

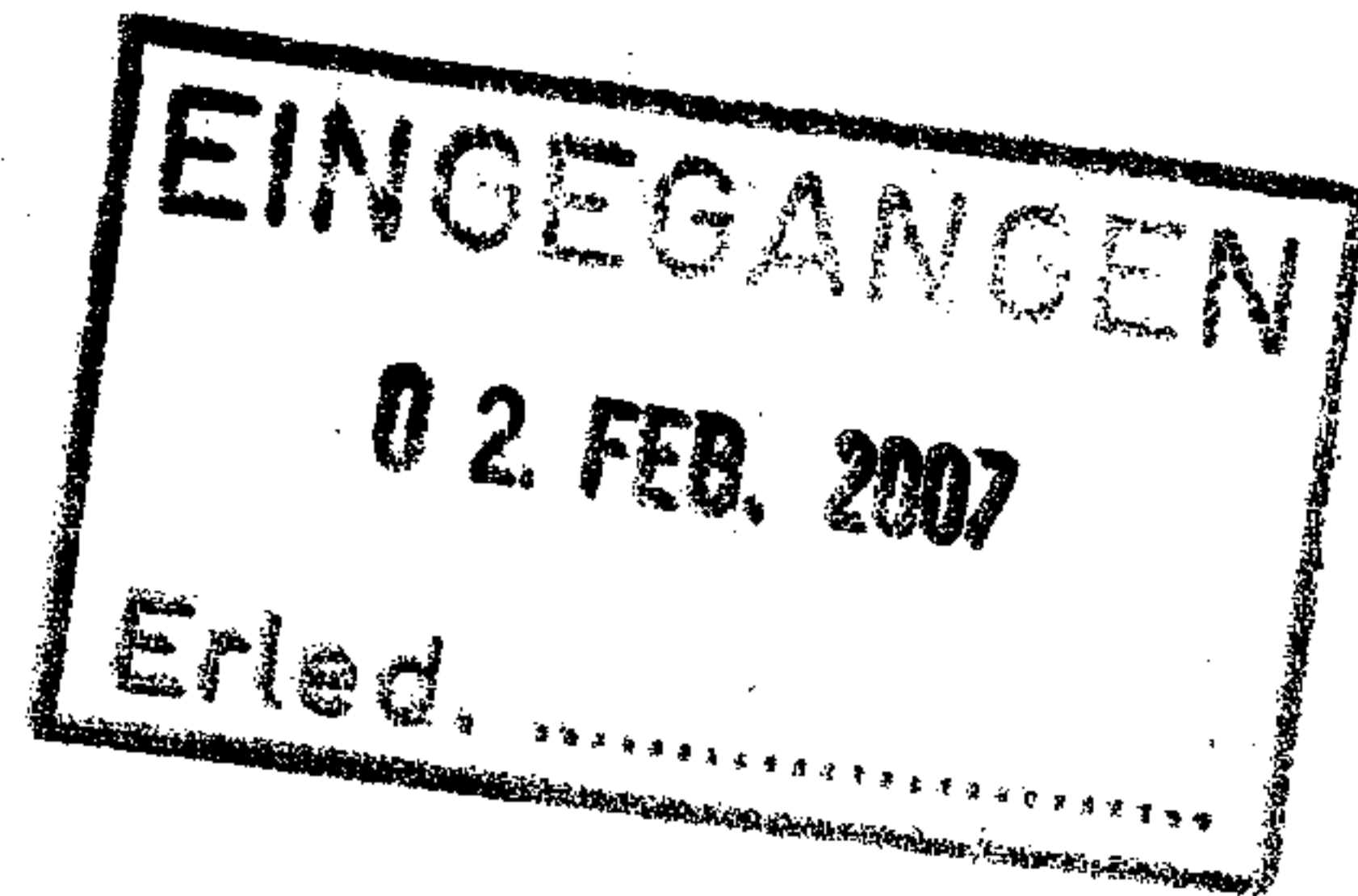


# Bundesverfassungsgericht

Erster Senat  
- Geschäftsstelle -

Bundesverfassungsgericht ♦ Postfach 1771 ♦ 76006 Karlsruhe

Herrn Rechtsanwalt  
Meinhard Starostik  
Schillstraße 9  
10785 Berlin



**Aktenzeichen**

1 BvR 1299/05  
(bei Antwort bitte angeben)

**Bearbeiter**

☎ (0721)

9101-317

**Datum**

31.01.2007

**Verfassungsbeschwerde**

d. [REDACTED] u.a.

**Ihr Aktenzeichen: 42/05**

Sehr geehrter Herr Rechtsanwalt Starostik,

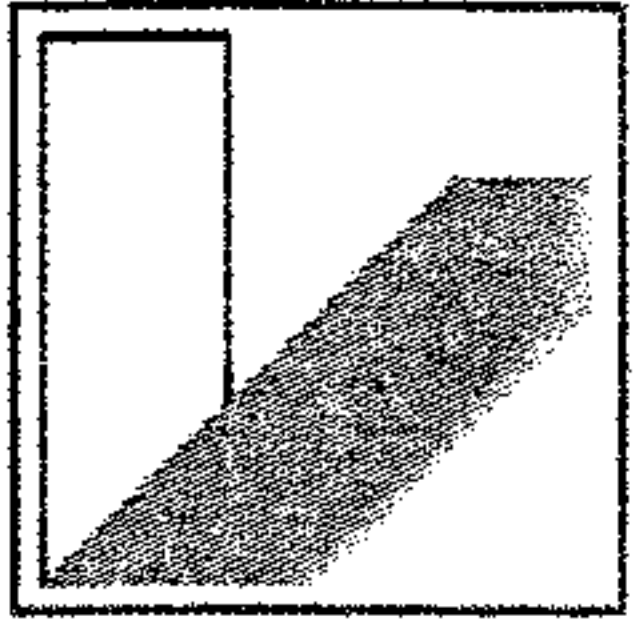
in vorgenanntem Verfassungsbeschwerdeverfahren werden Ihnen anliegend Abschriften der hier eingegangenen Stellungnahmen der Bundesregierung vom 22. Januar 2007, des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit vom 22. Januar 2007, des Berliner Beauftragten für Datenschutz und Informationsfreiheit vom 29. Januar 2007 sowie der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht vom 24. Januar 2007 zur Kenntnisnahme übersandt.

Mit freundlichen Grüßen

Auf Anordnung

[REDACTED]

Regierungsschreiberin



UNIVERSITÄT  
BAYREUTH

Mandant hat Abschrift

De

LEHRSTUHL FÜR ÖFFENTLICHES RECHT II

PROFESSOR DR. [REDACTED]

Universität Bayreuth • 95440 Bayreuth

An das  
Bundesverfassungsgericht  
Erster Senat  
Schlossbezirk 3  
76131 Karlsruhe

Postanschrift:  
Universität Bayreuth  
95440 Bayreuth

privat:

Telefon: 0921 / 55 - [REDACTED]  
0921 / 50 - [REDACTED]

Telefax: 0921 / 55 - [REDACTED]

e-mail: [REDACTED]@uni-bayreuth.de

Bayreuth, den 22.1.2007

**1 BvR 1299/05**

Betr.: Verfassungsbeschwerde

1. [REDACTED]

2. [REDACTED]

– Bevollmächtigter: Rechtsanwalt Meinhard Starostik, Schillerstr. 9,  
10785 Berlin –

gegen § 95 Abs. 3 und 4, §§ 111, 112, 113 des Telekommunikationsgesetzes  
(TKG) vom 22. Juni 2004 (BGBl. I S. 1190)

Zu der oben genannten Verfassungsbeschwerde – soweit diese noch zur Entscheidung ansteht – äußere ich mich aufgrund der bereits mit Schreiben vom 22. 9. 2006 vorgelegten Vollmacht namens der Bundesregierung.

Es bestehen – zumindest teilweise – bereits Zweifel an der Zulässigkeit der Verfassungsbeschwerde. Auch soweit die Verfassungsbeschwerde zulässig ist, ist sie jedenfalls **unbegründet**.

## A) Zum Sachverhalt

### I. Vorgeschichte

Kern des vorliegenden Verfahrens ist die Frage, inwieweit die in den §§ 111 ff. TKG geregelten Verfahren der Auskunft über von den Telekommunikationsunternehmen vorzuhaltende bzw. tatsächlich vorgehaltene Bestandsdaten ihrer Kunden (insbes. Name, Anschrift und Rufnummer) an Sicherheitsbehörden mit den Grundrechten des Grundgesetzes vereinbar sind.

Die Auskunftsverfahren der §§ 111 ff. TKG werden bisweilen – zu Unrecht – in den größeren Kontext einer angeblichen Gesamttendenz zu immer weitergehenden und vielfach neuartigen Überwachungsbefugnissen der Sicherheitsbehörden im Zuge der Bekämpfung neuartiger Gefahrenlagen (Terrorismus, organisierte Kriminalität etc.) gestellt und geradezu als Beispiel für diese Gesamttendenz präsentiert.

Beispielhaft: Saurer, NVwZ 2005, 275/277. Auch der Beschwerdeführer zu 1. hat sich in diese Richtung geäußert, vgl. Breyer, RDV 2003, 218/222.

Sie erscheinen dann in einem gleichsam von vornherein problematischen Lichte; sie sehen sich eingebettet in das allgemeinere Problem, welche Grenzen die Verfassung einer Ausweitung der Befugnisse und Fortentwicklung klassischer rechtsstaatlicher Bindungen angesichts neuer Bedrohungslagen setzt.

Hierzu z.B. BVerfG, Beschluss vom 4.4.2006 – 1 BvR 518/02 (Rasterfahndung), Abs. 135 ff.

Der so umrissenen Einordnung muss von Beginn an entschieden widersprochen werden. Der sicherheitsbehördliche Zugriff auf Bestandsdaten mag in jüngerer Zeit in tatsächlicher Hinsicht an Bedeutung gewonnen haben und technisch verfeinert worden sein; auch ist es selbstverständlich und geradezu unvermeidlich, dass die Bestandsdatenabfrage – gelegentlich und unter anderem – auch im Zusammenhang mit neuartigen Ermittlungsmethoden (z.B. sog. Funkzellenabfrage nach § 100h Abs. 1 Satz 2 StPO) oder im Rahmen der Bekämpfung von Terrorismus, organisierter Kriminalität etc. zum Einsatz kommt (siehe dazu unten II., S. 7 ff.). Dies alles ändert jedoch nichts daran, dass die Grundentscheidung, dass Bestandsdaten für die Sicherheitsbehörden zugänglich sein sollen, keineswegs etwas Neues ist, sondern bereits auf eine jahrzehntelange Praxis zurückblicken kann. Auch ist der sicherheitsbehördliche Zugriff auf Bestandsdaten von Beginn an keineswegs ein Instrument, das auf die Bekämpfung besonderer oder neuartiger Bedrohungslagen beschränkt gewesen wäre. Vielmehr handelt es sich um ein Instrument, das namentlich von den Strafverfolgungsbehörden bereits seit langem im Rahmen ihrer täglichen Arbeit eingesetzt wird.

Deutlich wird dies, wenn man sich vergegenwärtigt, dass bereits vor der Postprivatisierung zu Beginn der 1990er Jahre etwa 30.000 bis 40.000 Mal pro Monat strafverfolgungs- und sicherheitsbehördliche Abfragen von Kundendaten bei der Deutschen Bundespost stattfanden. Die bereits damals hohe Praxisbedeutung der Bestandsdatenabfrage fand bis in die 1990er Jahre hinein – anders als heute – freilich keinen Niederschlag in einer besonderen gesetzlichen Regelung (für Verkehrsdaten gab es den Jahrzehnte alten § 12 FAG). Was das Rechtsverhältnis zum Kunden, dessen Daten abgefragt werden, anbetrifft, so war die Notwendigkeit einer gesetzlichen Ermächtigung vor Entwicklung des Rechts auf informationelle Selbstbestimmung durch das Bundesverfassungsgericht im Volkszählungsurteil (BVerfGE 65, 1 ff.) des Jahres 1983 nicht gesehen worden; andererseits ging und geht die ständige Staatspraxis – wie zu zeigen sein wird – zu Recht davon aus, dass die Abfrage bloßer Bestandsdaten keinen Eingriff in Art. 10 GG darstellt, so dass auch insoweit eine besondere gesetzliche Befugnisnorm entbehrlich schien. Was hingegen das Rechtsverhältnis zur Deutschen Bundespost anbetrifft, war es erneut nicht nötig, etwa eine besondere Pflicht der Deutschen Bundespost zur Herausgabe der Daten an die zuständigen Behörden zu normieren, denn die Deutsche Bundespost war bereits nach Amtshilfegrundsätzen bzw. nach § 161 Satz 1 StPO (a. F.) zur Herausgabe dieser Daten verpflichtet.

Vgl. BT-Drucks. 13/3609, S. 55. Der Einwand der Beschwerdeschrift (S. 82), das Recht auf informationelle Selbstbestimmung sei „schon immer“ amtshilfefest gewesen, ist nicht falsch, geht im hiesigen Kontext aber doch am Kern der Sache vorbei: Dass nach dem Volkszählungsurteil im Rechtsverhältnis zum Bürger eine Befugnisnorm zur Datenerhebung erforderlich geworden ist und die Amtshilfegrundsätze für sich genommen keinen Eingriff in das Recht auf informationelle Selbstbestimmung mehr legitimieren konnten, ist völlig unbestritten. Dies ist indes eine Erkenntnis, die sich erst nach und nach durchsetzte und in den 1980er und 1990er Jahren auch erst nach und nach dazu führte, dass die entsprechenden Befugnisnormen geschaffen wurden (z.B. durch entsprechende Datenerhebungsbefugnisse in den Polizeigesetzen). Richtig bleibt indes, dass die Deutsche Bundespost – was das Rechtsverhältnis der Sicherheitsbehörde nicht zum Bürger, sondern zu ihr anbelangt – zur Amtshilfe verpflichtet war, soweit die Sicherheitsbehörde auf der Basis einer entsprechenden Befugnisnorm zu Recht um Auskunft nachsuchte. Im Übrigen würde aus dem Einwand der Beschwerdeschrift allenfalls folgen, dass auch bereits vor Erlass des TKG 1996 Normen in der Art der späteren §§ 89 Abs. 6, 90 TKG a.F. bzw. §§ 112 f. TKG n.F. hätten geschaffen werden müssen, wie sie dann später – nach erfolgter Privatisierung (siehe sogleich) – auch tatsächlich geschaffen wurden. Nichts jedoch ändert sich an der hier entscheidenden Feststellung, dass der Abruf von Bestandsdaten bereits vor 1996 gang und gäbe war.

Vor eine neue Situation sah sich die Praxis der Bestandsdatenabfrage gestellt, als die Deutsche Bundespost privatisiert und der Telekommunikationsmarkt liberalisiert wurde. Die Sicherheitsbehörden bedurften nunmehr, da sie sich nicht mehr amtshilfepflichtigen Stellen, sondern privaten Unternehmen gegenüber sahen, einer Rechtsgrundlage und Befugnisnorm, um die Telekommunikationsunternehmen zu einer Auskunft verpflichten zu können. Nur in einem schmalen Segment (allein der Strafverfolgung) sowie in einem für alle Seiten (Strafverfolgungsbehörden und Unternehmen) aufwändigen Verfahren stand mit § 161a StPO eine Basis für durchsetzbare Auskunftsverpflichtungen zur Verfügung. Desgleichen hat die Liberalisierung des Marktes mit der nunmehr großen Vielzahl an Anbietern (statt des vormaligen Monopols) dazu geführt, dass die Daten nicht mehr ohne weiteres bei nur einer Stelle abgefragt werden konnten; sollte die Bestandsdatenabfrage als wirksames Ermittlungsinstrument erhalten bleiben und eine Situation vermieden werden, bei der die Sicherheitsbehörden zunächst bei einer Vielzahl von Unternehmen anfragen müssen, um zum Erfolg zu kommen, musste irgendeine Form einer zentralen Stelle oder Datei geschaffen werden, über die die von vielen Telekommunikationsunternehmen stammenden Informationen gebündelt abgefragt werden können. Dies ist die geänderte Ausgangslage, auf die man 1996 durch Normierung einer ausdrücklichen Auskunftspflicht der Telekommunikationsunternehmen sowie durch Einrichtung eines gebündelt über die Regulierungsbehörde abzuwickelnden automatisierten Auskunftsverfahrens in § 89 Abs. 6 und § 90 TKG a.F. reagiert hat. Ziel dieser Normen ist es demnach nicht gewesen, die Sicherheitsbehörden mit neuen Instrumenten und Befugnissen auszustatten, sondern diese auch in einem nunmehr privatisierten und liberalisierten Umfeld in den Stand zu setzen, so wie bereits früher zur Erfüllung ihrer Aufgaben verlässlich auf Bestandsdaten zugreifen zu können. Durch die nunmehr ausdrückliche Regelung ist nur transparenter geworden, was bereits zuvor im Amtshilfewege praktiziert worden war.

So ausdrücklich BT-Drucks. 13/3609, S. 55; zum Ganzen auch: BeckTKG-Komm/Ehmer, 2. Aufl. 2000, § 90, Rdnr. 1 f.; Scheurle/Mayen/Löwnau-Iqbal, 2002, § 90, Rdnr. 1; BerlKommTKG/Kleszczewski, 2006, § 111, Rdnr. 2; Trute, in Trute/Spoerr/Bosch, TKG, 2001, § 90, Rdnr. 2; Gramlich, in Manssen (Hrsg.), Telekommunikations- und Multimediarecht, § 90 TKG, Rdnr. 1.

Die streitgegenständlichen §§ 111 ff. TKG n.F. ihrerseits knüpfen an den durch § 89 Abs. 6 TKG a.F. geschaffenen Rechtszustand an und setzen ihn – bei einer nunmehr übersichtlicheren Normstruktur – in der Grundsubstanz unverändert fort. Nur im Detail ist es zu sachlichen Änderungen gekommen. Neben ausdrücklichen Eingrenzungen der Befugnisse (namentlich der Begrenzung der am automatisierten Auskunftsverfahren teilnehmenden Unternehmen auf solche, die Telekommunikationsdienste

für die Öffentlichkeit anbieten) sind auch einzelne Ausweitungen zu verzeichnen. Auch diese jedoch sind nicht von der Tendenz geprägt, den Sicherheitsbehörden etwa grundlegend neuartige Ermittlungsinstrumente oder -methoden an die Hand zu geben, prägend ist vielmehr der Versuch, einzelne in der Praxis des Abrufverfahrens zu Tage getretene Lücken zu schließen und bestehende Unklarheiten zu beseitigen:

- Die Normierung einer Pflicht zur Datenvorhaltung, auch soweit die Daten nicht für betriebliche Zwecke erforderlich sind, in § 111 Abs. 1 S. 1 TKG n.F. – relevant wird dies in erster Linie bei Verträgen über Prepaidprodukte – erklärt sich daraus, dass es nach dem Urteil des BVerwG vom 22.10.2003 in Sachen 6 C 23.02 (BVerwGE 119, 123) zu einer Situation gekommen war, in der erhebliche Teile der Telekommunikationsteilnehmer (nämlich die Kunden von Prepaidprodukten) aus dem System des automatisierten Abrufs herausfielen, was die Effektivität des Abrufverfahrens schmälerte und eine an sich systemwidrige Ausnahme von der Grundentscheidung für die prinzipielle Zugänglichkeit der Bestandsdaten für Sicherheitsbehörden geschaffen hatte. Dass die Bedeutung von Prepaidprodukten stark gestiegen war, hatte diesen Mangel des alten Abrufverfahrens nur umso gravierender gemacht.

- Die Pflicht zur Datenspeicherung bis zum Ablauf des auf die Vertragsbeendigung folgenden Kalenderjahres in § 111 Abs. 1 S. 4 TKG (parallel zum entsprechenden und bereits zuvor bestehenden [§ 4 Abs. 2 TDSV a.F.] Recht nach § 95 Abs. 3 TKG) ist Konsequenz der in der Praxis zutage getretenen Schwierigkeiten, bei denen Ermittlungen von Strafverfolgungsbehörden daran gescheitert waren, dass Vertragsverhältnisse mittlerweile beendet worden waren und eine Ermittlung der hinter einer Rufnummer stehenden Person daher nicht mehr möglich war.

- Dass der Kreis der im automatisierten Verfahren vorzuhaltenden Bestandsdaten geringfügig erweitert wurde (z.B. Geburtsdatum, Anschrift des Festnetzanschlusses, Datum des Vertragsbeginns), sollte die Verlässlichkeit der Datenabfragen nach § 112 TKG steigern und insbesondere unnötige Anfragen im aufwändigeren manuellen Verfahren nach § 113 TKG vermeiden, nicht aber verschafft es den Sicherheitsbehörden neuartige Ermittlungsmöglichkeiten (die entsprechenden Informationen werden bislang nach § 113 TKG abgerufen, siehe z.B. unten S. 13 Fallbeispiel 4); die Abrufbarkeit der neuen Datenkategorien ist bis zum Erlass der entsprechenden Verordnung noch nicht umgesetzt).

- Ähnliches gilt für die neu geschaffene (bis zum Erlass der entsprechenden Verordnung noch nicht realisierte) Möglichkeit des Abrufs unter Verwendung unvollständiger Abfragedaten oder der Suche mittels einer sog. Ähnlichenfunktion nach § 112 Abs. 1 S. 4 TKG. Rechnung getragen wird mit ihr der praktischen Erfahrung, dass es insbesondere bei ausländischen Namen (mit unsicherer Schreibweise oder nichtlateinischem Alphabet), bei Doppelnamen und Doppelvornamen (mit oder ohne Bindestrich etc.) sowie bei Firmenangaben aufgrund der unklaren Schreibweise oder wegen der unterschiedlichen Handhabung der Eingabefelder bei den Telekommuni-

kationsunternehmen immer wieder zu – in der Sache unrichtigen – Fehlanzeigen oder aber auch zu unnötigen Mehrfachanfragen (mit je unterschiedlicher Schreibweise) kommt. Das neue Verfahren will diesem Manko, d.h. konkreten Schwierigkeiten in der bisherigen Handhabung abhelfen, nicht jedoch grundlegend neue Ermittlungsmethoden erschließen, schon gar nicht die in der Beschwerdeschrift (S. 85) „an die Wand gemalten“ Szenarien einer Art systematischen Rasterfahndung. Eine derartige „Rasterung“ ist durch die neu geschaffene Suchfunktion weder praktisch umsetzbar (schon wegen der geringen Aussagekraft der Daten, selbst soweit man sie kombiniert), noch wird sie auf der Basis der noch zu erlassenden Rechtsverordnung nach § 112 Abs. 3 TKG (in der eingrenzende Kriterien zu bestimmen sind) zulässig sein. Das Vorbringen der Beschwerdeschrift geht insoweit an der zu erwartenden Praxis vorbei.

- Die punktuellen Ausweitungen des Kreises der zu Auskunftersuchen im automatisierten Verfahren berechtigten Behörden sind überwiegend Konsequenz geänderter oder neu geschaffener Zuständigkeiten; in keinem Fall fällt die Berechtigung aus dem Rahmen der schon zuvor bestehenden Konzeption einer prinzipiellen Zugänglichmachung von Bestandsdaten für Zwecke der Sicherheitsgewährleistung.

- Die Regelungen zur Auskunft über sog. Zugriffsdaten (näher dazu s.u. S. 36) in § 113 Abs. 1 S. 2 und 3 TKG bezwecken angesichts in der Praxis aufgetretener Meinungsverschiedenheiten zwischen Sicherheitsbehörden und Diensteanbietern in erster Linie eine Klarstellung dahingehend, dass der Zugriff auf diese Daten – nach Einschätzung des einfachen Gesetzgebers – nicht dem Fernmeldegeheimnis unterfällt und daher auf der Basis der regulären (v.a. strafprozessualen oder polizeirechtlichen) Datenerhebungsbefugnisse zulässig ist, sowie dass andererseits ein Eingriff in Daten, die tatsächlich dem Fernmeldegeheimnis unterliegen, auf der Basis des § 113 TKG jedenfalls ausgeschlossen sein soll. Erneut geht es nicht um die Schaffung neuartiger Befugnisse.

Leitbild der 2004 erfolgten Novelle und der neuen §§ 111 ff. TKG ist nach alledem nicht die Schaffung neuartiger Befugnisse. Vielmehr geht es darum, die bereits 1996 vom Gesetzgeber getroffene Grundentscheidung für eine prinzipielle Zugänglichmachung der Telekommunikationsbestandsdaten für die Zwecke der Sicherheitsbehörden, die ihrerseits nichts Neues war, sondern auf eine jahrzehntelange Praxis zurückblicken konnte, angesichts konkreter in der Praxis aufgetretener Schwierigkeiten konsequent umzusetzen, indem spezifische Mängel des bisherigen Verfahrens beseitigt wurden.

Zu den Zwecken der in §§ 111 ff. TKG getroffenen Neuerungen: BT-Drucks 15/2316, S. 95 bis 97, 124; Thiede, Kriminalistik 2004, S. 104/105, 107 ff.

## II. Zur heutigen Praxis und Praxisbedeutung der Auskunftsverfahren

Das bis hierher Gesagte – dass der sicherheitsbehördliche Zugriff auf Bestandsdaten nichts wesensmäßig Neues ist und bereits auf eine jahrzehntelange Praxis zurückblicken kann – kann und soll nicht darüber hinwegtäuschen, dass die praktische Bedeutung des Auskunftsrechts in Bezug auf Bestandsdaten in den letzten Jahren stark angestiegen ist. Dass das Recht auf Auskunft über Telekommunikationsbestandsdaten in der täglichen Arbeit der Sicherheitsbehörden zu einem zunehmend wichtigen und unverzichtbaren Ermittlungsinstrument geworden ist, spiegelt sich nicht zuletzt in der Statistik zu dem automatisierten Auskunftsverfahren nach § 112 TKG (§ 90 TKG a.F.) wieder, die für die letzten Jahre einen Anstieg auf nunmehr 3,4 Mio. Ersuchen pro Jahr ausweist (2001: 1,5 Mio.; 2002: 2,0 Mio.; 2003: 2,7 Mio.; 2004: 2,9 Mio., 2005: 3,4 Mio.). Für 2006 ist allenfalls mit einem leichten, nicht jedoch mit einem sprunghaften Anstieg zu rechnen.

Die Zahl der Ersuchen pro Jahr wird von der Bundesnetzagentur in ihren Jahresberichten veröffentlicht. (Der Jahresbericht 2005 findet sich z.B. auf <http://www.bundesnetzagentur.de/media/Archive/5278.pdf>; dort S. 96.) Auskunft geben auch die Tätigkeitsberichte des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (z.B. der 20. Tätigkeitsbericht 2003-2004, S. 144, der von etwas über 2,5 Mio. Ersuchen pro Jahr spricht). Die veröffentlichten Statistiken der Bundesnetzagentur verzeichnen neben der Zahl von Auskunftersuchen (Anfragen von Sicherheitsbehörden) auch die Zahl der Abfragen bei TK-Diensteanbietern, die deutlich höher liegt. Für die sicherheitsbehördliche Praxis aussagekräftig ist allein die Zahl der Auskunftersuchen; die Zahl der Abfragen bei TK-Anbietern meint die Zahl der technischen Abrufe bei ggf. mehreren TK-Unternehmen, die notwendig sind, um das Ersuchen einer Sicherheitsbehörde zu beantworten (sollen z.B. die Rufnummern einer Person ermittelt werden, so ist die Abfrage bei allen TK-Anbietern nötig).

Der Grund für diesen Anstieg kann allenfalls zum Teil mit den Vorzügen des automatisierten Verfahrens erklärt werden (in dringenden Fällen, die aber nur 2 % der Ersuchen ausmachen, ist die Beantwortung beispielsweise in nur 3 Minuten möglich; 88 % der Ersuchen werden binnen 24 Stunden beantwortet). Er ist auch nicht Ausdruck eines sorgloseren Umgangs mit der Auskunftsbefugnis (in den jeweiligen Behörden ist die Zahl der auskunftsberechtigten Personen typischerweise stark begrenzt; bei der Bayerischen Polizei sind z.B. nur ca. 2.200 von insgesamt ca. 35.000 Vollzugsbeamten abfrageberechtigt). Vor allem aber – das wurde unter I. (S. 2 ff.) dargelegt – hat der Anstieg der Ersuchen seinen Grund sicher nicht in einer grundlegend geänderten oder ausgeweiteten Befugnisstruktur, denn die prinzipielle Ausgestaltung der Befugnisse ist zumindest seit 1996, im Grunde aber sogar noch länger,

gleich geblieben (zentrale Neuerungen der Novelle von 2004, wie die zusätzlichen Abfragedaten nach § 111 TKG oder die Suchfunktionen nach § 112 Abs. 1 S. 4 TKG sind gegenwärtig noch nicht einmal umgesetzt; außerdem müssen sie, da sie Nachfragen bzw. unnötige Mehrfachanfragen vermeiden helfen, keineswegs zu einem weiteren Anstieg der Auskunftersuchen führen). Die Gründe für den Anstieg der Anzahl der Auskunftersuchen sind demnach nicht in erster Linie in der rechtlichen oder technischen Ausgestaltung des Auskunftsverfahrens zu suchen, sondern können allein in den tatsächlichen Gegebenheiten liegen, auf die dieses Verfahren trifft. Zu nennen ist hierbei vor allem das seit den 1990er Jahren dramatisch geänderte Telekommunikationsverhalten der Bevölkerung im Allgemeinen, aber auch – nach übereinstimmender Aussage der Sicherheitsbehörden – der für diese Behörden relevanten Personengruppen im Besonderen. Vergegenwärtigt man sich den gewaltigen wirtschaftlichen Aufschwung des Telekommunikationssektors in den letzten Jahren und, wie sich beispielsweise das Kommunikationsverhalten allein dadurch geändert hat, dass in diesem Zeitraum die Mobiltelefone aufgekommen und zum alltäglichen Kommunikationsinstrument für jedermann (auch und gerade für kriminelle Kreise, die im Visier der Sicherheitsbehörden stehen) geworden sind, so verwundert es nicht, wenn die Abfragehäufigkeit telekommunikationsspezifischer Bestandsdaten mit dieser Entwicklung Schritt hält und ihrerseits ansteigt.

Die Zahl der Mobilfunkanschlüsse beispielsweise ist nach Auskunft der Bundesnetzagentur allein im Zeitraum 2000 bis 2005 von 48.200.000 auf 79.200.000 angestiegen.

Das Bundesverfassungsgericht selbst hat jüngst eindringlich darauf hingewiesen, wie die vermehrte Nutzung elektronischer und digitaler Kommunikationsmittel die Bedingungen der Strafverfolgung verändert hat, indem sie eine effektive Strafverfolgung einerseits erheblich erschwert, andererseits aber – wenn die Strafverfolgung mit der technischen Entwicklung Schritt hält – auch neue Ermittlungsansätze schafft.

BVerfG, Kammerbeschluss vom 22.8.2006 – 2 BvR 1345/03, Abs. 75.

Die Verfolgung von Telekommunikationsspuren hat vor diesem Hintergrund in der Arbeit der Ermittlungsbehörden generell stark an Relevanz gewonnen. Es liegt hierin begründet, dass auch die Auskunft über Bestandsdaten bedeutungsvoller und häufiger unverzichtbar geworden ist.

Das automatisierte Auskunftsverfahren nach § 112 TKG wird weit überwiegend zu Zwecken der Strafverfolgung genutzt. Sowohl Gefahrenabwehrzwecke wie auch nachrichtendienstliche Zwecke sind zwar nicht ohne Praxisrelevanz, treten zahlenmäßig demgegenüber jedoch deutlich in den Hintergrund; das Bundesamt für Verfassungsschutz beispielsweise stellt mit ca. 32.000 Anfragen weniger als 1 % aller

Anfragen liegt erfahrungsgemäß zwischen 3 % und 5 % der Anfragen nach § 112 TKG.

BeckTKG-Komm/Bock, 3. Aufl. 2006, § 112, Rdnr. 9 spricht von einer – nach Jahren des kontinuierlichen Anstiegs – in jüngerer Zeit eher verhaltenen Entwicklung der Anfragezahlen im manuellen Verfahren.

Zum Ausdruck kommt hierin, dass das Verfahren nach § 113 TKG gegenüber dem nach § 112 TKG – die gesetzliche Anordnung bringt dies nunmehr klarer zum Ausdruck – sowohl rechtlich subsidiär ist

BerlKommTKG/Kleszczewski, 2006, § 113, Rdnr. 1, spricht von Auffangregelung,

als auch in der Praxis der Sicherheitsbehörden als subsidiär gehandhabt wird; dies ist im Übrigen schon wegen der Kostenfolge nach § 113 Abs. 2 TKG so. Die Auskunft nach § 113 TKG kommt demnach zum einen im Nachgang zu einem Auskunftersuchen nach § 112 TKG in Betracht, wenn dieses entweder fehlgeschlagen ist oder aber in einem zweiten Schritt zusätzliche Informationen (die über § 111 TKG hinausgehen) abgefragt werden sollen. Zum anderen wird § 113 TKG dann eingesetzt, wenn von vornherein klar ist, dass man mit § 112 TKG nicht zum Ziel kommen kann. Dies kann erstens der Fall sein, wenn es um die Abfrage von Daten geht, die nicht § 111 TKG unterfallen, aber vom Telekommunikationsanbieter nach § 95 TKG zu Recht vorgehalten werden. Dies kommt zweitens in Betracht, wenn die ersuchende Behörde nicht zum Kreis der anfrageberechtigten Sicherheitsbehörden nach § 112 Abs. 2 TKG gehört. Und dies ist drittens denkbar, wenn es um die Anfrage bei Telekommunikationsdienstleistern geht, die ihre Telekommunikationsdienste nicht für die Öffentlichkeit erbringen und daher nicht § 112 TKG, sondern allein § 113 TKG unterfallen. Hierzu gehören auch Betreiber von internen und geschlossenen Netzen, also z.B. Unternehmen, Universitäten, Hotels, Krankenhäuser etc.

BerlKommTKG/Kleszczewski, 2006, § 113, Rdnr. 3.

Fehl geht es indes, wenn die Beschwerdeführer hieraus die Befürchtung ableiten, die Bestandsdatenabfrage bei geschlossenen Netzen könnte zur Ausforschung bestimmter Lebensumstände und -gewohnheiten genutzt werden.

Beschwerdeschrift S. 10. Das dort gewählte Beispiel einer Aids-Selbsthilfegruppe ist freilich ganz fern liegend. Denn es erscheint kaum denkbar, dass eine derartige Selbsthilfegruppe ein geschlossenes Telefonnetz betreibt; und auch, dass sie etwa selbst statische, d.h. feste IP-Adressen vergibt, scheint nicht plausibel. Sollte es dagegen – weitaus wahrscheinlicher – um die Ausforschung eines Internet-Chatforums o.Ä. gehen, ginge es um Verkehrs-, nicht aber um Bestandsdaten, so dass §

113 TKG nicht einschlägig ist (so zu Recht Kühling, K&R 2004, 105/107, Fn. 20).

Die Auskunft nach § 113 TKG ist für Zwecke einer derartigen Ausforschung wenig geeignet. Zu bedenken ist dabei, dass bei § 113 TKG, bei dem sich das Auskunftersuchen stets spezifisch an einen bestimmten Diensteanbieter richtet, bereits bekannt sein muss, an welchen Betreiber eines geschlossenen Netzes man sich wendet; der jeweilige Lebensumstand (Zugehörigkeit zu einem Unternehmen, Aufenthalt in einem Krankenhaus etc.), der angeblich ausgeforscht werden soll, müsste also bereits – zumindest in Form konkreter und in gewissem Umfang verdichteter Anhaltspunkte – bekannt sein, bevor man § 113 TKG überhaupt zum Einsatz bringen kann. Hinzu kommt ein Zweites: Liegt ein derartiger Verdacht eines bestimmten Lebensumstandes bereits vor und soll nunmehr Gewissheit geschaffen werden, gibt es für Ermittlungsbehörden typischerweise andere – effektivere – Ermittlungsmethoden, z.B. Zeugenbefragungen im Unternehmen, im Krankenhaus, um zum Erfolg zu kommen. Diese benötigen hierfür nicht die Möglichkeit des § 113 TKG. In der Praxis des § 113 TKG dagegen geht es um die Aufhellung der spezifischen Verknüpfung von Person und Rufnummer/fester IP-Adresse/PIN o.Ä., d.h. um eine telekommunikationsbezogene Auskunft, die anderweitig nicht zu beschaffen ist.

Die Verfahren nach §§ 112, 113 TKG sind ein wertvolles und unverzichtbares Ermittlungsinstrument. Im Folgenden soll anhand der vor allem praxisrelevanten Strafverfolgung aufgezeigt werden, in welchen typischen Situationen die Strafverfolgungsbehörden um Auskunft über Bestandsdaten nachsuchen und welche Erfolge hiermit erzielt werden können. Das Bayerische Landeskriminalamt und das Bundeskriminalamt haben einige Fallbeispiele für einen erfolgreichen Einsatz der Auskunftsverfahren nach §§ 112, 113 TKG aus der tatsächlichen Praxis der letzten Jahre zusammengestellt, die an jeweils geeigneter Stelle zur Illustration eingefügt werden. Vor allem drei große Fallgruppen können unterschieden werden, in denen in der Praxis der Strafverfolgungsbehörden um Auskunft über Bestandsdaten nachgesucht wird:

#### (1) Auskunftersuchen ohne jeden Zusammenhang mit Eingriffen in Art. 10 GG

Der Hauptanwendungsfall der Bestandsdatenrecherche betrifft eine Situation, die in keinerlei Zusammenhang mit Maßnahmen der Telekommunikationsüberwachung oder sonstigen Eingriffen in Art. 10 GG steht. Nach Auskunft von Polizeibehörden wird man bei grober Schätzung von mindestens zwei Drittel der Fälle ausgehen können, die in diese Kategorie fallen. Zumeist geht es um Situationen, in denen aufgrund „normaler“ Ermittlungsmaßnahmen (d.h. ohne Eingriff in Art. 10 GG) Informationen über Rufnummern erlangt werden, die nun bezüglich der dahinter stehenden Perso-

nen weiter ausgewertet werden sollen. Ein typischer Fall wäre etwa, wenn ein Drogendealer angibt, er stehe in geschäftlichem Kontakt mit jemandem, von dem er nur eine Mobilfunkrufnummer und den Vornamen wisse, dessen Identität und Anschrift er ansonsten jedoch nicht kenne. Soll der Betreffende ausfindig gemacht werden, hilft allein die Bestandsdatenrecherche. Ähnlich wäre es, wenn etwa Aufzeichnungen (Notizbücher oder dergleichen) sichergestellt werden, in denen unbekannte Rufnummern vermerkt sind. Da nach der Rechtsprechung des Bundesverfassungsgerichts der Zugriff auf Verkehrsdaten im Herrschaftsbereich des Kommunikationsteilnehmers (z.B. wenn Verkehrsdaten auf einem Mobiltelefon gespeichert sind) nicht dem Art. 10 GG unterfällt,

BVerfG, Urteil vom 2.3.2006 – 2 BvR 2099/04,

läge ein Beispiel der Fallgruppe „Einsatz ohne jeden Bezug zu Eingriffen in Art. 10 GG“ über die zuerst genannten klassischen Beispiele hinausgehend auch vor, wenn nach Ermittlung derartiger Verkehrsdaten nunmehr recherchiert werden soll, wer hinter einer Rufnummer steht.

Fallbeispiel 1: Im Zusammenhang mit Durchsuchungen wegen schweren sexuellen Missbrauchs von Kindern wurden beim Hauptbeschuldigten eine Vielzahl von Asservaten, insbesondere Telefonverzeichnisse und Einzelverbindungsanfragen, sichergestellt. Über die Feststellung der Anschlussinhaber und die sich anschließenden Ermittlungen (Lichtbildvergleiche, Dokumenten- und Aktenauswertungen) gelang die Aufhellung eines Netzwerkes Pädophiler mit bundesweiten Verzweigungen. Dadurch konnten weitere Verdachtsmomente für sexuelle Missbrauchshandlungen an anderen geschädigten Kindern und Jugendlichen gewonnen werden.

Fallbeispiel 2: Im Rahmen eines Ermittlungsverfahrens (betr. Unterstützung einer terroristischen Vereinigung) wurde bei den beschuldigten Personen durchsucht und u.a. ein Notizbuch mit Aufzeichnungen sichergestellt. Unter diesen Aufzeichnungen befanden sich offensichtlich Rufnummern z.T. in Verbindung mit Rufnamen. Zur Identifizierung dieser Kontaktpersonen wurden Anschlussinhaberfeststellungen (Abfragen nach §§ 112, 113 TKG) getroffen. Dies ermöglichte weitere strafprozessuale Maßnahmen.

Fallbeispiel 3: In einem Ermittlungsverfahren wegen Schleusung, Zuhälterei u.a. nutzte der Hauptbeschuldigte ein Mobiltelefon. Das Telefon war auf eine unbeteiligte Person registriert. Als Rechnungsanschrift wurde durch eine Anfrage nach 113 TKG jedoch eine den Ermittlungsbehörden bis dahin unbekannte Adresse mitgeteilt. Bei dieser Adresse handelte es sich um den tatsächlichen Wohnort (abweichend von der Auskunft aus dem Melderegister) des Hauptverdächtigen, den er bewusst verschleierte. Die Durchsuchung dieser Wohnung auf richterlichen Durchsuchungsbeschluss trug wesentlich zur Tataufklärung bei.

Fallbeispiel 4: In einem Ermittlungsverfahren wegen international organisierten Heroinhandels wurde die Mobilfunkrufnummer des Hauptbeschuldigten bekannt. Es wurde bewusst eine Anfrage nach § 113 TKG gehalten, um die Dauer des Vertragsverhältnisses zu ermitteln. Durch die Antwort wurde bekannt, dass der Beschuldigte bereits Jahre zuvor Anschlussinhaber war. Da die Rufnummer bereits in einem früheren Ermittlungsverfahren einer LKA-Dienststelle aufgetreten war, konnte nunmehr geklärt werden, dass der Beschuldigte bereits in dem vorangegangenen Verfahren aufgetreten war. Die Telefonnummer und die Erkenntnis, dass ein- und dieselbe Person in der relevanten Zeitspanne Anschlussinhaber war, führten letztlich dazu, dass beide Verfahren im Zusammenhang gesehen werden konnten.

## (2) Auskunftersuchen zur Vorbereitung von Eingriffen in Art. 10 GG

Eine weitere Fallgruppe betrifft Fälle, in denen im Vorfeld etwaiger Telekommunikationsüberwachungsmaßnahmen (TKÜ-Maßnahmen) in einem ersten Schritt herausgefunden werden muss, über welche Rufnummern und Anschlüsse eine bestimmte Person verfügt. Daraus, dass, wie oben dargelegt, nur ca. 5 % der Auskunftersuchen so gestaltet sind, dass von einer Person auf die Rufnummer geschlossen werden soll, und auch von diesen 5 % viele Fälle sicherlich keinerlei Bezug zu etwaigen TKÜ-Maßnahmen aufweisen, wird deutlich, dass die Fallgruppe „Vorbereitung von TKÜ-Maßnahmen“ ein zwar wichtiges, aber zahlenmäßig keineswegs dominierendes Einsatzfeld ist.

Fallbeispiel 5: Im Rahmen von gezielten Fahndungsmaßnahmen nach einem mit internationalem Haftbefehl wegen Mordes in vier Fällen, Mitgliedschaft in einer kriminellen Vereinigung, des internationalen Handels mit Betäubungsmitteln und Sprengstoffanschlägen gesuchten italienischen Staatsangehörigen wurde festgestellt, dass die Tochter der gesuchten Person in München wohnt. Mit einer Anfrage zunächst gem. § 112 TKG und anschließend gem. § 113 TKG konnten Ansätze für die Einleitung von Maßnahmen gem. §§ 100a, 100b StPO gewonnen werden. Die Überwachung des Telefonanschlusses der Tochter führte zur Ermittlung des von dem Tatverdächtigen in Deutschland benutzten Mobiltelefons und schließlich zur Festnahme.

## (3) Auskunftersuchen zur Nachbereitung von Eingriffen in Art. 10 GG

Eine letzte Fallgruppe betrifft Situationen, in denen mithilfe von Eingriffen in Art. 10 GG Rufnummern ermittelt wurden und nunmehr in einem zweiten Schritt herausgefunden werden soll, an wen eine der ermittelten Rufnummern vergeben ist. Dies ist etwa der Fall, wenn über die Erhebung von Verkehrsdaten ermittelt wurde, mit welchen Rufnummern eine Person telefoniert hat, oder wenn über eine Funkzellenabfrage ermittelt wurde, dass aus einer bestimmten Funkzelle zu einem bestimmten

Zeitpunkt von einem bestimmten Mobilfunkanschluss aus telefoniert wurde etc. In all diesen Fällen liefert der z.B. durch § 100g StPO gerechtfertigte Eingriff in Art. 10 GG als solcher allein die Ermittlung einer oder mehrerer Rufnummern, die zunächst keinen direkten Personenbezug aufweisen. Soll in der Nachbereitung dieser Maßnahme bezüglich einer oder aller dieser Rufnummern weiter ermittelt und auf die zugehörige Person geschlossen werden, so geschieht dies über Auskunftersuchen nach §§ 112, 113 TKG.

Fallbeispiel 6: Am Flughafen Schiphol/Amsterdam wird bei der Einreise aus Surinam ein in München wohnhafter deutscher Staatsangehöriger mit 2,4 kg Kokain festgenommen. Wegen der Auslandsstraftat wurde bei der Staatsanwaltschaft München I ein Ermittlungsverfahren eingeleitet. Der Festgenommene bestritt bei seinen ersten Vernehmungen eine Tatbeteiligung und gab an, dass man das Rauschgift in Surinam unbemerkt in seinem Koffer versteckt habe. Durch die Auswertung der beauskunfteten Verkehrsdaten des von ihm benutzten Mobiltelefons und anschließende Auskunftersuchen gem. § 112 TKG konnte ihm nachgewiesen werden, dass er bereits vor dem Abflug nach Surinam Kontakt zu seinem Auftraggeber gehabt hatte. Nach einem erneuten Tatvorhalt räumte er seine Tatbeteiligung ein und machte umfangreiche Angaben, die zur Festnahme zahlreicher weiterer Mittäter und der Aufhellung internationaler Strukturen führten.

Fallbeispiel 7: Im Rahmen von Ermittlungen gegen den Betreiber eines der größten bisher festgestellten illegalen Drogenlabore zur Herstellung eines Amphetamins in Bayern wurden gem. §§ 100g, 100h StPO die beim Beschuldigten angefallenen Telefonverkehrsdaten erhoben. Die Feststellung der Anschlussinhaber gem. § 112 TKG führten zu weiteren Ermittlungsansätzen gegen Chemikalienlieferanten und Abnehmer der produzierten Drogen.

Fallbeispiel 8: Bei der Sicherstellung gefälschter US-Banknoten im (Nominal-)Wert von 1 Million US-Dollar im April/Mai 2005 bei München und der Ermittlung einer deutsch-jugoslawischen Tätergruppierung mit insgesamt 21 Beschuldigten sind die Täterkontakte u.a. durch TKÜ-Maßnahmen und durch die Auswertung der Verkehrsdaten aus sichergestellten Mobiltelefonen in Verbindung mit den zahlreichen hierzu erfolgten Auskunftersuchen gem. § 112 TKG ermittelt und nachgewiesen worden. Die Ergebnisse brachten Erkenntnisse über die Täterstruktur, die Zusammenhänge mit weiteren Geldfälschungsdelikten in Deutschland (Bayern, Sachsen, Nordrhein-Westfalen, Baden-Württemberg) sowie die Herkunft des Falschgeldes und führten zur Identifizierung des Falschgeldlieferanten.

Fallbeispiel 9: In einem Ermittlungsverfahren wegen international organisierten Heroinschmuggels teilte eine Zeugin mit, dass der Hauptbeschuldigte telefonisch zu einem bestimmten Zeitpunkt mit dem bis dahin unbekannten Mitbeschuldigten wesentliche Absprachen zur weiteren Tatausführung getroffen hat. Ein Abgleich der Verkehrsdaten mit dem von der Zeugin benannten Zeitpunkt führte zu einer Mobilfunkrufnummer. Eine Ab-

frage nach § 112 TKG führte zur Namhaftmachung der fraglichen Person und zu weiteren Ermittlungen.

Fallbeispiel 10: Im Rahmen von TKÜ-Maßnahmen wurde ein Gesprächspartner des Beschuldigten (Verdacht: geheimdienstliche Agententätigkeit) bekannt, der von diesem als Informant eingesetzt werden sollte. Aus dem Gesprächsinhalt ergab sich zur Person des Informanten lediglich dessen Vorname. Durch die Anschlussinhaberfeststellung nach dem TKG konnten Name und Adresse des vorgesehenen Informanten festgestellt werden. Die endgültige Identifizierung gelang im Anschluss durch eine Einwohnermeldeamtsanfrage, die ohne die vorherige Auskunft nach dem TKG nicht möglich/aussichtslos gewesen wäre. Der im Telefonat benutzte Vorname stellte sich im Zuge der weiteren Ermittlungen als falsch bzw. nicht im Melderegister verzeichnet heraus. Die Aussage des identifizierten Gesprächspartners konnte zur Aufklärung der Ausspähungsaktivitäten des Beschuldigten beitragen.

### III. Der nationale und europäische Regelungskontext

Die Beschwerdeführer versuchen, vor allem das automatische Auskunftsverfahren nach § 112 TKG als etwas im nationalen und internationalen Kontext Ungewöhnliches und aus dem Rahmen Fallendes darzustellen.

Die Beschwerdeschrift spricht auf S. 81 von einem „weltweit einzigartigen automatischen Online-Abfrageverfahren“; auf S. 53 ist von einem „einzigartigen“ Präzedenzfall vorsorglicher staatlicher Überwachung der Bürger“ die Rede.

Dieser Charakterisierung muss widersprochen werden. Das Auskunftsverfahren fällt im internationalen Vergleich keineswegs aus dem Rahmen. Und auch im nationalen Kontext ist der Bestandsdatenabruf keineswegs die einzige automatisierte Zugriffsmöglichkeit von Sicherheitsbehörden auf Daten zu Identität, Wohnsitz und Erreichbarkeit einer Person; vielmehr gibt es vergleichbare Auskunftsregister (Melderegister, Fahrzeugregister), mit denen sich hinsichtlich Voraussetzungen und Modalitäten des automatisierten Abrufs durchaus vergleichbare und übergreifende Regelungsstrukturen ergeben.

Was zunächst den internationalen Vergleich angeht, so erwähnt der Beschwerdeführer zu 1) an anderer Stelle selbst, dass auch in Großbritannien ca. 1 Mio. Mal pro Jahr TK-Bestandsdaten abgefragt werden.

Breyer, RDV 2003, 218/219.

Bedenkt man, dass sich diese Angaben auf eine Zeit vor 2003 beziehen müssen, zu der die Anfragezahlen auch in Deutschland noch unter 2 Mio. lagen, so wird deutlich, dass schon insoweit die deutschen Zugriffsmöglichkeiten nichts Ungewöhnliches sein können. Im Gegenteil ist es so, dass in Großbritannien sogar Verkehrsdaten im automatisierten Abruf abgefragt werden können. Auch die Niederlande beispielsweise haben ein System der Bestandsdatenabfrage, das dem deutschen sehr ähnlich ist.

Die dem § 111 TKG zugrunde liegende Idee einer obligatorischen Vorhaltung von Telekommunikationsbestandsdaten für Zwecke der Sicherheitsgewährleistung ist mittlerweile auch vom europäischen Gemeinschaftsrecht aufgegriffen worden und dem deutschen Gesetzgeber insoweit zwingend vorgegeben.

Richtlinie 2006/24/EG vom 15. März 2006 (ABl. Nr. L 105/54) über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (Vorratsdatenspeicherungsrichtlinie). Zur Bestandsdatenspeicherung siehe Art. 5 Abs. 1 a Nr. 1 ii, b Nr. 1 ii der Richtlinie.

Etwa in der Erstreckung der Bestandsdatenerfassung auf Dienste der elektronischen Post sowie vor allem in der Pflicht zur Vorhaltung auch von Telekommunikationsverkehrsdaten geht die Richtlinie über das bisherige deutsche Recht sogar hinaus.

Systemkonform fügt sich der Regelungskomplex der §§ 111 ff. TKG auch in Regelungsstrukturen des nationalen Rechts ein. Zu verweisen ist insbesondere darauf, dass es auch andere – in ihrer Ausgestaltung durchaus vergleichbare – automatisierte Zugriffsmöglichkeiten der Sicherheitsbehörden auf grundlegende Daten zu Identität und Auffindbarkeit/Erreichbarkeit einer Person gibt:

- Grundlegend ist das Melderegister und das in § 18 MRRG und im konkretisierenden Landesrecht (für Bayern z.B. Art. 31 BayMeldeG, § 8 BayMeldeDÜV) geregelte automatisierte Abrufverfahren für die Polizei. In ihm sind die Basisdaten zu Identität und Aufenthalt (Wohnsitz) einer Person gespeichert. Sie stehen der Polizei unter ähnlichen Voraussetzungen (Erforderlichkeit der Kenntnis für die Erfüllung polizeilicher Aufgaben) und unter ähnlichen Modalitäten (z.B. keine besondere Statuierung einer Mitteilungspflicht an den Betroffenen im Falle automatisierter Abrufe) zur Verfügung, wie dies auch in § 112 TKG für Telekommunikationsbestandsdaten der Fall ist. Die im Melderegister gespeicherte Verknüpfung von Name und Anschrift weist im Übrigen einen ähnlichen potentiellen Bezug zu Fragen des Art. 10 GG auf, wie dies auch bei den Telekommunikationsbestandsdaten der Fall ist. Denn die vorbereitende Klärung der Anschrift einer Person über das Melderegister steht zu einem etwa nachfolgenden Eingriff in das Postgeheimnis in keinem anderen Verhältnis, als dies bei der vorbereitenden Ermittlung der Rufnummer einer Person über § 112 TKG

in Bezug auf eine nachfolgende Telekommunikationsüberwachungsmaßnahme dar Fall ist.

- Eine ähnliche Regelungsstruktur findet sich auch in §§ 35, 36 StVG, § 12 FRV zum automatisierten Abruf aus dem Fahrzeugregister u.a. zu Zwecken der Gefahrenabwehr und Strafverfolgung; erneut etwa findet sich die Voraussetzung der Erforderlichkeit für die Aufgabenerfüllung der ersuchenden Stelle, erneut werden keine besonderen Mitteilungspflichten an den Betroffenen statuiert.

Der in §§ 111, 112 TKG geregelte automatisierte Zugriff auf Telekommunikationsbestandsdaten fügt sich in diese Linie bruchlos ein. Auch bei den nach § 111 TKG zu erhebenden Daten, die im Wesentlichen die Verknüpfung von Person und Rufnummer betreffen, geht es um ein grundlegendes Identifikationsmerkmal, das gerade in Zeiten der modernen elektronischen Kommunikationsformen demjenigen des Wohnsitzes (Melderegister) oder des Kraftfahrzeugs (Fahrzeugregister) an Bedeutung in keiner Weise nachsteht. So wie es beim Wohnsitz um die räumlichen Verortung und Auffindbarkeit einer Person geht, so wie die Fahrzeugdaten Auskunft über genutzte Kraftfahrzeuge geben, so geben die Telekommunikationsbestandsdaten darüber Auskunft, wie (d.h. unter welcher Rufnummer) der Einzelne mit seiner Umwelt kommuniziert und wie er fernmündlich erreichbar ist; die Telekommunikationsbestandsdaten betreffen gleichsam die telekommunikative Verortung des Einzelnen. Bezüglich aller drei Datensätze (Wohnsitz, Kraftfahrzeug, Rufnummer), die je auf ihre Weise die räumliche, verkehrsmäßige und telekommunikative Verortung und Erreichbarkeit einer Person betreffen, hat der Gesetzgeber in im Grunde vergleichbarer Weise die Entscheidung getroffen, dass es sich um Daten handelt, auf die die Sicherheitsbehörden nach Maßgabe der jeweiligen gesetzlichen Voraussetzungen sollen zugreifen dürfen, weil ohne derartige Befugnisse eine effektive staatliche Gefahrabwehr oder Strafverfolgung nicht möglich wäre.

Die jüngere Rechtsentwicklung hat der Liste der automatisierten Auskunftsverfahren noch ein weiteres hinzugefügt, den automatisierten Abruf von Kontoinformationen nach § 24c KWG, auch i. V. m. § 93 Abs. 7 AO.

## B) Zur Zulässigkeit der Verfassungsbeschwerde

Die Zulässigkeit der Verfassungsbeschwerde unterliegt, wie im Folgenden zu zeigen ist, in mehreren Punkten Zweifeln, besonders soweit die Verfassungswidrigkeit von § 95 Abs. 3 und 4 TKG gerügt wird.

### I. Sind die Beschwerdeführer durch §§ 112, 113 TKG selbst, gegenwärtig und unmittelbar betroffen?

Zweifelhaft ist zunächst, ob die Beschwerdeführer durch die das automatisierte und das manuelle Auskunftsverfahren regelnden §§ 112, 113 TKG – diese bilden den zentralen Verfahrensgegenstand – überhaupt selbst, gegenwärtig und unmittelbar betroffen sind.

Hierzu S. 7 der Beschwerdeschrift.

Die §§ 112, 113 TKG werden durch konkrete Vollzugsakte, nämlich entsprechende Auskunftersuchen von Sicherheitsbehörden im konkreten Einzelfall, ausgeführt. Er gibt sich die konkrete Betroffenheit somit erst aus der Anwendung eines Gesetzes, kann die Verfassungsbeschwerde – mangels unmittelbarer Beschwer – grundsätzlich nicht gegen das Gesetz, sondern nur gegen den Vollzugsakt gerichtet werden. Etwas anderes kann indes dann gelten, wenn der Betroffene keine Kenntnis von dem Vollzugsakt erlangt und daher auch nicht den Rechtsweg gegen ihn beschreiten kann. Dies ist auch dann der Fall, wenn eine nachträgliche Kenntniserlangung zwar möglich ist, aber aufgrund weitreichender Ausnahmetatbestände auch langfristig unterbleiben kann.

Hierzu und auch zum Folgenden: BVerfGE 100, 313/354; 109, 279/306 ff.; 113, 348/362 ff.

Das TKG selbst sieht, worauf die Beschwerdeführer hinweisen, keine Benachrichtigung oder Auskunftsansprüche vor. Dies indes kann nicht entscheidend sein, weil es nicht Aufgabe des TKG, sondern des jeweiligen Fachrechts der ersuchenden Behörde (StPO, Polizeigesetze, Verfassungsschutzgesetze etc.) ist, über die Fragen der Benachrichtigung und Auskunftsansprüche im Rechtsverhältnis zwischen Bürger und ersuchender Behörde zu bestimmen (das TKG regelt dieses Rechtsverhältnis nicht oder allenfalls sehr partiell, siehe dazu näher unten C.I.3. S. 39 ff.). Zu den Fragen der Unterrichtung nach dem jeweiligen Fachrecht jedoch enthält die Beschwerdeschrift keine Aussagen. Selbst jedoch wenn man unterstellt, dass auch nach diesen Fachgesetzen eine Unterrichtung nicht vorgesehen ist oder aufgrund entsprechender Ausnahmetatbestände unterbleiben kann, und wenn man insoweit ein Vorgehen unmittelbar gegen das Gesetz gestatten wollte, bleiben gewichtige Zweifel an der Zu-

lässigkeit im Übrigen. Denn neben der unmittelbaren Beschwer müsste der Beschwerdeführer gemäß § 90 Abs. 1, § 23 Abs. 1 S. 2, § 92 BVerfGG auch darlegen, dass er durch die Regelung selbst und gegenwärtig betroffen ist. Dies setzt nach den Kriterien des BVerfG eine Darlegung voraus, dass die Beschwerdeführer „mit einiger Wahrscheinlichkeit“ durch die auf den angegriffenen Normen beruhenden Maßnahmen in ihren Grundrechten berührt werden.

Zu den relevanten Kriterien: BVerfGE 113, 348/363 f.; zur Problematik siehe auch HessStGH NVwZ 2006, 685 ff.

Dass die Beschwerdeführer mit einiger Wahrscheinlichkeit Objekt einer automatisierten oder manuellen Bestandsdatenabfrage werden könnten, ist jedoch in keiner Weise dargelegt worden. Zwar sind an eine solche Darlegung geringere Anforderungen zu stellen, wenn Maßnahmen eine große Streubreite haben oder Dritte auch zufällig erfassen können und daher die Möglichkeit einer Betroffenheit gleichsam für jedermann besteht. So liegen die Dinge hier indes nicht. Automatisierte Auskunftersuchen mögen in großer Zahl vorkommen, sie betreffen jedoch stets einen konkreten Einzelfall (vgl. die Notwendigkeit der Protokollierung des Aktenzeichens in § 112 Abs. 4 S. 4 TKG) und haben dabei weder irgendeine Streubreite noch können Dritte zufällig erfasst werden (erfasst wird allein die zu einer Rufnummer gehörige Person oder umgekehrt). Dies mag bis zu einem gewissen Grade anders werden, wenn die nunmehr vorgesehene Möglichkeit der unvollständigen Dateneingabe und der Ähnlichkeitenfunktion (§ 112 Abs. 1 S. 4 TKG) einmal rechtlich und praktisch realisiert sein wird. Dies ist aber gegenwärtig – mangels Rechtsverordnung und Technischer Richtlinie nach § 112 Abs. 3 TKG – noch nicht der Fall, so dass gerade noch keine gegenwärtige Betroffenheit gegeben ist. Außerdem wird die Rechtsverordnung, in der eingrenzende Merkmale zu bestimmen sein werden, die Streubreite und mögliche Zufallsbetroffenheit Dritter erheblich einschränken.

Vgl. z.B. § 8 ZStVBetrV vom 23.9.2005 (BGBl. I S. 2885), der einen gewissen Anhaltspunkt gibt, wie die von der Rechtsverordnung nach § 112 Abs. 3 TKG zu leistende Eingrenzung in etwa aussehen könnte.

In jedem Fall wird somit die mögliche Streubreite beispielsweise weit entfernt sein von einer Art „Rasterung“, und selbst bei dieser wäre, wie die oben zitierte Entscheidung des HessStGH zeigt, die Bejahung einer gegenwärtigen Selbstbetroffenheit alles andere als selbstverständlich (die gegenwärtige Selbstbetroffenheit wurde dort bzgl. einer Norm zur Rasterfahndung verneint). Erst recht fehlt es bzgl. § 113 TKG an der substantiierten Darlegung einer gegenwärtigen Selbstbetroffenheit; hier ist noch deutlicher als bei § 112 TKG, dass die Anfrage allein „im Einzelfall“ erfolgt (so ausdrücklich § 113 Abs. 1 S. 1 TKG) und hierbei keinerlei Streubreite oder zufällige Drittbetroffenheit auslöst.

## II. Weitere Probleme der Beschwerdebefugnis, insbesondere zur Unzulässigkeit der Rügen gegen § 95 Abs. 3 und 4 TKG

Auch ansonsten ist fraglich, ob die Beschwerdeführer ihre Beschwer und die Möglichkeit einer Grundrechtsverletzung in allen Punkten hinreichend dargetan haben:

- So sind, was die Pflicht zur Erhebung und Speicherung von Bestandsdaten nach § 111 TKG betrifft, die Auswirkungen der Richtlinie zur sog. Vorratsdatenspeicherung vom 15.3.2006 (Richtlinie 2006/24/EG, ABl. Nr. L 105/54) nicht bedacht worden. Zwar geht die Speicherungspflicht nach § 111 TKG sowohl nach ihren Zweckrichtungen (die Bestandsdaten dienen zwar auch, aber keineswegs nur der Vor- oder Nachbereitung von Verkehrsdatenerhebungen, siehe oben A.II. S. 7 ff., während die „Vorratsdatenspeicherungsrichtlinie“ die Vorhaltung von Bestandsdaten nur im Zusammenhang mit ihrerseits vorzuhaltenden Verkehrsdaten verlangt) als auch hinsichtlich der Anzahl der zu speichernden Datenarten (nicht nur Name und Anschrift) als auch hinsichtlich der Speicherdauer (bis ein Jahr nach Vertragsende) über die Mindestanforderungen der Richtlinie hinaus. Dies ändert jedoch nichts daran, dass die Grundentscheidung, dass die wesentlichen Bestandsdaten zu Zwecken der Strafverfolgung „auf Vorrat“ gespeichert werden müssen, nunmehr gemeinschaftsrechtlich zwingend vorgegeben ist. Die wesentliche Substanz des von § 111 TKG geregelten Grundrechtseingriffs ist nunmehr gemeinschaftsrechtlich determiniert; nur in Details (hinsichtlich zu speichernder Datenarten, Speicherdauer und zusätzlicher Speicherungszwecke) kann das deutsche Gesetz eigenständige Regelungskraft entfalten. Im Maße der gemeinschaftsrechtlichen Determiniertheit können indes wegen des grundsätzlichen Anwendungsvorrangs des Gemeinschaftsrechts deutsche Grundrechte als Prüfungsmaßstab nicht mehr in Betracht kommen bzw. jedenfalls keine die Geltung der Norm in Frage stellende Kraft mehr entfalten (eine Prüfung und Bestätigung, dass die Regelung auch mit dem Grundgesetz übereinstimmt, bleibt natürlich unbenommen), es sei denn, es würde dargelegt, der europäische Grundrechtsschutz sei unter das vom Grundgesetz verlangte Mindestmaß wesentlicher Vergleichbarkeit herabgesunken. Hiervon kann keine Rede sein; hierzu ist vor allem nichts vorgetragen worden.

BVerfGE 95, 173/181; 102, 147/164.

- Hinsichtlich §§ 112, 113 TKG übersieht die Beschwerdeschrift, dass die geltend gemachte Beschwer zu einem Großteil gar nicht von §§ 112, 113 TKG ausgeht, sondern sich allenfalls aus dem jeweils anwendbaren Fachrecht (StPO, Polizeirecht

etc.) ergibt (näher dazu in der Begründetheit, C.I.3., S. 39 ff.). Der gegen die §§ 112, 113 TKG gerichtete Angriff geht damit im Kern fehl.

- Was den Angriff gegen Auskunftersuchen mittels unvollständigen Anfragedaten oder mittels Ähnlichenfunktion (§ 112 Abs. 1 S. 4 TKG) anbelangt, so ist bereits darauf hingewiesen worden, dass diese – mangels Rechtsverordnung und Technischer Richtlinie nach § 112 Abs. 3 TKG – derzeit noch gar nicht praktiziert werden können. Eine gegenwärtige Beschwer liegt demnach nicht vor.

- Unzulässig ist die Rüge bzgl. § 95 Abs. 3 TKG. Dieser regelt ausschließlich die Reichweite des Rechts der Diensteanbieter, Bestandsdaten über das Vertragsende hinaus zu speichern; eine entsprechende Pflicht begründet er nicht. Diese ergibt sich vielmehr allein aus § 111 Abs. 1 S. 4 TKG.

BerIKommTKG/Kleszczewski, 2006, § 95, Rdnr. 16; § 111, Rdnr. 23.

Die Beschwerdeschrift (S. 96 f.) prüft § 95 Abs. 3 und § 111 Abs. 1 S. 4 TKG in einem Zug. Hierbei kann sie nicht plausibel darlegen; inwieweit aus § 95 Abs. 3 TKG, was die gerügte Speicherungspflicht anbelangt, gegenüber § 111 Abs. 1 S. 4 TKG eine selbständige Beschwer folgen soll. Da es bei § 95 Abs. 3 TKG allein um die Reichweite von Rechten privater Unternehmen (die selbst nicht unmittelbar grundrechtsgebunden sind) gegenüber ihren Kunden geht, steht bei ihm die Dimension eines Eingriffs in Grundrechte als Abwehrrechte gegen den Staat überhaupt nicht zur Debatte.

Falsch daher in anderem Kontext auch die Ausführungen der Beschwerdeschrift auf S. 18 ff.

Wenn überhaupt, könnte bzgl. § 95 Abs. 3 TKG allenfalls gerügt werden, der Staat habe durch Zulassung einer maximalen Speicherdauer von einem Jahr seine grundrechtliche Schutzpflicht gegenüber den Kunden (d.h. seine Pflicht, sie datenschutzrechtlich gegen übermäßige Datenspeicherung der Unternehmen zu schützen) verletzt. Die Schutzpflichtdimension der Grundrechte steht freilich nicht im Zeichen des Übermaßverbotes, d.h. der Gesetzgeber ist nicht verpflichtet, private „Eingriffe“ in das Recht auf informationelle Selbstbestimmung auf ein Minimum zu begrenzen und ein Maximum an Datenschutz zu gewährleisten. Maßgebend ist umgekehrt ein bloßes Untermaßverbot; ein hinreichendes Minimum an Datenschutz gegenüber anderen Privaten muss gewährleistet sein. Noch zurückhaltender hat das Bundesverfassungsgericht sogar formuliert, gesetzgeberische Schutzpflichten seien nur verletzt, wenn der Gesetzgeber entweder völlig untätig geblieben sei oder aber seine Schutzmaßnahmen offensichtlich völlig ungeeignet oder unzulänglich seien.

BVerfGE 77, 170/215; BVerfG NJW 1996, 651; dazu auch Möstl, DÖV 1998, 1029/1037 f.

Legt man diese Maßstäbe zugrunde, kann es als ausgeschlossen bezeichnet werden, dass die ausdrückliche Statuierung einer einjährigen Maximalfrist für Datenspeicherungen, die privaten Datensammlungen eine wirksame zeitliche Grenze setzt, gegen grundrechtliche Schutzpflichten verstößt. Eine Beschwerdebefugnis liegt insoweit nicht vor. Zumindest aber sind die Anforderungen verletzt, die an die hinreichende Substantiierung der geltend gemachten Grundrechtsverletzung zu stellen sind (§ 90 Abs. 1, § 23 Abs. 1 S. 2, § 92 BVerfGG). Die Beschwerdeführer sind auf die Frage einer Schutzpflichtverletzung nicht einmal eingegangen; ihr Vortrag bleibt damit weit hinter den Anforderungen des Bundesverfassungsgerichts zurück.

BVerfGE 77, 170/215; dazu Möstl, DÖV 1998, 1029/1032.

- Unzulässig ist die Verfassungsbeschwerde auch, falls und soweit sie sich gegen § 95 Abs. 4 TKG richtet. § 95 Abs. 4 TKG regelt im Wesentlichen, dass Diensteanbieter bei Vertragsschluss die Vorlage eines amtlichen Ausweises verlangen können (aber nicht müssen!). Hierbei ist im Ausgangspunkt schon fraglich, ob die Beschwerdeführer ihre Verfassungsbeschwerde überhaupt gegen § 95 Abs. 4 TKG richten wollten. Bei der Bezeichnung der Verfassungsbeschwerde auf S. 1 des Schriftsatzes taucht § 95 Abs. 4 TKG jedenfalls nicht auf, bei der Formulierung des Antrags auf S. 2 dann aber schon. Ob dies bewusst geschah oder hier (auf S. 2) ein Schreibfehler vorliegt (gemeint sein könnte, so wie auf S. 95 f. des Schriftsatzes, § 95 Abs. 3 und § 111 Abs. 1 S. 4 [statt und Abs. 4]; dagegen spricht andererseits, dass § 111 TKG ohnehin Beschwerdegegenstand ist), bleibt unklar. Beim Inhaltsverzeichnis zu den Gründen auf S. 3 f. taucht § 95 Abs. 4 sodann wiederum nicht unter den Beschwerdegegenständen auf. Auch im Text selbst wird § 95 Abs. 4 nicht als selbständiger Beschwerdegegenstand behandelt. Thematisch wird er zweimal – jedoch ohne ausdrückliche Nennung (einmal wird die entsprechende Regelung des Gesetzentwurfs zitiert) – gestreift, nämlich auf S. 28 und auf S. 55, wo jeweils moniert wird, die erhobenen Bestandsdaten seien nicht verlässlich, wenn es den Anbietern überlassen bleibe, ob sie sich einen amtlichen Ausweis vorzeigen ließen. Moniert wird also, die Norm sei nicht streng genug, indem sie die Diensteanbieter nicht verpflichte, die personenbezogenen Daten zu verifizieren. Dies wäre als selbständige Rüge nur schwer verständlich, weil in der Sache ein Mehr an Eingriff in das Recht auf informationelle Selbstbestimmung gefordert würde. Näher liegt es hier schon, dass die Verfassungsbeschwerde § 95 Abs. 4 TKG nicht selbständig angreifen will, sondern ihm allein im Rahmen der Geeignetheit und Verhältnismäßigkeit der hauptsächlich gerügten §§ 111 ff. TKG angesprochen wissen will – mit der Stoßrichtung näm-

lich, dass infolge der nicht verifizierten Datenerhebung die Eignung der Bestandsdatenspeicherung und -abfrage für die Zwecke der Sicherheitsbehörden geschmälert sein könnte. Richtigerweise dürfte sich die Verfassungsbeschwerde nach alledem nicht unmittelbar gegen § 95 Abs. 4 TKG richten, auch wenn dieser vom Bundesverfassungsgericht in der Nichtannahmeentscheidung vom 21.6.2006 sowie im Zustellungsschreiben vom 10.7.2006 jeweils unter den Gegenständen der Verfassungsbeschwerde mit aufgeführt wurde. Sollte ein Angriff auf § 95 Abs. 4 TKG dagegen wirklich gewollt sein, so müsste die entsprechende Rüge als unzulässig angesehen werden. Denn es fehlt in der Beschwerde an jeglichem verwertbaren Vortrag zu dieser Norm – es sei denn die Einlassung, § 95 Abs. 4 TKG solle tiefer in das Recht auf informationelle Selbstbestimmung eingreifen, was indes keine plausible Geltendmachung einer Grundrechtsverletzung darstellt. § 90 Abs. 1, § 23 Abs. 1 S. 2, § 92 BVerfGG ist somit nicht genüge getan. Theoretisch wäre es vielleicht möglich gewesen – hierfür finden sich jedoch keinerlei Anhaltspunkt im Text – zu rügen, dass § 95 Abs. 4 TKG, indem er es den (selbst nicht grundrechtsverpflichteten) Diensteanbietern erlaube, den Ausweis zu verlangen, so wie bereits bei § 95 Abs. 3 TKG besprochen, den Kunden nicht hinreichend vor der Erhebung personenbezogener Daten durch die Diensteanbieter schütze und so eine grundrechtliche Schutzpflicht verletze. Angesichts der berechtigten Interessen der Diensteanbieter, die Identität ihrer Vertragspartner zu kennen, scheint die Möglichkeit einer derartigen Grundrechtsverletzung hingegen als von vornherein ausgeschlossen, so dass eine derartige Rüge – für die der Text der Verfassungsbeschwerde, wie gesagt, nichts hergibt – ihrerseits als wegen fehlender Beschwerdebefugnis unzulässig angesehen werden müsste, ganz abgesehen davon, dass erneut die aus § 90 Abs. 1, § 23 Abs. 1 S. 2, § 93 BVerfGG folgenden Substantiierungspflichten verletzt wären.

### III. Subsidiarität der Verfassungsbeschwerde

Zweifel an der Zulässigkeit der Verfassungsbeschwerde ergeben sich schließlich auch, was die zu fordernde Subsidiarität der Verfassungsbeschwerde anbelangt. Nach dem Maßstab, den auch die 1. Kammer des Ersten Senats in ihrem die vorliegende Verfassungsbeschwerde teilweise nicht zur Entscheidung annehmenden Beschluss vom 21. Juni 2006 zur Anwendung gebracht hat, ist in Verfassungsbeschwerden gegen Gesetze hinreichend substantiiert darzulegen, dass es den Beschwerdeführern unmöglich oder unzumutbar wäre, sich gegen die auf der Grundlage der angegriffenen Normen ergehenden Maßnahmen fachgerichtlich zu wehren (S. 3 f. des Beschlusses). Dies haben die Beschwerdeführer – nicht nur in Bezug auf die nicht zur Entscheidung angenommenen Beschwerdegegenstände, sondern auch in Bezug auf die §§ 111 ff. TKG – nicht getan:

- Was die Erhebungs- und Speicherungspflicht in § 111 TKG anbetrifft, so scheint es nicht ausgeschlossen, dass nicht zumindest indirekt – etwa in einem Rechtsstreit des Kunden gegen den die Daten erhebenden und speichernden Diensteanbieter – die angebliche Verfassungswidrigkeit dieser Norm hätte geltend gemacht werden können.

- Was §§ 112, 113 TKG angeht, wird zwar vorgebracht, die Beschwerdeführer würden über Bestandsdatenabfragen nicht benachrichtigt. Denkbar wäre jedoch, dass diese einen Anspruch auf Auskunft über Bestandsdatenabfragen geltend machen könnten, um dann – nach Auskunftserteilung – gegebenenfalls Rechtsschutz vor den Fachgerichten zu suchen. Dies gilt zum einen gegenüber den Akteuren, die im TKG näher geregelt sind: So erscheint es z.B. nicht als völlig ausgeschlossen, dass etwa gegen die Bundesnetzagentur Auskunftsansprüche bestehen könnten; § 112 Abs. 4 S. 5 TKG könnte dem zwar entgegenstehen, andererseits schließt § 19 Abs. 2 BDSG Auskunftsansprüche auch bzgl. nur für Zwecke der Datenschutzkontrolle gespeicherter Daten nicht kategorisch aus. Und auch dass über den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, an den man sich nach bei Ablehnung der Auskunftserteilung ggf. wenden kann (§ 19 Abs. 5 BDSG), vielleicht Informationen erlangt werden könnten, die dann in einen fachgerichtlichen Rechtsschutz führen, scheint nicht von vornherein ausgeschlossen. Wichtiger ist jedoch etwas Anderes: Die Frage, inwieweit Auskunftsansprüche über Bestandsdatenabfragen nach §§ 112, 113 TKG bestehen, ist nicht in erster Linie eine Frage, die im TKG geregelt werden müsste, sondern eine Frage, die zuallererst vom Gesetzgeber des jeweiligen für die ersuchende Sicherheitsbehörde geltenden Fachgesetzes (StPO, Polizeigesetz, Verfassungsschutzgesetze etc.) geregelt werden muss und, da die Abwägung zwischen Offenlegungs- und Geheimhaltungsinteresse in jedem Rechtsgebiet unterschiedlich ausfällt, auch nur von ihm sinnvoll getroffen werden kann. Die einschlägigen Fachgesetze (z.B. die Polizeigesetze) enthalten entsprechende Auskunftsansprüche auch, ebenso wie eine genaue Regelungen der Gründe, die zur Auskunftsverweigerung berechtigen. Die Beschwerdeführer haben nicht dargelegt, weshalb im Falle des Verdachts der missbräuchlichen Anwendung der §§ 112, 113 TKG durch eine Behörde effektiver Rechtsschutz über diese fachgesetzlichen Auskunftsansprüche nicht möglich sein soll.

Teilergebnis: Die Verfassungsbeschwerde ist jedenfalls unzulässig, soweit sie sich gegen § 95 Abs. 3 und Abs. 4 TKG richtet. Ansonsten – soweit §§ 111 bis 113 TKG angegriffen werden – unterliegt die Zulässigkeit der Verfassungsbeschwerde in mehreren Punkten zumindest Zweifeln.

## C) Zur Begründetheit der Verfassungsbeschwerde

### I. Übergreifende Fragestellungen

1. *Berührt ist nicht das Fernmeldegeheimnis (Art. 10 GG), sondern allein das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG)*

Die Argumentation der Beschwerdeführer ist von der zentralen Weichenstellung geprägt, die von ihnen gerügten Normen berührten den Schutzbereich des Fernmeldegeheimnisses (Art. 10 GG); nur hilfsweise wird auf das Recht auf informationelle Selbstbestimmung abgestellt.

Für § 111 TKG: Beschwerdeschrift, S. 51, 55; für §§ 112, 113 TKG: S. 79, 85; begründet wird die angebliche Einschlägigkeit von Art. 10 GG auf S. 9 ff.; in diesem Sinne auch Breyer, RDV 2003, S. 218 f.

Gerade diese zentrale Weichenstellung ist indes, wie im Folgenden zu zeigen sein wird, unzutreffend. Die in den §§ 111 ff. TKG geregelte Vorhaltung und Abrufbarkeit von Bestandsdaten berührt allein das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG), nicht jedoch den Schutzbereich des Fernmeldegeheimnisses (Art. 10 GG).

Dass durch die §§ 111 ff. TKG nicht Art. 10 GG, sondern allein Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG berührt ist, entspricht zunächst der eindeutigen Einschätzung des Gesetzgebers. Denn dass – im Blick auf das Zitiergebot des Art. 19 Abs. 1 S. 2 GG – Art. 10 GG vom Gesetzgeber nicht als durch die §§ 111 ff. TKG eingeschränktes Grundrecht genannt wird, ist ja nicht etwa Konsequenz einer Nachlässigkeit, sondern kann nur als eindeutiger Ausdruck der Einschätzung des Gesetzgebers gedeutet werden, dass Art. 10 GG durch diese Normen eben nicht berührt ist. Dass dies so ist, kommt im Gesetz überdies noch in einer weiteren Hinsicht explizit und unzweideutig zum Ausdruck: Dadurch nämlich, dass der Gesetzgeber in Satz 3 des § 113 Abs. 1 TKG – hier geht es teilweise um intensivere Eingriffe als bei § 112 TKG (z.B. Zugriff auf PIN und PUK), bei denen zum Teil auch streitig war, ob Art. 10 GG erfasst sein könnte –

BT-Drucks. 15/2316, S. 97.

klar geregelt hat, dass Eingriffe in das Fernmeldegeheimnis nur unter den Voraussetzungen der hierfür einschlägigen Vorschriften zulässig sind. Durch diese Klarstellung kommt im Umkehrschluss eindeutig zum Ausdruck, dass auf der Basis des § 113 TKG (gleiches gilt für den eher weniger eingriffsintensiven § 112 TKG) Eingriffe

in das Fernmeldegeheimnis gerade nicht zulässig sein sollen. Deutlich wird, dass der Gesetzgeber davon ausgeht, dass der in §§ 112, 113 TKG geregelte Zugriff auf Bestandsdaten das Fernmeldegeheimnis weder im Allgemeinen noch im Besonderen (unmittelbar vor § 113 Abs. 1 Satz 3 TKG geregelten) Fall des Zugriffs auf PIN und PUK berührt. Zugleich wird – gleichsam vorsorglich – deutlich gemacht, dass, sollte es irgendwelche Grenz- und Streitfälle geben, bei denen der Zugriff auf bestimmte Daten vielleicht doch als Eingriff in Art. 10 GG gewertet werden müsste, dieser Eingriff jedenfalls nicht auf der Basis von § 113 TKG zulässig sein soll; § 113 TKG wäre dann so auszulegen, dass das betreffende – dem Art. 10 GG unterfallende – Datum eben kein nach § 113 TKG abfragbares Bestandsdatum i. S. v. §§ 95, 111 TKG ist.

Relevant sein könnte dies beispielsweise bei der Frage, ob die Auskunft darüber, welcher Nutzer sich hinter einer dynamischen IP-Adresse verbirgt, von § 113 TKG erfasst wird oder nicht (siehe unten S. 36). Selbst wenn bei einer derartigen Abfrage Art. 10 GG berührt sein sollte, so folgte hieraus nicht etwa die teilweise Verfassungswidrigkeit von § 113 TKG; vielmehr wäre er dann eben – verfassungskonform und im Lichte der Klarstellung des § 113 Abs. 1 S. 3 TKG – so auszulegen, dass ihm die betreffende Auskunft nicht unterfällt. Etwaige Streitfragen im Grenzbereich von Bestands- und Verkehrsdaten sind damit keine Fragen zur Verfassungskonformität des § 113 TKG, die in diesem Verfahren geklärt werden müssten; sie sind vielmehr eine Frage der richtigen Auslegung und Anwendung des § 113 TKG, zu der zunächst die Fachgerichte berufen sind.

Mit seiner Einschätzung, die Speicherung und der Abruf von Bestandsdaten nach §§ 111 ff. TKG berühre allein das Recht auf informationelle Selbstbestimmung, nicht jedoch das Fernmeldegeheimnis, bewegt sich der Gesetzgeber sowohl auf dem gesicherten Terrain der von der Rechtsprechung (z.B. des BVerwG) eingeschlagenen Linie als auch im Einklang mit der in der Literatur klar überwiegenden Ansicht.

Zur Rspr.: BVerwGE 119, 123/126; OVG Münster MMR 2002, 563/564; für IP-Adressen: LG Hamburg, CR 2005, 832 ff.; LG Stuttgart, CR 2005, 598 f.; LG Würzburg, NStZ-RR 2006, 46 f. (auch die Gegenansicht des LG Bonn im Beschluss vom 21.5.2004, 31 Qs 65/04 behauptet keineswegs, dass der Zugriff auf Bestandsdaten Art. 10 GG unterfällt; vertreten wird vielmehr allein, die Verknüpfung von dynamischer IP-Adresse und hinter ihr stehender Person sei überhaupt kein Bestands-, sondern ein Verkehrsdatum, so dass bereits aus diesem Grund § 113 TKG nicht einschlägig sein kann).

Aus der Literatur: BerlKommTKG/Kleszczewski, 2006, § 111, Rn. 7; § 112, Rn. 3, § 113, Rn. 8; Trute, Trute/Spoerr/Bosch, TKG, 2001, § 89, Rn. 53; Thiede, Kriminalistik 2004, 104/107.

Die von den Beschwerdeführern in der Beschwerdeschrift und vom Beschwerdeführer zu 1) auch andernorts (RDV 2003, 218 f.) vertretene Ansicht, Bestandsdaten un-

terfielen grundsätzlich und in prinzipiell gleicher Weise wie Verkehrsdaten dem Schutzbereich des Art. 10 GG, ist, soweit ersichtlich, eine Einzelmeinung geblieben.

Die dahingehende Aussage von Bizer, in Alternativkommentar, GG, 3. Aufl. Art. 10, Rn. 66 bleibt ohne nähere Begründung und ist in ihrer Tragweite daher schwer einzuschätzen; Ähnliches gilt für die Stellungnahme von Simitis, in Deutscher Bundestag, Ausschussdrucksache 15 (9) 969, S. 225 f.

Eher schon findet sich der Versuch, besondere Konstellationen und Verwendungszusammenhänge zu identifizieren, in denen der Zugriff auf Bestandsdaten ausnahmsweise dem Art. 10 GG unterfallen soll. Dass Bestandsdaten nicht als solche und grundsätzlich von Art. 10 GG erfasst werden, wird von dieser Ansicht nicht abgestritten (näher hierzu siehe unten).

Neumann/Wolff, TKMR 2003, 110/113 f.; Kühling, K&R 2004, 105/107 f. (ausdrücklich ablehnend bzgl. der vom Beschwerdeführer zu 1) befürworteten pauschalen Gleichsetzung von Bestands- und Verkehrsdaten).

Die von Gesetzgeber, Rechtsprechung und herrschender Meinung zugrunde gelegte Ansicht, dass Maßnahmen der Bestandsdatenspeicherung und -abfrage nach §§ 111 ff. TKG nicht das Fernmeldegeheimnis des Art. 10 GG berühren, ist zutreffend. Das Bundesverfassungsgericht hat – in anderem Zusammenhang – in jüngster Zeit wiederholt Gelegenheit gehabt, den spezifischen Schutzbereich des Art. 10 GG in seiner Abgrenzung zur allgemeinen Gewährleistung des Rechts auf informationelle Selbstbestimmung näher zu konkretisieren.

BVerfG, Urteil vom 2.3.2006 – 2 BvR 2099/04 (Sicherstellung von Mobiltelefonen und Computerfestplatten und Auswertung der auf ihnen gespeicherten Verkehrsdaten); BVerfG, Kammerbeschluss vom 22.8.2006 – 2 BvR 1345/03 (IMSI-Catcher).

Legt man diese Maßstäbe zugrunde, so ist Art. 10 GG im vorliegenden Fall nicht berührt. Maßgeblich sind zwei Gründe:

Erstens: Art. 10 GG schützt in erster Linie die Vertraulichkeit des Kommunikationsinhalts. Darüber hinaus wird jedoch auch die Vertraulichkeit der näheren Umstände eines Kommunikationsvorgangs geschützt, denn auch die Kenntnis von Häufigkeit, Dauer und Zeitpunkt von Kommunikationsvorgängen gibt Hinweise auf Art und Intensität von Beziehungen und ermöglicht auf den Inhalt bezogene Schlussfolgerungen. Es ist daher völlig unumstritten, dass der Zugriff auf die Verkehrsdaten (§ 3 Nr. 30 TKG), die anlässlich eines konkreten Kommunikationsvorgangs – als digitale Spuren – erhoben und gespeichert werden und Aufschluss über die Umstände dieses konkreten Kommunikationsvorgangs geben können, grundsätzlich (d.h. jedenfalls bei

einem Zugriff beim Diensteanbieter, nicht bei im Herrschaftsbereich des Empfängers gespeicherten Daten, siehe dazu sogleich) dem Fernmeldegeheimnis unterfallen. Um solche Verkehrsdaten geht es bei den §§ 111 ff. TKG indes gerade nicht; vielmehr geht es allein um sog. Bestandsdaten im Sinne des § 3 Nr. 3 TKG, d.h. um Daten eines Teilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste vom Diensteanbieter erhoben werden. Bestandsdaten betreffen daher nicht einen konkreten Kommunikationsvorgang, sondern lediglich die vertraglichen Rahmenbedingungen für die Nutzung eines Telekommunikationsdienstes.

BerIKommTKG/Säcker, 2006, § 3, Rn. 5.

Damit fehlt Bestandsdaten freilich der für Art. 10 GG entscheidende Bezug zu einem konkreten Kommunikationsvorgang.

BerIKommTKG/Kleszczewski, 2006, § 112, Rn. 3.

Aus Bestandsdaten kann allein erschlossen werden, dass jemand überhaupt – abstrakt – die Möglichkeit hat, mittels eines bestimmten Telekommunikationsdienstes in konkrete Kommunikationsvorgänge einzutreten. Dies ist jedoch eine so unspezifische Information, dass der spezifische – letztlich vom Schluss auf den Inhalt eines konkreten Kommunikationsvorgangs herkommende – Schutzzweck des Art. 10 GG hierdurch nicht berührt ist.

Kühling, K&R 2004, 105/107.

Sehr deutlich lässt sich dieses Ergebnis auch im Vergleich mit der kürzlich ergangenen IMSI-Catcher-Entscheidung des Bundesverfassungsgerichts herausarbeiten.

BVerfG, Kammerbeschluss vom 22.8.2006 – 2 BvR 1345/03, Abs. 55 ff.

Dort ist – zu Recht – sogar die Ausforschung des konkreten Bereitschaftszustands eines Mobiltelefons, der die bloße Voraussetzung für einzelne Kommunikationsvorgänge darstellt, nicht jedoch selbst im Zusammenhang mit einem solchen konkreten Kommunikationsvorgang steht, nicht als Eingriff in Art. 10 GG gewertet worden. Wenn aber selbst „die Ausforschung der Kommunikationsbereitschaft“, die sich in einem in der konkreten Situation eingeschalteten Mobiltelefon manifestiert, (konkrete Kommunikationsbereitschaft) als nicht Art. 10 GG-relevant angesehen wird, um wie viel weniger noch wird Art. 10 GG durch eine Ausforschung der abstrakten Kommunikationsbereitschaft und -möglichkeit berührt, die sich allein dadurch manifestiert, dass es überhaupt zu einem Vertragsschluss über Telekommunikationsdienstleistungen gekommen ist (dass also jemand z.B. überhaupt einen Vertrag über einen Mobiltelefonanschluss abgeschlossen hat), wie dies bei einem Abruf von Bestandsdaten

der Fall ist! Ein bloßes „Für-möglich-halten“ von Kommunikation stellt, wie das BVerfG formuliert, noch keine solche dar.

Hinzu kommt ein Zweites: Selbst soweit bestimmte Daten (wie z.B. Verkehrsdaten) ihrer Art nach dem Art. 10 GG unterfallen können, schützt Art. 10 GG doch nicht gegen jede Form von Kenntnisnahme dieser Daten, sondern nur gegen solche Formen der Kenntnisnahme, in der sich die spezifischen Risiken der Einschaltung eines technischen Kommunikationsmittlers ergeben. Abgesehen vom eigentlichen Gesprächsinhalt sind es – im Zeitalter der Digitalisierung – vor allem jene digitalen Spuren eines konkreten Kommunikationsvorgangs, die anlässlich dieses Vorgangs beim Telekommunikationsunternehmen anfallen und dort gespeichert werden, deren Vertraulichkeit Art. 10 GG schützen möchte; denn gerade hier realisiert sich das spezifische Risiko einer über ein Telekommunikationsunternehmen technisch vermittelten Kommunikation; Art. 10 GG geht es um die Kompensation des technisch bedingten Verlusts an Privatsphäre, der sich aus der Einschaltung eines Telekommunikationsunternehmens ergibt. Anders liegen die Dinge, wenn es um Daten geht (und seien es auch Verkehrsdaten), die nicht beim Telekommunikationsunternehmen erhoben werden, sondern im Herrschaftsbereich des Kommunikationsteilnehmers selbst (z.B. auf einem Mobilfunkgerät gespeicherte Verkehrsdaten); dies hat das Urteil des Bundesverfassungsgerichts vom 2.3.2006 zu Recht klargestellt.

BVerfG, Urteil vom 2.3.2006 – 2 BvR 2099/04, v.a. Abs. 72 ff.; ähnlich auch der Kammerbeschluss IMSI-Catcher (vom 22.8.2006 – 2 BvR 1345/03), wo unter anderem auch darauf abgestellt wurde, dass die Daten gerade nicht im Herrschaftsbereich eines Telekommunikationsunternehmens erhoben wurden (Abs. 62). Ähnlich wäre es z.B. auch schon immer gewesen, wenn eine Behörde etwa über Zeugenaussagen erfährt, dass jemand zu einem bestimmten Zeitpunkt mit einem anderen telefoniert hat; auch hier realisieren sich keine Gefahren technisch vermittelter Fernkommunikation, weil man über ein unmittelbares Gespräch genauso über Zeugenaussagen Aufschluss erhalten kann.

Die Bestandsdaten, um die es bei §§ 111 ff. TKG geht, werden zwar im Herrschaftsbereich des Telekommunikationsunternehmens gespeichert, sie sind jedoch in keiner Weise Ausdruck der spezifischen Gefahren, die aus dem technischen Vorgang einer durch einen Kommunikationsmittler vermittelten Kommunikation erwachsen. Die Vertragsdaten müssen nach § 111 TKG ausdrücklich vor der Freischaltung erhoben werden. Die Pflicht zur Führung der Datenbank liegt damit im Vorfeld der erst später möglichen einzelnen Kommunikationsvorgänge; er steht in keinem Zusammenhang mit den technischen Risiken, die sich aus der Vermittlung einzelner Gespräche ergeben.

OVG Münster MMR 2004, 563/564.

Denn Bestandsdaten sind definitionsgemäß ja gerade keine Daten, die anlässlich des einzelnen Kommunikationsvorgangs anfallen, sondern Daten betreffend den Vertragsschluss. Ihre Schutzwürdigkeit wird von Art. 10 GG genauso wenig erfasst, wie dies bei der Speicherung irgendeines anderen Vertragsdatums in einer anderen Branche der Fall wäre.

Die Argumente, die die Beschwerdeführer auf den S. 9 ff. ihres Schriftsatzes für die Gleichsetzung von Bestands- und Verkehrsdaten, d.h. für eine Unterschützstellung auch von Bestandsdaten unter Art. 10 GG anführen, sind demgegenüber nicht überzeugend:

Dies gilt zum einen für die ausdrücklich angeführten (Beschwerdeschrift S. 10 f.) Beispiele vermeintlich besonders brisanter Bestandsdaten, die Rückschlüsse auf konkrete Gesprächsinhalte erlauben sollen. Fehl geht zunächst das Beispiel der Teilnahme an Meinungsforen oder der Mitgliedschaft in einer Aids-Selbsthilfegruppe: Denn es erscheint äußerst unplausibel, dass diese Chat-Foren Rufnummern oder IP-Adressen vergeben; mittels bloßer Bestandsdaten ist es demnach unmöglich, eine derartige Teilnahme zu ermitteln; hierzu bedarf es vielmehr des Zugriffs auf Verkehrsdaten.

So zu Recht Kühling, K&R 2004, 105/107, Fn. 20.

Ein Vertragsverhältnis mit einer ausländischen Telefongesellschaft dürfte bei der Internationalisierung des heutigen Telekommunikationsmarktes für sich genommen keinen besonderen Aussagegehalt haben (nicht einmal den einer besonderen Beziehung zu dem jeweiligen Land), schon gar nicht erlaubt es irgendeinen Rückschluss auf Gesprächsinhalte und -umstände. Gleiches gilt für die Tatsache einer Flatrate, die allenfalls (auch das ist bei der heutigen Üblichkeit von Flatrates keineswegs sicher) die Bereitschaft zu einer intensivierten Nutzung signalisiert; die Ausforschung bloßer Telekommunikationsbereitschaften reicht nach der IMSI-Catcher-Entscheidung indes gerade nicht.

BVerfG, Kammerbeschluss vom 22.8.2006 – 2 BvR 1345/03, Abs. 61.

Dies ist auch der Grund, warum es keinen Eingriff in Art. 10 GG darstellt, wenn über eine Bestandsdatenabfrage etwa herausgefunden werden sollte, dass der Teilnehmer mit fünf Rufnummern verbilligt telefonieren kann. Auch diese Tatsache signalisiert eine bloße Telekommunikationsbereitschaft und lässt keine Rückschlüsse auf die näheren Umstände oder gar Inhalte konkreter Gespräche zu. Überdies geht es um Daten, die bei Vertragsschluss erhoben werden und keinerlei Bezug zu den spezifischen Risiken einer technisch vermittelten Kommunikation haben; ihr Aussagege-

halt ist kein anderer, als wenn man beispielsweise über eine Zeugenaussage erfährt, dass jemand häufiger Telefonkontakt mit einer anderen Person hat: Auch dies aber wäre kein Eingriff in Art. 10 GG. Nichts anderes gilt schließlich, wenn sich im Rahmen von § 113 TKG die Zugehörigkeit zu einem geschlossenen Netz (Unternehmen, Universität, Krankenhaus, Hotel etc.) ergibt; auch hier kann allenfalls auf bestimmte Lebensumstände (die indes zumeist bereits bekannt sein werden und jedenfalls auch auf andere, einfachere Weise ermittelbar wären; zu der Praxisfremdheit des Einwands siehe bereits oben S. 11), nicht jedoch auf die Umstände oder gar Inhalte konkreter Gespräche geschlossen werden (erneut geht es allein um ein „Für-möglich-halten“ von Kommunikation); überdies hat die Datenerhebung nichts mit den spezifischen Gefahren distanzierter, technisch vermittelter Kommunikation zu tun; der Aussagegehalt ist kein anderer, als wenn man auf sonstige Weise erfährt, dass jemand bei einem bestimmten Unternehmen arbeitet, zu einer bestimmten Zeit in einem Krankenhaus oder einem Hotel war etc.

Fehl geht es, wenn die Beschwerdeführer am Beispiel der IP-Adressen aufzeigen wollen, dass die Unterscheidung von Bestands- und Verkehrsdaten überhaupt hinfällig sei (Beschwerdeschrift S. 11). Wollte man jede Abgrenzungsschwierigkeit in einzelnen Grenzfällen zum Anlass nehmen, gleich die gesamte – bewährte und ansonsten unangreifbare – Kategorienbildung aufzugeben, so wäre das das Ende jeder Jurisprudenz. Freilich kann nicht übersehen werden, dass über die Frage der Behandlung dynamischer IP-Adressen im Rahmen des § 113 TKG (dass statische IP-Adressen Bestandsdaten sind, kann als gesichert gelten) vorübergehend gewisse Unsicherheiten bestanden, die von der Rechtsprechung inzwischen weitgehend geklärt worden sind.

LG Hamburg, CR 2005, 832 ff.; LG Stuttgart, CR 2005, 598 f.; LG Würzburg, NSTZ-RR 2006, 46 f.; a.A. LG Bonn im Beschluss vom 21.5.2004, 31 Qs 65/04;

Derartige anfängliche Einordnungsschwierigkeiten bei neuen technischen Phänomenen sind jedoch völlig normal, und es kann kein Zweifel bestehen, dass eine sinnvolle Zuordnung möglich ist.

Fehl geht des weiteren das Argument, Bestandsdaten müssten deswegen dem Schutzbereich des Art. 10 GG unterfallen, weil Bestandsdatenabfragen (Rufnummernermittlung) oftmals eine Vorbedingung für später durchgeführte Telekommunikationsüberwachungsmaßnahmen darstellten (S. 10, 12 der Beschwerdeschrift). Bereits unter A.II. (S. 7 ff.) ist ausgeführt worden, dass die in Bezug genommene Fallgruppe (Vorbereitung von TKÜ-Maßnahmen) zwar vorkommt, aber zahlenmäßig eine eher untergeordnete Rolle spielt. Erneut wird also von den Beschwerdeführern die

fragwürdige Methode gewählt, von einem Randphänomen her gleich aufs Ganze zu schließen, obwohl die meisten Bestandsdatenabfragen, wie dargelegt, mit Telekommunikationsüberwachungsmaßnahmen nichts zu tun haben. Aber selbst soweit man allein auf die in der Tat existierende Fallgruppe „Vorbereitung eines Art. 10 GG-Eingriff“ abstellt, ist es nicht gerechtfertigt, die beiden sowohl faktisch wie rechtlich unterscheidbaren Handlungen (Vorbereitungsmaßnahme und TKÜ-Maßnahme) schlichtweg gleich zu setzen. Die bloße Vorbereitung/Vorbedingung eines Eingriffs ist eben noch nicht der Eingriff selbst. Das bloße Herausfinden einer Rufnummer ist genauso wenig ein Eingriff in das Fernmeldegeheimnis wie das Herausfinden einer Adresse ein Eingriff in das Postgeheimnis oder die Sicherstellung eines Schlüssels ein Eingriff in Art. 13 GG.

Kühling, K&R 2004, 105/107; Thiede, Kriminalistik 2004, 104/105. So nunmehr ausdrücklich auch BVerfG vom 22.8.2006 – 2 BvR 1345/03, Abs. 63 a.E. (IMSI-Catcher).

Überspitzt ist es schließlich, wenn die Beschwerdeführer argumentieren, Schutzzweck des Art. 10 GG sei es, den Telekommunikationsteilnehmer umfassend so zu stellen, wie er bei unmittelbarer Kommunikation stünde; bei unmittelbarer Kommunikation aber wären keine Bestandsdaten angefallen. Dass diese Auslegung zu weit geht, haben die beiden jüngeren Entscheidungen des BVerfG zu den Verbindungsdaten im Mobiltelefon und zum IMSI-Catcher

BVerfG, Urteil vom 2.3.2006 – 2 BvR 2099/04; BVerfG Kammerbeschluss vom 22.8.2006 – 2 BvR 1345/03, dort v.a. Abs. 61: „Zwar verfügt der potentielle Kommunikationsteilnehmer nicht über die gleiche Sicherheit, die bestünde, wenn er sich bei der beabsichtigten Kommunikation keines technischen Mediums bediente“.

deutlich gemacht, denn auch die dort nach Ansicht des BVerfG nicht von Art. 10 GG geschützten Daten wären bei unmittelbarer Kommunikation nicht angefallen. Stets geht es allein darum, ob eines der spezifischen Risiken gegeben ist, vor denen Art. 10 GG schützen will. Dies ist bei Bestandsdaten aber nicht der Fall.

Es bedarf noch einer Auseinandersetzung mit der von den Beschwerdeführern nicht eigens in Bezug genommenen vermittelnden Ansicht in Teilen der Literatur, die den Zugriff auf Bestandsdaten zwar nicht an sich und grundsätzlich, aber doch in bestimmten Situationen, d.h. ausnahmsweise als Eingriff in Art. 10 GG ansieht. Argumentiert wird, es komme stets auf den konkreten Verwendungszusammenhang an. Liege die Konstellation aber so, dass es um die Ausforschung eines konkreten Telekommunikationsvorgangs gehe und werde mittels eines Eingriffs in Art. 10 GG (z.B.

Erhebung von Verkehrsdaten nach § 100g StPO) etwa die Rufnummer eines Gesprächsteilnehmers ermittelt, so sei auch noch der nachfolgende, letzte Schritt, die Ermittlung, an wen die Rufnummer vergeben ist, Teil der Gesamtmaßnahme „Ausforschung dieses Gesprächs“, so dass auch die Bestandsdatenabfrage in diesem Fall das Fernmeldegeheimnis berühre. Vertreten wird im Ergebnis also, die Bestandsdatenabfrage unterfalle in der oben (A.II., S. 13 ff.) skizzierten Fallgruppe „Nachbereitung von Eingriffen in Art. 10 GG“ – aber auch nur in dieser – dem Fernmeldegeheimnis.

Neumann/Wolff, TKMR 2003, 110/113 f.; Kühling, K&R 2004, 105/107 f.

Auch diese Ansicht ist abzulehnen. Das Gesetz und die bisherige Rechtspraxis haben sich – in großer gedanklicher Schärfe und vor allem mit dem großen Vorzug einer einheitlichen, für alle Fallgruppen anwendbaren Unterscheidung – bislang bemüht, die (in Art. 10 GG eingreifende) Ermittlung eines Verkehrsdatums und die – ggf. vorausgehende oder auch nachfolgende – (allein Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG berührende) Bestandsdatenabfrage klar voneinander zu trennen. Deutlich wird dies etwa, wenn man § 100g StPO betrachtet (im Landespolizeirecht würde aber z.B. für Art. 34b Abs. 2 und 3 BayPAG nichts anderes gelten). Über die Befugnis des § 100g StPO, der als der maßgebliche Eingriff in Art. 10 GG angesehen und an entsprechende Voraussetzungen gebunden wird, können allein Verkehrsdaten erhoben werden; diese sind gemäß § 100g Abs. 3 StPO u.a. Rufnummern und Kennungen, nicht aber die hinter diesen Nummern stehenden Personen. Sollen auch diese ermittelt werden, bedarf es hierzu eines zweiten Eingriffs – der Bestandsdatenabfrage –, der nunmehr allerdings nicht mehr Art. 10 GG berührt (dieser ist durch § 100g StPO gleichsam vollständig „abgearbeitet“) und daher so wie alle Bestandsdatenabfragen auch auf der Basis der allgemeinen Rechtsgrundlagen, namentlich §§ 112, 113 TKG (i. V. m. §§ 161, 163 StPO) zulässig ist. Von dieser Zweiteilung gehen der Gesetzgeber, die Praxis und die Kommentarliteratur aus.

Karlsruher Kommentar/Nack, StPO, 5. Aufl. 2003, § 100g, Rn. 12; Meyer-Goßner, StPO, 49. Aufl. 2006, § 100g, Rn. 4; Pfeiffer, StPO, 5. Aufl. 2005, § 100g, Rn. 6.

Es wäre ein erheblicher rechtsstaatlicher Rückschritt, wenn man diese Unterscheidung aufgäbe und Verkehrsdatenerhebung und nachfolgende Bestandsdatenerhebung als einen einheitlichen Eingriff in Art. 10 GG ansehen wollte. Hierfür seien folgende Gründe angeführt:

- Festzuhalten ist im Ausgangspunkt, dass in der Tat zwei faktisch unterscheidbare, aufeinander folgende Ermittlungshandlungen gegeben sind. Die Telekommunikationsunternehmen speichern, wie die Beschwerdeführer auf S. 12 selbst ausführen, in ihren Aufzeichnungen zu konkreten Verbindungen (Verkehrsdaten) regelmä-

ßig nur Nummern, nicht aber die zugehörigen Namen. Es ist nur folgerichtig, dass § 100g StPO die Namen nicht zu den Verkehrsdaten zählt. Durch den § 100g-StPO-Eingriff in Art. 10 GG bekommt man die hinter etwaigen Nummern stehenden Namen nicht. Will man diese ermitteln (dies wird wohl kaum bzgl. aller ermittelten Nummern der Fall sein), bedarf es einer zweiten Ermittlungshandlung, die auch einen Zugriff auf einen anderen Datensatz, nämlich Bestandsdaten, darstellt.

- Es wäre kein rechtsstaatlicher Gewinn, den nachfolgenden Bestandsdateneingriff auch unter Art. 10 GG zu fassen. Denn es hat in den hier diskutierten Konstellationen ja bereits ein Eingriff in Art. 10 GG stattgefunden; die hierfür geltenden strengen Voraussetzungen sind bereits erfüllt worden; die spezifischen Anforderungen, die Art. 10 GG stellt, sind bereits abgearbeitet. Würde man auch den nachfolgenden Eingriff als Art. 10 GG-relevant ansehen, wäre nichts gewonnen, da die für Art. 10 GG geltenden Voraussetzungen ohnehin bereits beachtet worden sind

- Es wäre im Gegenteil ein rechtsstaatlicher Verlust, auch die Bestandsdatenabfrage (oder eine sonstige Zuordnung Nummer - Name) als Teil einer Gesamtmaßnahme unter Art. 10 GG zu fassen. Denn konsequenterweise müsste man dann diese Bestandsdatenabfrage als von § 100g StPO bereits implizit mitumfasst ansehen, d.h. auch die (dann einheitliche) Befugnisnorm entsprechend ausweiten. Eine erneute Prüfung (§§ 112, 113 TKG verlangen ja eine erneute Erforderlichkeitsprüfung) könnte unterbleiben, da ja auch kein zusätzlicher Grundrechtseingriff (in Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) vorläge. Alternativ könnte man die Telekommunikationsunternehmen – im Rahmen einer dann Art. 10 GG-konformen neuen Gesetzesfassung – verpflichten, den Ermittlungsbehörden von vornherein auch gleich alle „hinter den Nummern stehenden“ Namen mitzuteilen (wenn Art. 10 GG nur durch die Gesamtmaßnahme berührt ist, wäre dies geradezu konsequent). Dies freilich wäre keineswegs grundrechtsschonender, weil die personenbezogenen Daten aller möglicher Teilnehmer offengelegt würden, obwohl bei der bisherigen zweistufigen Ausgestaltung (mangels Erforderlichkeit) im zweiten Schritt vielleicht nicht alle Namen ermittelt worden wären. Deutlich wird, dass die bisherige Lösung eines zweistufigen Vorgehens, die auch die zweite Stufe einer vollen grundrechtlichen Rechtfertigungslast unterwirft, deutlich freiheitsschonender ist. Der „Verlust“, die zweite Stufe eigenständig prüfen zu müssen, ist bei weitem höher, als der „Gewinn“, auch die Namensermittlung unter den vermeintlich strengeren (aber bereits „abgearbeiteten“) Art. 10 GG zu fassen.

- Hinzu kommt schließlich: Es kann bei logischer Betrachtung hinsichtlich der grundrechtlichen Beurteilung eigentlich keinen Unterschied machen, ob eine Bestandsdatenabfrage dem Eingriff in Art. 10 GG vorausgeht und ihn vorbereitet (durch Zuordnung einer Nummer zu einem Namen) oder ihm nachfolgt und ihn nachbereitet (durch Zuordnung des Namens zu einer Nummer). Für die Vorbereitung eines Eingriffs in das Fernmeldegeheimnis ist jedoch weitgehend unstrittig (auch bei den Ver-

treten der hier zu besprechenden Ansicht), dass diese selbst noch nicht Art. 10 GG berührt.

So insbesondere Kühling, K&R 2004, 105/107.

Für die Nachbereitung kann nichts anderes gelten. Beide Male – bei der Vor- wie bei der Nachbereitung – liegen je eigenständige Grundrechtseingriffe vor, die auch je eigenständig zu beurteilen sind.

Keinen Eingriff in Art. 10 GG stellt es auch dar, wenn im Rahmen von § 113 TKG sog. Zugriffsdaten (PIN, d.h. Personal Identity Number, und PUK, d.h. Personal Unblocking Key) abgefragt werden. Dass dies auch nach Auffassung des Gesetzgebers so ist, sollte – nach entsprechenden Unsicherheiten in der Praxis – durch den neuen § 113 Abs. 1 S. 2 und 3 TKG ausdrücklich klargestellt werden.

BT-Drucks. 15/2316, S. 97.

Mit dieser Auffassung liegt der Gesetzgeber auch richtig. Denn auch diese Zugriffsdaten ermöglichen allenfalls einen Zugriff auf etwaige (vermeintlich, siehe sogleich) durch Art. 10 GG geschützte Verkehrsdaten; ihre Erhebung ist jedenfalls aber noch nicht selbst der Zugriff; dies ist damit genauso wenig Eingriff in Art. 10 GG wie etwa die Sicherstellung eines Wohnungsschlüssels ein Eingriff in Art. 13 GG wäre.

Thiede, Kriminalistik 2004, 104/105.

Hinzu kommt, dass die Zugriffsdaten Bestandsdaten sind, deren Speicherung bei den Telekommunikationsunternehmen nicht von jenen spezifischen Risiken technisch vermittelter Kommunikation herrührt, vor denen Art. 10 GG schützen will. Entscheidend ist aber ein Letztes: Der Streit um die Frage, ob die Abfrage von Zugriffsdaten Art. 10 GG berührt, konnte eigentlich überhaupt nur aufkommen, weil man vorübergehend geglaubt hatte, die Ermittlung der auf einem (zunächst mittels PIN und PUK zu entsperrenden) Mobiltelefon gespeicherten Verbindungsdaten sei ein Eingriff in Art. 10 GG, mit dem der Zugriff auf PIN und PUK in engem Zusammenhang stehe.

In diese Richtung z.B. BerlKommTKG/Kleszczewski, 2006, § 113, Rn. 9.

Mittlerweile hat das Bundesverfassungsgericht jedoch klargestellt, dass der Zugriff auf die im Herrschaftsbereich des Teilnehmers gespeicherten Verkehrsdaten gerade kein Eingriff in Art. 10 GG ist.

BVerfG, Urteil vom 2.3.2006 – 2 BvR 2099/04.

Umso fernliegender ist es geworden, den im Vorfeld angesiedelten Abruf der Zugriffsdaten mit Art. 10 GG in Verbindung zu bringen.

Kurz zu erwähnen bleibt die Frage, ob mittels Anfrage nach § 113 TKG Auskunft darüber verlangt werden darf, welche Person sich hinter einer (bereits ermittelten) dynamischen IP-Adresse verbirgt. Die Handhabung der Landgerichte war zunächst uneinheitlich; weitgehend durchgesetzt hat sich in der Rechtsprechung mittlerweile indes die Meinung, eine derartige Abfrage sei ein nicht in Art. 10 GG eingreifender Zugriff auf ein bloßes Bestandsdatum, der auf § 113 TKG gestützt werden könne.

LG Hamburg, CR 2005, 832 ff.; LG Stuttgart, CR 2005, 598 f. (m. Anm. Gercke; s.a. Anm. Bär, MMR 2005, 626 ff.); LG Würzburg, NStZ-RR 2006, 46 f.; aA LG Bonn im Beschluss vom 21.5.2004, 31 Qs 65/04; siehe dazu auch (in die Richtung der jetzt überwiegenden Meinung gehend) BT-Drucks. 14/7008, S. 7; aktuell: Referentenentwurf für ein „Gesetz zur Neuordnung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ (Stand 27.11.2006) S. 56 f.

Für das hiesige Verfahren ist die Frage nicht unmittelbar entscheidungserheblich. Denn selbst wenn man (anders als die jetzt überwiegende Auffassung) der Ansicht folgte, Art. 10 GG sei berührt, so hätte dies angesichts des eindeutigen § 113 Abs. 1 S. 3 TKG, der Eingriffe in Art. 10 GG ausdrücklich verbietet, nur zur Folge, dass der Auskunftsanspruch eben nicht auf § 113 TKG gestützt werden kann (sondern dass nach § 100g StPO vorgegangen werden muss). Die Frage berührt also allein die Problematik der richtigen (ggf. verfassungskonformen) Auslegung von § 113 TKG; zur Verfassungswidrigkeit des § 113 TKG kann sie jedenfalls nicht führen.

Zusammenfassend kann ohne jede Einschränkung festgehalten werden, dass Art. 10 GG durch die in den §§ 111 ff. TKG geregelten Verfahren der Vorhaltung von und Auskunft über Bestandsdaten nicht berührt wird. Berührt ist stets allein das Recht auf informationelle Selbstbestimmung.

## *2. Keine Verletzung des Gleichheitssatzes (Art. 3 Abs. 1 GG)*

Die Beschwerdeführer behaupten eine Verletzung des Gleichheitssatzes (Art. 3 Abs. 1 GG). Auch bzgl. der hier allein noch entscheidungserheblichen Bestandsdatenspeicherung und -abrufbarkeit bei Telekommunikationsunternehmen reklamieren sie eine Ungleichbehandlung zu anderen Formen der Fernkommunikation (v.a. Post), zur räumlich-unmittelbaren Kommunikation (ohne Kommunikationsmittler) sowie zu anderen Dienstleistungen, die für den Staat nützliche Daten bereitstellen könnten.

Die entsprechenden, über gestufte Verweisungen operierenden, Passagen der Beschwerdeschrift finden sich auf den S. 29 ff., 56 ff., 85 f. Überwiegend haben sich die Ausführungen infolge des teilweisen Nichtannahmebeschlusses vom 21.6.2006 erledigt.

Diese Behauptung geht fehl. Eine Verletzung des Art. 3 Abs. 1 GG durch die §§ 111 ff. TKG liegt nicht vor.

Die Überzeugungskraft der Argumentation der Beschwerdeführer leidet darunter, dass alle Passagen, in denen die Ungleichbehandlung nicht nur behauptet (wie auf S. 85 f. der Beschwerdeschrift), sondern näher begründet werden (S. 30 ff., 56 ff.), ausschließlich auf die Verkehrsdatenerfassung zugeschnitten sind, nicht jedoch ausdrücklich auf die Bestandsdatenerfassung eingehen, die hier jedoch – nach dem teilweisen Nichtannahmebeschluss – allein entscheidungserheblich ist. Alle Ausführungen zum Vergleich mit anderen Kommunikationsformen, zum Gefahrenpotential der Telekommunikation, zum Nutzen des Eingriffs, zu Massenkommunikation und Computerdaten (S. 30 ff.) heben ausschließlich auf Verkehrsdaten ab und passen daher auf den hier nur noch zu entscheidenden Fall nicht. Es ist nicht korrekt, bei der Bestandsdatenabfrage gemäß §§ 112, 113 TKG (S. 85 f.) schlichtweg nach vorne zu verweisen, obwohl dort doch eine ganz andere Fallkonstellation behandelt wird. Ebenso wenig kann es angehen, bei § 111 TKG (S. 56 ff.) Ausführungen zu zitieren und abzudrucken, die erneut (gleich im ersten Satz und dann durchwegs) allein die „Vorratsspeicherung“ von Verkehrsdaten behandeln. Wenn im Folgenden also aufgezeigt wird, dass keine ungerechtfertigte Ungleichbehandlung vorliegt, so haben diese Ausführungen, einen etwas spekulativen Charakter, weil die Ungleichbehandlung gerade im Punkt Bestandsdatenerfassung von den Beschwerdeführern schon gar nicht schlüssig begründet worden ist.

Was die Erhebung von Bestandsdaten und insbesondere auch ihre automatisierte Abrufbarkeit angeht, so sind die wesentlichen Ausführungen zur Systemkonformität dieses Regelungskomplexes bereits oben unter A.III. (S. 16 ff.) gemacht worden. Dort wurde gezeigt, worin die spezifische Rechtfertigung der Erfassung der Telekommunikationsbestandsdaten liegt. Darin nämlich, dass es sich bei der im Zentrum stehenden Zuordnung von Person und Rufnummer um ein – etwa mit dem Wohnsitz oder den Fahrzeugdaten vergleichbares – sehr grundlegendes Identifikationsmerkmal handelt, das gleichsam die kommunikative Verortung und Erreichbarkeit einer Person im Verhältnis zu seiner Umwelt betrifft. Die Rufnummer einer Person ist – gerade in einem Zeitalter der elektronischen Kommunikation – ein Basisdatum zur Identifikation einer Person, das an Bedeutung demjenigen des Wohnsitzes oder z.B. des Fahrzeugs in nichts nachsteht. Die Entscheidung, die Telekommunikationsbestandsdaten dem staatlichen Zugriff zu öffnen, fügt sich deshalb stimmig in ein Ge-

samtsystem ein, in dem auch andere derartige Basisdaten (insbesondere Wohnsitz: Melderegister; Fahrzeug: Fahrzeugregister) bereits seit langem erfasst werden und dem – auch automatisierten – Abruf der Sicherheitsbehörden offen stehen.

Für eine Erfassung gerade der Telekommunikationsbestandsdaten lässt sich im Übrigen anführen, dass sich das Telekommunikationsverhalten in jüngerer Zeit (Mobiltelefone, Internet etc.) grundlegend verändert hat – und zwar in einer Weise, die die Arbeit der Sicherheitsbehörden einerseits erschwert hat (moderne Kommunikationsmittel werden bei der Begehung von Straftaten zunehmend eingesetzt), andererseits aber auch neue Ermittlungsansätze schafft.

Hierzu BVerfG, Kammerbeschluss vom 22.8.2006 – 2 BvR 1345/03, Abs. 75.

Die Bedeutung von Telekommunikationsspuren bei der Straftatenverfolgung hat daher generell sehr zugenommen. Auch im Zusammenhang damit ist ein verlässliches System der Bestandsdatenerfassung unerlässlich.

Fehl geht die Einlassung der Beschwerdeführer, es sei nicht rechtfertigbar, warum Telekommunikationsdaten erfasst werden, die Bestandsdaten anderer Dienstleistungsbranchen (Verkehrssektor, Versorgungsbetriebe, Banken) dagegen nicht. Soweit es in diesen Branchen überhaupt vergleichbare Bestandsdaten gibt (z.B. Strom- und Gaslieferungsvertrag, Bahncard etc.; Informationen über einzelne Verkehrsvorgänge, z.B. Flüge, Bahnfahrten, dagegen entsprechen eher den Verkehrsdaten), stellen diese nicht in derselben Weise wie die Rufnummer ein Basisdatum zur Identifikation und Erreichbarkeit des Einzelnen in der Öffentlichkeit dar; regelmäßig dürften sie auch nicht über die gleiche Ermittlungsrelevanz verfügen. Soweit derartige Daten im Einzelfall dennoch für strafrechtliche Ermittlungen relevant sind, (z.B. seinerzeit, als es bei der Aufklärung des RAF-Terrorismus eine Rolle spielte, dass Stromrechnungen bar beglichen wurden), ist es außerdem keineswegs so, dass es für die Strafverfolgungsbehörden keine Möglichkeit gäbe, auf diese Daten zuzugreifen (durch Zeugenbefragung, durch Beschlagnahme oder äußerstenfalls auch durch Rasterfahndung). Was nur als nicht notwendig angesehen wird, ist die generelle Einrichtung eines Systems zur planmäßigen Vorhaltung und Abrufbarkeit dieser Daten. Im Übrigen ist es in Teilbereichen, wo der Zugriff auf bestimmte Daten sich z.B. aufgrund neuer Bedrohungslagen doch als wichtig und für die Sicherheitsbehörden interessant erweist, auch nicht so, dass der Gesetzgeber sich derartigen Entwicklungen verschlüsse. So ist es etwa in dem von den Beschwerdeführern ausdrücklich erwähnten Bankenbereich so, dass mittlerweile über § 24c KWG, § 93 Abs. 7 AO für bestimmte Zwecke (auch der Strafverfolgung) ja sogar ein automatisiert abrufbares System der Konten-Stammdatenerfassung geschaffen wurde. Und auch das Terro-

rismusbekämpfungsergänzungsgesetz vom 5. Januar 2007 (BGBl. I S. 2) hat die Befugnisse des Bundesamts für Verfassungsschutz für Auskünfte von Luftfahrtunternehmen und Kredit- und Finanzdienstleistungsinstituten verlängert und vergleichbare Befugnisse für den Militärischen Abschirmdienst und den Bundesnachrichtendienst geschaffen.

§ 8a Abs. 2 BVerfSchG; § 4a MADG, § 2a BNDG, eingefügt durch Artikel 1 Nr. 2 des Terrorismusbekämpfungsergänzungsgesetzes; man denke auch an den Streit zur Übermittlung von Passagierdaten an die USA.

Von einer gleichheitswidrigen Schlechterstellung des Telekommunikationsbereichs kann nach alledem keine Rede sein.

Unzutreffend ist schließlich der Vergleich sowohl mit der Post als auch mit der unmittelbaren Kommunikation. Dies beginnt schon damit, dass es bei der Post regelmäßig keine Bestandsdaten (sondern allenfalls Verkehrsdaten) gibt. Außerdem könnten diese, was das Interesse der Sicherheitsbehörden betrifft, normalerweise allein in der für die Post allein relevanten Zuordnung von Person und Adresse liegen; die Post weist einem ja (anders als die Telekommunikationsunternehmen mit der Rufnummer) üblicherweise kein neues Identifikationsmerkmal zu; die Adresse ist aber bereits über das Melderegister hinreichend erfasst, so dass insoweit an einer Bestandsdatenerfassung der Post kein Interesse besteht.

Eine Ausnahme besteht bzgl. der Postfächer. Gerade diese werden aber bereits über § 8a Abs. 1 BVerfSchG erfasst, so dass erneut keine Rede davon sein kann, der Gesetzgeber sei gleichheitswidrig untätig geblieben.

Schon von vornherein nicht vergleichbar sind schließlich Telekommunikation und räumlich unmittelbare Kommunikation – dies schon deswegen, weil bei der unmittelbaren Kommunikation von Mensch zu Mensch keine Bestandsdaten anfallen; diese aber sind hier der entscheidende Punkt.

### *3. Das Zusammenspiel von §§ 112, 113 TKG einerseits und dem jeweils einschlägigen Fachrecht der ersuchenden Behörde (StPO, Polizeigesetze etc.) andererseits*

Die Argumentation der Beschwerdeführer geht bei der Behandlung der Auskunftsverfahren nach §§ 112, 113 TKG offenbar völlig selbstverständlich davon aus, der im Zuge dieser Verfahren erfolgende Eingriff in Grundrechte des betroffenen Bürgers sei allein den §§ 112, 113 TKG zurechenbar – mit der Folge, dass auch die Last der ver-

fassungsrechtlichen Rechtfertigung des Eingriffs ausschließlich „auf den Schultern“ dieser beiden Normen ruht.

So zum Teil – ohne nähere Darlegung – auch Stimmen der Literatur, z.B. BerlKommTKG/Kleszczewski, 2006, § 112, Rn. 3 („regelt ... die Voraussetzungen für einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung“); immerhin wird dort (Rn. 13) zumindest gesehen, dass bzgl. der Folgefragen (Mitteilungspflicht, Auskunftsansprüche etc.) auch das jeweils einschlägige Fachrecht eine Rolle spielt.

Völlig übersehen wird dabei, dass die um Auskunft nachsuchenden Sicherheitsbehörden jeweils zugleich auf der Basis eines für sie geltenden Fachgesetzes (StPO, Polizeigesetze, Verfassungsschutzgesetze etc.) handeln, das seinerseits eingehende Regelungen darüber enthält, wann und unter welchen Voraussetzungen die Behörde personenbezogene Daten erheben darf und wie sie mit diesen weiter zu verfahren hat (z.B. hinsichtlich Zweckbindung, Mitteilung oder Auskunft an den Betroffenen etc.). All diese Fragestellungen werden bereits in den jeweiligen Fachgesetzen einer differenzierten und auf die spezifischen Bedürfnisse und Eigenarten des Rechtsgebiets zugeschnittenen Regelung zugeführt, so dass sich die Regelungen auch keineswegs gleichen:

- Die Ermittlungsbefugnisse der StPO stehen ganz unter dem Vorzeichen und festen Bezugspunkt eines je nach Verfahrensstand unterschiedlich stark verdichteten Tatverdachts in Bezug auf eine konkrete, bereits begangene Straftat. Aufgrund dieses festen Bezugspunkts, der alles strafprozessuale Ermitteln gleichsam an eine natürliche Eingriffsschwelle bindet, kann die Regelung der allgemeinen Ermittlungsbefugnisse von Staatsanwaltschaft und Polizei (§§ 161, 163 StPO – diese sind auch für Anfragen nach §§ 112 f. TKG maßgeblich) relativ generalklauselartig ausfallen. Korrespondierende Auskunftspflichten des Befragten müssen besonders statuiert sein (z.B. § 161a StPO) und folgen nicht schon aus den §§ 161, 163 StPO. Auch die Folgefragen (v.a. bzgl. Benachrichtigungspflichten und Auskunftsansprüchen) sind differenziert geregelt. Besondere Benachrichtigungspflichter gibt es nur in besonderen Fällen (z.B. § 101 StPO), anderenfalls geht die Frage nach Benachrichtigung und Auskunft auf im allgemeinen Verfahrensgang (Mitteilung von der Einstellung des Verfahrens, § 170 Abs. 2 S. 1 StPO, ansonsten die allgemeinen Verfahrens- und Akteneinsichtsrechte z.B. § 147 StPO); für Dritte regelt § 475 StPO ein Auskunftsrecht; besondere Auskunftsregelungen gibt es auch für Dateien (§§ 491, 495 StPO).

- Das präventive Polizeirecht hingegen steht unter dem Vorzeichen der Gefahr und Gefahrenabwehr. Liegt eine konkrete Gefahr vor, reichen die Polizeibefugnisse weit; hier könnte erforderlichenfalls auf der Basis der polizeilichen Generalklausel ad hoc eine Auskunftspflicht gegenüber Bürgern und Unternehmen verfügt werden. Ansonsten kann die Befugnis, personenbezogene Daten zu erheben, freilich nicht an die Gefahrenschwelle gebunden sein, denn typischerweise dienen polizeiliche Ermitt-

lungen ja gerade dazu, erst herauszufinden, wo und ob Gefahren bestehen, um dann gegen sie einschreiten zu können. Indem der Gefahrbegriff für die eigentliche Gefahrenabwehr eine hinreichende, d.h. auf einer ausreichenden Wissens- und Prognosebasis beruhende Wahrscheinlichkeit des Schadenseintritts verlangt, setzt er geradezu voraus, dass zunächst, d.h. im Gefahrenvorfeld, durch Ermittlungen die nötige Wissensbasis geschaffen wird. Zu Recht binden die Polizeigesetze die allgemeine Datenerhebungsbefugnis der Polizei daher nicht an die Gefahrenschwelle, sondern formulieren vorsichtiger, die Datenerhebung müsse für die Erfüllung der Gefahrenabwehraufgabe erforderlich sein (z.B. Art. 31 Abs. 1 BayPAG, der auch für Auskunftersuchen nach den §§ 112, 113 TKG einschlägig wäre); hieraus resultiert freilich noch keine korrespondierende Auskunftspflicht des Befragten (diese müsste vielmehr gesondert normiert sein, z.B. Art. 12 BayPAG). Für besondere Ermittlungsbefugnisse (technische Mittel, heimliche Observationen, Eingriffe in Art. 10, 13 GG etc.) stehen spezielle Befugnisnormen mit abgestuften Eingriffsschwellen zur Verfügung. Diese sehen zum Teil auch besondere Benachrichtigungspflichten vor (z.B. Art. 34c Abs. 5 BayPAG), ansonsten gilt bzgl. gespeicherten Daten das allgemeine Auskunftsrecht (z.B. Art. 48 BayPAG) mit seinen auf die spezifischen Interessen der Polizei Rücksicht nehmenden Grenzen.

Zum polizeilichen Informationsrecht: Möstl, Die staatliche Garantie für die öffentliche Sicherheit und Ordnung, 2002, S. 208 ff.

- Ein wieder eigenes Gepräge hat die Datenerhebung durch die Nachrichtendienste, die einerseits geradezu typischerweise weit im Gefahrenvorfeld ansetzt und auch heimlich abläuft, andererseits aber nur auf den Schutz spezifischer Rechtsgüter bezogen ist und den Nachrichtendiensten vor allem keine Kompetenz gibt, selbst die Konsequenzen aus den erlangten Informationen zu ziehen und z.B. gegen ermittelte Gefahren einzuschreiten (keine polizeilichen Befugnisse). Erneut gibt es eine – auf die spezifische Arbeitsweise des jeweiligen Dienstes zugeschnittene – allgemeine Befugnisnorm (z.B. § 8 Abs. 1 BVerfSchG – hierauf wären auch Auskunftersuchen nach §§ 112, 113 TKG zu stützen; eine Auskunftspflicht resultiert hieraus nicht) sowie spezielle Befugnisnormen. Erneut auch ist ein Auskunftsrecht des Betroffenen geregelt, das den Ausgleich zu der besonderen Interessenlage des Dienstes sucht (z.B. § 15 BVerfSchG).

Es kann nicht Sinn und Zweck der §§ 112, 113 TKG sein, die so umrissenen – auf die Besonderheiten des jeweiligen Fachrechts zugeschnittenen – differenzierten Weichenstellungen der Fachgesetze schlicht aufzugeben, und durch eine für alle Sicherheitsbehörden geltende abschließende Einheitsregelung zu ersetzen. §§ 112, 113 TKG dürfen nicht als abschließende Regelung des Themenkomplexes „sicherheitsbehördliche Auskunftersuchen zu Bestandsdaten“ verstanden werden, sondern

sind von vornherein auf ein Zusammenspiel mit dem jeweils anwendbaren Fachrecht hin konzipiert. Das zwischen Fachrecht und §§ 112, 113 TKG bestehende Verhältnis des Zusammenspiels und der wechselseitigen Ergänzung sieht in seinem Kern folgendermaßen aus: Die eigentliche Befugnis zur Erhebung des personenbezogenen Datums kann nur aus dem jeweiligen – für die ersuchende Behörde maßgeblichen und ihre spezifischen Rechte gegenüber dem Bürger normierenden – Fachrecht kommen (z.B. §§ 161, 163 StPO, Art. 31 Abs. 1 BayPAG, § 8 Abs. 1 BVerfSchG). Aufgabe des TKG ist es, in Ergänzung hierzu die telekommunikationsrechtlichen Voraussetzungen dafür zu schaffen, dass eine Behörde diejenigen Auskünfte, die sie erheben darf, auch tatsächlich bekommt, indem zum einen eine korrespondierende Datenvorhaltungs- bzw. Auskunftspflicht der Telekommunikationsunternehmen normiert wird (die nach dem jeweiligen Fachrecht so noch nicht besteht) und zum anderen – v.a. unter den Bedingungen einer Vielfalt der Anbieter – ein funktionstüchtiges Verfahren bereitgestellt wird, in dem die nötigen Auskünfte angefragt und zur Verfügung gestellt werden. Zur Begründung des so verstandenen Ergänzungsverhältnisses von §§ 112, 113 TKG und Fachrecht lassen sich folgende Gründe anführen:

- Aufschlussreich ist zunächst die Entstehungsgeschichte (vgl. dazu schon A.I., S. 2 ff.). Der maßgebliche Entstehungsgrund für §§ 89 Abs. 6, 90 TKG a.F. war die durch die Postprivatisierung und -liberalisierung eingetretene Veränderung gewesen. Mit Wegfall der Deutschen Bundespost fehlte es an einer amtshilfe- und daher ohne weiteres auskunftspflichtigen Behörde; vielmehr bedurfte es „gegenüber den nunmehr privaten Anbietern“ (so die Entwurfsbegründung) einer Rechtsgrundlage und Befugnisnorm, um diese zur Auskunft verpflichten zu können. Überdies war mit dem Monopolisten Deutsche Bundespost die einheitliche Auskunftsstelle weggefallen; es bedurfte eines neuen, über eine zentrale Stelle laufenden Verfahrens, um die Effektivität des Auskunftssystems zu erhalten.

BT-Drucks. 13/3609, S. 55.

Entscheidend ging es damit um die Ausgestaltung des Rechtsverhältnisses zwischen ersuchender Sicherheitsbehörde und abgefragten (nunmehr privaten) Unternehmen (entweder direkt oder über die Regulierungsbehörde). Nicht jedoch war etwa die Erkenntnis Auslöser für die neuen TKG-Normen, dass es nach der Volkszählungsentcheidung (BVerfGE 65, 1 ff.) auch im Rechtsverhältnis zum Bürger einer Befugnisnorm bedurfte, um den Eingriff in sein Recht auf informationelle Selbstbestimmung zu rechtfertigen. Die Konsequenzen aus dem Volkszählungsurteil wurden vielmehr in den jeweiligen Fachgesetzen gezogen, z.B. durch Einfügung großer neuer Regelungsabschnitte über die polizeiliche Erhebung personenbezogener Daten in den Polizeigesetzen.

- Schon hieraus lässt sich eine erste Faustformel für die Charakterisierung des Zusammenspiels von §§ 112, 113 TKG und jeweiligem Fachrecht aufstellen: Zu un-

terscheiden sind verschiedene Rechtsverhältnisse. §§ 112, 113 TKG regeln unstreitig das Rechtsverhältnis zwischen Staat und Telekommunikationsunternehmen; sie statuieren hier eine Pflicht der Telekommunikationsunternehmen, bestimmte Daten zum automatischen Abruf bereitzuhalten (§ 112 Abs.1 Satz 4 TKG) bzw. über sie Auskunft zu erteilen (§ 113 Abs.1 Satz 1 und 2 TKG), sowie die näheren Modalitäten der Auskunftsverfahren. §§ 112, 113 TKG betreffen zugleich und implizit auch das Rechtsverhältnis zwischen Telekommunikationsunternehmen und Kunde, denn die Datenverhaltens- und Auskunftspflicht dispensiert das Telekommunikationsunternehmen von den ansonsten einzuhaltenden Datenschutzbestimmungen (z.B. § 95 Abs. 1 S. 3 TKG). Diese Rechtsverhältnisse (Staat - Unternehmen; Unternehmen - Kunde) sind die beiden eigentlich telekommunikationsspezifischen und daher zu Recht im TKG geregelten Rechtsverhältnisse. Etwas anderes gilt für das „sicherheitsrechtliche“ Rechtsverhältnis zwischen Sicherheitsbehörde und Bürger. Dieses unterfällt dem jeweiligen Fachrecht; das TKG regelt es nicht (oder allenfalls sehr partiell und mittelbar, siehe unten). Die eigentliche Befugnis zur Erhebung des personenbezogenen Datums im Rechtsverhältnis zum Bürger kann die Sicherheitsbehörde gerade nicht aus den §§ 112, 113 TKG ableiten; hierzu muss sie sich vielmehr auf die einschlägigen Ermittlungsbefugnisse des jeweiligen Fachrechts stützen.

Wie hier: Trute, in Trute/Spoerr/Bosch, TKG, 2001, § 89, Rn. 57; BeckTKG-Komm/Bock, 3. Aufl. 2006, § 111, Rdnr. 3, § 113, Rdnr. 9; ähnlich auch: Wuermeling/Felixberger, CR 1997, 555/559 f.; Bär, MMR 2000, 477/479; BeckTKG-Komm./Büchner, 2. Aufl. 2000, § 89, Rn. 45; Gramlich, in: Manssen (Hrsg.), Telekommunikations- und Multimediarecht, § 90 TKG, Rn. 30, 33, 35; Würmeling., in Heun (Hrsg.), Handbuch Telekommunikationsrecht, 2002, Teil 9, Rn. 6.

- Dass das Gesetz selbst von der hier vertretenen „Aufgabenverteilung“ zwischen TKG und Fachrecht ausgeht, wird nunmehr in § 113 Abs. 1 S. 2 TKG ganz deutlich, wo ausdrücklich die Befugnisnormen der §§ 161, 163 StPO sowie die allgemeinen Datenerhebungsvorschriften der Polizeigesetze und der Verfassungsschutzgesetze etc. in Bezug genommen werden und von Auskunftersuchen „nach“ diesen Fachgesetzen gesprochen wird. Freilich wird dies in einem ganz speziellen Kontext (Auskunftersuchen bzgl. PIN und PUK) gesagt, hieraus darf aber nicht der Umkehrschluss gezogen werden, dass ansonsten etwa allein das TKG (und nicht das Fachrecht) maßgeblich wäre. Denn auch die Auskunftersuchen bzgl. PIN und PUK betreffen ganz normale Bestandsdaten, die an sich bereits § 113 Abs. 1 S. 1 TKG unterfallen. In § 113 Abs. 1 S. 2 TKG sollten diese Auskunftersuchen nicht etwa an zusätzliche Anforderungen des Fachrechts gebunden werden (die ansonsten etwa nicht gälten), vielmehr sollte klargestellt werden, dass innerhalb der stets hinzuzudenkenden Befugnisnormen des Fachrechts eben nicht auf die besonderen Befugnisnormen zum Eingriff in Art. 10 GG zurückgegriffen werden muss (vgl. Satz 3),

sondern dass die normalen allgemeinen Ermittlungsbefugnisse der Fachgesetze ausreichen sollen. Dies kann genau besehen freilich allenfalls eine deklaratorische Klarstellung sein. Nichtsdestoweniger handelt es sich um eine Klarstellung, die deutlich macht, dass das TKG selbst vom selbstverständlichen Hinzutreten einer fachrechtlichen Befugnisnorm ausgeht.

BT-Drucks. 15/2316, S. 97.

- Die hier umrissene „Aufgabenverteilung“ zwischen TKG und Fachrecht, nach der die Befugnisnorm für den Datenerhebungseingriff im Verhältnis zum Bürger aus dem Fachrecht kommen muss, ist auch sonst für das TKG typisch. Dies wird nicht zuletzt bei den Eingriffen in Art. 10 GG deutlich. § 110 TKG regelt hier zwar verschiedene Mitwirkungspflichten der Telekommunikationsdienstleister in Bezug auf die Ermöglichung staatlicher Eingriffe in Art. 10 GG. Die eigentliche Befugnis zum Art. 10 GG-Eingriff muss jedoch aus dem jeweiligen Fachrecht kommen (§§ 100a ff. StPO, Art. 34a ff. BayPAG etc.). Zuzugeben ist, dass die Abgrenzung TKG-Fachrecht bei Art. 10 GG-Eingriffen nicht ganz die gleiche ist wie bei §§ 112, 113 TKG, da diesbezüglich auch das jeweilige Fachrecht noch Mitwirkungs- und Auskunftspflichten der Diensteanbieter regelt (§ 100b Abs. 3, § 100g Abs. 1 S. 1 StPO; Art. 34b Abs. 1 BayPAG); das Rechtsverhältnis zum Unternehmen ist hier also zum Teil im Fachrecht mitgeregelt. Deutlich wird, dass der Gesetzgeber in der Abgrenzung von TKG und Fachrecht nicht immer einer ganz einheitlichen Struktur folgt. Deutlich wird aber auch, dass jedenfalls die Befugnis zum Grundrechtseingriff gegenüber dem Bürger immer dem Fachrecht entstammt.

- Das Angewiesensein auf eine hinzutretende Befugnisnorm des Fachrechts wird überdies auch aus §§ 112, 113 TKG selbst deutlich. Die in ihnen formulierte tatbestandliche Voraussetzung der Erforderlichkeit für die fachgesetzlichen Aufgabenerledigung der Sicherheitsbehörden (§ 112 Abs. 2 a.E., § 113 Abs. 1 S. 1 TKG), die gerade bei § 112 TKG von der Bundesnetzagentur ja regelmäßig noch nicht einmal nachgeprüft werden muss (§ 112 Abs. 4 S. 2 TKG), ist eher ein Verweis auf die Maßstäbe des jeweiligen Fachrechts als eine eigenständig durchgebildete telekommunikationsrechtliche Eingriffsvoraussetzung. Auch dass die Verantwortlichkeit für die Zulässigkeit der Datenübermittlung bei der ersuchenden Stelle liegt (§ 112 Abs. 4 S. 3 TKG), verweist letztlich auf deren Recht.

- Die Notwendigkeit der Hinzunahme der fachrechtlichen Befugnisnorm ist ein rechtsstaatlicher Gewinn, weil die differenzierten Eingriffsvoraussetzungen des Fachrechts zusätzlich zur Anwendung kommen. Sie ist zumindest partiell auch eine bundesstaatliche Notwendigkeit, weil es kompetenziell äußerst fragwürdig wäre, ob die Voraussetzungen etwa für einen landespolizeilichen Datenerhebungseingriff im TKG geregelt werden dürften. Jedenfalls das sicherheitsrechtliche Rechtsverhältnis zum Bürger dürfte im Schwerpunkt nicht telekommunikationsrechtlicher Art und auch kein

notwendiger Annex zur TKG-Regelung sein, so dass eine einheitliche bundesrechtliche Regelung insoweit ausscheidet.

- Eine parallele Struktur (Auseinanderfallen von Befugnisnorm gegenüber dem Bürger und Befugnis-/Verfahrensnorm im Rechtsverhältnis zu den Unternehmen) findet sich neuerdings auch in der Abgabenordnung in Bezug auf die Kontenabfrage: § 93b AO erstreckt die Dateiführungs- und Auskunftspflichten der Kreditinstitute nach § 24c KWG auf die Zwecke der AO, § 93 Abs. 7 AO enthält die hierzu passende Befugnisnorm im Verhältnis zum Steuerpflichtigen. Implizit wird daraus zugleich deutlich, dass der § 112 TKG nachgebildete § 24c KWG keine Befugnisnorm im Verhältnis zum Bürger ist.

Das bis hierher Gesagte hat für die Erfolgsaussichten der hiesigen Verfassungsbeschwerde freilich weittragende Konsequenzen. Zugespitzt könnte man formulieren: Wenn §§ 112, 113 TKG primär das Rechtsverhältnis Staat – Unternehmen regeln (dieses Rechtsverhältnis ist nach dem Nichtannahmebeschluss vom 21.6.2006 nicht mehr verfahrensgegenständlich!) und die maßgebliche Befugnis zum Datenerhebungseingriff gegenüber dem Bürger (dies ist das allein noch verfahrensgegenständlich Rechtsverhältnis) dagegen dem Fachrecht zu entnehmen ist und gerade nicht isoliert aus §§ 112, 113 TKG folgt, so haben die Beschwerdeführer den falschen Streitgegenstand angegriffen (bzw. zumindest hätten sie ihren Angriff auf Normen des Fachrechts erstrecken müssen). Denn dann geht der maßgebliche Grundrechtseingriff gerade nicht von §§ 112, 113 TKG aus, ebenso wenig wie die Last der verfassungsrechtlichen Rechtfertigung auf diese Normen konzentriert werden kann.

Die soeben aufgestellte These vom falsch gewählten Streitgegenstand – dem der hier maßgebliche Grundrechtseingriff gar nicht zuzurechnen ist – trifft den Kern der Sache, ist aber, wenn man ihn so kategorisch formuliert, doch überspitzt und bedarf einer gewissen Modifikation. Es würde, so sehr der datenschutzrechtliche Eingriff im Kern dem Fachrecht zuzurechnen ist und auf seiner Basis gerechtfertigt werden muss, doch zu weit gehen, wenn man sagte, von §§ 112, 113 TKG ginge überhaupt kein Eingriff in das Recht auf informationelle Selbstbestimmung aus. Der im Kern vom jeweiligen Fachrecht ausgehende und getragene Grundrechtseingriff wird bei genauerer Betrachtung von §§ 112, 113 TKG, die auch insoweit das Fachrecht ergänzen, doch immerhin effektiviert und verschärft, so dass jedenfalls ein Teil der verfassungsrechtlichen Rechtfertigung auch in datenschutzrechtlicher Hinsicht vom TKG zu leisten ist. Zu bedenken ist dabei, dass das jeweilige Fachrecht zumeist allein die Befugnis der anfragenden Sicherheitsbehörde ausspricht, das Bestandsdatum zu erheben (Erhebungsrecht), nicht aber die entsprechende Pflicht der Unternehmen statuiert, die Auskunft auch zu erteilen (Auskunftspflicht). Dies ist im Strafprozess-

recht so, wo aus §§ 161, 163 StPO selbst noch keine Auskunftspflicht folgt (eine Auskunftspflicht kann allenfalls über § 161a StPO begründet werden, oder – mittelbar – vielleicht auch, indem man eine Beschlagnahme von Bestandsdatensätzen nach § 94 ff. StPO androht und das Unternehmen so zur Preisgabe zwingt). Dies ist auch im Polizeirecht so, wo aus der jeweiligen Datenerhebungsgrundnorm (z.B. Art. 31 Abs. 1 BayPAG) noch keine Auskunftspflicht folgt (diese besteht nur in besonderen Fällen, z.B. aufgrund entsprechender Anordnung auf der Basis der Generalklausel, was allerdings das Bestehen einer konkreten Gefahr voraussetzt). Dies ist schließlich erst recht im Bereich der Nachrichtendienste so, denen ja gerade keine durchsetzbaren polizeilichen Befugnisse zustehen. Eine Datenerhebungsbefugnis ohne entsprechende Garantie, dass man die entsprechenden Daten von dem Befragten auch erhält, ist freilich nur von begrenztem Wert. Hier wird nun deutlich, inwieweit §§ 112, 113 TKG eben doch für eine Vertiefung des im Prinzip nach Fachrecht zulässigen Eingriffs in das Recht auf informationelle Selbstbestimmung sorgen: dadurch nämlich, dass sie dem fachrechtlichen Recht der Sicherheitsbehörden, bestimmte Daten zu erfragen und zu erheben, eine telekommunikationsrechtliche Pflicht des Diensteanbieters, die erfragten Daten zum automatisierten Abruf bereitzuhalten (§ 112 Abs. 1 Satz 4 TKG) bzw. über sie Auskunft zu erteilen (§ 113 Abs. 1 TKG) hinzufügen und dadurch garantieren, dass der vom Fachrecht nur erlaubte, noch nicht aber selbst abschließend bewerkstelligte Grundrechtseingriff auch Wirklichkeit wird. Erst das TKG garantiert die volle Effektivität des nach Fachrecht erlaubten Auskunftsrechts. Erst der Verbund von fachrechtlicher Befugnis, nach Daten zu fragen und sie zu erheben, auf der einen und telekommunikationsrechtlicher Verpflichtung der Unternehmen, die zu Recht erfragten Daten in einem bestimmten Verfahren auch tatsächlich herauszugeben, auf der anderen Seite bewirkt zusammen den vollen Grundrechtseingriff. §§ 112, 113 TKG leisten damit einen eigenständigen Beitrag dazu, dass der nach Fachrecht erlaubte Grundrechtseingriff auch wirklich zustande kommt. Von ihnen geht somit ein Teil der gerügten Beschwer aus – mit der Folge, dass ein Teil der verfassungsrechtlichen Rechtfertigung auch von ihnen zu leisten ist.

Der Eingriff in das Recht auf informationelle Selbstbestimmung und die damit einhergehende Rechtfertigungslast können daher zwar im Schwerpunkt, aber eben nicht vollständig auf das jeweilige Fachrecht abgewälzt werden; auch von §§ 112, 113 TKG geht ein Eingriffsbeitrag aus, der der Rechtfertigung bedarf. Die Befugnisnorm für Bestandsdatenerhebungen im Rechtsverhältnis zum Bürger bereitzustellen und seine Voraussetzungen zu regeln, ist und bleibt zwar die Aufgabe des jeweiligen Fachrechts der ersuchenden Sicherheitsbehörde. Das Telekommunikationsrecht flankiert indes die fachrechtlich erlaubte Datenerhebung durch die Normierung von Auskunfts-/Datenbereithaltungspflicht und Auskunftsverfahren; diesen eigenständigen Beitrag – aber auch nur diesen – zum Grundrechtseingriff muss sich das Tele-

kommunikationsrecht zurechnen lassen und selbständig rechtfertigen. Auch auf der Basis der hier entwickelten vermittelnden Linie bleibt es folglich dabei, dass es falsch ist, wie in der Beschwerdeschrift geschehen, den Eingriff in das Recht auf informationelle Selbstbestimmung allein §§ 112, 113 TKG zuzurechnen und sie als abschließende Regelung des datenschutzrechtlichen Rechtsverhältnisses zum Bürger anzusehen. Das einschlägige Fachrecht tritt stets hinzu und ist stets hinzuzudenken, ja ihm obliegt es sogar im Schwerpunkt, das datenschutzrechtliche Rechtsverhältnis zum Bürger – zugeschnitten auf die besonderen Bedingungen und Eigenarten des jeweiligen Fachrechts – im Einzelnen auszugestalten.

Was bis hierher zu den Eingriffsvoraussetzungen gesagt wurde, gilt in noch weitaus höherem Maße für alle mit dem Eingriff zusammenhängenden Folgefragen, insbesondere: Wird dem Betroffenen der Eingriff mitgeteilt oder hat er wenigstens einen Auskunftsanspruch? Die Beschwerdeschrift begeht den grundlegenden Fehler, dass sie, wenn sie das Fehlen von Mitteilungspflichten, Auskunftsrechten etc. moniert (S. 80, 83), allein auf die §§ 112, 113 TKG abstellt und überhaupt nicht bedenkt, dass die entsprechenden Regelungen zuallererst im jeweils einschlägigen Fachrecht normiert sein müssen und auch dort zu suchen sind. Sind die §§ 112, 113 TKG schon bezüglich der Eingriffsvoraussetzungen nicht eigentlich die maßgebliche Befugnisnorm, sondern nur flankierende und effektivierende Verfahrensregelungen (wenn gleich mit eigenem Eingriffsbeitrag), so gilt für alle aus der Datenerhebung resultierenden Folgefragen noch viel mehr, dass diese nicht oder allenfalls sehr partiell in §§ 112, 113 TKG geregelt sind, sondern sich zuallererst nach dem jeweils einschlägigen Fachrecht richten.

Trute, in Trute/Spoerr/Bosch, TKG, 2001, § 89, Rn. 55; BeckTKG-Komm/Büchner, 2. Aufl. 2000, § 89, Rn. 45; BeckTKG-Komm/Bock, 3. Aufl. 2006, § 113, Rdnr. 9; Wuermeling/Felixberger, CR 1997, 595/560.

Gerade die Frage, ob und wann der Betroffene benachrichtigt werden kann, kann sinnvollerweise auch nur im Fachrecht entschieden werden, denn sie lässt sich nicht für alle Sicherheitsbehörden einheitlich beantworten (das Geheimhaltungsinteresse wird beim Verfassungsschutz beispielsweise ein anderes sein als in der Strafverfolgung), sondern bedarf differenzierter, auf das jeweilige Fachrecht zugeschnittener Regelungen. Solche Regelungen existieren auch in großer Zahl, wie bereits oben dargelegt (S. 40 ff.). Wenn das TKG Regelungen enthält, die geradezu verhindern, dass der Bürger Kenntnis von Bestandsdatenabfragen erhält (§§ 112 Abs. 1 S. 6 [keine Kenntnisnahme der Unternehmen], Abs. 4 S. 5 [Protokolldaten nur für Zwecke der Datenschutzkontrolle], 113 Abs. 1 S. 4 TKG [Stillschweigen gegenüber Kunden und Dritten]), so darf dies nicht als Absage an ggf. bestehende fachrechtliche Auskunftsansprüche gewertet werden. Maßgebend für diese Regelungen sind vielmehr

zwei Gründe: Zum einen gilt es zu verhindern, dass von den Akteuren, die im TKG näher geregelt sind, zusätzliche Gefahren für den Datenschutz ausgehen; folglich wird verhindert, dass die Telekommunikationsunternehmen Kenntnis von § 112 TKG-Abfragen erlangen (um das Vertrauensverhältnis zwischen Unternehmen und Kunden nicht zu gefährden); folglich wird eine strenge Zweckbindung der §112 TKG-Protokolldaten angeordnet; folglich müssen Unternehmen im Rahmen von § 113 TKG gegenüber Dritten Stillschweigen bewahren. Hinzu kommt ein Zweites: Mitteilungspflichten gegenüber dem Bürger oder Auskunftsansprüche des Bürgers gegenüber den Telekommunikationsunternehmen oder der Bundesnetzagentur will das TKG in der Tat nicht selbst anordnen. Grund hierfür ist aber nicht, dass es die Kenntnisnahme der Bürger schlechthin verhindern möchte; der maßgebliche Grund ist vielmehr, dass es die Frage der Kenntnisnahme schlichtweg nicht als sein Regelungsthema betrachtet. Die spezifisch telekommunikationsrechtlichen Akteure (Unternehmen, Bundesnetzagentur) sollen bei der Frage der Information des Bürgers außen vor bleiben, der TKG-Gesetzgeber will „seine“ Akteure mit diesen Fragen nicht behelligen und schottet sie daher von Benachrichtigungspflichten und Auskunftsansprüchen ab. Umso klarer wird hierdurch, dass der TKG-Gesetzgeber es als ein Problem des jeweiligen Fachrechts ansieht, ob und wie weit die Kenntnisnahme ermöglicht wird. Der TKG-Gesetzgeber stellt den verschiedenen Sicherheitsbehörden für deren Zwecke ein effektives Verfahren zur Verfügung und erwartet im Gegenzug, dass diese Behörden – die die volle datenschutzrechtliche Verantwortung für den Eingriff tragen (§ 112 Abs. 4 S. 3 TKG) – auf der Basis des für sie geltenden Fachrechts das Problem der Betroffenenbenachrichtigung bewältigen. Gegen diese Aufgabenverteilung ist auch aus verfassungsrechtlicher Sicht nichts einzuwenden.

Im Gegenteil ist es interessant, dass das Bundesverfassungsgericht in dem teilweise parallel gelagerten Fall der Kontenabfrage durch Steuerbehörden nach §§ 93 Abs. 7, 93b AO, § 24c KWG, die Frage, ob eine hinreichende Kenntnisnahme des Abgefragten möglich ist, nur im Ausgangspunkt auf § 24c KWG (dies ist die Parallelnorm zu § 112 TKG) bezogen hat, um dann vor allem danach zu fragen, welche Mitteilungs- und Auskunftsrechte nach der Abgabenordnung (und dem – dies war zur Ablehnung der einstweiligen Anordnung ausreichend – Erlassrecht zur AO) bestehen. Insistiert wird also jedenfalls nicht auf in § 24c KWG zu regelnde Mitteilungspflichten der Kreditinstitute oder der Bundesanstalt (diese entsprächen den Telekommunikationsunternehmen und der Bundesnetzagentur), vielmehr wird das Hauptaugenmerk darauf gerichtet, ob und wie die Kenntnisnahme auf der Basis des jeweiligen Fachrechts und durch die jeweilige Fachbehörde möglich ist; vgl. BVerfG, Beschluss vom 22.3.2005 – 1 BvR 2357/04, 1 BvQ 2/05. Freilich handelt es sich nur um eine Entscheidung im einstweiligen Rechtsschutz, und doch wird deutlich, dass die Fragen der Kenntnisnahme – anders als die Beschwerdeführer dies tun – jedenfalls nicht ohne Blick auf das Fachrecht beantwortet werden können.

Erneut also richten die Beschwerdeführer ihren Angriff gegen Normen, auf die die geltend gemachte Beschwer nicht oder allenfalls sehr partiell zurückgeht.

#### 4. *Zum Gewicht der mit §§ 111 ff. TKG verfolgten Zwecke*

Bevor mit der Prüfung der angegriffenen Normen im Einzelnen begonnen werden kann, ist noch auf einen letzten übergreifenden Grundfehler der Beschwerdeschrift hinzuweisen. Sie trägt dem hohen verfassungsrechtlichen Gewicht der Zwecke, denen die §§ 111 ff. TKG zu dienen bestimmt sind, im Rahmen der Prüfung der verfassungsrechtlichen Rechtfertigung nicht hinreichend Rechnung. Leitthema der angegriffenen Normen ist die staatliche Sicherheitsgewährleistung, d.h. der präventive und repressive Schutz der öffentlichen Sicherheit durch die staatlichen Organe der Strafverfolgung, der Gefahrenabwehr und der Nachrichtendienste. Es handelt sich dabei nicht um irgendwelche Staatsaufgaben, sondern um eine namentlich in den grundrechtlichen Schutzpflichten und im Rechtsstaatsprinzip verankerte Verfassungsaufgabe von hohem Rang, von der die Institution Staat ihre eigentliche und letzte Rechtfertigung herleitet.

BVerfGE 49, 24/56 f.; Möstl, Die staatliche Garantie für die öffentliche Sicherheit und Ordnung, 2002, § 2 (S. 37 ff.).

Besonders eklatant und in offenem Widerspruch zur ständigen Rechtsprechung des Bundesverfassungsgerichts ist die Geringschätzung, die die Beschwerdeführer der Bedeutung der Strafverfolgung entgegenbringen. Bezeichnend ist etwa die Aussage, eine intensivierete Strafverfolgung lasse „ohnehin keinen verbesserten Rechtsgüterschutz erwarten“.

Beschwerdeschrift, S. 28, 52 sowie die im Anhang abgedruckten Auszüge aus der Dissertation des Beschwerdeführers zu 1, namentlich S. 118 ff., 138 ff. der Beschwerdeschrift.

Die diesbezüglichen Aussagen spotten der ständigen Rechtsprechung des Bundesverfassungsgerichts, die den unabweisbaren Bedürfnissen einer wirksamen Strafverfolgung stets hohes Gewicht beigemessen hat und die Aufklärung von Straftaten als einen wesentlichen Auftrag eines rechtsstaatlichen Gemeinwesens ansieht.

Z.B. BVerfGE 100, 131/388 f.; zuletzt etwa BVerfG, Kammerbeschluss vom 6.8.2006 – 2 BvR 1345/03, Abs. 72.

Der der Beschwerdeschrift beigefügte Anhang spricht in diesem Zusammenhang ausdrücklich davon, „diese Ansicht des Bundesverfassungsgerichts“ sei „abzuleh-“

nen“ (S. 119); weiter unten (S. 122) heißt es: „Angesichts dessen muss man dem Bundesverfassungsgericht vorwerfen, falsche Prioritäten zu setzen“.

Würdigt man die Ausführungen der Beschwerdeschrift zur verfassungsrechtlichen Rechtfertigung, so darf nicht aus dem Auge verloren werden, dass diese Ausführungen in ihrem grundlegenden Ausgangspunkt, dem Gewicht der mit den angegriffenen Normen verfolgten Zwecke, nicht auf dem Boden der Rechtsprechung des Bundesverfassungsgerichts stehen.

## II. Zu den angegriffenen Normen im Einzelnen

### 1. § 111 TKG

#### a) Das berührte Grundrecht

Die in § 111 TKG geregelte Pflicht zur Erhebung und Speicherung bestimmter Telekommunikationsbestandsdaten berührt, wie unter I.1. (S. 25 ff.) im Einzelnen dargelegt wurde, im Verhältnis zum datenschutzrechtlich Betroffenen allein das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG), nicht jedoch das Fernmeldegeheimnis (Art. 10 GG).

#### b) Eingriff

Die Pflicht zur Datenerhebung und -speicherung wird durch § 111 TKG statuiert; das Fachrecht der an der Speicherung interessierten Sicherheitsbehörden spielt in diesem Stadium noch keine Rolle und kommt erst später – im Zusammenhang mit dem Abruf und der weiteren Verwendung der Daten (zum diesbezüglichen Verhältnis von Fachrecht und §§ 112 f. TKG siehe oben I.3., S. 39 ff.) – zum Tragen. Soweit überhaupt ein staatlicher Grundrechtseingriff durch die Datenerhebung und -speicherung gegeben ist, ist dieser also jedenfalls § 111 TKG selbst, und nicht dem Fachrecht zuzurechnen.

Vorgelagert ist indes die Frage, ob die in § 111 TKG geregelte Datenerhebung/-speicherung durch Privatunternehmen überhaupt als staatlicher Grundrechtseingriff qualifiziert werden kann. § 111 TKG betrifft das Ausmaß der Erhebung und Speicherung personenbezogener Daten durch private – d.h. selbst nicht unmittelbar grundrechtsgebundene und so zu einem „Eingriff“ in das Recht auf informationelle Selbstbestimmung nicht fähige – Diensteanbieter; um die Kenntniserlangung durch staatliche – d.h. grundrechtsgebundene und zu einem Grundrechtseingriff fähige – Stellen geht es im diesem Stadium gerade noch nicht.

Vgl. hierzu Kühling, K&R 2004, 105/108.

Die Argumente, die die Beschwerdeschrift für einen staatlichen Eingriff durch § 111 TKG ins Feld führt,

Beschwerdeschrift, S. 51, 13 ff.

können nicht überzeugen. So betreffen die von den Beschwerdeführern in Bezug genommenen Aussagen des Bundesverfassungsgerichts zur mittelbaren Eingriffsqualität einer gegenüber dem Diensteanbieter getroffenen Anordnung

BVerfGE 107, 199/313 f. = NJW 2003, 1787/1789.

einen in einem entscheidenden Punkt anders gelagerten Fall: Dort nämlich ging es um die hoheitliche Anordnung einer *Datenübermittlung* durch den Diensteanbieter an den Staat, d.h. um die hoheitliche Anordnung eines Vorgangs, der gerade den Übergang der Daten von der privaten in die staatliche Sphäre anbetrifft, während es im hiesigen Fall allein um die (gesetzliche) Anordnung von Datenverarbeitungsvorgängen geht, die noch ganz in der privaten Sphäre verbleiben. Fehl geht aus diesem Grund auch der Verweis auf die Ausführungen des Bundesverfassungsgerichts zur Eingriffsqualität vorbereitender (der eigentlichen Kenntnisnahme vorgelagerter) Arbeitsschritte,

BVerfGE 100, 313/366.

da die dort gemeinten vorbereitenden Datenaufbereitungsschritte – anders als hier – erneut bereits voll in der staatlichen Sphäre stattfanden. Zu verweisen ist schließlich darauf, dass die Beschwerdeschrift ihr Ergebnis der Bejahung eines Eingriffs nur mit einer Argumentation zu erreichen vermag, die sich bewusst von einer „gegenteiligen Ansicht“ des Bundesverfassungsgerichts (zur Zielwahlsuche) distanziert und diese ablehnt.

BVerfGE 109, 299/327 f., dazu Beschwerdeschrift S. 16 bis 18.

Für die Bejahung eines Grundrechtseingriffs spricht andererseits, dass § 111 TKG, so sehr die von ihm geregelten Datenspeicherungen – im Überschneidungsbereich mit § 95 TKG – von den Unternehmen zumeist ohnehin aus eigenem Interesse vorgenommen werden würden, gleichwohl eine hoheitliche Anordnung dieser Datenspeicherungen darstellt, die das Gesetz ausdrücklich zugunsten eines staatlichen Zweckzusammenhangs vornimmt („für die Auskunftsverfahren nach den §§ 112, 113“) und nunmehr auch insoweit als verpflichtend ausgestaltet, als „diese Daten für betriebliche Zwecke nicht erforderlich sind“. Der Aspekt einer nicht freiwillig und im privaten Interesse erfolgenden, sondern hoheitlich und im öffentlichen Interesse angeordneten Datenverarbeitung indes kann allein mit der Dimension der grundrechtlichen Schutzpflicht nicht adäquat erfasst werden. Nimmt man hinzu, dass die informationelle „Selbstbestimmung“ (d.h. der grundsätzlichen Verfügungsmacht über personenbezogenen Daten) auch durch erzwungene Datenoffenbarungen gegenüber Privaten (und nicht erst durch staatliche Kenntnisnahme) eine Einbuße erfährt, und dass es eben gerade § 111 TKG ist, der diese Datenoffenbarung anordnet, so sprechen gute Gründe auch dafür, trotz fehlender staatlicher Kenntnisnahme bereits von

einem staatlichen Eingriff in das Recht auf informationelle Selbstbestimmung auszu-  
gehen.

So BVerwGE 119, 123/126; Kühling, K&R 2004, 105/108; BerlKommTKG/Kleszczewski, 2006, § 111, Rn. 7 f. Richtig wäre in diesem Zusammenhang auch, dass allein in dem Vertragsschluss mit dem Diensteanbieter keine eingriffsausschließende Einwilligung („Grundrechtsverzicht“) in den gesetzlich angeordneten Datenerhebungsvorgang erblickt werden kann (vgl. BVerwG aaO, S. 127).

Die Frage, ob ein Eingriff gegeben ist, kann aber letztlich offen bleiben. Denn jedenfalls lässt sich dieser Eingriff verfassungsrechtlich rechtfertigen.

### c) Verfassungsrechtliche Rechtfertigung

#### aa) Einschränkung des Grundrechts

Das Recht auf informationelle Selbstbestimmung ist nicht schrankenlos gewährleistet. Der Einzelne muss – auf entsprechender gesetzlicher Grundlage – vielmehr solche Beschränkungen hinnehmen, die durch überwiegende Allgemeininteressen gerechtfertigt sind.

BVerfGE 65, 1/43 f.; BVerfG, Beschluss vom 4.4.2006 – 1 BvR 518/02, Abs. 81.

#### bb) Gewicht des Eingriffs

Ausgangspunkt der Prüfung der verfassungsrechtlichen Rechtfertigung und namentlich der Verhältnismäßigkeit hat die Feststellung zu sein, dass der durch § 111 TKG bewirkte Eingriff – unterstellt, er lässt sich überhaupt als solcher qualifizieren, siehe soeben b., S. 53 ff.) – jedenfalls nur ein Eingriff von sehr geringer Intensität ist. Allen Versuchen der Beschwerdeschrift, aber auch von Teilen der Literatur, die von § 111 TKG statuierte Speicherungspflicht als einen tiefgreifenden oder gar als „besonders schweren“ Grundrechtseingriff zu darzustellen,

Beschwerdeschrift, S. 53 f.; Kühling, K&R 2004, 105/109.

muss von Beginn an entschieden widersprochen werden. Folgende Gründe sind maßgeblich:

- Von vornherein kein relevanter Eingriff kann insoweit vorliegen, als die Daten (auch) in ein öffentliches Teilnehmerverzeichnis eingetragen sind; dann nämlich ist das Recht auf informationelle Selbstbestimmung nicht oder allenfalls geringfügig berührt.

BerIKommTKG/Kleszczewski, 2006, § 111, Rn. 8.

- Keine relevante zusätzliche Beschwer gegenüber dem bereits durch § 95 TKG gegebenen Rechtszustand ergibt sich des Weiteren bezüglich all derjenigen Daten, die das Unternehmen bereits aus eigenem betrieblichem Interesse erheben würde und kraft § 95 TKG auch erheben darf. Mit Ausnahme der besonderen Fallgruppe der Prepaidprodukte

Dazu BVerwGE 119, 123. Selbst hier hat eine vom damaligen Bundesministerium für Wirtschaft und Arbeit am 19. Dezember 2003 durchgeführte Sachstandsabfrage bei den großen Telekommunikationsunternehmen ergeben, dass diese zum Teil jedenfalls bereits aus eigenen betrieblichen Zwecken gleichwohl Daten erheben und speichern (etwa für die Fälle des Auslandsroaming, zu Marketingzwecken etc.).

freilich hat ein Unternehmen ein eigenes Interesse daran, die wesentlichen Grunddaten zur Identifikation ihres Vertragspartners ohnehin zu erheben und zu speichern. Abgesehen von den Prepaidprodukten bewirkt § 111 TKG somit – jedenfalls im Kern – keine nennenswerte zusätzliche Beschwer.

Freilich könnte gefragt werden, ob das Unternehmen jedes Einzelne der in § 111 TKG genannten Daten von sich aus erheben würde; zumindest die wesentlichen Grunddaten würde es aber in jedem Fall erheben.

Die Problematik reduziert sich somit im Wesentlichen darauf, ob der Gesetzgeber auch bezüglich der Prepaidprodukte eine Erhebungs- und Speicherungspflicht anordnen darf.

- Die wesentliche Substanz des von § 111 TKG bewirkten Grundrechtseingriffs ist inzwischen überdies auch gemeinschaftsrechtlich unterlegt und wird dem deutschen Gesetzgeber zwingend vorgegeben. Die Richtlinie zur sog. Vorratsdatenspeicherung

Richtlinie 2006/24/EG vom 15. März 2006, ABl. Nr. L 105/54 ff.

verlangt – so sehr sie in erster Linie auf Verkehrsdaten zugeschnitten ist – in diesem Zusammenhang auch die Speicherung von Telekommunikationsbestandsdaten (Art. 5 Abs. 1 Buchstabe a Nr. 1, Buchstabe b Nr. 1: Teilnehmer und Rufnummer); es ist nicht ersichtlich, dass hierbei für Prepaidprodukte irgendeine Ausnahme gemacht würde. Zwar ist es so, dass die Vorhaltung dieser Daten nicht gerade für die Zwecke

der §§ 112, 113 TKG verlangt wird; auch wird nicht die Speicherung aller von § 111 TKG erfassten Daten verlangt und auch nicht unbedingt die Speicherungsfrist des § 111 Abs. 1 S. 4 TKG; im Einzelnen ist es daher so, dass § 111 TKG hinsichtlich Speicherungszwecken, Datenarten und Speicherdauer durchaus über die Vorgaben der Richtlinie hinausgeht und insoweit noch eigenständigen Eingriffswert behält. Die eigentliche Substanz des Eingriffs – dass nämlich die wesentlichen Bestandsdaten überhaupt systematisch gespeichert und vorgehalten werden müssen –, ist mittlerweile indes nicht mehr dem § 111 TKG zurechenbar, der insoweit nur eine europarechtliche Vorgabe erfüllt.

- Soweit § 111 TKG nach dem Gesagten überhaupt ein eigenständiger Eingriffswert zukommt, ist die Beeinträchtigung des Rechts auf informationelle Selbstbestimmung als geringfügig einzustufen. Hauptgrund hierfür ist, dass es sich bei den von § 111 TKG erfassten Daten um Daten mit geringer Sensibilität und beträchtlichem (entsprechende Eingriffe rechtfertigenden) Sozialbezug handelt. Bereits unter A.III. (S. 16 ff.) ist – im Vergleich mit ähnlichen Datenkategorien (Melderegister, Fahrzeugregister) – gezeigt worden, dass die den Kern des § 111 TKG ausmachende Verknüpfung von Person und Rufnummer (alle anderen Daten dienen nur der näheren Konkretisierung dieser Grundverknüpfung, siehe dazu unten dd. am Ende, S. 67) unter den Bedingungen moderner Kommunikation ein Basisdatum zur Identifikation einer Person und zur Bestimmung seiner kommunikativen Erreichbarkeit darstellt, das denen des Wohnsitzes (Melderegister) oder des Kraftfahrzeuges (Fahrzeugregister), die seit jeher in öffentlichen Registern gespeichert sind, in nichts nachsteht. Die Rufnummer gibt Auskunft darüber, wie (d.h. von welchem Anschluss aus) eine Person mit ihrer Umwelt kommuniziert und ist somit ein Datum mit vergleichsweise hohem Sozialbezug, das gleichsam die grundlegende (tele-)kommunikative Verortung des Einzelnen in Bezug auf seine Umwelt und die Allgemeinheit beschreibt. Ohne Kenntnis der wesentlichen Grunddaten zur Identifikation und Erreichbarkeit einer Person (Wohnsitz, Rufnummer, Fahrzeug etc.) ist effektives Verwalten und namentlich effektive Sicherheitsgewährleistung zum Scheitern verurteilt. Der Gesetzgeber hat daher bereits in der Vergangenheit Regelungen zur systematischen Vorhaltung und auch zur automatischen Abrufbarkeit derartiger Daten ergriffen (MRRG, StVG, siehe oben A.III., S. 16 ff.). Es ist nur folgerichtig, wenn auch die Rufnummer, die jedenfalls unter heutigen Bedingungen zu jenen Basisdaten gehört, deren Kenntnis für den Staat, namentlich für die Sicherheitsgewährleistung unerlässlich ist und die daher planmäßig erhoben und vorgehalten werden müssen, nunmehr vom Gesetzgeber zu jenen Grunddaten gerechnet wird, bzgl. derer eine systematische Speicherungspflicht angeordnet wird.

- Das Gewicht des Eingriffs wird noch zusätzlich dadurch begrenzt, dass allein eine dezentrale private Speicherung angeordnet und nicht ein zentrales staatliches Register angelegt wird. Freilich mag die private Speicherung ihre eigenen Missbrauchsgefahren bergen, denen durch entsprechende Maßnahmen aber auch effektiv begegnet werden kann (vgl. § 95 TKG). Aufs Ganze gesehen dürfte indes kein Zweifel bestehen, dass die gefundene Lösung, die eine staatliche Kenntnisnahme zunächst ausschließt und allein auf die Fälle des im Einzelfall erforderlichen Abrufs (§§ 112 f. TKG) beschränkt, im Vergleich zu der denkbaren Alternative, dass sogleich ein staatliches Register angeordnet wird, das mildere Mittel darstellt. Die Fälle der eigentlich „problematischen“ staatlichen Kenntnisnahme werden so auf das notwendige Maß beschränkt.

- Der von § 111 TKG ausgehende Eingriff ist nicht etwa deswegen von gesteigerter Brisanz, weil er gerade die Telekommunikation betrifft und hierbei in einem möglichen Zusammenhang mit Eingriffen in Art. 10 GG steht.

Die unsaubere Vermengung mit Art. 10 GG-Problemen, die dazu führt, dass die Problematik von Telekommunikationsüberwachungseingriffen gleichsam auf Bestandsdatenfragen abfärbt, dürfte nicht selten der Hauptgrund sein, warum die §§ 111 ff. TKG kritisch betrachtet werden. So verfährt die Beschwerdeschrift, die ja ohnehin von einem Eingriff in Art. 10 GG ausgeht. Dies wird z.B. auch bei Kühling, K&R 2004, 105 ff. deutlich, wo Bestandsdatenabfragen erneut (jedenfalls in bestimmten Konstellationen) als Teilaspekt des Gesamtkomplexes „Eingriff in Art. 10 GG“ erscheinen.

Zum Verhältnis zwischen dem Recht auf informationelle Selbstbestimmung und Fernmeldegeheimnis im Kontext von Bestandsdatenspeicherungen und -abfragen ist bereits oben (I.1., S. 25 ff.) das Nötige gesagt worden. Regelmäßig haben Bestandsdatenabfragen von vornherein keinen Bezug zu irgendwelchen Eingriffen in Art. 10 GG. Die Abfrage der sich „hinter einer Person verbergenden“ Rufnummer (oder umgekehrt) steht in diesen Fällen in keinerlei Zusammenhang mit irgendwelchen Informationen, die Art. 10 GG unterfallen könnten; namentlich ist keinerlei Rückschluss auf Inhalte oder konkrete Umstände einer Telekommunikationsverbindung möglich. Die Abfrage der Rufnummer hat in diesen Fällen – trotz ihres Telekommunikationsbezugs – keinen anderen Eingriffswert als etwa die seit langem vertraute Abfrage des einer Person zuzuordnenden Wohnsitzes (bei dem auch niemand auf die Idee käme, sie allein wegen des theoretischen Bezugs zu Eingriffen in das Postgeheimnis als problematisch anzusehen). Aber selbst wenn es ausnahmsweise so ist, dass Bestandsdatenabfragen tatsächlich der Vorbereitung oder Nachbereitung von Eingriffen in Art. 10 GG dienen, ist es nötig, die jeweiligen Eingriffe sauber auseinanderzuhalten. Die eigentliche Brisanz erhält die – ggf. aus mehreren unterscheidbaren Einzelakten (vorbereitende Bestandsdatenabfrage, Art. 10 GG-Eingriff, nachbereitende Be-

standsdatenabfrage) zusammengesetzte – Gesamtmaßnahme dadurch, dass in ihrem Zentrum mittels Eingriff in Art. 10 GG Verkehrs- oder sogar Inhaltsdaten gewonnen werden. Dieser Eingriff ist denn auch an entsprechende – Art. 10 GG genügende – Eingriffsvoraussetzungen gebunden. Die gesamte Brisanz der Maßnahme ist damit jedoch „abgearbeitet“. Es besteht kein Grund, einer etwa vorbereitenden Bestandsdatenabfrage (Welche Rufnummer hat eine Person?) oder einer etwa nachbereitenden Bestandsdatenabfrage (Wer „steht hinter einer Rufnummer“?) eine irgendwie geartete erhöhte Brisanz deswegen zuzuschreiben, weil zusätzlich auch ein Eingriff in Art. 10 GG stattgefunden hat, dessen Problematik von der entsprechenden (zum Eingriff in Art. 10 GG berechtigenden) gesonderten Befugnisnorm indes bereits vollständig aufgefangen wird.

- Der von der Bestandsdatenspeicherung des § 111 TKG ausgehende Eingriff hat auch nicht etwa deswegen besonderes Gewicht, weil er anonymes Telefonieren unmöglich macht.

Hierzu z.B. BerlKommTKG/Kleszczewski, 2006, § 111, Rn. 5, 10, mit einem Verweis auf Erwägungsgründe der EG-Datenschutzrichtlinie, der sich mittlerweile infolge der EG-Vorratsspeicherungs-Richtlinie freilich erledigt haben dürfte. Siehe auch Beschwerdeschrift, S. 54.

Hierfür ist noch nicht einmal maßgeblich, dass anonymes Telefonieren tatsächlich allenfalls erschwert, nicht aber völlig unmöglich gemacht wird (nach wie vor gibt es ja öffentliche Fernsprengeräte). Entscheidend ist vielmehr, dass nicht ersichtlich ist, dass anonymes Telefonieren – über den allgemeinen Schutz des Rechts auf informationelle Selbstbestimmung, das soeben geprüft wird, sowie den Schutz des Fernmeldegeheimnisses (Art. 10 GG, siehe sogleich) hinausgehend – unter irgendeinem besonderen Schutz des Grundgesetzes stünde. In diesem Zusammenhang gehen auch die Einlassungen der Beschwerdeführer fehl, durch die Erschwerung anonymen Telefonierens werde das Kommunikationsverhalten verändert. Die für ein ungestörtes Kommunikationsverhalten unerlässliche Vertraulichkeit der Telekommunikation schützt das Grundgesetz bereits durch Art. 10 GG, der es unter strengen Voraussetzungen aber auch gestattet, auf Inhalte und Umstände von Telefonaten zuzugreifen und so die Anonymität des Telefonierens aufzuheben.

- Abzulehnen wäre auch eine Argumentation, die dem Eingriff deswegen erhöhtes Gewicht beimäße, weil nach § 111 TKG – „verdachtslos“ und insoweit mit großer „Streubreite“ – Daten von quasi jedermann erhoben und gespeichert werden, auch wenn viele der Betroffenen vielleicht niemals Objekt einer Bestandsdatenabfrage werden, und selbst wenn sie es würden, vielleicht keinerlei Anlass (im Sinne des Begehens einer Straftat oder der Verursachung einer Gefahr) hierfür gegeben haben.

In diese Richtung: Kühling K&R 2004, 105/110.

Zu prüfen ist die Rechtfertigung des durch § 111 TKG bewirkten Eingriffs in die Grundrechte der Beschwerdeführer. Dieser Eingriff wird nicht dadurch schwerwiegender, dass auch andere einen vergleichbaren Eingriff erleiden. Die besondere Beschwerde, dass von den Beschwerdeführern in verdachtsloser Weise Daten erhoben und nunmehr gespeichert werden, ohne dass sie hierfür einen besonderen Anlass geboten hätten, wird bereits durch die Prüfung ihrer individuellen Grundrechte „abgearbeitet“ (genau besehen handelt es sich hierbei um keinen Aspekt der Eingriffstiefe, sondern um die Frage hinreichender Eingriffsvoraussetzungen, siehe dazu unten bei der Verhältnismäßigkeitsprüfung). Eines zusätzlichen Abstellens auf die Streubreite des Eingriffs auch gegenüber anderen bedarf es nicht. Im Gegenteil ist es so, dass die Tatsache, dass die Erhebungs- und Speicherungspflicht des § 111 TKG jedermann – und zwar völlig verdachtslos – trifft, eher ein zusätzliches Indiz dafür ist, dass der damit verbundene Eingriff in das informationelle Selbstbestimmungsrecht ein vergleichsweise geringer ist. Denn je verdachtsloser ein Eingriff ist und je mehr er wirklich unterschiedslos jedermann trifft, umso offensichtlicher ist, dass mit der Datenerfassung als solcher keinerlei Abstempelungs- oder stigmatisierende Wirkung dahingehend verbunden sein kann, dass der Betroffene in sicherheitsrechtlicher Hinsicht etwa besonders „verdächtig“ sein könnte. Die Bestandsdatenerfassung liefert nichts weiter als eine jedermann erfassende Rufnummernliste, die – über die Tatsache hinaus, dass sie die von § 111 TKG geforderten Daten enthält und insoweit bereits in das Recht auf informationelle Selbstbestimmung eingreift – keinerlei zusätzlichen Aussagegehalt und keinerlei zusätzliche negative Auswirkungen auf das Persönlichkeitsrecht (durch Abstempelung, Stigmatisierung etc.) hat.

- Soweit eine besondere Eingriffstiefe deswegen bejaht wird, weil die Zwecke, um derentwillen die Bestandsdatenerfassung nach § 111 TKG erfolgt (dies sind die Zwecke der §§ 112, 113 TKG), angeblich weit gefasst seien

In diese Richtung: Kühling, K&R 2004, 105/109.

so fällt dieses Problem mit der unten noch ausführlicher zu behandelten Fragestellung zusammen, ob die Zwecke der „Vorratsdatenspeicherung“ hinreichend bestimmt konzipiert sind. Im Übrigen ist zweifelhaft, ob die Größe des Kreises der nach §§ 112, 113 TKG Abfrageberechtigten – bei den Datenabfragen geht es ja um gegenüber der Datenspeicherung eigenständige Grundrechtseingriffe – überhaupt für die Tiefe des Eingriffs nach § 111 TKG relevant sein kann. § 111 TKG als solcher regelt alleine, dass bestimmte Bestandsdaten von privaten Unternehmen erhoben und vorgehalten werden müssen; wer im Einzelnen abfrageberechtigt ist, ist eine zweite, erst in §§ 112, 113 TKG geregelte Frage, die für die Eingriffstiefe des § 111 TKG nichts Unmittelbares hergibt.

- Die Eingriffstiefe wird schließlich nicht etwa dadurch erhöht, dass die Datenerfassung heimlich und für den Betroffenen unbemerkt abläufe.

Zu diesem Kriterium: BVerfG vom 4.4.2006 – 1 BvR 518/02, Abs. 113.

Dass von jedem Telefonkunden ausnahmslos bestimmte Daten erhoben und gespeichert werden müssen, ordnet vielmehr das Gesetz in § 111 TKG in einer für jedermann offensichtlichen Weise an; an einer besonderen Heimlichkeit fehlt es insoweit. Etwas anderes mag für den einzelnen Datenabruf gelten. Dieser aber richtet sich nach §§ 112, 113 TKG sowie dem einschlägigen Fachrecht und ist für den hier zu prüfenden § 111 TKG ohne unmittelbare Relevanz.

Für den unmittelbar durch § 111 TKG bewirkten Eingriff kann damit als Teilergebnis festgehalten werden: Es handelt sich nicht um einen schwerwiegenden, sondern allenfalls um einen geringfügigen Eingriff. Vor allem zwei Gründe sind maßgeblich: Erstens, dass sich die Erhebungs- und Speicherungspflicht des § 111 TKG ausschließlich auf vergleichsweise wenig sensible Grunddaten zur Identifikation und Erreichbarkeit einer Person mit hohem Sozialbezug und ohne jeglichen besonderen Aussagewert bezieht, sowie zweitens, dass zunächst gerade keine staatliche Kenntnisnahme, sondern allein eine Speicherung durch solche Unternehmen vorgesehen ist, die diese Daten in aller Regel ohnehin aus eigenem Antrieb speichern würden und dürften.

#### cc) Gewicht der verfolgten Zwecke

Die Regelung des § 111 TKG steht im Dienste der Auskunftsverfahren nach den §§ 112, 113 TKG. Sie möchte die informationelle Basis für die dort geregelten Auskunftersuchen der Sicherheitsbehörden liefern. Ihrem Zweck nach zielt sie somit – wie es bereits die Einordnung in den Dritten Abschnitt „Öffentliche Sicherheit“ nahe legt – auf die Gewährleistung öffentlicher Sicherheit (vgl. auch § 2 Abs.2 Nr. 9 TKG). Die präventive und repressive Gewährleistung öffentlicher Sicherheit aber ist, wie bereits in I.4. (S. 53 f.) dargelegt, eine Verfassungsaufgabe von hohem Rang. Einem Grundrechtseingriff von vergleichsweise geringfügiger Intensität steht auf diese Weise ein wichtiger Gemeinwohlzweck gegenüber.

#### dd) Verhältnismäßigkeit

- (1) Die in § 111 TKG normierte Pflicht zur Vorhaltung bestimmter Telekommunikationsbestandsdaten ist zur Förderung der mit ihr verfolgten Sicherheitszwecke ge-

eignet. § 111 TKG gewährleistet, dass den Sicherheitsbehörden ein Datenpool zur Verfügung steht, auf den sie bei Bedarf – im Rahmen der in §§ 112, 113 TKG geregelten Auskunftsverfahren – zugreifen können. Bei dieser Datensammlung geht es im Kern um die spezifische Verknüpfung von Rufnummer und Person, d.h. um die Identifikation der Person, die hinter einer Rufnummer steht, bzw. umgekehrt um die Frage, welche Rufnummern einer Person zugeordnet sind. Unter A.II. (S. 7 ff.) ist im Einzelnen gezeigt worden, wie wichtig es für die tägliche Praxis der Sicherheitsbehörden ist, auf diese spezifische Datenverknüpfung verlässlich zugreifen zu können. An konkreten Beispielen konnte illustriert werden, zu welchen Ermittlungserfolgen die Bestandsdatenabfrage in den unterschiedlichsten Konstellationen beitragen kann. Nicht zuletzt die sich hieraus ergebende hohe und in den letzten Jahren weiter angestiegene Zahl von automatisierten Anfragen nach § 112 TKG (2005: 3,4 Mio.) belegt eindrucksvoll, wie unverzichtbar der Zugriff auf die nach § 111 TKG bereitzustellenden Daten in der täglichen Praxis der Sicherheitsbehörden ist.

Die Beschwerdeführer stellen die Eignung der Bestandsdatenerfassung speziell im Bereich der Prepaidprodukte mit dem Argument in Frage, dass es unwahrscheinlich sei, dass Kriminelle bei Vertragsschluss die korrekten Daten angäben und dass Prepaidkarten zudem in großem Umfang weitergegeben würden; in diesem Zusammenhang wird auch bemängelt, dass § 95 Abs. 4 TKG es nur erlaube, nicht aber vorschreibe, dass die Daten bei Vertragsschluss durch Vorlage eines amtlichen Ausweises verifiziert würden.

Beschwerdeschrift, S. 53, 55.

Die genannten Einwände vermögen die Geeignetheit der Bestandsdatenerfassung – auch im Prepaidbereich – nicht in Frage zu stellen. Zunächst ist zu bedenken, dass es für das Kriterium der Geeignetheit im Rahmen der Verhältnismäßigkeitsprüfung bereits ausreicht, dass die Maßnahme für die Zielerreichung überhaupt förderlich ist; nicht aber ist es nötig, dass das Ziel auch in jedem Einzelfall vollständig erreicht wird. Es schadet demnach nicht, wenn eine Bestandsdatenabfrage in einzelnen Fällen nicht sogleich einen verwertbaren Treffer erzielt (weil die Angaben unzutreffend sind oder Karten weitergegeben wurden; auch hier freilich werden sich häufig weitere Ermittlungsansätze ergeben), wenn andererseits in vielen anderen Fällen sehr wohl verwertbare Resultate erreicht werden. Die Geeignetheit eines insgesamt nützlichen Datenerfassungssystems wird nicht dadurch in Frage gestellt, dass es Einzelnen gelingen mag, sich durch Manipulationen oder auf sonstige Weise einer korrekten Erfassung zu entziehen.

So auch Kühling, K&R 2004, 105/109; s.a. Thiede, Kriminalistik 2004, 104/106 (mit dem Beispiel, dass etwa auch die Pflicht zur Anbringung eines Kfz-Kennzeichens nicht dadurch in Frage gestellt werden kann, dass Kfz-Kennzeichen im Einzelfall verschmutzt (nicht lesbar) oder manipuliert sein könnten).

Hinzu kommt, dass auch speziell im Prepaidbereich die Praxis der Datenerfassung keineswegs so wenig verlässlich ist, wie von den Beschwerdeführern suggeriert. Viele Anbieter lassen sich die Ausweise vorlegen; auch wo dies nicht der Fall ist oder auch nicht der Fall sein kann (z.B. Verkauf über Internet), findet im Zuge des Versandes der Karte an die angegebene Adresse eine gewisse automatische Identitätskontrolle statt; insgesamt ist das Interesse der Diensteanbieter, die richtige Identität ihrer Prepaidkunden zu kennen, angesichts auch dort aufgetretener Missbrauchsfälle, die zu Mehrkosten bei den Diensteanbietern führen (Manipulationen der SIM-Karten; Anrufe an Mehrwertdienste aus dem Ausland), in letzter Zeit eher gestiegen. Auch im Bereich der Prepaidprodukte kann die Erfolgsquote richtiger Abfragen laut Angaben von Sicherheitsbehörden daher auf mindestens 90 % geschätzt werden. Freilich ist richtig, dass die Dunkelziffer unrichtiger Angaben steigt, je mehr die betroffenen Personen tatsächlich dem engeren Kern krimineller Kreise angehören. Gerade auch aus Sicherheitskreisen wird daher kritisiert, dass etwa die Ausweispflicht beim Kauf von Guthabekarten noch nicht normiert worden ist und daher fiktive Angaben ermöglicht werden.

Thiede, Kriminalistik 2004, 104/108.

Dennoch wird die Bestandsdatenerfassung auch im Prepaidbereich von den Sicherheitsbehörden als ein nützliches und unverzichtbares Instrument eingeschätzt.

Beleg hierfür ist nicht zuletzt auch die Tatsache, dass es den am Gesetzgebungsverfahren Beteiligten bei Erlass des neuen TKG ein so wichtiges Anliegen war, die nach der Entscheidung des BVerwG (E 119, 123) entstandene Lücke im Prepaidbereich nunmehr verlässlich zu schließen, vgl. BT-Drucks. 15/2316, S. 95, 124; 15/2345, S. 8.

Zu bedenken ist hierbei, dass, selbst soweit die Angaben z.B. wegen zwischenzeitlicher Weitergabe der Karten im Einzelfall nicht mehr richtig sein sollten, die über die Bestandsdatenabfrage mögliche Kenntnis des ursprünglichen Karteninhabers doch einen wertvollen Ansatz für weitere Ermittlungen liefern kann. Was dagegen das Problem bereits ursprünglich falscher Angaben anbelangt, so wird man den Umstand, dass der Gesetzgeber bislang von einer über § 95 Abs. 4 TKG hinausgehenden Pflicht zur Ausweisvorlage abgesehen hat, gerade unter Verhältnismäßigkeitsgesichtspunkten schwerlich angreifen können. Freilich wird insoweit eine gewisse Verlässlichkeitslücke offen gelassen; sie zu schließen, wäre andererseits nur mittels eines zusätzlichen Eingriffs in das informationelle Selbstbestimmungsrecht der Betroffenen (durch Statuierung einer Ausweisvorlagepflicht) möglich. Man wird es dem

Gesetzgeber nicht anlasten können, wenn er bislang davon abgesehen hat, eine Ausweispflicht zu statuieren.

(2) Die in § 111 TKG normierte Bestandsdatenvorhaltung ist zur Erreichung der mit ihr verfolgten Zwecke auch *erforderlich*. Ein milderer Mittel, das einen ebenso verlässlichen und lückenlosen Zugriff auf die Bestandsdaten aller Telefonkunden möglich machen würde, ist nicht ersichtlich.

So auch Kühling, K&R 2004, 105/109; BerlKommTKG/Kleszczewski, 2006, § 111, Rn. 10.

Namentlich die Aussparung der Kunden von Prepaidprodukten würde die Bestandsdatenerfassung als lückenhaft und in ihrer Effektivität geschwächt erscheinen lassen. Ein wichtiger, und an Bedeutung eher noch zunehmender Anteil der Telefonkunden würde, ohne dass eine besondere Schutzwürdigkeit ersichtlich wäre, von der Wertung des Gesetzgebers ausgenommen, dass die Bestandsdaten grundsätzlich aller Telefonteilnehmer für die Zwecke der Sicherheitsbehörden zur Verfügung stehen sollen. Die systematische Erfassung der Telefonbestandsdaten hat für die Sicherheitsbehörden gegenüber dem Zugriff auf anderweitige Datenbestände auch einen unverzichtbaren Mehrwert (mit der Konsequenz, dass die Erforderlichkeit der Bestandsdatenspeicherung nicht mit dem Argument angegriffen werden kann, es gebe bereits andere Register, auf die die Sicherheitsbehörden zugreifen könnten): Nur mithilfe der Telekommunikationsbestandsdaten lässt sich die für die tägliche Ermittlungsarbeit so wichtige Verknüpfung von Rufnummer und „hinter ihr stehender“ Person bzw. Person und ihr zugeordnete Rufnummer herstellen. Namentlich das Melderegister (vgl. § 2 MRRG) gibt hierüber keine Auskunft, schon gar nicht bzgl. des Bereichs der Mobiltelefonie. Unter A.II. (S. 9) ist gezeigt worden, dass es in der Tat genau jene Verknüpfung (und hierbei in 95 % der Fälle um die Frage nach der „hinter einer Rufnummer stehenden“ Person) ist, die den spezifischen Zweck der Bestandsdatenerfassung ausmacht. Der Vorwurf der Beschwerdeschrift, die Daten würden als allgemeinen Adressregister missbraucht, ist unrichtig.

Beschwerdeschrift, S. 79, 82 (siehe dazu bereits oben A.II. S. 9). Im Übrigen könnte selbst insoweit die Erforderlichkeit der Bestandsdatenerfassung nicht in Frage gestellt werden, denn diese Bestandsdaten sind häufig aktueller – und insofern zur Zielerreichung geeigneter – als jene der Meldebehörden (Rieß, RDV 1996, 109/111), siehe dazu auch die Beispielsfälle 3 und 10 oben unter A.II., S. 12 ff.

(3) Die in § 111 TKG geregelte Bestandsdatenvorhaltung ist schließlich in Anbetracht der mit ihr verfolgten Zwecke auch *angemessen* und *zumutbar*.

Wie hier: BerlKommTKG/Kleszczewski, 2006, § 111, Rn. 10 (unter Ausklammerung des Problems der „Vorratsdatenspeicherung“ für bestimmte Zwecke, das auch hier gesondert behandelt wird, siehe unten ee., S. 68 ff.).

Die von der Beschwerdeschrift und von einzelnen Stimmen der Literatur vertretene Gegenansicht, § 111 TKG sei unverhältnismäßig, beruht auf der unrichtigen Prämisse, bei der Bestandsdatenspeicherung stünden ein fragwürdiger Nutzen bzw. vage Hoffungen auf mehr Sicherheit einem schwerwiegenden Grundrechtseingriff gegenüber.

Beschwerdeschrift, S. 52, 54; Kühling, K&R 2004, 105/110.

Das Gegenteil ist richtig: Der Nutzen von Bestandsdatenabfragen, ihre Unverzichtbarkeit für Zwecke effektiver Sicherheitsgewährleistung, steht, wie in A.I. und II. (S. 2 ff.) dargelegt, außer Zweifel; Bestandsdatenabfragen können auf eine jahrzehntelange Praxis zurückblicken und haben in jüngerer Zeit aufgrund des geänderten Kommunikationsverhaltens erneut an Bedeutung gewonnen. Selbst im Bereich der Prepaidprodukte sieht sich, wie oben bei der „Geeignetheit“ erläutert, der Nutzen der Bestandsdatenerfassung allenfalls im Einzelfall geschwächt, keineswegs jedoch grundsätzlich in Frage gestellt. Dieser enormen Praxisbedeutung der Bestandsdatenerfassung steht ein Grundrechtseingriff gegenüber, der nach den oben unter bb. (S. 53 ff.) gemachten Ausführungen allenfalls als Eingriff von geringer Intensität eingestuft werden kann; alle Versuche, ihn als schwerwiegenden Eingriff darzustellen, gehen fehl. Einem offensichtlichen und in der Praxis bewährten Nutzen steht also ein nur geringfügiger Eingriff gegenüber, der angesichts dieses Gewichtsverhältnisses als ohne weiteres angemessen erscheinen muss.

Die von § 111 TKG aufgeworfene Zumutbarkeitsproblematik lässt sich auf die Frage zuspitzen, inwieweit es dem Staat erlaubt ist, zur Erfüllung bestimmter Verwaltungszwecke (namentlich der Sicherheitsgewährleistung) die systematische Erfassung und Vorhaltung wenigstens der grundlegenden Daten zur Identifikation und Erreichbarkeit des Einzelnen vorzuschreiben. Die Praxiserfahrung lehrt, dass ohne die verlässliche Verfügbarkeit derartiger grundlegender Identifikationsdaten ein effektives Verwalten und namentlich eine effektive Sicherheitsgewährleistung unmöglich sind. Bereits seit langem gibt es denn auch entsprechende Register (insbesondere das Melderegister, das Fahrzeugregister, siehe oben A.III., S. 16 ff.). Die einer Person zugeordnete Rufnummer aber ist – wie bereits mehrfach angesprochen – ein Grunddatum zur Identifikation und Erreichbarkeit einer Person, das unter den Bedingungen moderner Kommunikation den altbewährten Kriterien des Wohnsitzes oder des Fahrzeugs an Bedeutung in keiner Weise nachsteht, ja sie an Bedeutung z.T. eher noch übertrifft. Es ist nur folgerichtig, wenn auch bezüglich der Telekommunikationsbestandsdaten

eine systematische Datenerfassung für Zwecke der Sicherheitsgewährleistung (hier nicht in Gestalt eines öffentlichen Registers, sondern einer privaten Vorhaltung) vorgeschrieben wird. Es handelt sich um Daten ohne gesteigerten, über die bloße Identifikation und Rufnummernzuordnung hinausgehenden Persönlichkeitsbezug, mithin um personenbezogene Daten verhältnismäßig geringer Schutzwürdigkeit. Zugleich geht es um Daten mit hohem Sozialbezug, die die grundlegende (tele-)kommunikative Verortung und Erreichbarkeit des Einzelnen in Bezug auf seine Umwelt betreffen. Es wäre überspitzt und würde jegliche effektive Sicherheitsgewährleistung lähmen, wenn man den Staat selbst bezüglich derartiger grundlegender Identifikationsdaten darauf verweisen würde, diese Daten nicht systematisch und ohne weiteres abrufbar vorzuhalten, sondern in jedem Einzelfall mühsam zu ermitteln. Freilich ist unbestreitbar, dass, je sensibler die betroffenen Daten sind, umso mehr auch an bestimmte Eingriffsschwellen und tatbestandliche Voraussetzungen geknüpfte Datenermittlungsbefugnisse im Einzelfall verlangt werden können. Jedenfalls für die einfachen Grunddaten zu Identifikation und Erreichbarkeit des Einzelnen müssen bereits durch den Gesetzgeber, d.h. generell angeordnete und der Last zur Einzelfallermittlung enthobene Register und Datenspeicher zulässig sein. Die den Kern des § 111 TKG ausmachende Verknüpfung von Rufnummer und Person betrifft ein solches Grunddatum bzgl. dessen eine systematische Vorhaltung als zumutbar erscheint.

Die Bestandsdatenerfassung nach § 111 TKG ist auch nicht deswegen unverhältnismäßig, weil sie sich „verdachtslos“ und „mit großer Streubreite“ gegen quasi jedermann richtet, unabhängig davon, ob jemals gerade in Bezug auf ihn Ermittlungen der Sicherheitsbehörden nötig sein werden.

Vgl. die dahingehende Kritik bei Kühling, K&R 2004, 105/110.

Freilich kann nicht übersehen werden, dass, was die verfassungsrechtliche Zulässigkeit von Informationseingriffen der Sicherheitsbehörden anbelangt, die Frage nach den zu fordernden Eingriffs- und Verdachtsschwellen einerseits sowie die Frage nach dem Kreis der Betroffenen bzw. einer hinreichenden Nähebeziehung des Betroffenen zum jeweiligen Untersuchungszweck andererseits eine ganz herausragende Rolle spielt.

Vgl. z.B. BVerfGE 100, 313; 107, 299; 110, 33; 113, 348; BVerfG, Beschluss vom 4.4.2006 – 1 BvR 518/02.

Dennoch wäre es verfehlt, im hiesigen Fall aus Gründen der Streubreite und Verdachtslosigkeit ein Monitum ableiten zu wollen. Folgende Gründe sind maßgeblich:

- Zu bedenken ist erstens, dass sich die genannten Entscheidungen des Bundesverfassungsgerichts durchgehend auf die Frage der Ausgestaltung von Befugnisnormen für sicherheitsbehördliche Informationseingriffe im Einzelfall beziehen. Hier indes geht es um eine unmittelbar durch Gesetz angeordnete Datenvorhaltungspflicht durch Private. Es stellt sich hierbei schon im Ausgangspunkt die Frage, ob sich die gewonnenen Leitlinien überhaupt übertragen lassen: Der Aspekt der Verdachtslosigkeit und Streubreite erscheint beim sicherheitsbehördlichen Einzelfallhandeln von vornherein problematischer als bei einer abstrakt-generellen (d.h. naturgemäß auf große „Streubreite“ angelegten und nicht unter dem Vorbehalt einer zusätzlichen Eingriffsschwelle stehenden) gesetzlichen Anordnung. Pendant der vom Bundesverfassungsgericht behandelten Fallgruppen ist allenfalls der sicherheitsbehördliche Zugriff auf Bestandsdaten nach §§ 112, 113 TKG: Hierfür wird man in der Tat eine einzelfallbezogene Eingriffsvoraussetzung fordern können; auch hat dieser Eingriff keinerlei Streubreite mehr (da es um eine gezielte Anfrage geht). Für die vorgelegte Anordnung des Zur-Verfügung-Haltens von Daten durch Private, die gerade noch keine behördliche Kenntnisnahme impliziert, dagegen passen die genannten Kategorien nicht.

- Es muss zweitens grundsätzlich hinterfragt werden, inwieweit sich die Kriterien des Verdachts oder der Nähebeziehung in Bezug auf staatliches Informationshandeln verallgemeinern lassen. Sicherlich: Soweit es in bestimmten (präventiven oder repressiven) Ermittlungssituationen bereits einen auf einen bestimmten Personenkreis eingrenzbaren Verdacht gibt, wird man aus Gründen der grundrechtlichen Schonung sagen können, dass sich Ermittlungseingriffe, soweit möglich, vorrangig gegen den Verdächtigenkreis richten sollen. Eine darüber hinausgehende Regel, dass sich der Staat seine Informationen stets nur beim „Verdächtigen“ oder beim „Störer“ holen dürfte, gibt es dagegen nicht (man denke an die drittbezogene Zeugenpflicht im Strafprozess oder daran, dass es in Situationen, in denen erst herausgefunden werden muss, ob und ggf. wo eine Gefahr besteht, einen Störer noch gar nicht gibt). Naheliegender ist schon, dass sich der Staat seine Informationen dort holt und holen darf, wo er mit hinreichender Wahrscheinlichkeit erwarten kann, dass Informationen und Auskünfte gegeben werden können, die der Staat für seine Aufgabenerfüllung benötigt. Es ist deswegen kein Zufall, sondern Konsequenz der Eigenart von Informationseingriffen, dass sowohl die Datenschutzgesetze (z.B. § 13 Abs. 1 BDSG) als auch viele polizeigesetzliche Grundnormen zur Datenerhebung (z.B. Art. 31 Abs. 1 BayPAG) Informationseingriffe gestatten, soweit sie zur Aufgabenerfüllung der jeweiligen Behörde erforderlich sind. Informationseingriffe sind zu vielgestaltig, um durchgehend mit Kriterien wie „Verdacht“, „Nähebeziehung“ etc. auf den Nenner gebracht werden zu können. Trifft nun der Gesetzgeber in § 111 TKG in abstrakt-genereller Form die Wertung, dass Sicherheitsbehörden des verlässlichen Zugriffs auf bestimmte grundlegende Telekommunikationsbestandsdaten für ihre Arbeit be-

dürfen und dass es hierfür unerlässlich ist, dass die Diensteanbieter die entsprechenden Daten vollständig erheben und vorhalten, so ist hiergegen aus grundrechtlicher Sicht nichts zu erinnern, solange nur dargetan werden kann, dass diese Datenvorhaltung für die Aufgabenerfüllung der Sicherheitsbehörden erforderlich ist. Dies aber ist der Fall, denn die Bestandsdatenvorhaltung etwa von vornherein auf bestimmte Verdächtige zu beschränken, ist nicht möglich; auf die Bestandsdatenvorhaltung hingegen ganz zu verzichten und die Sicherheitsbehörden durchgehend auf entsprechende Ermittlungen der Bestandsdaten im Einzelfall (ohne das in §§ 111, 112 TKG statuierte System der vollständigen Vorhaltung und des automatisierten Abrufs) zu verweisen, würde ihre Arbeit erheblich erschweren. Kann aber die Erforderlichkeit einer jedermann verdachtslos betreffenden Datenvorhaltung aufgezeigt werden, so ist es nicht statthaft, ihre Verhältnismäßigkeit aus Gründen der Streubreite in Frage zu stellen.

- Entscheidend ist drittens: Die Aussagen des Bundesverfassungsgerichts zu Verdachtsschwellen und zu fordernden Nähebeziehungen beziehen sich ausnahmslos auf Fallkonstellationen, in denen es um die Rechtfertigung schwerwiegender Grundrechtseingriffe ging (typischerweise Telefonüberwachungen oder aber z.B. die Rasterfahndung). Das Bundesverfassungsgericht hat stets gesehen, dass sich seine Aussagen zu Verdachtsgraden und Nähebeziehungen auf Eingriffe von geringer Intensität nicht übertragen lassen, sondern insoweit überzogen wären. So verlangt der Verhältnismäßigkeitsgrundsatz nach seiner Rechtsprechung nur für „intensive Grundrechtseingriffe“, dass diese erst von bestimmten Verdachts- oder Gefahrenstufen an vorgesehen werden dürfen; und auch die Aussage des Rasterfahndungsbeschlusses, dass eine fehlende Nähebeziehung durch erhöhte Wahrscheinlichkeitsanforderungen zu kompensieren sei, bezog sich nur auf „Eingriffe von erheblichem Gewicht“.

BVerfGE 100, 313/383 f.; 109, 279/350 ff.; 110, 33/68; 113, 348/382 ff.; BVerfG, Beschluss v. 4.4.2006 – 1 BvR 518/02, Abs. 137, 140.

Im hiesigen Fall dagegen geht es, wie unter bb. (S. 53 ff.) im Einzelnen aufgezeigt, um einen Eingriff von verhältnismäßig geringer Intensität. Maßgebend hierfür war insbesondere, dass es sich bei den Bestandsdaten um sehr grundlegende Identifikationsdaten ohne besonderen Persönlichkeits-, dafür aber mit hohem Sozialbezug handelt, die auf unterer Schutzwürdigkeitsstufe anzusiedeln sind. Bezüglich derart grundlegender Identifikationsdaten trifft das Gesetz auch an anderer Stelle die Wertung, dass ihre „verdachtslose“ Vorhaltung für eine effektive Sicherheitsgewährleistung unumgänglich und daher einwandfrei ist (siehe oben zum Melderegister, Fahrzeugregister u.ä.). Eine ähnliche Wertung lässt sich auch dem Polizeirecht entnehmen: So ist gegenüber der Polizei jedermann zur Auskunft über seine Identitätsdaten verpflichtet (z.B. Art. 12 BayPAG), und auch die sog. Schleierfahndung kann, weil es

dort allein um die Identitätsfeststellung geht und so gesehen eine nur „geringfügige Grundrechtsbeeinträchtigung vorliegt“,

BayVerfGH 56, 28/43 ff., siehe auch BayVerfGH vom 7.2.2006 – Vf. 69-VI-04 unter 5a. (dort anders zur schwerer wiegenden Durchsuchung).

als sog. „verdachts- und ereignisunabhängige“ Kontrollbefugnis ausgestaltet werden. Die Wertung der genannten Beispiele kann verallgemeinert werden und hat dabei auch vor der Verfassung Bestand: Es gibt einen gewissen Kreis Identifikationsdaten, bzgl. derer der Gesetzgeber anordnen darf, dass sie den Sicherheitsbehörden für deren Zwecke grundsätzlich (d.h. nicht erst ab gewissen Schwellen oder bzgl. bestimmter Verdächtiger) zur Verfügung stehen, weil ohne Rückgriff auf diese Basisdaten eine effektive Sicherheitsgewährleistung schlechthin nicht möglich erscheint. Telekommunikationsbestandsdaten gehören zu diesem Kreis für die Arbeit der Sicherheitsbehörden unerlässlicher Basisdaten, die verdachtslos vorgehalten werden dürfen, um dann von den Sicherheitsbehörden – freilich stets nach Maßgabe einer Erforderlichkeitsprüfung im konkreten Einzelfall – nach §§ 112, 113 TKG i. V. m. dem jeweils einschlägigen Fachrecht abgerufen zu werden.

- Hinzu kommt ein Letztes: Gerade die – jedermann unterschiedslos treffende – völlige Verdachtslosigkeit der Datenvorhaltung nach § 111 TKG hat (wie in bb., S. 57 f., bereits gezeigt) zur Folge, dass mit der Einstellung in den entsprechenden Datensatz nicht die geringste abstempelnde oder stigmatisierende Wirkung verknüpft ist; niemand kann ernstlich behaupten, dass aus der Tatsache, dass über jemanden Bestandsdaten gespeichert sind, irgendwelche Schlüsse negativer Art gezogen werden können. Gerade weil der Eingriff verdachtslos ist, ist er auch von so geringer Intensität. Forderte man für Bestandsdatenerfassungen irgendeine Verdachtsschwelle oder Nähebeziehung zu irgendwelchen Straftaten oder Gefahrenlagen, wäre dies grundlegend anders; die Datensammlung hätte dann ihre Harmlosigkeit verloren. Die Forderung nach Verdachtsschwellen (bzw. die Klage über ihr Fehlen) hat insofern etwas Zirkuläres an sich, weil sie mithilfe einer vermeintlich rechtsstaatlicheren Eingriffsschwelle den Eingriff überhaupt erst richtig gravierend macht.

Als verhältnismäßig erweist sich § 111 TKG nicht nur, wie bis hierher gezeigt, in seiner grundsätzlichen Regelungsstruktur, sondern auch in seinen Einzelheiten. Zwar ist der Kreis der nach § 111 TKG zu erfassenden Daten im Zuge der Novellierung des Jahres 2004 geringfügig erweitert worden (z.B. Geburtsdatum; Anschrift des Festnetzanschlusses; Datum des Vertragsbeginns). Ziel dieser Erweiterung indes ist es gewesen, die Verlässlichkeit der Datenabfragen nach § 112 TKG zu steigern und insbesondere unnötige Nachfragen (nach erstmaligem Fehlschlag oder zur Erlangung zusätzlicher Kenntnisse) im manuellen Verfahren nach § 113 TKG (nach denen diese Informationen bereits bisher zu erlangen waren) zu vermeiden, nicht soll-

ten den Sicherheitsbehörden neuartige Ermittlungsmöglichkeiten verschafft werden. Nach wie vor geht es allein um die Verknüpfung von Rufnummer und Person, die nunmehr nur treffsicherer ausgestaltet worden ist. Der näheren Konkretisierung dieser Grundverknüpfung (in zeitlicher Hinsicht) dient auch die Aufnahme des Datums des Vertragsschlusses in den Kreis der vorzuhaltenden Daten: Denn das grundlegende Identifikationsmerkmal der Rufnummer bedarf, um aussagekräftig zu sein, stets der zeitlichen Einordnung dahingehend, für welchen Zeitraum dieses Identifikationsmerkmal zugetroffen hat. Gerade auch in dieser zeitlichen Dimension ist die Basisverknüpfung Person-Rufnummer für die Sicherheitsbehörden von besonderer Bedeutung, wie das Fallbeispiel 4 (oben unter A.II., S. 13) deutlich macht. In diesen – zeitlichen – Kontext gehört schließlich auch die Pflicht zur Datenspeicherung bis zum Ende des Kalenderjahres nach Vertragsende (§ 111 Abs. 1 S. 4 TKG); auch diese ist als verhältnismäßig anzusehen. Sie ist nämlich Reaktion auf in der Praxis zutage getretene Schwierigkeiten, bei denen Ermittlungen von Strafverfolgungsbehörden daran gescheitert waren, dass Vertragsverhältnisse mittlerweile beendet worden waren und eine Aufklärung der „hinter einer Rufnummer stehenden“ Person daher nicht mehr möglich war. Hat man diese Schwierigkeiten vor Augen und bedenkt man andererseits, dass die einjährige Speicherung bereits zuvor ohnehin zulässig war (jetzt § 95 Abs. 3 TKG, zuvor § 4 Abs. 3 TDSV), so erscheint die Dauer der Speicherungspflicht nicht als übermäßig.

BT-Drucks. 15/2316, S. 95.

ee) Insbesondere zur „Vorratsdatenspeicherung“ und zur hinreichenden Bestimmtheit ihrer Zwecke

§ 111 TKG wird sowohl in der Beschwerdeschrift wie von Stimmen der Literatur mit dem Vorwurf angegriffen, er normiere eine unzulässige „Vorratsdatenspeicherung“ oder komme einer solchen immerhin nahe.

Beschwerdeschrift, S. 52 ff., Kühling, K&R 2004, 105/108 f.; BerlKommTKG/Kleszczewski, 2006, § 111, Rn. 9; Simitis, BT-Ausschussdrucksache 15(9)969 vom 5.2.2004, S. 222/224 f.

Angespielt wird hierbei auf das Diktum des Bundesverfassungsgerichts im Volkszählungsurteil, die Sammlung nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbareren Zwecken sei mit dem aus dem Recht auf informationelle Selbstbestimmung folgenden Gebot bereichsspezifischer und präziser Bestimmung des Verwendungszwecks durch den Gesetzgeber nicht zu vereinbaren.

BVerfGE 65, 1/46.

Das Verbot der Datenspeicherung „auf Vorrat“ darf nicht missverstanden werden. Jede Speicherung von Daten in Dateien zum Zweck ihrer späteren Abrufbarkeit bei entsprechender Erforderlichkeit ist eine Speicherung „auf Vorrat“. Jede zum Abruf bereit stehende Datei ist ein Vorratsspeicher; Vorratsspeicherung ist keineswegs eine Besonderheit. Das bloße Wort von der Vorratsspeicherung ist somit für die Frage der Reichweite des Grundrechtseingriffs ohne Aussagekraft.

Dies hat auch der Beschwerdeführer zu 1) an anderer Stelle selbst eingeräumt: Breyer, Die systematische Aufzeichnung und Vorhaltung von Telekommunikations-Verkehrsdaten für staatliche Zwecke in Deutschland, 2005, S. 113 f.; s.a. Thiede, Kriminalistik 2004, 104/106 (auch zum Folgenden).

Sollten die Beschwerdeführer mit „Vorratsspeicherung“ die Konstellation meinen, dass der Staat, anstelle selbst eine Datei anzulegen, Unternehmen dazu verpflichtet, auch jenseits ihrer betrieblichen Zwecke (und insoweit „auf Vorrat“) Daten für den Staat vorzuhalten, so bedeutet dies in datenschutzrechtlicher Hinsicht (anders in Bezug auf die Unternehmen) im Gegenteil sogar, dass der entsprechende Eingriff in das Recht auf informationelle Selbstbestimmung ein geringerer ist, als dies bei einer unmittelbar staatlichen Datenvorhaltung der Fall wäre.

Die eigentliche und allein maßgebliche Stoßrichtung des „Vorratsspeicherungsverbots“ ist somit die Anforderung einer hinreichend bestimmten Festlegung des Verwendungszwecks der betroffenen Daten:

- Eine Einbuße an Präzision des Verwendungszwecks hat § 111 TKG gegenüber der vormaligen Rechtslage nicht dadurch bewirkt, dass er nunmehr die Datenvorhaltung ausdrücklich und von vornherein (neben den betrieblichen Zwecken des § 95 TKG) auch für staatliche Zwecke vorschreibt.

Anders aber offenbar Kühling, K&R 2004, 105/109.

Im Vergleich zur früheren Rechtslage, die zunächst allein von für betriebliche Zwecke erhobenen Daten ausging und diese dann im Wege der gesetzlich zugelassenen Zweckänderung auch den staatlichen Auskunftsverfahren zugänglich machte, ist es im Gegenteil ein rechtsstaatlicher Gewinn, wenn das Gesetz in § 111 TKG nunmehr ausdrücklich regelt, dass die zu erhebenden Bestandsdaten von vornherein auch in einem staatlichen Zweckzusammenhang stehen.

- § 111 TKG ist mit „Daten für Auskunftsersuchen der Sicherheitsbehörden“ überschrieben, er steht im Abschnitt „öffentliche Sicherheit“ und er verweist auch in

seinem Text (Abs. 1 S. 1) ausdrücklich auf die Auskunftsverfahren nach §§ 112 und 113 TKG, für die die Daten vorzuhalten sind. Hinsichtlich der Zweckbestimmung weist die „Vorratsdatenspeicherung“ somit ein recht klares Profil aus: Die Daten stehen für Zwecke der öffentlichen Sicherheit zur Verfügung. Öffentliche Sicherheit ist ein klar bestimmbarer Zweck, ein Rechtsbegriff, der insbesondere im Polizeirecht in jahrzehntelanger Rechtsprechung konkretisiert worden ist und klare Konturen aufweist: Er umfasst den Schutz der Unversehrtheit der elementaren Rechtsgüter des Einzelnen und der Allgemeinheit (Rechtsgüterschutz) sowie die Unversehrtheit der Rechtsordnung (Rechtsdurchsetzung); bei alledem hat dieser Schutz eine präventive (im Polizei- und Ordnungsrecht, im Recht der Nachrichtendienste) und eine repressive (im Straf- und Ordnungswidrigkeitsrecht) Seite. So umrissen lässt sich die Aufgabe der Gewährleistung öffentlicher Sicherheit auch trennscharf von anderen Feldern der Staatsverwaltung (Wohlfahrtspflege, Steuerverwaltung etc.) abgrenzen, die an der Sicherheitsaufgabe allenfalls insoweit teilnehmen, als ihre Tätigkeit ggf. auch die Verfolgung von Ordnungswidrigkeiten einschließen kann.

Vgl. Möstl, Die staatliche Garantie für die öffentliche Sicherheit und Ordnung, 2002, S. 119 ff., S. 147 ff.

Innerhalb dieses seinerseits schon hinreichend klar konturierten Feldes schränkt § 112 Abs. 2 TKG für das automatisierte Auskunftsverfahren den Kreis zulässiger Behörden und Abfragezwecke noch näher ein, indem es im Einzelnen aufzählt, welche Behörden für ggf. welche (alle oder nur einen Teil ihrer) Aufgaben auskunftsbe-rechtigt sind. Es ist nicht ersichtlich, wie gegen diese Regelungstechnik der Vorwurf der Unbestimmtheit erhoben werden kann.

So auch BerlKommTKG/Kleszczewski, 2006, § 111, Rn. 9; zu § 90 Abs. 3 TKG a.F. auch Trute, in Trute/Spoerr/Bosch, TKG, 2001, § 90, Rn. 17; anders allerdings Simitis, BT-Ausschussdrucksache 15(9)949, S. 225. Freilich mag der Verweis auf „Strafverfolgungsbehörden“ oder auf „Polizeivollzugsbehörden“ „für Zwecke der Gefahrenabwehr“ ein in der Sache breites Aufgabenfeld bezeichnen (dazu sogleich), nicht jedoch kann gesagt werden, dieses Aufgabenfeld sei nicht klar abgrenzbar.

Breiter ist die Zugriffsberechtigung bei § 113 TKG geregelt. Auch hier jedoch verlässt die Regelung in keiner Weise das oben umrissene Feld präventiver und repressiver Sicherheitsgewährleistung. Wenn etwa auch die ordnungsbehördliche „Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung“ umfasst wird, so weitet dies die Zugriffsberechtigung gegenüber § 112 TKG zwar aus, nicht jedoch kann gesagt werden, dass es sich in der deutschen Rechtstradition nicht um einen klar umreißbaren Zweck handelte (das Polizei- und Ordnungsrecht weist eine Vielzahl von Aufgaben- und Befugnisnormen auf – und zwar in Bezug auf Eingriffe, die den hier zu Erörtern-den an Intensität weit übersteigen –, die allein an diese Zweckbestimmung anknüp-

fen). Gleiches gilt für die Einbeziehung des Gesamtfeldes der Verfolgung von Ordnungswidrigkeiten: Freilich können hier viele Behörden zugriffsberechtigt sein, dies aber gerade nicht im Rahmen ihrer gesamten Aufgabenerfüllung, sondern nur, soweit sie mit der Verfolgung von Ordnungswidrigkeiten befasst sind, was voraussetzt, dass ein entsprechendes Verfahren eingeleitet worden ist. Es ist nicht nachvollziehbar, wie hier davon gesprochen werden kann, die Verwendungszwecke verlören sich „ins Unbestimmbare“; es ist auch nicht ersichtlich, dass es in der Praxis irgendwelche Abgrenzungsschwierigkeiten bzgl. der Frage gäbe, welche Behörden in welchen Situationen abfrageberechtigt seien.

A.A. BerlKommTKG/Kleszczewski, 2006, § 111, Rn. 9; die Verwendungszwecke mögen weit sein (dazu sogleich), nicht aber sind sie unbestimmbar.

- Freilich kann nicht bestritten werden, dass es eine Vielzahl von Behörden und Aufgaben ist, für die die Daten nach § 111 TKG vorgehalten werden. Erstens aber ist die Frage der Vielzahl möglicher Verwendungszwecke scharf von der Frage ihrer hinreichenden Bestimmtheit zu unterscheiden: Die Zwecke mögen in der Sache vielfältig sein, sie sind aber durchwegs klar bestimmbar. Zweitens ist es so, dass die Vielzahl der Verwendungszwecke, die (jedenfalls über § 113 TKG) letztlich das Gesamtfeld öffentlicher Sicherheitsgewährleistung umfasst, nur die Kehrseite der geringen Schutzwürdigkeit der Daten ist, um die es bei § 111 TKG geht. Wenn, wie dargelegt worden ist, in einer mit dem Verhältnismäßigkeitsprinzip in vollem Einklang stehenden Weise gesagt werden kann, dass es einen Kreis an Grunddaten zur Identifikation und Erreichbarkeit einer Person gibt, die so wenig schutzwürdig sind, dass der Gesetzgeber legitimerweise die Wertung treffen darf, diese Daten den Sicherheitsbehörden für ihre Zwecke grundsätzlich zugänglich zu machen, so ist eine engere und präzisere Beschreibung zulässiger Zwecke der Datenvorhaltung von Verfassung wegen nicht geboten. Die Frage der zulässigen Verwendungszwecke kann nicht gelöst werden von der Schutzwürdigkeit der Daten, um die es geht. Telekommunikationsbestandsdaten sind, wie dargelegt, einerseits so wenig schutzwürdig und andererseits für die staatliche Sicherheitsgewährleistung so wichtig, dass sie der Gesetzgeber den Sicherheitsbehörden nach Maßgabe des Erforderlichkeitsprinzips generell zur Verfügung stellen darf. Dann aber muss es auch zulässig sein, die Zwecke in der Form zu beschreiben, wie dies der Gesetzgeber getan hat.

ff) Zitiergebot

Eingriffe in das Recht auf informationelle Selbstbestimmung unterfallen nicht dem Zitiergebot des Art. 19 Abs. 1 S. 2 GG. Da das Recht auf informationelle Selbstbe-

stimmung im Schwerpunkt in Art. 2 Abs. 1 GG verankert ist, dessen Gewährleistung von vornherein nur in den Grenzen der verfassungsmäßigen Ordnung besteht, ist dies auch folgerichtig.

Dazu Simitis in: ders. (Hrsg.), Kommentar zum Bundesdatenschutzgesetz, 5. Aufl. 2003, § 1, Rn. 102 ff.

d) Teilergebnis

Das Recht auf informationelle Selbstbestimmung wird durch § 111 TKG nicht verletzt.

2. § 112 TKG

a) Das berührte Grundrecht

Durch das in § 112 TKG geregelte automatisierte Auskunftsverfahren wird, wie oben in I.1. (S. 25 ff.) dargelegt, in Bezug auf den datenschutzrechtlich Betroffenen ausschließlich das Recht auf informationelle Selbstbestimmung, nicht jedoch das Fernmeldegeheimnis berührt.

b) Eingriff (einschließlich: Zurechenbarkeit und Intensität des Eingriffs)

Dass es einen Eingriff in das Recht auf informationelle Selbstbestimmung darstellt, wenn eine Sicherheitsbehörde in dem in § 112 TKG geregelten Verfahren um Auskunft über Telekommunikationsbestandsdaten nachsucht und diese über die Bundesnetzagentur erhält, kann nicht zweifelhaft sein.

„Auf einem anderen Blatt“ steht allerdings die Frage, inwieweit dieser Eingriff überhaupt dem § 112 TKG zurechenbar ist. Bereits unter I.3. (S. 39 ff.) – worauf hier verwiesen sei – ist im Einzelnen aufgezeigt worden, dass § 112 TKG nicht als eine isolierte und abschließende Befugnisnorm zur Bestandsdatenauskunft verstanden werden darf, sondern stets im Zusammenspiel mit dem jeweils einschlägigen Fachrecht der ersuchenden Behörde (StPO, Polizeigesetze, BVerfSchG etc.) gesehen werden muss. § 112 TKG regelt unmittelbar grundsätzlich allein die Rechtsverhältnisse zwischen ersuchender Behörde, Bundesnetzagentur und Telekommunikationsunternehmen sowie zwischen Telekommunikationsunternehmen und Kunden (dies sind die beiden spezifisch telekommunikationsrechtlichen Rechtsverhältnisse), nicht jedoch das „sicherheitsrechtliche“ Rechtsverhältnis zwischen Sicherheitsbehörde und

datenschutzrechtlich Betroffenen, dessen Regelung vielmehr dem jeweils einschlägigen Fachrecht vorbehalten ist. Die eigentliche Befugnisnorm zur Erhebung des personenbezogenen Telekommunikationsbestandsdatums durch die Sicherheitsbehörde ergibt sich folglich aus dem jeweils einschlägigen Fachgesetz (§§ 161, 163 StPO; Art. 31 Abs. 1 BayPAG oder ähnliche Normen der anderen Polizeigesetze; § 8 Abs. 1 BVerfSchG oder ähnliche Normen der Nachrichtendienstesetze usw.), nicht dagegen aus § 112 TKG. Dem Fachgesetz bleibt es daher vorbehalten, die genaueren Voraussetzungen und Modalitäten (vor allem auch datenschutzrechtlicher Folgefragen: Mitteilung, Auskunft, weitere Verwendung etc.) der Datenerhebung zu regeln. § 112 TKG tritt zu dieser fachrechtlichen Befugnisnorm nur hinzu und schafft – flankierend – die telekommunikationsrechtlichen Voraussetzungen dafür, dass die nach Fachrecht zulässige Datenabfrage auch erfolgreich ist, indem sie erstens eine telekommunikationsrechtliche Pflicht der Unternehmen statuiert, die entsprechenden Daten für einen automatisierten Abruf bereitzuhalten (§ 112 Abs. 1 S. 4 TKG) sowie zweitens ein über eine zentrale Stelle (die Bundesnetzagentur) ablaufendes, bundesweit funktionstüchtiges und alle relevanten Unternehmen einschließendes Verfahren bereitstellt. Der von dem Gesamtvorgang „Auskunft über Bestandsdaten“ ausgehende Grundrechtseingriff ist damit nur sehr beschränkt überhaupt dem § 112 TKG zurechenbar. Die eigentliche Befugnisnorm – und damit die Entscheidung über die Zulässigkeit der Datenerhebung – kommt von anderswo (dem Fachrecht) her; der solchermaßen vom Fachrecht ermöglichte und ihm zurechenbare Eingriff wird durch § 112 TKG nur ergänzt und verstärkt, indem telekommunikationsrechtlich gewährleistet wird, dass die Datenerhebung, die nach Fachrecht zulässig ist, auch tatsächlich funktionieren kann. Nur ein Teil des Eingriffs ist also § 112 TKG zurechenbar; auch nur ein Teil der verfassungsrechtlichen Rechtfertigung lastet folglich „auf seinen Schultern“.

Der im Zuge der Auskunftserteilung stattfindende Grundrechtseingriff – zumal, soweit er dem § 112 TKG überhaupt zuzurechnen ist – ist erneut als Eingriff von nur geringer Intensität einzustufen. Maßgebend ist erneut vor allem, dass es bei den von §§ 111, 112 TKG erfassten Bestandsdaten um grundlegende Identifikationsdaten mit schwacher Persönlichkeitsrelevanz und hohem Sozialbezug geht, die innerhalb des Rechts auf informationeller Selbstbestimmung auf unterer Schutzwürdigkeitsstufe anzusiedeln sind (insoweit kann auf die Ausführungen zu § 111 TKG verwiesen werden, siehe 1.c.bb., S. 53 ff.). Nur folgende Aspekte sind (im Vergleich zu § 111 TKG) von zusätzlicher Bedeutung:

- Der im Zuge des § 112 TKG erfolgende Eingriff ist im Vergleich zu § 111 TKG insofern von einem Stück zusätzlicher Beschwer gekennzeichnet, als es nunmehr – auf der Stufe des konkreten Auskunftersuchens – erstmals zu einer staatlichen Kenntnisnahme kommt. Diese zusätzliche Beschwer muss dadurch aufgefangen

werden, dass diese Kenntnisnahme an eine zusätzliche Befugnisnorm (des Fachrechts i. V. m. § 112 TKG) gebunden wird, die nunmehr (anders als die generelle gesetzliche Speicherungsanordnung bei § 111 TKG) auch eine einzelfallbezogene Eingriffsvoraussetzung statuieren muss. Soweit die von der staatlichen Kenntnisnahme im Einzelfall ausgehende zusätzliche Beschwer von entsprechenden Eingriffsvoraussetzungen aufgefangen wird (dazu im Einzelnen bei der verfassungsrechtlichen Rechtfertigung), kann im Übrigen indes nicht davon gesprochen werden, bei § 112 TKG finde ein tiefgreifenderer Grundrechtseingriff als bei § 111 TKG statt. Vielmehr bezieht sich der Eingriff auf die gleichen – wenig schutzwürdigen – Daten wie der nach § 111 TKG. Ganz im Gegenteil fällt eingriffsmindernd ins Gewicht, dass von § 112 TKG nur ein Teil des Eingriffs ausgeht, während seine prinzipielle Rechtfertigung dem Fachrecht obliegt.

- Der besondere Aspekt, dass Maßnahmen nach § 112 TKG heimlich und für den Betroffenen unbemerkt durchgeführt werden, hat jedenfalls nicht das gleiche Gewicht wie in anderen Konstellationen. Zwar misst das Bundesverfassungsgericht dem Umstand der Heimlichkeit grundsätzlich eingriffserhöhende Bedeutung zu.

Z.B. BVerfG, Beschluss vom 4.4.2006 – 1 BvR 518/02, Abs. 113.

Diese Aussagen des Bundesverfassungsgerichts beziehen sich jedoch regelmäßig auf Maßnahmen außergewöhnlicher Art und hoher Intensität (Art. 10 GG-Eingriffe, Rasterfahndung). Auf Fälle wie den hiesigen, bei dem es um alltägliche Eingriffe von nur geringer Intensität geht, lassen sich diese Aussagen nicht ohne weiteres übertragen. Je mehr der Gesetzgeber durch eine Norm wie den § 112 TKG, mit dem ein häufig benötigtes Verfahren zur automatisierten Auskunftserteilung geschaffen wird, in typisierender Weise die Wertung vorwegnimmt, dass festgelegte Basisdaten einem abgegrenzten Kreis von Behörden nach Maßgabe bestimmter Kriterien (hier des Erforderlichkeitskriteriums) grundsätzlich zur Verfügung stehen, umso weniger kann dem Umstand Gewicht beigemessen werden, dass der einzelne Datenabruf unbemerkt abläuft.

Vgl. insoweit die Wertung der §§ 19a Abs. 2 Nr. 3, 33 Abs. 2 Nr. 4 BDSG (hierzu Mallmann in Simitis [Hrsg.], Kommentar zum Bundesdatenschutzgesetz, 5. Aufl. 2003, § 19, Rn. 45 f., § 33, Rn. 78 ff.), wonach eine Mitteilung entbehrlich sein kann, wenn der Datenverarbeitungsvorgang gesetzlich vorgesehen ist.

- Als tendenziell eingriffsmindernd im Vergleich zu § 111 TKG wirkt es sich aus, dass Maßnahmen nach § 112 TKG regelmäßig keinerlei Streubreite (im Sinne des Miterfasstseins Dritter) aufweisen, sondern eine auf eine bestimmte Rufnummer oder Person gemünzte spezifische Auskunft betreffen (zur Frage, inwieweit das Streubreitenkriterium überhaupt Relevanz hat siehe 1.c.bb., S. 57 f.). Etwas anderes kann allein in Bezug auf – bislang rechtlich und technisch noch nicht mögliche – Abfragen

mittels Ähnlichenfunktion oder unvollständigen Abfragedaten gelten, auf die gesondert einzugehen sein wird (unten c.dd., S. 87 ff.).

### c) Verfassungsrechtliche Rechtfertigung

Auch hinsichtlich der verfassungsrechtlichen Rechtfertigung kann weitgehend auf die zu § 111 TKG gemachten Ausführungen (oben 1 c.) verwiesen werden. Die maßgeblichen Verhältnismäßigkeitserwägungen sind bereits dort angestellt worden. Vor allem – dies ist der eigentliche Kern der hier entscheidenden Verhältnismäßigkeitsfrage – ist dort im Einzelnen aufgezeigt worden, dass der Gesetzgeber in Bezug auf die von §§ 111, 112 TKG erfassten Telekommunikationsbestandsdaten legitimerweise die Wertung treffen darf, dass diese – aufgrund ihrer geringen Schutzwürdigkeit einerseits und ihrer hohen Bedeutung für die Arbeit der Sicherheitsbehörden andererseits – für die Zwecke der Sicherheitsbehörden grundsätzlich zur Verfügung stehen. Das automatisierte Abrufverfahren des § 112 TKG ist nichts weiter als die angemessene Konsequenz der bereits in § 111 TKG getroffenen Grundentscheidung für diese grundsätzliche Verfügbarkeit der Daten. Nur auf Einzelfragen zur Ausgestaltung des § 112 TKG muss an dieser Stelle gesondert eingegangen werden:

#### aa) Zu den Eingriffsvoraussetzungen

Die Beschwerdeführer rügen, § 112 TKG sehe keine Eingriffsschwelle vor.

Beschwerdeschrift, S. 79, 82.

Dieser Angriff ist unberechtigt.

Hinzuweisen ist zunächst darauf, dass es gemäß der in I.3 (S. 39 ff.) entwickelten und soeben (b., S. 72 ff.) erneut dargelegten Aufgabenverteilung zwischen Fachrecht und § 112 TKG schon gar nicht die Aufgabe des § 112 TKG ist, die maßgebliche Eingriffsschwelle für den Bestandsdatenzugriff zu formulieren. Die eigentliche datenschutzrechtliche Befugnisnorm – im Rechtsverhältnis zum betroffenen Bürger – muss vielmehr vom jeweiligen Fachrecht der ersuchenden Behörde zur Verfügung gestellt werden. Dort – und nicht in § 112 TKG – sind die maßgeblichen Eingriffsvoraussetzungen zu regeln. Derartige fachrechtliche Befugnisnormen sind auch durchwegs vorhanden; beispielhaft zu nennen sind §§ 161, 163 StPO für den Bereich der Strafverfolgung, § 21 Abs. 1 BPolG, Art. 31 Abs. 1 BayPAG für den Bereich des präventiven Polizeirechts und § 8 Abs. 1 BVerfSchG für den nachrichtendienstlichen Bereich. Überwiegend stellen diese Normen – insoweit auf einer Linie mit § 112 Abs. 2 TKG

(siehe sogleich) – zumindest darauf ab, dass die Datenerhebung für die Erfüllung der jeweiligen Aufgaben der Sicherheitsbehörde „erforderlich“ sein muss.

Das Erforderlichkeitskriterium ist auch in §§ 161, 163 StPO unausgesprochen selbstverständlich mitenthaltend, siehe Karlsruher Kommentar/Wache, StPO, 5. Aufl. 2003, § 161, Rn. 12, § 163, Rn. 11.

Hinzu kommt für den besonders praxisrelevanten Bereich der Strafverfolgung die strafprozessuale Eingriffsschwelle, dass strafprozessuale Ermittlungen stets nur bei bestehendem Anfangsverdacht in Bezug auf eine bereits begangene Straftat zulässig sind. Wollen die Beschwerdeführer geltend machen, diese Eingriffsvoraussetzungen seien ungenügend oder trügen Bestandsdatenabfragen nicht, so ist dies jedenfalls keine Rüge, die gegen § 112 TKG vorgebracht werden könnte.

Die Bedeutung des § 112 TKG beschränkt sich darauf, die fachrechtliche Befugnisnorm durch Statuierung eines von der Bundesnetzagentur koordinierten funktionsfähigen Verfahrens sowie einer Pflicht der Unternehmen, Daten für einen automatisierten Abruf in diesem Verfahren bereitzuhalten, zu flankieren. Zu diesem Zweck normiert § 112 Abs. 2 TKG eine zusätzliche Eingriffsvoraussetzung, die zu der jeweiligen fachrechtlichen Befugnisnorm ergänzend hinzutritt: Er verlangt, dass die Bestandsdatenauskunft zur Erfüllung der gesetzlichen Aufgaben der Behörde erforderlich sein müssen. Dieses telekommunikationsrechtliche Erforderlichkeitskriterium liegt zwar sachlich weitgehend auf einer Linie mit den Eingriffsvoraussetzungen des Fachrechts (die z.B. im strafprozessualen Bereich – Verdachtskriterium! – indes auch darüber hinausgehen können), es muss rechtstechnisch im Sinne einer zusätzlichen und anders gelagerten Eingriffsvoraussetzung nichtsdestoweniger von der fachrechtlichen Befugnisnorm unterschieden werden. Die fachrechtliche Befugnisnorm legitimiert die Datenerhebung gegenüber dem betroffenen Bürger, die telekommunikationsrechtliche Eingriffsvoraussetzung dagegen bestimmt, wann die Sicherheitsbehörden von dem Verfahren nach § 112 TKG Gebrauch machen dürfen und die Unternehmen sowie die Bundesnetzagentur in diesem Rahmen zur Datenbereithaltung und -übermittlung verpflichtet sind; nur mittelbar wird hierdurch zugleich der Eingriff gegenüber dem Bürger mitgestaltet und vertieft. Legt man die so umrissene – begrenzte – Funktion des Erforderlichkeitskriteriums des § 112 Abs. 2 TKG zugrunde, so muss dieses als verfassungsrechtlich einwandfrei eingestuft werden, denn es ist dem Bestandsdaten einer Vielzahl unterschiedlicher Sicherheitsbehörden zur Verfügung stellenden Gesetzgeber des Telekommunikationsgesetzes schlechthin unmöglich, ein anderes Kriterium als das der Erforderlichkeit zu formulieren. Ins Einzelne gehende Eingriffsschwellen kann, wenn überhaupt, allein der jeweilige Fachgesetzgeber formulieren, weil diese auf die spezifische Befugnisstruktur der jeweiligen Fachbehörde zugeschnitten sein müssen. Der Telekommunikationsgesetzgeber, der

sein automatisiertes Verfahren vielerlei Behörden mit je unterschiedlicher Befugnisstruktur öffnet, kann allein ein allgemein formuliertes Erforderlichkeitskriterium statuieren, das letztlich auf die Regelungen des jeweiligen Fachrechts verweist. Mehr muss er auch nicht: Denn er trifft nicht die abschließende Entscheidung über die Zulässigkeit der Bestandsdatenabfrage. Er tut nichts weiter, als den Fachbehörden unter der Voraussetzung der Erforderlichkeit einen Datenbestand zu öffnen. Die Entscheidung darüber, ob die Fachbehörde auf diesen Datenbestand zugreifen darf, kann und muss der Fachgesetzgeber treffen.

So verwundert es auch nicht, dass auch in vergleichbaren Fällen des Zur-Verfügung-Stellens eines automatisierten Abrufverfahrens für eine Vielzahl an Behörden in dem die jeweilige Datei regelnden Gesetz stets nur das Erforderlichkeitskriterium normiert ist: vgl. z.B. § 8 BayMeldeDÜV, § 35 Abs. 1 StVG, § 24c Abs. 3 KWG.

Entscheidend ist schließlich auch folgende Überlegung: Selbst wenn § 112 TKG als eine abschließende Befugnisnorm in Bezug auf den Eingriff in das informationelle Selbstbestimmungsrecht anzusehen wäre und wenn folglich die gesamte Last der verfassungsrechtlichen Rechtfertigung auf dem Erforderlichkeitskriterium des § 112 Abs. 2 TKG ruhte, wäre gegen dieses Erforderlichkeitskriterium aus verfassungsrechtlicher Sicht nichts einzuwenden. Zwar ist es richtig, dass die Suche nach hinreichenden Verdachts- und Gefahrenschwellen bzgl. sicherheitsbehördlicher Informationseingriffe in der Rechtsprechung des Bundesverfassungsgerichts eine große Rolle spielt. Bezogen haben sich die entsprechenden Judikate indes stets auf Grundrechtseingriffe von hoher Intensität (namentlich Art. 10 GG-Eingriffe, Rasterfahndung etc.). Nur für derart intensive Grundrechtseingriffe hat das Bundesverfassungsgericht gefordert, dass diese aus Verhältnismäßigkeitsgründen grundsätzlich erst ab der Schwelle bestimmter Verdachts- oder Gefahrenstufen zulässig sein dürfen.

BVerfGE 100, 313/383 f.; 109, 279/350 ff.; 110, 33/68; 113, 348/382 ff.; BVerfG v. 4.4.2006 – 1 BvR 518/02, Abs. 137, 140.

Stets einbegriffen ist dabei der Vorbehalt, dass für Eingriffe von nur geringer Intensität auch allgemeiner formulierte Eingriffsvoraussetzungen zulässig sein können, dass also gerade nicht für jeden staatlichen Informationseingriff ganz bestimmte Gefahren- oder Verdachtsstufen gefordert werden können. Dass für gewöhnliche Informationseingriffe das Erforderlichkeitskriterium ausreicht, entspricht ständiger – und insoweit auch unbeanstandet gebliebener – Gesetzgebungspraxis. Deutlich wird dies nicht zuletzt daran, dass auch die jeweiligen für Bestandsdatenabfragen einschlägigen Befugnisnormen des Fachrechts (typischerweise die dort jeweils statuierten informationellen Generalklauseln) auf genau dieses Erforderlichkeitskriterium abstellen. Dies ist auch keineswegs als „bloße Verlegenheitslösung“ zu betrachten. Informationsbe-

schaffung ist ihrer Natur nach typischerweise eine Hilfs- und Vorbereitungsaufgabe für die jeweiligen gesetzlichen Verwaltungsaufgaben einer Behörde; Informationsgewinnung dient regelmäßig der jeweiligen Hauptaufgabe der Behörde, indem sie die informationelle Basis für die Erledigung der jeweils übertragenen Aufgaben liefert (im Bereich der Gefahrenabwehr etwa bedarf es hinreichender Informationen, um überhaupt erst jene Gefahrenprognose anstellen zu können, auf deren Basis dann erst Gefahrenbeseitigungseingriffe möglich werden, mithilfe derer die Behörde ihre Gefahrenabwehraufgabe erfüllt). Die Voraussetzung, dass Informationserhebungen für die Erledigung der einer Behörde zugewiesenen Aufgaben erforderlich sein muss, ist demgemäß – jedenfalls für Eingriffe geringer Intensität – als die „natürliche“ und dem informationellen Bereich angemessene Tatbestandsstruktur anzusehen. Es ist nur folgerichtig, dass sowohl das Datenschutzrecht (§ 13 Abs. 1 BDSG) als auch z.B. die Polizeigesetze (§ 21 Abs. 1 BPolG, Art. 31 Abs. 1 BayPAG) in ihren jeweiligen Grundnormen zur Datenerhebung auf genau jenes Erforderlichkeitskriterium abstellen.

Mörtl, Die staatliche Garantie für die öffentliche Sicherheit und Ordnung, 2002, S. 232.

Das Erforderlichkeitskriterium des § 112 Abs. 2 TKG fügt sich in diesen Rahmen voll und ganz ein. Es geht bei § 112 TKG um einen Eingriff von geringer Intensität, der Daten betrifft, die so wenig schutzwürdig sind, dass sie für die Arbeit der Sicherheitsbehörden grundsätzlich zur Verfügung gestellt werden dürfen. Es ist verfassungsrechtlich einwandfrei, den Zugriff auf solchermaßen für die Arbeit der Sicherheitsbehörden zur Verfügung stehende Daten allein an das Kriterium der Erforderlichkeit für die sicherheitsbehördliche Aufgabenerfüllung zu binden.

Der Tatbestandsstruktur des § 112 TKG kann auch nicht vorgeworfen werden, sie sei zu unbestimmt (siehe bereits oben S. 69 ff.).

So aber Beschwerdeschrift, S. 80.

Freilich müssen Eingriffe in das Recht auf informationelle Selbstbestimmung der Vorgabe des Bundesverfassungsgerichts gerecht werden, dass die Voraussetzungen und Grenzen des Eingriffs vom Gesetzgeber bereichsspezifisch, präzise und normenklar geregelt werden müssen.

BVerfGE 65, 1/44, 46; 100, 313/359.

Die diesbezüglichen Anforderungen aus dem rechtsstaatlichen Bestimmtheitsgebot dürfen sich indes nicht in Widerspruch zu dem setzen, was das Verhältnismäßigkeitsprinzip als ausreichend ansieht. Wenn das Verhältnismäßigkeitsprinzip die Wer-

tung trägt, dass Telekommunikationsbestandsdaten dem Zugriff der Sicherheitsbehörden für die Zwecke ihrer jeweiligen Aufgaben nach Maßgabe eines bloßen Erforderlichkeitsprinzips grundsätzlich geöffnet werden dürfen, so kann dieses Ergebnis nicht mithilfe des Bestimmtheitsgebots konterkariert werden. Infolgedessen muss zwischen der Breite der zulässigen Eingriffsvoraussetzungen und -zwecke einerseits und ihrer hinreichenden Bestimmtheit unterschieden werden. Das Auskunftsverfahren des § 112 TKG mag hinsichtlich der Vielzahl der erfassten Behörden und der Fülle ihrer Aufgaben sowie der Weite des Erforderlichkeitskriteriums ein breites Anwendungsfeld haben. Dies freilich ist nichts weiter als die Kehrseite der Verhältnismäßigkeitserwägung, dass die Daten so wenig schutzwürdig sind, dass sie einem entsprechend breiten Anwendungsfeld zur Verfügung gestellt werden dürfen. „Auf einem anderen Blatt“ steht die Frage, ob dieses Anwendungsfeld hinreichend bestimmt umrissen worden ist. Auch ein breites Anwendungsfeld kann hinreichend scharfe Konturen haben. So verhält es sich bei § 112 TKG. Hier werden zum einen die erfassten Behörden im Einzelnen aufgezählt; an der eindeutigen Bestimmbarkeit des Berechtigtenkreises kann keinerlei Zweifel bestehen. Sodann wird auf ihren gesetzlichen Aufgabenkreis verwiesen, der aus dem jeweiligen Fachrecht zweifelsfrei abgelesen werden kann. Schließlich wird ein Erforderlichkeitskriterium begründet, das in der deutschen Rechtslehre und -praxis einen klaren Bedeutungsgehalt hat. Ein – freilich breites – Anwendungsfeld wird so gesehen durchgehend mit der nötigen Präzision umrissen.

Wie hier: BerlKommTKG/Kleszczewski, 2006, § 111, Rn. 9; zu § 90 Abs. 3 TKG a.F. auch Trute, in Trute/Spoerr/Bosch, TKG, 2001, § 90, Rn. 17; a.A.: Simitis BT-Ausschussdrucksache 15(9)949, S. 225.

Fehl geht schließlich die Einlassung der Beschwerdeführer (S. 79), dem § 112 TKG fehle es an einer Subsidiaritätsklausel. Zunächst ist schon nicht recht klar, woraus sich ein solches Erfordernis in verfassungsrechtlicher Hinsicht ergeben sollte. Zudem fungiert das ausdrücklich statuierte Erforderlichkeitsprinzip als eine Art „Subsidiaritätsklausel“, weil sie nicht erforderliche, d.h. auch auf milderem Wege mögliche Informationsgewinnungen verbietet. Des Weiteren ist der Vorwurf, § 112 TKG werde als allgemeine Adressauskunft missbraucht, unzutreffend (vgl. bereits A.II., S. 9). Schließlich könnte selbst eine Verwendung als Adressauskunft unter dem Erforderlichkeitsprinzip rechtfertigbar sein, wenn z.B. die Daten nach §§ 111, 112 TKG aktueller als diejenigen des Melderegisters wären.

So Rieß, RDV 1996, 109/111, siehe auch Fallbeispiel 3 unter A.II., S: 12.

bb) Zur Frage der Benachrichtigung bzw. von Auskunftsrechten Betroffener

Die Beschwerdeführer rügen, dass in § 112 TKG keine zumindest nachträgliche Benachrichtigung Betroffener über Bestandsdatenabfragen vorgesehen ist, sondern dass § 112 TKG (v.a. in Absatz 1 S. 6 und Absatz 4 S. 5 und 6) im Gegenteil geradezu verhindern, dass der Betroffene Kenntnis über Bestandsdatenabfragen erlangen könne.

Beschwerdeschrift, S. 80, 83.

Angespielt wird hierbei auf eine Rechtsprechung des Bundesverfassungsgerichts, die es in der Tat wiederholt als aus grundrechtlichen Gründen erforderlich angesehen hat, den Betroffenen über stattgefundene Informationseingriffe Mitteilung zu machen, damit diese ggf. (zumindest nachträglichen) Rechtsschutz suchen könnten. Hierbei kommt neben oder in Verbindung mit dem durch den Informationseingriff betroffenen Grundrecht (hier: Recht auf informationelle Selbstbestimmung; in der Rechtsprechung des BVerfG haben v.a. Art. 10 GG und Art. 13 GG eine Rolle gespielt) auch die Garantie effektiven Rechtsschutzes nach Art. 19 Abs. 4 GG zum Tragen.

Z.B. BVerfGE 100, 313/361, 397 ff.; 109, 279/363 ff.

Auf dieses Vorbringen ist zunächst zu erwidern, dass sich der Angriff – mit § 112 TKG – auf den falschen Prüfungsgegenstand bezieht. Bereits unter I.3. (S. 39 ff.) ist bzgl. des Verhältnisses von § 112 TKG und dem jeweiligen Fachrecht der betroffenen Sicherheitsbehörde im Einzelnen aufgezeigt worden, dass die Frage, inwieweit dem Betroffenen Mitteilung über Bestandsdatenabfragen zu machen ist oder inwieweit er diesbezüglich Auskunftsrechte hat, in gesetzessystematisch einwandfreier Weise kein Regelungsgegenstand des § 112 TKG ist, sondern sinnvoll und auf die spezifischen Bedürfnisse des jeweiligen Rechtsgebiets abgestimmt nur vom jeweils zuständigen Fachgesetzgeber geregelt werden kann.

Trute, in Trute/Spoerr/Bosch, TKG, 2001, § 89, Rn. 55; BeckTKG-Komm/Büchner 2. Aufl. 2000, § 89, Rn. 45; BeckTKG-Komm/Bock, 3. Aufl. 2006, § 113, Rdnr. 9; Wuermeling/Felixberger, CR 1997, 595/560.

Die Frage, ob und wann dem Betroffenen Mitteilungen gemacht werden können, kann schon deswegen sinnvollerweise nur im Fachrecht entschieden werden, weil sie sich nicht für alle Sicherheitsbehörden und für die je unterschiedlichen Ermittlungssituationen einheitlich beantworten lässt. Regelungen zu Mitteilungspflichten oder Auskunftsrechten enthält das Fachrecht auch in großer Zahl.

Vgl. dazu bereits oben I.3, S. 39 ff. Soweit Bestandsdatenabfragen zur Vorbereitung oder Nachbereitung von Eingriffen in Art. 10 GG erfolgen, ist die Benachrichtigung Betroffener bereits über die im Zusammenhang mit dem jeweiligen Art. 10 GG-Eingriff speziell normierten Mitteilungspflichten gewährleistet (§ 101 StPO, Art. 34 Abs. 5 BayPAG). Ansonsten bestehen überwiegend keine speziellen Benachrichtigungspflichten, vielmehr fügen sich die Betroffenenrechte in die in dem jeweiligen Rechtsgebiet allgemein bestehenden Regelungen über Auskunftsrechte, Mitteilungen in Bezug auf Ermittlungsmaßnahmen etc. ein; typischerweise besteht – in gewissen Grenzen – ein Auskunftsanspruch jedenfalls über gespeicherte Daten (z.B. Art. 48 BayPAG, § 15 BVerfSchG, §§ 491, 495 StPO, ansonsten § 19 BDSG); im Rahmen der StPO geht die Frage nach Mitteilung und Auskunft im Übrigen im allgemeinen Verfahrensgang auf (Mitteilung von der Einstellung des Verfahrens, § 170 Abs. 2 S. 1 StPO, ansonsten die allgemeinen Verfahrens- und Akteneinsichtsrechte z.B. § 147 StPO). Siehe auch Gramlich in: Manssen (Hrsg.), Telekommunikations- und Multimediarecht, § 90, Rn. 24.

Wenn das TKG Regelungen enthält, die es erschweren, dass der Bürger Kenntnis von Bestandsdatenabfragen erhält (§ 112 Abs. 1 S. 6 TKG [keine Kenntnisnahme der Unternehmen], § 112 Abs. 4 S. 5 TKG [Protokolldaten nur für Zwecke der Datenschutzkontrolle]), so darf dies nicht als Absage an ggf. bestehende fachrechtliche Auskunftsansprüche gewertet werden. Maßgebend für diese Regelungen sind vielmehr zwei Gründe: Zum einen gilt es zu verhindern, dass von den Akteuren, die im TKG näher geregelt sind, zusätzliche Gefahren für den Datenschutz ausgehen; folglich wird verhindert, dass die Telekommunikationsunternehmen Kenntnis von § 112 TKG-Abfragen erlangen (um das Vertrauensverhältnis zwischen Unternehmen und Kunden nicht zu gefährden),

Die Regelung wird daher vom Bundesdatenschutzbeauftragten auch positiv gewürdigt, vgl. BfD-Info 5 („Datenschutz in der Telekommunikation“, S. 62), dazu auch BerlKommTKG/Kleszczewski, 2006, § 112, Rn. 12.

folglich auch wird eine strenge Zweckbindung der §112 TKG-Protokolldaten angeordnet. Hinzu kommt ein Zweites: Mitteilungspflichten gegenüber dem Bürger oder Auskunftsansprüche des Bürgers gegenüber den Telekommunikationsunternehmen oder der Bundesnetzagentur will das TKG in der Tat nicht selbst anordnen.

Gegenüber der Bundesnetzagentur ist ein Auskunftsanspruch zumindest sehr erschwert. Zwar ist nach § 19 Abs. 2 BDSG der Auskunftsanspruch bzgl. zu Zwecken der Datenschutzkontrolle gespeicherter Kontrolldaten (wie gemäß § 112 Abs. 4 S. 5 TKG) nicht kategorisch ausgeschlossen, sofern die Auskunftserteilung keinen unverhältnismäßigen Aufwand erfordert. Zu beachten wären jedoch die Grenzen des § 19 Abs. 3 und Abs. 4 BDSG. Vgl. BerlKommTKG/Kleszczewski, 2006, § 112, Rn. 13; Gramlich in: Manssen (Hrsg.), Telekommunikations- und Multimediarecht, § 90, Rn. 24.

Grund hierfür ist aber nicht, dass es die Kenntnisnahme der Bürger schlechthin verhindern möchte; der maßgebliche Grund ist vielmehr, dass es die Frage der Kennt-

nisnahme schlichtweg nicht als sein Regelungsthema betrachtet. Die spezifisch telekommunikationsrechtlichen Akteure (Unternehmen, Bundesnetzagentur) sollen bei der Frage Inkennntnissetzung des Bürgers außen vor bleiben, der TKG-Gesetzgeber will „seine“ Akteure mit diesen Fragen nicht behelligen und schottet sie daher von Auskunftsansprüchen ab. Umso klarer wird hierdurch, dass der TKG-Gesetzgeber es als ein Problem des jeweiligen Fachrechts ansieht, ob und wie weit die Kenntnisnahme ermöglicht wird. Der TKG-Gesetzgeber stellt den verschiedenen Sicherheitsbehörden für deren Zwecke ein effektives Verfahren zur Verfügung und erwartet im Gegenzug, dass diese Behörden – die die volle datenschutzrechtliche Verantwortung für den Eingriff tragen (§ 112 Abs. 4 S. 3 TKG) – auf der Basis des für sie geltenden Fachrechts das Problem der Betroffenenbenachrichtigung/-auskunftserteilung bewältigen.

Auch im teilweise parallel gelagerten Fall der Kontenabfrage durch Steuerbehörden nach §§ 93 Abs. 7, 93b AO, § 24c KWG scheint das Bundesverfassungsgericht vor allem der Ausgestaltung des Fachrechts (dort: Abgabenordnung, samt Anwendungserlasse hierzu) die entscheidende Bedeutung beizumessen (BVerfG vom 22.3.2005 – 1 BvR 2357/04, 1 BvQ 2/05).

Der von den Beschwerdeführern erhobene Vorwurf unzureichender Benachrichtigungspflichten/Auskunftsrechte kann nach alledem jedenfalls nicht zur Verfassungswidrigkeit des § 112 TKG führen.

Hinzu kommt: Die von den Beschwerdeführern vertretene Ansicht, eine – über die allgemeinen Auskunfts- und Verfahrensrechte des Fachrechts hinausgehende – besondere Benachrichtigung Betroffener über Bestandsdatenabfragen sei aus grundrechtlichen Gründen unverzichtbar, dürfte auch in der Sache falsch sein. Zu bedenken ist dabei, dass die in der Rechtsprechung des Bundesverfassungsgerichts zu Benachrichtigungspflichten dominierenden Fälle (Nachweise S. 80) typischerweise Fallkonstellationen betreffen,

- in denen es um schwerwiegende Grundrechtseingriffe (z.B. in Art. 10 GG, Art. 13 GG) geht, bzgl. derer das Gebot effektiven Rechtsschutzes besonderes Gewicht hat,
- in denen entsprechend der Tiefe des Eingriffs auch die Zulässigkeit des Eingriffs an hohe Hürden tatbestandlicher Art gebunden ist, deren Subsumtion und Anwendung im Einzelfall typischerweise fehleranfällig ist und bzgl. derer das Gebot richterlicher Nachprüfbarkeit infolgedessen erneut große Bedeutung hat,
- in denen es um außergewöhnliche Ermittlungsmaßnahmen (Telefonüberwachung, akustische Wohnraumüberwachung) geht, bzgl. derer der Einzelne typi-

scherweise nicht damit rechnen muss, dass er Gegenstand einer solchen Überwachungsmaßnahme wird.

Der hier zu behandelnde Fall dagegen liegt genau umgekehrt:

- Es handelt sich um einen Eingriff von nur geringfügiger Intensität bzgl. allgemeiner Identifikationsdaten geringer Schutzwürdigkeit.
- Es handelt sich um eine Maßnahme, die (was § 112 TKG anbelangt) an ein schlichtes Erforderlichkeitskriterium, nicht dagegen z.B. an eine im Einzelfall etwa schwierig zu beurteilende Verdachtsschwelle, geknüpft ist. Soweit die Maßnahme in der konkreten Situation vernünftigerweise geboten ist und keine mildereren Mittel vorhanden sind, ist die Bestandsdatenabfrage – gemäß der gesetzgeberischen Wertung des § 111 TKG, dass diese Daten für Zwecke der Sicherheitsgewährleistung prinzipiell zur Verfügung stehen – rechtmäßig. Freilich ist es vorstellbar, dass von der Bestandsdatenabfrage bewusst missbräuchlich (z.B. für private Zwecke) Gebrauch gemacht wird; insoweit wurden Vorkehrungen für eine hinreichende Missbrauchskontrolle getroffen (§ 112 Abs. 4 Sätze 2 und 4 TKG).
- Es handelt sich um ein automatisiertes Auskunftsverfahren, das der Gesetzgeber – erneut aufgrund der Wertung, dass es um Daten geht, die den Sicherheitsbehörden prinzipiell zur Verfügung stehen sollen – bewusst und für jedermann erkennbar als ein Massenverfahren für alltägliche Eingriffe ausgestaltet hat. Dem besonderen Aspekt der „Heimlichkeit“ des einzelnen Abrufs kann in diesen Fällen nicht das gleiche Gewicht beigemessen werden, wie das bei außergewöhnlichen Ermittlungseingriffen der Fall ist.

Es wäre nicht sachgerecht, die vom Bundesverfassungsgericht zu eingriffsintensiven, an komplizierte rechtliche Bewertungen gebundenen und unerwarteten heimlichen Ermittlungsmaßnahmen entwickelten Wertungen, was die Frage der Notwendigkeit besonderer Benachrichtigungen anbelangt, auf den hiesigen Fall eines geringfügigen, prinzipiell zulässigen und vielfach stattfindenden Informationseingriffs schlichtweg zu übertragen. Die Aussagen des Bundesverfassungsgerichts, bei dem Betroffenen verborgenen Maßnahmen bestehe grundsätzlich ein Anspruch auf zumindest nachträgliche Kenntnis, dürfen nicht vorschnell verallgemeinert werden. Zu bedenken ist dabei:

- Die Forderung nach einer gesonderten Benachrichtigungspflicht auch bzgl. gewöhnlicher Ermittlungsmaßnahmen wäre ein folgenschwerer Bruch mit der ständigen Staatspraxis. Weder die StPO noch die Polizeigesetze folgen diesem Prinzip. Alle diese Gesetze kennen spezielle Benachrichtigungspflichten nur bei eingriffsintensiven Maßnahmen. Ansonsten bestehen bzgl. gespeicherter Informationen (begrenzte) allgemeine Auskunftsansprüche. Ein Teil der alltäglichen Informationstätigkeit wird sich einem Auskunftsanspruch aber auch ganz entziehen. Speziell in der

StPO geht die Frage nach Benachrichtigung und Auskunft auf in den allgemeinen Verfahrensrechten des Beschuldigten/Angeklagten und seines Verteidigers. Jedenfalls besteht kein Recht des Betroffenen, über alle Ermittlungsmaßnahmen gesondert benachrichtigt zu werden. Würde die Polizei beispielsweise die Rufnummer einer Person nicht über das Verfahren nach § 112 TKG klären, sondern indem sie hierüber – für den Betroffenen verborgen – Dritte befragt, so würde auch das nicht zu einer gesonderten Benachrichtigungspflicht führen.

- Die Wertung, dass jedenfalls über gesetzlich ausdrücklich vorgesehene, routinemäßig zulässige Datenübermittlungen keine gesonderte Mitteilung zu machen ist, kommt im Gesetz auch anderwärtig zum Ausdruck, so namentlich in §§ 19a Abs. 2 S. 1 Nr. 3, 33 Abs. 2 S. 1 Nr. 4 BDSG.

Hierzu (im Zusammenhang mit § 24c KWG) Kokemoor, BKR 2004, 135/140.

- Aus der Tatsache, dass das Bundesverfassungsgericht im einstweiligen Verfahren zu § 24c KWG, §§ 93 Abs. 7, 8, 93b AO der Frage der Kenntnisnahme des Bürgers relativ großes Gewicht beigemessen hat,

BVerfG vom 22.3.2005 – 1 BvR 2357/04, 1 BvQ 2/05.

sollte nicht vorschnell auf die hiesige Problematik zurückgeschlossen werden. Zwar geht es um ein strukturell ähnlich gelagertes automatisiertes Abrufverfahren. Zu bedenken ist allerdings, dass es bei der Telekommunikationsbestandsdatenabfrage um Identifikationsdaten von vergleichsweise niedriger Schutzwürdigkeit geht sowie dass sich das Besteuerungsverfahren als reguläres Verwaltungsverfahren mit den typischen Ermittlungssituationen der Sicherheitsbehörden kaum vergleichen lässt, so dass sich die Wertungen nicht ohne weiteres übertragen lassen.

- Gründe der Verwaltungspraktikabilität hat das Bundesverfassungsgericht in BVerfGE 100, 313/398 keineswegs so kategorisch als Rechtfertigungsgrund für den Ausschluss von Benachrichtigungspflichten verworfen, wie von den Beschwerdeführern suggeriert. Im Fall der Bestandsdatenauskunft nach § 112 TKG würde es angesichts der Geringfügigkeit des Eingriffs und der Zahl von 3,4 Mio. Ersuchen pro Jahr einen unverhältnismäßigen Aufwand bedeuten, prinzipiell ein Benachrichtigungsverfahren vorzusehen.

- Auch in anderen vergleichbaren automatisierten Auskunftsverfahren (Melderegister, Fahrzeugregister) sehen die gesetzlichen Regelungen keine Benachrichtigungspflichten vor.

- Zu bedenken ist schließlich, dass hinsichtlich der bei § 112 TKG einzig realistischen Gefahr rechtswidriger Handhabung – der Gefahr missbräuchlichen Zugriffs im Einzelfall (z.B. zu privaten Zwecken) – bereits der TKG-Gesetzgeber selbst wirksame Schutzvorkehrungen organisations- und verfahrensrechtlicher Art getroffen hat.

So ist die Bundesnetzagentur nach § 112 Abs. 4 S. 2 TKG – trotz datenschutzrechtlicher Verantwortlichkeit der ersuchenden Stellen – zur Überprüfung der Zulässigkeit der Übermittlung bei entsprechendem Anlass berechtigt. Angesichts der Position der Bundesnetzagentur als bewusst zwischen ersuchender Behörde und Diensteanbieter geschaltetem neutralen Informationsmittler wird man ihr auch eine gegenüber dem Bürger bestehende Verantwortung zusprechen müssen, bei entsprechenden Anhaltspunkten (z.B. auf Beschwerde oder Nachfrage des Betroffenen hin), von dieser Befugnis Gebrauch zu machen und so ein Stück Grundrechtssicherung durch Organisation und Verfahren zu verwirklichen.

Trute, in Trute/Spoerr/Bosch, TKG, 2001, § 90, Rn. 16.

Hinzu kommt zweitens, dass der Telekommunikationsgesetzgeber durch Statuierung der Protokollierungspflichten des § 112 Abs. 4 S. 4 TKG für Zwecke der Datenschutzkontrolle eine effektive Nachprüfung durch den Bundesdatenschutzbeauftragten ermöglicht; da auch das Aktenzeichen der ersuchenden Behörde zu protokollieren ist, ist auch sichergestellt, dass auch deren Verhalten – ggf. über den zuständigen Landesdatenschutzbeauftragten – einer Kontrolle unterzogen werden kann. Der Bundesdatenschutzbeauftragte selbst schätzt seine Möglichkeiten der Missbrauchs-kontrolle nach § 112 Abs. 4 S. 4 TKG als effektiv ein.

Tätigkeitsbericht 2001 und 2002 des Bundesbeauftragten für den Datenschutz – 19. Tätigkeitsbericht, S. 79.

All dies zusammengekommen kann man die sich aus einem Zusammenspiel von § 112 TKG und jeweiligem Fachrecht ergebende Rechtslage,

- dass jedenfalls im Zusammenhang mit Eingriffen in Art. 10 GG Benachrichtigungspflichten bestehen,
- dass sich die Frage der Kenntnisnahme von Bestandsdatenabfragen ansonsten nicht anders beurteilt als vergleichbare andere Ermittlungseingriffe der Fachbehörden auch, d.h. dass es auf die allgemeinen Auskunftsrechte des jeweiligen Fachrechts ankommt,

- dass im TKG selbst Vorkehrungen für eine wirksame Datenschutzkontrolle durch den Bundesdatenschutzbeauftragten sowie Kontrollmöglichkeiten der Bundesnetzagentur geschaffen wurden,

angesichts der Geringfügigkeit, der regelmäßigen Zulässigkeit und der Häufigkeit der im Zusammenhang mit § 112 TKG erfolgenden Eingriffe nicht als einen Verstoß gegen das Recht auf informationelle Selbstbestimmung (ggf. i. V. m. Art. 19 Abs. 4 GG) ansehen. Selbst aber soweit man einen insgesamt unzureichenden Rechtszustand annehmen wollte, so wäre dieser jedenfalls nicht § 112 TKG anzulasten. Die Bewäl-

tigung des Ausgleichs von Kenntnisnahme- und Geheimhaltungsinteresse kann sinnvoll allein im jeweiligen Fachrecht geleistet werden.

cc) Weitere Rügen

Die Beschwerdeführer rügen, dass § 112 TKG für die ersuchenden Behörden bzgl. der erlangten Bestandsdaten kein ausdrückliches Zweckbindungsgebot vorgesehen habe.

Beschwerdeschrift, S. 80, 83.

Diese Rüge geht fehl. Die weitere Verwendung der im automatisierten Auskunftsverfahren erlangten Daten durch die ersuchenden Behörden ist nicht Regelungsgegenstand des § 112 TKG, sondern richtet sich allein nach dem jeweils einschlägigen Fachrecht.

BeckTKG-Komm/Büchner, 2. Aufl. 2000, § 89, Rn. 45; BeckTKG-Komm/Bock, 3. Aufl. 2006, § 113, Rdnr. 9; Wuermeling/Felixberger, CR 1997, 595/560; einzige Ausnahme: § 112 Abs. 1 Nr. 5 TKG.

Im jeweiligen Fachrecht sind dergleichen Zweckbindungsgebote auch geregelt (für die bayerische Polizei z.B. Art. 37 Abs. 2 PAG).

Aus einem ähnlichen Grund fehlt geht auch die Rüge der Beschwerdeführer (Beschwerdeschrift S. 80, 83), es fehle an einer ausdrücklichen Anordnung der Protokollierung jeder Erhebung, Verwendung, Übermittlung oder Vernichtung der Bestandsdaten durch die ersuchende Behörde. Auch diese Frage ist ausschließlich vom jeweiligen Fachgesetzgeber zu regeln. Soweit der Telekommunikationsgesetzgeber zur Regelung von Protokollierungsfragen berufen war, nämlich in Bezug auf die Bundesnetzagentur, hat er dies getan (§ 112 Abs. 4 S. 4 TKG). Im Übrigen wäre zu prüfen, ob die aus BVerfGE 100, 313/395 f. entnommene Protokollierungspflicht (dort geht es um Art. 10 GG) wirklich auf jeden Eingriff in das Recht auf informationelle Selbstbestimmung übertragbar ist.

Gerügt wird schließlich, dass keine Evaluierungsregelungen zu Belastungen und Nutzen der Bestandsdatenabfrage vorgesehen seien.

Beschwerdeschrift, S. 84.

Unklar bleibt insoweit, woraus sich eine derartige Evaluierungspflicht verfassungsrechtlich ergeben soll. Dem Grundgesetz sind prozedurale Evaluierungspflichten im Sinne moderner Gesetzesfolgeabschätzung grundsätzlich fremd, d.h. es steht ihrer

gesetzlichen Einführung zwar nicht entgegen, verlangt sie aber auch nicht. Vielmehr vertraut das Grundgesetz – in verfahrensmäßiger Hinsicht – ganz auf die Richtigkeitsgewähr des parlamentarischen Gesetzgebungsverfahrens sowie auf die Kontrollkompetenz des Bundesverfassungsgerichts. Vereinzelt kann es Konsequenz des Verhältnismäßigkeitsprinzips sein, dass der Gesetzgeber zur laufenden Beobachtung verpflichtet ist; dies ist vor allem in Situationen strukturell unsicheren Wissens der Fall.

Z.B. BVerfGE 110, 141/166.

Eine solche Situation ist hier aber nicht gegeben. Die – geringfügigen – Belastungen, die aus der Bestandsdatenabfrage resultieren, liegen auf der Hand. Hinsichtlich ihres Nutzens gibt es eine jahrzehntelange Praxiserfahrung; die statistischen Daten über die Häufigkeit der Ersuchen werden regelmäßig sowohl von der Bundesnetzagentur als auch vom Bundesdatenschutzbeauftragten veröffentlicht.

dd) Unvollständige Abfragedaten/Ähnlichenfunktion (§ 112 Abs. 1 S. 4, Abs. 3 TKG)

Von den Beschwerdeführern bemängelt wird insbesondere die nunmehr in § 112 Abs. 1 S. 4 TKG geschaffene Möglichkeit einer Verwendung unvollständiger Abfragedaten oder der Suche mittels einer Ähnlichenfunktion. Der hierdurch ermöglichte Eingriff in die Rechte Betroffener wird als besonders stark angesehen; zugleich wird gerügt, die Regelung eingrenzender Maßgaben erst durch Rechtsverordnung (§ 112 Abs. 3 S. 1 Nr. 3 TKG) sei ein Verstoß gegen den Parlamentsvorbehalt.

Beschwerdeschrift, S. 80, 85; von einer „eingriffsintensiven“ Auskunftsvariante sprechen auch Koenig/Loetz/Neumann, Telekommunikationsrecht, 2004, S. 212.

Der maßgebliche sachliche Hintergrund zu dieser neuen Auskunftsvariante ist bereits eingangs unter A.1. (S. 5 f.) kurz umrissen worden. Rechnung getragen wird mit ihr der praktischen Erfahrung, dass es insbesondere bei ausländischen Namen (mit unsicherer Schreibweise oder nichtlateinischem Alphabet), bei Doppelnamen und Doppelvornamen (mit oder ohne Bindestrich etc.) sowie bei Firmenangaben aufgrund der unklaren Schreibweise oder wegen der unterschiedlichen Handhabung der Eingabefelder bei den Telekommunikationsunternehmen immer wieder zu unnötigen Fehlanzeigen oder aber auch zu unnötigen Mehrfachanfragen (mit je unterschiedlicher Schreibweise) kommt. Das neue Verfahren will diesem Manko, d.h. konkreten Schwierigkeiten in der bisherigen Handhabung abhelfen, indem es die Verwendung

von sog. Jokerzeichen (z.B. M\*ller, wenn unsicher ist, ob der Gesuchte Möller oder Müller heißt) zulässt oder aber (das ist vor allem bei der Transkription aus anderen Alphabeten wichtig) die Ähnlichensuche (z.B. Suche mit ähnlichen Buchstaben) erlaubt. Die neuen Suchfunktionen wurden auf ausdrücklichen Wunsch der Strafverfolgungs- und Sicherheitsbehörden in das Gesetz aufgenommen.

BT-Drucks. 15/2316, S. 96; s.a. Koenig/Loetz/Neumann, Telekommunikationsrecht, 2004, S. 212; Thiede, Kriminalistik 2004, S. 104/108.

Das neue Verfahren ist gegenwärtig noch nicht einsatzfähig, denn noch fehlt es sowohl an der entsprechenden Verordnung nach § 112 Abs. 3 S. 1 Nr. 3 TKG, in der Mindestanforderungen an den Umfang der einzugebenden Daten und an den zulässigen Umfang der zu übermittelnden Treffer festzulegen sind, als auch an der entsprechenden technischen Richtlinie nach § 112 Abs. 3 S. 4 TKG.

Wie eine entsprechende Verordnung mit eingrenzenden Merkmalen aussehen könnte, zeigt z.B. § 8 ZStVBetrV (Verordnung über den Betrieb des Zentralen Staatsanwaltschaftlichen Verfahrensregisters) vom 23.9.2005, BGBl. I S. 2885, wo eine Begrenzung der Trefferzahl auf zunächst 20 vorgesehen ist.

Beurteilt man die Schwere des im Zuge der Anwendung dieser Suchfunktion erfolgenden Grundrechtseingriffs, so ist zunächst dem Eindruck entgegenzutreten, es handele sich um einen besonders intensiven Eingriff:

- Auch bei der Ähnlichensuche oder der Suche mit „Jokerzeichen“ geht es allein um den Zugriff auf die grundlegenden Telekommunikationsbestandsdaten des § 111 TKG, die als Basisdaten zur Identifikation und Erreichbarkeit einer Person eine nur geringe Schutzwürdigkeit aufweisen. Es handelt sich um Daten, von denen der Gesetzgeber in § 111 TKG zu Recht die Grundentscheidung getroffen haben, dass sie für die Aufgaben der Sicherheitsbehörden zur Verfügung stehen sollen. Zu diesen Aufgaben gehört auch die Aufklärung bei unsicherer Schreibweise, für die die neue Suchfunktion geschaffen wurde.
- Zu berücksichtigen ist, dass, wie unter A.II. (S. 9) dargelegt, in 95 % der Fälle, in denen von § 112 TKG Gebrauch gemacht wird, von einer Rufnummer auf einen Namen geschlossen werden soll; für diesen Hauptanwendungsfall ist die neue Suchfunktion ohne jede Relevanz. Nur bei der – vergleichsweise seltenen – umgekehrten Suchrichtung kann sie nützlich sein.
- Der einzig in Bezug auf die Eingriffstiefe relevante Unterschied zur bislang möglichen Standardsuche besteht darin, dass ggf. eine erhöhte Trefferzahl erzielt werden kann, d.h. dass auch Personen von dem Suchvorgang erfasst werden können, nach denen letztlich gar nicht gesucht wird; die neue Suchfunktion hat so gese-

hen eine gewisse Streubreite, während die Standardsuche gezielt ist und nur eine Person erfasst. Zur Frage, ob die Streubreite (d.h. die zahlenmäßige Vermehrung der Eingriffe) angesichts der Tatsache, dass stets nur der Grundrechtseingriff eines konkret Betroffenen (hier der Beschwerdeführer) geprüft werden kann, überhaupt als eingriffsvertiefend ins Gewicht fallen kann, sind bereits oben unter 1.c.bb. (S. 57) Ausführungen gemacht worden. Immerhin ist es so, dass sich durch die neue Suchfunktion die Wahrscheinlichkeit eines Treffers erhöht und dass man ggf. auch als Dritter (nach dem nicht gesucht wird) mitbetroffen sein kann, so dass mit guten Gründen von einer zusätzlichen Rechtfertigungsbedürftigkeit gesprochen werden kann. Gleichwohl erscheint es verfehlt, schon deswegen von einem besonders intensiven Grundrechtseingriff auszugehen. Im Kern bleibt es dabei, dass die Daten, die über einen Betroffenen ermittelt werden können, von geringer Schutzwürdigkeit sind. Nur der Grund, warum diese Daten ermittelt werden, hat sich etwas verschoben: Hat sich bei der Standardsuche die Suche unmittelbar auf eine bestimmte Person (bzw. auf eine Person mit dieser Schreibweise) bezogen, so kann es nunmehr sein, dass man von der Suche nach einer anderen Person mitbetroffen wird. Auf die Relevanz der Daten an sich hat dies keinen Einfluss; nur die Rechtfertigung der Datenerhebung liegt etwas anders. Dass im Vergleich zu früher kein wesentlicher Unterschied besteht, wird auch daran deutlich, dass es den Sicherheitsbehörden auch bei der bisherigen Standardsuche unbenommen ist, hintereinander Suchen mit je unterschiedlichen Schreibweisen durchzuführen; jede Suche für sich kann für die Aufgabenerfüllung der Sicherheitsbehörde erforderlich sein, weil nur so die Rufnummer einer Person mit unsicherer Schreibweise ermittelt werden kann. Auf manuellem Wege ist es daher bis zu einem gewissen Grade auch bereits bisher möglich, dasselbe Ergebnis zu erzielen, wie künftig mit der Ähnlichensuche; die neue Suchfunktion hat so gesehen auch den Zweck, unnötige Mehrfachanfragen zu reduzieren und kann insofern durchaus zu einer Reduzierung der Anfragen führen. Ein Moment der Drittbetroffenheit war also auch bereits dem bisherigen System immanent; die neue Suchfunktion macht dies nur transparenter.

- Keine eingriffserhöhende Wirkung kommt der neuen Suchfunktion entgegen dem Vorbringen der Beschwerdeführer dahingehend zu, dass mit ihr auch nur im Entferntesten eine Art „Rasterung“ möglich sein könnte.

So aber die Beschwerdeschrift S. 85; ähnlich auch BeckTKG-Komm 3. Aufl. 2006, § 112, Rdnr. 24; Dies würde selbst dann gelten, wenn – was keineswegs sicher ist und erst in der zu erlassenden Verordnung zu klären wäre – über die bisher geschilderten Verwendungsmöglichkeiten hinaus z.B. eine Häuserabfrage (d.h. die Ermittlung aller zu einem Haus gemeldeten Anschlüsse) ermöglicht werden sollte, dazu Thiede, Kriminalistik 2004, 104/108.

Die spezifische eingriffserhöhende Wirkung einer Rasterfahndung besteht darin, dass aus der Verknüpfung je für sich „harmloser“ Daten nach gewissen Täterprofilen sensible Erkenntnisse gewonnen werden können.

BVerfG, Beschluss vom 4.4.2006 – 1 BvR 518/02, Abs. 96 ff.

Die Bestandsdatenabfrage ist hierfür völlig ungeeignet, weil die einzelnen von § 111 TKG erfassten und nach § 112 TKG abrufbaren Bestandsdaten nicht nur je für sich, sondern auch in ihrer Kombination keine Merkmale enthalten, die irgendein Täterprofil erkennen ließen. Die noch zu erlassende Rechtsverordnung mit ihren eingrenzenden Maßgaben wird ihr übriges tun, die neue Suchfunktion als für jede Art von großflächiger Rasterung ungeeignet zu erweisen. Die Zwecke der neuen Suchfunktion sind ganz spezielle: Im Kern geht es um die Bewältigung des Problems unsicherer Schreibweisen; theoretisch denkbar sind weitere Anwendungsfelder wie Häuserabfragen. Mit einer Rasterfahndung hat all dies nichts zu tun.

Was die verfassungsrechtliche Rechtfertigung der neuen Suchfunktion angeht, so ist zunächst erneut darauf hinzuweisen, dass ihre Last nicht allein auf den Schultern des § 112 Abs. 1 S. 4 TKG ruht. Der Telekommunikationsgesetzgeber stellt den Sicherheitsbehörden bestimmte Daten und Suchfunktionen gemäß den Voraussetzungen des § 112 TKG zur Verfügung. Es ist sodann Sache des jeweiligen Fachrechts der ersuchenden Behörde, darüber zu befinden, ob die Sicherheitsbehörde von diesem Angebot im Blick auf die Rechte des Betroffenen auch Gebrauch machen darf. Die eigentliche Befugnisnorm kommt vom Fachrecht her.

In Bezug auf § 112 TKG (und seinen Teil der verfassungsrechtlichen Rechtfertigung) ist sodann zu bedenken, dass die Einbeziehung Dritter über „Jokerzeichen“ und Ähnlichensuchen von der gewöhnlichen Eingriffsvoraussetzung des § 112 Abs. 2 TKG, dass das Auskunftersuchen für die Erfüllung der Aufgaben der Sicherheitsbehörde erforderlich sein muss, voll und ganz erfasst ist. Das Merkmal der Erforderlichkeit ist eben keine Verdachtsschwelle, infolge derer Eingriffe nur gegen in bestimmter Weise „Verdächtige“ gerichtet werden dürften, vielmehr ist es eine Eingriffsvoraussetzung, die – soweit erforderlich – auch das Mitbetroffensein Dritter rechtfertigen kann. Soweit die Behörde, etwa weil die Schreibweise unsicher ist, mithilfe der gezielten Suche nicht zum Ziel kommen und somit ihre Aufgabe nicht erfüllen kann, rechtfertigt das Erforderlichkeitskriterium auch einen erweiterten (Dritte einschließenden) Datenzugriff, soweit hiermit ein Treffer erzielt werden kann. Dies war genau besehen – wie bereits gesagt – auch schon bisher so, weil es bei Fehl- oder Falschanzeigen infolge unsicherer Schreibweise nötig sein konnte, Mehrfachanfragen zu starten, um zum Ziel zu gelangen. All dies hält sich ohne weiteres innerhalb der dem ganzen Normenkomplex der §§ 111 – 113 TKG zugrunde liegenden Grundwertung, dass die Be-

standsdaten des § 111 TKG als so wenig schutzwürdig angesehen werden, dass sie den Sicherheitsbehörden für ihre Zwecke (d.h. auch für Aufklärungszwecke bei unsicherer Schreibweise) prinzipiell zur Verfügung stehen sollen. Diese Wertung aber hat, wie gezeigt, vor dem Verhältnismäßigkeitsprinzip Bestand.

Mit seiner Wertung, dass Bestandsdateneingriffe nicht nur gegenüber „Verdächtigen“, sondern – ihre Erforderlichkeit vorausgesetzt – auch gegenüber jedermann, d.h. auch gegenüber Dritten, zulässig sein können, hält sich § 112 Abs. 1 S. 4 TKG – so wie bereits im Kontext mit § 111 TKG ausgeführt (oben 1.c.dd., S. 65 f.) – auch Rahmen der sonst üblichen Wertungen des Gesetzesrechts. So bringt z.B. gerade das Polizeirecht (etwa durch die dort statuierte Jedermann-Pflicht zur Auskunft über Identitätsdaten oder durch die „verdachtslos“ mögliche Schleierfahndung, bei der es ihrerseits um Identitätsfeststellung geht) zum Ausdruck, dass es einen Kreis von Identifikationsdaten gibt, die jedermann – unabhängig davon, ob er verdächtig oder gar „Störer“ ist – nach Maßgabe des Erforderlichkeitsprinzips preisgeben muss. Um derartige – wenig schutzwürdige – Grunddaten, die den Sicherheitsbehörden prinzipiell zugänglich gemacht werden dürfen, geht es auch bei § 112 TKG.

Gegen diese Wertung ist auch aus verfassungsrechtlicher Sicht nichts einzuwenden. Der Vorgang, dass ein Unverdächtiger oder Dritter von einem Informationseingriff betroffen wird, wird in der Literatur und Rechtsprechung bisweilen unnötig „dramatisiert“, so als sei dieser Vorgang an sich schon etwas Ungewöhnliches oder besonders Rechtfertigungsbedürftiges. Im Zusammenhang mit der Schleierfahndung ist dann z.B. davon die Rede, der Betroffene werde ohne Legitimation „wie ein Störer“ in Anspruch genommen oder dürfe deswegen nicht in Anspruch genommen werden, weil er „Nichtstörer“ sei.

LVerfG MV DÖV 2003, 71/73; Schewe, NWVBI 2004, 415/417.

Derartige Einschätzungen gehen fehl. Nimmt man das Gefahrenabwehrrecht als Beispiel, so besagt die rechtsstaatliche Systembildung Gefahr - Störer unmittelbar nur, dass – bei bereits feststehender Gefahr – grundsätzlich allein der Störer (der die Gefahr verursacht hat) zur Gefahrenbeseitigung (d.h. zur Unterbrechung des schadensträchtigen Kausalverlaufs) herangezogen werden darf. Soll dagegen – durch Informationseingriffe – erst herausgefunden werden, ob und wo eine Gefahr besteht, so versagt diese Systembildung, weil es einen Störer noch nicht gibt und weil auch in der Sache ganz fraglich ist, inwieweit die der Störerhaftung zugrundeliegenden Kriterien der Verursachung und Zurechenbarkeit in einem Stadium, in dem es gerade noch nicht um Eingriffe in Kausalverläufe, sondern nur um Informationseingriffe geht, überhaupt Gültigkeit haben kann. Es gibt daher keine Regel, dass im Polizeirecht Informationseingriffe nur gegen Störer gerichtet werden dürften. Ähnlich ist es auch

im Strafprozessrecht: Die Strafverfolgung, bei der es typischerweise darum geht, aus einer Vielzahl von Personen den Täter zu ermitteln und ihm die Tat nachzuweisen, ist bereits der Grundanlage nach ein Vorgang, bei dem es zunächst darum geht auszufiltern, wer verdächtig ist. Hierbei geraten notwendig auch letztlich Unverdächtige zwischenzeitlich in den Blick der Strafverfolgungsbehörden. Hinzu kommt, dass über die Zeugenpflicht seit jeher auch Dritte in den Prozess der Informationsbeschaffung eingebunden sind. Sicherlich mag es sein, dass je mehr sich der Verdacht bereits konkretisiert hat und je tiefer etwaige Ermittlungseingriffe sind, diese aus Verhältnismäßigkeitsgründen vorrangig gegen den Verdächtigen zu richten sind (z.B. § 100a S. 2 StPO). Nicht jedoch ist es richtig, in der Einbeziehung Dritter etwas an sich Ungewöhnliches zu sehen; das Strafprozessrecht kennt solche Maßnahmen seit jeher. Auch beispielsweise der typische Einsatz des Auskunftsverfahrens nach § 112 TKG – die Situation, in der der Polizei bestimmte Kontaktrufnummern eines Verdächtigen bekannt werden, und nunmehr ermittelt werden soll, wer hinter diesen Rufnummern steht, um sein Umfeld aufzuklären – ist an sich bereits (und zwar ganz ohne die neue „Jokerzeichen“-Suchfunktion) eine Maßnahme mit Streubreite, weil sich nicht bei jedem Beteiligten Verdachtsmomente oder eine Verwendbarkeit als Zeuge ergeben werden. Die Streubreite, die im Wege der neuen Suchfunktion zusätzlich erzeugt wird, hält sich so gesehen ganz im Rahmen des Üblichen und ist nicht etwa etwas besonders Rechtfertigungsbedürftiges.

Selbstverständlich ist allein, dass sich jede Ausweitung auf Dritte, jede Vergrößerung der Streubreite stets im Rahmen des Erforderlichen und Verhältnismäßigen halten muss; der Kreis der Betroffenen darf nicht außer Verhältnis zu dem jeweiligen Ermittlungszweck stehen. Dieser Anforderung des Verhältnismäßigkeitsprinzips indes kann bereits mit dem in § 112 TKG normierten Erforderlichkeitskriterium voll und ganz genügt werden. Auch ohne den ausdrücklichen Auftrag des Absatzes 3 an den Verordnungsgeber, eingrenzende Maßgaben festzulegen, wäre § 112 TKG, was die in ihm normierte Eingriffsvoraussetzung anbelangt, daher verfassungsrechtlich einwandfrei. Dies gilt auch für die in § 112 Abs. 1 S. 5 TKG ausdrücklich normierte unverzügliche Löschungspflicht für unbenötigte Daten, die ihrerseits Ausfluss des Verhältnismäßigkeitsprinzips ist.

Der Gesetzgeber hat – über das an sich bereits ausreichende Erforderlichkeitskriterium hinaus – noch eine zusätzliche Schutzvorkehrung vorgesehen, um das Ausmaß der Streubreite von Anfragen nach § 112 Abs. 1 S. 4 TKG in Grenzen zu halten, nämlich die Verordnungsermächtigung des Absatzes 3, die in Satz 1 Nr. 3 auch die Regelung von Mindestanforderungen an den Umfang der einzugebenden Daten sowie die Höchstzahl der zulässigen Treffer betrifft. Laut Gesetzgebungsmaterialien ging man davon aus, dass eine eingrenzende Regelung, um der Gefahr großer Ant-

wortmengen zu begegnen, sowohl aus Praktikabilitätserwägungen und Kostengründen wie aus datenschutzrechtlichen Gründen unverzichtbar sei.

BT-Drucks. 15/2316, S. 96, s.a. BerlKommTKG/Kleszczewski, 2006, § 112, Rn. 25.

Diese politisch sicher richtige Einschätzung trägt keine verfassungsrechtliche Züge, dergestalt, dass die neue Suchfunktion ohne die eingrenzende Verordnung verfassungswidrig wäre. Denn wie oben ausgeführt, ist dem Verhältnismäßigkeitsprinzip bereits durch das Erforderlichkeitskriterium genügt. Letztlich kommt es auf die Frage aber nicht an. Denn aus der Entstehungsgeschichte heraus wie im Übrigen auch aus der Formulierung „Mindestanforderungen“, „zulässiger Umfang“ etc. lässt sich ablesen, dass jedenfalls das einfache Gesetz die Anordnung trifft, dass die neue Suchfunktion erst zulässig sein soll, wenn die Verordnung erlassen ist. Dementsprechend wird von ihr gegenwärtig auch kein Gebrauch gemacht.

Die Beschwerdeführer rügen – zu Unrecht –, mit der Verordnungsermächtigung sei der Parlamentsvorbehalt verletzt. Den Bestimmtheitsanforderungen des Art. 80 Abs. 1 S. 2 GG ist ersichtlich genügt, dem Ordnungsgeber ist ein klares Programm zur Eingrenzung der Abfragevarianten unter Verhältnismäßigkeitsgesichtspunkten an die Hand gegeben; auch die Regelungsinhalte (Eingabevollständigkeit, Trefferzahl) sind genannt. Dass darüber hinaus der Parlamentsvorbehalt im Sinne der Wesentlichkeitslehre verletzt sein könnte, ist abzulehnen. Wenn die hier vertretene Auffassung, dass bereits das Erforderlichkeitskriterium dem Verhältnismäßigkeitsprinzip genügt und dass es der Verordnungsermächtigung aus grundrechtlichen Gründen nicht bedurft hätte, zutrifft, liegt dies auf der Hand. Denn dann ist es gerade nicht grundrechtswesentlich, ob es zusätzliche eingrenzende Kriterien gibt oder nicht. Aber selbst wenn man dies anders sehen und die Normierung zusätzlicher Kriterien für unerlässlich halten wollte, so wäre es jedenfalls eine Überspannung der Wesentlichkeitslehre, die diesbezügliche Gesamtregelung dem parlamentarischen Gesetzgeber vorbehalten zu wollen und eine Verordnungsermächtigung für überhaupt unstatthaft zu erachten. Die Entwurfsbegründung sagt ganz zu Recht, dass die Regelung wegen ihres Detaillierungsgrades für eine delegierte Ordnungsgebung prädestiniert ist.

BT-Drucks. 15/2316, S. 96.

Unter Wesentlichkeitsgesichtspunkten muss es, wenn es eingrenzender Kriterien wirklich bedarf, ausreichen, dass der Gesetzgeber die Entscheidung trifft, dass solche tatsächlich unverzichtbar und daher vom Ordnungsgeber vorzusehen sind, sowie dass ohne Verordnung von der neuen Suchfunktion nicht Gebrauch gemacht werden darf. Dies hat der Gesetzgeber getan. Von ihm auch noch zu fordern, die

technischen Details der Eingrenzung (Anzahl der Treffer, Gestaltung der Eingabefelder etc.) zu regeln, würde einem Totalvorbehalt des Gesetzes im Informationsrecht gleichkommen. Dies wäre auch ein Bruch mit den ansonsten in der Gesetzgebungspraxis bestehenden Regelungstechniken.

Vgl. die ihrerseits als Verordnung erlassene ZStVBetrV mit ihrem § 8 (Nachweis siehe S. 88).

d) Zitiergebot

Das Zitiergebot nach Art. 19 Abs. 1 S. 2 GG gilt für Eingriffe in das informationelle Selbstbestimmungsrecht nicht (siehe bereits oben 1.c.ff., S. 71)

e) Teilergebnis

Durch § 112 TKG werden Grundrechte der Beschwerdeführer nicht verletzt.

### 3. § 113 TKG

a) Das berührte Grundrecht

Das manuelle Auskunftsverfahren nach § 113 TKG berührt, was das hier streitentscheidende Rechtsverhältnis zum datenschutzrechtlich Betroffenen anbetrifft, wie unter I.1. (S. 25 ff.) aufgezeigt, allein das Recht auf informationelle Selbstbestimmung, nicht jedoch das Fernmeldegeheimnis. Dies gilt, wie in I.1. bereits im Einzelnen nachgewiesen wurde, auch, soweit der Kreis der zugriffsfähigen Bestandsdaten bei § 113 TKG größer ist als derjenige bei § 112 TKG (Daten nach § 95 TKG, die über die von § 111 TKG erfassten hinausgehen können), namentlich auch, soweit gemäß § 113 Abs. 1 S. 2 TKG um Auskunft über sog. Zugriffsdaten (PIN/PUK) nachgesucht wird. Streitig kann allenfalls sein, inwieweit der Zugriff auf die einer dynamischen IP-Adressen zugeordneten Rufnummer Art. 10 GG-relevant ist und daher von § 113 TKG erfasst sein kann (siehe oben S. 36). Allerdings stellt § 113 Abs. 1 S. 3 TKG eindeutig klar, dass Eingriffe in das Fernmeldegeheimnis auf der Basis von § 113 TKG nicht erlaubt sein sollen. Selbst soweit man im Sonderfall der Auskunft über dynamische IP-Adressen Art. 10 GG als berührt ansehen wollte, wäre Konsequenz demnach nicht, dass § 113 TKG an Art. 10 GG zu messen wäre; vielmehr folgte daraus allein, dass entsprechende Auskunftsverlangen eben nicht auf § 113 TKG gestützt werden können. Art. 10 GG ist von § 113 TKG daher in keinem Fall berührt.

## b) Eingriff

Verlangt eine Sicherheitsbehörde von einem Diensteanbieter Auskunft über Bestandsdaten und kommt dieser dem Ersuchen nach, so stellt dies einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung dar. Zu bedenken ist allerdings, dass dieser Eingriff nur in sehr beschränktem Maße § 113 TKG zurechenbar ist (vgl. dazu im Einzelnen I.3., S. 39 ff.). Die in § 113 TKG normierte Auskunftspflicht der Diensteanbieter bedeutet allein, dass der Telekommunikationsgesetzgeber die Voraussetzungen dafür schafft, dass den Sicherheitsbehörden unter bestimmten Voraussetzungen ein bestimmter Datenbestand telekommunikationsrechtlich zur Verfügung steht. Ob die Sicherheitsbehörden dann auch das Recht haben, sich dieses Datenbestandes zu bedienen, d.h. die telekommunikationsrechtlich zur Verfügung stehenden Daten auch tatsächlich zu erheben, ist eine Frage, die sich allein nach dem jeweiligen Fachrecht der Sicherheitsbehörde richtet. Die eigentliche Befugnisnorm für die Datenerhebung kommt daher stets aus dem Fachrecht. Dass dies so ist, bringt am speziellen Beispiel der Auskunft über Zugriffsdaten namentlich § 113 Abs. 1 S. 2 TKG sehr klar zum Ausdruck (Auskunftsersuchen nach §§ 161, 163 StPO, nach Polizeirecht etc.).

Trute, in Trute/Spoerr/Bosch, TKG, 2001, § 89, Rn. 57; BeckTKG-Komm/Bock, 3. Aufl. 2006, § 113, Rdnr. 9.

## c) Verfassungsrechtliche Rechtfertigung

### aa) Verhältnismäßigkeit

Was die Verhältnismäßigkeit von § 113 TKG anbelangt, kann weitgehend auf die Ausführungen zu §§ 111 und 112 TKG verwiesen werden. Auch § 113 TKG hält sich im Rahmen der unter Verhältnismäßigkeitsgesichtspunkten einwandfreien Wertung des Gesetzgebers, dass Telekommunikationsbestandsdaten den Sicherheitsbehörden für deren Zwecke prinzipiell zur Verfügung gestellt werden dürfen. Speziell im Vergleich zum automatisierten Auskunftsverfahren nach § 112 TKG fällt ins Gewicht, dass das manuelle Verfahren nach § 113 TKG für die ersuchende Behörde sowohl aufwändiger als auch – nach Maßgabe des § 113 Abs. 2 TKG und anders als bei § 112 TKG – kostenpflichtig ist. Das Gebrauchmachen von § 113 TKG erscheint insoweit als im Vergleich zu § 112 TKG erschwert, auch soweit beide Normen – in einem sehr großen sachlichen Überschneidungsbereich – den gleichen Behörden Zugriff auf die gleiche Art von Daten gestatten. In Bezug auf die Verhältnismäßigkeit des § 113 TKG folgt hieraus, jedenfalls soweit es um diesen großen Überschnei-

dungsbereich der Anwendungsfelder geht, dass, wenn § 112 TKG verhältnismäßig ist, gleiches erst recht für § 113 TKG zu gelten hat und insoweit voll und ganz auf die Ausführungen zu § 112 TKG zu verweisen ist. Einer eigenständigen Beurteilung unter Verhältnismäßigkeitsgesichtspunkten bedarf § 113 TKG allein, als sein tatbestandliches Anwendungsfeld – jenseits des großen sachlichen Überschneidungsbereichs von §§ 112 und 113 TKG, der den eigentlichen Kern der Bestandsdatenauskunft ausmacht – in einzelnen Randbereichen über § 112 TKG hinausgeht. Drei Aspekte sind hierbei zu unterscheiden:

(1) Kein Verstoß gegen den Verhältnismäßigkeitsgrundsatz kann erstens darin erblickt werden, dass der Kreis der auskunftsberechtigten Stellen in § 113 Abs. 1 TKG über den des § 112 Abs. 2 TKG hinausgeht. Der relevante Unterschied besteht vor allem darin, dass nicht allein die polizeiliche, sondern auch die ordnungsbehördliche Gefahrenabwehr, sowie dass über die Strafverfolgung hinaus auch die gesamte Verfolgung von Ordnungswidrigkeiten in das manuelle Auskunftsverfahren einbezogen ist.

BerlKommTKG/Kleszczewski, 2006, § 113, Rn. 7; Gramlich in: Manssen, Telekommunikations- und Multimediarecht, § 89, Rn. 133.

Zu bedenken ist hierbei, dass es vor allem technische und praktische Gründe sein dürften, die dazu geführt haben, die ordnungsbehördliche Gefahrenabwehr sowie die Ordnungswidrigkeitenverfolgung nicht in das Verfahren nach § 112 TKG einzubeziehen. Die Einbeziehung auch aller mit diesen Aufgaben betrauten Behörden in das automatisierte Verfahren nach § 112 TKG hätte angesichts der großen Zahl dieser Behörden einerseits und der erfahrungsgemäß eher geringen Häufigkeit von Auskunftersuchen dieser Behörden einen übertriebenen praktischen und technischen Aufwand (Registrierung, technische Vorkehrungen etc.) bedeutet. Nicht jedoch kann der Differenzierung des Kreises der auskunftsberechtigten Stellen etwa eine gesetzgeberische Wertung dahingehend entnommen werden, die allein in § 113 TKG, nicht jedoch in § 112 TKG aufgeführten Aufgaben seien etwa als weniger wichtig oder von geringerer eingriffsrechtfertigender Kraft. Dies kann schon deswegen nicht richtig sein, weil § 113 TKG, wie im Folgenden noch zu erörtern sein wird, ja auch in anderer Hinsicht – je nach den Umständen des Einzelfalls – sogar weiter gehende Rechtsfolgen (hinsichtlich des Kreises der auskunftspflichtigen Diensteanbieter, hinsichtlich der Art der abzufragenden Daten) zu tragen vermag, als dies bei § 112 TKG der Fall ist. Es wäre überdies aber auch in der Sache falsch: Es ist nicht ersichtlich, weshalb der ordnungsbehördlichen Gefahrenabwehr von Verfassungs wegen etwa geringeres Gewicht zukommen sollte als der polizeilichen. Und auch das Gewicht der Verfolgung von Ordnungswidrigkeiten sollte nicht unterschätzt werden: Freilich mag die Strafverfolgung – d.h. die Verfolgung kriminellen Unrechts – bedeutender sein als

die Verfolgung von Ordnungswidrigkeiten; nichtsdestoweniger stellt jedoch auch die ordnungswidrigkeitsrechtliche Sanktionsbewehrung ein unverzichtbares Instrument zur Sicherung der Unverbrüchlichkeit der Rechtsordnung und somit zum Schutz der öffentlichen Sicherheit dar. Die Einbeziehung der Ordnungswidrigkeitenverfolgung hält sich folglich voll und ganz innerhalb der den §§ 111 ff. TKG zugrunde liegenden Grundwertung, dass die Bestandsdaten für Sicherheitszwecke zur Verfügung stehen sollen. Es ist nur folgerichtig, dass einzelne Ordnungswidrigkeitstatbestände ja durchaus auch vom automatisierten Verfahren nach § 112 TKG erfasst werden (§ 112 Abs. 2 Nr. 7). Auch die ordnungsbehördliche Gefahrenabwehr sowie die Ordnungswidrigkeitenverfolgung haben demnach hinreichendes Gewicht, um den in einem Bestandsdatenabruf liegenden Eingriff in das Recht auf informationelle Selbstbestimmung zu rechtfertigen.

(2) Unter Verhältnismäßigkeitsgesichtspunkten unproblematisch ist es auch, dass – anders als bei § 112 TKG – im Rahmen des manuellen Auskunftsverfahrens des § 113 TKG auch Unternehmen, die ihre Dienste nicht für die Öffentlichkeit erbringen (interne und geschlossene Nutzergruppen, d.h. insbesondere unternehmensinterne Nebenstellenanlagen, Universitätsnetze, Telefonanlagen in Hotels etc.) zu den auskunftspflichtigen Stellen gehören. Der Grund, warum sie nicht bereits § 112 TKG unterstellt wurden, ist erneut ein in erster Linie technisch-praktischer: All diese Nebenstellenanlagen dem automatisierten Auskunftsverfahren (mit all seinen technischen Anforderungen, Kosten usw.) zu unterwerfen, würde nicht nur für die Bundesnetzagentur einen unsachgemäßen Aufwand bedeuten, sondern müsste auch gegenüber den nicht-öffentlichen Diensteanbietern als unverhältnismäßig erscheinen.

Vgl. BT-Drucks. 16/2316; der zu weit geratene § 90 TKG a.F. hatte an sich noch bis zu 400.000 Diensteanbieter erfasst; tatsächlich konnten aber nur ca. 72 Unternehmen in das automatisierte Verfahren einbezogen werden; siehe auch BerlKommTKG/Kluszczewski, § 111, Rn. 3, § 113, Rn. 3.

Nicht jedoch ist es so, dass die Zugriffsmöglichkeit der Sicherheitsbehörden auf die Bestandsdaten derartiger Nebenstellenanlagen weniger wichtig wäre. Sinn des § 113 TKG ist es insoweit, wenigstens eine manuelle Auskunft möglich zu machen, wo eine Einbeziehung in das automatisierte Verfahren nicht praktikabel ist. Der Zugriff auf die Bestandsdaten nicht-öffentlicher Anbieter ist auch nicht etwa deswegen besonders problematisch, weil, wie in der Beschwerdeschrift angedeutet, über eine derartige Auskunft besondere Lebenslagen (Anwesenheit in einem Hotel, in einem Krankenhaus etc.) näher ausgeforscht werden könnten.

Beschwerdeschrift, S. 10 f.

Das hierzu Notwendige ist bereits oben in A.I. (S. 10 f.) gesagt worden: Es ist praxisfremd zu meinen, das Auskunftsverfahren würde in dieser Weise eingesetzt. Zu be-

denken ist dabei, dass man bei § 113 TKG mangels zentraler Auskunftsstelle bereits wissen muss, bei welchem nicht-öffentlichen Diensteanbieter man anfragt; es müssen also bzgl. der angeblich erst auszuforschenden Lebenssituation (Zugehörigkeit zu einem Unternehmen, Krankenhausaufenthalt, Hotelbesuch) bereits feste Kenntnisse oder ein zumindest konkreter Verdacht bestehen; damit aber liegt eine Situation vor, in der die Behörde typischerweise nicht gerade die Auskunft nach § 113 TKG braucht, um die entsprechende Information zu erhalten. Vielmehr ist es in derartigen Situationen weitaus einfacher und effektiver, vor Ort, durch Zeugenbefragungen o.ä., zum Ergebnis zu kommen. Das Auskunftsverfahren wird folglich auch hier gerade nicht dazu eingesetzt, um derartige Lebensumstände aufzuklären, sondern um telekommunikationsspezifische Auskünfte (Rufnummer, feste IP-Adresse, PIN) zu erhalten, die man ansonsten gerade nicht bekommt.

(3) Kein Verstoß gegen das Verhältnismäßigkeitsprinzip ist schließlich darin zu sehen, dass § 113 TKG je nach den Umständen des Einzelfalles auch den Zugriff auf nach § 95 TKG freiwillig erhobene Bestandsdaten erlaubt, die über den engeren Kreis des nach § 111 TKG verpflichtend zu speichernden Bestandsdatensatzes hinausgehen können.

- Was speziell den Zugriff auf PIN und PUK (§ 113 Abs. 1 S. 2 TKG) anbelangt, so trifft es nicht zu, dass diese Daten, bloß weil sie ggf. Voraussetzung für den Zugriff auf Verkehrsdaten oder eine Mailbox sind, etwa besonders schutzwürdig wären (anders die Beschwerdeschrift, S. 80, 85). Das hierzu Entscheidende ist bereits oben bei I.1 (S. 35) ausgeführt worden. So wie der allgemeine Zugriff auf Bestandsdaten nach §§ 112, 113 TKG nicht etwa allein deswegen besonders problematisch ist, wenn er der Vorbereitung einer Telefonüberwachung dient,

Bestandsdateneingriff und Telekommunikationsüberwachung sind vielmehr zwei zu unterscheidende Eingriffe. Der eigentlich „brisante“ Eingriff ist allein die Telekommunikationsüberwachung, dessen Brisanz jedoch vollständig dadurch „abgearbeitet“ wird, dass die hierfür bestehenden besonderen gesetzlichen Voraussetzungen vorliegen müssen. Der vorgelagerte Bestandsdateneingriff für sich genommen lässt genauso wenig Rückschlüsse auf Kommunikationsinhalte oder -umstände zu wie sonst auch.

so ist auch der Zugriff auf PIN und PUK nicht etwa deswegen problematischer, weil er z.B. der Vorbereitung der Kenntnisnahme von Verkehrsdaten dient (wenn etwa – so der typische Fall – ein sichergestelltes Mobiltelefon erst mittels PIN und PUK entsperrt werden muss, um die darauf gespeicherten Verkehrsdaten abzurufen). Die besondere Problematik der Sicherstellung von Mobiltelefonen zum Zweck der Kenntnisnahme von Verkehrsdaten wird bereits vollständig von den hierfür einschlägigen Befugnisgrundlagen der StPO (§§ 94 ff., 102 ff.) „abgearbeitet“; das Bundesverfas-

sungsgericht hat im Einzelnen dargelegt, welche Anforderungen (obwohl kein Eingriff in Art. 10 GG anzunehmen ist) hierbei einzuhalten sind.

BVerfG, Urteil vom 2.3.2006 – 2 BvR 2099/04.

Der hiervon zu unterscheidende Zugriff auf PIN und PUK, der erst die Voraussetzungen für diese – anderweitig gerechtfertigte – Kenntnisnahme schafft, für sich genommen indes lässt ebenso wenig den Schluss auf irgendwelche Kommunikationsinhalte und -umstände zu wie andere Bestandsdatenauskünfte auch. Es ist nur folgerichtig, dass er auch keine andere Befugnisgrundlage braucht als gewöhnliche Bestandsdatenzugriffe (z.B. §§ 161, 163 StPO i. V. m. § 113 TKG).

Siehe auch Thiede, Kriminalistik 2004, 104/105. Gleiches würde gelten, wenn im Einzelfall mittels der Auskunft über PIN/PUK ein Eingriff in Art. 10 GG vorbereitet werden soll (zur Möglichkeit einer derartigen Fallkonstellation: BeckTKG-Komm/Bock, 3. Aufl. 2006, § 113, Rdnr. 20).

- Was den Zugriff auf sonstige ggf. nach § 95 TKG gespeicherte Bestandsdaten betrifft, die über § 112 TKG nicht erfragt werden können (z.B. E-Mail-Adressen, feste IP-Adresse, Kontonummer, Beruf, sonstige Vertragsbesonderheiten), so ist zu unterscheiden. Zum Teil sind Informationen erfasst, die von vornherein keine erhöhte Schutzwürdigkeit im Vergleich zu den normalen Bestandsdaten nach § 111 TKG aufweisen: Etwa die E-Mail-Adresse oder eine feste IP-Adresse sind unter den Bedingungen moderner Kommunikation grundlegende Identifikationsdaten zur Erreichbarkeit und telekommunikativen Verortung einer Person, die sich hinsichtlich Schutzwürdigkeit von z.B. einer Rufnummer oder einer Wohnadresse nicht grundsätzlich unterscheiden. Anders liegt es hingegen bzgl. sonstiger Vertragsinformationen, bei denen jedenfalls zum Teil denkbar ist, dass sie nicht zum Kreis jener grundlegenden Identifikationsdaten zu rechnen sind, um die es ansonsten bei der Bestandsdatenabfrage geht (z.B. die Nummer des Bankkontos, von dem aus Rechnungen bezahlt werden; Informationen über das Zahlungsverhalten, über besondere Vertragsmodalitäten, z.B. billiger anzurufende Anschlüsse, über den Beruf im Falle von Sondertarifen etc.). Die Meinungen diesbezüglich gehen auseinander: Während ein Teil der Literatur und auch der Bundesdatenschutzbeauftragte eine einschränkende Auslegung des § 113 TKG befürworten, wonach allein Auskünfte mit spezifischem Kommunikationsbezug (also z.B. nicht Auskünfte über Bankkonten) von § 113 TKG gedeckt sein sollen,

BfD-Info 5, S. 60 f; BerlKommTKG/Kluszczewski, 2006, § 113 Rn. 6; BeckTKG-Komm/Büchner, 2. Aufl. 2000, § 89, Rn. 45.

sieht sich die Praxis der Sicherheitsbehörden nicht daran gehindert – freilich stets nur, soweit dies im Einzelfall erforderlich ist – auch Auskunft über solche Daten zu verlangen, da auch diese Daten Vertragsdaten i. S. v. § 95 TKG seien.

Nach BeckTKG-Komm/Bock, 3. Aufl. 2006, § 113, Rn. 15 werden von der Diensteanbietern dergleichen Auskünfte auch erteilt.

Nach hier vertretener Ansicht ist eine einschränkende Auslegung jedenfalls nicht aus verfassungsrechtlichen Gründen zwingend. Der unter Umständen geringfügig erhöhten Schutzwürdigkeit der Daten (auch hier wird es kaum jemals um Daten mit wirklich intensivem Persönlichkeitsbezug gehen) lässt sich mithilfe des in § 113 TKG normierten Erforderlichkeitskriteriums nämlich in einer dem Verhältnismäßigkeitsprinzip voll und ganz genügenden Weise Rechnung tragen. Das Erforderlichkeitsprinzip verlangt, dass gerade auch der Umfang der Auskunft (Welche Bestandsdaten werden erfragt?) stets auf das im Einzelfall (vgl. § 113 Abs. 1 S. 1 TKG: „im Einzelfall“) nötige Maß beschränkt wird.

Es ist demnach keineswegs so, dass etwaige besondere Bestandsdaten ohne weiteres oder routinemäßig abgefragt werden dürften. Vielmehr bedarf es stets einer einzelfallbezogenen Prüfung der Erforderlichkeit in der je spezifischen Ermittlungssituation. Legt man aber eine auf die spezifische Ermittlungssituation bezogene Erforderlichkeitsprüfung zugrunde, so ist nicht ersichtlich, weshalb mit ihr nicht dem Verhältnismäßigkeitsgrundsatz genügt werden könnte. Hinzu kommt schließlich: Selbst wenn man – entgegen der hier vertretenen Ansicht – der Meinung sein sollte, das Erforderlichkeitskriterium sei unzureichend und z.B. eine strengere Eingriffsschwelle vonnöten, so wäre dies jedenfalls nicht § 113 TKG anzulasten. Nicht vergessen werden darf hierbei, dass § 113 TKG nur die telekommunikationsrechtlichen Voraussetzungen dafür schafft, dass eine Bestandsdatenabfrage verlässlich möglich ist. Der Telekommunikationsgesetzgeber stellt den verschiedensten Sicherheitsbehörden gleichsam eine Auskunftsquelle zur Verfügung und kann hierbei gar nicht anders, als die Pflicht zur Auskunft an ein mehr oder weniger allgemeines Erforderlichkeitskriterium zu binden. Die Frage, ob es im Blick auf das informationelle Selbstbestimmungsrecht und das Verhältnismäßigkeitsprinzip für eine bestimmte Sicherheitsbehörde in einer bestimmten Ermittlungssituation zulässig ist, sich der Auskunftsquelle zu bedienen und ein bestimmtes Datum – z.B. eine Kontonummer – auch wirklich zu erheben, ist eine Frage, die – abgestimmt auf die spezifischen Eigenarten der jeweiligen Sicherheitsbehörde und Sicherheitsaufgabe – allein das Fachrecht beantworten kann und auch muss. Sollte man – anders als hier vertreten – für bestimmte Datenarten also wirklich besondere, über das Erforderlichkeitskriterium hinausgehende Anforderungen verlangen wollen, so wäre es jedenfalls das Fachrecht – und nicht § 113 TKG –, das diese zu statuieren hätte.

- Zu bedenken ist schließlich: Alle Zugriffsrechte der Sicherheitsbehörden auf über den Kreis der verpflichtend vorzuhaltenden Daten nach § 111 TKG hinausgehende Bestandsdaten nach § 113 TKG stehen von vornherein unter dem Vorbehalt, dass sie nur Erfolg haben werden, soweit diese Daten von den Diensteanbietern für

eigene Zwecke erhoben worden und daher – unabhängig von staatlichen Sicherheitsinteressen – ohnehin rechtmäßigerweise vorhanden sind. Dem staatlichen Zugriff nach § 113 TKG mit seinen speziellen Eingriffsvoraussetzungen vorgelagert ist daher stets die weitere tatbestandliche Voraussetzung, dass ein privater Unternehmer berechtigt war, das Datum für eigene Zwecke zu erheben (Erforderlichkeitskriterium des § 95 Abs. 1 TKG), und von diesem Recht auch tatsächlich Gebrauch gemacht hat. Das Zugriffsrecht der Sicherheitsbehörden ist so gesehen kein absolutes, sondern ein relatives – das Gewicht des Eingriffs scheint insoweit reduziert.

#### bb) Bestimmtheit

Bereits unter 1.c.aa. (S. 70 f.) ist ausgeführt worden, dass § 113 Abs. 1 TKG – entgegen den Einlassungen der Beschwerdeführer (S. 80) und einzelnen Stimmen der Literatur – nicht etwa zu unbestimmt ist und daher auch nicht gegen das rechtsstaatliche Bestimmtheitsgebot verstößt. Die Zahl der berechtigten Behörden mag groß und die Einsatzfelder mögen breit sein, nicht jedoch sind sie zu unbestimmt, d.h. in ihren Konturen zu unscharf. Vielmehr lässt sich von den in § 113 Abs. 1 TKG aufgeführten Aufgaben zweifelsfrei auf die berechtigten Behörden zurückschließen; Gefahrenabwehr, Verfolgung von Ordnungswidrigkeiten – all dies sind klar subsumierbare Rechtsbegriffe. Ein zugegebenermaßen breites Einsatzfeld ist damit konturenscharf umrissen. Ein Verstoß gegen das Bestimmtheitsgebot kann hierin nicht gesehen werden.

#### cc) Benachrichtigung, Auskunftsrechte

Bezüglich der Frage etwaiger Benachrichtigungspflichten gegenüber dem Betroffenen bzw. etwaiger Auskunftsansprüche des Betroffenen kann weitgehend auf das unter § 112 TKG Ausgeführte (2.c.bb., S. 80 ff.) verwiesen werden. Auch hier ist es so, dass etwa die Regelung des § 113 Abs. 1 S. 4 TKG, wonach das verpflichtete Unternehmen gegenüber seinen Kunden Stillschweigen zu bewahren hat, keineswegs verhindern will, dass ggf. nach dem jeweiligen Fachrecht Benachrichtigungspflichten der Sicherheitsbehörde bzw. Auskunftsrechte gegen sie bestehen. Zweck des § 113 Abs. 1 S. 4 TKG ist es, zusätzliche datenschutzrechtliche Gefahren (durch Inkennntnissetzung Dritter) auszuschließen, sowie ansonsten jedenfalls nicht die Unternehmen mit der schwierigen Frage zu behelligen, inwieweit unter Abwägung von Kenntnisnahme- und Sicherheitsinteressen Auskunft zu geben oder zu verweigern ist. Vielmehr handelt es sich hierbei um eine Frage, die sinnvoll und auf die spezifischen Bedürfnisse des jeweiligen Rechtsgebiets abgestimmt allein vom Fachgesetzgeber beantwortet werden kann.

Auch in der Sache wird man die bestehende Rechtslage im Hinblick auf Benachrichtigung und Auskunft, wie sie sich aus § 113 TKG i. V. m. dem jeweiligen Fachrecht oder subsidiär den allgemeinen Datenschutzgesetzen ergibt, nicht angreifen können. Soweit Maßnahmen nach § 113 TKG im Zusammenhang mit Art. 10 GG-Eingriffen erfolgen, sorgt das hierfür maßgebliche Recht (z.B. § 101 StPO) in den hierfür allgemein bestehenden Grenzen (die hier nicht nachzuprüfen sind) für die erforderliche Benachrichtigung; erfolgt z.B. ein Zugriff auf PIN/PUK im Zusammenhang mit einer offen durchgeführten Durchsuchung und Sicherstellung, ist regelmäßig schon rein faktisch sichergestellt, dass der Betroffene in Bezug auf die Möglichkeit der Kenntnisnahme von Telekommunikationsdaten gewarnt ist. Ansonsten jedoch treffen die einschlägigen Gesetze (namentlich die StPO, die Polizeigesetze, die Nachrichtendienstgesetze) ganz allgemein – d.h. *auch* bzgl. Daten nach § 113 TKG – die Wertung, dass Betroffene nicht über jede verborgene Datenerhebung zu informieren sind. Dies kann, wie im Zusammenhang mit § 112 TKG gezeigt, jedenfalls bezüglich Daten unterer Schutzwürdigkeitsstufe (wie bei Bestandsdaten regelmäßig der Fall) und einer routinemäßigen Datenerhebungserlaubnis des Gesetzgebers (die dem Eingriff das Unerwartete nimmt) nicht beanstandet werden; jedenfalls gewöhnliche Bestandsdateneingriffe nach § 113 TKG lösen demnach keine Benachrichtigungspflicht aus. Allein bei den oben behandelten Zugriffen auf besondere, ggf. schutzwürdigere Bestandsdaten, die einer strengeren Erforderlichkeitsprüfung im Einzelfall zu unterziehen sind (z.B. Kontonummer), könnte man überlegen, ob eine diesbezügliche ausnahmsweise Benachrichtigungspflicht greifen könnte. Aber auch hier – jenseits von Eingriffen der unteren Stufe – bewegt man sich noch in einem Bereich, den das Recht der Sicherheitsbehörden auch im Allgemeinen nicht als so gravierend ansieht, dass hier etwa durchgehend Benachrichtigungspflichten bestünden. Als ausreichend müssen daher die allgemeinen Auskunftsansprüche und Verfahrensrechte des jeweiligen Fachrechts, hilfsweise des allgemeinen Datenschutzrechts (z.B. § 19 BDSG) angesehen werden, welche in einer allgemeinen und insoweit auch unbeanstandet gebliebenen Weise versuchen, einen Ausgleich zwischen den relevanten Informations- und Geheimhaltungsinteressen zu finden.

Keinen Unterschied macht es in diesem Zusammenhang, dass einige der in § 112 TKG normierten Schutzmechanismen – Missbrauchskontrolle durch die Bundesnetzagentur, Datenschutzkontrolle durch den Bundesdatenschutzbeauftragten, § 112 Abs. 4 TKG – bei § 113 TKG mangels zentral zwischengeschalteter Bundesnetzagentur naturgemäß nicht greifen können. Der Wegfall der Missbrauchskontrolle durch die Bundesnetzagentur wird dadurch kompensiert, dass bei § 113 TKG (an-

ders als bei § 112 TKG) gerade die auskunftsverpflichteten Unternehmen mit der Sache befasst werden und zu einer Nachprüfung der formellen Zulässigkeit des Auskunftersuchens in der Lage sind.

Zur Reichweite des Prüfungsrechts: Trute, in Trute/Spoerr/Bosch, TKG, 2001, § 89, Rn. 54; BeckTKG-Komm/Bock, 3. Aufl. 2006, § 113, Rdnr. 7, 9. Die erhebliche Anzahl an Rechtsstreitigkeiten um die Rechtmäßigkeit einer Inanspruchnahme von Unternehmen nach § 113 TKG im Zusammenhang mit Auskunftersuchen bzgl. dynamischen IP-Adressen (siehe dazu oben I.1., S. 36) macht hierbei auch deutlich, dass sich die Unternehmen nicht scheuen, den Rechtsweg zu beschreiten, wenn sie ein Auskunftersuchen für unberechtigt halten.

Hinsichtlich der Datenschutzkontrolle ist zu betonen, dass diese bei den ersuchenden Sicherheitsbehörden freilich unberührt bleibt.

dd) Sonstiges

Hinsichtlich Fragen der Zweckbindung und Protokollierung durch die Sicherheitsbehörden kann auf oben 2c.cc. (S. 86 f.) verwiesen werden; einschlägig ist insoweit allein das jeweilige Fachrecht. Auch die Notwendigkeit einer Evaluierung ist mit den bei 2.c.cc. dargelegten Gründen abzulehnen.

d) Zitiergebot

Das Zitiergebot gilt für Eingriffe in das Recht auf informationelle Selbstbestimmung nicht.

e) Teilergebnis

Grundrechte der Beschwerdeführer werden durch § 113 TKG nicht verletzt.

**D) Gesamtergebnis**

Die Verfassungsbeschwerde ist allenfalls teilweise zulässig. Auch soweit sie zulässig ist, ist sie jedenfalls unbegründet.

Bayreuth, den 22.1.2007

Prof. Dr. [Redacted]

## Anhang: Inhaltsübersicht:

|           |                                                                                                                                                           |           |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| <b>A)</b> | <b>Zum Sachverhalt</b>                                                                                                                                    | <b>2</b>  |
| I.        | Vorgeschichte                                                                                                                                             | 2         |
| II.       | Zur heutigen Praxis und Praxisbedeutung der Auskunftsverfahren                                                                                            | 7         |
| III.      | Der nationale und europäische Regelungskontext                                                                                                            | 15        |
| <b>B)</b> | <b>Zur Zulässigkeit der Verfassungsbeschwerde</b>                                                                                                         | <b>18</b> |
| I.        | Sind die Beschwerdeführer durch §§ 112, 113 TKG selbst, gegenwärtig und unmittelbar betroffen?                                                            | 18        |
| II.       | Weitere Probleme der Beschwerdebefugnis, insbesondere zur Unzulässigkeit der Rügen gegen § 95 Abs. 3 und 4 TKG                                            | 20        |
| III.      | Subsidiarität der Verfassungsbeschwerde                                                                                                                   | 23        |
| <b>C)</b> | <b>Zur Begründetheit der Verfassungsbeschwerde</b>                                                                                                        | <b>25</b> |
| I.        | Übergreifende Fragestellungen                                                                                                                             | 25        |
| 1.        | Berührt ist nicht das Fernmeldegeheimnis (Art. 10 GG), sondern allein das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 iVm 1 Abs. 1 GG).     | 25        |
| 2.        | Keine Verletzung des Gleichheitssatzes (Art. 3 Abs. 1 GG)                                                                                                 | 36        |
| 3.        | Das Zusammenspiel von §§ 112, 113 TKG einerseits und dem jeweils einschlägigen Fachrecht der ersuchenden Behörde (StPO, Polizeigesetze etc.) andererseits | 39        |
| 4.        | Zum Gewicht der mit §§ 111 ff. TKG verfolgten Zwecke                                                                                                      | 49        |
| II.       | Zu den angegriffenen Normen im Einzelnen                                                                                                                  | 51        |
| 1.        | § 111 TKG                                                                                                                                                 | 51        |
| a)        | Das berührte Grundrecht                                                                                                                                   | 51        |
| b)        | Eingriff                                                                                                                                                  | 51        |
| c)        | Verfassungsrechtliche Rechtfertigung                                                                                                                      | 53        |
| aa)       | Einschränkbarkeit des Grundrechts                                                                                                                         | 53        |
| bb)       | Gewicht des Eingriffs                                                                                                                                     | 53        |

|     |                                                                                               |     |
|-----|-----------------------------------------------------------------------------------------------|-----|
| cc) | Gewicht der verfolgten Zwecke                                                                 | 59  |
| dd) | Verhältnismäßigkeit                                                                           | 59  |
| ee) | Insbesondere zur „Vorratsdatenspeicherung“ und zur<br>hinreichenden Bestimmtheit ihrer Zwecke | 68  |
| ff) | Zitiergebot                                                                                   | 71  |
| d)  | Teilergebnis                                                                                  | 72  |
| 2.  | § 112 TKG                                                                                     | 72  |
| a)  | Das berührte Grundrecht                                                                       | 72  |
| b)  | Eingriff (einschließlich: Zurechenbarkeit und Intensität<br>des Eingriffs)                    | 72  |
| c)  | Verfassungsrechtliche Rechtfertigung                                                          | 75  |
| aa) | Zu den Eingriffsvoraussetzungen                                                               | 75  |
| bb) | Zur Frage der Benachrichtigung bzw. von<br>Auskunftsrechten Betroffener                       | 80  |
| cc) | Weitere Rügen                                                                                 | 86  |
| dd) | Unvollständige Abfragedaten/Ähnlichkeitenfunktion<br>(§ 112 Abs. 1 S. 4, Abs. 3 TKG)          | 87  |
| d)  | Zitiergebot                                                                                   | 94  |
| e)  | Teilergebnis                                                                                  | 94  |
| 3.  | § 113 TKG                                                                                     | 94  |
| a)  | Das berührte Grundrecht                                                                       | 94  |
| b)  | Eingriff                                                                                      | 95  |
| c)  | Verfassungsrechtliche Rechtfertigung                                                          | 95  |
| aa) | Verhältnismäßigkeit                                                                           | 95  |
| bb) | Bestimmtheit                                                                                  | 101 |
| cc) | Benachrichtigung, Auskunftsrechte                                                             | 101 |
| dd) | Sonstiges                                                                                     | 103 |
| d)  | Zitiergebot                                                                                   | 103 |
| e)  | Teilergebnis                                                                                  | 103 |
| D)  | Gesamtergebnis                                                                                | 103 |



## Stellungnahme

des

### Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

zur

#### Verfassungsbeschwerde

1. d. [REDACTED]
2. d. [REDACTED]  
jeweils gegen die §§ 88 Abs. 3 Satz 1, 92, 95 Abs. 3 S. 3 und Abs. 4, 100, 111,  
112, 113 des Telekommunikationsgesetzes (TKG) vom 22. Juni 2004 (BGBl I  
S. 1190)
- sowie der
3. d. [REDACTED]  
vertreten durch den Geschäftsführer [REDACTED]  
[REDACTED]
4. d. [REDACTED]  
vertreten durch die Geschäftsführerin [REDACTED]  
[REDACTED]
5. d. [REDACTED]  
jeweils gegen § 95 Abs. 3 und § 110 des Telekommunikationsgesetzes (TKG)  
vom 22. Juni 2004 (BGBl I S. 1190)

- Verfahrensbevollmächtigter zu 1 bis 5 : Rechtsanwalt Meinhard Starostik,  
Schlüterstraße 38,  
10629 Berlin -



Die Vorschriften über den Datenschutz in der Telekommunikation waren aufgrund der Europäischen Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG) vom 12. Juli 2002 durch das Gesetz vom 22. Juni 2004 in das Telekommunikationsgesetz (TKG) integriert worden. Die Tatsache der Eingliederung der früheren Telekommunikations-Datenschutzverordnung in den siebten Teil des Telekommunikationsgesetzes (TKG 2004) habe ich in meinem 20. Tätigkeitsbericht (Nr. 13.1) grundsätzlich begrüßt, da hierdurch eine Vereinfachung im Datenschutz erreicht und Doppelregelungen abgeschafft wurden. In diesen Teil des Telekommunikationsgesetzes fallen auch die von den Verfahrensbeteiligten gerügten Vorschriften des Telekommunikationsgesetzes, die bereits im Gesetzgebungsverfahren von den Datenschutzbeauftragten des Bundes und der Länder in ihrer Entschließung vom 21. November 2003 (abgedruckt in meinem 20. Tätigkeitsbericht, S. 136) kritisiert worden war. Insbesondere haben die Datenschutzbeauftragten des Bundes und der Länder bemängelt, dass den Strafverfolgungsbehörden, der Polizei und den Nachrichtendiensten ohne Bindung an einen Straftatenkatalog oder einen Richtervorbehalt der Zugriff auf Passwörter, PINs, PUKs usw. eröffnet werden soll, mit denen die Inhalte oder nähere Umstände einer Telekommunikation geschützt werden. Hierdurch wird die Gefahr eines unkontrollierten Gebrauches dieser Befugnis eröffnet. Außerdem haben die Datenschutzbeauftragten darauf hingewiesen, dass die Befugnis zudem häufig ins Leere laufen dürfte, da die Anbieter diese Daten aus Gründen der Datensicherheit für sie selbst unlesbar verschlüsselt speichern.

Zur Vereinbarkeit der von den Verfahrensbeteiligten gerügten Regelungen mit dem Grundgesetz nehme ich wie folgt Stellung:

### **I. Schutzbereich des Fernmeldegeheimnisses (Art. 10 GG)**

Wesentlicher verfassungsrechtlicher Maßstab der hier angesprochenen Regelungen im Telekommunikationsgesetz ist Art. 10 GG, der die vertrauliche Inanspruchnahme der Telekommunikation frei von staatlicher Kenntnisnahme schützt (Fernmeldegeheimnis). Die Inanspruchnahme der Telekommunikation unterliegt besonderem Schutz, da sie besonderen Gefährdungen der Kenntnisnahme durch Dritte ausgesetzt ist (BVerfG, Beschluss vom 9. Oktober 2002 - 1 BvR 1611/96, 805/98 -, BVerfGE 106, S. 28 [36] m.w. Nachw.). Dabei sind nach ständiger Rechtsprechung des BVerfG nicht nur die Inhalte der Kommunikation, sondern auch deren nähere Umstände (insbesondere ob, wann und wie oft zwischen welchen Personen oder Anschlüssen Kommunikation stattgefunden hat) vom Fernmeldegeheimnis geschützt (vgl. BVerfG, Urteil vom 14. Juli 1999 - 1 BvR 2226/94, 2420, 2437/95 -, BVerfGE 100, S. 313 [358] m.w.N., BVerfG, Urteil vom 12. März 2003 - 1 BvR 330/96, 348/99, BVerfGE 107, S. 299 [312 f.]). Das Fernmeldegeheimnis begründet zudem nicht nur ein Abwehrrecht gegen den Staat, sondern eine Schutzpflicht des Staates, Zugriffe von privaten Dritten zu unterbinden ((BVerfG, Urteil vom 9. Oktober 2002, BVerfGE 106, S. 28 [37]).



Dem Schutz des Art. 10 GG unterfallen deshalb auch die so genannten Verkehrsdaten im Sinne des § 3 Nr. 30 Telekommunikationsgesetz 2004 (im Urteil des BVerfG vom 12. März 2003, a.a.O., Verbindungsdaten genannt). Sie sind definiert als „Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden“ (§ 3 Nr. 30 TKG 2004). Dazu gehören im Wesentlichen:

- die Nummer oder Kennung der beteiligten Anschlüsse oder der Endeinrichtung,
  - personenbezogene Berechtigungskennungen,
  - bei Verwendung von Kundenkarten auch die Kartenummer,
  - bei mobilen Anschlüssen auch die Standortdaten,
  - den Beginn und das Ende der jeweiligen Verbindung nach Datum und Uhrzeit
- und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen,
- den vom Nutzer in Anspruch genommenen Telekommunikationsdienst,
  - die Endpunkte von festgeschalteten Verbindungen, ihren Beginn und ihr Ende nach Datum und Uhrzeit

und, soweit die Entgelte davon abhängen,

- die übermittelten Datenmengen,
- sonstige zum Aufbau und zur Aufrechterhaltung der Telekommunikation

sowie

- zur Entgeltabrechnung notwendige Verkehrsdaten. All diese Daten geben Auskunft über die näheren Umstände der Telekommunikation einzelner Teilnehmer (§ 96 Abs. 1 TKG 2004).

In der Literatur umstritten ist dagegen, ob der Schutzbereich des Fernmeldegeheimnisses auch die so genannten Bestandsdaten im Sinne des § 3 Nr. 3 TKG 2004 umfasst. Bestandsdaten sind die Daten, „die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden“. Dazu gehören Name, Anschrift und Geburtsdatum des Kunden, dessen Kontoverbindungen, Art des kontrahierten Dienstes sowie die dem Kunden zum Gebrauch überlassenen Telekommunikations-einrichtungen, die zugewiesene Rufnummer und PIN zur Ermöglichung der Nutzung des Dienstes, Datum des Vertragsschlusses und -endes etc. (vgl. hierzu nur Säcker, in: Säcker (Hrsg.) Berliner Kommentar zum TKG, § 3 TKG Rdn. 5). Während der Beschwerdeführer zu 1) aus den in der Beschwerdeschrift (S. 10 ff., unter Hinweis auf Breyer, RDV 2003, 218 [218 f.]) genannten Gründen annimmt, dass Bestandsdaten ebenfalls unter den Schutzbereich des Art. 10 GG fallen, lehnt dies die überwiegende Ansicht in der Literatur ab (vgl. Kleczewski, in: Säcker (Hrsg.) Berliner Kommentar zum TKG, § 88 TKG Rdn. 14; vorsichtig ablehnend auch Wuermeling/Felixberger, Fernmeldegeheimnis und Datenschutz, CR 1997, S. 230 [234]). Begründet wird dies damit, dass die Bestandsdaten lediglich die Daten des Teilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung des Vertragsverhältnisses über Telekommunikationsdienste umfassen und sich nicht auf einen konkreten Telekommunikationsvorgang beziehen. Das Fernmeldegeheimnis schützt jedoch in erster Linie die Vertraulichkeit der ausgetauschten Informationen und damit den Kommunikationsinhalt gegen unbefugte Kenntniserlangung durch Dritte (BVerfG,



Urteil vom 2. März 2006 – 2 BvR 2099/04 –, NJW 2006, S. 976 [978]). Zwar kann ein Bestandsdatum, z.B. die Telefonnummer, wenn dieses für einen konkreten Telekommunikationsvorgang benutzt wird, auch zum Verbindungsdatum im Sinne des § 96 Abs. 1 TKG 2004 werden und in diesem Fall dem Schutzbereich des Art. 10 GG unterfallen. Dies mache es aber in seiner Eigenschaft als Bestandsdatum nicht zu einem Datum, das dem Fernmeldegeheimnis unterliegt (Kleczewski, a.a.O.). Aus dem Sinn und Zweck des Fernmeldegeheimnisses aus Art. 10 GG, die Kommunikation zwischen zwei Grundrechtsträgern zu schützen, ist dies überzeugend. Zweck des Art. 10 GG ist es nicht, das Vertragsverhältnis zwischen Telekommunikationsdienstleistungsanbieter und Kunden, losgelöst vom einzelnen Kommunikationsvorgang des Kunden, einem grundrechtlichen Schutz zu unterwerfen. Aus diesen Bestandsdaten ist nur zu entnehmen, dass zwischen den Vertragsparteien ein Vertrag über Telekommunikationsdienstleistungen zustande gekommen ist. Wann der Kunde diese Leistungen, die in ihrer konkreten Ausgestaltung dem Schutzbereich des Art. 10 GG unterliegen, wahrnimmt, ergibt sich aus diesen Daten nicht. Dies bedeutet nicht, dass Bestandsdaten, bei denen es sich ebenfalls um personenbezogene Daten im Sinne des § 3 Abs. 1 BDSG handelt, keinen grundrechtlichen Schutz genießen. Bestandsdaten unterliegen dem Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG.

Zu den einzelnen Vorschriften:

## **II. Verfassungsmäßigkeit des § 95 Abs. 3 TKG 2004 (Löschungsfrist)**

§ 95 Abs. 3 Satz 1 TKG verpflichtet die Diensteanbieter, Bestandsdaten mit Ablauf des auf die Beendigung des Vertragsverhältnisses folgenden Kalenderjahrs zu löschen. Der Wortlaut legt eine „starre“, einzelfallunabhängige Fristregelung ohne Prüfung der Erforderlichkeit weiterer Speicherung bis zum Ende des folgenden Kalenderjahres nahe. Ob angesichts des Wortlautes eine grundrechtsfreundliche Interpretation im Sinne einer Maximalfrist, die erst nach positiv verlaufener Prüfung der weiteren Erforderlichkeit ausgeschöpft werden darf, noch zulässig ist, erscheint zweifelhaft. An der Verfassungsmäßigkeit des § 95 Abs. 3 Satz 1 TKG bestehen deshalb mit Blick auf den Grundsatz der Verhältnismäßigkeit und das Gebot der Normenklarheit dieser Regelung, mit der in das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) eingegriffen wird, Zweifel.

## **III. Vereinbarkeit des § 111 TKG 2004 (Daten für Auskunftersuchen der Sicherheitsbehörden) mit dem Recht auf informationelle Selbstbestimmung Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG**

Nach meiner Auffassung verstößt § 111 TKG 2004 zwar nicht gegen das grundrechtlich durch Art. 10 GG geschützte Fernmeldegeheimnis. Bei den in § 111 Abs. 1 Satz 1 TKG 2004 ge-



nannten Daten handelt es sich um Bestandsdaten im Sinne von § 3 Nr. 3 TKG 2004, die nicht vom Schutzbereich des Art. 10 GG umfasst sind.

Die in § 111 Abs. 1 TKG 2004 aufgestellte Verpflichtung jedes geschäftsmäßigen Erbringers von Telekommunikationsdiensten, bestimmte Bestandsdaten für die Auskunftsverfahren nach §§ 112, 113 TKG 2004 zu erheben und zu speichern, verstößt jedoch gegen das Recht auf informationelle Selbstbestimmung, weil sie nicht dem Grundsatz der Verhältnismäßigkeit entspricht.

Soweit die in § 111 Abs. 1 Satz 1 TKG 2004 aufgeführten Daten auf natürliche Personen zurückzuführen sind, liegen personenbezogene Daten im Sinne des § 3 Abs. 1 BDSG vor, deren verfassungsrechtlicher Schutz durch das Grundrecht auf informationelle Selbstbestimmung gegeben ist. Soweit der Gesetzgeber in § 111 Abs. 1 TKG 2004 anordnet, die dort genannten Daten für Zwecke der Sicherheitsbehörden zu speichern und zu übermitteln – insbesondere wenn diese für die Erfüllung der vertraglichen Pflichten zwischen dem Telekommunikationsanbieter und seinem Kunden nicht benötigt werden – liegt ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung vor.

Die Regelung des § 111 Abs. 1 TKG 2004 ist im Hinblick auf ihre Zweckbestimmung weder geeignet, noch erforderlich und verhältnismäßig im engeren Sinne.

### III.1. Geeignetheit der Norm

Die Erhebungs- und Speicherpflicht aus § 111 Abs. 1 TKG 2004 zielt zwar in erster Linie auf die Nutzer von sog. Prepaid-Karten im Mobilfunk ab, so dass diese nicht mehr anonym telefonieren können sollen. Die Regelung betrifft jedoch auch die Identifikationspflicht bei sämtlichen geschäftsmäßig angebotenen Telekommunikationsdiensten, bei denen die Nutzer Inhaber einer Rufnummer sind. Hierzu gehören z.B. auch Unternehmen und Verwaltungen, die ihren Mitarbeitern die private Nutzung von Telekommunikation ermöglichen, Hotels und Krankenhäuser sowie sonstige geschlossene Benutzergruppen (z.B. Corporate Networks, Schulen, Hochschulen).

Wie sich aus der Systematik und dem Kontext der Vorschrift ergibt, ist der Zweck des § 111 Abs. 1 TKG 2004 ausschließlich, die Daten für die sicherheitsbehördliche Ermittlungstätigkeit auch dann zur Verfügung zu haben, wenn diese Daten für betriebliche Zwecke des Anbieters (vgl. § 95 Abs. 1 TKG) nicht erforderlich sind. Aus der Gesetzesbegründung selbst (BT-Drs. 15/2316, S. 95) lassen sich keine Erkenntnisse zur Notwendigkeit der verpflichtenden Speicherung und Erhebung gewinnen. Dort wird lediglich bei der Begründung der Löschungsfrist (Absatz 1 Satz 4) genauer auf den Hintergrund der Regelung eingegangen.



Bereits bevor es zu der umfassenden Novellierung des Telekommunikationsgesetzes im Jahre 2004 kam, hatte das Bundesministerium für Wirtschaft im Jahr 2002 Entwürfe für eine Änderung des damaligen § 90 TKG 1997 vorgelegt, in dem die gleiche Verpflichtung vorgesehen war. Damals wurde die geplante Regelung vor allem mit der aus Sicht der Sicherheitsbehörden unbefriedigenden Situation begründet, dass gerade im Mobilfunkbereich und hier insbesondere bei den Prepaid-Angeboten Straftäter bewusst und gezielt in kurzen Abständen neue SIM-Karten erwarben, die Karten häufig wechselten, mehrere Karten parallel benutzten oder untereinander tauschten und weitergaben. Allerdings wurde bisher nicht nachvollziehbar und überzeugend dargelegt, inwieweit eine Erhebungs- und Speicherpflicht diese behaupteten Schwierigkeiten lösen kann. Auch eine solche gesetzliche Pflicht kann nicht verhindern, dass Straftäter Strohleute zum Kauf von SIM-Karten auf Prepaid-Basis einsetzen, eine Vielzahl von Karten erwerben, diese mit vielen verschiedenen Personen so oft tauschen, dass damit die Inhaber dieser Karten kaum noch ermittelt werden können. Das Gesetz sieht insoweit zu Recht auch keinerlei Einschränkungen oder weitere Identifizierungspflichten vor, wenn der Erstinhaber einer SIM-Karte diese an Dritte weitergibt. Die Telekommunikationsdiensteanbieter könnten auch nicht verpflichtet werden, eine Weitergabe der SIM-Karte zu kontrollieren.

Die verpflichtende Erhebung und Speicherung bestimmter Bestandsdaten ist daher bereits aus diesem Grund nicht geeignet, ihren Zweck zu erreichen.

Hinzu kommt, dass die von Seiten der Sicherheitsbehörden geschilderten Schwierigkeiten bei der Ermittlung von Anschlussinhabern auch nicht dadurch gelöst werden konnten, dass die Anbieter bereits seit 1997 verpflichtet waren, die Kundendaten auch von Prepaid-Kunden unter Vorlage amtlicher Ausweise nach den Leitlinien der damaligen Regulierungsbehörde zu erheben. Dieses rechtswidrige Verfahren wurde bis zur Rechtskraft des Urteils des BVerwG vom 22. Oktober 2003 (- 6 C 23.02 -, BVerwGE 119, 123) unverändert beibehalten, da die Leitlinien während des gesamten gerichtlichen Verfahrens anwendbar blieben. Trotz dieser über sechs Jahre formal bestehenden rechtlichen Verpflichtung ist ein Sicherheitsgewinn für die berechtigten Stellen nicht dargelegt.

In welchem Umfang und Ausmaß die Verwendung anonym erworbener SIM-Karten tatsächlich die Ermittlungstätigkeit erschwert hat, wurde bislang nicht dargelegt. Zwar wurden Fallgruppen dargelegt, in denen es zu einer Erschwerung der Ermittlungstätigkeit kommen könnte. Ob diese Fälle tatsächlich eine Quantität und Qualität annehmen, dass überhaupt von einer Erschwerung der Ermittlungen gesprochen werden kann, ist ebenfalls nicht dargelegt.

Ergänzend möchte ich darauf hinweisen, dass in anderen Staaten die genannten Daten nicht erhoben werden. Straftäter haben daher auch weiterhin die Möglichkeit, SIM-Karten auf Prepaid-Basis in anderen Ländern anonym zu erwerben und im Rahmen des Roamings in Deutschland zu nutzen.



### III.2. Erforderlichkeit der Norm

Bereits in ihrer Entschlieung vom 24. Mai 2002 „Geplanter Identifikationszwang in der Telekommunikation“ haben die Datenschutzbeauftragten des Bundes und der Lnder (Anlage 1) darauf hingewiesen, dass die Regelung dem in den Datenschutzrichtlinien der Europischen Union verankerten Grundsatz, dass Unternehmen nur solche personenbezogenen Daten verarbeiten drfen, die sie selbst zur Erbringung einer bestimmten Dienstleistung benotigen, widerspricht. Diese Haltung haben die Datenschutzbeauftragten des Bundes und der Lnder in ihrer Entschlieung vom 28. April 2003 „Verbesserung statt Absenkung des Datenschutzniveaus in der Telekommunikation“ unterstrichen (Anlage 2).

§ 111 Abs. 1 TKG 2004 verpflichtet die Telekommunikationsdienstleistungsanbieter zur Speicherung von personenbezogenen Daten, die fur die Durchfuhrung eines Vertragsverhaltnisses i.S.v. § 95 i.V.m. § 3 Nr. 3 TKG nicht erforderlich sind.

Die Regelung in § 111 Abs. 1 TKG 2004 widerspricht den Vorgaben des Bundesverfassungsgerichts, wonach die Sammlung von Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbareren Zwecken nicht mit dem Grundgesetz zu vereinbaren ist (BVerfG, Urteil vom 15. Dezember 1983 - 1 BvR 209 u.a./83 -, BVerfGE 65, 1 [46]). Zum Zeitpunkt der Erhebung der Daten nach § 111 Abs. 1 TKG steht der konkrete Zweck der Erhebung noch nicht fest. Die Zweckbestimmung in den §§ 112, 113 TKG 2004 „Erfullung der gesetzlichen Aufgaben“ (§ 112 Abs. 2 TKG) bzw. Verfolgung von Straftaten oder Ordnungswidrigkeiten, Abwehr von Gefahren fur die offentliche Sicherheit oder Ordnung oder die Erfullung gesetzlicher Aufgaben bestimmter Geheimdienste (§ 113 Abs. 1 TKG 2004) bezieht sich erst auf die spatere Nutzung der Daten im Einzelfall, nicht auf einen tatsachlichen konkreten Nutzungszweck zum Zeitpunkt der Erhebung. Mit Blick auf diese Kernaussage des Volkszahlungsurteiles bestehen deshalb erhebliche Zweifel an der Erforderlichkeit der „auf Vorrat“ und fur einen im Zeitpunkt der Erhebung noch vagen, „eventuellen“ Zweck erhobenen Daten und dem mit der Erhebung und Speicherung verbundenen Eingriff.

Berucksichtigt werden muss auch, dass Bestandsdaten selbst zwar nicht vom Fernmeldegeheimnis geschutzt werden, der Schutzbereich des Art. 10 GG durch § 111 TKG 2004 aber indirekt tangiert wird. Durch die Verpflichtung der Diensteanbieter zur Identifizierung von Telekommunikationsnutzern werden auch vom Fernmeldegeheimnis geschutzte Verkehrsdaten direkt personenbeziehbar. Die Bestandsdaten dienen als Schlussel zur Herstellung des Personenbezugs fur Informationen, die dem besonderen Schutz des Fernmeldegeheimnisses unterliegen. Sie haben den Zweck, etwa bei Manahmen nach §§ 100g, 100h Abs. 1 Satz 2 StPO, bekannte Telekommunikationsvorgange erst einer konkreten Person zuordnen zu konnen. Dieser Aspekt darf bei der Verhaltnismaigkeitsprufung nicht unberucksichtigt bleiben.



Die in § 111 Abs. 1 Satz 4 TKG vorgesehene Löschungsfrist von bis zu zwei Jahren nach Vertragsende verstärkt die Zweifel an der Erforderlichkeit des § 111 TKG 2004 noch. Die Gesetzesbegründung führt hierzu lediglich aus, dass die Strafverfolgungsbehörden „nicht selten“ vor der Situation stünden, dass Bestandsdaten nach Vertragsende nicht mehr vorhanden seien. Weder wird dies quantitativ belegt, noch kann der qualitative Gehalt dieser Aussage wegen ihrer Allgemeinheit überprüft werden. Auch wird nicht belegt, dass die Länge der Frist den Erfordernissen der berechtigten Stellen angemessen Rechnung trägt oder ob eine wesentlich kürzere Frist hierfür auch ausreichen würde.

### III.3. Angemessenheit der Norm

Durchgreifende Bedenken bestehen schließlich auch unter dem Aspekt der Angemessenheit. Die Verpflichtung nach § 111 Abs. 1 TKG 2004 gilt für alle Anbieter, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken. Sie beschränkt sich nicht auf Anbieter, die öffentlich Telekommunikationsdienstleistungen anbieten, sondern bezieht sich auf jeden, der nachhaltig – auch ohne Gewinnerzielungsabsicht – Telekommunikation erbringt (vgl. § 3 Nr. 10 TKG 2004). Damit sind auch Betreiber von Hotels, Krankenhäusern, Corporate Networks, aber auch Unternehmen und Behörden verpflichtet, wenn sie ihren Mitarbeitern die private Nutzung der dienstlichen Telekommunikationsanlagen erlauben. In diesen Fällen lassen sich ebenfalls bereits durch die Identität des Anbieters weitere Rückschlüsse auf die Person des Nutzers ziehen, die ggf. eines besonderen Schutzes bedürften (z.B. die Tatsache eines Krankenhausaufenthaltes oder des/der Mitarbeiters/in einer Behörde oder eines bestimmten Unternehmens). Auch wenn diese Frage insbesondere erst bei der Nutzung relevant wird, ist bereits schon eine verpflichtende Erhebung und Speicherung vor diesem Hintergrund zu sehen. Der Eingriff in das Recht auf informationelle Selbstbestimmung steht hier in keinem Verhältnis zu einem völlig ungewissen und unbestimmten möglichen Nutzen der Speicherung.

Schließlich widerspricht die Erhebungs- und Speicherungspflicht der gegenüber den Telekommunikationsanbietern bestehenden Verpflichtung nach § 3a BDSG, sich an dem Ziel von Datenvermeidung und Datensparsamkeit auszurichten. Gerade die Prepaid-Angebote waren ein gutes praktisches Beispiel für den Einsatz datenschutzfreundlicher Technologien, da sie anonymes Kommunizieren auf unkomplizierte Weise ermöglichten. Die potentielle staatliche Überwachung aller Prepaid-Kunden konterkariert dieses Ziel völlig.

Die in § 111 Abs. 1 Satz 4 TKG vorgesehene Löschungsfrist von in der Praxis bis zu zwei Jahren nach Vertragsende verstärkt die Zweifel an der Verhältnismäßigkeit des § 111 TKG 2004 noch. Die Gesetzesbegründung führt hierzu lediglich aus, dass die Strafverfolgungsbehörden „nicht selten“ vor der Situation stünden, dass Bestandsdaten nach Vertragsende nicht mehr vorhanden seien. Weder wird dies quantitativ belegt, noch kann der qualitative Gehalt dieser Aussage wegen ihrer Allgemeinheit überprüft werden. Auch wird nicht be-



legt, dass die Länge der Frist den Erfordernissen der berechtigten Stellen angemessen Rechnung trägt oder ob eine wesentlich kürzere Frist hierfür auch ausreichen würde.

#### **IV. Vereinbarkeit des § 112 TKG 2004 (Daten für Auskunftersuchen der Sicherheitsbehörden in automatisierten Verfahren) mit dem Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG)**

§ 112 TKG 2004 ist ebenfalls mit dem durch Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG geschützten Grundrecht auf informationelle Selbstbestimmung nicht vereinbar.

Auch bei der in § 112 Abs. 1 TKG 2004 vorgesehenen Speicherung der Kundendaten und deren Bereithalten zum Abruf durch die Bundesnetzagentur sowie hinsichtlich der Auskunftsbe-fugnisse nach § 112 Abs. 2 handelt es sich um den Umgang mit personenbezogenen Daten, deren verfassungsrechtlicher Schutz durch Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG gegeben ist. Sowohl die Verpflichtung zur Speicherung und das Bereithalten zum Abruf als auch der be-sondere Fall des Abrufes mit „Joker-Abfragen“ und Abfragen mit „Ähnlichenfunktion“ (§ 112 Abs. 1 Satz 4 Nr. 2 TKG) begegnen verfassungsrechtlichen Bedenken.

##### **IV.1. Anlegen von Kundendateien und Bereithalten zum Abruf nach § 112 Abs. 1 TKG**

Soweit in § 112 Abs. 1 TKG 2004 angeordnet wird, die in § 111 Abs. 1 TKG 2004 genannten Daten in Kundendateien zu speichern und zum Abruf bereitzuhalten, kann hinsichtlich der fehlenden Geeignetheit, Erforderlichkeit und Verhältnismäßigkeit zunächst auf die Ausführungen zu § 111 Abs. 1 TKG 2004 verwiesen werden. Dies gilt umso mehr für die Daten, deren Speicherung und weitere Verarbeitung für die Vertragsgestaltung i.S.v. § 95 Abs. 1 TKG 2004 nicht erforderlich sind.

##### **IV.2. Auskünfte aus den Kundendateien nach § 112 Abs. 2 TKG 2004**

Die derzeit bestehenden Befugnisse der Auskunftserteilung nach § 112 Abs. 2 TKG 2004 sind unverhältnismäßig. Gemessen an der Zweckbestimmung der Auskünfte sind sie zu weitgehend und zu unbestimmt.

Zwar ist das Recht auf informationelle Selbstbestimmung nicht schrankenlos gewährleistet. Der Einzelne hat nicht nur ein Recht im Sinne einer absoluten, uneinschränkbaren Herrschaft über „seine“ Daten. Grundsätzlich muss der Betroffene Einschränkungen seines Rechts auf informationelle Selbstbestimmung im überwiegenden Allgemeininteresse hinnehmen. Für eine Beschränkung des Grundrechts bedarf es einer verfassungsmäßigen gesetzlichen Grundlage, aus der sich die Voraussetzungen und der Umfang der Beschränkung klar und für den Bürger erkennbar ergeben und die damit dem rechtstaatlichen Gebot der Normenklarheit ent-



spricht (ständige Rechtsprechung des BVerfG, vgl. nur BVerfG, Urteil vom 15. Dezember 1983, - 1 BvR 209 u.a./83 -, BVerfGE 65, S. 1 [44]; Beschluss vom 7. März 1995 - 1 BvR 1564/92 - BVerfGE 92, S. 191 [197]). Das Gebot der Bestimmtheit des Gesetzes zwingt den Gesetzgeber, seine Regelungen so bestimmt zu fassen, „wie dies nach der Eigenart des zu ordnenden Lebenssachverhalts mit Rücksicht auf den Normzweck möglich ist“ (BVerwG, Urteil vom 22. Oktober 2003 - 6 C 23.02 -, BVerwGE 119, S. 123 [128]). Außerdem richten sich die Bestimmtheitsanforderungen nach der Intensität der Einwirkungen auf den Regelungsadressaten. Die von der gesetzlichen Regelung Betroffenen müssen in zumutbarer Weise den Regelungsinhalt der Norm erkennen können. Dabei reicht es aus, wenn sich im Wege der Auslegung mit Hilfe der anerkannten Auslegungsregeln feststellen lässt, was der Gesetzgeber vom Normunterworfenen an Tun oder Unterlassen verlangt. Bei Anwendung der anerkannten Auslegungsregeln – die notwendigerweise beeinflusst wird von dem Grundrecht, in das eingegriffen wird – stellt sich die Frage, ob auch mit Blick auf die Intensität der in Betracht kommenden Grundrechtsbeeinträchtigung eine dem Gebot der Normenklarheit genügende Legitimation für die Rechtsbeeinträchtigung angenommen werden kann. Dabei ist zu berücksichtigen, dass durch die Auskünfte an Gerichte, Strafverfolgungsbehörden und Nachrichtendienste nach § 112 Abs. 2 TKG 2004 in erheblichem Maße in das Recht auf informationelle Selbstbestimmung eingegriffen wird. Diesen verfassungsrechtlichen Anforderungen genügt die katalogartige Aufzählung der Auskunftsberechtigten nach § 112 Abs. 2 TKG 2004 nicht, da keine Begrenzung auf konkrete Zwecke erfolgt, sodass im automatischen Verfahren übermittelte Daten für alle gesetzlichen Aufgaben des Empfängers genutzt werden dürfen. Dies ist angesichts der nicht unerheblichen Eingriffe in das Recht auf informationelle Selbstbestimmung zu unbestimmt und zu weitgehend.

Zudem sieht die Regelung keine zusätzliche Eingriffsschwelle vor, so dass weitere Zweifel an der Beachtung des Grundsatzes der Verhältnismäßigkeit bestehen. Es sollte daher gesetzlich festgelegt werden, dass die Daten im automatisierten Verfahren nur dann abgerufen werden dürfen, wenn sie auf andere Weise nicht ermittelt werden können.

Sowohl das Grundrecht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG als auch Art. 11 und 12 der Datenschutzrichtlinie 95/46/EG gewähren den von den Abfragen betroffenen Grundrechtsträgern einen Anspruch auf Information über die Verarbeitung ihrer personenbezogenen Daten. Art. 10 GG verlangt, dass zumindest eine Benachrichtigung dann stattfinden muss, wenn die Datenerhebung heimlich erfolgt und ein Auskunftsanspruch nicht eingeräumt wird (vgl. BVerfG, Urteil vom 14. Juli 1999 - 1 BvR 2226/94, 2420, 2437/95 -, BVerfGE 100, 313 [361]). Entsprechendes muss bei heimlichen Eingriffen in das Recht auf informationelle Selbstbestimmung gelten.

Diesen verfassungsrechtlichen Anforderungen genügt § 112 Abs. 2 TKG 2004 nicht, da schon der Verpflichtete nach § 112 Abs. 1 Satz 6 TKG 2004 selbst nichts von den Abrufen erfährt. Dass der Betroffene die Möglichkeit hat, von den berechtigten Stellen nach § 112 Abs. 2 TKG



eine Auskunft zu erhalten, genügt nicht, denn der Betroffene wird nur selten von dem Eingriff in das Grundrecht erfahren. Dies widerspricht dem Recht des Betroffenen zu wissen, „wer was wann und bei welcher Gelegenheit über sie weiß“ (vgl. hierzu (BVerfG, Urteil vom 15. Dezember 1983 - 1 BvR 209 u.a./83 -, BVerfGE 65, 1 [43]) und damit einer Kernaussage des Volkszählungsurteiles.

Das Gesetz sollte daher zur Gewährleistung eines effektiven Grundrechtsschutzes sicherstellen, dass die Betroffenen zumindest zu einem späteren Zeitpunkt benachrichtigt werden.

#### IV.3. „Joker-Abfragen“/Abfragen mit „Ähnlichenfunktion“

Die Möglichkeit der „Joker-Abfrage“ nach § 112 Abs. 1 Satz 4 Nr. 2 TKG 2004 begegnet Bedenken wegen eines Verstoßes gegen die verfassungsrechtlichen Grundsätze der Erforderlichkeit und der Verhältnismäßigkeit. Die „Joker-Abfrage“, bei der nach Art eines „Schrotflinteneinsatzes“ Daten abgerufen werden, führt in jedem Falle zu einer Übermittlung personenbezogener Daten unbeteiligter Dritter, solange sie in die gesuchte Kategorie fallen. Diese Form der Abfrage muss im Gesetz zumindest auf das verhältnismäßige Maß beschränkt werden. Die gleichen Bedenken richten sich gegen die Möglichkeit, beim Abruf auch phonetische Suchbegriffe verwenden zu dürfen. Auch hier sind die Möglichkeiten, dass Daten Unbeteiligter in einem unverhältnismäßig hohen Umfang mit übermittelt werden, bereits durch das Gesetz zu beschränken.

§ 112 Abs. 1 Satz 4 Nr. 2 TKG sieht ferner vor, dass Abfragen auch unter Verwendung unvollständiger Abfragedaten oder mittels einer Ähnlichenfunktion erfolgen können. Nähere Präzisierungen nimmt das Gesetz nicht vor. Vielmehr soll dies einer Rechtsverordnung nach § 112 Abs. 3 Satz 1 Nr. 3 TKG überlassen werden. Eine solche Rechtsverordnung wurde jedoch bis heute nicht erlassen.

Die Entscheidung des Gesetzgebers, die Mindestanforderungen an den Umfang der einzugebenden Daten sowie den zulässigen Umfang der zu übermittelnden Treffer (§ 112 Abs. 3 Satz 1 Nr. 3 Buchstabe a und b TKG 2004) nicht unmittelbar im Gesetz zu regeln, sondern der Bestimmung in einer Rechtsverordnung zu überlassen, verstößt gegen das sich aus dem Grundgesetz - insbesondere aus Art. 20 GG - ergebende Demokratieprinzip. Dies gebietet es, dass die Entscheidung aller grundsätzlichen Fragen, die den Bürger unmittelbar betreffen, durch den Gesetzgeber selbst zu treffen ist. Dies gilt vor allem dann, wenn nicht unerhebliche Eingriffe in die Freiheitsrechte des Einzelnen in Rede stehen. Es genügt deshalb nicht den Anforderungen an Art. 20 Abs. 3 GG, dass die wesentlichen Fragen eines Grundrechtseingriffs einer Rechtsverordnung der Exekutive überlassen werden, ohne dass der Gesetzgeber sich selbst damit auseinandergesetzt hat.



Dieser verfassungsrechtlichen Vorgabe widersprechend, eröffnet § 112 Abs. 1 Satz 4 Nr. 2 TKG 2004 die Möglichkeit, mittels „Jokerzeichen“ bzw. einer Ähnlichenfunktion auf die Bestandsdaten zuzugreifen. Der Gesetzgeber hat nicht festgelegt, wie weitreichend diese Eingriffe sein dürfen. Die Frage, ob z.B. bei numerischen Begriffen (wie der Telefonnummer) ein, zwei oder drei Zeichen eines Suchbegriffs durch „Jokerzeichen“ ersetzt werden, entscheidet darüber, ob auf 10, 100 oder 1000 Datensätze zugegriffen wird. Bei alphabetischen Begriffen wie dem Namen ist der Faktor noch höher. Dies zeigt, dass der Rechtsverordnung die Entscheidung vorbehalten bleiben soll, in welchem Umfang in die Grundrechte von Bürgern eingegriffen wird, deren Daten weit überwiegend nicht erforderlich sein werden. Damit wird dem Verordnungsgeber nicht nur die Entscheidung über die Ausgestaltung des Eingriffs, sondern über die Rechtmäßigkeit des Grundrechtseingriffs selbst überlassen. Diese Entscheidung ist so wesentlich für die Grundrechte der Betroffenen, dass der Gesetzgeber sie selbst treffen sollte.

#### **V. Vereinbarkeit des § 113 TKG 2004 (Manuelles Auskunftsverfahren) mit dem Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG)**

§ 113 TKG 2004 ist ebenfalls mit dem durch Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG geschützten Grundrecht auf informationelle Selbstbestimmung nicht vereinbar.

§ 113 TKG regelt das manuelle Auskunftsverfahren für Bestandsdaten. Wenn aufgrund von § 113 Abs. 1 TKG 2004 Bestandsdaten an die in § 113 Abs. 1 TKG 2004 genannten Stellen übermittelt werden, wird in den Schutzbereich des Rechts auf informationelle Selbstbestimmung eingegriffen.

##### **V.1. Auskunftserteilung nach § 113 Abs. 1 Satz 1 TKG 2004**

Auch die in § 113 Abs. 1 Satz 1 TKG 2004 geregelte Befugnis zur Auskunftserteilung widerspricht dem verfassungsrechtlichen Grundsatz der Verhältnismäßigkeit, da hier ein weiterer Adressatenkreis als nach § 112 TKG zur Übermittlung eines gegenüber § 112 TKG erweiterten Datenkranzes verpflichtet wird.

Durch § 113 TKG 2004 werden alle geschäftsmäßigen Erbringer von Telekommunikationsdiensten nach § 3 Nr. 10 TKG 2004 verpflichtet. Die Regelung ist also weder auf Anbieter von Telekommunikationsdiensten für die Öffentlichkeit (§ 112 TKG 2004) noch auf solche Anbieter beschränkt, die Rufnummern vergeben (§ 111 TKG 2004). Dies bedeutet, dass auch die Betreiber von Nebenstellenanlagen, Corporate Networks, Hotels, Krankenhäusern usw. Auskünfte nach § 113 TKG 2004 zu erteilen haben. Hinzu kommt die Verpflichtung aller Anbieter von nicht rufnummernbezogenen Diensten, vor allem E-Mail-Anbieter und Internet-Zugangsanbieter.



Dabei muss bei der Prüfung der Verhältnismäßigkeit innerhalb der erforderlichen Rechtsgüterabwägung besonders berücksichtigt werden, dass es sich bei den in § 113 Abs. 1 Satz 1 TKG 2004 in Bezug genommenen Daten um Bestandsdaten handelt, die in Umfang und Sensitivität deutlich über das hinausgehen, was im Rahmen des automatisierten Abrufverfahrens nach § 112 TKG 2004 bereitgestellt bzw. nach § 111 TKG 2004 erhoben und gespeichert wird.

Der Umfang der Daten, über die nach § 113 Abs. 1 Satz 1 TKG Auskunft erteilt werden muss, ist wesentlich größer als bei § 112 TKG. § 113 Abs. 1 Satz 1 TKG beschränkt sich nicht nur auf die nach § 111 TKG erhobenen Daten, sondern erfasst zusätzlich alle nach § 95 TKG erhobenen Bestandsdaten. Hierzu gehören Informationen wie besondere Tarifgestaltungen, E-Mail-Adressen, statische IP-Adressen und als besonders sensitive Daten, wie Nutzerkennungen, die PIN (Personal Identification Number) und die PUK (Personal Unblocking Key), die Bankverbindungsdaten etc.

Zwar gilt auch hier, dass die Bestandsdaten für sich genommen nicht unmittelbar Auskunft über konkrete Kommunikationsvorgänge geben. Jedoch haben die Daten je nach Fallgestaltung eine erhöhte Aussagekraft über die Kommunikationsgewohnheiten und das Kommunikationsverhalten der Betroffenen. Dadurch stehen sie dem Schutzbereich des Fernmeldegeheimnisses nach Art. 10 GG deutlich näher als die nach § 111 TKG 2004 zu erhebenden Daten. Beispielsweise kann aus der Inanspruchnahme eines so genannten Family&Friends-Tarifs geschlossen werden, mit welchen Personen ein Nutzer überwiegend telefoniert. Beim Internet-Zugang dient die statische IP-Adresse ganz unmittelbar als Schlüssel zur Identifizierung und Individualisierung jedes einzelnen Nutzungsvorgangs, die dynamische IP-Adresse mittelbar über den entsprechenden Server des Zugangs-Providers. Die statische IP-Adresse ist in diesem Fall sowohl Verkehrs- als auch Bestandsdatum. Denkbar wäre auch, dass sich ein Nutzer eines Anbieters bedient, der besonders günstige Tarife für bestimmte Zielländer anbietet. Dann lässt sich bereits den Bestandsdaten entnehmen, in welche Länder der Betroffene kommuniziert. Diese Beispiele lassen sich beliebig erweitern.

In seinem Urteil vom 2. März 2006 (- 2 BvR 2099/04 -, NJW 2006, S. 976 [980]) hat das BVerfG festgestellt, dass Daten, die zunächst vom Fernmeldegeheimnis geschützt waren und zum Zeitpunkt eines staatlichen Eingriffs bereits in der ausschließlichen Verfügungsgewalt des Betroffenen sind, auch im Rahmen des Rechts auf informationelle Selbstbestimmung als Ergänzung zum Fernmeldegeheimnis einem erhöhten Schutz unterliegen, der im Rahmen der Verhältnismäßigkeitsprüfung zu berücksichtigen ist. Dies gilt erst recht für den vorliegenden Fall, in dem es sich umgekehrt um Daten handelt, die (noch) nicht vom Fernmeldegeheimnis geschützt sind. Sie sind jedoch zwingend notwendig, um Zugang zu den Informationen über die von Art. 10 GG geschützten näheren Umstände der Telekommunikation zu erhalten und außerdem geeignet, Aussagen über das konkrete Kommunikationsverhalten zu treffen. Sobald



diese Daten die konkrete Telekommunikationsverbindung individualisieren, werden diese Bestandsdaten zusätzlich zu Verbindungsdaten und unterliegen dann dem Schutzbereich des Art. 10 GG. Außerdem muss berücksichtigt werden, dass die Abrufe der Daten auch nach § 113 Abs. 1 Satz 4 TKG 2004 heimlich und ohne Wissen des Betroffenen stattfinden.

Diesem erhöhten Schutzbedarf der Bestandsdaten wird § 113 Abs. 1 Satz 1 TKG 2004 nicht gerecht. Die hohe Aussagekraft und Sensitivität der Daten verlangt, dass Eingriffe nur dann verhältnismäßig sind, wenn sie einem legitimen Zweck dienen, der sich präzise und konkret aus dem Gesetz ergeben muss. Da die Daten in ihrer Aussagekraft und damit Schutzbedürftigkeit inzwischen den Verkehrsdaten i.S.v. § 3 Nr. 30 TKG 2004 kaum nachstehen, sind an die Eingriffsschwelle ähnlich hohe Anforderungen zu stellen. Der heimliche Abruf von Bestandsdaten ist daher nur verhältnismäßig, wenn wichtige öffentliche Interessen dies gebieten.

Dies spricht dafür, die Eingriffsschwelle soweit heraufzusetzen, dass die Daten in erster Linie zur Vorbereitung und Durchführung von Maßnahmen nach §§ 100a ff. StPO, dem G-10-Gesetz, den §§ 23a ff. ZFdG und den Vorschriften zur präventiven Überwachung der Telekommunikation in den Sicherheits- und Ordnungsgesetzen der Länder abgerufen werden dürfen. Damit würde die Eingriffsschwelle erheblich angehoben und der Abruf auf telekommunikationsrelevante Sachverhalte beschränkt.

Ferner sollte eine Subsidiaritätsklausel eingeführt werden, die den Datenabruf erst dann erlaubt, wenn die Bestandsdaten auf andere Weise nicht erhoben werden können.

V.2. Abruf von Daten nach § 113 Abs. 1 Satz 2 TKG 2004, mit deren Hilfe der Zugriff auf Endgeräte oder in diesen oder im Netz eingesetzten Speichereinrichtungen geschützt wird

Auch gegen die in § 113 Abs. 1 Satz 2 TKG 2004 geregelte Befugnis, Daten abzurufen, mittels derer der Zugriff auf Endgeräte oder Speichereinrichtungen geschützt wird, bestehen mit Blick auf den Grundsatz der Verhältnismäßigkeit erhebliche Bedenken.

Nicht nachvollziehbar ist, weshalb der Zugriff auf diese Daten unter derart leichten Bedingungen möglich sein soll, wenn für den Zugriff auf die „dahinter“ liegenden geschützten (Gesprächs-) Inhaltsdaten die Voraussetzungen der §§ 100a ff. StPO, des G 10, der §§ 23a ff. ZFdG oder der Polizeigesetze der Länder gegeben sein müssen. Eine Mitteilung dieser Daten ohne die Voraussetzungen, unter denen eine Überwachung der Inhalte oder der näheren Umstände der Telekommunikation zulässig wäre, birgt die Gefahr von missbräuchlichen Eingriffen in das Fernmeldegeheimnis ohne Vorliegen der gesetzlichen Voraussetzungen. Im Übrigen ist zu bedenken, dass die Anbieter diese Daten in vielen Fällen aus Gründen der Datensicherheit für sie selbst verschlüsselt speichern und daher auch nicht mitteilen könnten.



Die vom Gesetzgeber in der Begründung erwünschte Klarstellung ( vgl. BT-Drs. 15/2316, S. 97) kann auch dadurch erreicht werden, dass eindeutig geregelt wird, dass auch diese Daten vom Fernmeldegeheimnis i.S.v. § 88 TKG 2004 geschützt sind oder zumindest so behandelt werden. In diesem Falle wäre eine Mitteilung dieser Daten an Sicherheitsbehörden klar und eindeutig nur nach den für die Überwachung einschlägigen Bestimmungen (§§ 100a ff. StPO, G10 etc.) möglich.

Auch diese Daten unterliegen einem erhöhten Schutz, da sie unmittelbar dazu dienen, vor dem Zugang zu solchen Daten zu schützen, die dem Fernmeldegeheimnis unterliegen. Auch hier liegt die Ergänzungsfunktion des Rechts auf informationelle Selbstbestimmung im Sinne einer Vorwirkung des Fernmeldegeheimnisses auf der Hand.

### V.3. Fehlende Information des Betroffenen nach § 113 Abs. 1 Satz 4 TKG 2004

Die Vorschrift verpflichtet die Telekommunikationsdienstleister, die erfolgten Abrufe auch gegenüber dem Betroffenen geheim zu halten. Da dem betroffenen Bürger effektiver Grundrechtsschutz nicht gewährt wird, verstößt dies nicht nur gegen Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, sondern auch gegen Art. 19 Abs. 4 GG.

Auch hier sollte nach den Vorgaben des BVerfG (BVerfG, Urteil vom 14. Juli 1999 - 1 BvR 2226/94, 2420, 2437/95 -, BVerfGE 100, 313 [361]) eine nachträgliche Benachrichtigung vorgesehen werden.

Auf die anliegenden Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu den Änderungen des Telekommunikationsgesetzes, die während des Gesetzgebungsverfahrens beschlossen wurde, weise ich besonders hin.

Schaar



**EntschlieÙung**  
**zwischen der 63. und 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder**  
**vom 24. Mai 2002**

**Geplanter Identifikationszwang in der Telekommunikation**

Das Bundesministerium für Wirtschaft und Technologie hat einen Entwurf zur Änderung des Telekommunikationsgesetzes veröffentlicht. Der Entwurf hat das Ziel, jeden Anbieter, der geschäftsmäßig Telekommunikationsdienste erbringt, dazu zu verpflichten, Namen, Anschriften, Geburtsdaten und Rufnummern seiner Kundinnen und Kunden zu erheben. Die Kundinnen und Kunden werden verpflichtet, dafür ihren Personalausweis vorzulegen, dessen Nummer ebenfalls gespeichert werden soll. Die beabsichtigten Änderungen sollen in erster Linie dazu führen, auch Nutzerinnen und Nutzer von Prepaid-Karten (also die Erwerberinnen und Erwerber von SIM-Karten ohne Vertrag) im Mobilfunk erfassen zu können. Die erhobenen Daten sollen allein dem Zweck dienen, den Sicherheitsbehörden zum jederzeitigen Online-Abruf über die Regulierungsbehörde für Telekommunikation und Post bereitzustehen. Im gleichen Zuge sollen die Zugriffsmöglichkeiten der Sicherheitsbehörden auf diese Daten dadurch erheblich erweitert werden, indem auf die Kundendateien nach abstrakten Merkmalen zugegriffen werden kann. Die Datenschutzbeauftragten des Bundes und der Länder lehnen dieses Vorhaben ab. Unter der unscheinbaren Überschrift „Schließen von Regelungslücken“ stehen grundlegende Prinzipien des Datenschutzes zur Disposition. Kritikwürdig an dem geplanten Gesetz sind insbesondere die folgenden Punkte:

- Der geplante Grundrechtseingriff ist nicht erforderlich, um die Ermittlungstätigkeit der Sicherheitsbehörden zu erleichtern. Seine Eignung ist zweifelhaft: Auch die Gesetzesänderung wird nicht verhindern, dass Straftäterinnen und Straftäter bewusst und gezielt in kurzen Zeitabständen neue Prepaid-Karten erwerben, Strohleute zum Erwerb einsetzen, die Karten häufig – teilweise nach jedem Telefonat – wechseln oder die Karten untereinander tauschen. In der Begründung wird nicht plausibel dargelegt, dass mit dem geltenden Recht die Ermittlungstätigkeit tatsächlich behindert und durch die geplante Änderung erleichtert wird. Derzeit laufende Forschungsvorhaben beziehen diese Frage nicht mit ein.
- Der Entwurf widerspricht auch dem in den Datenschutzrichtlinien der Europäischen Union verankerten Grundsatz, dass Unternehmen nur solche personenbezogenen Daten verarbeiten dürfen, die sie selbst zur Erbringung einer bestimmten Dienstleistung benötigen.
- Die Anbieter würden eine Reihe von Daten auf Vorrat speichern müssen, die sie selbst für den Vertrag mit ihren Kunden nicht benötigen. Die ganz überwiegende Zahl der Nutzerinnen und Nutzer von Prepaid-Karten, darunter eine große Zahl Minderjähriger, würde registriert, obwohl sie sich völlig rechtmäßig verhalten und ihre Daten demzufolge für die Ermittlungstätigkeit der Strafverfolgungsbehörden nicht benötigt werden. Das Anhäufen von sinn- und nutzlosen Datenhalden wäre die Folge.
- Die gesetzliche Verpflichtung, sich an dem Ziel von Datenvermeidung und Datensparsamkeit auszurichten, würde konterkariert. Gerade die Prepaid-Karten sind ein gutes praktisches Beispiel für den Einsatz datenschutzfreundlicher Technologien, da sie anonymes Kommunizieren auf unkomplizierte Weise ermöglichen. Die Nutzung dieser Angebote darf deshalb nicht von der Speicherung von Bestandsdaten abhängig gemacht werden.



- Mit der Verpflichtung, den Personalausweis vorzulegen, würden die Anbieter zusätzliche Informationen über die Nutzerinnen und Nutzer erhalten, die sie nicht benötigen, z.B. die Nationalität, Größe oder Augenfarbe. Die vorgesehene Pflicht, auch die Personalausweisnummern zu registrieren, darf auch künftig keinesfalls dazu führen, dass die Ausweisnummern den Sicherheitsbehörden direkt zum Abruf bereit gestellt werden und sie damit diese Daten auch für die Verknüpfung mit anderen Datenbeständen verwenden können.
- Auch Krankenhäuser, Hotels, Schulen und Hochschulen sowie Unternehmen und Behörden, die ihren Mitarbeiterinnen und Mitarbeitern das private Telefonieren gestatten, sollen verpflichtet werden, die Personalausweisnummern der Nutzerinnen und Nutzer zu registrieren.
- Die Befugnis, Kundendateien mit unvollständigen oder ähnlichen Suchbegriffen abzufragen, würde den Sicherheitsbehörden eine Vielzahl personenbezogener Daten unbeteiligter Dritter zugänglich machen, ohne dass diese Daten für ihre Aufgaben erforderlich sind. Die notwendige strikte Beschränkung dieser weitreichenden Abfragebefugnis durch Rechtsverordnung setzt voraus, dass ein entsprechender Verordnungsentwurf bei der Beratung des Gesetzes vorliegt.

Der Formulierungsvorschlag des Bundeswirtschaftsministeriums lässt eine Auseinandersetzung mit dem Recht auf informationelle Selbstbestimmung der Kundinnen und Kunden der Telekommunikationsunternehmen weitgehend vermissen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Bundesregierung und den Gesetzgeber auf, auf die geplante Änderung des Telekommunikationsgesetzes zu verzichten und vor weiteren Änderungen die bestehenden Befugnisse der Sicherheitsbehörden durch unabhängige Stellen evaluieren zu lassen.



**EntschlieÙung  
zwischen der 65. und 66. Konferenz der Datenschutzbeauftragten des Bundes und der Länder  
vom 28. April 2003**

**Verbesserung statt Absenkung des Datenschutzniveaus in der Telekommunikation**

Im Zuge der bevorstehenden Novellierung des Telekommunikationsgesetzes plant die Bundesregierung neben der Abschaffung der Unternehmensstatistik (vgl. dazu EntschlieÙung der 65. Konferenz vom 28. März 2003 zur Transparenz bei der Telefonüberwachung) eine Reihe weiterer Änderungen, die zu einer Absenkung des gegenwärtigen Datenschutzniveaus führen würden.

Zum einen ist vorgesehen, die Zweckentfremdung von Bestandsdaten der Telekommunikation (z.B. Art des Anschlusses, Kontoverbindung, Befreiung vom Telefonentgelt aus sozialen oder gesundheitlichen Gründen) für Werbezwecke weitergehend als bisher schon dann zuzulassen, wenn der Betroffene dem nicht widerspricht. Dies muss – wie bisher – die informierte Einwilligung des Betroffenen voraussetzen.

Außerdem plant die Bundesregierung, Daten, die den Zugriff auf Inhalte oder Informationen über die näheren Umstände der Telekommunikation schützen (wie z.B. PINs und PUKs – Personal Unblocking Keys –), in Zukunft der Beschlagnahme für die Verfolgung beliebiger Straftaten zugänglich zu machen. Bisher kann der Zugriff auf solche Daten nur angeordnet werden, wenn es um die Aufklärung bestimmter schwerer Straftaten geht. Diese Absenkung oder gar Aufhebung der verfassungsmäßig gebotenen Schutzwelle für Daten, die dem Telekommunikationsgeheimnis unterliegen, wäre nicht gerechtfertigt; dies ergibt sich auch aus dem Urteil des Bundesverfassungsgerichts vom 12. März 2003.

Aus der Sicht des Datenschutzes ist auch die Versagung eines anonymen Zugangs zum Mobilfunk problematisch. Die beabsichtigte Gesetzesänderung führt dazu, dass z.B. der Erwerb eines „vertragslosen“ Handys, das mit einer entsprechenden – im Prepaid-Verfahren mit Guthaben aufladbaren – SIM-Karte ausgestattet ist, einem Identifikationszwang unterliegt. Dies hat zur Folge, dass die Anbieter von Prepaid-Verfahren eine Reihe von Daten wegen eines möglichen Zugriffs der Sicherheitsbehörden auf Vorrat speichern müssen, die sie für ihre Betriebszwecke nicht benötigen. Die verdachtslose routinemäßige Speicherung zu Zwecken der Verfolgung eventueller, noch gar nicht absehbarer künftiger Straftaten würde auch zur Entstehung von selbst für die Sicherheitsbehörden sinn- und nutzlosen Datenhalden führen. So sind erfahrungsgemäß z.B. die Erwerber häufig nicht mit den tatsächlichen Nutzern der Prepaid-Angebote identisch.

Insgesamt fordern die Datenschutzbeauftragten des Bundes und der Länder den Gesetzgeber auf, das gegenwärtige Datenschutzniveau bei der Telekommunikation zu verbessern, statt es weiter abzusinken. Hierzu sollte jetzt ein eigenes Telekommunikations-Datenschutzgesetz verabschiedet werden, das den Anforderungen einer freiheitlichen Informationsgesellschaft genügt und später im Zuge der noch ausstehenden zweiten Stufe der Modernisierung des Bundesdatenschutzgesetzes mit diesem zusammengeführt werden könnte.



**EntschlieÙung**  
**Konferenz der Datenschutzbeauftragten des Bundes und der Länder**  
vom 21. November 2003

**Gravierende Verschlechterungen des Datenschutzes im Entwurf des neuen  
Telekommunikationsgesetzes**

Die Bundesregierung hat am 15. Oktober 2003 den Entwurf für ein neues Telekommunikationsgesetz beschlossen. Dieser Entwurf sieht jetzt zwar – entsprechend der Forderung der Datenschutzbeauftragten – die vorläufige Beibehaltung der Unternehmensstatistik zu Überwachungsmaßnahmen vor; im übrigen enthält er aber gravierende Verschlechterungen des Datenschutzniveaus.

Insbesondere berechtigt der Gesetzentwurf die Diensteanbieter, grundsätzlich alle entstehenden Verkehrsdaten (also auch alle Zielrufnummern) unverkürzt bis zu sechs Monaten nach Versendung der Rechnung zu speichern. Damit wird ohne Not und ohne überzeugende Begründung eine Regelung aufgegeben, die bisher die Speicherung von verkürzten Zielrufnummern vorsieht, wenn die Kundinnen und Kunden sich nicht für die vollständige Speicherung oder vollständige Löschung entscheiden. Die bisherige Regelung berücksichtigt in ausgewogener Weise sowohl die Datenschutz- als auch die Verbraucherschutzinteressen der beteiligten Personen und hat sich in der Praxis bewährt. Vollends inakzeptabel ist die inzwischen vom Rechtsausschuss des Bundesrates vorgeschlagene Pflicht zur Vorratsdatenspeicherung für sechs Monate. Gegen eine solche Regelung bestehen erhebliche verfassungsrechtliche Bedenken.

Schon die von der Bundesregierung vorgeschlagene Regelung würde dazu führen, dass Millionen von Verkehrsdatensätzen selbst dann noch unverkürzt gespeichert bleiben und dem Zugriff anderer Stellen ausgesetzt sind, wenn die Diensteanbieter sie für ihre Abrechnungszwecke nicht mehr benötigen. Das im Entwurf weiterhin vorgesehene Recht der Kundinnen und Kunden, die Speicherung gekürzter Zielrufnummern oder ihre vollständige Löschung nach Rechnungsversand zu verlangen, wird daran wenig ändern, weil nur eine Minderheit es wahrnehmen wird. Die Beibehaltung des bisherigen angemessenen Datenschutzstandards sollte nicht von der Initiative der Betroffenen abhängig gemacht werden, sondern allen zugute kommen, die nicht ausdrücklich einer weitergehenden Speicherung zustimmen. Zudem sind die Rechte der angerufenen Teilnehmerinnen und Teilnehmer zu berücksichtigen, in die durch eine Speicherung der unverkürzten Verkehrsdaten zusätzlich eingegriffen wird.

Die Datenschutzbeauftragten haben zudem stets die Zwangsidentifizierung beim Erwerb von vertragslosen (prepaid) Handys als gesetzwidrig kritisiert und sehen sich jetzt in dieser Auffassung durch das Urteil des Bundesverwaltungsgerichts vom 22. Oktober 2003 (Az.: 6 C 23.02) bestätigt. Zugleich wenden sie sich gegen die mit der TKG-Novelle geplante Einführung einer derartigen Identifikationspflicht, die zu einer verdachtslosen Datenspeicherung auf Vorrat führen würde. Wer ein solches Handy kauft, gibt es häufig ab oder verschenkt es, und ist deshalb nicht identisch mit der Person, die das Handy nutzt. Deshalb bringen diese Daten keinen nennenswerten Informationsgewinn für die Sicherheitsbehörden.

Schließlich soll den Strafverfolgungsbehörden, der Polizei und den Nachrichtendiensten ohne Bindung an einen Straftatenkatalog oder einen Richtervorbehalt der Zugriff auf Passwörter, PINs, PUKs usw. eröffnet werden, mit denen die Inhalte oder nähere Umstände einer Telekommunikation geschützt werden. Dies würde die Möglichkeit eröffnen, von dieser Befugnis unkontrolliert Gebrauch zu machen. Die Befugnis dürfte zudem häufig ins Leere laufen, da die Anbieter diese Daten aus Gründen der Datensicherheit für sie selbst unlesbar verschlüsselt speichern.



**Die Datenschutzbeauftragten des Bundes und der Länder fordern den Gesetzgeber auf, den Entwurf bei den bevorstehenden Beratungen in diesen sensiblen Punkten zu korrigieren und den gebotenen Schutz des Telekommunikationsgeheimnisses sicherzustellen.**

**Berliner Beauftragter für  
Datenschutz und Informationsfreiheit**

Dr. Alexander Dix



Berlin sagt Nein  
zu Fremdenfeindlichkeit  
und Gewalt

Berliner Beauftragter für  
Datenschutz und Informationsfreiheit  
An der Urania 4 - 10, 10787 Berlin

*Leseabschrift*

Bundesverfassungsgericht  
Herrn BVR Prof. Dr. Hoffmann-Riem  
Schlossbezirk 3  
76131 Karlsruhe

GeschZ. (bitte angeben)    Bearbeiter(in)

Tel.: (030) 13 889-0  
Durchwahl 13 889 App.:

Datum

50.370.3

Herr Dr. Petri

300

29. Januar 2007

**Stellungnahme zur Verfassungsbeschwerde 1 BvR 1299/05;  
Verfassungsbeschwerde der [REDACTED]**

Sehr geehrter Herr Professor Hoffmann-Riem,

für die mit Schreiben des Bundesverfassungsgerichts vom 10. Juli 2006 eingeräumte Gelegenheit zur Äußerung im Verfassungsbeschwerdeverfahren 1 BvR 1299/05 bedanke ich mich.

Ich halte die Verfassungsbeschwerde im wesentlichen für zulässig und begründet. Da die Frage der Annahmefähigkeit der Verfassungsbeschwerde durch Beschluss der Ersten Kammer vom 21. Juni 2006 weitgehend geklärt ist, werde ich mich im Folgenden ganz überwiegend darauf beschränken, zur Vereinbarkeit der angegriffenen § 95 Abs. 3, Abs. 4, §§ 111-113 des Telekommunikationsgesetzes (TKG) vom 22. Juni 2004 (BGBl. I S. 1190) mit dem Grundgesetz Stellung zu nehmen.

I. Bei isolierter Betrachtung des § 95 TKG kommt es vor allem in Betracht, dass diese Vorschrift in das Recht der Beschwerdeführer auf informationelle Selbstbestimmung eingreift. Die Frage einer kombinierten Anwendung der §§ 95, 113 TKG wird später erörtert.

1) Entgegen der Auffassung der Beschwerdeführer stößt § 95 Abs. 3 TKG nicht auf durchgreifende verfassungsrechtliche Bedenken.

Diese Vorschrift gestattet es den Diensteanbietern, die Bestandsdaten bis zum Ablauf des auf die Beendigung folgenden Kalenderjahres zu speichern. Im Extremfall kann ein Diensteanbieter also Bestandsdaten bis zu einer Dauer von zwei Kalenderjahren speichern. Die Regelung des Abs. 3 weicht damit im Wortlaut von der datenschutzrechtlich üblichen Vorgabe des § 35 Abs. 2 Nr. 3 BDSG ab, wonach eine Datenspeicherung für eigene Geschäftszwecke durch Löschung zu beenden ist, soweit die Kenntnis der Daten „für die Erfüllung des Zweckes der Speicherung nicht mehr



Sprechzeiten: tgl. 9-15 Uhr,  
Do. 9-18 Uhr  
oder nach Vereinbarung  
Besuchereingang:  
An der Urania 4 - 10  
auch für Behinderte  
Der Umwelt zuliebe verwenden wir  
Recyclingpapier.

U1, U2 und U3:  
Nollendorfplatz,  
Wittenbergplatz

S-Bahnhof:  
Zoologischer Garten  
Bus: M29, 100, 187

Fax: (030) 215 50 50  
E-Mail:  
mailbox@datenschutz-berlin.de  
Internet:  
http://www.datenschutz-berlin.de  
http://www.informationsfreiheit.de



erforderlich ist.“ § 95 Abs. 3 TKG dürfte gleichwohl noch im Einklang mit den verfassungsrechtlichen Vorgaben des Art. 3 Abs. 1 GG bzw. der Art. 2 Abs. 1, 1 Abs. 1 GG stehen.

a) Insbesondere liegt kein Verstoß gegen den allgemeinen Gleichheitssatz aus Art. 3 Abs. 1 GG vor. Es trifft zwar zu, dass der Gesetzgeber Anbieter von Telekommunikationsdiensten datenschutzrechtlich anders behandelt als den übrigen Teil der Privatwirtschaft, indem sie für Diensteanbieter eine von der Erforderlichkeit der weiteren Speicherung unabhängige, fixe Löschfrist vorsieht.

Zielrichtung der Gewährleistungen des Gleichheitssatzes aus Art. 3 Abs. 1 GG ist jedoch die Gleichbehandlung von Personen in vergleichbaren Situationen. Vereinfacht ausgedrückt wäre eine Ungleichbehandlung vor allem dann verfassungsrechtlich problematisch, wenn zwei vergleichbare Sachverhalte unterschiedlich behandelt würden. Die Löschfrist in § 95 Abs. 3 TKG berücksichtigt jedoch die Besonderheiten des Telekommunikationsmarktes, in dem im Vergleich zu anderen Branchen ungewöhnlich zahlreiche Vertragsabschlüsse, -beendigungen und -wechsel stattfinden. Mit anderen Worten sollen Anbieter von Telekommunikationsdiensten nicht jeden Tag Millionen von Verträgen daraufhin überprüfen müssen, ob die zugrundeliegenden Verträge noch bestehen oder bereits beendet worden sind. Es soll vielmehr ein Suchdurchlauf zum Ende des Kalenderjahres genügen. Eine solche unternehmensfreundliche Regelung halte ich zwar für verbraucherfeindlich und damit für rechtspolitisch bedenklich (ebenso Büttgen in Beck'scher TKG-Kommentar, 3. Aufl., § 95 Rdn. 24), sie überschreitet jedoch nicht die Schwelle zur verfassungsrechtlich ungerechtfertigten Ungleichbehandlung.

Es wäre überdies ein Trugschluss anzunehmen, dass die Löschpflichten des § 35 Abs. 2 Nr. 3 BDSG in der Praxis zur Folge hätte, dass ein nicht der Telekommunikationsbranche angehöriges Unternehmen personenbezogene Daten grundsätzlich sogleich nach Vertragsbeendigung löschen müsste. Vielmehr entspricht es der Erfahrung, dass die verantwortlichen Stellen personenbezogene Daten zumindest eine gewisse Dauer nach Beendigung des Vertragsverhältnisses mit dem Betroffenen dessen Daten unabhängig von gesetzlichen Aufbewahrungspflichten speichern. Eine Speicherung für die Dauer einer Verjährungsfrist wäre zwar datenschutzrechtlich-einfachgesetzlich unzulässig. Eine Datenspeicherung über das Vertragsende hinaus ist jedoch zumindest solange nicht zu beanstanden, wie eine verantwortliche Stelle vernünftiger Weise mit der Geltendmachung zivilrechtlicher Ansprüche rechnen muss. Dies kann in Einzelfällen auch an die in § 95 Abs. 4 TKG vorgesehene Frist heranreichen. Dem entsprechend käme einer Ungleichbehandlung auch nicht ein besonderes erhebliches Gewicht zu.

b) § 95 Abs. 3 TKG greift zwar in das informationelle Selbstbestimmungsrecht der Teilnehmer ein. Entsprechend den vorstehend dargelegten Gegebenheiten verfolgt diese Beeinträchtigung jedoch einen legitimen Zweck und dürfte sich noch im Rahmen der Verhältnismäßigkeit bewegen.

2) Jedoch verletzt Art. 95 Abs. 4 TKG das Grundrecht der Teilnehmer auf informationelle Selbstbestimmung aus Art. 2 Abs. 1, 1 Abs. 1 GG, zumindest soweit die Vorschrift die Anfertigung von Kopien der Ausweispapiere der Teilnehmer erlaubt.

§ 95 Abs. 4 TKG sieht vor, dass der Diensteanbieter im Zusammenhang mit dem Begründen und dem Ändern des Vertragsverhältnisses sowie dem Erbringen von Telekommunikationsdiensten die Vorlage eines amtlichen Ausweises verlangen kann, wenn dies zur Überprüfung der Angaben des Teilnehmers erforderlich ist. Er kann von dem Ausweis eine Kopie erstellen. Die Kopie ist von dem Diensteanbieter unverzüglich nach Feststellung der für den Vertragsabschluss erforderlichen Angaben des Teilnehmers zu vernichten. Der Umfang der dabei verwendeten Daten darf nach Abs. 4 S. 4 denjenigen des Abs. 1 nicht überschreiten.

a) Soweit der jeweilige Diensteanbieter nach Abs. 4 S. 1 im Zusammenhang mit der Vertragsbegründung die Vorlage eines Personalausweises verlangen kann, kann dies aus datenschutzrechtlicher Sicht noch hingenommen werden (zur nach §§ 111 Abs. 1, 95 Abs. 4 TKG erfolgenden Erhebung von Daten, die nicht zur Vertragsabwicklung erforderlich sind, vgl. unter II.).

Der Abschluss eines Telekommunikationsvertrags begründet formal ein Dauerschuldverhältnis, in dem der Diensteanbieter häufig zunächst in Vorleistung tritt. Rechtsprechung und Literatur weisen insoweit nachvollziehbar darauf hin, dass die Verschaffung einer Gewissheit über die Identität des Kunden von gesteigerter Bedeutung für den Diensteanbieter ist. Dieser wird hierdurch zugleich in die Lage versetzt, eine Bonitätsprüfung des potentiellen Kunden vorzunehmen (vgl. Büttgen in Beck'scher TKG-Kommentar, 3. Aufl., § 95 Rdn. 28). Die Vorschrift erleichtert somit den Vertragsabschluss und die Vertragsabwicklung erheblich (vgl. BGH NJW 2003, 1237 (1241), zustimmend Kleszczewski, Berliner Kommentar zum TKG, § 95 Rdn. 18).

Soweit eine nichtöffentliche Stelle ausschließlich die Vorlage eines Personalausweises zur bloßen Kenntnisnahme verlangt, ohne den Ausweis zu kopieren oder in anderer Weise zu erfassen, wäre dies im Übrigen nach den Vorschriften des BDSG einfachgesetzlich-datenschutzrechtlich zumindest nicht generell verboten. Zwar ist das BDSG auch auf die Kenntnisnahme von Personalausweisen anwendbar, weil diese offenbar einer „automatisierten Datenverarbeitung“ entstammen (vgl. § 27 Abs. 2 BDSG). Es gibt aber Geschäftsvorgänge, bei denen die Überprüfung der Identität des Betroffenen durch ein Unternehmen legitim ist. Dies gilt insbesondere für Dauerschuldverhältnisse, bei denen das Unternehmen einseitig in erhebliche Vorleistungen tritt.

b) Demgegenüber greift die in Abs. 4 Sätze 2 und 3 vorgesehene Befugnis zur Anfertigung von Personalausweiskopien unverhältnismäßig in das Grundrecht auf informationelle Selbstbestimmung der Teilnehmer aus Art. 2 Abs. 1, 1 Abs. 1 GG ein.

aa) Es liegt ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung vor. Grundsätzlich kann jeder (hoheitlicher) Umgang personenbezogener Daten ohne Einwilligung des Betroffenen einen Eingriff in dessen Grundrecht auf informationelle Selbstbestimmung darstellen. Ermöglicht der Gesetzgeber privaten Stellen den Umgang mit personenbezogenen Daten, beschränkt er somit zugleich das Recht auf informationelle Selbstbestimmung der von der Datenverarbeitung Betroffenen.

In nunmehr gefestigter Rechtsprechung hat das Bundesverfassungsgericht allerdings festgestellt, dass es an einer subjektiven Eingriffsqualität fehlt, sofern im Rahmen von automatisierten Massendatenabgleichen personenbezogene Daten ungezielt und allein technikbedingt zunächst miterfasst, aber unmittelbar nach der Erfassung technisch wieder anonym, spurenlos und ohne Erkenntnisinteresse für die Behörden ausgesondert werden (vgl. BVerfGE 100, 313 <366>; 107, 299 <328>, BVerfG, NJW 2006, S. 1939 (1941, Rdn. 74) - Rasterfahndung). Diese Rechtsprechung ist jedoch auf den vorliegenden Regelungsgehalt nicht übertragbar.

Zwar sieht Abs. 4 S. 3 vor, dass der Diensteanbieter die Kopie unverzüglich nach Feststellung der für den Vertragsabschluss erforderlichen Angaben des Teilnehmers zu vernichten hat. Abgesehen von der Frage der Vergleichbarkeit von Datenabgleichen durch staatliche Stellen mit solchen von privaten Stellen ist eine solche Situation jedoch nicht mit derjenigen der Fertigung von Ausweiskopien vergleichbar. Diese dient gerade dazu, die Richtigkeit der Angaben des Teilnehmers festzustellen. Es erfolgt somit gerade keine „anonyme und spurenlose“ Aussonderung der personenbezogenen Daten. Im Übrigen erfolgt die Vernichtung der Ausweiskopien in der Praxis zeitlich nicht unmittelbar nach ihrer Erhebung: Üblicherweise erfolgt die Anfertigung von Kopien in den Servicezentren

der Diensteanbieter. Demgegenüber erfolgt die Überprüfung häufig durch zentrale Stellen des jeweiligen Diensteanbieters (vgl. dazu Büttgen in Beck'scher TKG-Komm., 3. Aufl., § 95 Rdn. 29; Kleczewski in Berliner Komm. zum TKG, § 95 Rdn. 18).

Zwar schweigen hierzu die Gesetzesmaterialien zum derzeitigen § 95 Abs. 4 TKG (im Gesetzesentwurf: 93 Abs. 4), man mag aber davon ausgehen, dass der Gesetzgeber diese Fallkonstellation im Blick hatte: Die Vorschrift wurde im Jahr 2000 mit dieser Begründung in die Vorgängervorschrift des § 95 Abs. 4 TKG, § 5 Abs. 4 TDSV eingefügt, nachdem zuvor lediglich die Vorlage des Ausweises verlangt werden durfte. § 5 Abs. 4 TDSV sollte die – bis dahin datenschutzrechtswidrige – Praxis der Servicezentren der Diensteanbieter legalisieren (vgl. BR-Drs. 300/00 - zur Frage der Normenklarheit siehe die Ausführungen zu bb)).

Der Gesetzgeber greift folglich in das Grundrecht der Teilnehmer auf informationelle Selbstbestimmung ein.

bb) Es bestehen erhebliche Zweifel, ob der Regelungszweck des § 95 Abs. 4 TKG diesen Eingriff rechtfertigen kann.

Zwar ist das Recht auf informationelle Selbstbestimmung nicht schrankenlos gewährleistet, sodass der Betroffene einzelne Einschränkungen dieses seines Rechts im überwiegenden Allgemeininteresse hinnehmen muss (vgl. bereits BVerfGE 65, 1 (43, 44)). Eine solche Beschränkung muss jedoch auf einer verfassungsmäßigen gesetzlichen Grundlage beruhen, aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben und die damit dem rechtsstaatlichen Gebot der Normenklarheit entspricht. Bei seiner Regelung hat der Gesetzgeber überdies den Grundsatz der Verhältnismäßigkeit zu beachten (gefestigte Rspr. seit BVerfGE 65, 1 (44)).

(1) Die Vorschrift ist bereits hinsichtlich ihrer Normenklarheit verfassungsrechtlich nicht unproblematisch. Wenn nach dem Wortlaut des § 95 Abs. 4 S. 3 TKG die Ausweiskopie „unverzüglich nach Feststellung der für den Vertragsabschluss erforderlichen Angaben des Teilnehmers zu vernichten“ ist, bedürfte es bei unselbständigen Servicezentren der Diensteanbieter überhaupt keiner Anfertigung von Kopien, da die Handlung der dortigen Angestellten dem Diensteanbieter ohnehin zuzurechnen sind. „Sinnvoll“ wäre eine Regelung allenfalls, wenn Vertriebspartner die Befugnis zur Anfertigung der Ausweiskopien erhielten. Denn rechtlich gesehen kann nur bei der Datenerhebung durch Vertriebspartner überhaupt aus Sicht des Teilnehmers eine „Feststellung der Angaben“ durch „den Diensteanbieter“ zu einem späteren Zeitpunkt erfolgen als zum Zeitpunkt der Datenerhebung. Abs. 4 S. 3 bezieht jedoch anders als § 111 Abs. 2 TKG „Vertriebspartner“ nicht mit in die Befugnis ein, Kopien anzufertigen. Die Vorschrift ist mit anderen Worten widersinnig.

(2) Sieht man über diese Bedenken der Normenklarheit hinweg und unterstellt man, dass die Vorschrift des § 95 Abs. 4 darauf abzielt, dass zwar die Erfassung (Kopieerstellung) in den Dienstleistungszentren oder bei den Vertriebspartnern erfolgt, die Feststellung nach Abs. 4 S. 3 jedoch erst in zentralen Stellen des Diensteanbieters zu erfolgen hat, ist es sehr zweifelhaft, ob § 95 Abs. 4 TKG einen legitimen Zweck erfüllt. Denn in diesem Fall würde § 95 Abs. 4 TKG letztlich darauf abzielen, dem Diensteanbieter die effektive Kontrolle seiner Dienstleistungszentren und Vertriebspartner zu ermöglichen. Die Verbesserung der Vertriebsstruktur durch Private ist jedoch im Verhältnis zum jeweiligen Teilnehmer kein legitimer Grund zur Datenerfassung, sondern ausschließlich ein unternehmensinternes Problem des Anbieters.

(3) Auch im Übrigen bestehen weitere Bedenken hinsichtlich der Verhältnismäßigkeit der Vorschrift. Die Vorschrift leistet der rechtsmissbräuchlichen Verwendung der Ausweiskopien Vorschub, selbst wenn § 25 Abs. 2 Nr. 4b i.V.m. § 18 Abs. 2, 3 PassG das Einscannen des Ausweises und das automatisierte Auslesen von Passdaten bußgeldbewehrt untersagt. Hiervon abgesehen legt die Vorschrift dem Teilnehmer die Duldung der Fertigung von Ausweiskopien auf, die ihm ansonsten im Rechtsverkehr regelmäßig nur zur Zwecken der Inneren Sicherheit und Ordnung abverlangt werden (vgl. z.B. § 9 GwG). Dem entsprechend erscheint § 95 Abs. 4 S. 2, 3 TKG als unangemessener Eingriff in das Recht auf informationelle Selbstbestimmung des Teilnehmers.

II. § 111 Abs. 1 TKG ist, zumindest soweit er einen Diensteanbieter dazu verpflichtet, Daten zu erfassen und vorzuhalten, die er für die Vertragserfüllung nicht benötigt, mit dem Grundrecht der Teilnehmer auf informationelle Selbstbestimmung nicht vereinbar. Art. 10 Abs. 1 GG ist durch die Verpflichtung zur Vorhaltung von Bestandsdaten allerdings nicht berührt. Insoweit nehmen wir Bezug auf die Ihnen bereits übersandte Stellungnahme der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht des Landes Brandenburg vom 24. Januar 2007, deren Begründung wir in Bezug auf die rechtliche Bewertung des § 111 TKG inhaltlich teilen.

III. § 112 Abs. 1 TKG ist in mehrfacher Hinsicht mit dem Grundrecht der Teilnehmer auf informationelle Selbstbestimmung aus Art. 2 Abs. 1, 1 Abs. 1 GG unvereinbar. § 112 Abs. 2, Abs. 4 TKG ist nicht mit dem Fernmeldegeheimnis aus Art. 10 Abs. 1 GG vereinbar, soweit er Auskünfte aus Kundendateien an diverse Behörden gestattet, welche diesen die Identifikation von bislang unbekannten Telekommunikationsteilnehmern ermöglicht. Soweit § 112 Abs. 2 TKG die Erhebung der nach § 111 Abs. 1, Abs. 2 TKG zu speichernden Daten im Vorgriff auf einen Telekommunikationsvorgang ermöglichen, liegt kein Eingriff in das Fernmeldegeheimnis aus Art. 10 Abs. 1 GG vor. In Betracht kommt jedoch, dass jene Vorschriften das Recht auf informationelle Selbstbestimmung unzulässig einschränken.

1) § 112 Abs. 1 TKG ist in mehrfacher Hinsicht mit dem Grundrecht der Teilnehmer auf informationelle Selbstbestimmung unvereinbar. Demgegenüber ist Art. 10 Abs. 1 GG nicht berührt. Auch insoweit nehmen wir Bezug auf die bereits zitierte Stellungnahme der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht des Landes Brandenburg vom 24. Januar 2007, deren Begründung wir in Bezug auf die rechtliche Bewertung des § 112 Abs. 1 TKG inhaltlich teilen.

2) Demgegenüber ist § 112 Abs. 2, Abs. 4 TKG nicht mit dem Fernmeldegeheimnis aus Art. 10 Abs. 1 GG vereinbar, soweit er Auskünfte aus Kundendateien an diverse Behörden gestattet, welche diesen die Identifikation von bislang unbekannten Telekommunikationsteilnehmern ermöglicht. Der Schutz des Grundrechts auf informationelle Selbstbestimmung aus Art. 2 Abs. 1, 1 Abs. 1 GG tritt insoweit gegenüber dem spezielleren Schutz des Art. 10 Abs. 1 GG zurück (vgl. BVerfGE 100, 313 (358)). Die Abgrenzung der beiden grundrechtlichen Gewährleistungen ist nicht zuletzt deshalb geboten, weil das Zitiergebot und nach der bisherigen Rechtsprechung lediglich für Eingriffe in das Grundrecht aus Art. 10 Abs. 1 GG besondere Kennzeichnungspflichten zu beachten sind (vgl. dazu Vgl. BVerfGE 100, 313 (360 f.); BVerfGE 110, 33 (70 f.)).

a) Der Schutz des Fernmeldegeheimnisses umfasst den Kommunikationsinhalt und die Kommunikationsumstände. Die öffentliche Gewalt soll grundsätzlich nicht die Möglichkeit haben, sich Kenntnis vom Inhalt der über Fernmeldeanlagen abgewickelten mündlichen oder schriftlichen Information zu verschaffen. Dabei bezieht sich der Grundrechtsschutz auf alle mittels der Fernmeldetechnik ausgetauschten Informationen (vgl. BVerfGE 100, 313 [358]; 106, 28 [37]; 110, 33 [52 f.]; 113, 348 [364 f.]). In den Schutzbereich fällt auch die Erlangung der Kenntnis, ob, wann, wie oft und zwischen welchen Personen Telekommunikation stattgefunden hat oder versucht worden ist (vgl.

BVerfGE 67, 157 [172]; 85, 386 [395]; 100, 313 [358]; 107, 299 [312 f.]; 113, 348 [365]). Dabei erstreckt sich die Schutzwirkung des Art. 10 GG auch auf den Informations- und Datenverarbeitungsprozess, der sich an die Kenntnisnahme von geschützten Kommunikationsvorgängen anschließt und in dem Gebrauch von den erlangten Kenntnissen gemacht wird (vgl. BVerfGE 100, 313 [359]; 113, 348 [365]).

b) Ein Eingriff liegt insbesondere vor, wenn sich staatliche Stellen aufgrund der angegriffenen Normen (unmittelbar) ohne Zustimmung der Beteiligten Kenntnis vom Inhalt und den Umständen eines fernmeldetechnisch vermittelten Kommunikationsvorgangs verschaffen können (vgl. BVerfGE 100, 313 [366]; 107, 299 [313]; 113, 348 [365]).

§ 112 Abs. 2 i.V.m. § 111 Abs. 1 S. 1, Abs. 2 TKG ermöglicht solche Eingriffe. Den in der Vorschrift genannten Sicherheitsbehörden können Auskünfte über Rufnummern, den Namen und die Anschrift des Rufnummerninhabers, das Datum des Vertragsbeginns, bei natürlichen Personen deren Geburtsdatum, sowie bei Festnetzanschlüssen auch die Anschrift des Anschlusses, Datum des Vertragsendes an die in § 112 Abs. 2 genannten Behörden erteilt werden.

Ohne die Vorschriften des § 112 Abs. 2 TKG, § 111 Abs. 1, Abs. 2 TKG stünden die Sicherheitsbehörden gerade in einem liberalisierten Telekommunikationsmarkt vor dem Problem, dass Telekommunikationsanschlüsse, Rufnummern usw. für sie häufig als nicht auflösbares Pseudonym des jeweiligen Anschlussinhabers darstellt. Dieses Problem löst § 112 Abs. 2 TKG auf, indem die Sicherheitsbehörden in die Lage versetzt werden, die konkrete Identität von Telekommunikationsteilnehmern eines ganz bestimmten Telekommunikationsvorgangs zu klären. Der Informationsabruf durch die in § 111 Abs. 2 TKG genannten Stellen dient damit der Klärung näherer Umstände einer konkreten Telekommunikation. Zwar nicht notwendig, aber regelmäßig ist der Anschlussinhaber auch der Telekommunikationsteilnehmer. Jedenfalls zielt die Bestandsdatenabfrage unmittelbar auf die Ermittlung des konkreten Telekommunikationsteilnehmers.

Dem steht auch nicht entgegen, dass der Zweite Senat in seinem Urteil vom 2. März 2006 (2 BvR 2099/04, NStZ 2006, 641) im Zusammenhang mit der Beschlagnahme von Mobilboxdaten durch Strafverfolgungsbehörden festgestellt hat, dass der Schutz des Art. 10 Abs. 1 GG sich nicht auf Inhalte und Umstände der (Tele-)Kommunikation erstreckt, wenn sie außerhalb des laufenden Kommunikationsvorgangs im Herrschaftsbereich des Kommunikationsteilnehmers gespeichert werden (BVerfG a. a. O., Rdnr. 68, 72 ff.). Denn der Datenzugriff erfolgt hier bei dem Diensteanbieter und damit gerade nicht im Einflussbereich des Betroffenen, sondern bei einem Dritten.

Auch der Umstand, dass der Staat zur Gewährleistung der öffentlichen Sicherheit mit den Diensteanbietern als solchen Dritten private Stellen einschaltet, um an Bestandsdaten der Teilnehmer zu gelangen, schließt einen Eingriff in das Fernmeldegeheimnis nicht aus. Zwar richten sich die Grundrechte regelmäßig nur an die Gesetzgebung, vollziehende Gewalt und Rechtsprechung, mithin an staatliche Stellen, vgl. Art. 1 Abs. 3 GG. Zu berücksichtigen ist hierbei jedoch der bereits in der Entscheidung des Ersten Senats vom 10. Februar 1960 angedeutete Rechtsgedanke, dass Maßnahmen Privater den Charakter von Grundrechtseingriffen haben können, wenn die Maßnahmen vom Staat veranlasst und nur für ihn durchgeführt werden (vgl. BVerfGE 10, 302 (326 f.)). Aus Sicht des Teilnehmers ist mit anderen Worten die Verpflichtung von Diensteanbietern zur Übermittlung von Bestandsdaten an Sicherheitsbehörden nicht seiner eigenen Einflussosphäre, sondern der Herrschaftssphäre des Staats zuzuordnen.

c) Dieser Eingriff ist verfassungsrechtlich nicht gerechtfertigt. Zunächst bestehen Bedenken hinsichtlich der Erfordernisse der Normenklarheit und Normenbestimmtheit, des weiteren hinsichtlich der Verhältnismäßigkeit.

aa) Insgesamt bedarf es einer bereichsspezifischen und präzisen Bestimmung des Verwendungszweckes (st. Rspr. seit BVerfGE 65, 1 (46), vgl. aus jüngerer Zeit z. B. BVerfGE 110, 33 (70); BVerfGE 113, 29 (51)). Das Gebot einer bereichsspezifischen und konkreten gesetzlichen Eingriffsbefugnis gilt dabei auch für Weitergabe von Daten (vgl. BVerfG NJW 2006, S. 1939, (1947 f., Rdnr. 149 ff.)). Aufgrund der Ermächtigung zu Überwachungsmaßnahmen muss zwar nicht die konkrete Maßnahme vorhersehbar sein. Dies wäre insbesondere bei heimlichen Überwachungsmaßnahmen auch kontraproduktiv. Die betroffene Person muss aber zumindest anhand der Befugnisnorm grundsätzlich erkennen können, bei welchen Anlässen und unter welchen Voraussetzungen sein Verhalten das Risiko einer Überwachung erzeugt (vgl. BVerfG NJW 2005, 2603 (2607) für Art. 10 GG). Die gesetzlichen Eingriffsbefugnisse dienen dazu, hinreichend klare Maßstäbe vorzugeben, um die Entscheidung über die Grenzen der Freiheit des Bürgers nicht einseitig in das Ermessen der Polizei und den sonstigen Sicherheitsbehörden zu stellen (vgl. z. B. BVerfGE 78, 214 (226), BVerfG NJW 2005, 2603 (2607)). Deshalb müssen Bestimmtheit und Klarheit der gesetzlichen Regelung die Exekutivgewalt in ihrem Verhalten nach Inhalt, Zweck und Ausmaß binden können (vgl. BVerfGE 56, 1 (12); BVerfGE 110, 33 (54); BVerfG NJW 2005, 2603 (2607)). Zugleich soll die Rechtsprechung in die Lage versetzt werden, die Verwaltung anhand rechtlicher Maßstäbe kontrollieren zu können (vgl. BVerfGE 110, 33 (54); BVerfG NJW 2005, 2603 (2607)).

bb) Diesen Anforderungen wird § 112 Abs. 2 TKG nicht gerecht. Zwar sind die abrufberechtigten Behörden abschließend aufgezählt. Hinsichtlich der Übermittlungszwecke beschränkt sich § 112 Abs. 2 TKG bei einigen abrufberechtigten Behörden darauf zu verlangen, dass die Auskünfte „zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich sind.“ Weitere inhaltliche Präzisierungen, unter welchen inhaltlichen Voraussetzungen eine Abfrage zulässig sein soll, sieht die Vorschrift nicht vor.

Da Auskünfte aus den Kundendateien auch nicht nur zum Zweck der Vorbereitung von Maßnahmen der Telekommunikationsüberwachung erteilt werden müssen, erhält § 112 Abs. 2 TKG den Charakter einer Blankettermächtigung.

Für die verfassungsrechtliche Bewertung der Vorschrift ist weiterhin von Relevanz, dass die Regulierungsbehörde, welche die Funktion der Daten übermittelnden Stelle übernimmt, § 112 Abs. 4 TKG noch nicht einmal ausdrücklich gehalten ist zu überprüfen, ob sich das Übermittlungsersuchen im Rahmen des jeweiligen Aufgabenbereichs bewegt. Damit bleibt § 112 Abs. 2, 4 TKG hinter einem Standard an Vorkehrungen des Datenübermittlers gegen missbräuchliche Datenabrufe zurück, die selbst bei relativ unproblematischen Datenübermittlungsvorgängen zum rechtsstaatlichen Mindeststandard gehören (vgl. § 15 Abs. 2 S. 3 BDSG, vgl. für den Polizeibereich z. B. § 33 Abs. 1 S. 2 BPolG). Mit dem Wegfall dieser Prüfungspflicht entfällt auch weitgehend die Möglichkeit, eine Datenübermittlung zu unterlassen, wenn ihr überwiegende schutzwürdige Belange des Betroffenen entgegenstehen (vgl. § 33 Abs. 3 BPolG). Dies verstößt gegen die verfassungsrechtliche Vorgabe an den einfachen Gesetzgeber, für hinreichende Vorkehrungen zu sorgen, die einer unangemessenen Beeinträchtigung des Persönlichkeitsrechts entgegenwirken (vgl. BVerfGE 65, 1, (46)).

3) Soweit § 112 Abs. 2 TKG die Erhebung der nach § 111 Abs. 1, Abs. 2 TKG zu speichernden Daten im Vorgriff auf einen Telekommunikationsvorgang ermöglichen, liegt kein Eingriff in das Fernmeldegeheimnis aus Art. 10 Abs. 1 GG vor. Hiernach dient die Datenerhebung der Vorbereitung eines Eingriffs in das Fernmeldegeheimnis, ist ihm also vorgelagert. Hierzu wenden die Beschwerdeführer zwar ein, dass es Schutzzweck des Fernmeldegeheimnisses sei, die an der Telekommu-

nikation Beteiligten so zu stellen, wie sie bei unmittelbarer Kommunikation miteinander stünden. Bei einer unmittelbaren Kommunikation würden aber keine Bestandsdaten anfallen und gespeichert werden (vgl. S.10 der Verfassungsbeschwerde). Selbst wenn man diese Prämisse teilt, ist ein Eingriff in das Fernmeldegeheimnis insoweit nach den oben entwickelten Kriterien zu verneinen. Allerdings dürfte ein erheblicher, nicht gerechtfertigter Eingriff in das Recht der Teilnehmer auf informationelle Selbstbestimmung aus Art. 2 Abs. 1, 1 Abs. 1 GG vorliegen.

IV. Soweit § 113 Abs. 1 TKG im Wege der manuellen Auskunftserteilung wie § 112 Abs. 2 TKG die Identifizierung von Telekommunikationsteilnehmern ermöglicht, verletzt die Vorschrift das Fernmeldegeheimnis aus Art. 10 Abs. 1 GG. Die zu III. gemachten Ausführungen sind weitgehend auf die rechtliche Bewertung des § 113 Abs. 1 TKG übertragbar. Soweit im Übrigen ein Eingriff in das Recht der Teilnehmer auf informationelle Selbstbestimmung vorliegt, schließe ich mich der Stellungnahme der Landesbeauftragten für Datenschutz und für das Recht auf Akteneinsicht vom 24. Januar 2007 an. Diese Stellungnahme lediglich ergänzend halte ich es insbesondere für eine unangemessene Grundrechtsbeschränkung, dass § 113 Abs. 1 S. 1 TKG zur Verfolgung einfacher Ordnungswidrigkeiten oder zur Abwehr von Gefahren für die öffentlichen Ordnung eine Auskunftspflicht der Diensteanbieter begründet. Damit leistet der Gesetzgeber erheblichen Grundrechtseingriffen zur Verfolgung von Bagatellen bzw. zur Abwehr von normabweichendem, aber legalem Verhalten Vorschub.

V. Soweit den Diensteanbietern durch §§ 111-113 TKG die Pflicht auferlegt wird, Vorrichtungen für Datenabrufe zu treffen sowie Daten zu erfassen und vorzuhalten, die für die Vertragsabwicklung mit den Teilnehmern nicht erforderlich sind, liegen Eingriffe in die Wirtschaftsgrundrechte der Diensteanbieter vor. Durch den staatlichen Einfluss auf die Gestaltung des konkreten Vertragsverhältnisses dürfte eine Berufsausübungsregel und damit ein Eingriff in die Berufsfreiheit aus Art. 12 I GG vorliegen. Im Übrigen greifen die Vorschriften zumindest in die wirtschaftliche Handlungsfreiheit der Diensteanbieter aus Art. 2 I GG ein. Aufgrund meiner gesetzlich auf den Persönlichkeitsrechtsschutz beschränkten Funktion verzichte ich insoweit auf eine ausführliche rechtliche Bewertung, möchte jedoch auf den Umstand aufmerksam machen, dass die Verpflichtung zur Ermöglichung von Überwachungsmaßnahmen den Diensteanbietern weitgehende Mitwirkungsleistungen an der staatlichen Sicherheitsarchitektur abverlangt, die das Vertrauensverhältnis zwischen Diensteanbieter und Kunde nachhaltig zu beeinträchtigen vermag.

Mit freundlichen Grüßen

Dix

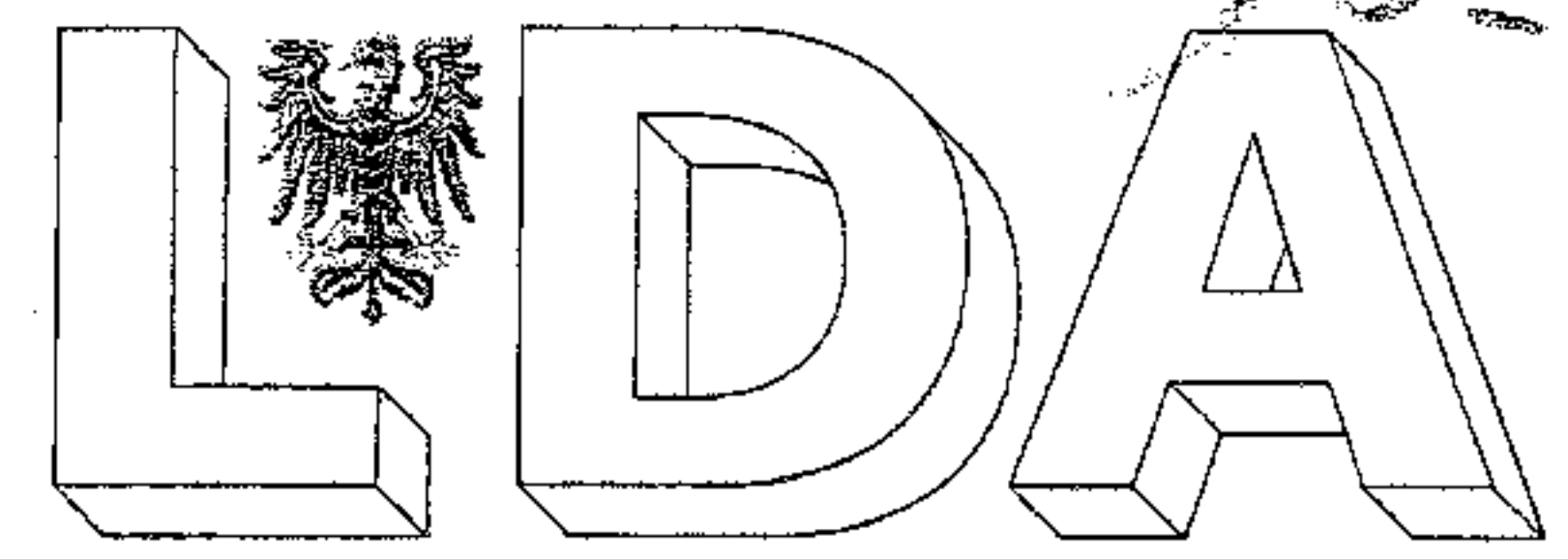
**Die Landesbeauftragte  
für den Datenschutz und  
für das Recht auf Akteneinsicht**

**Dagmar Hartge**

**Mandant hat Abschrift**

LDA Bbg. • Stahnsdorfer Damm 77 • Haus 2 • 14532 Kleinmachnow

LAND  
BRANDENBURG



*Schutz der*

- *Persönlichkeitsrechte*
- *Informationsfreiheit*

Bundesverfassungsgericht  
Erster Senat  
Postfach 1771

**76006 Karlsruhe**

Datum: 24. Januar 2007

Bearbeiter/in: [REDACTED]

Telefon: 033203 [REDACTED]

Telefax: 033203 [REDACTED]

Geschäftszeichen: Ha/136/06/318

(bei Antwortschreiben bitte angeben)

**Verfassungsbeschwerde gegen Vorschriften des Telekommunikationsgesetzes**

- Ihr Schreiben vom 10. Juli 2006, Az.: 1 BvR 1299/05

Sehr geehrter Herr Prof. Dr. Hoffmann-Riem,

in dem Verfahren über die Verfassungsbeschwerde

1. [REDACTED]  
[REDACTED]

2. [REDACTED]  
[REDACTED]

gegen § 95 Abs. 3 und 4, §§ 111, 112, 113 des Telekommunikationsgesetzes (TKG)  
vom 22. Juni 2004 (BGBl. I S. 1190)

bedanke ich mich für die Gelegenheit zur Stellungnahme. Ebenso darf ich Ihnen für die Verlängerung der Stellungnahmefrist bis zum 31. Januar 2007 danken.

Meine ausführliche Stellungnahme zur Verfassungsmäßigkeit der angegriffenen Normen des Telekommunikationsgesetzes habe ich als Anlage beigefügt. In meiner Funktion als Vorsitzende des Arbeitskreises Medien der Datenschutzbeauftragten des Bundes und der Länder habe ich die Stellungnahme mit der Mehrzahl meiner Kolleginnen und Kollegen abgestimmt.

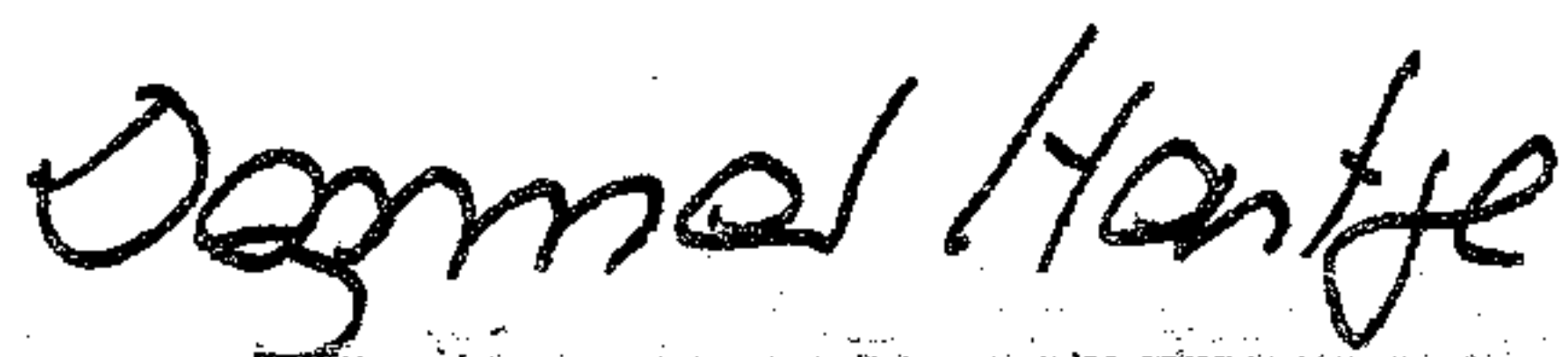
Ich gebe meine Stellungnahme deshalb gleichzeitig auch im Namen

- des Landesbeauftragten für den Datenschutz Baden-Württemberg,
- des Bayerischen Landesbeauftragten für den Datenschutz,
- des Landesbeauftragten für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen,
- des Hessischen Datenschutzbeauftragten,
- des Landesbeauftragten für den Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern,
- des Landesbeauftragten für den Datenschutz Niedersachsen,
- der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen,
- des Landesbeauftragten für den Datenschutz Rheinland-Pfalz,
- des Landesbeauftragten für Datenschutz und Informationsfreiheit des Saarlandes,
- des Sächsischen Datenschutzbeauftragten,
- des Landesbeauftragten für den Datenschutz Sachsen-Anhalt und
- des Thüringer Landesbeauftragten für den Datenschutz

ab.

Meinem Schreiben sind fünf Abzüge beigelegt.

Mit freundlichen Grüßen



Dagmar Hartge

**1 Anlage**

**Die Landesbeauftragte  
für den Datenschutz und  
für das Recht auf Akteneinsicht**

Dagmar Hartge



**Verfassungsbeschwerde gegen § 95 Abs. 3 und 4, §§ 111, 112, 113 des Tele-  
kommunikationsgesetzes (TKG) vom 22. Juni 2004, 1 BvR 1299/05**

**Gemeinsame Stellungnahme**

des Landesbeauftragten für den Datenschutz Baden-Württemberg,  
des Bayerischen Landesbeauftragten für den Datenschutz,  
des Landesbeauftragten für Datenschutz und Informationsfreiheit der Freien Hansestadt  
Bremen,  
des Hessischen Datenschutzbeauftragten,  
des Landesbeauftragten für den Datenschutz und Informationsfreiheit Mecklenburg-  
Vorpommern,  
des Landesbeauftragten für den Datenschutz Niedersachsen,  
der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen,  
des Landesbeauftragten für den Datenschutz Rheinland-Pfalz,  
des Landesbeauftragten für Datenschutz und Informationsfreiheit des Saarlandes,  
des Sächsischen Datenschutzbeauftragten,  
des Landesbeauftragten für den Datenschutz Sachsen-Anhalt,  
des Thüringer Landesbeauftragten für den Datenschutz und  
der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht  
Brandenburg

Kleinmachnow, den 24. Januar 2007

## **Vorbemerkung**

Aufgrund des Beschlusses der 1. Kammer des 1. Senats des BVerfG vom 21. Juni 2006 ist nur noch über die Verfassungsmäßigkeit der §§ 95 Abs. 3 und 4, 111, 112 und 113 des Telekommunikationsgesetzes (TKG) zu befinden. Im Übrigen wurde die Verfassungsbeschwerde nicht zur Entscheidung angenommen.

## **Zur Vereinbarkeit der angegriffenen Vorschriften mit dem Grundgesetz**

### **I. § 95 Abs. 3 TKG**

§ 95 Abs. 3 TKG ist für sich gesehen mit dem Grundgesetz vereinbar. Er bedarf jedoch der verfassungskonformen Auslegung.

Der Schutzbereich von Art. 10 GG ist nicht eröffnet, da Bestandsdaten der Telekommunikation nicht dem Fernmeldegeheimnis unterliegen (dazu näher unten III. 1).

§ 95 Abs. 3 TKG greift allerdings in den Schutzbereich des Rechts auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) ein. § 95 Abs. 3 TKG verpflichtet die Diensteanbieter, Bestandsdaten mit Ablauf des auf die Beendigung des Vertragsverhältnisses folgenden Kalenderjahrs zu löschen. Die Vorschrift enthält lediglich eine Maximalfrist, nach deren Ablauf die Daten spätestens gelöscht werden müssen. Insbesondere werden die Diensteanbieter hierdurch nicht verpflichtet, die Daten über die gesamte Frist zu speichern. § 95 Abs. 3 TKG lässt es vielmehr zu, Bestandsdaten zu einem wesentlich früheren Zeitpunkt zu löschen.

§ 95 Abs. 3 TKG bezieht sich allein auf die i. S. v. § 95 Abs. 1 Satz 1 TKG erforderlichen Bestandsdaten und die dort festgelegte Zweckbestimmung. An dieser Stelle besteht insbesondere kein rechtlicher Zusammenhang mit den nach § 111 TKG erhobenen Daten. Allerdings führen die Verpflichtungen des § 111 Abs. 1 Satz 4 TKG regelmäßig dazu, dass eine vorzeitige Löschung nach § 95 Abs. 3 Satz 1 TKG nicht in Betracht kommt. Für die in § 95 Abs. 1 TKG festgelegten Zwecke müssten die Daten in diesem Falle gem. § 95 Abs. 3 Satz 2 TKG i. V. m. § 35 Abs. 3 BDSG gesperrt werden, bis sie nach § 111 Abs. 1 Satz 4 TKG gelöscht werden können.

Bestandsdaten, die nicht von § 111 Abs. 1 Satz 1 TKG erfasst werden, gleichwohl aber nach § 95 Abs. 1 Satz 1 TKG erforderlich waren (z. B. Informationen über bestimmte Tarifgestaltungen, statische IP-Adressen oder E-Mail-Adressen), können nach § 95 Abs. 3 Satz 1 TKG in jedem Falle auch vor Ablauf der Frist gelöscht werden.

Der aus dem Recht auf informationelle Selbstbestimmung folgende Anspruch, dass Eingriffe nur dann verfassungsgemäß sind, wenn sich die Verwendung personenbezogener Daten auf das zur Erreichung eines definierten Zweckes erforderliche Maß beschränkt (vgl. BVerfGE 65, 1 [46]), kann hier durch eine Löschung bzw. Sperrung vor Ablauf der in § 95 Abs. 3 Satz 1 TKG festgelegten Frist in verfassungsgemäßer Weise erfüllt werden. Dies ist mit dem Wortlaut noch vereinbar, da die Formulierung „sind ... zu löschen“ auch eine vorzeitige Löschung sprachlich zulässt. So – und nur so – kann durch eine verfassungskonforme Auslegung die Vereinbarkeit von § 95 Abs. 3 Satz 1 TKG mit dem Grundgesetz gewahrt werden.

Verfassungsrechtlich problematisch wird die Speicherung und die Löschungsfrist für Bestandsdaten erst durch die in § 111 TKG vorgesehene zwangsweise Erhebung und Speiche-

rung für Zwecke der Sicherheitsbehörden. Auf diese Aspekte wird deshalb unten bei der Bewertung von § 111 TKG (III.) genauer eingegangen.

## **II. § 95 Abs. 4 TKG**

Gegen die Vereinbarkeit von § 95 Abs. 4 TKG mit dem Grundgesetz bestehen Bedenken. Er verstößt nach hiesiger Auffassung gegen das Recht auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG.

### 1. Schutzbereich

Das Recht auf informationelle Selbstbestimmung gewährleistet die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen (BVerfGE 65, 1 [43]). Dazu gehört ohne Zweifel auch die Freiheit, mit den in amtlichen Ausweispapieren gespeicherten personenbezogenen Daten selbstbestimmt umzugehen, sodass der Schutzbereich des Grundrechts eröffnet ist.

### 2. Eingriff

Das Gesetz schreibt in § 95 Abs. 4 TKG vor, dass die Diensteanbieter die Vorlage amtlicher Ausweispapiere beim Vertragsabschluss verlangen können. Zudem enthält Satz 2 die zusätzliche Befugnis, das jeweilige Ausweispapier auch kopieren zu können. Damit greift die Norm in das Grundrecht aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG ein.

### 3. Verfassungsrechtliche Rechtfertigung

Eingriffe in das Recht auf informationelle Selbstbestimmung sind im überwiegenden Allgemeininteresse durch ein Gesetz oder auf Grund eines Gesetzes zulässig. Sie bedürfen zu ihrer verfassungsrechtlichen Rechtfertigung einer gesetzlichen Grundlage, die dem Gebot der Normenklarheit entspricht und die den Grundsatz der Verhältnismäßigkeit beachtet.

Bei § 95 Abs. 4 TKG bestehen Zweifel hinsichtlich der Verhältnismäßigkeit. Daran vermögen auch die verfahrensmäßigen Sicherungen der Sätze 3 und 4 des Absatzes (Löschungspflicht und Verwendungsbeschränkung) nichts zu ändern.

Zweckbestimmung der Vorlage amtlicher Ausweise ist nach dem Gesetzeswortlaut die Überprüfung der Angaben des Teilnehmers. Soweit die Erhebung von Bestandsdaten nach § 95 Abs. 1 TKG erforderlich ist, ist die Vorlage eines Ausweises geeignet, den genannten Zweck zu erfüllen.

Es ist jedoch fraglich, ob die Vorlage und Kopie von Ausweispapieren erforderlich und verhältnismäßig im engeren Sinne ist. Die Verpflichtung zur Vorlage eines amtlichen Ausweises könnte aus datenschutzrechtlicher Sicht noch hingenommen werden. Zwar erhält der Diensteanbieter in der Regel zusätzliche Informationen über die Nutzer, die für die Erbringung des Dienstes nicht erforderlich sind. Hierzu gehören insbesondere Angaben zur Nationalität und biometrische Merkmale (Größe, Augenfarbe) sowie die Ausweisnummer, die auf dem Ausweis vermerkt sind. Ferner ist nicht auszuschließen, dass bei Ausländern durch die Vorlage eines Ausweispapiers der ausländerrechtliche Status offenbart wird. Durch die bloße

Vorlage würden die Daten jedoch ohne Speicherung lediglich erhoben werden, sodass wegen der Flüchtigkeit der Informationen die Intensität des Eingriffs äußerst gering ist.

Anders ist die Befugnis zum Kopieren des Ausweises zu betrachten. Hier werden die nicht zur Authentifizierung erforderlichen Daten nicht nur erhoben, sondern auch gespeichert. Daran ändert auch die nachträgliche Vernichtung der Kopien nichts. Auch die vorübergehende Speicherung führt bereits zu einer weit höheren Missbrauchsgefahr als die bloße Vorlage ohne Speicherung.

Eine Kopierbefugnis amtlicher Ausweise ist außerhalb der Telekommunikation nur in seltenen Fällen und in erster Linie zur Aufdeckung und Verfolgung nicht unerheblicher Straftaten, nicht aber zur Überprüfung von Angaben in Vertragsbeziehungen gesetzlich vorgesehen, vgl. z. B. § 9 des Geldwäschegesetzes.

Gemessen an der Zweckbestimmung des § 95 Abs. 4 TKG, die sich nur auf die Überprüfung der betriebsnotwendigen Angaben nach § 95 Abs. 1 TKG bezieht, erscheint die Kopierbefugnis wegen des Übermaßes der Verarbeitung nicht erforderlicher personenbezogener Daten unangemessen.

### **III. § 111 TKG**

§ 111 TKG ist nach hiesiger Ansicht mit dem Grundrecht auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG nicht vereinbar und somit verfassungswidrig.

#### **1. Vereinbarkeit mit Art. 10 GG**

§ 111 TKG verstößt nicht gegen das grundrechtlich durch Art. 10 GG geschützte Fernmeldegeheimnis. Der Schutzbereich von Art. 10 GG ist nicht eröffnet, da die von der Regelung betroffenen Bestandsdaten nicht vom Fernmeldegeheimnis geschützt sind.

##### **a. Schutzbereich**

Der Grundrechtsschutz bezieht sich auf jede mittels Fernmeldetechnik ausgetauschte Kommunikation. Das Fernmeldegeheimnis schützt die vertrauliche Inanspruchnahme der Telekommunikation. Die Nutzung der Telekommunikation bedarf eines besonderen verfassungsrechtlichen Schutzes, weil sie besonderen Gefährdungen der Kenntnisnahme durch Dritte ausgesetzt ist (BVerfGE 106, 28 [36]). Dabei sind nach ständiger Rechtsprechung des Bundesverfassungsgerichts nicht nur die Inhalte der Kommunikation, sondern auch deren nähere Umstände (insbesondere ob, wann und wie oft zwischen welchen Personen oder Anschlüssen Kommunikation stattgefunden hat) vom Fernmeldegeheimnis geschützt, vgl. BVerfGE 100, 313 (358). Das Fernmeldegeheimnis begründet zudem nicht nur ein Abwehrrecht gegen den Staat, sondern eine Schutzpflicht des Staates, Zugriffe von privaten Dritten zu unterbinden (BVerfGE 106, 28 [37]).

##### **b. Reichweite des Schutzbereiches**

Daten über die näheren Umstände der Telekommunikation sind zunächst die in § 3 Nr. 30 TKG definierten und in § 96 Abs. 1 TKG präzisierten Verkehrsdaten. So sind zum Beispiel Kennziffern oder Identifizierungsmerkmale, die nicht unmittelbar vom Teilnehmer stammen,

sondern die der Dienstanbieter zur Ermöglichen eines konkreten Kommunikationsvorganges nutzt, nähere Umstände der Telekommunikation. Bestandsdaten gehören jedoch nicht zu den näheren Umständen einer Telekommunikation. Bestandsdaten umfassen gem. § 3 Nr. 3 TKG Daten der Telekommunikationsteilnehmerinnen und -teilnehmer die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden. Sie beziehen sich nicht auf einen konkreten Kommunikationsvorgang. Es gibt jedoch Bestandsdaten, wie beispielsweise die Rufnummer oder die statische IP-Adresse, die bei einem Kommunikationsvorgang zu den näheren Umständen der Kommunikation werden. Ohne Rufnummer oder IP-Adresse kann die Verbindung nicht hergestellt werden, so dass in diesem Fall die Daten zu Verkehrsdaten im Sinne des § 96 TKG werden.

§ 111 TKG betrifft jedoch ausschließlich Daten über das Vertragsverhältnis, die gleichzeitig zu den Bestandsdaten i. S. v. § 3 Nr. 3 TKG gehören können. Auch wenn, etwa bei Prepaid-Angeboten, die nach § 111 TKG zu erhebenden und speichernden Daten nicht nach § 95 Abs. 1 TKG erforderlich sind, so entspricht ihr Charakter den Bestandsdaten i. S. v. § 3 Nr. 3 TKG. Jedenfalls handelt es sich bei den in § 111 TKG aufgeführten Daten nicht um Verkehrsdaten i. S. v. § 3 Nr. 30 TKG.

Im Unterschied zu den Verkehrsdaten ist den Daten über die Vertragsgestaltung nicht zu entnehmen, ob, wann und wie oft zwischen welchen Personen bzw. Anschlüssen Telekommunikation stattgefunden hat. Die nach § 111 Abs. 1 TKG zu erhebenden Daten Rufnummer, Name und Anschrift des Nummerninhabers, Datum des Vertragsbeginns, Geburtsdatum, Anschrift des Festnetzanschlusses sowie ggf. Vertragsende sind allein nicht geeignet, Rückschlüsse darauf zuzulassen, wann und wie oft zwischen welchen Personen bzw. Anschlüssen Telekommunikation stattgefunden hat.

Zwar kann aus der Tatsache, dass jemand sich überhaupt des Mittels der Telekommunikation bedient, geschlossen werden, dass er dieses sehr wahrscheinlich auch in Anspruch nehmen wird. Es ist den hier in Rede stehenden Daten jedoch weder zu entnehmen, wann die Kommunikation in Anspruch genommen wird noch wie oft und mit wem. Aus der Definition der näheren Umstände der Telekommunikation kann daher nur geschlossen werden, dass hiermit konkrete einzelne Kommunikationsvorgänge gemeint sind. Auch bei Kenntnis der Daten nach § 111 Abs. 1 TKG durch einen Dritten stehen die an der Kommunikation Beteiligten so, wie sie bei unmittelbarer Kommunikation miteinander stünden (vgl. BVerfGE 100, 313 [363]). Ein Dritter, der sich Zugang zu diesen Daten verschaffte, wüsste auch mit ihrer Kenntnis nicht, ob überhaupt Telekommunikation stattfindet oder wann, wie oft und mit wem.

Im Ergebnis ist der Schutzbereich von Art. 10 GG nicht eröffnet.

## 2. Vereinbarkeit mit Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG

Die in § 111 Abs. 1 TKG aufgestellte Verpflichtung jedes geschäftsmäßigen Erbringers von Telekommunikationsdiensten, bestimmte Daten für die Auskunftsverfahren nach §§ 112, 113 TKG zu erheben und zu speichern, verstößt gegen das Recht auf informationelle Selbstbestimmung, weil sie nicht dem Grundsatz der Verhältnismäßigkeit entspricht.

### *a. Schutzbereich*

Der Schutzbereich des Rechts auf informationelle Selbstbestimmung ist durch die gesetzliche Verpflichtung, bestimmte personenbezogene Daten anzugeben, eröffnet.

## *b. Eingriff*

Ebenso unstreitig ist, dass eine gesetzliche Anordnung, bestimmte Daten für Zwecke der Sicherheitsbehörden angeben zu müssen sowie deren obligatorische Speicherung durch die Anbieter für die gleichen Zwecke als ein vom Staat veranlasster Eingriff in das Grundrecht angesehen werden muss.

Der Eingriff geschieht nur vermittelt über die privatrechtlich organisierten Telekommunikationsunternehmen. Der Eingriff ist jedoch hoheitlich angeordnet. Die Privatunternehmen haben keinen Handlungsspielraum, so dass die Datenspeicherung gem. § 111 TKG rechtlich auch der öffentlichen Gewalt zuzurechnen ist (siehe auch BVerfG 1 BvR 330/96).

## *c. Verfassungsrechtliche Rechtfertigung*

### *aa. Bestimmtheit der Regelung*

Ein Eingriff in das Recht des Einzelnen darf nur insoweit erfolgen, wie es zum Schutz öffentlicher Interessen unerlässlich ist (BVerfGE 19, 342 [348], st. Rspr.). Der Gesetzgeber hat den Verwendungszweck der zu erhebenden Daten bereichsspezifisch und präzise zu bestimmen. Der Verwendungszweck ist das Auskunftsverfahren nach §§ 112 und 113. Somit müsste der Verwendungszweck in §§ 112 und 113 präzise und bereichsspezifisch geregelt sein.

### *bb. Verhältnismäßigkeit*

§ 111 TKG ist im Hinblick auf seine Zweckbestimmung weder geeignet, erforderlich noch verhältnismäßig im engeren Sinne.

Nach der Systematik und dem Kontext der Vorschrift ist es ihr ausschließlicher Zweck, die Daten für die sicherheitsbehördliche Ermittlungstätigkeit auch dann zur Verfügung zu haben, wenn sie für die betrieblichen Zwecke des Anbieters (vgl. § 95 Abs. 1 TKG) nicht erforderlich sind. Aus der Gesetzesbegründung selbst (BT-Drs. 15/2316, S. 95) lassen sich keine Erkenntnisse zur Notwendigkeit der verpflichtenden Speicherung und Erhebung gewinnen. Dort wird lediglich bei der Begründung der Löschungsfrist (Abs. 1 Satz 4) genauer auf den Hintergrund der Regelung eingegangen.

Der umfassenden Novellierung des TKG im Jahre 2004 ging im Jahre 2002 jedoch ein Gesetzgebungsverfahren voraus, bei dem in § 90 TKG a. F. bereits die gleiche Verpflichtung geplant war. Dies wurde zum damaligen Zeitpunkt vor allem mit der aus Sicht der Sicherheitsbehörden unbefriedigenden Situation begründet, dass gerade im Mobilfunkbereich und hier insbesondere bei den Prepaid-Angeboten Straftäter bewusst und gezielt in kurzen Abständen neue SIM-Karten erwerben, die Karten häufig wechseln, mehrere Karten parallel benutzen oder untereinander tauschen und weitergeben.

Auch wenn die Erhebungs- und Speicherpflicht vor allem auf die Nutzer von Prepaid-Karten im Mobilfunk abzielt, die dann nicht mehr anonym telefonieren können sollen, betrifft die Identifikationspflicht sämtliche geschäftsmäßig angebotenen Telekommunikationsdienste, bei denen die Nutzer Inhaber einer Rufnummer sind. Hierzu gehören z. B. auch Unternehmen und Verwaltungen, die ihren Mitarbeitern die private Nutzung von Telekommunikation ermöglichen, Hotels und Krankenhäuser sowie sonstige geschlossene Benutzergruppen (z. B. Corporate Networks, Schulen, Hochschulen).

Die verpflichtende Erhebung und Speicherung bestimmter Bestandsdaten ist nicht geeignet, ihren Zweck zu erreichen. Wie zuvor dargestellt, besteht das Hauptproblem der Sicherheitsbehörden darin, dass Straftäter bewusst und gezielt in kurzen Zeitabständen neue Prepaid-Karten erwerben, die Karten häufig – teilweise nach jedem Telefonat – wechseln, mehrere Karten parallel benutzen oder die Karten untereinander tauschen.

Es wurde vom Gesetzgeber bisher nicht nachvollziehbar und überzeugend dargelegt, inwieweit eine Erhebungs- und Speicherpflicht die behaupteten Schwierigkeiten lösen soll. Auch bei einer gesetzlich angeordneten Pflicht werden Straftäter Strohleute zum Kauf von SIM-Karten auf Prepaid-Basis einsetzen, eine Vielzahl von Karten erwerben, diese mit vielen verschiedenen Personen soweit tauschen, dass auch damit kaum noch die Inhaber dieser auf Prepaid-Basis erworbenen SIM-Karten ermittelt werden können. Das Gesetz sieht insoweit zu Recht auch keinerlei Einschränkungen oder weitere Identifizierungspflichten vor, wenn der Erstinhaber einer SIM-Karte diese an Dritte weitergibt.

Die von Seiten der Sicherheitsbehörden bis zum Jahr 2004 immer wieder geschilderten Schwierigkeiten bei der Ermittlung von Anschlussinhabern konnten offenbar auch nicht dadurch gelöst werden, dass in der Praxis die Anbieter bereits seit 1997 verpflichtet waren, die Kundendaten auch von Prepaid-Kunden unter Vorlage amtlicher Ausweise nach den Leitlinien der damaligen Regulierungsbehörde zu erheben. Dieses rechtswidrige Verfahren wurde bis zur Rechtskraft eines Urteils des BVerwG vom 22. Oktober 2003 (BVerwGE 119, 123) unverändert beibehalten, da die genannten Leitlinien auch im Verfahren des vorläufigen Rechtsschutzes während des gesamten gerichtlichen Verfahrens sofort vollziehbar blieben. Trotz dieser über sechs Jahre formal bestehenden rechtlichen Verpflichtung gab es offenbar keinen Sicherheitsgewinn für die berechtigten Stellen.

Unabhängig davon werden in einer Reihe von Staaten solche Daten nicht zwangsweise erhoben. Somit wird für Straftäter auch weiterhin die einfache Möglichkeit bestehen, SIM-Karten auf Prepaid-Basis in anderen Staaten anonym zu erwerben und im Rahmen des Roamings in Deutschland zu nutzen.

Weder aus der Begründung noch aus früheren Dokumenten ist zudem ersichtlich, in welchem Umfang und Ausmaß die Verwendung anonym erworbener SIM-Karten tatsächlich die Ermittlungstätigkeit erschwert hat. So wurden zwar gelegentlich Fallgruppen genannt, in denen es zu einer Erschwerung der Ermittlungstätigkeit kommen kann, es finden sich aber keine Belege dafür, ob diese Fälle tatsächlich eine Qualität und Quantität annehmen, dass von einer Erschwerung der Ermittlungen überhaupt gesprochen werden kann. Es ist nach wie vor keine eingehende Untersuchung oder Evaluierung bekannt, ob und in welchem Umfang der Identifikationszwang geeignet ist, die Ermittlungstätigkeit nennenswert zu erleichtern.

Insofern ist kein wesentlich anderer Sachstand zu verzeichnen, als derjenige, der einer Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 24. Mai 2002 zugrunde lag. Die dort aufgestellten Forderungen sind nach wie vor aktuell (Entschließung „Geplanter Identifikationszwang in der Telekommunikation“ vom 24. Mai 2002 ([http://www.lida.brandenburg.de/sixcms/detail.php?gsid=5lbn1.c.79792.de&template=lda\\_entschl](http://www.lida.brandenburg.de/sixcms/detail.php?gsid=5lbn1.c.79792.de&template=lda_entschl))).

Das Recht jedes Einzelnen auf anonyme Kommunikation wird durch die Verpflichtung zur Bestandsdatenerfassung und -speicherung für die Sicherheitsbehörden in hohem Maße beschnitten. Die Möglichkeit, anonym zu kommunizieren, verschwindet gleichsam mit dem Angebot an öffentlichen Telefonzellen.

Die in § 111 Abs. 1 Satz 4 TKG vorgesehene Löschungsfrist von in der Praxis bis zu zwei Jahren nach Vertragsende verstärkt die Zweifel an der Verhältnismäßigkeit des § 111 TKG noch. Die Gesetzesbegründung führt hierzu lediglich aus, dass die Strafverfolgungsbehörden „nicht selten“ vor der Situation stünden, dass Bestandsdaten nach Vertragsende nicht mehr vorhanden seien. Weder wird dies quantitativ belegt, noch kann der qualitative Gehalt dieser Aussage wegen ihrer Allgemeinheit überprüft werden. Auch wird nicht belegt, dass die Länge der Frist den Erfordernissen der berechtigten Stellen angemessen Rechnung trägt oder ob eine wesentlich kürzere Frist hierfür auch ausreichen würde.

Selbst wenn die Erhebungs- und Speicherpflicht in Einzelfällen geeignet sein sollte, die Ermittlungen der Sicherheitsbehörden zu erleichtern, so ist sie im Rahmen dieser Zweckbestimmung jedenfalls weder erforderlich noch verhältnismäßig.

#### cc.Vorratsdatenspeicherung

Die Erhebungs- und Speicherpflicht führt dazu, dass eine Reihe von Daten gespeichert werden, die weder für die Durchführung eines Vertragsverhältnisses i. S. v. § 95 TKG noch für die in § 111 TKG genannten Zwecke selbst erforderlich sind. Die ganz überwiegende Zahl der Nutzer von Telekommunikation verhält sich rechtmäßig, so dass ihre Bestandsdaten nie für die Ermittlungstätigkeit der Sicherheitsbehörden benötigt werden. Dies ist auch bei der besonders im Blickfeld befindlichen Gruppe der Nutzer von Prepaid-Angeboten, unter denen eine nicht unerhebliche Zahl Minderjähriger ist, nicht anders.

Die Datenerfassung und -speicherung gemäß § 111 TKG widerspricht deshalb den Vorgaben des Bundesverfassungsgerichts, wonach die Sammlung von Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbareren Zwecken nicht mit dem Grundgesetz zu vereinbaren ist (BVerfGE 65, 1 [46]). Zum Zeitpunkt der Erhebung der Daten nach § 111 Abs. 1 TKG steht der konkrete Zweck der Erhebung noch nicht fest. Die Zweckbestimmung in den §§ 112, 113 TKG "Erfüllung der gesetzlichen Aufgaben" (§ 112 Abs. 2 TKG) bzw. Verfolgung von Straftaten oder Ordnungswidrigkeiten, Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder die Erfüllung gesetzlicher Aufgaben bestimmter Geheimdienste (§ 113 Abs. 1 TKG) bezieht sich erst auf die spätere Nutzung der Daten im Einzelfall, nicht auf einen tatsächlichen konkreten Nutzungszweck zum Zeitpunkt der Erhebung. Die Zwecke sind viel zu unbestimmt, um bereits die Erhebung aller Bestandsdaten zu rechtfertigen. Auch hier ist zu berücksichtigen, dass die meisten Daten für die genannten Zwecke nie benötigt werden. Ein Zwang zur Angabe bestimmter personenbezogener Daten setzt voraus, dass der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmt (BVerfGE 65, 1 [46]). Diesen Anforderungen wird § 111 Abs. 1 TKG in keiner Weise gerecht, da gerade nicht präzise feststeht, ob und wofür die Daten jemals erforderlich sein werden.

Die Verfassungsmäßigkeit der Erhebung der Bestandsdaten für Auskunftersuchen der Sicherheitsbehörden nach § 111 TKG ist auch angesichts des Beschlusses des Bundesverfassungsgerichts zur Rasterfahndung vom 04.04.2006 (Az. 1 BvR 518/02) zweifelhaft. In dem Beschluss hat das Bundesverfassungsgericht ausgeführt, dass eine Rasterfahndung in das Grundrecht auf informationelle Selbstbestimmung einer Vielzahl von Grundrechtsträgern eingreift und dass ein solcher Eingriff nur bei Vorliegen einer konkreten Gefahr für ein hochrangiges Rechtsgut zulässig ist. Dieselben Grundsätze müssen für die Speicherung der Bestandsdaten nach § 111 TKG gelten. Durch die Speicherung der dort genannten Daten (Rufnummer, Name, Anschrift, Datum des Vertragsbeginns, Geburtsdatum, Anschrift des Festnetzanschlusses vor der Freischaltung, Vertragsende) wird ebenfalls in das Grundrecht auf informationelle Selbstbestimmung einer Vielzahl von Personen, nämlich jedes Kunden eines geschäftsmäßigen Erbringers von Telekommunikation, eingegriffen. Der Eingriff in das in-

informationelle Selbstbestimmungsrecht wiegt beim Auskunftersuchen bezüglich der Bestandsdaten im Vergleich zur Rasterfahndung sogar schwerer, da sich die Rasterfahndung lediglich auf die bereits für dienstliche oder betriebliche Zwecke erhobenen Daten bezieht, wohingegen die Anbieter von Telekommunikationsdiensten zur Speicherung der Bestandsdaten i. S. einer Vorratsdatenspeicherung auch dann verpflichtet sind, wenn sie für betriebliche Zwecke nicht erforderlich sind und nicht in Teilnehmerverzeichnisse aufgenommen werden. Im Gegensatz zur Rechtsprechung des Bundesverfassungsgerichts zur Rasterfahndung ist der Anspruch auf Auskunft über die Bestandsdaten jedoch nicht vom Vorliegen einer konkreten Gefahr für ein hochrangiges Rechtsgut abhängig, sondern kann im automatisierten Verfahren nach § 112 TKG von den Sicherheitsbehörden schon dann verlangt werden, wenn sie diese zur Erfüllung ihrer Aufgaben benötigen.

Die Bestandsdaten selbst sind zwar nicht vom Fernmeldegeheimnis geschützt; indirekt ist aber auch durch § 111 TKG das Fernmeldegeheimnis durchaus berührt. Hierbei kann der spätere Verwendungszweck (Abfrage der Daten nach den §§ 112, 113 TKG) nicht außer Betracht bleiben, da er in § 111 Abs. 1 Satz 1 TKG bereits für die Erhebung in Bezug genommen wird. Durch die Verpflichtung der Diensteanbieter zur Identifizierung von Telekommunikationsnutzern werden auch sämtliche unstreitig vom Fernmeldegeheimnis geschützten Verkehrsdaten direkt personenbezogen. Sie dienen gewissermaßen als Schlüssel zur Herstellung des Personenbezugs für Informationen, die dem besonderen Schutz des Fernmeldegeheimnisses unterliegen. Die Bestandsdaten haben hier den Zweck, beispielsweise bei Maßnahmen nach §§ 100g, 100h Abs. 1 Satz 2 StPO, bekannte Telekommunikationsvorgänge erst einer konkreten Person zuordnen zu können. Dieser Aspekt kann bei der Verhältnismäßigkeitsprüfung im Rahmen von Eingriffen in das Recht auf informationelle Selbstbestimmung nicht unberücksichtigt bleiben.

Im Übrigen wird auf die Berücksichtigung des Fernmeldegeheimnisses bei der Abfrage der Bestandsdaten unten im Rahmen der verfassungsrechtlichen Bewertung der §§ 112, 113 TKG (IV.2.a und V.) genauer eingegangen.

Auch wenn § 111 Abs. 1 TKG lediglich zur Erhebung bestimmter Bestandsdaten zwingt und auch nur solche Anbieter verpflichtet, die Rufnummern bereitstellen, kommt den Bestandsdaten durch die technische Entwicklung und den Wettbewerb eine immer höhere Bedeutung und Sensitivität zu. So lässt sich bereits an der Wahl eines bestimmten Anbieters ggf. ablesen, welche Vorlieben ein Nutzer bei der Kommunikation hat.

Hinzukommt, dass die Verpflichtung nach § 111 TKG für alle Anbieter gilt, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken. Sie beschränkt sich somit nicht auf Anbieter für die Öffentlichkeit, sondern bezieht sich auf jeden, der nachhaltig – auch ohne Gewinnerzielungsabsicht – Telekommunikation anbietet, § 3 Nr. 10 TKG. Damit sind auch Betreiber von Hotels, Krankenhäusern, Corporate Networks, aber auch Unternehmen und Behörden verpflichtet, wenn sie ihren Bediensteten die private Nutzung der Telekommunikation erlauben. In diesen Fällen lassen sich ebenfalls bereits durch die Identität des Anbieters weitere Rückschlüsse auf die Person des Nutzers ziehen, die ggf. eines besonderen Schutzes bedürften (z. B. die Tatsache eines Krankenhausaufenthaltes). Auch wenn diese Frage insbesondere bei der Nutzung (nach § 113 TKG) erst relevant wird, ist bereits schon eine verpflichtende Erhebung und Speicherung vor diesem Hintergrund zu sehen. Der Eingriff in das Recht auf informationelle Selbstbestimmung steht hier in keinem Verhältnis zu einem völlig ungewissen und unbestimmten möglichen Nutzen der Speicherung.

Schließlich widerspricht die Erhebungs- und Speicherungspflicht der gegenüber den Telekommunikationsanbietern bestehenden Verpflichtung nach § 3a BDSG, sich an dem Ziel von Datenvermeidung und Datensparsamkeit auszurichten. Gerade die Prepaid-Angebote waren

ein gutes praktisches Beispiel für den Einsatz datenschutzfreundlicher Technologien, da sie anonymes Kommunizieren auf unkomplizierte Weise ermöglichen. Die potentielle staatliche Überwachung aller Prepaid-Kunden konterkariert dieses Ziel völlig.

#### **IV. § 112 TKG**

§ 112 TKG regelt das automatisierte Auskunftsverfahren hinsichtlich bestimmter Bestandsdaten und steht in einem engen Zusammenhang mit der Erhebungs- und Speicherverpflichtung nach § 111 TKG. An vielen Stellen kann daher auf die obigen Ausführungen zu III. Bezug genommen werden.

§ 112 TKG verstößt in der geltenden Form gegen das durch Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG garantierte Recht auf informationelle Selbstbestimmung.

##### 1. Schutzbereich und Eingriff

Der Schutzbereich von Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG ist eröffnet; die vom Gesetzgeber vorgegebene Speicherung der Kundendateien nach § 112 Abs. 1 TKG greift in das Recht auf informationelle Selbstbestimmung ein. Insofern kann weitgehend auf die obigen Ausführungen zu § 111 TKG (III.1. und 2.) verwiesen werden. Als zusätzliche Eingriffe müssen einerseits das Bereithalten der gespeicherten Daten zum Abruf (§ 112 Abs. 1 Satz 4 Nr. 1 TKG), der Abruf unter Verwendung von unvollständigen Suchbegriffen oder mittels Ähnlichkeitsfunktion (§ 112 Abs. 1 Satz 4 Nr. 2 TKG) sowie die Auskunftsbefugnisse nach § 112 Abs. 2 TKG betrachtet werden. Hierdurch räumt der Gesetzgeber den Sicherheitsbehörden und der Bundesnetzagentur Befugnisse ein, personenbezogene Daten über die Vertragsbeziehungen der Kunden für Zwecke zu verarbeiten, die mit der Eingehung, Durchführung und Abwicklung dieser Vertragsbeziehungen in keinem Zusammenhang stehen. Insofern ist hier das Recht des Einzelnen, über Verwendung und Preisgabe seiner Daten selbst bestimmen zu können, unzweifelhaft betroffen.

Der Schutzbereich von Art. 10 GG ist auch hier nicht eröffnet, da die Abrufe der Bestandsdaten durch die berechtigten Stellen für sich genommen keinen unmittelbaren Schluss auf konkrete Kommunikationsvorgänge zulassen. Im Übrigen wird auf die obigen Ausführungen unter III.1 verwiesen.

##### 2. Verfassungsrechtliche Rechtfertigung

###### *a. Anlegen von Kundendateien und Bereithalten zum Abruf nach § 112 Abs. 1 TKG*

Die Verpflichtung, Kundendateien anzulegen, bezieht sich auf die nach § 111 TKG erhobenen Daten zuzüglich der an andere Anbieter zu vergebenden Rufnummern(kontingente) und der Portierungskennungen.

Die Vorschrift ist insoweit die logische Konsequenz der Speicherung von Daten nach § 111 TKG, die ihrerseits bereits die Zweckbestimmung des § 112 TKG u. a. in Bezug nimmt. Insofern kann hier hinsichtlich der fehlenden Geeignetheit, Erforderlichkeit und Verhältnismäßigkeit zunächst auf die dortigen Ausführungen verwiesen werden (s. o., III.2.c bb).

Das Speichern in Kundendateien und das Bereithalten zum Abruf ist insbesondere bei den Bestandsdaten unverhältnismäßig, die nach § 95 Abs. 1 TKG nicht erforderlich sind.

Zusätzlich ist zu berücksichtigen, dass sich das in § 112 Abs. 1 Satz 4 Nr. 1 TKG vorgesehene Bereithalten zum Abruf auf das durch Art. 10 GG geschützte Fernmeldegeheimnis auswirkt. Zwar eröffnet die Abfrage der Bestandsdaten für sich genommen mangels Aussage über einen konkreten Kommunikationsvorgang noch nicht den Schutzbereich von Art. 10 GG. Bei Abfragen der beschriebenen Art werden die Bestandsdaten aber den konkreten Umständen eines Telekommunikationsvorgangs zugeordnet, welcher unstreitig vom Fernmeldegeheimnis geschützt ist. Dieser Aspekt kann bei der Verhältnismäßigkeitsprüfung im Rahmen von Eingriffen in das Recht auf informationelle Selbstbestimmung nicht unberücksichtigt bleiben. Dem Recht auf informationelle Selbstbestimmung kommt auch insoweit eine Ergänzungsfunktion zu Art. 10 GG zu (vgl. auch BVerfG, Urteil vom 2. März 2006, 2 BvR 2099/04, CR 2006, 383 [386 ff.]).

#### *b. Auskünfte aus den Kundendateien nach § 112 Abs. 2 TKG*

Die derzeit bestehenden Befugnisse der Auskunftserteilung nach Abs. 2 sind unverhältnismäßig, da sie gemessen an der Zweckbestimmung der Auskünfte zu weitgehend und unbestimmt sind.

Eingriffe in das Recht auf informationelle Selbstbestimmung müssen sich möglichst präzise aus einem normklaren Gesetz ergeben und den Umfang der Verarbeitung personenbezogener Daten auf das erforderliche Minimum beschränken (BVerfGE 65, 1 [46]). Diesen Anforderungen genügt die Aufzählung der Empfänger nicht. So wird an einigen Stellen keine Begrenzung auf konkrete Zwecke vorgenommen, sodass sich die Zweckbestimmung auf die gesetzlichen Aufgaben des Empfängers beschränken. Dies ist angesichts des erheblichen Eingriffs in das Recht auf informationelle Selbstbestimmung nicht ausreichend bestimmt.

Außerdem bestehen Zweifel an der Verhältnismäßigkeit dahingehend, dass die Vorschrift keine zusätzliche Eingriffsschwelle vorsieht und nicht in irgendeiner Weise subsidiär zur Anwendung kommen soll. Es ist vielmehr möglich, die Daten für telekommunikationsfremde Zwecke jederzeit abzufragen und damit die Dateien als allgemeines Adress- und Telefonverzeichnis zu nutzen. Dies entspricht nicht der eigentlichen Intention von § 112 TKG und wird dem besonderen Charakter und der Zweckbestimmung der Bestandsdaten als Daten der Telekommunikation nicht gerecht. Im Gesetz fehlt bislang eine Regelung zur eindeutigen Zweckbestimmung und Begrenzung des Auskunftsrechts, sodass die Daten nur dann abgerufen werden dürfen, wenn sie auf andere Weise nicht ermittelt werden können.

Das Grundgesetz vermittelt den von den Abfragen betroffenen Grundrechtsträgern zudem einen Anspruch auf Kenntnis von der Verarbeitung ihrer personenbezogenen Daten. Dies ist auch durch die Art. 11 und 12 der Richtlinie 95/46/EG grundsätzlich vorgesehen. Die Verfassung gebietet es, dass zumindest eine Benachrichtigung dann stattfinden muss, wenn Datenerhebungen heimlich erfolgen und ein Auskunftsanspruch nicht eingeräumt wird (vgl. BVerfGE 100, 313 [361]).

§ 112 TKG genügt diesen Anforderungen nicht, da der Verpflichtete nach § 112 Abs. 1 Satz 6 TKG nicht einmal selbst von den Abrufen erfährt. Es reicht nicht aus, dass der Betroffene unter Umständen die Möglichkeit hat, von den berechtigten Stellen nach § 112 Abs. 2 TKG eine Auskunft zu erhalten. Angesichts der Vielzahl von Betroffenen, bei denen aus unterschiedlichen Gründen davon auszugehen ist, dass der Datenabruf durch die berechtigten Stellen keine weiteren Folgen hat, würden die Betroffenen mangels eines Bewusstseins nie von dem Eingriff erfahren können.

Das Gesetz müsste daher zur Gewährleistung eines effektiven Grundrechtsschutzes sicherstellen, dass die Betroffenen zu einem späteren Zeitpunkt durch die berechtigten Stellen zumindest benachrichtigt werden können (BVerfGE 100, 313 [361]). Hinsichtlich der praktischen Umsetzung der Benachrichtigung wird auf die Vorschläge in der Verfassungsbeschwerde (S. 84) Bezug genommen.

*c. Abfrage mittels „Jokerzeichen“ und Ähnlichenfunktion, § 112 Abs. 1 Satz 4 Nr. 2 i. V. m. § 112 Abs. 3 Satz 1 Nr. 3 TKG*

In § 112 Abs. 1 Satz 4 Nr. 2 TKG wird geregelt, dass die Abfragen der Bestandsdaten auch unter Verwendung unvollständiger Abfragedaten (sog. Joker-Abfrage) oder mittels einer Ähnlichenfunktion erfolgen können. Nähere Präzisierungen nimmt das Gesetz nicht vor; dies wird vielmehr einer Rechtsverordnung gem. § 112 Abs. 3 Satz 1 Nr. 3 TKG überlassen, die nach wie vor nicht geschaffen wurde.

Bei der Joker-Abfrage wie bei der Ähnlichenfunktion bestehen zunächst Zweifel hinsichtlich der Erforderlichkeit und Verhältnismäßigkeit des damit verbundenen Grundrechtseingriffs. Die Jokerabfrage, bei der nach Art eines "Schrotflinteneinsatzes" Daten abgerufen werden, führt in jedem Falle zu einer Übermittlung personenbezogener Daten unbeteiligter Dritter, solange sie in die gesuchte Kategorie fallen. In jedem Falle muss diese Form der Abfrage im Gesetz auf das verhältnismäßige Maß beschränkt werden. Die gleichen Bedenken richten sich gegen die Möglichkeit, beim Abruf auch phonetische Suchbegriffe verwenden zu dürfen. Auch hier sind die Möglichkeiten, dass Daten Unbeteiligter in einem unverhältnismäßig hohen Umfang mit übermittelt werden, bereits durch das Gesetz auf ein Minimum zu beschränken, was hier nicht der Fall ist. Dadurch kommt es zu einem massiven Eingriff in das informationelle Selbstbestimmungsrecht einer Vielzahl von Grundrechtsträgern, siehe auch die Entscheidung zur Rasterfahndung vom 04.04.2006 (Az.: 1 BvR 518/02).

Die Entscheidung des Gesetzgebers, die Mindestanforderungen an den Umfang der einzugebenden Daten sowie den zulässigen Umfang der zu übermittelnden Treffer (§ 112 Abs. 3 Satz 1 Nr. 3 litt. a und b TKG) einer Rechtsverordnung zu überlassen, verstößt zudem gegen das Demokratieprinzip.

Art. 20 Abs. 3 GG gebietet es nach der vom BVerfG vertretenen Wesentlichkeitstheorie, dass die Entscheidung aller grundsätzlichen Fragen, die den Bürger unmittelbar betreffen, durch den Gesetzgeber selbst zu treffen ist (vgl. BVerfGE 40, 237 [249]). Dies gilt vor allem dann, wenn nicht unerhebliche Eingriffe in die Freiheitsrechte des Einzelnen in Rede stehen. Es genügt deshalb nicht den Anforderungen an Art. 20 Abs. 3 GG, dass die wesentlichen Fragen eines Grundrechtseingriffs einer Rechtsverordnung der Exekutive überlassen werden, ohne dass der Gesetzgeber sich selbst damit auseinandergesetzt hat. Außerdem verstößt die Verordnungsermächtigung auf diese Weise gegen das Gebot der Normenklarheit bei Eingriffen in das Recht auf informationelle Selbstbestimmung (BVerfGE 65, 1 [44]).

In § 112 Abs. 1 Satz 4 Nr. 2 TKG wird lediglich die grundsätzliche Möglichkeit eröffnet, mittels Jokerzeichen bzw. einer Ähnlichenfunktion auf die Bestandsdaten zuzugreifen. Das Gesetz legt jedoch nicht fest, wie weit reichend diese Eingriffe sein dürfen. Die Frage, ob z. B. bei numerischen Begriffen (wie der Telefonnummer) ein, zwei oder drei Zeichen eines Suchbegriffs durch Jokerzeichen ersetzt werden, entscheidet darüber, ob lediglich auf 10, 100 oder 1000 Datensätze zugegriffen wird. Bei alphabetischen Begriffen wie dem Namen ist der Faktor noch höher. Dies zeigt, dass der Rechtsverordnung die Entscheidung vorbehalten bleiben soll, in welchem Umfang in die Grundrechte unbeteiligter Betroffener eingegriffen wird, deren Daten überwiegend nicht erforderlich sein werden. Damit wird dem Verord-

nungsgeber nicht nur die Entscheidung über die Ausgestaltung des Eingriffs, sondern über die Rechtmäßigkeit des Grundrechtseingriffs selbst überlassen. Diese Entscheidung ist nach hiesiger Auffassung so wesentlich für die Grundrechte der Betroffenen, dass sie durch den Gesetzgeber selbst zu treffen ist.

Anzumerken ist, dass die Befugnisse des § 112 Abs. 1 Satz 4 Nr. 2 TKG zur Zeit eigentlich nicht ausgeübt werden dürften, da die wesentlichen Rechtmäßigkeitsanforderungen wegen der nach wie vor fehlenden Verordnung nicht feststehen.

## **V. § 113 TKG**

§ 113 TKG regelt das manuelle Auskunftsverfahren über Bestandsdaten. Die Vorschrift verstößt gegen das durch Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG garantierte Grundrecht auf informationelle Selbstbestimmung.

### 1. Schutzbereich und Eingriff

Ebenso wie beim automatisierten Abrufverfahren ist auch beim manuellen Abrufverfahren unzweifelhaft der Schutzbereich von Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG eröffnet, in den durch die Befugnis zum Abruf der Daten eingegriffen wird. Auf die Ausführungen zu IV.1 wird Bezug genommen.

Es wird allerdings zu Bedenken gegeben, dass ein Eingriff in den Schutzbereich des Art. 10 GG nur dann nicht gegeben ist, wie der Anwendungsbereich von § 113 TKG nicht überdehnt wird. So sind in der Rechtsprechung Tendenzen erkennbar, dass auf der Basis von § 113 Abs. 1 Satz 1 TKG auch Auskünfte über die näheren Umstände der Telekommunikation erteilt werden, was unzweifelhaft einen Eingriff in den Schutzbereich des Art. 10 GG darstellt. So wird z. B. die Auskunftserteilung durch den Access Provider über die Identität eines Internetnutzers bei bekannter dynamischer IP-Adresse als Auskunft über Bestandsdaten im Sinne von § 113 Abs. 1 Satz 1 TKG betrachtet, obwohl es sich hier bei näherer Betrachtung zusätzlich um eine Auskunft über Verkehrsdaten handelt (vgl. Sankol, MMR 2006, 361 ff. m. w. N.). Mithilfe der dynamischen IP-Adresse muss nämlich zunächst ein konkreter Kommunikationsvorgang ermittelt werden (welcher Nutzerkennung war zu welchem Zeitpunkt wie lange die jeweilige IP-Adresse zugeordnet), bevor aus diesen Verkehrsdaten wiederum die Bestandsdaten ermittelt werden können. Dies ist allerdings eine Frage möglicherweise rechtswidriger und verfassungswidriger Gesetzesanwendung und betrifft nicht die Vereinbarkeit der Norm mit Art. 10 GG.

### 2. Verfassungsrechtliche Rechtfertigung

#### *a. Auskunftserteilung, § 113 Abs. 1 Satz 1 TKG*

Die in § 113 Abs. 1 Satz 1 TKG geregelte Befugnis zur Auskunftserteilung verstößt gegen den Grundsatz der Verhältnismäßigkeit. Die mit der Befugnis verbundenen nicht unerheblichen Eingriffe in das Recht auf informationelle Selbstbestimmung sind durch die Zweckbestimmung nicht gerechtfertigt.

Bei der Abwägung im Rahmen der Verhältnismäßigkeitsprüfung ist zum einen zu berücksichtigen, dass es sich bei den in § 113 Abs. 1 Satz 1 TKG in Bezug genommenen Daten um Bestandsdaten handelt, die in Umfang und Sensitivität deutlich über das hinausgehen, was

im Rahmen des automatisierten Abrufverfahrens nach § 112 TKG bereitgestellt bzw. nach § 111 TKG erhoben und gespeichert werden muss.

So werden durch § 113 TKG alle geschäftsmäßigen Erbringer von Telekommunikation i. S. v. § 3 Nr. 10 TKG verpflichtet. Die Vorschrift ist also weder – wie § 112 TKG – auf Anbieter von Telekommunikationsdiensten für die Öffentlichkeit noch auf solche Anbieter – wie in § 111 TKG – beschränkt, die Rufnummern vergeben. Dies bedeutet zum einen, dass die oben bei § 111 TKG erwähnten Betreiber von Nebenstellenanlagen, Corporate Networks, Hotels, Krankenhäusern usw. Auskünfte nach § 113 TKG erteilen müssen. Zum anderen verpflichtet die Vorschrift auch alle Anbieter von nicht rufnummernbezogenen Diensten, vor allem E-Mail-Anbieter oder Internet-Zugangsanbieter.

Außerdem ist der Umfang der Daten, über die nach § 113 Abs. 1 Satz 1 TKG Auskunft erteilt werden muss, wesentlich größer als bei § 112 TKG. § 113 Abs. 1 Satz 1 TKG beschränkt sich nicht nur auf die nach § 111 TKG erhobenen Daten, sondern zusätzlich auf alle nach § 95 Abs. 1 TKG erhobenen Bestandsdaten. Hierzu gehören Informationen wie besondere Tarifgestaltungen, E-Mail-Adressen, statische IP-Adressen, Nutzerkennungen usw.

Dies bedeutet, dass die Nähe zum Fernmeldegeheimnis noch einmal wesentlich größer ist als bei den nach § 111 TKG zu erhebenden und nach § 112 TKG zum Abruf bereitgehaltenen Daten. Auch hier gilt zwar, dass die Bestandsdaten für sich genommen nicht unmittelbar Auskunft über konkrete Kommunikationsvorgänge geben. Allerdings haben die Daten je nach Fallgestaltung eine erhöhte Aussagekraft über die Kommunikationsgewohnheiten und das Kommunikationsverhalten der Betroffenen.

So kann z. B. aus einem Family & Friends Tarif geschlossen werden, mit welchen Personen ein Nutzer überwiegend telefoniert. Beim Internet-Zugang dient die statische IP-Adresse ganz unmittelbar als Schlüssel zur Identifizierung und Individualisierung jedes einzelnen Nutzungsvorgangs. Sie ist in diesem Fall sowohl Verkehrs- als auch Bestandsdatum. Denkbar wäre auch, dass sich ein Nutzer eines Anbieters bedient, der besonders günstige Tarife für bestimmte Zielländer anbietet. Dann lässt sich bereits den Bestandsdaten entnehmen, in welche Länder der Betroffene kommuniziert. Diese Beispiele lassen sich beliebig erweitern.

Das BVerfG hat in seinem Urteil vom 2. März 2006 (CR 2006, 383) festgestellt, dass Daten, die zunächst vom Fernmeldegeheimnis geschützt waren und zum Zeitpunkt eines staatlichen Eingriffs bereits in der ausschließlichen Verfügungsgewalt des Betroffenen sind, auch im Rahmen des Rechts auf informationelle Selbstbestimmung als Ergänzung zum Fernmeldegeheimnis einem erhöhten Schutz unterliegen, der im Rahmen der Verhältnismäßigkeitsprüfung zu berücksichtigen ist (BVerfG, CR 2006, 383 [387 f.]). Dies muss erst recht für den vorliegenden Fall gelten, in dem es sich umgekehrt um Daten handelt, die (noch) nicht vom Fernmeldegeheimnis geschützt, aber zwingend notwendig sind, um Zugang zu den Informationen über die von Art. 10 GG geschützten näheren Umstände der Telekommunikation zu erhalten und die außerdem geeignet sind, Aussagen über das konkrete Kommunikationsverhalten zu treffen. Zudem befinden sich die Daten hier in der ausschließlichen Verfügungsgewalt des Diensteanbieters und gerade nicht in der des Betroffenen. Wie sich aus § 113 Abs. 1 Satz 4 TKG ergibt, findet die Auskunft heimlich und ohne Wissen des Betroffenen statt, sodass ihm Abrufe nicht einmal bekannt sind. Die direkte Anwendung von Art. 10 GG scheitert hier allein daran, dass die Daten keine unmittelbare Auskunft über konkrete Kommunikationsvorgänge geben.

Diesem erhöhten Schutzbedarf der Bestandsdaten wird § 113 Abs. 1 Satz 1 TKG nicht gerecht. Die hohe Aussagekraft und Sensitivität der Daten verlangt zum einen, dass Eingriffe nur dann verhältnismäßig sind, wenn sie einem legitimen Zweck dienen, der sich präzise und

konkret aus dem Gesetz ergeben muss. Da die Daten in ihrer Aussagekraft und damit Schutzbedürftigkeit inzwischen den Verkehrsdaten i. S. v. § 3 Nr. 30 TKG kaum nachstehen, sind an die Eingriffsschwelle genauso hohe Anforderungen zu stellen. Der heimliche Abruf von Bestandsdaten kann daher nur verhältnismäßig sein, wenn wichtige öffentliche Interessen dies gebieten.

Wie der Gesetzgeber dies löst, kann hier nicht vorgegeben werden. Es sollte jedoch zum einen die Eingriffsschwelle insoweit heraufgesetzt werden, dass die Daten in erster Linie zur Vorbereitung und Durchführung von Maßnahmen nach §§ 100a ff. StPO, dem G 10, den §§ 23a ff. ZFdG und den Vorschriften zur präventiven Überwachung der Telekommunikation in den Sicherheits- und Ordnungsgesetzen der Länder abgerufen werden dürfen. Dies würde einerseits die Eingriffsschwelle erheblich anheben und andererseits den Abruf auf telekommunikationsrelevante Sachverhalte beschränken.

Erforderlich wäre auch hier eine Subsidiaritätsklausel, wonach die Daten erst dann abgerufen werden dürfen, wenn sie auf andere Weise nicht erhoben werden können.

#### *b. Abruf von Daten nach § 113 Abs. 1 Satz 2 TKG*

Gegen die Befugnis, Daten abzurufen, mittels derer der Zugriff auf Endgeräte oder Speichereinrichtungen geschützt wird, bestehen ebenfalls hinsichtlich der Verhältnismäßigkeit erhebliche Bedenken.

Die Eingriffsschwelle (§§ 161, 163 StPO und die weiteren genannten Vorschriften) ist gemessen an der Grundrechtsrelevanz des Eingriffs unverhältnismäßig. Zum einen ist hier zu berücksichtigen, dass auch diese Daten wiederum einem erhöhten Schutz deshalb unterliegen, weil sie unmittelbar dazu dienen, vor dem Zugang zu solchen Daten zu schützen, die dem Fernmeldegeheimnis unterliegen. Auch hier liegt die Ergänzungsfunktion des Rechts auf informationelle Selbstbestimmung im Sinne einer Vorwirkung des Fernmeldegeheimnisses auf der Hand.

Zudem ist die Befugnis des § 113 Abs. 1 Satz 2 TKG nicht zielführend. Es ist nicht einzusehen, weshalb der Zugriff auf diese Angaben unter derart leichten Bedingungen möglich sein soll, wenn für den Zugriff auf die „dahinter“ liegenden geschützten Angaben ohnehin die Voraussetzungen der §§ 100a ff. StPO, des G 10, der §§ 23a ff. ZFdG oder der Polizeigesetze der Länder gegeben sein müssen. Eine Mitteilung dieser Daten ohne die Voraussetzungen, unter denen eine Überwachung der Inhalte oder der näheren Umstände zulässig wäre, liefe ins Leere und birgt die unübersehbare Gefahr von missbräuchlichen Eingriffen in das Fernmeldegeheimnis ohne Vorliegen der gesetzlichen Voraussetzungen, auch wenn dies durch § 113 Abs. 2 Satz 3 TKG ausdrücklich verboten wird. Im Übrigen ist zu bedenken, dass die Anbieter diese Daten in vielen Fällen aus Gründen der Datensicherheit für sie selbst verschlüsselt speichern und daher auch nicht mitteilen könnten.

Die vom Gesetzgeber in der Begründung erwünschte Klarstellung (BT-Drs. 15/2316, S. 97) könnte auch dadurch erreicht werden, dass eindeutig – z. B. in § 88 TKG – geregelt würde, dass auch diese Daten vom Fernmeldegeheimnis geschützt sind oder zumindest so behandelt werden. In diesem Falle wäre eine Mitteilung dieser Daten an Sicherheitsbehörden klar und eindeutig nur nach den für die Überwachung einschlägigen Bestimmungen (§§ 100a ff. StPO, G10 etc.) möglich.

*c. Information der betroffenen Nutzer, § 113 Abs. 1 Satz 4 TKG*

Die Vorschrift verpflichtet die Verpflichteten, auch an die Betroffenen keine Auskünfte über erfolgte Abrufe zu erteilen. Dies verstößt gegen Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG, weil effektiver Grundrechtsschutz nicht gewährt wird.

Zur Argumentation wird auf die obigen Ausführungen unter IV.2.b. am Ende Bezug genommen. Auch hier sollte nach den Vorgaben des BVerfG (BVerfGE 100, 313 [361]) eine nachträgliche Benachrichtigung vorgesehen werden.

gez.

Sven Hermerschmidt