Meinhard Starostik

Rechtsanwalt/vereidigter Buchprüfer

Schillstr. 9 • 10785 Berlin
Tel.: 030 - 88 000 3-0
Fax: 030 - 88 000 346
email: Kanzlei@Starostik.de
internet: www.Starostik.de
USt-ID-Nr. DE165877648

RA/vBP Starostik, Schillstr. 9, 10785 Berlin

An das
Bundesverfassungsgericht
Schloßbezirk 3
76131 Karlsruhe

Berlin, den 30.Juni 2013

AZ: 100/2013
(bitte stets angeben)

Verfassungsbeschwerde

der Frau Katharina Nocun, XXXXXXXXXXXXXXX

Beschwerdeführerin zu 1)

und

des Herrn Dr. Patrick Breyer, XXXXXXXXXXXXXXXXXXXX

Beschwerdeführer zu 2)

Namens und Kraft Vollmacht der Beschwerdeführer wird Verfassungsbeschwerde erhoben und beantragt, zu erkennen:

> §§ 113 TKG, 7 Abs. 3 bis 7, 20b Abs. 3 bis 7, 22 Abs. 2 bis 4 BKAG, 22a BPolG, 7 Abs. 5 bis 9, 15 Abs. 2 bis 6 ZFdG, 8d BVerfSchG, 2b BNDG und 4b MADG in der Fassung des Gesetzes zur Änderung des Telekommunikationsgesetzes und zur Neuregelung der Bestandsdatenauskunft – BGBl. I 2013, S. 1602 - sind mit Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 sowie 10 Absatz 1 des Grundgesetzes unvereinbar.

Die schriftlichen Vollmachten der Beschwerdeführer werden ohne besondere Aufforderung nachgereicht werden.

Inhaltsverzeichnis

1 Sachverhalt

Die Beschwerdeführer wenden sich gegen Vorschriften des Gesetzes zur Änderung des Telekommunikationsgesetzes und zur Neuregelung der Bestandsdatenauskunft. Sie rügen eine

Verletzung des Rechts auf informationelle Selbstbestimmung gemäß Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG sowie des Telekommunikationsgeheimnisses gemäß Art. 10 Abs. 1 GG.

Die Beschwerdeführerin zu 1) ist Inhaberin eines Mobilfunkanschlusses, nutzt meherer E-Mail-Postfächer, sie nutzt ein Smartphone damit verbundene Google-Dienste und mobiles Internet, Skype und den Mikroblogging-Dienst Twitter sowie Cloud-Dienste. Als Journalistin für netzwelt.de ist sie darauf angewiesen, anonyme und nicht rückverfolgbare Hinweise oder Dokumente erhalten zu können, da diese nicht selten nur im Schutz der Anonymität gegeben werden. In diesem Zusammenhang muss sie auch selbst geschützt kommunizieren und im Internet recherchieren können.

Der Beschwerdeführer zu 2) ist Inhaber eines Festnetz- und Internetanschlusses und mehrerer E-Mail-Postfächer, er nutzt außerdem ein Mobiltelefon. Als Abgeordneter im schleswig-holsteinischen Landtag ist er darauf angewiesen, anonyme und nicht rückverfolgbare Hinweise beispielsweise über Missstände im Land erhalten zu können, da diese nicht selten nur im Schutz der Anonymität gegeben werden. In diesem Zusammenhang muss er auch selbst geschützt kommunizieren und im Internet recherchieren können.

Die Beschwerdeführer nehmen u.a. auch häufig an Demonstrationen teil, benutzen währenddessen und auch außerhalb von Demonstrationen ihre Smartphones zum Telefonieren, Versenden von Textnachrichten (SMS) und Emails, die Beschwerdeführerin auch den Telekommunikationsanbieter Twitter zum Versenden von Tweets.

2 Zulässigkeit der Beschwerde

Die angegriffenen Vorschriften betreffen die Beschwerdeführer unmittelbar, selbst und gegenwärtig. An einer unmittelbaren Selbstbetroffenheit fehlt es in Bezug auf die angegriffenen Vorschriften nicht deshalb, weil diese erst auf der Grundlage weiterer Vollzugsakte in Form von Auskunftsersuchen oder -verlangen und dann der Auskunftserteilung wirksam werden. Von Auskünften über ihre Daten werden die Beschwerdeführer wahrscheinlich keine Kenntnis erlangen. Viele Auskünfte führen nicht zu weiteren Maßnahmen gegen die Betroffenen, etwa wenn die Identitäten zu Rufnummern eines aufgefundenen Telefonbuchs oder der sich in einer Funkzelle aufhaltenden Personen abgefragt werden. Eine Benachrichtigung ist in vielen Fällen nicht vorgesehen (z.B. § 100j Abs. 4 StPO i.V.m. Abs. 1 Satz 1). Bei Abfragen von IP-Adressen und Zugangssicherungscodes unterliegt die Benachrichtigungspflicht so vielen Einschränkungen (z.B. Vereitelung des Zwecks der Auskunft, übergreifende Nachteile für das Wohl des Bundes oder eines Landes oder überwiegende schutzwürdige Belange Dritter oder der betroffenen Person selbst), dass die Beschwerdeführer auch von solchen Maßnahmen in den meisten Fällen nicht erfahren werden.

Da die Beschwerdeführer keine Kenntnis von den Vollzugsakten erlangen, reicht die Darlegung aus, mit einiger Wahrscheinlichkeit von solchen Maßnahmen berührt zu werden. Maßgeblich ist hierfür insbesondere, dass die durch die angefochtenen Vorschriften ermöglichten Auskünfte eine große Streubreite haben und Dritte auch zufällig erfassen können. Darlegungen, durch die sich die Beschwerdeführer selbst einer Straftat bezichtigen müssten, sind zum Beleg der Selbstbetroffenheit ebenso wenig erforderlich wie der Vortrag, für sicherheitsgefährdende oder nachrichtendienstlich relevante Aktivitäten verantwortlich zu sein (vgl. BVerfGE 125, 260 <305>).

3 Begründetheit der Beschwerde

Prüfungsmaßstab ist im Schwerpunkt das Recht auf informationelle Selbstbestimmung gemäß Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG. Soweit die Vorschriften zur Zuordnung von

dynamischen IP-Adressen ermächtigen, greifen sie in das Telekommunikationsgeheimnis gemäß Art. 10 GG ein. (BVerfGE 130, 151 (179 ff.)

3.1 § 113 TKG

3.1.1 Mangelnde Gesetzgebungskompetenz

Nach der Rechtsprechung des Bundesverfassungsgerichts kann der Bund auf der Grundlage des Art. 73 Abs. 1 Nr. 7 GG eine Verpflichtung privater Telekommunikationsunternehmen, einem Auskunftsbegehren Folge zu leisten, nicht abschließend begründen. (BVerfGE 130, 151 (201), Abs. 167) Dies gehört nicht mehr zur Bestimmung der Grenzen des Datenschutzes, sondern ist untrennbarer Bestandteil des Datenabrufs. Der Bund kann auf der Grundlage des Art. 73 Abs. 1 Nr. 7 GG nur die Öffnung der Datenbestände für die staatliche Aufgabenwahrnehmung regeln, nicht aber auch den Zugriff auf diese Daten selbst.

In welcher Form, in welchem Zeitrahmen und Umfang Auskünfte zu erteilen sind ("unverzüglich und vollständig") und ob der Anbieter seine Kunden informieren darf, betrifft nicht lediglich die "Öffnung der Datenbestände". Deswegen ist der Bund für § 113 Abs. 3 und 4 unzuständig. (Ebenso für § 113 Abs. 4 S. 1 TKG Bäcker, Stellungnahme gegenüber dem Innenausschuss des Bundestags vom 8. März 2013, [https://www.bundestag.de/bundestag/ausschuesse17/a04/Anhoerungen/Anhoerung26/Stellungnahmen_SV/Stellungnahme_03.pdf ADrs. 17(4)680 C], 5.) Im Zuständigkeitsbereich der Länder muss es diesen überlassen bleiben, in welchem Zeitrahmen und Umfang sie zur Auskunfterteilung verpflichten und ob sie den Anbieter zu Stillschweigen verpflichten wollen. Die Länder könnten beispielsweise vorsehen, dass der Anbieter gegenüber seinem Kunden nur auf besondere Anordnung zu schweigen hat ("Gag-Order"). Dies erscheint etwa bei Datenerhebungen zur Suche nach vermissten Personen geboten, weil diesen die Suche nicht vorenthalten zu werden braucht.

3.1.2 Verletzung des Verhältnismäßigkeitsgebots

3.1.2.1 Unverhältnismäßige Abrufschnittstelle

Es greift unverhältnismäßig weit in die Grundrechte der Beschwerdeführer ein, dass der Gesetzgeber den staatlichen Zugriff auf Telekommunikationsdaten einerseits durch Einführung einer elektronischen Schnittstelle zum direkten Datenaustausch (§ 113 Abs. 5 TKG) drastisch ausweitet, auf der anderen Seite die Voraussetzungen des Zugriffs aber nicht entsprechend eingrenzt.

Das Bundesverfassungsgericht hat die "sehr weit" reichende staatliche Einsicht in Telekommunikationsdaten über § 113 TKG nur deswegen als "verfassungsrechtlich noch hinnehmbar" bezeichnet, weil "im Vergleich zu § 112 TKG [...] ein manuelles Auskunftsverfahren für die abfragende Behörde einen gewissen Verfahrensaufwand mit sich bringt, der dazu beitragen dürfte, dass die Behörde die Auskunft nur bei hinreichendem Bedarf einholt." (BVerfGE 130, 151, 206, Absatz-Nr. 178 und 180) Wenn über eine elektronische Schnittstelle der Behördenaufwand nun auf das Maß des automatisierten Abrufverfahrens nach § 112 TKG reduziert wird, gleichwohl aber die ausufernde Weite der Zugriffsbefugnisse beibehalten und sogar weiter ausgedehnt wird, ist das Gebot der Verhältnismäßigkeit verletzt und die Vorschrift verfassungswidrig. Dass im Vergleich zu § 112 TKG die Auskunft nach § 113 TKG zeitlich verzögert nach einer formellen Prüfung erteilt wird, erhöht den Verfahrensaufwand "für die abfragende Behörde", auf den das Bundesverfassungsgericht abstellt, nicht.

Die automatisierte Schnittstelle wird insofern zu einer drastischen Ausweitung des staatlichen Zugriffs auf Kommunikationsdaten führen als sich Datenabfragen damit unmittelbar in die behördliche Datenverarbeitung integrieren lassen. Die Abfrage von Bestandsdaten wird auf Mausklick möglich. Die maschinenlesbar eingehende Antwort kann von der Software in Sekundenschnelle aufbereitet, ausgewertet, verknüpft oder weitergegeben werden. Die integrierten Informationssysteme etwa der Polizei erlauben es, Bestandsdaten zusammen mit anderen Datensammlungen zu einem teilweise oder weitgehend vollständigen Persönlichkeitsbild zusammenzufügen.

Die automatisierte Schnittstelle entfernt die Bestandsdatenauskunft vom Leitbild eines Zugriffs im Einzelfall und ermöglicht automatisierte Massendatenabfragen und -auswertungen. So können Polizei und Nachrichtendienste beispielsweise tausende von Teilnehmer an einer Demonstration, deren Handynummern über eine Funkzellenabfrage bekannt geworden sind, identifizieren und deren Identität mit ihren vielfältigen Datenbanken abgleichen. Die Schnittstelle macht es auch möglich, Zehntausende von Internetnutzern zu identifizieren, die nach bestimmten Wörtern gesucht oder auf einen bestimmten Inhalt im Internet zugegriffen haben. Die zur Abfrage erforderlichen IP-Adressen und Zugriffszeiten können in Form von "Logfiles" von den Serverbetreibern bezogen werden. Insgesamt kann so die Internetnutzung in weitem Umfang gläsern gemacht werden, wie es vergleichbarem nicht-digitalen Informationsaustausch (z.B. Bibliotheksnutzung, Lesen von Zeitungen, Hören von Radio) nicht denkbar ist.

3.1.2.2 Fehlende Beschränkung auf Einzelfälle

Sowohl in § 113 TKG als auch in den fachrechtlichen Datenerhebungsbefugnissen fehlt die im geltenden § 113 TKG enthaltene Bestimmung, dass Auskünfte über Telekommunikationsdaten nur "im Einzelfall" eingeholt dürfen und nicht routinemäßig oder massenhaft. Da die Beschränkung auf Einzelfälle fehlt, andererseits aber die ausufernd weiten Auskunftsrechte unverändert beibehalten werden sollen, ist das Verhältnismäßigkeitsgebot verletzt und die Neufassung verfassungswidrig. (Unabhängiges Landesdatenschutzzentrum, Stellungnahme vom 27.11.2012, https://www.datenschutzzentrum.de/polizei/20121127-stellungnahme-tkg-aenderung.html, Ziff. I; Bundesrat, BT-Drs. 17/12034, 17; Wirtschaftsausschuss des Bundesrats, BR-Drs. 664/1/12, 2.)

Da es sich bei der Preisgabe von Bestandsdaten um einen schweren Grundrechtseingriff handelt, muss verhindert werden, dass die Auslieferung von Bestandsdaten zur Massenüberwachung ausartet, in der Bestandsdaten routinemäßig aufgrund kleinster Anlässe oder gar zur Vorsorge im Übermaß angefragt werden. Deshalb muss die Auslieferung von Bestandsdaten wie bisher (§ 113 TKG a.F.) ausdrücklich auf Einzelfälle beschränkt bleiben.

Das Bundesverfassungsgericht hat § 113 TKG ausdrücklich nur deswegen als "verfassungsrechtlich noch hinnehmbar" angesehen, weil "Auskünfte nach § 113 Abs. 1 Satz 1 TKG im Einzelfall angefordert werden und erforderlich sein müssen" (BVerfGE 130, 151, 205 f., Absatz-Nr. 177 f.). Es hat die "Erfordernis der Erforderlichkeit auch im Einzelfall" als Anforderung des Verhältnismäßigkeitsgrundsatzes eingeordnet (BVerfGE 130, 151, 200, Absatz-Nr. 163 a.E.). Weil die Beschränkung von Auskünften auf Einzelfälle fehlt, sind sie verfassungswidrig.

Es kann dabei letztlich offen bleiben, ob die Beschränkung auf Einzelfälle in der Öffnungsnorm des § 113 TKG oder aber in den fachspezifischen Abrufermächtigungen geregelt werden muss, denn sie ist an keiner der beiden Stellen verankert. Die neuen Erhebungsbefugnisse bestimmen

nicht, dass "Auskünfte ... im Einzelfall angefordert werden" müssen. Sie machen nicht eine "Erforderlichkeit auch im Einzelfall" zur Voraussetzung der Bestandsdatenerhebung. Zwar sollen die Anbieter Auskünfte nur erteilen dürfen, wenn sie "im Einzelfall ... verlangt" werden (§ 113 Abs. 2 TKG). Die Anbieter sind aber weder berechtigt noch in der Lage, zu prüfen, ob Auskünfte im Einzelfall erforderlich sind; sie führen nur eine formale Prüfung durch (vgl. § 113 Abs. 2 S. 3 und Abs. 5 S. 3 TKG). Die Bundesregierung meint in ihrer Gegenäußerung (http://dipbt.bundestag.de/dip21/btd/17/120/1712034.pdf#page=20 BT-Drs. 17/12034, 20])dass die Beschränkung auf Einzelfälle "nicht (mehr) in § 113 TKG geregelt werden kann", weil sie "nicht die Übermittlungspflicht des Telekommunikationsanbieters, sondern die Erhebungsbefugnis der Behörden" betrifft. In den eigentlichen Befugnisnormen fehlt die Voraussetzung einer "Erforderlichkeit auch im Einzelfall" jedoch ebenfalls.

3.1.2.3 Mangelndes Zitiergebot

§ 113 TKG verletzt das Verhältnismäßigkeitsgebot, indem er Telekommunikationsanbieter in unangemessen weit reichendem Umfang zur Herausgabe von Kommunikationsdaten ermächtigt, ohne spezifische Rechtsgrundlagen der Länder vorauszusetzen, die eine Auskunftsverpflichtung der Telekommunikationsunternehmen eigenständig begründen (BVerfGE 130, 151, 201 f., Absatz-Nr. 167).

Das Bundesverfassungsgericht hat festgestellt, dass für die Datenabfrage in Form eines unmittelbar an private Dritte gerichteten Auskunftsverlangens spezifische Rechtsgrundlagen erforderlich sind, die eine Auskunftsverpflichtung der Telekommunikationsunternehmen eigenständig begründen, während allgemeine Datenerhebungsbefugnisse nicht genügen (BVerfGE 130, 151, 202, Absatz-Nr. 168). § 113 Abs. 2 TKG fordert indes nur eine gesetzliche Bestimmung, die "eine Erhebung der in Absatz 1 in Bezug genommenen Daten erlaubt". Ihrem Wortlaut nach erlauben die allgemeinen Datenerhebungsbefugnisse die Erhebung sämtlicher personenbezogener Daten, auch von Bestandsdaten. Ferner öffnet § 113 Abs. 2 TKG den Zugriff auf Kommunikationsdaten auch auf Grund von Vorschriften zur Vernehmung von Zeugen oder zur Beschlagnahme/Sicherstellung von Daten.

Zwar hat das Bundesverfassungsgericht § 113 TKG im Wege der verfassungskonformen Auslegung entnommen, dass er spezifische Rechtsgrundlagen der Länder voraussetze, die eine Auskunftsverpflichtung der Telekommunikationsunternehmen eigenständig begründeten (BVerfGE 130, 151, 201 f., Absatz-Nr. 167). Nachdem der Gesetzgeber dies aber bei der Neuregelung wieder nicht zur Voraussetzung einer Übermittlungsbefugnis der Anbieter gemacht hat, ist eine solche Auslegung nicht mehr möglich. Sie wäre auch mit dem Gebot der Normenklarheit nicht vereinbar. Denn der - juristisch möglicherweise nicht vorgebildete - Rechtsanwender kann § 113 Abs. 2 S. 1 TKG nicht mit hinreichender Klarheit entnehmen, dass eine spezifische Rechtsgrundlage Voraussetzung eines Zugriffs ist. Dasselbe gilt für den Bürger, dessen Daten dem staatlichen Zugriff ausgesetzt werden. Verfehlt wird so auch die Forderung des Bundesverfassungsgerichts, es bedürfe "klarer Bestimmungen, gegenüber welchen Behörden die Anbieter konkret zur Datenübermittlung verpflichtet sein sollen" (BVerfGE 130, 151, 201 f., Absatz-Nr. 171).

Gegen eine einschränkende Auslegung spricht außerdem: Der Bundesgesetzgeber unterlässt es nicht nur, spezifische Rechtsgrundlagen, die eine Auskunftsverpflichtung der Telekommunikationsunternehmen eigenständig begründen, zur Voraussetzung von Datenübermittlungen zu machen. Er definiert selbst sogar geringere Voraussetzungen. Als Rechtsgrundlage lässt er in § 113 Abs. 2 S. 1 TKG ausdrücklich jede Norm genügen, die "eine Erhebung der in Absatz 1 in Bezug genommenen Daten erlaubt". Dagegen hat das

Bundesverfassungsgericht Rechtsgrundlagen gefordert, "die eine Auskunftsverpflichtung der Telekommunikationsunternehmen eigenständig begründen" (BVerfGE 130, 151, 201 f., Absatz-Nr. 167). Die allgemeinen Datenerhebungsbefugnisse begründen dagegen keine Auskunftsverpflichtung bezüglich der in § 113 TKG benannten Daten.

Der Bundesgesetzgeber ist verantwortlich dafür, die Bedingungen und Voraussetzungen einer Übermittlung von Kommunikationsdaten so zu regeln, dass die verfassungsrechtlichen Grenzen des staatlichen Datenzugriffs gewahrt bleiben (BVerfGE 130, 151, 186, Absatz-Nr. 129 und S. 192f. Absatz-Nr. 146) Er kann sich nicht darauf zurückziehen, dass die Länder ihrerseits eine abschließende Regelung treffen könnten (z.B. durch Verwendung des Wortes "nur"). Dies ergibt sich schon daraus, dass die Länder nicht verpflichtet sind, ihren Behörden einen Zugriff auf Bestandsdaten zu eröffnen. Man kann von einem Land, welches auf eine entsprechende Ermächtigung verzichtet, nicht verlangen, sämtliche Generalklauseln zur Datenerhebung, Aussagepflichten usw. dahin zu ändern, dass sie nicht für Kommunikationsdaten gelten sollten. Es ist Aufgabe des Bundesgesetzgebers, Kommunikationsdatenbestände nur für Auskunftsersuchen auf spezifischer Rechtsgrundlage zu öffnen.

Mittel der Wahl wäre dazu ein "einfachgesetzliches Zitiergebot", wie es in § 88 TKG und § 113b TKG vorgesehen ist. § 113 TKG darf die Erteilung von Auskünften nur auf der Grundlage von Gesetzen erlauben, die dies unter ausdrücklicher Bezugnahme auf § 113 TKG vorsehen. Nur durch ein Zitiergebot können die Anbieter, die Eingriffsbehörden und die Betroffenen zuverlässig erkennen, ob eine Norm "eine Erhebung der in Absatz 1 in Bezug genommenen Daten erlaubt". Der Innenausschuss des Bundestags ist vergeblich auf das Erfordernis eines Zitiergebots hingewiesen worden. (Stellungnahme des Arbeitskreises Vorratsdatenspeicherung vom 12.03.2013,
[https://www.bundestag.de/bundestag/ausschuesse17/a04/Anhoerungen/Anhoerung26/Stellungnahmen_weitere/Stellungnahme_02.pdf)

3.1.2.4 Ausufernde Identifizierung von Internetnutzern

Die Identifizierung von Internetnutzern stellt einen besonders schwerwiegenden Grundrechtseingriff dar, weil sie die personenbezogene Nachverfolgung des Inhalts der abgerufenen oder geschriebenen Texte und Daten im Internet erlaubt. Anders als Auskünfte über Rufnummerninhaber geht die Identifizierung von Internetnutzern mit einem Eingriff in das Grundrecht aus Art. 10 Abs. 1 GG einher.

Die Begründung von behördlichen Auskunftsansprüchen ermöglicht es in Verbindung mit der Speicherung der Internetzugangsdaten nach § 100 TKG in weitem Umfang, die Identität von Internetnutzern zu ermitteln. Auch ist die mögliche Persönlichkeitsrelevanz einer Abfrage des Inhabers einer IP-Adresse eine andere als die des Inhabers einer Telefonnummer: Schon vom Umfang der Kontakte her, die jeweils durch das Aufrufen von Internetseiten neu hergestellt werden, ist sie aussagekräftiger als eine Telefonnummernabfrage. Auch hat die Kenntnis einer Kontaktaufnahme mit einer Internetseite eine andere inhaltliche Bedeutung: Da der Inhalt von Internetseiten anders als das beim Telefongespräch gesprochene Wort elektronisch fixiert und länger wieder aufrufbar ist, lässt sich mit ihr vielfach verlässlich rekonstruieren, mit welchem Gegenstand sich der Kommunizierende auseinander gesetzt hat. Die Individualisierung der IP-Adresse als der „Telefonnummer des Internet“ gibt damit zugleich Auskunft über den Inhalt der Kommunikation. Die für das Telefongespräch geltende Unterscheidung von äußerlichen Verbindungsdaten und Gesprächsinhalten löst sich hier auf. Wird der Besucher einer bestimmten Internetseite mittels der Auskunft über eine IP-Adresse individualisiert, weiß man nicht nur, mit wem er Kontakt hatte, sondern kennt in der Regel auch den Inhalt des Kontakts (BVerfGE 125, 260, 342, Absatz-Nr. 259).

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 - so das Bundesverfassungsgericht ausdrücklich - nicht gleichgesetzt werden (BVerfGE 130, 151, 204, Absatz-Nr. 174).

Eben dies tut aber das Gesetz, und zwar sowohl in der Übermittlungsbefugnis nach § 113 TKG als auch in den fachspezifischen Datenerhebungsbefugnissen. Die "Deanonymisierung" der Internetnutzung im selben weit reichenden Umfang zuzulassen wie den Blick ins Telefonbuch ist nicht hinnehmbar. (Unabhängiges Landesdatenschutzzentrum vom 17.04.2013, https://www.datenschutzzentrum.de/polizei/20130417-anschreiben-tkg-bestandsdaten.pdf ; vgl. auch Stellungnahme vom März 2013 des Deutschen Anwaltvereins durch den Ausschuss Gefahrenabwehrrecht, http://anwaltverein.de/downloads/Stellungnahmen-11/DAV-SN17-13.pdf, 14) Zur Wahrung des Verhältnismäßigkeitsgebots muss zumindest eine Gleichstellung mit der Verwendung sonstiger Verkehrsdaten (§ 100g StPO) erfolgen, also im Bereich der Strafverfolgung eine richterliche Anordnung zur Voraussetzung gemacht werden (Ebenso: Unabhängiges Landesdatenschutzzentrum, Stellungnahme vom 27.11.2012, https://www.datenschutzzentrum.de/polizei/20121127-stellungnahme-tkg-aenderung.html, Ziff. II.4) und eine Beschränkung auf Straftaten von erheblichem Gewicht sowie auf Gefahren für wichtige Rechtsgüter erfolgen. Die aktuelle Privilegierung einer Internet-Zielwahlsuche anhand von IP-Adressen gegenüber einer Telefon-Zielwahlsuche (§ 100g StPO) ist sachlich nicht zu rechtfertigen. Es ist nicht plausibel zu machen, weshalb unbedeutende Verkehrsdaten zu schon bekannten Verbindungen (z.B. Datenvolumen, genaue Anrufdauer) einen besseren Schutz genießen sollen als die äußerst grundrechtsbedeutsame Identität eines noch unbekannten Internetnutzers.

Hiervon ausgehend ist § 113 Abs. 1 S. 3 TKG mit dem Verhältnismäßigkeitsgebot unvereinbar. Der Telekommunikationsgesetzgeber ist zur Gewährleistung des Datenschutzes und des Telekommunikationsgeheimnisses verantwortlich dafür, die Bedingungen und Voraussetzungen einer Übermittlung von Kommunikationsdaten so zu regeln, dass die verfassungsrechtlichen Grenzen des staatlichen Datenzugriffs gewahrt bleiben (BVerfGE 130, 151, 186, Absatz-Nr. 129; BVerfGE 130, 151, 192 f., Absatz-Nr. 146). Nach dem Wortlaut des § 113 TKG dürfen Anbieter Internetnutzer identifizieren, sobald eine in § 113 Abs. 3 TKG genannte Stelle dies in Textform im Einzelfall zum Zweck der Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Aufgaben der in § 113 Abs. 3 Nr. 3 TKG genannten Stellen unter Angabe einer gesetzlichen Bestimmung verlangt, die ihr eine Erhebung der Daten erlaubt. Dies geht weit über die Grenzen hinaus, die das Gesetz anderen Verkehrsdatenzugriffen setzt.

Die sehr weitreichenden Bedingungen, denen das Bundesverfassungsgericht IP-Auskünfte im Jahre 2010 unterworfen hat, sind durch die Neuregelung des Verfahrens zur Bestandsdatenauskunft nicht gewahrt. Das Gesetz erlaubt über § 46 OWiG i.V.m. § 100j StPO die Identifizierung von Internetnutzern zur Verfolgung von Ordnungswidrigkeiten jeder Art. Das erhebliche Gewicht des Eingriffs solcher Auskünfte erlaubt es indessen selbst nach der frühen Rechtsprechung des Bundesverfassungsgerichts nicht, diese allgemein und uneingeschränkt auch zur Verfolgung jedweder Ordnungswidrigkeiten zuzulassen. Die Aufhebung der Anonymität im Internet bedürfe zumindest einer Rechtsgutbeeinträchtigung, der von der Rechtsordnung auch sonst ein hervorgehobenes Gewicht beigemessen wird. Dies schließe entsprechende Auskünfte zur Verfolgung oder Verhinderung von Ordnungswidrigkeiten nicht vollständig aus. Es müsse sich insoweit aber um - auch im Einzelfall - besonders gewichtige Ordnungswidrigkeiten handeln, die der Gesetzgeber ausdrücklich benennen müsse (BVerfGE

125, 260, 344, Absatz-Nr. 262). Das Gesetz versäumt dies und verfehlt folglich auch insoweit die verfassungsrechtlichen Anforderungen. (Ebenso Unabhängiges Landesdatenschutzzentrum vom 27.11.2012, https://www.datenschutzzentrum.de/polizei/20121127-stellungnahme-tkg-aenderung.html, II.1.)

Das Urteil des Bundesverfassungsgerichts vom 2.3.2010 ist ungeachtet dessen einschlägig, dass die dortigen Ausführungen zu § 113 TKG im Zusammenhang mit der mittelbaren Nutzung anlasslos und flächendeckend erhobener Verkehrsdaten erfolgt sind. Auf diesen Umstand hat das Bundesverfassungsgericht bei Darstellung der für § 113 TKG maßgeblichen verfassungsrechtlichen Eingriffsgrenzen nicht abgestellt. Es hat umgekehrt Literatur zitiert, welche die Beauskunftung nicht auf Vorrat gespeicherter Daten behandelt (BVerfGE 125, 260, 344, Absatz-Nr. 261). Auch bei der Bestimmung der Eingriffstiefe hat das Gericht auf die Verwendungsmöglichkeiten der Daten abgestellt und nicht darauf, wie sie erhoben worden sind (BVerfGE 125, 260, 344, Absatz-Nr. 258 f.).

Entgegen der teilweise vertretenen Argumentation schließt § 46 Abs. 3 OWiG die Identifizierung von IP-Adressen zur Verfolgung von Ordnungswidrigkeiten nicht normenklar aus. Nach der Rechtsprechung des Bundesverfassungsgerichts sollen Auskunftsersuchen betreffend die Identität des Inhabers einer IP-Adresse keine Umstände, die dem Fernmeldegeheimnis unterliegen, zum Gegenstand haben. Einen Eingriff in das Fernmeldegeheimnis sieht das Gericht lediglich in der Auswertung von Verkehrsdaten durch den Anbieter zum Zweck der Auskunfterteilung (BVerfGE 130, 151, 181 f., Absatz-Nr. 116), nur diese Verkehrsdaten unterlägen dem Telekommunikationsgeheimnis. Gegenstand des Auskunftersuchens sind demgegenüber Bestandsdaten, welche nach der Rechtsprechung des Bundesverfassungsgerichts nicht dem Telekommunikationsgeheimnis unterliegen sollen.

3.1.2.5 Fehlende Beschränkung auf rechtmäßig gespeicherte Daten

Es ist unverhältnismäßig, dass § 113 Abs. 1 S. 4 TKG von den Anbietern zur Auskunfterteilung die Heranziehung "sämtlicher unternehmensinterner Datenquellen" fordert, weil dies auch rechtswidrig gespeicherte Daten einschließt.

Deutsche Internet-Zugangsanbieter speichern unter Verstoß gegen die §§ 96, 97 TKG verbreitet über das Ende der Verbindung hinaus tagelang auf Vorrat, welcher Anschlussinhaber wann unter welcher IP-Adresse das Internet genutzt hat. Von § 100 TKG ist diese anlassunabhängige Datenspeicherung nicht gedeckt (vgl.: Breyer, MMR 2011, 573) über entsprechende Unterlassungsklagen ist allerdings noch nicht rechtskräftig entschieden.

Wenn § 113 Abs. 1 S. 4 TKG zur Auskunfterteilung die Heranziehung "sämtlicher unternehmensinterner Datenquellen" fordert, sind davon dem Wortlaut nach auch rechtswidrig erhobene oder gespeicherte Daten erfasst. Erforderlich wäre die Klarstellung, dass Auskunft nur anhand rechtmäßig gespeicherter Daten erteilt werden darf. Speichert der Anbieter Daten rechtswidrig, darf er sie erst recht nicht weiter verarbeiten. Auch Eingriffsbehörden dürfen nach der Rechtsprechung auf rechtswidrige Beweismittel nur zugreifen, wenn das Beweisinteresse die schutzwürdigen Interessen des Betroffenen überwiegt. Im Bereich von Ordnungswidrigkeiten und sonstigen Bagatellfällen, für welche § 113 TKG die Datenbestände öffnet, ist ein solches Überwiegen keinesfalls anzunehmen.

Der Innenausschuss des Bundestags ist vergeblich auf das Erfordernis einer Klarstellung hingewiesen worden. (Stellungnahme des Arbeitskreises Vorratsdatenspeicherung vom 12.03.2013,
[https://www.bundestag.de/bundestag/ausschuesse17/a04/Anhoerungen/Anhoerung26/Stellungnahmen_weitere/Stellungnahme_02.pdf ADr. 17(4)686], 7)

3.1.2.6 Fehlender Schutz des Fernmeldegeheimnisses

Die Formulierung des § 113 TKG birgt die Gefahr, dass er zur Umgehung der Vorschriften über die Verkehrsdatenerhebung genutzt wird, indem offene Anfragen zu Anschlussinhabern gestellt werden, deren Telekommunikationsverbindungen nicht bekannt sind (z.B. "Wie lauten die Bestandsdaten des Anschlusses, über den am 01.01.2013 um 12.01 Uhr die Rufnummer ... angerufen worden ist?"). Das Bundesverfassungsgericht musste § 113 TKG a.F. verfassungskonform auslegen, um diese Gefahr auszuschließen, denn die Vorschrift bestimmt nicht, welche Angaben in Auskunftersuchen mindestens zu machen sind.

Der Gesetzgeber hat es indes seinem Prüfauftrag zuwider (BVerfGE 125, 260, 357, Absatz-Nr. 290) nicht nur versäumt, anzuordnen, dass die Verwendung von Verkehrsdaten zur Erteilung von Bestandsdatenauskünften nur im Fall der Identifizierung von IP-Adressen zulässig sei. Er hat sogar die bisherige Bestimmung des § 113 Abs. 1 S. 3 TKG gestrichen ("Ein Zugriff auf Daten, die dem Fernmeldegeheimnis unterliegen, ist nur unter den Voraussetzungen der hierfür einschlägigen gesetzlichen Vorschriften zulässig.") (Kritisch auch Wirtschaftsausschuss des Bundesrats, BR-Drs. 664/1/12, 3) und umgekehrt angeordnet, zur Auskunfterteilung müssten "sämtliche unternehmensinterne Datenquellen" - zu denen auch Verkehrs- und Inhaltsdaten gehören - herangezogen werden. Durch die undifferenzierte Beschränkung des Fernmeldegeheimnisses laut Artikel 9 des Gesetzes riskiert dies dahin verstanden zu werden, dass Auskünfte zu einzelnen Telekommunikationsvorgängen möglich werden. Tatsächlich ist § 113 TKG a.F. in diesem Sinne auch angewandt worden. Es kommt hinzu, dass es der Gesetzgeber trotz Mahnung im Gesetzgebungsverfahren (Stellungnahme des Arbeitskreises Vorratsdatenspeicherung vom 12.03.2013, [https://www.bundestag.de/bundestag/ausschuesse17/a04/Anhoerungen/Anhoerung26/Stellungnahmen_weitere/Stellungnahme_02.pdf ADr. 17(4)686], 9) abgelehnt hat, Abfragen betreffend einzelne Telekommunikationsvorgänge auszuschließen.

All dies schützt das Telekommunikationsgeheimnis nicht ausreichend und stellt folglich eine Verletzung des Art. 10 GG dar.

3.2 Die fachgesetzlichen Datenerhebungsvorschriften

3.2.1 Mangelnde Klarheit der Befugnisse zur Abfrage von Zugangssicherungscodes

Die gesetzlichen Voraussetzungen einer Anforderung von Zugangssicherungscodes (wie Passwörter, PIN oder PUK) sind in den fachgesetzlichen Datenerhebungsvorschriften nicht normenklar und präzise geregelt.

Zugangssicherungscodes sichern den Zugang zu Endgeräten und Speicherungseinrichtungen und damit die Betroffenen vor einem Zugriff auf äußerst sensible Inhalte. Die Herausgabe von Zugangssicherungscodes an Behörden nimmt Anbieter und Betroffenem die Kontrolle über Art und Umfang der durchgeführten Überwachung. Daher stellt die Verpflichtung von Anbietern zur Herausgabe von Zugangssicherungscodes einen besonders schwerwiegenden Grundrechtseingriff dar.

Das Bundesverfassungsgericht hat entschieden, dass Staatsbehörden PINs und Passwörter nur anfordern dürfen, wenn die gesetzlichen Voraussetzungen für ihre Nutzung gegeben sind. Der Gesetzgeber hat diese Formulierung einfach in das Gesetz übernommen, ohne selbst zu definieren, unter welchen Voraussetzungen er die Nutzung von Zugangssicherungscodes erlauben will. Was die "gesetzlichen Voraussetzungen für die Nutzung der Daten" sein sollen, erschließt sich weder dem Rechtsanwender noch dem betroffenen Bürger. Es gibt schlichtweg kein Gesetz, welches die Nutzung von Zugangssicherungscodes regelt. Zwar wendet die

Rechtsprechung auf diese Frage bestimmte allgemeine Normen an (z.B. Telekommunikationsüberwachung, Beschlagnahme). Dies entbindet den Gesetzgeber aber nicht von seiner Verpflichtung, die jetzt getroffene Regelung normenklar und präzise zu formulieren. Die Entscheidung des Hohen Gerichts, die Voraussetzungen der Datennutzung müssten vorliegen, war nicht als Gesetzestext gedacht, sondern bedarf der normenklaren Umsetzung durch den Gesetzgeber. Im Hinblick auf die extreme Sensibilität persönlicher Zugangskennungen muss die Regelung ein hohes Maß an Normenklarheit gewährleisten.

Verfassungsrechtlich verletzt die lapidare Bezugnahme auf "die gesetzlichen Voraussetzungen für die Nutzung der Daten" das Bestimmtheitsgebot (Ebenso Unabhängiges Landesdatenschutzzentrum, Stellungnahme vom 27.11.2012, https://www.datenschutzzentrum.de/polizei/20121127-stellungnahme-tkg-aenderung.html, Ziff. II.3. und Unabhängiges Landesdatenschutzzentrum vom 17.04.2013, https://www.datenschutzzentrum.de/polizei/20130417-anschreiben-tkg-bestandsdaten.pdf, 2; vgl. auch Stellungnahme vom März 2013 des Deutschen Anwaltvereins durch den Ausschuss Gefahrenabwehrrecht, http://anwaltverein.de/downloads/Stellungnahmen-11/DAV-SN17-13.pdf, 9). Sie ermöglicht weder der handelnden Behörde, noch dem verpflichteten Anbieter oder dem kontrollierenden Gericht, mit hinreichender Klarheit zu bestimmen, welche Voraussetzungen vorliegen müssen. Auch ist nicht gewährleistet, dass der Anbieter das Vorliegen der Zugriffsvoraussetzungen (z.B. richterliche Anordnung der Telekommunikationsüberwachung) anhand behördlich zur Verfügung gestellter Unterlagen kontrollieren kann. Wenn eine Behörde einen Zugriffscode anfordert, weiß der Anbieter nicht, ob dies zum Zweck der Telekommunikationsüberwachung oder zur Auswertung abgeschlossener Telekommunikation geschieht. Es ist nicht akzeptabel, die Kontrolle der gesetzlichen Voraussetzungen durch den Telekommunikationsanbieter bei der Anforderung von Zugriffscodes quasi ausfallen zu lassen, obwohl solche Codes besonders weitreichende und unkontrollierte Zugriffe ermöglichen.

Es ist aus diesen Gründen verfassungsrechtlich geboten, abschließend zu bestimmen, welche materiellen und formellen gesetzlichen Voraussetzungen für die Nutzung von Zugangscodes vorliegen müssen. Dass dies möglich ist, zeigt etwa die abschließende Regelung des § 180a Abs. 2 SH-LVwG.

3.2.2 Verletzung des Verhältnismäßigkeitsgebots

3.2.2.1 Mangelnde Kontrolle durch fehlende Statistik

Der Quick-Freeze-Referentenentwurf des Bundesjustizministeriums sah vor, dass eine Statistik über die Identifizierung von Internetnutzern geführt wird, damit der Gesetzgeber die Entwicklung der Fallzahlen beobachten kann (§ 100k Abs. 4 StPO-RefE) Registriert werden sollte auch Erfolg oder Misserfolg der Maßnahme. Eine solche verfahrensrechtliche Sicherung erscheint bei Bestandsdatenzugriffen allgemein geboten, damit der Gesetzgeber die Entwicklung seiner ausufernd weiten Blankobefugnis beobachten und sie gegebenenfalls wieder eindämmen kann. Besonders beobachtungsbedürftig ist die Nutzung der elektronischen Schnittstelle zum Datenaustausch, welche übrigens statistisch besonders leicht zu erfassen wäre.

Keine der fachgesetzlichen Abrufnormen in dem angefochtenen Gesetz sehen eine statistische Erfassung vor, obwohl der Datenzugriff erheblich ausgeweitet werden soll. Dies genügt dem Verhältnismäßigkeitsgebot nicht.

3.2.2.2 Fehlende Subsidiarität des Zugriffs auf Zugangssicherungscodes (PINs, Passwörter)

Zugangssicherungscodes ermöglichen den Zugriff auf äußerst sensible Inhalte der Telekommunikation und weitere persönliche Inhalte wie Fotos, Tagebücher und Dokumente. Mit ihrer Herausgabe an Staatsbeamte begibt sich der Anbieter der Kontrolle über ihre Verwendung. Der unmittelbare staatliche Fernzugriff auf Speichereinrichtungen (z.B. E-Mail-Postfächer) greift vor diesem Hintergrund weit tiefer ein als die Inanspruchnahme des Anbieters zur Erhebung gespeicherter Daten. Im Fall der Inpflichtnahme des Anbieters kann diesem die Herausgabe lediglich bestimmter Inhalte aufgegeben werden, ohne dass der Staat sämtliche Daten durchsehen muss. Die Inpflichtnahme des Anbieters kann auch zeitlich befristet werden, während im Fall eines unmittelbaren Staatszugriffs keine externe Kontrolle der zeitlichen Schranken durch den Anbieter erfolgen kann.

Vor diesem Hintergrund ist aus dem Verhältnismäßigkeitsgebot abzuleiten, dass der Staat Zugangssicherungscodes allenfalls dann erheben darf, wenn die damit bezweckte Datenerhebung auf andere Weise - insbesondere durch Inanspruchnahme des Anbieters - nicht erfolgen kann. In Anbetracht der Schwere des Grundrechteeingriffs hätte der Gesetzgeber eine entsprechende Subsidiaritätsklausel ausdrücklich aufnehmen müssen. Im Umkehrschluss zu den Subsidiaritätsklauseln der Strafprozessordnung ergibt sich nach der jetzigen Gesetzesfassung nämlich, dass keine Subsidiarität gewollt ist. (Gegen Subsidiarität auch Buermeyer, Stellungnahme 16/639, https://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMST16-639.pdf, 9) Dies wird dem empfindlichen Grundrechtseingriff nicht gerecht. Deswegen muss zur Wahrung des Verhältnismäßigkeitsgebots der Vorrang der Telekommunikationsüberwachung unter Mitwirkung des Anbieters vor dem unmittelbaren Zugriff mithilfe von Zugangssicherungscodes ausdrücklich festgeschrieben werden. In der Anhörung des Innenausschusses ist dies vergeblich gefordert worden.

3.2.2.3 Mangelnder Richtervorbehalt für Zugriff auf Zugangssicherungscodes (PINs, Passwörter)

Die Erhebung von Zugangssicherungscodes wie Passwörter zu E-Mail-Postfächern oder Speicherdiensten stellt einen tiefgreifenden Grundrechtseingriff dar, da sie der Schlüssel für die Nutzung weiterer Daten sind, die der Nutzer im Vertrauen auf den Zugangsschutz gespeichert hat. Die Herausgabe von Passwörtern ermöglicht den Zugriff auf Inhalte der Telekommunikation und weitere persönliche Inhalte wie Fotos, Tagebücher und Dokumente.

Um von einer unabhängigen Instanz überprüfen zu lassen, dass die gesetzlichen Voraussetzungen des Zugriffs auf diese hochsensiblen Daten vorliegen, muss eine richterliche Anordnung durchgängig zur Voraussetzung der Herausgabe von Passwörtern gemacht werden. Diese verfahrensrechtliche Sicherung ist aus dem Verhältnismäßigkeitsgebot abzuleiten.

Die fachgesetzlichen Abrufermächtigungen werden dieser Anforderung nur unzureichend gerecht. Wenn der Betroffene von einer beabsichtigten Passwortabfrage Kenntnis hat oder „haben muss“, ersetzt dies eine richterliche Prüfung der gesetzlichen Voraussetzungen des Zugriffs nicht. Die Kenntnis des Betroffenen hat mit der Erforderlichkeit einer richterlichen Anordnung nichts zu tun. Kein anderer Richtervorbehalt steht unter dem Vorbehalt einer Kenntnis durch den Betroffenen. Ebenso wenig ist einsichtig, warum die richterliche Anordnung einer Telekommunikationsüberwachung oder Handybeschlagnahme eine Entscheidung darüber entbehrlich machen soll, ob dazu die Anforderung eines Zugangssicherungscodes erforderlich ist. Oftmals ist eine Telekommunikationsüberwachung oder Auswertung eines Handyspeichers auch ohne Kenntnis von Passwörtern möglich. Über die Erforderlichkeit der Herausgabe persönlicher Zugangssicherungscodes muss aufgrund der Schwere des Grundrechtseingriffs der Richter entscheiden (vorbehaltlich Eilfällen).

3.2.2.4 Mangelnde Sicherheit erhobener Zugangssicherungscodes

Zu beanstanden ist ferner, dass das Gesetz keinerlei Vorkehrung zur Gewährleistung der Sicherheit erhobener Zugangssicherungscodes trifft. Es ist keine separate Aufbewahrung vorgesehen, kein besonderer Schutz vor Übermittlung von Codes oder ihrer Nutzung zu ganz anderen Zwecken (Zweckänderung) und keine Pflicht zu ihrer frühestmöglichen Vernichtung. Dies wird dem Verhältnismäßigkeitsgebot nicht gerecht.

3.2.2.5 Überschüssiger Zugriff auf Zugangssicherungscodes

§ 7 Abs. 3 S. 2 BKAG und § 7 Abs. 5 S. 2 ZFdG eröffnen BKA und ZKA als Zentralstellen den Zugang zu PINs und Passwörtern. Dies ist unzulässig, weil BKA und ZKA als Zentralstellen nicht zur Nutzung von Zugangssicherungscodes befugt sind. Als Zentralstellen dürfen BKA und ZKA keine Onlinedurchsuchung vornehmen, keine Telekommunikation überwachen und auch keine Datenträger sicherstellen, wie es Voraussetzung eines Zugriffs z.B. für die auf in einem Mobiltelefon gespeicherten Daten wäre.

3.2.2.6 Unzureichende Eingriffsschwellen für BKA, ZKA und Bundespolizei

§ 7 Abs. 3 und 4 BKAG, § 20b Abs. 3 und 4 BKAG, § 22 Abs. 2 und 3 BKAG, § 22a BPolG, § 7 Abs. 5 und 6 ZFdG sowie § 15 Abs. 2 und 3 ZFdG sind ihrer Ausgestaltung nach verfassungswidrig. (Ebenso Bäcker, Stellungnahme gegenüber dem Innenausschuss des Bundestags vom 8. März 2013,
[https://www.bundestag.de/bundestag/ausschuesse17/a04/Anhoerungen/Anhoerung26/Stellungnahmen_SV/Stellungnahme_03.pdf ADrs. 17(4)680 C], 6; vgl. auch Wirtschaftsausschuss des Bundesrats, BR-Drs. 664/1/12, 3; Stellungnahme vom März 2013 des Deutschen Anwaltvereins durch den Ausschuss Gefahrenabwehrrecht,
http://anwaltverein.de/downloads/Stellungnahmen-11/DAV-SN17-13.pdf, 16 f.)

Im Bereich der Gefahrenabwehr ist eine konkrete Gefahr und im Bereich der Strafverfolgung der Verdacht einer Straftat (Anfangsverdacht) Mindestvoraussetzung einer verhältnismäßigen staatlichen Bestandsdatenerhebung (BVerfGE 130, 151, 205 f., Absatz-Nr. 177). Die genannten Normen bestimmen aber weder selbst noch durch normenklare Verweisung, dass BKA, Bundespolizei und ZKA Bestandsdaten nur zur Abwehr einer konkreten Gefahr oder zur Aufklärung eines Tatverdachts erheben dürfen.

Zwar dürfen TK-Anbieter Auskünfte an BKA, Bundespolizei und ZKA gemäß § 113 Abs. 2 TKG nur erteilen, wenn diese es "zum Zweck der Verfolgung von Straftaten oder Ordnungswidrigkeiten" oder "zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung" verlangen. Der Anbieter kann und darf diese materielle Frage jedoch nicht prüfen (§ 113 Abs. 2 S. 3 TKG). Auch die Bundesregierung bestätigte in ihrer Stellungnahme im Gesetzgebungsverfahren (vgl.: [http://dipbt.bundestag.de/dip21/btd/17/120/1712034.pdf#page=20 Gegenäußerung]), dass die materielle Eingrenzung "nicht (mehr) in § 113 TKG geregelt werden kann", weil sie "nicht die Übermittlungspflicht des Telekommunikationsanbieters, sondern die Erhebungsbefugnis der Behörden" betrifft. Die Befugnisnorm des § 7 BKAG aber lässt ausdrücklich eine Erforderlichkeit der Datenerhebung "zur Erfüllung der Aufgabe des Bundeskriminalamtes als Zentralstelle nach § 2 Absatz 2 Nummer 1" genügen; zu diesen Aufgaben zählen nicht nur die Aufklärung des Verdachts einer Straftat oder Ordnungswidrigkeit und die Abwehr konkreter Gefahren. Ebenso verhält es sich mit den übrigen genannten Normen. Eine so weitreichende Öffnung für das gesamte Feld der Aufgabenerfüllung verletzt das Verhältnismäßigkeitsgebot grob.

3.2.2.7 Unzureichende Eingriffsschwellen für Nachrichtendienste

Das Bundesverfassungsgericht leitet aus dem Verhältnismäßigkeitsgebot ab, Auskünfte an Nachrichtendienste müssten zur Aufklärung einer bestimmten, nachrichtendienstlich

beobachtungsbedürftigen Aktion oder Gruppierung geboten sein (BVerfGE 130, 151, 205 f., Absatz-Nr. 177). § 8d BVerfSchG, § 2b BNDG und § 4b MADG setzen dies nicht um, sondern lassen die Erforderlichkeit zur Aufgabenerfüllung genügen. Dies verletzt das Verhältnismäßigkeitsgebot.

3.2.2.8 Unzureichende Eingriffsschwellen für Identifizierung von IP-Adressen

Sämtliche fachgesetzlichen Ermächtigungen zur Identifizierung von IP-Adressen verletzen das Verhältnismäßigkeitsgebot, weil diese eingriffsintensive Maßnahme unter denselben weit reichenden Voraussetzungen zugelassen wird wie "einfache" Bestandsdatenabfragen. Zu § 113 TKG ist bereits ausgeführt worden, dass diese Gleichsetzung unzulässig ist (ebenso Unabhängiges Landesdatenschutzzentrum, Stellungnahme vom 27.11.2012, https://www.datenschutzzentrum.de/polizei/20121127-stellungnahme-tkg-aenderung.html, Ziff. II.2.) und dieselben Anforderungen gestellt werden müssen wie an sonstige Eingriffe in das Fernmeldegeheimnis.

Im Fall von § 8d BVerfSchG, § 2b BNDG und § 4b MADG ist nicht einmal die frühe Rechtsprechung des Bundesverfassungsgerichts beachtet worden, wonach Nachrichtendiensten die Identifizierung von Internetnutzern nur erlaubt werden dürfe, wenn aufgrund tatsächlicher Anhaltspunkte von dem Vorliegen einer konkreten Gefahr auszugehen sei. Die rechtlichen und tatsächlichen Grundlagen entsprechender Auskunftsbegehren seien aktenkundig zu machen (BVerfGE 125, 260, 343 f., Absatz-Nr. 261). § 8d BVerfSchG, § 2b BNDG und § 4b MADG bestimmen weder selbst noch durch normenklare Verweisung, dass die Nachrichtendienste Internetnutzer nur identifizieren dürfen, wenn aufgrund tatsächlicher Anhaltspunkte von dem Vorliegen einer konkreten Gefahr auszugehen ist. Auch bestimmen sie nicht, dass tatsächliche Grundlagen aktenkundig zu machen sind.

3.2.2.9 Exzessive Einschränkung des Fernmeldegeheimnisses

Es ist unverhältnismäßig, dass das angefochtene Gesetz das Fernmeldegeheimnis über die Identifizierung von IP-Adressen hinaus einschränkt.

§ 70 Satz 1 BPolG bestimmt nunmehr, das Fernmeldegeheimnis werde "nach Maßgabe dieses Gesetzes eingeschränkt". In Artikel 9 heißt es, durch die Artikel 1 bis 8 des Gesetzes werde das Fernmeldegeheimnis (Artikel 10 des Grundgesetzes) eingeschränkt. Diese Grundrechtsbeschränkungen sind exzessiv. Der Gesetzgeber hat es (anders als in § 8d BVerfSchG, § 2b BNDG und § 4b MADG) versäumt, die Beschränkung des Telekommunikationsgeheimnisses auf die Identifizierung von IP-Adressen zu beschränken. Ohne diese Beschränkung kann auch anderen Normen die Befugnis zu Eingriffen in das Fernmeldegeheimnis entnommen werden, beispielsweise sämtlichen Befugnissen der Bundespolizei (z.B. Befragung, Sicherstellung). Dies wird dem Verhältnismäßigkeitsgebot nicht gerecht. Der Gesetzgeber muss die Beschränkung des Fernmeldegeheimnisses auf diejenigen Normen begrenzen, die den Anforderungen des Fernmeldegeheimnisses gerecht werden.

Starostik

-Rechtsanwalt-