Gutachterliche Stellungnahme

zu dem Antrag

der Fraktion der PIRATEN

im Landtag NRW

LANDTAG
NORDRHEIN-WESTFALEN
16. WAHLPERIODE
NEUDRUCK
STELLUNGNAHME
16/668
A05

Zum Schutz der Vertraulichkeit und Anonymität der Telekommunikation

- Landtags-Drucksache 16/1467 –

von Meinhard Starostik

Rechtsanwalt und vereidigter Buchprüfer

Richter am Verfassungsgerichtshof des Landes Berlin

Berlin, im April 2013

I.

Rechtsrahmen der Neuregelung der Bestandsdatenabfrage auf Bundesebene

Das Bundesverfassungsgericht hat in seiner zweiten Vorratsdatenspeicherungsentscheidung im Verfassungsbeschwerdeverfahren I BvR 1299/05 vom 24. Januar 2012 (diese und aller weiteren Entscheidungen des Bundesverfassungsgerichts ab 1998 zitiert nach: www.bundesverfassungericht.de/entscheidungen.html)

den Anlass für das nunmehr vom Bundestag beschlossene Gesetz zur Änderung des Telekommunikationsgesetzes gegeben.

Anlass zum Tätigwerden des Bundesgesetzgebers bestand, weil das Bundesverfassungsgericht zu der in § 113 Abs. 1 geregelten Auskunft über sogenannte Bestandsdaten:

1. § 113 Abs. 1 Satz 1 TKG verfassungskonform ausgelegt hat und ab dem 01.07.2013 für die Anwendung dieser Vorschrift eine qualifizierte Rechtsgrundlage für den Datenabruf verlangt,

2. ab dem 01.07.2013 die Zuordnung dynamischer IP-Adressen auf Grund der derzeitigen Fassung des § 113 Abs. 1 Satz 1 für verfassungswidrig erklärt hat,

3. § 113 Abs. 1 Satz 2 TKG mit Art. 2 Abs.1 i. V. m. Art. 1 Abs. 1 des GG für unvereinbar erklärt hat und lediglich bis zum 30.06.2013 übergangsweise unter einschränkenden Bedingungen die Fortgeltung dieser Vorschrift erlaubt hat.

§ 113 Abs. 1 TKG hat z. Z. folgende Fassung:

(1) Wer geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, hat im Einzelfall den zuständigen Stellen auf deren Verlangen unverzüglich Auskünfte über die nach den §§ 95 und 111 erhobenen Daten zu erteilen, soweit dies für die Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes oder des Militärischen Abschirmdienstes erforderlich ist. Auskünfte über Daten, mittels derer der Zugriff auf Endgeräte oder in diesen oder im Netz eingesetzte Speichereinrichtungen geschützt wird, insbesondere PIN oder PUK, hat der nach Satz 1 Verpflichtete auf Grund eines Auskunftsersuchens nach § 161 Abs. 1 Satz 1, § 163 Abs. 1 der Strafprozessordnung, der Datenerhebungsvorschriften der Polizeigesetze des Bundes oder der Länder zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung, § 8 Abs. 1 des

Bundesverfassungsschutzgesetzes, der entsprechenden Bestimmungen der Landesverfassungsschutzgesetze, § 2 Abs. 1 des BND-Gesetzes oder § 4 Abs. 1 des MAD-Gesetzes zu erteilen; an andere öffentliche oder nicht öffentliche Stellen dürfen diese Daten nicht übermittelt werden. Ein Zugriff auf Daten, die dem Fernmeldegeheimnis unterliegen, ist nur unter den Voraussetzungen der hierfür einschlägigen gesetzlichen Vorschriften zulässig. Über die Auskunftserteilung hat der Verpflichtete gegenüber seinen Kundinnen und Kunden sowie Dritten gegenüber Stillschweigen zu wahren.

Die verfassungskonforme Auslegung zu § 113 Abs. 1 Satz 1 TKG durch das Bundesverfassungsgericht lautet:

IV.

…

1. § 113 Abs. 1 TKG ist von der Gesetzgebungskompetenz des Bundes gemäß Art. 73 Abs. 1 Nr. 7 GG gedeckt, sofern er verfassungskonform ausgelegt wird.

166

Zu der aus Art. 73 Abs. 1 Nr. 7 GG kraft Sachzusammenhang folgenden Kompetenz des Bundes für datenschutzrechtliche Regelungen gehört, wie dargelegt, auch die Schaffung von Bestimmungen, mit denen die mögliche Verwendung der bei den Telekommunikationsunternehmen gespeicherten Daten für die öffentliche Aufgabenwahrnehmung festgelegt werden. Hiernach kann der Bund die Telekommunikationsdiensteanbieter berechtigen und - in Korrespondenz zu einer fachrechtlich begründeten Auskunftspflicht - auch verpflichten, für bestimmte, von ihm im Einzelnen zu regelnde Zwecke (vgl. BVerfGE 125, 260 <344 ff.>) solche Daten bei Vorliegen eines wirksamen Datenabrufs an bestimmte Behörden zu übermitteln. Demgegenüber kann die Ermächtigung zu einem solchen Datenabruf selbst nicht auf die Kompetenz für das Telekommunikationsrecht gestützt werden, sondern bedarf einer fachrechtlichen Kompetenzgrundlage.

167

Dementsprechend bedarf es - wie bei § 112 TKG - auch für ein Auskunftsverlangen gemäß § 113 Abs. 1 TKG einer eigenen fachrechtlichen Rechtsgrundlage. Anders als im Fall des § 112 TKG, durch den der Bund einer Bundesbehörde die Pflicht auferlegt, Auskunft zu erteilen, kann der Bund jedoch auf der Grundlage des Art. 73 Abs. 1 Nr. 7 GG eine Verpflichtung privater Telekommunikationsunternehmen, einem Auskunftsbegehren Folge zu leisten, nicht abschließend begründen. Vielmehr gehört eine Inpflichtnahme Privater, die diese zugleich zur Preisgabe der Daten ihrer Kunden zwingt, nicht mehr zur Bestimmung der Grenzen des Datenschutzes, sondern ist untrennbarer Bestandteil des Datenabrufs. Weil der Bund auf der Grundlage des Art. 73 Abs. 1 Nr. 7 GG nur die Öffnung der Datenbestände für die staatliche Aufgabenwahrnehmung regeln kann, nicht aber auch den Zugriff auf diese Daten selbst, muss die Inpflichtnahme der Telekommunikationsdiensteanbieter als privater Auskunftspersonen in Materien, die der Regelung der Länder vorbehalten sind, in der Abrufnorm geregelt werden. Hierfür reichen Rechtsgrundlagen nicht aus, die bloß eine schlichte Datenerhebung von frei zugänglichen Informationen erlauben, nicht aber auch selbst eine Auskunftspflicht Dritter begründen (wie etwa § 26 Polizei- und Ordnungsbehördengesetz Rheinland-Pfalz; Art. 31 des Gesetzes über die Aufgaben und Befugnisse der Bayerischen Staatlichen Polizei; § 13 Abs. 1 des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung; Art. 5 Bayerisches Verfassungsschutzgesetz; § 4 Abs. 1 Sächsisches Verfassungsschutzgesetz). Entsprechend ist § 113 Abs. 1 TKG im Lichte der Kompetenzordnung des Grundgesetzes so auszulegen, dass er für Auskunftsverlangen in Bereichen, deren Regelung dem Landesrecht vorbehalten ist, spezifische Rechtsgrundlagen der Länder voraussetzt, die eine Auskunftsverpflichtung der Telekommunikationsunternehmen eigenständig begründen.

168

2. Auch mit Rücksicht auf den Grundsatz der Normenklarheit, dem bei Eingriffen in das Recht auf informationelle Selbstbestimmung eine spezifische Funktion zukommt, ist § 113 Abs. 1 TKG so auszulegen, dass er für die Datenabfrage in Form eines unmittelbar an private Dritte gerichteten Auskunftsverlangens spezifische Rechtsgrundlagen voraussetzt, die eine Auskunftsverpflichtung der Telekommunikationsunternehmen eigenständig begründen. Damit bedarf es auch für bundesrechtliche Materien qualifizierter Abrufnormen, die über eine schlichte Datenerhebungsbefugnis hinausgehen.

169

a) Ermächtigt eine gesetzliche Regelung zu einem Eingriff in das Recht auf informationelle Selbstbestimmung, so hat das Gebot der Bestimmtheit und Klarheit auch die spezifische Funktion, eine hinreichend präzise Umgrenzung des Verwendungszwecks der betroffenen Informationen sicherzustellen. Auf diese Weise wird das verfassungsrechtliche Gebot der Zweckbindung der erhobenen Information verstärkt (vgl. BVerfGE 118, 168 <187>; 120, 378 <408>). Anlass, Zweck und Umfang des jeweiligen Eingriffs sind dabei durch den Gesetzgeber bereichsspezifisch, präzise und normenklar festzulegen (vgl. BVerfGE 100, 313 <359 f., 372>; 13, 348 <375>; 125, 260 <328>; stRspr). Bei gestuften oder in verschiedene Eingriffe gegliederten Formen des Informationsaustauschs erstreckt sich das Gebot der Normenklarheit auf jede dieser Stufen.

170

b) Diesen Anforderungen genügt § 113 Abs. 1 Satz 1 TKG, wenn er lediglich als Öffnungsklausel verstanden wird, die festlegt, in welchen Fällen die Telekommunikationsunternehmen zur Übermittlung der betreffenden Daten berechtigt - und bei Vorliegen eines fachrechtlich eigens begründeten, wirksamen Verlangens auch verpflichtet - sind. Die Vorschrift fasst die möglichen Zwecke einer solchen Übermittlung zwar sehr weit, aber noch hinreichend bestimmt. Als Vorschrift, die zunächst nur die möglichen Verwendungszwecke der Daten festlegt, genügt sie den verfassungsrechtlichen Bestimmtheitsanforderungen, wenn die Aufgaben, deren Wahrnehmung die Auskunftserteilung legitimieren soll, nur abstrakt umschrieben und unabhängig von konkret berechtigten Behörden genannt werden.

171

c) Demgegenüber kann § 113 Abs. 1 Satz 1 TKG nicht so verstanden werden, dass er alle Voraussetzungen für den Datenabruf bereits selbst schafft mit der Folge, dass alle Behörden allein auf der Grundlage ihrer schlichten Datenerhebungsbefugnisse im Rahmen des § 113 Abs. 1 TKG zur Auskunft berechtigt wären. Zwar steht es dem Gesetzgeber grundsätzlich frei, Übermittlungs- und Abrufsbefugnis in derselben Vorschrift zu regeln. Jedoch hat der Bundesgesetzgeber eine solche Regelung in § 113 Abs. 1 Satz 1 TKG nicht getroffen. Für Materien, deren fachrechtliche Regelung den Ländern vorbehalten ist, fehlte ihm hierfür schon die Kompetenz (siehe oben C. IV. 1.). Aber auch für Materien, für deren fachrechtliche Regelung der Bund die Gesetzgebungskompetenz hat, regelt § 113 Abs. 1 Satz 1 TKG nicht mit hinreichender Klarheit, dass die Norm insoweit als Abrufnorm zu verstehen sein soll. Vielmehr hat der Bund die Vorschrift des § 113 TKG allein auf seine Kompetenz für das Telekommunikationsrecht gestützt (BTDrucks 15/2316, S. 55), die die Schaffung einer solchen Abrufnorm, wie dargelegt, nicht trägt. Auch wird der Kreis der abrufberechtigten Behörden und damit die Reichweite der Auskunftspflichten durch eine nur aufgabenbezogene Eingrenzung nicht in ausreichend bestimmter Weise eingegrenzt. Zur Begründung von Auskunftspflichten Privater bedarf es vielmehr klarer Bestimmungen, gegenüber welchen Behörden die Anbieter konkret zur Datenübermittlung verpflichtet sein sollen. Nur dies rechtfertigt dann auch den Eingriff in das Recht auf informationelle Selbstbestimmung gegenüber den Datenbetroffenen. Eine solche Regelung treffen aber weder § 113 Abs. 1 Satz 1 TKG selbst noch die Vorschriften, die - wie etwa § 8 Abs. 1 Bundesverfassungsschutzgesetz (vgl. Droste, Handbuch des Verfassungsschutzrechts, 2007, S. 230 f.) oder § 21 Abs. 1 Bundespolizeigesetz - lediglich eine Datenerhebungsbefugnis ohne ausdrückliche Auskunftsverpflichtung gegenüber Dritten enthalten.

172

3. § 113 Abs. 1 Satz 1 TKG bedarf weiterhin der verfassungskonformen Auslegung dahin, dass in ihm keine Rechtsgrundlage für die Zuordnung von dynamischen IP-Adressen gesehen werden kann.

173

Ein Rückgriff auf § 113 Abs. 1 Satz 1 TKG zur Identifizierung von dynamischen IP-Adressen verbietet sich schon deshalb, weil diese als Eingriff in Art. 10 Abs. 1 GG zu qualifizieren ist (siehe oben C. I. 1. a) cc). Für solche Eingriffe gilt das Zitiergebot gemäß Art. 19 Abs. 1 Satz 2 GG, wonach der Gesetzgeber das Grundrecht, in das eingegriffen wird, unter Angabe des Artikels nennen muss. Daran fehlt es vorliegend.

174

Im Übrigen scheidet eine Identifizierung dynamischer IP-Adressen auf der Grundlage von § 113 Abs. 1 Satz 1 TKG aber auch deshalb aus, weil dieser eine solche Befugnis nicht hinreichend normenklar regelt. Die Identifizierung von dynamischen IP-Adressen ermöglicht in weitem Umfang eine Deanonymisierung von Kommunikationsvorgängen im Internet. Zwar hat sie eine gewisse Ähnlichkeit mit der Identifizierung einer Telefonnummer. Schon vom Umfang, vor allem aber vom Inhalt der Kontakte her, über die sie Auskunft geben kann, hat sie jedoch eine erheblich größere Persönlichkeitsrelevanz und kann mit ihr nicht gleichgesetzt werden (vgl. BVerfGE 125, 260 <341 ff.>).

Insoweit bedarf es einer hinreichend klaren Entscheidung des Gesetzgebers, ob und unter welchen Voraussetzungen eine solche Identifizierung erlaubt werden soll. Eine solche Entscheidung lässt sich § 113 Abs. 1 Satz 1 TKG jedoch nicht mit hinreichender Deutlichkeit entnehmen. Ausdrücklich verhält sich die Vorschrift zu dieser Frage nicht. Auch im Wege der Auslegung lässt sich § 113 Abs. 1 Satz 1 TKG keine hinreichend klare Aussage entnehmen. § 113 Abs. 1 Satz 1 TKG nennt allein § 95 und § 111 TKG als Gegenstand der Auskunftspflicht, lässt aber nicht erkennen, dass die Telekommunikationsunternehmen in Vorbereitung solcher Auskünfte darüber hinaus auch die Verkehrsdaten nach § 96 TKG auszuwerten berechtigt und verpflichtet sein könnten; die abschließende Formulierung der Verwendungszwecke bezüglich der Verkehrsdaten in § 96 TKG spricht hierfür jedenfalls nicht. Dementsprechend ist die Frage auch in Rechtsprechung und Literatur seit langem umstritten (siehe oben A. I. 3.). Eine hinreichend normenklare Befugnis zur Identifizierung auch von dynamischen IP-Adressen liegt somit in § 113 Abs. 1 TKG nicht.

…

I. 1.

Gesetzgeberischer Regelungsgegenstand des § 113 Abs. 1 TKG

Nach der vom Bundestag in der Sitzung vom 21.03.2013 in zweiter und dritter Lesung beschlossenen Fassung des § 113 Abs. 1 TKG (vgl. BT-Drucksachen 17/12043 und 17/12879) darf im manuellen Auskunftsverfahren von geschäftsmäßigen Anbietern von Telekommunikationsdiensten bzw. denjenigen, die daran mitwirken, Auskunft über die nach § 95 und 111 erhobenen Daten erteilt werden.

Dies gilt auch für Zugriffsschutzdaten (PIN und PUK).

Die Bestandsdaten dürfen auch anhand einer zu bestimmt**en** Zeitpunkt**en** zugewiesen Internetprotokolladresse bestimmt werden. Hierbei dürfen Verkehrsdaten sowohl manuell als auch automatisiert ausgewertet werden.

Zu den Daten, über die Auskunft erteilt wird, gehören nach § 95 TKG alle Daten, die gem. § 3 Nr. 3 TKG:

> „für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste…“

erhoben werden.

Dieser Datenbestand ist wesentlich umfangreicher, als diejenigen Daten, die nach § 111 Abs. 1 TKG erhoben werden müssen.

Auskunft darf nach § 111 Abs. 1 TKG im Einzelnen über folgende Daten erteilt werden:

1. die Rufnummern und anderen Anschlusskennungen,
2. den Namen und die Anschrift des Anschlussinhabers,
3. bei natürlichen Personen deren Geburtsdatum,
4. bei Festnetzanschlüssen auch die Anschrift des Anschlusses,
5. in Fällen, in denen neben einem Mobilfunkanschluss auch ein Mobilfunkendgerät überlassen wird, die Gerätenummer dieses Gerätes sowie
6. das Datum des Vertragsbeginns

I.2.

Verfassungsrechtliche Einordnung der zu erhebenden Daten und der Datenzugriffsbefugnis in § 113 TKG durch das Bundesverfassungsgericht:

I.2.1.

Kompetenzrechtliche Einordnung

Verfassungsrechtliche Ermächtigungsnorm für die Regelung in § 113 TKG ist Art. 73 Abs. 1 Nr. 7 GG, der Kraft Sachzusammenhangs den Bund auch ermächtigt, Datenschutzregelungen für die bei Telekommunikationsunternehmen gespeicherten Daten und Verwendungsbestimmungen für die Auskunft über solche Daten zu treffen. Diese Kompetenz betrifft allerdings nur die Öffnung der Datenbestände für eine Anfrage einer öffentlichen Stelle und nur zu bestimmten Zwecken. Die Abrufberechtigung der öffentlichen Stelle ist in einer weiteren Ermächtigungsgrundlage - die ggfls. auf Landesrecht beruht - zu regeln. Dies ist das Doppeltürenmodell des Bundesverfassungsgerichts. (vgl. BVerfG Beschluss vom 24.01.2012, Rz 164, 170f.) Wegen der weiteren Einzelheiten verweise ich zur Vermeidung von Wiederholungen auf das Gutachten Buermeyer.

I.2.2.

Grundrechtliche Einordnung der Bestandsdaten:

Bestandsdaten fallen unter den Schutz des Grundrechts auf informationelle Selbstbestimmung, Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG. Der in § 113 Abs. 1 TKG geregelte Eingriff in dieses Grundrecht bedarf einer besonderen Zweckbindung, die Anlass, Zweck und Umfang des jeweiligen Eingriffs durch ein formelles Gesetz bereichsspezifisch, präzise und normenklar festlegt. (vgl. BVerfG aaO, Rz 169 mit den dortigen Nachweisen)

Die sehr weite Fassung der Zweckbindung in § 113 Abs. 1 TKG hat das Bundesverfassungsgericht für ausreichend gehalten, weil die Vorschrift nur der Öffnung der Datenbestände dient und auf der Stufe der Auskunftsermächtigung

nochmals eine Zweckbindung zu erfolgen hat. (vgl. BVerfG aaO, Rz 170f. ,176 mit den dortigen Nachweisen)

I.2.3

Einordnung der dynamischen IP-Adressen

Obwohl dynamisch zugeordnete IP-Adressen, der Standardfall bei DSL-Anschlüssen, nur zur Auskunft über den Anschlussinhaber verwendet werden, hat das Bundesverfassungsgericht dieses Auskunftsverfahren dem Schutzbereich des Art. 10 Abs. 1 GG zugeordnet. Dies beruht darauf, dass der Inhaber eines Internetanschlusses anhand der zu bestimmten Zeitpunkten zugewiesenen IP-Adresse vom Telekommunikationsanbieter retrograd nur unter Zugriff auf die nach § 96 TKG gespeicherten Verkehrsdaten ermittelt werden kann. Diese Verkehrsdaten geben unmittelbar Aufschluss über die Kommunikation, die über einen bestimmten Internetanschluss erfolgte. Zum Schutzbereich des Art. 10 Abs. 1 GG gehören der Inhalt und die näheren Umstände der Fernkommunikation. Zweck des Grundrechtes ist der Schutz der Vertraulichkeit der Kommunikation durch Brief, Telefon und Internet. Diese Kommunikation soll ohne unbefugte Beobachtung durch die öffentliche Gewalt genauso unbefangen erfolgen, als ob die Kommunikationsteilnehmer persönlich anwesend und unbeobachtet wären. (vgl. BVerfG Urteil vom 02.03.2010 - 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 - Rz 189f. mit weiteren Nachweisen)

§ 113 Abs. 1 Satz 1 TKG darf bereits deshalb nicht zur Auskunft über Bestandsdaten anhand der Kenntnis einer dynamischen IP-Adresse verwendet werden, weil er gegen das Zitiergebot des Art. 19 Abs. 1 Satz 2 GG verstößt.

Darüber hinaus hat die dynamische IP-Adresse eine größere Persönlichkeitsrelevanz als die Bestanddaten, denn Sie gibt unmittelbar Auskunft über das Kommunikationsverhalten des beteiligten Internetnutzers. Insofern genügt die geltende Fassung des § 113 Abs. 1 Satz 1 TKG nicht dem Bestimmtheitserfordernis. (vgl. BVerfG Beschluss vom 24.01.2012, Rz 174 : „Insoweit bedarf es einer hinreichend klaren Entscheidung des Gesetzgebers, ob und unter welchen Voraussetzungen eine solche Identifizierung erlaubt werden soll.“)

I.2.4.

Einordnung der statischen IP-Adressen

Statische IP-Adressen ordnet das Bundesverfassungsgericht den Bestandsdaten zu. Sie haben nicht am Schutz des Grundrechts aus Art. 10 Abs. 1 GG teil. Maßgebend hierfür war die Überlegung, dass eine statische IP-Adresse ohne Rückgriff auf Verkehrsdaten einem Anschlussinhaber zugeordnet werden kann, ferner die Tatsache, dass statische IP-Adressen derzeit hauptsächlich nur Institutionen und Großnutzern zugeteilt werden. Die Auskunft über eine solchen Anschluss hat wenig Persönlichkeitsbezug. (vgl. BVerfG Beschluss vom 24.01.2012, Rz 160f.)

Allerdings hat das Bundesverfassungsgericht dem Gesetzgeber eine Beobachtungspflicht auferlegt, weil die Eingriffstiefe einer Auskunft über eine

statische IP-Adresse sich sowohl mit der weiteren Verbreitung bei Privatnutzern als auch mit der Rückverfolgbarkeit der Internetnutzung bis zum Endgerät bei Einführung von IPV 6 qualitativ ändern kann. (BVerfG aaO, Rz 161)

I.2.5.

Richtervorbehalt bei Auskünften

Im Urteil zur Vorratsdatenspeicherung hat das Bundesverfassungsgericht die Erlaubnis zur Auskunft über die nach § 113a TKG gespeicherten Telekommunikationsdaten (Vorratsdaten) wegen des damit verbundenen schwerwiegenden Grundrechtseingriffs grundsätzlich unter Richtervorbehalt gestellt, nicht hingegen die Auskunft über den Anschlussinhaber einer IP-Adresse (vgl. BVerfG Urteil vom 02.03.2010, Rz 247 - 249, 261)

Maßgeblich war für das Bundesverfassungsgericht im Urteil zur Vorratsdatenspeicherung, dass die Auskunft über den Anschlussinhaber einer IP-Adresse in gewisser Weise der Auskunft über eine Telefonnummer gleicht und die Behörden selbst keine Kenntnis der zugrundeliegenden Verkehrsdaten erhielten. (BVerfG aaO, Rz 256f.)

Das Gericht maß dem durch eine solche Auskunft vorliegenden Grundrechtseingriff allerdings eine größere Eingriffstiefe zu, als der Auskunft über den Inhaber einer Telefonnummer. Zur Begründung verwies es auf die mittelbare Möglichkeit, über die IP-Adresse das Kommunikationsverhalten des Adresseninhabers zu erforschen, indem die IP-Adresse beim Besuch von Webseiten gespeichert wird. Solche **mittelbaren** Kenntnisse vom Kommunikationsverhalten unterliegen allerdings nicht dem Grundrechtsschutz des Art. 10 Absatz 1 GG. (vgl. BVerfG Beschluss vom 24.01.2012, Rz 113 - 116) Somit sah das Gericht in der Auskunft über den Inhaber einer IP-Adresse aufgrund von Vorratsdaten einen Grundrechtseingriff mittlerer Schwere, schützenswerter als die bloße Auskunft über den Inhaber einer Telefonnummer, weniger schützenswert aber als die Auskunft über detaillierte Telefonverbindungsdaten. (vgl. BVerfG Urteil vom 02.03.2010, Rz 256 - 262)

Dementsprechend definierte das Bundesverfassungsgericht -bezogen auf Vorratsdaten- folgende tatbestandliche Voraussetzungen für eine verfassungskonforme Regelung zur Auskunftserteilung über den Inhaber einer dynamisch zugewiesenen IP-Adresse:

1. Verfolgung von Straftaten, Gefahrenabwehr und Aufgabenwahrnehmung der Nachrichtendienste
2. Hinreichender Anfangsverdacht oder eine auf tatsächliche Anhaltspunkte gestützte konkrete Gefahr
3. Bei der Verfolgung oder Verhinderung von Ordnungswidrigkeiten muss es sich um eine - auch im Einzelfall - besonders gewichtige Ordnungswidrigkeit handeln, die der Gesetzgeber ausdrücklich benennen muss
4. Die rechtlichen und tatsächlichen Grundlagen des Auskunftsbegehrens sind aktenkundig zu machen.

(vgl. BVerfG aaO, Rz 261f.)

Anders dagegen wertet der Beschluss vom 24.01.2012 im Verfahren 1 BvR 1299/05 nunmehr auch den Rückgriff des Telekommunikationsanbieters auf Verkehrsdaten als unmittelbaren Eingriff in das Grundrecht aus Art. 10 Abs. 1 GG in Abgrenzung zur lediglich mittelbaren Kenntnis vom Kommunikationsverhalten eines Internetnutzers durch die Behörden (vgl. BVerfG Beschluss vom 24.01.2012, Rz 113 - 116). Dieser Änderung in der Rechtsprechung des Bundesverfassungsgerichts könnte wesentliche Bedeutung bei der Beurteilung der Eingriffstiefe der Auskunft über die Person eines Internetanschlussinhabers zukommen.

I.2.6.

Schutzwirkung des Richtervorbehaltes

Ein Rechtsschutzverfahren zur - zumindest nachträglichen - Kontrolle der Verwendung der Daten ist von Verfassung wegen geboten. (BVerfG Urteil vom 02.03.2010, Rz 251).

Das Bundesverfassungsgericht maß dem Richtervorbehalt erhebliche Schutzwirkung aus drei Gründen zu:

1. Die abzufragenden Daten sind hinreichend substantiiert zu begründen und zu begrenzen
2. Das Gericht prüft daraufhin die Eingriffsvoraussetzungen, insbesondere die gesetzlich vorgeschriebene Eingriffsschwelle
3. Der Anordnungsbeschluss des Gerichts wird gehaltvoll begründet

(vgl. vgl. BVerfG aaO, Rz 249)

Für das Verfahren nach §§ 112, 113 TKG soll dagegen ein besonderes Rechtsschutzverfahren nicht erforderlich sein, vielmehr die allgemeinen Rechtsschutzmöglichkeiten ausreichen (vgl. BVerfG Beschluss vom 24.01.2012, Rz 186). Unklar bleibt, ob sich dies auch auf die Inhaber von IP-Adressen bezieht, da die Auskünfte hierüber gerade nicht mehr zulässig sein sollen (vgl. BVerfG Beschluss vom 24.01.2012, Nummer 2 des Entscheidungstenors)

I.2.7

Transparenzgebot

Nachträglicher Rechtsschutz setzt die Benachrichtigung des Betroffenen voraus; zumindest als Regelfall (vgl. BVerfG Urteil vom 02.03.2010, Rz 243 - 245).

Grundsätzlich entfällt die Benachrichtigungspflicht auch nicht bei der Ermittlung des Inhabers einer IP-Adresse (vgl. BVerfG aaO, Rz 263)

Die vorstehenden Erwägungen bezogen sich auf die Speicherung und Auskunft nach §§ 113a und b TKG. Für die Auskunft nach §§ 112 und 113 TKG hat das Bundesverfassungsgericht ein „flächendeckendes Erfordernis zur Benachrichtigung der von der Auskunft Betroffenen“ (vgl. BVerfG Beschluss vom 24.01.2012, Rz 187)

nicht für erforderlich gehalten. Ausdrücklich offengelassen, weil nicht entscheidungserheblich, blieb die Frage, in welchen Fällen eine Benachrichtigungspflicht oder der Vorrang der Datenerhebung beim Betroffenen geboten sein kann und in der Abrufnorm zu regeln ist.

I.2.8.

Datensicherheit

Bezüglich der nach § 113a TKG zu speichernden Daten hat das Bundesverfassungsgericht erhebliche Sicherheitsanforderungen sowohl für die Speicherung als auch für den Datenzugriff aufgestellt. (vgl. BVerfG Urteil vom 02.03.2010, Rz 220 - 225)

In der Entscheidung zu §§ 111 bis 113 TKG ist offengelassen, welche Sicherheitsanforderungen für die Datenspeicherung und -übermittlung in diesem Zusammenhang aufzustellen sind, da dies mit der Verfassungsbeschwerde nicht gerügt worden war. (vgl. BVerfG Beschluss vom 24.01.2012, Rz 186) Man wird allerdings zumindest für die digitale Datenübermittlung die Sicherheitsanforderungen aus dem Urteil zur Vorratsdatenspeicherung annehmen müssen, wozu nach dem Stand der Technik auch eine entsprechende Datenverschlüsselung gehören dürfte. (vgl. BVerfG Urteil vom 02.03.2010, Rz 220 - 225)

Auch dürfte die Nämlichkeit des jeweils Abfragenden sicherzustellen sein, indem durch verfahrenstechnische Vorkehrungen sichergestellt ist, dass die anfragende Stelle sich auf eine sichere Weise identifiziert. Da die neue Fassung des Gesetzes in § 113 Abs. 2 Satz 1 lediglich die Textform für eine Abfrage verlangt (also auch per Email), dürfte dieser Sicherheitsanforderung nicht genüge getan sein. Eine Abfrage per Email kann leicht von einer gefälschten Absenderadresse versendet werden, wie allgemein bekannt ist. **Das Gesetz öffnet hier für unberechtigte Abfragen eine große Sicherheitslücke.**

Zusammenfassung:

Die Erarbeitung der jeweiligen verfassungsrechtlichen Grenzen der Zulässigkeit von Abfragen nach § 113 TKG ist außerordentlich kompliziert, wie der Vergleich der beiden Entscheidungen des Bundesverfassungsgerichts zur Bewertung der Auskunft über die Inhaber von IP-Adressen zeigt, vgl. oben 1.2.3 bis 1.2.7 . Die scharfsinnigen Abgrenzungen des Verfassungsgerichts zwischen den einzelnen Eingriffsvoraussetzungen und -schwellen, müssen vom Gesetzgeber in eine für die Alltagspraxis der abfragenden Behörden eindeutig anwendbaren gesetzlichen Regelung eingearbeitet werden. Soll der Grundrechtsschutz der Bürger gewahrt bleiben, so sind enge Grenzen zu setzen, denn es liegt in der Natur der Tätigkeit von Ermittlungsbehörden, die gesetzten Grenzen „auszureizen“ und möglichst weit auszunutzen, denn der Ermittler will und soll Erfolg haben. Dabei ist tendenziell der Grundrechtsschutz stets gefährdet.

II.

Zu den Gliederungspunkten des Antrages der Fraktion der Piraten:

1. **durch ein einfachgesetzliches Zitiergebot Klarheit darüber hergestellt wird, welche Gesetze einen staatlichen Zugriff auf Kommunikationsdaten erlauben sollen und welche nicht,**

Mit dieser Forderung wird das Gebot der Bestimmtheit und der Zweckbindung der Daten auf eindeutige Weise erfüllt. Das Bundesverfassungsgericht hat im Beschluss vom 24.01.2012, dort Rz 158, für die Verhältnismäßigkeit des automatisierten Datenabrufs nach § 112 TKG die enumerative Aufzählung der berechtigten Behörden als wichtiges Abwägungskriterium herangezogen, hingegen die lediglich aufgabenbezogene Benennung der berechtigten Behörden für nicht ausreichend gehalten, um eine Abrufermächtigung gegenüber den Telekommunikationsunternehmen zu schaffen. Dazu bedarf es weiterhin bereichsspezifischer Ermächtigungsgrundlagen. (vgl. BVerfG aaO, Rz 171).

Aus verfassungsrechtlicher Sicht spricht nichts dagegen, bereits in der Datenöffnungsnorm den Kreis der zum Abruf berechtigten Stellen einzugrenzen. Da der Bundesgesetzgeber die Öffnungskompetenz für die Datenbestände hat, vgl. oben 1.2.1 kann er selbst begrenzen, gegenüber wem er den Datenabruf ermöglicht. Aus Sicht des Grundrechtsschutzes wäre eine solche Regelung zu begrüßen.

2. **für die Auslieferung von Telekommunikations-Bestandsdaten (§ 113 Absatz 1 Satz 1 TKG) an Staatsbehörden mindestens dieselben verfahrensrechtlichen und inhaltlichen Voraussetzungen eingeführt werden wie für die Auslieferung von Telekommunikations-Verkehrsdaten (z.B. Richtervorbehalt, Eingriffsschwellen),**

Wie oben unter 1.2.3 bis 1.2.7 dargestellt bereitet die Einordnung des Eingriffsgewichts bei der Auskunft über IP-Adressen besondere Schwierigkeiten. Bereits aus diesem Grunde wäre eine vereinfachende Regelung, die bei allen Bestandsdatenabfragen nach § 113 TKG gleiche Zugriffsschwellen wie bei der Verkehrsdatenabfrage einführt, außerordentlich praxistauglich. Sie setzt die abfragende Behörde nicht dem Vorwurf aus, eigenmächtig oder willkürlich die Grenzen der eigenen Kompetenz überschritten zu haben und führt einen angemessenen Grundrechtsschutz für die Bürger ein. Dies ist auch deshalb angezeigt, weil, anders als im für die Behörden unkomplizierten Verfahren nach § 112 TKG, Daten in erheblichem Umfang abgefragt werden können, insbesondere auch Bankverbindungsdaten, das Kundenkennwort (neben PIN und PUK) und weitere kundenbezogene Daten, die nicht unter den

schlichten Katalog des § 111 TKG, vgl. oben I.1, fallen. Das Bundesverfassungsgericht hat die Verhältnismäßigkeit der Auskunft über diese weiteren Bestandsdaten, die nach § 95 TKG gespeichert worden sind, nicht abschließend geprüft, da dies nicht entscheidungserheblich war (vgl. BVerfG aaO, RZ 179). Gerade im Hinblick hierauf würde die vorgeschlagene Regelung den Grundrechtsschutz der Bürger verstärken und den abfragenden Behörden keinen unzumutbaren Mehraufwand aufbürden, denn Sinn und Zweck der Regelungen zum manuellen Auskunftsverfahren ist es auch, durch einen gewissen Verfahrensaufwand zu sichern, dass die Behörde die Daten nur bei entsprechendem Bedarf abfragt (vgl. BVerfG aaO, RZ 178). Die vorgeschlagenen einengenden Voraussetzungen sorgten so für Grundrechtsschutz durch Verfahrensgestaltung, ohne die Ermittlungsbefugnisse der Behörden messbar einzuschränken.

3. **die Auslieferung von Bestandsdaten (§ 113 Absatz 1 Satz 1 TKG) gesetzlich ausdrücklich auf Einzelfälle beschränkt bleibt und die Einführung einer elektronischen Auskunftsschnittstelle unterbleibt,**

Diese Forderung dürfte der vom Bundesverfassungsgericht vorausgesetzten Ausübungsschranke bei der Einholung von Auskünften (durch den damit verbundenen Arbeitsaufwand) gerecht werden (vgl. BVerfG ebenda). Die elektronische Auskunftsschnittstelle gleicht das manuelle Auskunftsverfahren praktisch dem automatisierten Verfahren an. Dies dürfte unter Verhältnismäßigkeitsgesichtspunkten bedenklich sein.

4. **eindeutig und restriktiv gesetzlich geregelt wird, unter welchen verfahrens-rechtlichen und inhaltlichen Voraussetzungen Zugangssicherungscodes (wie Passwörter, PIN oder PUK), die den Zugang zu Endgeräten (z.B. Mobiltelefonen) und Speicherungseinrichtungen (z.B. E-Mail-Postfächer) sichern, gegenüber Staatsbehörden preiszugeben sind und deren Nutzung zugelassen wird,**

Die Verhältnismäßigkeit der Datenöffnungsbefugnis, wenn eine der berechtigten Stellen dies „…unter Angabe einer gesetzlichen Bestimmung verlangt, die ihr eine Erhebung … der Daten erlaubt (vgl. die Gesetzesfassung in der Form des Änderungsantrages des Innenausschusses, BT-Drucksache 17/12879) erscheint mir fraglich. Das Gesetz verlangt nicht das konkrete Vorliegen der tatbestandlichen Voraussetzungen für eine Datenabfrage, sondern eine Bezugnahme der Behörde („Angabe“) auf eine mögliche Ermächtigungsnorm. Diese Regelung ist ausgesprochen fehleranfällig und stellt nicht hinreichend sicher, dass die Daten für die effektive Aufgabenwahrnehmung der Behörden erforderlich sind.

Hierbei ist auch zu berücksichtigen, dass in dem sich rasant verändernden Telekommunikationsmarkt seit dem Beschluss des Bundesverfassungsgerichts vom 24.01.2012 weitere Verlagerungen des Telekommunikationsverhaltens der Nutzer stattgefunden haben. Ich verweise insofern auf die zunehmende Bedeutung von Chats in sozialen Netzwerken und die Verknüpfung des IP-Telefoniedienstes SKYPE mit FACEBOOK. Der Anbieter SKYPE erbringt zweifellos geschäftsmäßig Telekommunikationsdienstleistungen. Da Skype-Nutzer sich auch über Ihren Facebook-Account einloggen können, dürfte Facebook an dieser geschäftsmäßigen Erbringung von Telekommunikationsdienstleistungen mitwirken,

vgl. § 113 Abs. 1 Satz 1 TKG und wäre somit auskunftspflichtig, auch hinsichtlich der Zugangscodes.

5. **der Vorrang der Telekommunikationsüberwachung unter Mitwirkung des Anbieters vor dem unmittelbaren Zugriff mithilfe von Zugangssicherungscodes festgeschrieben wird,**

Diese Forderung schränkt nach dem Grundsatz der Verhältnismäßigkeit den Zugriff auf die Telekommunikation auf das mildere, gleichgeeignete Mittel ein. Verfassungsrechtlich dient dies der Klarstellung dessen, was für die Verwaltungspraxis ohnehin gefordert werden, in der Hektik des Ermittlungsalltags aber leicht übersehen werden kann. Insofern erhalten die abfragenden Stellen eine eindeutige gesetzliche Leitlinie für ihr Handeln,

6. **die Herausgabe von Zugangssicherungscodes an unberechtigte Behörden oder Dritte bußgeldbewehrt verboten bleibt,**

Dies ist in der Ausschussfassung als § 149 Abs. 1 Nr. 33 TKG eingefügt worden, vgl. BT-Drucksache 17/12879.

7. **festgelegt wird, dass Anbieter Auskünfte ausschließlich anhand rechtmäßig gespeicherter Kommunikationsdaten erteilen dürfen,**

Diese Forderung führt praktisch zu einem Beweiserhebungsverbot für unrechtmäßig gespeicherte Daten. Die Anbieter erheben in großem Umfang Kommunikationsdaten, wobei fraglich ist, ob diese in dem Umfang und in dem zeitlichen Rahmen gespeichert werden dürfen, wie dies in der Praxis geschieht. Es entspricht einem verfassungskonformen Beweiserhebungsverfahren, dass über solche unrechtmäßig gespeicherten Daten keine Auskunft erteilt werden darf.

8. **darauf verzichtet wird, Bundeskriminalamt und Zollkriminalamt als Zentralstellen Zugriff auf Telekommunikationsdaten einzuräumen,**

Die vom Bundesgesetzgeber in Art. 4 und 5 des Gesetzes zur Änderung des Telekommunikationsgesetzes vorgesehene Abrufbefugnis des Bundeskriminalamtes und des Zollkriminalamtes als Zentralstellen ist zur Erfüllung der gesetzlichen Aufgaben dieser Behörden als Zentralstellen nicht erforderlich und daher unverhältnismäßig (vgl. zu diesem Maßstab auch: BVerfG aaO, Rz 183ff.).

9. **der Bund es dem zuständigen Fachgesetzgeber überlässt, zu regeln, in welchem Zeitrahmen und Umfang Auskünfte zu erteilen sind und ob der Anbieter seine Kunden informieren darf,**

Aus verfassungsrechtlicher Sicht bestehen keine Bedenken. Umfang der Abrufbefugnis (Zeitrahmen) und Regelung der Transparenz (Kundeninformation) können zweifelsfrei im Rahmen der Abrufnormen geklärt werden.

10. **eine Benachrichtigung der Betroffenen mindestens von Eingriffen in das Fernmeldegeheimnis (Identifizierung von Internetnutzern) und von der Auslieferung persönlicher Zugangssicherungscodes sichergestellt wird,**

Wie oben unter 1.2.5 dargelegt, dürfte das Bundesverfassungsgericht in dem Beschluss vom 24.01.2012 - 1 BvR 1299/05 - der Eingriffstiefe der IP-Adressenauskunft größere Bedeutung beigemessen haben als im Urteil zur Vorratsdatenspeicherung vom 02.03.2010 - 1 BvR 256/08 u.a. -, ohne allerdings die Voraussetzungen einer Benachrichtigungspflicht im Einzelnen festzulegen. Verfassungsrechtlich dürften keine Bedenken bestehen, die Benachrichtigungspflicht möglichst umfassend zu regeln. Der Grundrechtsschutz der Bürger würde dadurch verstärkt, ohne damit die Ermittlungstätigkeit der Behörden zu behindern.

11. **Zahl und Art der staatlichen Bestandsdatenabfragen statistisch erfasst und jährlich veröffentlicht werden,**

Der Gesetzgeber hat eine Beobachtungspflicht (vgl. BVerfG aaO, Rz 161). Die vorgeschlagene Regelung ergänzt diese Pflicht und dient der Transparenz des Verfahrens gegenüber den Grundrechtsbetroffenen (vgl. hierzu auch: BVerfG Urteil vom 02.03.2010, Rz 242).

12. **auch für staatliche Stellen eine Informationspflicht bei unrechtmäßiger Kenntniserlangung von Telekommunikationsdaten eingeführt wird.**

Diese Regelung dient sowohl der Transparenz, mindert die Furcht der Bürger vor einer ständigen Beobachtung durch den Staat und fängt die diffuse Bedrohlichkeit, die die Speicherung und Beauskunftung von Daten in diesem wichtigen Bereich hat, auf. Der Bürger weiß, dass Fehler korrigiert werden (vgl. auch: BVerfG ebenda).

Berlin, den 17.04.2013 Meinhard Starostik