DeutscherAnwaltVerein

# Stellungnahme

des Deutschen Anwaltvereins durch
den Ausschuss Gefahrenabwehrrecht

**zum Gesetzgebungsentwurf der Bundesregierung zur Neuregelung der Bestandsdatenauskunft auf Grund der Entscheidung des BVerfG vom 24.01.2012 (BT-Drucks. 17/12034 vom 09.01.2013)**

Stellungnahme Nr. 17/2013 Berlin, im März 2013

## Mitglieder des Ausschusses

- Rechtsanwältin Dr. Heide Sandkuhl, Potsdam (Vorsitzende)
- Rechtsanwalt Wilhelm Achelpöhler, Münster (Berichterstatter)
- Rechtsanwalt Prof. Dr. Matthias Dombert, Potsdam
- Rechtsanwalt Sönke Hilbrans, Berlin
- Rechtsanwalt Dr. Stefan König, Berlin
- Rechtsanwältin Dr. Regina Michalke, Frankfurt am Main (Berichterstatterin)
- Rechtsanwältin Kerstin Oetjen, Freiburg

## Zuständig in der DAV-Geschäftsführung

- Rechtsanwalt Thomas Marx

**Deutscher Anwaltverein**
Littenstraße 11, 10179 Berlin
Tel.: +49 (0)30 726152-0
Fax: +49 (0)30 726152-190
E-Mail: dav@anwaltverein.de

**Büro Brüssel**
Avenue de la Joyeuse Entrée 1
1040 Brüssel, Belgien
Tel.: +32 (0)2 28028-12
Fax: +32 (0)2 28028-13
E-Mail: bruessel@eu.anwaltverein.de
Registernummer: 87980341522-66

www.anwaltverein.de

**Verteiler**

- Bundeskanzleramt
- Bundesministerium des Innern
- Bundesministerium der Justiz

- Bundesrat
- Deutscher Bundestag - Rechtsausschuss
- Deutscher Bundestag - Innenausschuss

- Arbeitsgruppen Inneres der im Deutschen Bundestag vertretenen Parteien
- Arbeitsgruppen Recht der im Deutschen Bundestag vertretenen Parteien

- Justizministerien der Länder
- Landesministerien und Senatsverwaltungen des Innern
- Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
- Landesdatenschutzbeauftragte
- Innenausschüsse der Landtage
- Rechtsausschüsse der Landtage

- Bundesrechtsanwaltskammer
- Deutscher Richterbund
- Bundesverband der Freien Berufe
- Gewerkschaft der Polizei (Bundesvorstand)
- Deutsche Polizeigewerkschaft im DBB
- Verd.di, Recht und Politik

- Vorstand und Landesverbände des DAV
- Vorsitzende der Gesetzgebungs- und Geschäftsführenden Ausschüsse des DAV
- Vorsitzende des FORUM Junge Anwaltschaft des DAV

- Frankfurter Allgemeine Zeitung
- Süddeutsche Zeitung
- Berliner Zeitung

Der Deutsche Anwaltverein (DAV) ist der freiwillige Zusammenschluss der deutschen Rechtsanwältinnen und Rechtsanwälte. Der DAV mit derzeit ca. 67.000 Mitgliedern vertritt die Interessen der deutschen Anwaltschaft auf nationaler, europäischer und internationaler Ebene.

---

Die vorliegende Stellungnahme befasst sich mit dem Entwurf der Bundesregierung für eine Neuregelung der Bestandsdatenauskunft gemäß **§ 113 TKG** sowie der erforderlichen Folgeregelungen vom 09.01.2013[1]. Das BVerfG hat mit Beschluss vom 24.01.2012[2] diese Vorschrift teilweise als nicht verfassungskonform erachtet, bzw. eine verfassungskonforme Auslegung angemahnt und eine Überarbeitung bis zum 30.06.2013 aufgegeben.

## A. Die Entscheidung des BVerfG

### 1. Regelungsgegenstand: §§ 111 TKG - 113 a.F. TKG

Die Entscheidung des BVerfG hat das sog. manuelle Auskunftsverfahren zum Gegenstand. Ein manuelles Verfahren für Auskünfte aus den nach § 111 TKG gespeicherten Daten regelt § 113 TKG. Im Gegensatz zu dem automatisierten Auskunftsverfahren sieht dieses eine Verpflichtung zur Auskunftserteilung durch die Telekommunikationsunternehmen selbst vor. Ebenso wie im automatisierten Auskunftsverfahren ist über die Auskunftserteilung gegenüber den Datenbetroffenen Stillschweigen zu wahren (vgl. § 113 Abs. 1 Satz 4 TKG).

Nach § 113 **Abs. 1 S. 1** TKG sind die Anbieter von Telekommunikationsdiensten verpflichtet, die **Bestandsdaten** ihrer Kunden (d. h. die Daten gem. § 95 TKG „Vertragsverhältnisse“ und § 111 TKG „Daten für Auskunftsersuchen der Sicherheitsbehörden“) auf Grundlage der allgemeinen strafprozessualen Ermittlungsbefugnisse oder aufgrund der Datenerhebungsvorschriften der Polizeigesetze oder aufgrund der Ermächtigungsgesetze für die Nachrichtendienste preiszugeben. Dies gilt nach § 113 **Abs. 1 S. 2** TKG auch für Daten, die bestimmte **Schutzvorrichtungen** (z.B. durch Passwörter, PINs oder PUKs) auf-

[1] BT-Drucks. 17/12034
[2] Vom 24.01.2012 , 1 BvR 1299/05 = NJW 2012, 1419 ff.

weisen. Nach § 112 TKG kann die Bundesnetzagentur für derartige Auskunftsersuchen jederzeit Daten aus den von den Telekommunikationsunternehmen gespeicherten Dateien im **automatisierten Verfahren**, d. h. ohne Kenntnis der Anbieter bzw. mit Suchverfahren mit großer Streubreite (z. B. „Ähnlichkeitsfunktion“) abrufen.[3]

2. Korrektur durch das BVerfG

Ausgangspunkt der Entscheidung des BVerfG vom 24.01.2012 war die Klage von Nutzern von vorausbezahlten Mobilfunkkarten und Internetzugangsleistungen. Sie machten geltend, durch die Speicherung ihrer Daten nach § 111 TKG (Rufnummer, Anschlusskennung, Mobilfunkendgeräte-nummer, Kennung von elektronischen Postfächern) und die Übermittlung aufgrund von Auskunftsersuchen (§§ 112, 113 TKG) in ihren Grundrechten verletzt zu sein (Tz. 100).

a) Zugangssicherungscodes (§ 113 Abs. 1 S. 2 TKG)

Das BVerfG sah die Speicherungspflicht nach § 111 TKG (Tz. 126 ff.) wie auch das automatisierte Auskunftsverfahren nach § 112 TKG als verfassungskonform an (Tz. 143 ff.), nicht jedoch die Regelung in § 113 **Abs. 1 S. 2** TKG, die (u. a. geschäftsmäßige[4]) Telekommunikationsdienstleister zur Auskunftserteilung u. a. auch im Hinblick auf Zugangscodes (Passwörter, PIN, PUK) verpflichtet. Diese Art der Auskunft, die die Telekommunikationsanbieter zwinge, auch **Zugangssicherungscodes** preiszugeben, ohne dass gesichert sei, dass die Voraussetzungen für deren Nutzung vorliegen, stellt nach Auffassung des BVerfG einen unverhältnismäßigen Eingriff in das Grundrecht auf informationelle Selbstbestimmung dar; denn nach dieser (derzeit geltender) Regelung könne die Abfrage von Zugangssicherungscodes auf Grundlage des § 161 Abs. 1 StPO[5] selbst dann erfolgen, wenn deren Nutzung z. B. im Rahmen einer Tele-

[3] § 112 Abs. 3 Ziff. 3 TKG: „für Abrufe mit unvollständigen Abfragedaten und für die Suche mittels einer Ähnlichkeitsfunktion …“
[4] Z.B. Krankenhäuser und ggf. Hotels
[5] § 161 StPO: „Zu dem in § 160 Abs. 1 bis 3 bezeichneten Zweck ist die Staatsanwaltschaft befugt, von allen Behörden Auskunft zu verlangen …“
§ 160 Abs. 1 StPO: Sobald die Staatsanwaltschaft durch eine Anzeige oder auf anderem Wege von einem Verdacht einer Straftat Kenntnis erhält, hat sie … den Sachverhalt zu erforschen.“

kommunikationsüberwachung an wesentlich strengere Voraussetzungen geknüpft sei.

§ 113 **Abs. 1 S. 2** TKG (Sicherheitscodes) gilt längstens bis zum 30.06.2013 unter der Voraussetzung fort, dass diese Daten nur dann erhoben werden dürfen, wenn die gesetzlichen Voraussetzungen auch für deren **Nutzung** gegeben sind.

b) „Doppeltürenmodell“ und IP-Adressen (§ 113 Abs. 1 S. 1 TKG)

Im Hinblick auf § 113 **Abs. 1 S. 1** TKG (allgemeine Auskunftspflicht) wurde die Verfassungsbeschwerde zurückgewiesen (Tz. 175 ff.). Dies geschah jedoch mit der Maßgabe, dass die Vorschrift verfassungskonform auszulegen ist, was insbesondere aber die Schaffung von länderspezifischen Eingriffsermächtigungen für die Auskunftserteilung voraussetze. Hierzu hat das BVerfG das sog. **Doppeltürenmodell** entwickelt (Tz. 123, 164-174). Dieses Modell besagt im Kern Folgendes:

- Der Datenabruf darf nicht allein auf § 113 Abs. 1 TKG gestützt werden.

- Neben § 113 TKG sind spezielle Erhebungsvorschriften in Fachgesetzen erforderlich. Sowohl die Kompetenzordnung des GG (Art. 73 I Nr. 7 GG) wie auch der Grundsatz der Normenklarheit gebieten es, spezifische Rechtsgrundlagen der Länder zu schaffen, die eine Auskunftsverpflichtung von Telekommunikationsunternehmen (als Privaten) eigenständig begründen (Tz. 167 f.).

- § 113 Abs. 1 TKG stellt keine Rechtsgrundlage für die Zuordnung von **dynamischen IP-Adressen** dar. Deren Identifizierung ist als Eingriff in das Fernmeldegeheimnis gem. Art. 10 I GG anzusehen. Mangels eines Hinweises auf Art. 10 I GG in § 113 Abs. 1 TKG liege zum einen ein Verstoß gegen das **Zitiergebot** gem. Art. 19 I 2 GG vor (Tz. 173). Zum anderen regele § 113 Abs. 1 TKG nicht hinreichend **normenklar** die Befugnis zur Identifizierung der dynamischen IP-Adressen. Diese seien Verkehrsdaten

nach § 96 TKG, auf den (§ 96 TKG) das Auskunftsverfahren in § 113 Abs. 1 TKG aber nicht verweise[6]. Es bedürfe deshalb einer klaren Entscheidung des Gesetzgebers, ob und unter welchen Voraussetzungen eine solche Identifizierung erlaubt sein soll (Tz. 174).

Das Bild von der „Doppeltür“ soll also die Notwendigkeit eines je eigenen Zugangs für die beiden getrennt voneinander zu legitimierenden Grundrechtseingriffe kennzeichnen. In Tz. 123 der Entscheidung heißt es anschaulich:

„*Der Gesetzgeber muss, bildlich gesprochen, nicht nur die Tür zur Übermittlung von Daten öffnen, sondern auch die Tür zu deren Abfrage. Erst beide Rechtsgrundlagen gemeinsam, die wie eine Doppeltür zusammenwirken müssen, berechtigen zu einem Austausch personenbezogener Daten. Dies schließt – nach Maßgabe der Kompetenzordnung und den Anforderungen der Normenklarheit – nicht aus, dass beide Rechtsgrundlagen auch in einer Norm zusammengefasst werden können*.“

§ 113 **Abs. 1 S. 1** TKG kann nur noch bis zum 30.06.2013 übergangsweise auch ohne diese Voraussetzungen angewandt werden.

## B. Der Entwurf

Der vorliegende Entwurf der Bundesregierung vom 09.01.2013 hat die Umsetzung der Entscheidung des BVerfG zum Ziel. Er sieht Änderungen des TKG, der StPO sowie des BKAG, BPolG, ZFdG, BVerfSchG, BNDG und MADG wie folgt vor:

1. Änderung des manuellen Auskunftsverfahrens in § 113 TKG-E
   § 113 **Abs. 1** TKG-E soll – wie bisher – die Telekommunikationsunternehmen zur Erteilung von Auskünften über die nach den §§ 95 und 111 TKG erhobenen Daten verpflichten. Dabei sind in der vorgesehenen Bestimmung nach wie vor auch die mit einem Zugangscode (PIN, PUK) gesicherten Daten aufgeführt.

[6] § 113 Abs. 1 TKG nennt nur § 95 und § 111 TKG

Neu in den Katalog der der Auskunft unterliegenden Daten ist die Zuordnung der IP-Adressen aufgenommen. Es heißt insoweit in Absatz 1 des § 113 TKG-E, dass „*die in eine Auskunft aufzunehmenden Daten … auch anhand einer zu bestimmten Zeitpunkten zugewiesenen* ***Internet-Protokolladresse*** *bestimmt*“ werden dürfen. Für Letzteres dürfen nach der Entwurfsfassung „*Verkehrsdaten automatisiert ausgewertet werden*“ und es sind – auch dies ist neu – für „*die Auskunftserteilung … sämtliche unternehmensinternen Datenquellen zu berücksichtigen*“ (Hervorh. nur hier).

Auskunftsverpflichtet bleiben weiterhin die Anbieter für Telekommunikationsdienste[7], und wie bisher sollen die Auskünfte auch nur gegenüber einer berechtigten Stelle (jetzt in Abs. 3) erteilt werden müssen.

Durch den Entwurf wird in **Absatz 2** die Bezugnahme auf eine Ermächtigungsnorm für die Datenerhebung aufgenommen. Die Telekommunikationsunternehmen sollen nur dann zur Auskunft verpflichtet sein, wenn die ersuchende Stelle schriftlich die Auskunft „*unter Berufung auf eine gesetzliche Bestimmung verlangt, die ihr eine* ***Erhebung*** *der in Absatz 1 in Bezug genommenen Daten* ***erlaubt***“ (Hervorh. nur hier).

2. Neue Auskunftsverpflichtungsgrundlage in § 100 j StPO-E

Der Gesetzesentwurf sieht demgemäß (vgl. die vorausgehende Ziff. 1) eine gesonderte Regelung für die Auskunftsverpflichtung in einem neuen § 100 j StPO-E vor.

Nach dem bisherigen § 113 TKG dürfen u. a. Strafverfolgungsbehörden nach der allgemeinen Ermittlungsklausel der §§ 161 Abs. 1 S. 1, 163 i. V. m. § 113 TKG[8] die Herausgabe der Daten verlangen. Voraussetzung hierzu ist allein,

---

[7] Einschließlich derjenigen, die geschäftsmäßig Telekommunikationsdienste erbringen, s. Fn. 2

[8] Oder: „*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*“ (Abs. 1)

dass die Bestandsdaten für die Ermittlung der Straftat erforderlich sind. Einer gerichtlichen oder staatsanwaltlichen Anordnung bedarf es nicht.

In der Entwurfsbegründung wird hierzu erläutert, dass das BVerfG zwar die Erhebung der Bestandsdaten auf Grundlage der allgemeinen fachrechtlichen Eingriffsermächtigung in seinem Urteil zur Vorratsdatenspeicherung[9] grundsätzlich nicht beanstandet habe. Allerdings habe das Gericht dort angemerkt, es sei sicherzustellen, dass eine Auskunft nur aufgrund eines *„**hinreichenden Anfangsverdachts** oder einer **konkreten Gefahr** auf einzelfallbezogener Tatsachenbasis erfolgen darf“*[10] (Hervorh. nur hier). Auch in seinem Beschluss vom 24.01.2012[11] habe das BVerfG entschieden, dass es für den Abruf der nach den §§ 95, 111 TKG gespeicherten Daten grundsätzlich qualifizierter Rechtsgrundlagen bedürfte, die aus sich heraus eine Auskunftspflicht der Telekommunikationsunternehmen normenklar begründeten.[12] Dementsprechend sieht der Referentenentwurf eine gesonderte Regelung der Eingriffsvoraussetzung für die Datenerhebung in einem neuen § 100 j StPO-E vor.

§ 100 j StPO-E soll demgemäß denjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt, verpflichten, auf Verlangen Auskunft über die gemäß den §§ 95, 111 TKG erhobenen Daten zu erteilen, „*soweit dies für die **Erforschung des Sachverhalts** oder die **Ermittlung des Aufenthaltsortes eines Beschuldigten** erforderlich ist*“. Dies soll auch für Sicherungscodes („Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird“) gelten, jedoch soll hier die Auskunftserteilung von der zusätzlichen Bedingung abhängen, dass „*die gesetzlichen Voraussetzungen für die **Nutzung der Daten** vorliegen*“ (Abs. 1; Hervorh. nur hier).

Nach § 100 j Abs. 2 StPO-E darf eine Auskunft „*nach Absatz 1*“ unter denselben Voraussetzungen auch „*anhand einer zu bestimmten Zeitpunkten zugewiesenen **Internetprotokoll-Adresse** verlangt werden*“ (Hervorh. nur hier).

---

[9] BVerfG 1 BvR 256/08 – Urt. V. vom 2.3.2010 = NJW 2010, 833
[10] Urteil v. 2.3.2010, 1 BvR 256/08, Rn. 261, zitiert in Entwurfsbegründung S. 17
[11] V. 24.01.2012, 1 BvR 1299/05
[12] Entwurfsbegründung S. 17

3. Vergleichbare Ermächtigungen in Polizeigesetzen

Dem neuen § 100 j E-StPO entsprechende Ermächtigungsvorschriften im Hinblick auf entsprechende Auskunftsverlangen sind auch für das BKAG, BPolG, BVerfSchG, ZFdG, BNDG und das MADG vorgesehen. Die Bestandsdaten-Auskunft wird hier im Wesentlichen an die Erforderlichkeit der Aufgabenerfüllung der betreffenden Polizei- bzw. Sicherheitsbehörde geknüpft („… *soweit dies zur Erfüllung der Aufgabe des … erforderlich ist*“). Dabei werden für die Aufgaben der Strafverfolgung und die der Gefahrenabwehr je gesonderte Ermächtigungsnormen vorgesehen. So sollen z. B. in § 7 Abs. 3 BKAG-E Auskünfte dann zugelassen werden, wenn sie „*zur Erfüllung der Aufgabe des Bundeskriminalamtes als Zentralstelle nach § 2 Absatz 2 Nummer 1 erforderlich“* sind, während sie § 20 b Abs. 3 BKAG-E für Zwecke der Strafverfolgung davon abhängig machen will, dass(s*oweit) dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes einer Person … erforderlich ist*“.

## C. Stellungnahme

Die Anforderungen des Bundesverfassungsgerichts werden durch den Referentenentwurf nur unzureichend umgesetzt.

1. § 113 Abs. 1 Satz 2 TKG-E – **Zugangssicherungscodes**

Die Regelung im Referentenentwurf zur Auskunft über die Zugangssicherungscodes lässt Fragen offen und gewährleistet im Ergebnis nicht, dass die Vorgaben des Bundesverfassungsgerichts, das das bestehende Gesetz (§ 113 Abs. 1 S. 2 TKG a.F.) als einen unverhältnismäßigen Eingriff in das Grundrecht auf informationelle Selbstbestimmung angesehen hat, eingehalten werden.

Nach der Entwurfsfassung des § 113 Abs. 2 TKG-E ist nunmehr die Auskunft über die Zugangssicherungscodes von einer Erlaubnis der befugten Stelle „*in Textform unter Berufung auf eine gesetzliche Bestimmung verlangt (wird), die ihr eine Erhebung der in Absatz 1 in Bezug genommenen Daten*“, abhängig.

Die „*gesetzliche Bestimmung*“, die die **Erhebung** der PIN´s und PUK´s regelt, ist der neue § 100 j StPO-E, der seinerseits vorsieht, dass eine „*Auskunft nur verlangt werden (darf), wenn die gesetzlichen Voraussetzungen für die **Nutzung** der Daten vorliegen*“ (Hervorh. nur hier). Diese Regelung ist die Kehrseite des allgemein im Strafprozessrecht geltenden Grundsatzes, wonach ein Beweisverwertungsverbot auch ein Beweiserhebungsverbot bewirkt[13]. Welches die gesetzlichen Voraussetzungen für die Nutzung der Daten „Zugangscodes“ sind, ergibt sich aus § 100 j StPO-E selbst allerdings nicht. Da die PIN´s und PUK´s den Zugang zu den Inhalten von Telekommunikation sichern, gelten sie als Verkehrsdaten, deren Nutzung, d. h. Verwertung, an die Voraussetzungen des § 100 g StPO geknüpft ist (z. B. Tatverdacht auf eine Straftat „*von erheblicher Bedeutung*“, Richtervorbehalt).

Der Gesetzesentwurf sieht demnach für die Auskunft über die Zugangssicherungscodes eine Verweisungskette vor, die von § 113 Abs. 1 TKG-E, über § 113 Abs. 2 TKG-E, dann weiter über § 100 j StPO-E bis (im Regelfall) zu § 100 g StPO führt. Alle diese Bestimmungen haben spezielle und zum Teil komplizierte Anwendungsvoraussetzungen, ggf. bis hin zum Richtervorbehalt in § 100 g StPO. Das BVerfG[14] selbst verweist auf die je nach Fallgestaltung unterschiedlichen gesetzlichen Anforderungen im Hinblick auf die Nutzung von Zugangscodes. So sei z. B. die Nutzung von Zugangscodes zur Ermöglichung einer Onlinedurchsuchung oder zur Überwachung eines noch nicht abgeschlossenen Telekommunikationsvorgangs an andere (strengere) gesetzliche Voraussetzungen zu knüpfen (z. B. §§ 100a, 100b StPO mit Richtervorbehalt), als beispielsweise die Nutzung zum Auslesen eines beschlagnahmten Mobiltelefons. Der Bundesrat bemängelt zu Recht in seiner Stellungnahme zu dem Gesetzesvorhaben eine „*Beschränkung auf bestimmte, klare begrenzte Fälle*“ sowie das Fehlen jeglichen Hinweises auf die „*Hürde des Richtervorbehalts*“ oder einer „*sonstigen staatsanwaltlichen Anordnung*“.[15]

---

[13] Vgl. Eisenberg, Beweisrecht der StPO, 8. Aufl. 2012, Rz. 353
[14] Tz. 184
[15] BR-Drs. 664/1/12 vom 03.12.2012 S. 3

Der Gesetzesentwurf verhält sich des Weiteren nicht zu der in der Praxis relevanten Frage, wie ein um die Herausgabe von Daten ersuchtes Telekommunikationsunternehmen prüfen kann, ob das Auskunftsverlangen Recht und Gesetz entspricht oder unzulässig ist und gegen Grundrechte seiner Kunden verstößt. Aus eigenem Vermögen wird das Telekommunikationsunternehmen hierüber nicht befinden können. Dieses wird weder den Sachverhalt kennen, der die Ermittlungsbehörden zum Auskunftsersuchen veranlasst, und demzufolge auch nicht die rechtlichen Nutzungsvoraussetzungen beurteilen können. In Anbetracht dieser Bandbreite an möglichen Sachverhaltskonstellationen und der im Einzelfall potentiell drohenden Eingriffsintensitäten bei rechtswidriger Auskunftserteilung, kommt dieser Frage eine ausschlaggebende Bedeutung zu.

Der Bundesrat nennt es in seiner Stellungnahme „*problematisch*“, dass dem Entwurf zufolge „*die Verantwortung für die Prüfung auf Rechtmäßigkeit der Auskunftsersuchen nicht allein den staatlichen Stellen obliegt, sondern den Providern auferlegt werden soll*“. Es könne nicht zur Aufgabe der Provider und Telekommunikationsunternehmen gemacht werden, rechtsstaatliches Handeln der Behörden zu überprüfen. Nach dem Willen des Bundesrates sollen „*allein die staatlichen Stellen die Verantwortung für die Rechtmäßigkeit ihrer Anfragen von Bestandsdaten tragen*“, das Risiko einer Fehleinschätzung dürfe nicht auf den privaten Unternehmen lasten.[16] Die Bundesregierung vertrat in ihrer Gegenäußerung vom 09.01.2013 die Auffassung, dass dies durch den Regierungsentwurf gewährleistet ist.[17]

Der Ausschuss für Gefahrenabwehrrecht des DAV sieht bereits in den divergierenden Auffassungen des Bundesrats und der Bundesregierung zur Frage der Prüfungskompetenz ein gewichtiges Indiz dafür, dass die vorgestellte gesetzliche Regelung hinsichtlich der Normenklarheit verbesserungswürdig ist. Der Gesetzgeber muss eindeutig regeln, ob und ggf. inwieweit die Telekommunikationsunternehmen das Vorliegen der gesetzlichen Nutzungsvoraussetzungen zu überprüfen haben oder ob sie dazu nicht verpflichtet sind. Will der Gesetz-

[16] BR-Drs. 664/1/12 vom 03.12.2012, S. 3

[17] http://dip21.bundestag.de/dip21/btd/17/120/1712034.pdf#page=38

geber die Telekommunikationsunternehmen in die Pflicht nehmen, muss er den (privaten) Unternehmen klare Vorgaben machen und Kriterien für die Einzelfallprüfung festlegen; denn erst ein positives Prüfungsergebnis begründet die Herausgabepflicht. Aus der vorliegenden Entwurfsfassung ergeben sich keine derartigen (klaren und eindeutigen) Kriterien. Das in § 113 Abs. 2 TKG-E normierte Schriftlichkeitserfordernis (die befugte Stelle muss die Auskunft „*in Textform unter Berufung auf eine gesetzliche Bestimmung“* verlangen) ist ein rein formales Kriterium, das überdies bei „*Gefahr im Verzug*“ auch noch entbehrlich sein soll. Es besagt nichts darüber, ob die im konkreten Einzelfall maßgeblichen Nutzungsvoraussetzungen tatsächlich vorliegen. Dies kann auch die gemäß § 113 Abs. 5 TKG-E bei den Telekommunikationsunternehmen zu installierende „verantwortliche Fachkraft“ nicht; denn deren Aufgabe beschränkt sich darauf, das Vorliegen der Formalvoraussetzungen des Absatzes 2 (Schriftform und Bezeichnung einer Gesetzesnorm) zu überprüfen.

Sollen demgegenüber die Telekommunikationsunternehmen nur bloße „Vollziehungsbeauftragte“ der ersuchenden Behörden sein, und tragen die Behörden – wie die Bundesregierung in ihrer Stellungnahme erklärt[18] – die alleinige Verantwortung, stellt sich die Frage, wie und durch wen im Zeitpunkt des konkreten Ersuchens das Vorliegen der materiellen Nutzungsvoraussetzungen für die Daten und damit die Rechtmäßigkeit des Handelns *der ersuchenden Behörden* überprüft werden kann. Insoweit sieht der Entwurf keine Regelung vor und enthält hier eine empfindliche Lücke. Allein das Vertrauen darauf, dass die ersuchenden Behörden alles richtig machen, ist nicht ausreichend. Auch die theoretische Möglichkeit, dass die Inhaber der PIN´s und PUK´s die ihnen über die Rechtsschutzmöglichkeiten gegen rechtsfehlerhafte Eingriffe gemäß § 100 g StPO ausschöpfen könnten, ist nur ein schwacher Trost. Von der Herausgabe seiner PIN´s und PUK´s erfährt der Betroffene nichts, da § 113 Abs. 4 TKG-E die Telekommunikationsunternehmen zum Stillschweigen ihm gegenüber verpflichtet. Bis der Betroffene – ggf. erst im Zuge eines gegen ihn eingeleiteten Ermittlungsverfahrens – von der Herausgabe seiner Daten erfährt, sind diese längst „genutzt“, ohne dass er jemals die Möglichkeit gehabt hätte, auf die Un-

[18] S. Fn. 17

zulässigkeit der Datenherausgabe und Datenerhebung und den damit verbundenen Grundrechtseingriff hinzuweisen.

Der Bundesrat hat in seiner bereits erwähnten Stellungnahme mit Recht die in § 113 TKG-E fehlende Mitteilungspflicht gegenüber den Betroffenen bemängelt und auf die Rechtsschutzgarantie des Artikels 19 IV GG hingewiesen, die dann insbesondere an Bedeutung gewinnt, wenn die Mitteilung für den Betroffenen überhaupt erst die Möglichkeit eröffnet, gerichtlichen Rechtsschutz in Anspruchs zu nehmen.[19] So verhält es sich hier. Auch insofern bedarf der vorliegende Entwurf der (sehr) grundlegenden Korrektur, damit der Entscheidung des Bundesverfassungsgerichts gebührend Rechnung getragen wird.

2. § 113 Abs. 1 TKG-E i. V. m. § 111 j StPO-E – **IP-Adressen**

Das BVerfG hat in seiner Entscheidung vom 24.01.2012 klargestellt, dass § 113 a.F. TKG keine Rechtsgrundlage für die Zuordnung anhand von zu bestimmten Zeiten zugewiesenen IP-Adressen darstellt. Es handele sich bei einer solchen Zuordnung um einen Eingriff in das Fernmeldegeheimnis nach Art. 10 I GG, weshalb es einer eindeutigen Entscheidung des Gesetzgebers bedürfe, ob und unter welchen Voraussetzungen eine solche Identifizierung erlaubt sein soll. Das BVerfG beanstandete das Fehlen eines entsprechenden Hinweises nach Art. 19 I 2 GG und äußert Bedenken im Hinblick auf die Normenklarheit: IP-Adressen seien Verkehrsdaten i. S. des § 96 TKG. Eine Auskunftspflicht der Telekommunikationsdienstleister im Hinblick auf diese Daten werde in § 113 a.F. nicht erwähnt.

Auch diesen Anforderungen wird der Referentenentwurf nicht in vollem Umfang gerecht.

a) § 113 TKG-E ist nach wie vor nicht hinreichend normenklar. Dies gilt auch und gerade in Verbindung mit der (neuen) Auskunftsermächtigungsvorschrift § 100 j StPO-E.

[19] BR-Drs. 664/1/12 vom 03.12.2012, S. 5

Zunächst unterscheidet § 113 TKG-E nicht zwischen Verkehrsdaten und Bestandsdaten. § 113 Abs. 1 TKG-E verpflichtet die Telekommunikationsunternehmen vielmehr ohne jede Differenzierung zur Auskunft über die Zuordnung der IP-Adressen (als besonders schützenswerten Verkehrsdaten[20]) wie auch über die Bestandsdaten nach den §§ 95, 111 TKG.

Das Erfordernis einer differenzierenden Handhabung lässt sich auch nicht der Bezugnahme auf die vorgesehene neue Auskunftsermächtigungsgrundlage in § 100 j StPO-E entnehmen. Dort ist in **Absatz 2** zwar geregelt, dass „*die Auskunft nach **Absatz 1***“ auch anhand einer dynamischen IP-Adresse verlangt werden kann. **Absatz 1** des § 100 j StPO-E regelt allerdings (in demselben Absatz) zwei Fallkonstellationen mit unterschiedlichen Eingriffsvoraussetzungen: Zum einen die (niederschwellige) Auskunftspflicht bei den Bestandsdaten nach §§ 95, 111 TKG, die besteht, „*soweit dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich ist*“ (§ 100 j Abs. 1 S. 1 StPO-E), zum anderen die Auskunft über die Sicherungscodes, die „*nur verlangt werden* (kann), *wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen*“. Welche dieser beiden in Absatz 1 bezeichneten Voraussetzungen für die dynamischen IP-Adressen gelten sollen, ist § 100 j StPO-E nicht zu entnehmen.

Da es sich bei den IP-Adressen – ebenso wie bei den Sicherungscodes – um Verkehrsdaten handelt, deren Erhebung in § 100 g StPO abschließend unter speziellen Voraussetzungen (z. B. Tatverdacht „*von erheblicher Bedeutung*“, Richtervorbehalt) geregelt ist, kann zwar angenommen werden, dass mit dem Entwurf beabsichtigt ist, die Auskunft über die IP-Adressen an das Vorliegen der „*gesetzlichen Voraussetzungen an die Nutzung der Daten*“ zu knüpfen. Eindeutig ist dies der Entwurfsfassung jedoch nicht zu entnehmen. Hier bedarf es im Interesse der vom Bundesverfassungsgericht angemahnten Normenklar-

[20] Sollten in Zukunft auch für den privaten Gebrauch – wie geplant – die statischen IP-Adressen die dynamischen IP-Adressen ersetzen, wird sich die Problematik der Schwere des Eingriffs in Verkehrsdaten noch verschärfen. Für diesen Fall sieht der Entwurf keine Regelung vor, vgl. hierzu DAV-Stellungnahme 1/2012 zum „Gesetz zur Sicherung vorhandener Verkehrsdaten und Gewährleistung von Bestandsdatenauskünften im Internet“, S. 13

heit[21] einer eindeutigen Regelung. Dies gilt umso mehr, als in ein- und derselben Vorschrift § 113 Abs. 1 TKG-E unter der Überschrift „Manuelles Auskunftsverfahren“ sowohl die Herausgabe der IP-Adressen als besonders schützenswerten *Verkehrsdaten* wie auch die Herausgabe der einfachen *Bestandsdaten* geregelt ist. Hierdurch wird der Eindruck einer (materiellen) Gleichartigkeit erweckt, die aber tatsächlich nicht gegeben ist.

b) Das BVerfG hatte im Hinblick auf die dynamischen Internetprotokolladressen beanstandet, dass dem Zitiergebot des Art. 19 I 2 GG durch Hinweis auf den mit der Auskunft verbundenen Eingriff in Art. 10 I GG nicht entsprochen wurde. In der Entwurfsbegründung zu § 113 Abs. 1 TKG-E wird ausgeführt, dass nunmehr „*durch Satz 2, zweiter Halbsatz … die erforderliche Klarstellung*“ erfolgt sei.[22] Diese Klarstellung ergibt sich allerdings aus der Fassung des § 113 Abs. 1 TKG-E nicht.

3. Polizei- und Sicherheitsgesetze

Die obigen Ausführungen gelten sinngemäß auch für die Regelungen des Entwurfs bezüglich der **Polizei- und Sicherheitsgesetze** (BKAG, BPolG, BVerfSchG, ZFdG, BNDG und MADG). Soweit die entsprechenden Behörden repressiv tätig werden, sind sie unmittelbar zu übertragen.

Im Bereich der Gefahrenabwehr knüpfte § 113 Abs. 1 Satz 1 TKG die Befugnis zur Übermittlung der Daten an die eingrenzende Voraussetzung, dass eine solche Befugnis nur gegeben sei, *„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“ (*Hervorhebung nur hier).

[21] § 113 Abs. 1 TKG nennt nur § 95 und § 111 TKG
[22] BT-Drucks. 17/12034 vom 09.01.2013, S. 20

Das Bundesverfassungsgericht hatte deshalb in seiner Entscheidung vom 24.1.2012[23] darauf hingewiesen, dass mit diesem Wortlaut *„der Gesetzgeber die Gefahrenvorsorge gerade nicht einbezogen hat“* und *„sich bei verständiger Auslegung das Erfordernis einer „konkreten Gefahr“ im Sinne der polizeilichen Generalklauseln als Voraussetzung für solche Auskünfte“* ergebe. Diese Schwelle sei *„freilich niedrig und umfasst auch den Gefahrenverdacht“* und sei *„nicht von vornherein auf Polizeipflichtige im Sinne des allgemeinen Polizei- und Ordnungsrechts“* beschränkt. Dies führe jedoch nicht zu einer Unverhältnismäßigkeit der Norm, weil weiterhin im Einzelfall ein *„sicherheitsrechtlich geprägter Charakter der betreffenden Aufgabe“* Voraussetzung für die Übermittlung sei und Auskünfte nicht als *„allgemeines Mittel für einen gesetzesmäßigen Verwaltungsvollzug ermöglicht“* werden.

Der Gesetzentwurf verzichtet künftig auf jede eigene Eingrenzung der materiellen Voraussetzungen der Übermittlungsbefugnis. § 113 Abs. 3 Nr. 2 TKG-E führt zwar die Stellen auf, denen Auskünfte zu erteilen sind, so die *„für die Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung zuständigen Behörden“*. Aus dieser Begrenzung des Kreises der Behörden, denen die Erbringer von Telekommunikationsdienstleistungen Auskünfte erteilen dürfen, lässt sich jedoch nicht mit der erforderlichen Rechtsklarheit entnehmen, zu welchen Zwecken diese Stellen die Daten erheben dürfen. Insoweit verbleibt es vielmehr bei einem allgemeinen Bezug auf das Fachrecht. Damit spricht viel dafür, dass künftig derartige Auskunftsverlangen auch zur Gefahrenvorsorge verwendet werden können, so etwa im Falle des **BKA** aufgrund von dessen Aufgabe *als „Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen und für die Kriminalpolizei die Polizeien des Bundes und der Länder bei der Verhütung und Verfolgung von Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung“*. Die Neufassung der Befugnisnorm des § 7 Abs. 3 BKA-G E verweist jedenfalls auf diese Aufgabe des BKA, die mit der *„Verhütung von Straftaten“* gerade die Gefahrenvorsorge umfasst.[24]

[23] BVerfG Beschuss vom 24. Januar 2012- 1 BvR 1299/05- Rn. 177f
[24] Denninger in: Lisken/Denninger Handbuch des Polizeirechts, 4. Auflage, E 35

Auch im Hinblick auf die Zuständigkeit der **Bundespolizei** zur Verhütung von Straftaten gemäß § 1 Abs. 7 BPolG dürfte künftig eine Datenerhebung auch für Zwecke der Gefahrenvorsorge nicht ausgeschlossen sein, da § 22a BPolG-E gerade an die Aufgaben der Gefahrenvorsorge nach § 21 BPolG-E anknüpft.

Im Hinblick auf die **Nachrichtendienste** stellte das BVerfG fest, dass es in § 113 Abs. 1 TKG a.F. *„an einer vergleichbaren Eingriffsschwelle“* fehle, was jedoch „*aus deren beschränkten Aufgaben, die nicht unmittelbar auf polizeiliche Maßnahmen ausgerichtet sind, sondern nur auf eine Berichtspflicht gegenüber den politisch verantwortlichen Staatsorganen beziehungsweise der Öffentlichkeit zielen*“ gerechtfertigt sei. Jedoch ergebe sich hier aus Sicht des BVerfG *„aus dem Erfordernis der Erforderlichkeit im Einzelfall, dass eine Auskunft gemäß § 113 Abs. 1 Satz 1 TKG zur Aufklärung einer bestimmten, nachrichtendienstlich beobachtungsbedürftigen Aktion oder Gruppierung geboten sein muss. Soweit sich Auskünfte auf die Verfolgung von Straftaten und Ordnungswidrigkeiten beziehen, ergibt sich aus dem Erfordernis der Erforderlichkeit im Einzelfall, dass zumindest ein **Anfangsverdacht** vorliegen muss“* (Hervorh: nur hier).

Das Bundesverfassungsgericht hielt die in § 113 Abs. 1 Satz 1 TKG normierten Schwellen der Übermittlungsbefugnis *für „verfassungsrechtlich noch hinnehmbar“*. Der Gesetzentwurf senkt sie mit seiner Anknüpfung an die Aufgaben der Sicherheitsbehörden weiter ab, indem auch die ***„Gefahrenvorsorge“*** eine Datenübermittlung rechtfertigt. Gleichzeitig verzichtet der Gesetzentwurf darauf, die vom BVerfG geforderte Eingrenzung auf eine *„konkrete Gefahr“* zu übernehmen und die Übermittlungsbefugnisse an die Nachrichtendienste entsprechend den Ausführungen des BVerfG zu konkretisieren, was im Sinne der Normenklarheit wünschenswert wäre, weil es doch dem Rechtsanwender bereits durch die Norm selbst die Grenzen seiner Befugnisse vor Augen führt. Immerhin verbleibt auch weiterhin beim manuellen Auskunftsverfahren für die abfragende Behörde ein gewisser Verfahrensaufwand, *„der dazu beitragen dürfte, dass die Behörde die Auskunft nur bei hinreichendem Bedarf einholt“*, wie das BVerfG in seiner Entscheidung bereits anmerkte.