benachrichtigungspflichten gegenüber Personen, deren Telekommunikationsverkehrsdaten nur zufällig miterfasst wurden und die selbst nicht im Fokus des behördlichen Handelns standen. Solche Beteiligte kann es bei der Auswertung von Telekommunikationsverkehrsdaten in großem Umfang geben, ohne dass das kurzfristige Bekanntwerden ihrer Daten Spuren hinterlassen oder Folgen für den Betroffenen haben muss. Eine Benachrichtigung kann ihnen gegenüber im Einzelfall den Eingriff vielmehr vertiefen (vgl. BVerfGE 109, 279 <365>; BVerfGK 9, 62 <81>). In diesen Fällen kann eine Benachrichtigung grundsätzlich schon dann unterbleiben, wenn die Betroffenen von der Maßnahme nur unerheblich betroffen wurden und anzunehmen ist, dass sie kein Interesse an der Benachrichtigung haben. Einer richterlichen Bestätigung dieser Abwägungsentscheidung bedarf es nicht.

246 FÖR-Systematik: Cyberlaw Highlight – Effektiver Rechtsschutz und adäquate Sanktionen

b) Die verhältnismäßige Ausgestaltung einer vorsorglichen Speicherung der Telekommunikationsverkehrsdaten und ihrer Verwendung verlangt weiterhin die Gewährleistung eines effektiven Rechtsschutzes und adäquater Sanktionen.

247 aa) Für die Gewährleistung effektiven Rechtsschutzes ist eine Abfrage oder Übermittlung dieser Daten grundsätzlich unter Richtervorbehalt zu stellen.

248 Nach der Rechtsprechung des Bundesverfassungsgerichts kann bei Ermittlungsmaßnahmen, die einen schwerwiegenden Grundrechtseingriff bewirken, verfassungsrechtlich eine vorbeugende Kontrolle durch eine unabhängige Instanz geboten sein. Dies gilt insbesondere, wenn der Grundrechtseingriff heimlich erfolgt und für den Betroffenen unmittelbar nicht wahrnehmbar ist (vgl. BVerfGE 120, 274 <331>). Für die Abfrage und Übermittlung von Telekommunikationsverkehrsdaten kann dies der Fall sein. Angesichts des Gewichts des hierin liegenden Eingriffs reduziert sich der Spielraum des Gesetzgebers dahingehend, dass solche Maßnahmen grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen sind. Richter können aufgrund ihrer persönlichen und sachlichen Unabhängigkeit und ihrer ausschließlichen Bindung an das Gesetz die Rechte des Betroffenen im Einzelfall am besten und sichersten wahren (vgl. BVerfGE 77, 1 <51>; 103, 142 <151>; 120, 274 <332>). Eine Ausnahme gilt nach Art. 10 Abs. 2 Satz 2 GG für die Kontrolle von Eingriffen in die Telekommunikationsfreiheit durch die Nachrichtendienste. Hier kann an die Stelle einer vorbeugenden richterlichen Kontrolle die - gleichfalls spezifisch auf die jeweilige Maßnahme bezogene - Kontrolle durch ein von der Volksvertretung bestelltes Organ oder Hilfsorgan treten (vgl. BVerfGE 30, 1 <21>).

249 Der Gesetzgeber hat das Gebot vorbeugender richterlicher Kontrolle in spezifischer und normenklarer Form mit strengen Anforderungen an den Inhalt und die Begründung der gerichtlichen Anordnung zu verbinden (vgl. BVerfGE 109, 279 <358 f.>). Hieraus folgt zugleich das Erfordernis einer hinreichend substantiierten Begründung und Begrenzung der Abfrage der begehrten Daten, die es dem Gericht erst erlaubt, eine effektive Kontrolle auszuüben (vgl. BVerfGE 103, 142 <160 f.>). Erst auf dieser Grundlage kann und muss das anordnende Gericht sich eigenverantwortlich ein Urteil darüber bilden, ob die beantragte Verwendung der Daten den gesetzlichen Voraussetzungen entspricht. Dazu gehört eine sorgfältige Prüfung der Eingriffsvoraussetzungen einschließlich insbesondere der gesetzlich vorgeschriebenen Eingriffsschwelle. Der Anordnungsbeschluss des Gerichts muss gehaltvoll begründet werden. Überdies sind die zu übermittelnden Daten nach Maßgabe des Verhältnismäßigkeitsgrundsatzes hinreichend selektiv und in klarer Weise zu bezeichnen (vgl. BVerfGE 103, 142 <151>), so dass die Diensteanbieter eine eigene Sachprüfung nicht vornehmen müssen. Diese dürfen nur auf der Grundlage klarer Anordnungen zur Datenübermittlung verpflichtet und berechtigt sein.

250 Zur Wirksamkeit der Kontrolle gehört es auch, dass die Daten aufgrund der Anordnung von den Telekommunikationsunternehmen als speicherungsverpflichteten Dritten herausgefiltert und übermittelt werden, das heißt den Behörden also nicht ein Direktzugriff auf die Daten eröffnet wird. Auf diese Weise wird die Verwendung der Daten auf das Zusammenwirken verschiedener Akteure verwiesen und damit in sich gegenseitig kontrollierende Entscheidungsstrukturen eingebunden.

251 bb) Von Verfassungs wegen geboten ist auch die Eröffnung eines Rechtsschutzverfahrens zur nachträglichen Kontrolle der Verwendung der Daten. Sofern ein Betroffener vor Durchführung der Maßnahme keine Gelegenheit hatte, sich vor den Gerichten gegen die Verwendung seiner Telekommunikationsverkehrsdaten zur Wehr zu setzen, ist ihm eine gerichtliche Kontrolle nachträglich zu eröffnen.

252 cc) Schließlich setzt eine verhältnismäßige Ausgestaltung wirksame Sanktionen bei Rechtsverletzungen voraus. Würden auch schwere Verletzungen des Telekommunikationsgeheimnisses im Ergebnis sanktionslos bleiben mit der Folge, dass der Schutz des Persönlichkeitsrechts, auch soweit er in Art. 10 Abs. 1 GG eine spezielle Ausprägung gefunden hat, angesichts der immateriellen Natur dieses Rechts verkümmern würde (vgl. BVerfG, Beschluss der 1. Kammer des Ersten Senats vom 11. November 2009 - 1 BvR 2853/08 -, juris, Rn. 21; BGHZ 128, 1 <15>), widerspräche dies der Verpflichtung der staatlichen Gewalt, dem Einzelnen die Entfaltung seiner Persönlichkeit zu ermöglichen (vgl. BVerfGE 35, 202 <220 f.>; 63, 131 <142 f.>; 96, 56 <64>) und ihn vor Persönlichkeitsrechtsgefährdungen durch Dritte zu schützen (vgl. BVerfGE 73, 118 <210>; 97, 125 <146>; 99, 185 <194 f.>; BVerfGK 6, 144 <146>). Dies kann insbesondere der Fall sein, wenn unberechtigt gewonnene Daten weitgehend ungehindert verwendet werden dürften oder eine unberechtigte Verwendung der Daten mangels materiellen Schadens regelmäßig ohne einen der Genugtuung der Betroffenen dienenden Ausgleich bliebe.

253 Der Gesetzgeber hat diesbezüglich allerdings einen weiten Gestaltungsspielraum. Dabei kann er insbesondere in den Blick nehmen, inwieweit sich entsprechende Regelungen in die allgemeine Systematik des Strafprozessrechts oder des geltenden Haftungsrechts einfügen. Insoweit darf er auch berücksichtigen, dass bei schweren Verletzungen des Persönlichkeitsrechts bereits nach geltender Rechtslage sowohl Verwertungsverbote auf der Grundlage einer Abwägung (vgl. BVerfGE 34, 238 <248 ff.>; 80, 367 <375 f.>; 113, 29 <61>; BVerfGK 9, 174 <196>; BGHSt 34, 397 <401>; 52, 110 <116>) als auch eine Haftung für immaterielle Schäden begründet sein können (vgl. BVerfGE 34, 269 <282, 285 f.>; BVerfGK 6, 144 <146 f.>; BVerfG, Beschluss der 1. Kammer des Ersten Senats vom 11. November 2009 - 1 BvR 2853/08 -, juris, Rn. 21; BGHZ 128, 1 <12>). Für die Entscheidung, ob es diesbezüglich weitergehender Regelungen bedarf, ist er deshalb nicht gehindert, zunächst zu beobachten, ob der besonderen Schwere der Persönlichkeitsverletzung, die in der unberechtigten Erlangung oder Verwendung der hier in Frage stehenden Daten regelmäßig liegt, schon auf der Grundlage des geltenden Rechts von der Rechtsprechung in der verfassungsrechtlich gebotenen Weise Rechnung getragen wird.

254 FÖR-Systematik: Cyberlaw Highlight – Weniger strenge Prüfungsmaßstäbe bei „Bestandsdatenauskunft“

4. Weniger strenge verfassungsrechtliche Maßgaben gelten für eine nur mittelbare Verwendung der vorsorglich gespeicherten Daten in Form von behördlichen Auskunftsansprüchen gegenüber den Diensteanbietern hinsichtlich der Anschlussinhaber bestimmter IP-Adressen, die diese unter Nutzung der vorgehaltenen Daten zu ermitteln haben. Die Schaffung von solchen Auskunftsansprüchen ist unabhängig von begrenzenden Rechtsgüter- oder Straftatenkatalogen insgesamt weitergehend zulässig als die Abfrage und Verwendung der Telekommunikationsverkehrsdaten selbst.

255 a) Für Auskünfte über die Inhaber bestimmter IP-Adressen, für deren Ermittlung auf vorsorglich gespeicherte Telekommunikationsverkehrsdaten zurückgegriffen werden muss, müssen nicht von Verfassungs wegen die sonst für die Verwendung solcher Daten geltenden besonders strengen Voraussetzungen gegeben sein.

256 Von Bedeutung ist hierfür zum einen, dass die Behörden selbst keine Kenntnis der vorsorglich zu speichernden Daten erhalten. Die Behörden rufen im Rahmen solcher Auskunftsansprüche nicht die vorsorglich anlasslos gespeicherten Daten selbst ab, sondern erhalten lediglich personenbezogene Auskünfte über den Inhaber eines bestimmten Anschlusses, der von den Diensteanbietern unter Rückgriff auf diese Daten ermittelt wurde. Dabei bleibt die Aussagekraft dieser Daten eng begrenzt: Die Verwendung der vorsorglich gespeicherten Daten führt allein zu der Auskunft, welcher Anschlussinhaber unter einer bereits bekannten, etwa anderweitig ermittelten IP-Adresse im Internet angemeldet war. Eine solche Auskunft hat ihrer formalen Struktur nach eine gewisse Ähnlichkeit mit der Abfrage des Inhabers einer Telefonnummer. Ihr Erkenntniswert bleibt punktuell. Systematische Ausforschungen über einen längeren Zeitraum oder die Erstellung von Persönlichkeits- und Bewegungsprofilen lassen sich allein auf Grundlage solcher Auskünfte nicht verwirklichen.

257 Maßgeblich ist zum anderen, dass für solche Auskünfte nur ein von vornherein feststehender kleiner Ausschnitt der Daten verwendet wird, deren Speicherung für sich genommen unter deutlich geringeren Voraussetzungen angeordnet werden könnte. Eine Speicherung allein der für solche Auskünfte erforderlichen Internetzugangsdaten zur Identifizierung dynamischer IP-Adressen hätte ein erheblich weniger belastendes Gewicht als die nahezu vollständige Speicherung der Daten sämtlicher Telekommunikationsverbindungen. Aus dem Zusammenwirken dieser Gesichtspunkte ergibt sich, dass die für die Verwendung von vorsorglich gespeicherten Telekommunikationsverkehrsdaten ansonsten maßgeblichen Anforderungen für solche Auskünfte nicht gleichermaßen gelten.

258 b) Allerdings hat auch die Begründung von behördlichen Auskunftsansprüchen zur Identifizierung von IP-Adressen erhebliches Gewicht. Mit ihr wirkt der Gesetzgeber auf die Kommunikationsbedingungen im Internet ein und begrenzt den Umfang ihrer Anonymität. Auf ihrer Grundlage kann in Verbindung mit der systematischen Speicherung der Internetzugangsdaten in weitem Umfang die Identität von Internetnutzern ermittelt werden. Sofern Privatpersonen, die sich im Internet geschädigt sehen, die entsprechenden IP-Adressen registrieren und Anzeige erstatten oder soweit die Behörde selbst IP-Adressen ermittelt, können diese bestimmten Anschlussinhabern zugeordnet und die dahinter stehenden Kommunikationsvorgänge mit erheblicher Wahrscheinlichkeit individualisiert werden.

259 Dabei kann die Zuordnung einer IP-Adresse zu einem Anschlussinhaber vom Gewicht für den Betroffenen her auch trotz einer gewissen Ähnlichkeit mit der Identifizierung einer Telefonnummer nicht gleichgesetzt werden. Telefonnummern werden als auf Dauer vergebene Kennungen unter den Nutzern ausgetauscht, so dass eine Abfrage von deren Inhaber auch unabhängig von konkreten Telekommunikationsakten möglich ist. Demgegenüber enthält eine Auskunft über den Anschlussinhaber einer dynamischen IP-Adresse in sich notwendig zugleich die Information, dass und von welchem Anschluss aus diese IP-Adresse zu einer bestimmten Zeit genutzt wurde. Darüber hinaus kann die Telefonnummer gegenüber Privaten ohne weitere Schwierigkeiten unterdrückt werden, während die IP-Adresse grundsätzlich nur unter Nutzung von Anonymisierungsdiensten verschleiert werden kann. Auch ist die mögliche Persönlichkeitsrelevanz einer Abfrage des Inhabers einer IP-Adresse eine andere als die des Inhabers einer Telefonnummer: Schon vom Umfang der Kontakte her, die jeweils durch das Aufrufen von Internetseiten neu hergestellt werden, ist sie aussagekräftiger als eine

Telefonnummernabfrage. Auch hat die Kenntnis einer Kontaktaufnahme mit einer Internetseite eine andere inhaltliche Bedeutung: Da der Inhalt von Internetseiten anders als das beim Telefongespräch gesprochene Wort elektronisch fixiert und länger wieder aufrufbar ist, lässt sich mit ihr vielfach verlässlich rekonstruieren, mit welchem Gegenstand sich der Kommunizierende auseinander gesetzt hat. Die Individualisierung der IP-Adresse als der „Telefonnummer des Internet“ gibt damit zugleich Auskunft über den Inhalt der Kommunikation. Die für das Telefongespräch geltende Unterscheidung von äußerlichen Verbindungsdaten und Gesprächsinhalten löst sich hier auf. Wird der Besucher einer bestimmten Internetseite mittels der Auskunft über eine IP-Adresse individualisiert, weiß man nicht nur, mit wem er Kontakt hatte, sondern kennt in der Regel auch den Inhalt des Kontakts.

260 Freilich besteht umgekehrt auch ein gesteigertes Interesse an der Möglichkeit, Kommunikationsverbindungen im Internet zum Rechtsgüterschutz oder zur Wahrung der Rechtsordnung den jeweiligen Akteuren zuordnen zu können. Angesichts der zunehmenden Bedeutung des Internet für die verschiedenartigsten Bereiche und Abläufe des alltäglichen Lebens erhöht sich auch die Gefahr seiner Nutzung für Straftaten und Rechtsverletzungen vielfältiger Art. In einem Rechtsstaat darf auch das Internet keinen rechtsfreien Raum bilden. Die Möglichkeit einer individuellen Zuordnung von Internetkontakten bei Rechtsverletzungen von einigem Gewicht bildet deshalb ein legitimes Anliegen des Gesetzgebers. Soweit für entsprechende Auskünfte seitens der Diensteanbieter unter den derzeitigen technischen Bedingungen, nach denen IP-Adressen überwiegend nur für die jeweilige Sitzung („dynamisch“) vergeben werden, Telekommunikationsverkehrsdaten ausgewertet werden müssen, wirft dieses folglich keine prinzipiellen Bedenken auf. Auch kann der Gesetzgeber zur Gewährleistung einer verlässlichen Zuordnung dieser Adressen über einen gewissen Zeitraum die Vorhaltung der entsprechenden Daten beziehungsweise einen weitgehenden Rückgriff auf insoweit vorgehaltene Daten seitens der Diensteanbieter vorsehen. Er hat hierbei einen Gestaltungsspielraum.

261 c) Dementsprechend darf der Gesetzgeber solche Auskünfte auch unabhängig von begrenzenden Rechtsgüter- oder Straftatenkatalogen für die Verfolgung von Straftaten, für die Gefahrenabwehr und die Aufgabenwahrnehmung der Nachrichtendienste auf der Grundlage der allgemeinen fachrechtlichen Eingriffsermächtigungen zulassen (vgl. Bock, in: Geppert/Piepenbrock/Schütz/Schuster, Beck’scher Kommentar zum TKG, 3. Aufl. 2006, § 113 Rn. 7; Graulich, in: Arndt/Fetzer/Scherer, TKG, 2008, § 113 Rn. 8). Hinsichtlich der Eingriffsschwellen ist allerdings sicherzustellen, dass eine Auskunft nicht ins Blaue hinein eingeholt werden, sondern nur aufgrund eines hinreichenden Anfangsverdachts oder einer konkreten Gefahr auf einzelfallbezogener Tatsachenbasis erfolgen darf. Das Erfordernis einer auf Anhaltspunkte im Tatsächlichen gestützten konkreten Gefahr gilt dabei für die Nachrichtendienste ebenso wie für alle zur Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung zuständigen Behörden. Die rechtlichen und tatsächlichen Grundlagen entsprechender Auskunftsbegehren sind aktenkundig zu machen. Ein Richtervorbehalt muss demgegenüber für solche Auskünfte nicht vorgesehen werden.

262 Das erhebliche Gewicht des Eingriffs solcher Auskünfte erlaubt es indessen nicht, diese allgemein und uneingeschränkt auch zur Verfolgung oder Verhinderung jedweder Ordnungswidrigkeiten zuzulassen. Die Aufhebung der Anonymität im Internet bedarf zumindest einer Rechtsgutbeeinträchtigung, der von der Rechtsordnung auch sonst ein hervorgehobenes Gewicht beigemessen wird. Dies schließt entsprechende Auskünfte zur Verfolgung oder Verhinderung von Ordnungswidrigkeiten nicht vollständig aus. Es muss sich insoweit aber um - auch im Einzelfall - besonders gewichtige Ordnungswidrigkeiten handeln, die der Gesetzgeber ausdrücklich benennen muss.

263 Auch gibt es keinen Grund, für die Identifizierung von IP-Adressen den Grundsatz der Transparenz (siehe oben C V 3) zurückzunehmen. Der Betroffene, der in der Regel davon ausgehen kann, das Internet anonym zu nutzen, hat prinzipiell das Recht zu erfahren, dass und warum diese Anonymität aufgehoben wurde. Dementsprechend hat der Gesetzgeber jedenfalls Benachrichtigungspflichten vorzusehen, soweit und sobald hierdurch der Zweck der Auskunft nicht vereitelt wird oder sonst überwiegende Interessen Dritter oder des Betroffenen selbst nicht entgegenstehen. Soweit von einer Benachrichtigung nach Maßgabe entsprechender gesetzlicher Regelungen ausnahmsweise abgesehen wird, ist der Grund hierfür aktenkundig zu machen. Einer richterlichen Bestätigung des Absehens von der Benachrichtigung bedarf es hier demgegenüber nicht.

264 5. Die verfassungsrechtlich gebotene Gewährleistung der Datensicherheit sowie einer den Verhältnismäßigkeitsanforderungen genügenden normenklaren Begrenzung der Datenverwendung ist ein untrennbarer Bestandteil der Anordnung der Speicherungsverpflichtung und obliegt deshalb dem die Verpflichtung auferlegenden Bundesgesetzgeber. Demgegenüber richtet sich die Verantwortung für die Schaffung der Abrufregelungen selbst sowie für die Ausgestaltung der Transparenz- und Rechtsschutzbestimmungen nach den jeweiligen Sachkompetenzen.

265 a) Soweit im Zusammenhang mit der Verpflichtung der Diensteanbieter zu einer vorsorglich anlasslosen Speicherung von Telekommunikationsverkehrsdaten Fragen der Datensicherheit zu regeln sind, obliegt dies als unmittelbarer Bestandteil der Speicherungspflicht und der hiermit rechtlich verbundenen Folgen dem Bund gemäß Art. 73 Abs. 1 Nr. 7 GG. Hierzu gehören neben den Regelungen zur Sicherheit der gespeicherten Daten auch die Regelungen zur Sicherheit der Übermittlung der Daten sowie hierbei die Gewährleistung des Schutzes der Vertrauensbeziehungen (siehe oben C V 1 und C V 2 e).

266 Dem Bund obliegt darüber hinaus auch die Sicherstellung einer den verfassungsrechtlichen Anforderungen entsprechenden, hinreichend präzisen Begrenzung der Verwendungszwecke der Daten, die mit der Speicherung verfolgt werden. Seinen Grund hat dies in dem unaufhebbaren verfassungsrechtlichen Zusammenhang von Datenspeicherung und Verwendungszweck, wie es gefestigter Rechtsprechung des Bundesverfassungsgerichts entspricht: Daten dürfen von vornherein nur zu bestimmten, bereichsspezifischen, präzise und normenklar festgelegten Zwecken gespeichert werden, so dass bereits bei der Speicherung hinreichend gewährleistet ist, dass die Daten nur für solche Zwecke verwendet werden, die das Gewicht der Datenspeicherung rechtfertigen. Eine Speicherung kann nicht als solche abstrakt gerechtfertigt werden, sondern nur insoweit, als sie hinreichend gewichtigen, konkret benannten Zwecken dient (vgl. BVerfGE 65, 1 <46>; 118, 168 <187 f.>). Demgegenüber ist es unzulässig, unabhängig von solchen Zweckbestimmungen einen Datenpool auf Vorrat zu schaffen, dessen Nutzung je nach Bedarf und politischem Ermessen der späteren Entscheidung verschiedener staatlicher Instanzen überlassen bleibt. In einem solchen Fall könnte die Verfassungsmäßigkeit der Speicherung mangels hinreichend vorhersehbarer und begrenzter Zwecke zum Zeitpunkt des in der Speicherung liegenden Eingriffs noch nicht beurteilt werden. Auch wäre ihre Tragweite für den Bürger weder vorhersehbar noch nach Maßgabe des Verhältnismäßigkeitsgrundsatzes begrenzt. Diese materielle Verknüpfung von Speicherung und Verwendungszweck der Daten als maßgebliches Bindeglied zwischen Eingriff und Rechtfertigung darf auch im Zusammenspiel von Bund und Ländern nicht aufgebrochen werden. Die Kompetenz, diese Verknüpfung zu gewährleisten, erwächst dem Bund aus Art. 73 Abs. 1 Nr. 7 GG kraft Sachzusammenhangs (siehe oben C III 2).

267 Zu den vom Bund in Anknüpfung an die Speicherung demnach zu treffenden Regelungen gehört die Festlegung der qualifizierten Voraussetzungen für eine Verwendung der Daten zum Zwecke der Strafverfolgung, der Gefahrenabwehr oder der Gefahrenprävention durch die Nachrichtendienste nach den oben entwickelten Maßgaben. Auch zählen hierzu die notwendigen Regelungen zur Aufrechterhaltung der Zweckbindung bei der weiteren Verwendung der Daten, insbesondere in Form von Kennzeichnungs- und Protokollierungspflichten.

268 b) Demgegenüber fällt dem Bund mit der Anordnung der Speicherungspflicht nicht ohne weiteres auch die Verantwortung darüber zu, ob und wieweit auf die Daten im Rahmen der von ihm festzulegenden Zwecke tatsächlich zurückgegriffen werden darf. Der Erlass von Bestimmungen, die den Datenabruf selbst regeln, ist nicht mehr grundsätzlich Sache des Bundes, sondern richtet sich nach den allgemeinen Gesetzgebungskompetenzen. Danach kann die Ermächtigung zum Abruf der Daten nicht auf Art. 73 Abs. 1 Nr. 7 GG gestützt werden, sondern ist auf der Grundlage jeweils derjenigen Kompetenznorm zu schaffen, die die Gesetzgebung für die mit der Datenverwendung verfolgten Aufgaben regelt (vgl. BVerfGE 113, 348 <368>; 114, 371 <385>). Im Bereich der Gefahrenabwehr und der Aufgaben der Nachrichtendienste liegt die Zuständigkeit damit weithin bei den Ländern. Anders als die Gewährleistung der verfassungsrechtlich gebotenen Begrenzung der Verwendungszwecke, die wegen der datenschutzrechtlichen Verklammerung von Eingriff und Rechtfertigung uno actu mit der Speicherung geregelt werden muss, kann und muss neben der Abrufermächtigung auch die Wahrung der weiteren verfassungsrechtlichen Anforderungen an die Ausgestaltung der Datenverwendung wie

insbesondere die Regelungen zur Benachrichtigung der Betroffenen und die Gewährleistung eines effektiven Rechtsschutzes nachfolgenden Gesetzgebungsakten der Länder überlassen bleiben. Die Verantwortung für die Verfassungsmäßigkeit dieser Regelungen obliegt diesen insoweit unmittelbar selbst.

VI. FÖR-Systematik: „Minimal“quadriga aus IT-Sicherheit, Zweckbindungsgrundsatz, Transparenz der Datenorganisation sowie Rechtschutzgewährleistung

269 Die angegriffenen Vorschriften genügen diesen Anforderungen nicht. Zwar widerspricht § 113a TKG nicht schon deshalb dem Grundrecht auf Schutz des Telekommunikationsgeheimnisses nach Art. 10 Abs. 1 GG, weil die Reichweite der Speicherungspflicht gemäß § 113a Abs. 1 bis 7, 11 TKG von vornherein unverhältnismäßig wäre. **Jedoch entsprechen die Regelungen zur Datensicherheit, zu den Zwecken und zur Transparenz der Datenverwendung sowie zum Rechtsschutz nicht den verfassungsrechtlichen Anforderungen.** Damit fehlt es an einer dem Verhältnismäßigkeitsgrundsatz entsprechenden Ausgestaltung der Regelung insgesamt. §§ 113a, 113b TKG und § 100g StPO, soweit dieser den Abruf der nach § 113a TKG zu speichernden Daten erlaubt, sind deshalb mit Art. 10 Abs. 1 GG nicht vereinbar.

270 1. § 113a TKG ist nicht schon wegen seiner Reichweite verfassungswidrig. Der Gesetzgeber darf die mit ihm angeordnete Speicherungspflicht, die sich gemäß Absatz 1 bis 7 anlasslos auf annähernd alle Verkehrsdaten öffentlich zugänglicher Telekommunikationsdienste erstreckt, für die Effektivierung der Strafverfolgung und Gefahrenprävention als geeignet, erforderlich und verhältnismäßig im engeren Sinne beurteilen (siehe oben C IV). Trotz ihrer Reichweite bleibt die Regelung vom Umfang der erfassten Daten her noch hinreichend begrenzt. Der Inhalt von Telefongesprächen, Telefaxen und E-Mails darf, wie § 113a Abs. 8 TKG ausdrücklich klarstellt, ebenso wenig gespeichert werden wie die Internetseiten oder Diensteanbieter, die ein Nutzer im Internet kontaktiert hat. Auch hat der Gesetzgeber gemäß § 113a Abs. 1, 11 TKG mit sechs Monaten und einer sich hieran anschließenden Löschungsfrist von einem Monat eine verfassungsrechtlich noch vertretbare Speicherungsdauer bestimmt. Ebenfalls lässt sich zum gegenwärtigen Zeitpunkt nicht feststellen, dass die Regelung im Zusammenwirken mit anderen Vorschriften darauf zielt oder hinausläuft, eine allgemein umfassende Datensammlung zur weitestmöglichen Rekonstruierbarkeit jedweder Aktivitäten der Bürger zu schaffen. Von Bedeutung sind insoweit die Geltung des das Datenschutzrecht sonst weithin durchziehenden Grundsatzes der Datensparsamkeit sowie zahlreiche Löschungspflichten, mit denen der Gesetzgeber das Entstehen vermeidbarer Datensammlungen grundsätzlich zu verhindern sucht. Maßgeblich für diese Beurteilung sind insoweit insbesondere etwa die §§ 11 ff. TMG, die die Diensteanbieter nach dem Telemediengesetz grundsätzlich zur Löschung von nicht für die Abrechnung erforderlichen Daten verpflichten (vgl. § 13 Abs. 4 Nr. 2, § 15 TMG) und so auch gegenüber privatwirtschaftlichen Anreizen verhindern, dass die Internetnutzung inhaltlich in allgemeinen kommerziellen Datensammlungen festgehalten wird und damit rekonstruierbar bleibt. § 113a TKG kann damit nicht als Ausdruck einer allgemeinen öffentlichen Datenvorsorge für Zwecke der Strafverfolgung und Gefahrenprävention verstanden werden, sondern bleibt trotz seiner Weite eine begrenzte Ausnahme, die den besonderen Herausforderungen der modernen Telekommunikation für die Strafverfolgung und Gefahrenabwehr Rechnung zu tragen versucht.

271 2. Demgegenüber fehlt es an der für eine solche Datensammlung verfassungsrechtlich gebotenen Gewährleistung eines besonders hohen Sicherheitsstandards. § 113a Abs. 10 TKG statuiert insoweit allein die unbestimmt bleibende Pflicht, durch technische und organisatorische Maßnahmen sicherzustellen, dass der Zugang zu den gespeicherten Daten ausschließlich besonders ermächtigten Personen möglich ist, und verweist ansonsten nur auf die im Bereich der Telekommunikation allgemein erforderliche Sorgfalt. Damit fehlt es an einer Vorschrift, die den besonders hohen Anforderungen an die Sicherheit der umfangreichen und aussagekräftigen Datensammlung nach § 113a TKG Rechnung trägt. Die der Sache nach in Bezug genommenen §§ 88 und 109 TKG gewährleisten einen solchen besonders hohen Sicherheitsstandard nicht, sondern erlauben, ihrem weiten Anwendungsbereich entsprechend, vielfältige Relativierungen. Das gilt insbesondere für § 109 TKG. So hat nach § 109 Abs. 1 TKG jeder Diensteanbieter angemessene technische Vorkehrungen oder sonstige Maßnahmen

zum Schutz des Fernmeldegeheimnisses und der Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe zu treffen. Zur Bestimmung der Angemessenheit wird dabei auf § 109 Abs. 2 Satz 4 TKG zurückgegriffen (vgl. Klesczewski, in: Säcker, Berliner Kommentar zum TKG, 2. Aufl. 2009, § 109 Rn. 12). Danach sind die Maßnahmen angemessen, wenn der dafür erforderliche technische und wirtschaftliche Aufwand in einem angemessenen Verhältnis zur Bedeutung der zu schützenden Rechte steht. Ausgehend von den oben entwickelten Maßstäben sind hierdurch die spezifischen Anforderungen an den Schutz der gemäß § 113a TKG gespeicherten Daten nicht hinreichend gewährleistet. Der gesetzlich vorgegebene Standard der „angemessenen technischen Vorkehrungen oder sonstigen Maßnahmen“ verlangt lediglich, den Stand der technischen Entwicklung zu „berücksichtigen“ (vgl. § 109 Abs. 2 Satz 2 TKG; Klesczewski, in: Säcker, Berliner Kommentar zum TKG, 2. Aufl. 2009, § 109 Rn. 13), und relativiert die Sicherheitsanforderungen in unbestimmt bleibender Weise um allgemeine Wirtschaftlichkeitserwägungen im Einzelfall. Überdies bleibt die nähere Konkretisierung dieses Standards den einzelnen Telekommunikationsdienstleistern überlassen, die ihrerseits ihre Dienste unter den Bedingungen von Konkurrenz und Kostendruck anbieten müssen.

272 Eine Konkretisierung dieser Anforderungen wird auch nicht in Form von Rechtsverordnungen oder durch Verfügungen der Aufsichtsbehörden sichergestellt. Insbesondere gewährleistet § 110 TKG die Geltung hinreichender Sicherheitsstandards nicht. Zwar können im Rahmen der nach dieser Norm zu schaffenden untergesetzlichen Regelwerke (vgl. § 110 Abs. 2 und 3 TKG) Aspekte der Datensicherheit miterfasst werden. Jedoch enthält diese - primär durch technische Zielsetzungen bestimmte - Norm diesbezüglich weder inhaltliche Standards noch greift sie den Aspekt der Datensicherheit sonst auf. Im Übrigen ist auch zwei Jahre nach Inkrafttreten der Speicherungspflicht des § 113a TKG eine der Neuregelung Rechnung tragende Anpassung der Telekommunikationsüberwachungsverordnung nicht erfolgt. Entsprechend wird auch die - im Dezember 2009 gemäß § 110 Abs. 3 Satz 3 TKG auf der Internetseite der Bundesnetzagentur veröffentlichte (vgl. Bundesnetzagentur, Amtsblatt 2009, S. 4706) - technische Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation und zum Auskunftsersuchen für Verkehrsdaten (TR-TKÜV) gemäß § 110 Abs. 3 TKG erst ein Jahr nach dieser Anpassung wirksam werden (Inhaltsangabe 1 <Regelungsbereich> TR-TKÜV; Teil B 1 <Grundsätzliches> TR-TKÜV).

273 Eine hinreichende Datensicherheit gewährleistet auch nicht § 109 Abs. 3 TKG. Zwar schreibt die Norm vor, dass Betreiber von Telekommunikationsanlagen Sicherheitsbeauftragte zu benennen und ein Sicherheitskonzept zu erstellen haben, das der Bundesnetzagentur vorzulegen ist. Auch ist danach das Konzept, wenn sich die ihm zugrunde liegenden „Gegebenheiten“ ändern, anzupassen und erneut vorzulegen. Jedoch ist damit ein besonders hoher Sicherheitsstandard nicht verlässlich gewährleistet. So erfasst die Vorschrift allein Anlagenbetreiber, nicht jedoch den gesamten Adressatenkreis des § 113a TKG, der auch andere Diensteanbieter einbezieht. Darüber hinaus verweist § 109 Abs. 3 TKG materiell nur auf die unzureichenden Anforderungen des § 109 Abs. 1 und 2 TKG. Auch ist nicht in hinreichend normenklarer Form eine kontinuierliche und kontrollierbare Anpassung der Sicherheitsstandards an den Stand der technischen Entwicklung gewährleistet. Nicht eindeutig ist insoweit, ob § 109 Abs. 3 Satz 4 TKG auch eine Anpassung an die technische Entwicklung von Schutzvorkehrungen und an sich fortentwickelnde rechtliche Sicherheitsstandards fordert. Jedenfalls fehlt es an der Verpflichtung zu einer periodisierten Fortschreibung des Sicherheitskonzepts, die diesbezüglich eine effektive Kontrolle ermöglichen könnte.

274 Das Fehlen hinreichender Sicherheitsstandards im Telekommunikationsgesetz kann auch § 9 BDSG in Verbindung mit der zugehörigen Anlage nicht ausgleichen. Unbeschadet ihrer zum Teil abstrakt hohen Standards bleibt diese Norm, die ohnehin nur subsidiär anwendbar ist (vgl. Fetzer, in: Arndt/Fetzer/Scherer, TKG, 2008, vor § 91 Rn. 10; Klesczewski, in: Säcker, Berliner Kommentar zum TKG, 2. Aufl. 2009, § 91 Rn. 15), zu allgemein, um in hinreichend spezifischer und verlässlicher Weise die besonders hohen Sicherheitsstandards bezüglich der nach § 113a TKG zu speichernden Daten sicherzustellen.

275 Insgesamt ist damit ein besonders hoher Sicherheitsstandard für die nach § 113a TKG zu speichernden Daten nicht in verbindlicher und normenklarer Form gewährleistet. Weder sind den Speicherungspflichtigen die von den sachkundigen Auskunftspersonen in vorliegendem Verfahren als Kernelemente genannten Instrumente (getrennte Speicherung, asymmetrische Verschlüsselung, Vier-

Augen-Prinzip verbunden mit fortschrittlichen Verfahren zur Authentifizierung für den Zugang zu den Schlüsseln, revisionssichere Protokollierung von Zugriff und Löschung) durchsetzbar vorgegeben, noch sind ihnen anderweitige Vorkehrungen auferlegt, die ein vergleichbares Sicherheitsniveau garantieren. Auch fehlt es an einem ausgeglichenen Sanktionensystem, das Verstößen gegen die Datensicherheit kein geringeres Gewicht beimisst als Verstößen gegen die Speicherungspflichten selbst. Der Bußgeldrahmen für die Nichtbeachtung der Speicherungspflichten ist deutlich weiter als derjenige für die Verletzung der Datensicherheit (vgl. § 149 Abs. 2 Satz 1 i.V.m. § 149 Abs. 1 Nr. 36 und 38 TKG). Den verfassungsrechtlichen Anforderungen an die Sicherheit einer Datensammlung, wie sie durch § 113a TKG geschaffen wird, genügt die geltende Rechtslage damit nicht.

276 3. Die Bestimmungen zur Übermittlung und Nutzung der Daten gemäß § 113b Satz 1 Halbsatz 1 TKG genügen den verfassungsrechtlichen Anforderungen nicht.

277 a) Mit den aus dem Verhältnismäßigkeitsgrundsatz entwickelten Maßstäben unvereinbar sind zunächst die Regelungen zur Verwendung der Daten für die Strafverfolgung.

278 aa) § 113b Satz 1 Nr. 1 TKG in Verbindung mit § 100g StPO genügt nicht den besonders engen Voraussetzungen, unter denen allein auf die nach § 113a TKG gespeicherten Daten zurückgegriffen werden darf. Zwar hat der Gesetzgeber mit diesen Vorschriften eine in ihrem Zusammenwirken differenzierte und nach Art. 74 Abs. 1 Nr. 1 und Art. 72 Abs. 1 GG abschließende Zweckbestimmung der Datenverwendung für die Strafverfolgung getroffen. Der Gesetzgeber lässt dabei für die Verwendung der Daten jedoch ähnliche Anforderungen genügen wie sie bisher für die Erhebung von Telekommunikationsverkehrsdaten galten, die die Diensteanbieter nach Maßgabe ihrer betrieblichen und vertraglichen Erfordernisse in begrenzterem Umfang und für den Einzelnen durch Vertragsgestaltung teilweise vermeidbar gemäß § 96 TKG speichern dürfen. Dies trägt dem besonders schweren Eingriff, der in der vorsorglich anlasslosen und systematischen Datenspeicherung des §113a TKG liegt, nicht hinreichend Rechnung.

279 Schon § 100g Abs. 1 Satz 1 Nr. 1 StPO stellt nicht sicher, dass allgemein und auch im Einzelfall nur schwerwiegende Straftaten Anlass für eine Erhebung der entsprechenden Daten sein dürfen, sondern lässt - unabhängig von einem abschließenden Katalog - generell Straftaten von erheblicher Bedeutung genügen. Erst recht bleibt § 100g Abs. 1 Satz 1 Nr. 2, Satz 2 StPO hinter den verfassungsrechtlichen Maßgaben zurück, indem er unabhängig von deren Schwere jede mittels Telekommunikation begangene Straftat nach Maßgabe einer allgemeinen Abwägung im Rahmen einer Verhältnismäßigkeitsprüfung als möglichen Auslöser einer Datenabfrage ausreichen lässt. Mit dieser Regelung werden die nach § 113a TKG gespeicherten Daten praktisch in Bezug auf alle Straftatbestände nutzbar. Ihre Verwendung verliert damit angesichts der fortschreitenden Bedeutung der Telekommunikation im Lebensalltag ihren Ausnahmecharakter. Der Gesetzgeber beschränkt sich hier nicht mehr auf die Verwendung der Daten für die Verfolgung schwerer Straftaten, sondern geht hierüber - und damit auch über die europarechtlich vorgegebene Zielsetzung der Datenspeicherung, die sich auch ihrerseits allein auf die Verfolgung von schweren Straftaten ohne Einschluss der Gefahrenprävention beschränkt - weit hinaus. Zwar kann eine Verwendung dieser Daten gerade für die Verfolgung von mittels Telekommunikation begangenen Straftaten sehr nützlich sein, so dass ihre Einschränkung die Aufklärung in manchen Fällen erschweren oder auch verhindern kann. Es liegt indes in der Natur der Garantie des Art. 10 Abs. 1 GG und der hiermit verbundenen Verhältnismäßigkeitsanforderungen, dass nicht jede Maßnahme, die für die Strafverfolgung nützlich und im Einzelfall auch erforderlich sein kann, verfassungsrechtlich zulässig ist. Umgekehrt wird in der Konsequenz der hier maßgeblichen Anforderungen die Telekommunikation auch im Bereich weniger bedeutender Straftaten nicht insgesamt zum rechtsfreien Raum: Auskünfte nach § 113 Abs. 1 TKG kann der Gesetzgeber - auch unter mittelbarer Nutzung der nach § 113a TKG gespeicherten Daten - für die Aufklärung aller Straftaten vorsehen (siehe oben C V 4 c). Ebenso bleibt hierdurch ein Rückgriff gemäß § 100g StPO auf anderweitig als nach § 113a TKG gespeicherte Telekommunikationsverkehrsdaten möglich.

280 bb) Nicht den verfassungsrechtlichen Anforderungen entspricht § 100g StPO weiterhin insoweit, als er einen Datenabruf grundsätzlich auch ohne Wissen des Betroffenen zulässt (§ 100g Abs. 1 Satz 1 StPO). Die verfassungsrechtlichen Anforderungen an die Transparenz der Datenverwendung erlauben

eine geheime Erhebung der nach § 113a TKG gespeicherten Daten nur, wenn dies aus überwiegenden, gesetzlich näher zu konkretisierenden Gründen erforderlich und richterlich angeordnet ist.

281 cc) Auch die Ausgestaltung der Benachrichtigungspflicht genügt nicht in jeder Hinsicht den oben entwickelten Maßgaben. Allerdings ist der Umfang der vorgesehenen Benachrichtigungspflichten als solcher keinen verfassungsrechtlichen Bedenken ausgesetzt. § 101 Abs. 1, 4 und 5 StPO sieht in Übereinstimmung mit der Rechtsprechung des Bundesverfassungsgerichts (vgl. BVerfGE 109, 279 <363 ff.>) differenzierte Regelungen vor, die den Grundsatz einer nachträglichen Benachrichtigung des Betroffenen verfassungsrechtlich tragfähig in Ausgleich bringen mit im Einzelfall ausnahmsweise entgegenstehenden überwiegenden Belangen. Nicht zu beanstanden ist insoweit insbesondere auch, dass Betroffene, auf die sich die Datenabfrage nicht bezogen hat, gemäß § 101 Abs. 4 Satz 4 StPO nicht in jedem Fall, sondern nur nach Maßgabe einer Abwägung zu benachrichtigen sind. Im Rahmen dieser Abwägung kann und muss den Interessen von mittelbar Betroffenen hinreichend Rechnung getragen werden.

282 Unzureichend sind demgegenüber die Regeln zur richterlichen Kontrolle für Fälle, in denen eine Benachrichtigung unterbleiben kann. § 101 Abs. 6 StPO sieht eine gerichtliche Kontrolle nur für die Zurückstellung der Benachrichtigung gemäß § 101 Abs. 5 StPO vor, nicht jedoch für das Absehen von einer Benachrichtigung gemäß § 101 Abs. 4 StPO. Dies trägt dem hohen Stellenwert der Benachrichtigung für eine transparente Verwendung der nach § 113a TKG gespeicherten Daten nicht hinreichend Rechnung. Soweit sich eine Datenabfrage unmittelbar auf Verkehrsdaten einer bestimmten Person bezieht, darf auf deren nachträgliche Benachrichtigung nur nach einer gerichtlichen Kontrolle der entsprechenden Ausnahmegründe verzichtet werden. An einer solchen Kontrolle fehlt es in den Fällen, in denen von einer Benachrichtigung gemäß § 101 Abs. 4 Satz 3 StPO wegen überwiegender Belange einer betroffenen Person abgesehen werden soll.

283 dd) Demgegenüber ist die gerichtliche Kontrolle der Datenabfrage und Datennutzung selbst in einer den verfassungsrechtlichen Anforderungen entsprechenden Weise gewährleistet. Die Erhebung der nach § 113a TKG gespeicherten Daten bedarf gemäß § 100g Abs. 2 Satz 1, § 100b Abs. 1 Satz 1 StPO der Anordnung durch den Richter. Die richterliche Anordnung ermächtigt die Behörden auch nicht zu einem Direktzugriff auf die Daten, sondern verpflichtet die Diensteanbieter, diese in einem eigenen Zwischenschritt nach den Maßgaben der Anordnung herauszufiltern und zu übermitteln. Des Weiteren besteht gemäß § 101 Abs. 1, Abs. 7 Satz 2 bis 4 StPO die Möglichkeit, nachträglich eine gerichtliche Überprüfung der Rechtmäßigkeit der Maßnahme herbeizuführen. Dass diese Vorschriften einen effektiven Rechtsschutz insgesamt nicht gewährleisten, ist nicht ersichtlich.

284 Nicht hinreichend normenklar geregelt sind allerdings die gesetzlichen Bestimmungen zu den formalen Anforderungen an die richterliche Anordnung. § 100g Abs. 2 in Verbindung mit § 100b Abs. 2 StPO regelt lediglich Mindestanforderungen an die Entscheidungsformel; im Übrigen gilt die allgemeine Begründungspflicht für Entscheidungen gemäß § 34 StPO. Der Gesetzgeber sollte bei einer Neuregelung erwägen, ob es sachdienlich wäre, den strengen Anforderungen an eine substantiierte Begründung richterlicher Anordnungen (vgl. BVerfGE 103, 142 <151>; 107, 299 <325>; 109, 279 <358 f.>) durch eine spezielle und differenzierte Vorschrift Nachdruck zu verleihen. Jedenfalls ist gesetzlich sicherzustellen, dass der Umfang der zu übermittelnden Daten in der Anordnung in einer dem Verhältnismäßigkeitsgrundsatz entsprechenden Weise hinreichend selektiv und für die Diensteanbieter eindeutig beschrieben wird.

285 b) Die angegriffenen Vorschriften entsprechen den verfassungsrechtlichen Anforderungen auch nicht im Hinblick auf den Abruf und die Verwendung der nach § 113a TKG gespeicherten Daten für die Gefahrenabwehr und für die Aufgaben der Nachrichtendienste. § 113b Satz 1 Nr. 2 und 3 TKG genügt den Anforderungen an eine hinreichende Begrenzung der Verwendungszwecke schon seiner Anlage nach nicht. Der Bundesgesetzgeber begnügt sich hier damit, in lediglich generalisierender Weise die Aufgabenfelder zu umreißen, für die ein Datenabruf möglich sein soll, ohne konkret die Verwendungszwecke zu benennen. Deren Konkretisierung überlässt er vielmehr späterer Gesetzgebung, insbesondere auch der Gesetzgebung durch die Länder. Damit kommt er seiner Verantwortung für die verfassungsrechtlich gebotene Begrenzung der Verwendungszwecke nicht nach. Wenn er die Speicherung der Telekommunikationsverkehrsdaten anordnet, obliegt es ihm zugleich, auch die für

deren verfassungsrechtliche Rechtfertigung erforderlichen Verwendungszwecke und Eingriffsschwellen sowie die zur Gewährleistung der Zweckbindung erforderlichen Folgeregelungen verbindlich festzulegen. Solche Festlegungen enthält § 113b Halbsatz 1 TKG nicht. Vielmehr wird durch die Pflicht der Diensteanbieter zur vorsorglichen Speicherung aller Telekommunikationsverkehrsdaten und gleichzeitig die Freigabe dieser Daten für die Verwendung durch die Polizei und die Nachrichtendienste im Rahmen annähernd deren gesamter Aufgabenstellung ein für vielfältige und unbegrenzte Verwendungen offener Datenpool geschaffen, auf den - nur durch grobe Zielsetzungen beschränkt - jeweils aufgrund eigener Entscheidungen der Gesetzgeber in Bund und Ländern zugegriffen werden kann. Die Bereitstellung eines solchen seiner Zwecksetzung nach offenen Datenpools hebt den notwendigen Zusammenhang zwischen Speicherung und Speicherungszweck auf und ist mit der Verfassung nicht vereinbar (siehe oben C V 5 a).

286 Nicht zu beanstanden ist demgegenüber, dass in § 113b TKG keine übergreifenden Regelungen zu Benachrichtigungspflichten oder zur gerichtlichen Kontrolle für den Fall der Verwendung der nach § 113a TKG gespeicherten Daten zu Zwecken der Gefahrenabwehr und der Aufgabenwahrnehmung durch die Nachrichtendienste enthalten sind. Zwar sind solche Regelungen verfassungsrechtlich unverzichtbar. Der Bundesgesetzgeber durfte diese mit dem Abruf der Daten im Zusammenhang stehenden Regelungen aber der jeweiligen Ausgestaltung durch die Fachgesetze und damit gegebenenfalls auch durch Landesgesetze überlassen.

287 c) Die Ausgestaltung der Verwendung der nach § 113a TKG gespeicherten Daten ist auch insoweit unverhältnismäßig, als für die Übermittlung keinerlei Schutz von Vertrauensbeziehungen vorgesehen ist. Zumindest für einen engen Kreis von auf besondere Vertraulichkeit angewiesenen Telekommunikationsverbindungen ist ein solcher Schutz grundsätzlich geboten (siehe oben C V 2 e am Ende).

288 4. Schließlich genügt auch § 113b Satz 1 Halbsatz 2 TKG, der eine mittelbare Nutzung der nach § 113a TKG gespeicherten Daten für Auskünfte der Diensteanbieter gemäß § 113 Abs. 1 TKG vorsieht, nicht in jeder Hinsicht den Anforderungen der Verhältnismäßigkeit.

289 Nach den oben entwickelten Maßstäben unterliegt es allerdings keinen verfassungsrechtlichen Bedenken, dass der Gesetzgeber in § 113b Satz 1 Halbsatz 2 TKG Auskünfte über die Anschlussinhaber bestimmter, den Behörden bereits bekannter IP-Adressen nicht unter die besonders strengen Voraussetzungen stellt, die für einen unmittelbaren Abruf der nach § 113a TKG gespeicherten Daten beachtet werden müssen. Es ist insoweit nicht zu beanstanden, dass gemäß § 113b Satz 1 Halbsatz 2 TKG in Verbindung mit § 113 Abs. 1 TKG solche Auskünfte ohne vorherige richterliche Anordnung für die Verfolgung von Straftaten aller Art und allgemein für die Aufgaben der Gefahrenabwehr und der Nachrichtendienste zulässig sind. Nicht ganz eindeutig ist die Regelung jedoch hinsichtlich der erforderlichen Eingriffsschwellen. Bei verfassungskonformer Auslegung lässt sie sich jedoch dahingehend verstehen, dass § 113 Abs. 1 TKG auf die jeweiligen fachgesetzlichen Eingriffsgrundlagen verweist und für den Zugriff auf die Daten zumindest einen hinreichenden Anfangsverdacht gemäß §§ 161, 163 StPO oder eine konkrete Gefahr im Sinne der polizeilichen Generalklauseln voraussetzt (vgl. Bock, in: Geppert/Piepenbrock/Schütz/Schuster, Beck'scher Kommentar zum TKG, 3. Aufl. 2006, § 113 Rn. 7; Graulich, in: Arndt/Fetzer/Scherer, TKG, 2008, § 113 Rn. 8). Die Eingriffsschwelle der konkreten Gefahr muss der Vorschrift in verfassungskonformer Auslegung auch für Auskunftsverlangen der Nachrichtendienste entnommen werden.

290 Gleichfalls im Wege der verfassungskonformen Auslegung kann einem etwaigen Missbrauch der Vorschrift zur Umgehung des § 100g StPO begegnet werden. § 113b Satz 1 Halbsatz 2 in Verbindung mit § 113 Abs. 1 TKG ermächtigt bei verfassungsgemäßem Verständnis nicht zu offenen Abfragen der Behörden zu Anschlussinhabern, deren Telekommunikationsverbindungen diesen nicht bekannt sind. Vielmehr erlaubt er entsprechend seiner in der Gesetzesbegründung zum Ausdruck gekommenen Zielrichtung nur Auskünfte zu einzelnen, den Behörden bereits vorher bekannten IP-Adressen (vgl. BTDrucks 16/6979, S. 46). Der Gesetzgeber mag im Rahmen der notwendigen Neuregelung prüfen, ob er Anlass sieht, dies gesetzlich klarzustellen. Eine Verfassungswidrigkeit des § 113b Satz 1 Halbsatz 2 in Verbindung mit § 113 Abs. 1 TKG ist insoweit jedoch nicht festzustellen.

291 Unter Verhältnismäßigkeitsgesichtspunkten zu weitgehend ist § 113b Satz 1 Halbsatz 2 in Verbindung mit § 113 Abs. 1 TKG jedoch insoweit, als er allgemein auch die Ahndung von

Ordnungswidrigkeiten für solche Abfragen ausreichen lässt. Zwar ist dem Gesetzgeber nach den oben entwickelten Maßgaben nicht grundsätzlich verwehrt, solche Auskünfte in besonders wichtigen Fällen auch im Bereich des Ordnungswidrigkeitenrechts einzusetzen (siehe oben C V 4 c). Es bedarf hierfür jedoch normenklarer spezieller Regelungen, an denen es vorliegend fehlt. Verfassungswidrig ist § 113b Satz 1 Halbsatz 2 in Verbindung mit § 113 Abs. 1 TKG darüber hinaus auch insoweit, als es an Regelungen zu einer Benachrichtigung der Betroffenen fehlt. Gemäß § 113 Abs. 1 Satz 4 TKG haben die Auskunftsverpflichteten gegenüber den Betroffenen Stillschweigen zu wahren, und auch seitens der auskunftsersuchenden Behörden ist keinerlei Benachrichtigung gewährleistet. Dies genügt den verfassungsrechtlichen Anforderungen an eine transparente Verwendung der nach § 113a TKG gespeicherten Daten nicht (siehe oben C V 3 a).

292 5. Zusammenfassend genügen weder die gesetzlichen Vorgaben für die Datensicherheit noch die Vorschriften zur Verwendung der Daten gemäß § 113b Satz 1 Nr. 1 TKG in Verbindung mit § 100g StPO, § 113b Satz 1 Nr. 2 und 3 TKG und § 113b Satz 1 Halbsatz 2 TKG den verfassungsrechtlichen Anforderungen. Damit fehlt es zugleich auch der Speicherungspflicht gemäß § 113a TKG selbst an einer verfassungsrechtlich tragfähigen Rechtfertigung. Die angegriffenen Vorschriften sind folglich insgesamt mit Art. 10 Abs. 1 GG nicht vereinbar.

VII. FÖR-Systematik: Kostenüberantwortung

293 Demgegenüber sind die angegriffenen Vorschriften hinsichtlich Art. 12 Abs. 1 GG, soweit in diesem Verfahren hierüber zu entscheiden ist, keinen verfassungsrechtlichen Bedenken ausgesetzt. Die Beschwerdeführerin zu 4) im Verfahren 1 BvR 256/08 wird durch die angegriffenen Vorschriften und die hiermit verbundene finanzielle Belastung nicht in ihrer Berufsfreiheit verletzt.

294 1. Die Auferlegung von Speicherungspflichten, die die Beschwerdeführerin zumindest insoweit betreffen, als sie auch selbst einen öffentlich zugänglichen Anonymisierungsserver betreibt, stellt allerdings einen Eingriff in ihre Berufsfreiheit dar. Als kommerzielle Anbieterin eines Anonymisierungsdienstes kann sie sich auf die Berufsfreiheit gemäß Art. 12 Abs. 1 GG berufen. Auch hat die Regelung objektiv berufsregelnde Tendenz. Die Speicherungspflichten richten sich an solche Diensteanbieter, die öffentlich zugänglich Telekommunikationsdienste in der Regel gegen Entgelt für Endnutzer erbringen (vgl. § 113a Abs. 1, § 3 Nr. 24 TKG) und damit an Dienstleister, die die Dienste jedenfalls typischerweise zu Erwerbszwecken anbieten.

295 Bei dem Eingriff handelt es sich um eine Berufsausübungsregelung. Geregelt wird in § 113a TKG eine Speicherungs- und in § 113b Satz 1 Halbsatz 1 TKG eine Übermittlungspflicht, die sich als technische Maßgaben für die Erbringung von Telekommunikationsdiensten darstellen. Fehl geht dagegen das Vorbringen, die Speicherungspflicht wirke gegenüber Anonymisierungsdiensten als Berufswahlregelung, weil eine endgültige Anonymisierung nicht mehr angeboten werden könne. Zwar kommt eine Berufswahlregelung nicht nur dann in Betracht, wenn der Zugang zu einem Beruf rechtlich beschränkt wird, sondern auch dann, wenn die sinnvolle Ausübung eines Berufs faktisch unmöglich gemacht wird (vgl. BVerfGE 30, 292 <313>). Jedoch führt die Speicherungspflicht nach § 113a Abs. 6 TKG nicht dazu, dass Anonymisierungsdienste grundsätzlich nicht mehr betrieben werden können. Die Anonymisierungsdienste können ihren Nutzern weiterhin anbieten, ohne Identifizierungsmöglichkeit der IP-Adresse durch Private im Internet zu surfen. Sie ermöglichen damit Nutzern, die eine statische (und folglich offene) IP-Adresse haben, ihre Identität zu verbergen und schützen andere Nutzer vor Hackern oder sonstigem illegalen Zugriff. Aufgehoben wird die Anonymität nur gegenüber den staatlichen Behörden und dabei auch nur dann, wenn nach den engen Voraussetzungen für die unmittelbare Verwendung der nach § 113a TKG gespeicherten Verkehrsdaten ein Datenabruf ausnahmsweise erlaubt ist. Abgehalten werden damit folglich allein Kunden, deren Anonymisierungsinteresse sich gegen die in solchen besonders schwerwiegenden Fällen ermittelnden Behörden richtet. Das Angebot eines Anonymisierungsdienstes wird dadurch nicht insgesamt hinfällig.

296 2. Der durch die Auferlegung der Speicherungspflichten begründete Eingriff ist verfassungsrechtlich gerechtfertigt. Er ist weder hinsichtlich des technischen Aufwands noch hinsichtlich der damit verbundenen finanziellen Belastungen unverhältnismäßig.

297 Eingriffe in die Berufsausübungsfreiheit müssen durch ausreichende Gründe des Gemeinwohls gerechtfertigt sein (vgl. BVerfGE 94, 372 <390>; 101, 331 <347>; 121, 317 <346>). Dabei reichen grundsätzlich vernünftige Gründe des Allgemeinwohls aus (vgl. BVerfGE 7, 377 <405 f.>; 16, 286 <297>; 81, 156 <189>; stRspr). Auch hier gelten die Anforderungen des Verhältnismäßigkeitsgrundsatzes, das heißt der Eingriff muss zur Erreichung des Eingriffsziels geeignet, erforderlich und verhältnismäßig im engeren Sinne sein. Diese Voraussetzungen sind hier erfüllt.

298 a) Die Speicherungs- und Übermittlungspflichten legitimieren sich auch hinsichtlich des Eingriffs in die Berufsfreiheit aus der Zielsetzung einer Effektivierung der Strafverfolgung, der Gefahrenabwehr und der Aufgaben der Geheimdienste. Sie stützen sich damit auf vernünftige Gründe des Allgemeinwohls, für deren Förderung sie geeignet sind. Eine weniger eingreifende Regelung, die ebenso effektiv und für die öffentliche Hand kostengünstig ist, ist nicht ersichtlich. Da die Telekommunikationsverkehrsdaten seit der Privatisierung des Telekommunikationssektors nicht mehr beim Staat anfallen, ist dieser seinerseits zu einer direkten Speicherung nicht in der Lage. Eine Übermittlung aller Verbindungsdaten an den Staat, damit dieser die Speicherung selbst vornimmt, scheidet schon wegen der damit verbundenen Risiken sowohl für den Schutz des Telekommunikationsgeheimnisses als auch für die Sicherheit und Vollständigkeit der Daten aus. Auch entfällt die Erforderlichkeit bei Beeinträchtigungen der Berufstätigkeit durch die Auferlegung von Kostenlasten beziehungsweise kostenträchtigen Pflichten nicht schon deshalb, weil eine Finanzierung der betreffenden Aufgabe aus Steuermitteln für die Betroffenen ein milderes Mittel wäre (vgl. BVerfGE 81, 156 <193 f.>; 109, 64 <86>). Mildere Mittel sind nicht solche, die eine Kostenlast lediglich verschieben (vgl. BVerfGE 103, 172 <183 f.>; 109, 64 <86>).

299 b) Die Auferlegung der Speicherungspflicht wirkt gegenüber den betroffenen Diensteanbietern typischerweise nicht übermäßig belastend.

300 aa) Die Speicherungspflicht überschreitet die Grenze der Zulässigkeit nicht durch den technischen Aufwand, den sie den Diensteanbietern abverlangt. Da sich die betreffenden Diensteanbieter auf dem Telekommunikationsmarkt bewegen, müssen sie ohnehin ein hohes Maß an Technikbeherrschung im Bereich der Telekommunikationsdatenerfassung, -speicherung und -verarbeitung aufweisen. Über diese Fähigkeiten müssen auch kleine Unternehmen in diesem Sektor verfügen. Überdies wird jedenfalls ein Großteil der nach § 113a TKG zu speichernden Daten ohnehin von den betreffenden Telekommunikationsunternehmen vorübergehend für eigene Zwecke gespeichert. Anspruchsvolle organisatorische Anforderungen zur Gewährleistung von Datensicherheit entstehen nicht erst aus der Speicherungspflicht des § 113a TKG, sondern unabhängig davon schon aus dem Gegenstand der von den betreffenden Unternehmen angebotenen Dienste. Insoweit ist die Auferlegung der spezifischen Pflichten gemäß § 113a TKG in technisch-organisatorischer Hinsicht nicht unverhältnismäßig.

301 bb) Unverhältnismäßig ist die Speicherungspflicht auch nicht in Bezug auf die finanziellen Lasten, die den Unternehmen durch die Speicherungspflicht nach § 113a TKG und die hieran knüpfenden Folgeverpflichtungen wie die Gewährleistung von Datensicherheit erwachsen. Unzumutbar ist dieses insbesondere nicht deshalb, weil dadurch private Unternehmen unzulässig mit Staatsaufgaben betraut würden. Eine kategorische Trennung von „Staatsaufgaben“ und „privaten Aufgaben“ mit der Folge der grundsätzlichen Unzulässigkeit einer Indienstnahme für Gemeinwohlzwecke von Privaten auf deren Kosten lässt sich der Verfassung nicht entnehmen. Vielmehr hat der Gesetzgeber einen weiten Gestaltungsspielraum, welche Pflichten zur Sicherstellung von Gemeinwohlbelangen er Privaten im Rahmen ihrer Berufstätigkeit auferlegt (vgl. BVerfGE 109, 64 <85>). Grundsätzlich kann er Lasten und Maßnahmen zur Wahrung von Gemeinwohlbelangen, die als Folge kommerzieller Aktivitäten regelungsbedürftig sind, den entsprechenden Marktakteuren auferlegen, um die damit verbundenen Kosten auf diese Weise in den Markt und den Marktpreis zu integrieren. Dabei ist der Gesetzgeber nicht darauf beschränkt, Private nur dann in Dienst zu nehmen, wenn ihre berufliche Tätigkeit unmittelbar Gefahren auslösen kann oder sie hinsichtlich dieser Gefahren unmittelbar ein Verschulden trifft. Vielmehr reicht insoweit eine hinreichende Sach- und Verantwortungsnähe zwischen der beruflichen Tätigkeit und der auferlegten Verpflichtung (vgl. BVerfGE 95, 173 <187>).

302 Danach bestehen gegen die den Speicherungspflichtigen erwachsenden Kostenlasten keine grundsätzlichen Bedenken. Der Gesetzgeber verlagert auf diese Weise die mit der Speicherung verbundenen Kosten entsprechend der Privatisierung des Telekommunikationssektors insgesamt in den

Markt. So wie die Telekommunikationsunternehmen die neuen Chancen der Telekommunikationstechnik zur Gewinnerzielung nutzen können, müssen sie auch die Kosten für die Einhegung der neuen Sicherheitsrisiken, die mit der Telekommunikation verbunden sind, übernehmen und in ihren Preisen verarbeiten. Die den Unternehmen auferlegten Pflichten stehen in engem Zusammenhang mit den von ihnen erbrachten Dienstleistungen und können als solche nur von ihnen selbst erbracht werden. Auch werden hierbei nicht einzelnen Diensteanbietern einzelfallbezogen Sonderopfer auferlegt, sondern in allgemeiner Form die Rahmenbedingungen für die Erbringung von Telekommunikationsdiensten ausgestaltet. Es ist damit verfassungsrechtlich nicht zu beanstanden, wenn die Unternehmen hierfür dann auch die anfallenden Kosten grundsätzlich zu tragen haben. Allein die gemeinwohlbezogene Zielsetzung gebietet es nicht, hierfür einen Kostenersatz vorzusehen (vgl. BVerfGE 30, 292 <311>). Ein Gesetz, das die Berufsausübung in der Weise regelt, dass es Privaten bei der Ausübung ihres Berufs Pflichten auferlegt und dabei regelmäßig eine Vielzahl von Personen betrifft, ist nicht bereits dann unverhältnismäßig, wenn es einzelne Betroffene unzumutbar belastet, sondern erst dann, wenn es bei einer größeren Betroffenengruppe das Übermaßverbot verletzt (vgl. BVerfGE 30, 292 <316>). Dass die Kostenlasten in dieser Weise erdrosselnde Wirkungen haben, ist weder substantiiert vorgebracht noch erkennbar.

303 Insofern ist nicht weiter zu prüfen, ob hinsichtlich besonderer Fallgruppen (vgl. BVerfGE 30, 292 <327>) oder Sondersituationen aus dem Gesichtspunkt der Verhältnismäßigkeit Härteregelungen geboten sind. Denn jedenfalls ergibt sich hierfür aus dem Vorbringen der Beschwerdeführerin zu 4) im Verfahren 1 BvR 256/08 nichts. Insbesondere hat sie auch in Bezug auf Anonymisierungsdienste eine über die bei den sonstigen Telekommunikationsunternehmen hinausgehende Belastung weder für sich noch für andere Anbieter solcher Dienste hinreichend nachvollziehbar durch konkrete Zahlen belegt. Nur unter dieser Voraussetzung ließe sich aber eine Überschreitung des gesetzgeberischen Gestaltungsspielraums bei der Indienstnahme der Anonymisierungsdienste feststellen. Solange die Einschätzung des Gesetzgebers nur durch Vermutungen und Behauptungen in Frage gestellt wird, kann das Bundesverfassungsgericht dieser Frage nicht nachgehen (vgl. BVerfGE 114, 196 <248>).

304 Keinen grundsätzlichen Bedenken hinsichtlich möglicher verbleibender Kostenlasten unterliegt auch die Übermittlungspflicht gemäß § 113b Satz 1 Nr. 1 TKG in Verbindung mit § 100g StPO, für die der Gesetzgeber eine Entschädigungsregelung vorgesehen hat (vgl. § 23 Abs. 1 Justizvergütungs- und -entschädigungsgesetz). Die hier vorgesehenen Ausgleichsansprüche sind nicht Gegenstand des vorliegenden Verfahrens. […]

IX. FÖR-Systematik: „Impact“ der Rechtswidrigkeit sowie Mehrheit im Gericht

306 FÖR-Systematik: „Impact“

Der Verstoß gegen das Grundrecht auf Schutz des Telekommunikationsgeheimnisses nach Art. 10 Abs. 1 GG führt zur Nichtigkeit der §§ 113a und 113b TKG sowie von § 100g Abs. 1 Satz 1 StPO, soweit danach Verkehrsdaten gemäß § 113a TKG erhoben werden dürfen. Die angegriffenen Normen sind daher unter Feststellung der Grundrechtsverletzung für nichtig zu erklären (vgl. § 95 Abs. 1 Satz 1 und § 95 Abs. 3 Satz 1 BVerfGG). Dementsprechend müssen die aufgrund der einstweiligen Anordnung vom 11. März 2008 und 28. Oktober 2008 von den Diensteanbietern im Rahmen von Auskunftsersuchen erhobenen aber einstweilen nicht an die ersuchenden Behörden übermittelten, sondern gespeicherten Telekommunikationsverkehrsdaten unverzüglich gelöscht werden. Sie dürfen nicht mehr an die ersuchenden Stellen übermittelt werden. […]

308 FÖR-Systematik: Mehrheit im Gericht

Die Entscheidung ist hinsichtlich der europarechtlichen Fragen, der formellen Verfassungsmäßigkeit und der grundsätzlichen Vereinbarkeit der vorsorglichen Telekommunikationsverkehrsdatenspeicherung mit der Verfassung im Ergebnis einstimmig ergangen. Hinsichtlich der Beurteilung der §§ 113a und 113b TKG als verfassungswidrig ist sie im Ergebnis mit 7:1 Stimmen und hinsichtlich weiterer materiellrechtlicher Fragen, soweit aus den Sondervoten ersichtlich, mit 6:2 Stimmen ergangen.

309 Dass die Vorschriften gemäß § 95 Abs. 3 Satz 1 BVerfGG für nichtig und nicht nur für unvereinbar mit dem Grundgesetz zu erklären sind, hat der Senat mit 4:4 Stimmen entschieden. Demzufolge können die Vorschriften auch nicht in eingeschränktem Umfang übergangsweise weiter angewendet werden, sondern verbleibt es bei der gesetzlichen Regelfolge der Nichtigerklärung.

FÖR-Systematik: Abweichende Meinung der Richter Schluckebier und Eichberger […]