

2. V. 13.11.17

ULD



ULD · Postfach 71 16 · 24171 Kiel

Bundesverfassungsgericht  
Erster Senat  
Der Vorsitzende  
Schlossbezirk 3  
76006 Karlsruhe



vorab per Fax:

0721 9101-382

Holstenstraße 98  
24103 Kiel  
Tel.: 0431 988-1200  
Fax: 0431 988-1223  
Ansprechpartner/in:  
Barbara Körffer  
Durchwahl: 988-1216  
Aktenzeichen:  
LDi.V.-74.03/99.118

Kiel, 30. Oktober 2017

**Verfassungsbeschwerde 1 BvR 1732/14 gegen § 180a des Allgemeinen Verwaltungsgesetzes für das Land Schleswig-Holstein (Landesverwaltungsgesetz – LVwG) sowie § 8a Abs. 1 des Schleswig-Holsteinischen Landesverfassungsschutzgesetzes und gegen § 15 Abs. 5 S. 4 des Telemediengesetzes**  
Ihre Schreiben vom 26. April und vom 25. Juli 2017

Sehr geehrter Herr Vorsitzender,  
sehr geehrte Damen und Herren,

wir bedanken uns für die Übersendung der Verfassungsbeschwerde und die Gelegenheit zur Stellungnahme. Da das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) im Gesetzgebungsverfahren beteiligt war und gegenüber der Landesregierung sowie im parlamentarischen Verfahren Stellungnahmen hierzu abgegeben hat, nehmen wir die Gelegenheit zur Stellungnahme gern wahr, soweit die Verfassungsbeschwerde Vorschriften des Landesrechts berührt.

Im Einzelnen ist aus unserer Sicht zu den mit der Verfassungsbeschwerde angegriffenen Vorschriften Folgendes anzumerken:

#### **I. Zu § 180a, 180b des Landesverwaltungsgesetzes**

Die Vorschriften regeln die Voraussetzungen und das Verfahren für eine Abfrage von Bestandsdaten der Telekommunikation durch die Polizei zum Zweck der Gefahrenabwehr.

28 ✓

### 1. Zu 3.1.1 Eingriffsschwelle der „bevorstehenden Gefahr“

Die Beschwerdeführer rügen eine Verletzung des Gebots der Normenklarheit und Verhältnismäßigkeit, soweit die Vorschriften die Maßnahme „zur Abwehr einer im einzelnen Falle **bevorstehenden Gefahr** für die öffentliche Sicherheit“ erlaubt. Dies sei keine konkrete Gefahr, wie sie das Bundesverfassungsgericht für eine Bestandsdatenauskunft fordere, sondern vielmehr verlagere der Begriff der bevorstehenden Gefahr die Maßnahme in das Vorfeld einer Gefahr.

Dieser Gefahrenbegriff wird im Landesverwaltungsgesetz durchgängig als Bezeichnung für die konkrete Gefahr verwendet. Dass eine konkrete Gefahr gemeint ist, ergibt sich im Zusammenhang mit der Gesetzesbegründung, in der dieser Begriff wie folgt beschrieben wird:

*„Eine im einzelnen Falle bevorstehende Gefahr als Umschreibung der sog. konkreten Gefahr, wonach in absehbarer Zeit ein die öffentliche Sicherheit schädigendes Ereignis mit hinreichender Wahrscheinlichkeit eintreten wird“ (zitiert nach Schipper in: Schipper/Bock/Brenneisen/Schneider/Wilksen, Polizei- und Ordnungsrecht in Schleswig-Holstein, 4. Auflage, Rn. 34).*

Nach dieser Auslegung erfüllt der Gefahrenbegriff die Anforderungen an eine verhältnismäßige Schwelle für Bestandsdatenabfragen (BVerfG, Beschluss vom 24.1.2012 – 1 BvR 1299/05 Rn. 177)

### 2. Zu 3.1.2 Fehlende Beschränkung von Auskunftersuchen auf Einzelfälle

Die Beschwerdeführer rügen zudem, dass § 180a Abs. 1 LVwG **keine Beschränkung der Abfragen auf Einzelfälle** vorsieht. Zwar beschränkt § 180a Abs. 1 LVwG die Bestandsdatenabfrage auf Gefahrensituationen im Einzelfall. Die Vorschrift lässt in diesen Einzelfällen aber Gruppenauskünfte bzw. Auskünfte zu mehreren Anschlüssen und Anschlussinhabern zu und beschränkt die Ermächtigung nicht auf Einzelabfragen zu bestimmten Anschlüssen. Eine solche Beschränkung auf einzelne Anschlüsse ist nach unserer Auffassung verfassungsrechtlich nicht geboten; erforderlich und ausreichend ist nach unserem Verständnis vielmehr, dass eine Gefahr im Einzelfall vorliegt (BVerfG, Beschluss vom 24.1.2012 Rn. 177). Die Maßstäbe der Erforderlichkeit und Angemessenheit für die Abwehr der konkreten Gefahr sind nach § 180a Abs. 1 LVwG für jeden von der Bestandsdatenabfrage erfassten Anschluss bzw. Anschlussinhaber zu prüfen.

### 3. Zu 3.1.3 Fehlende Beschränkung auf Störer

Die Beschwerdeführer rügen, dass Bestandsdatenabfragen nach § 180a Abs. 1 LVwG sowie auch Abfragen von Zugriffssicherungscode nach § 180a Abs. 2 Satz 1 LVwG und Inhabern von IP-Adressen nach § 180a Abs. 2 S. 2 LVwG nicht auf Störer beschränkt sind.

Im Hinblick auf **Bestandsdatenabfragen** hat das Bundesverfassungsgericht die Eingriffsschwellen in § 113 Abs. 1 TKG a.F., die ebenfalls an die Schwelle der konkreten Gefahr für die öffentliche Sicherheit geknüpft und nicht auf Störer beschränkt waren, als „verfassungsrechtlich noch hinnehmbar“ angesehen (BVerfG, Beschluss vom 24.1.2017 Rn. 177 f.)

Hinsichtlich der **Abfrage von Zugriffssicherungs-codes** wird eine Beschränkung dadurch erreicht, dass den abfragenden Stellen auch der Zugriff auf die mit den Codes gesicherten Geräte erlaubt sein muss. § 180a Abs. 2 Satz 1 LVwG verweist hierfür auf die Voraussetzungen für die Telekommunikationsüberwachung, die in § 185a LVwG normiert sind, und alternativ auf die Voraussetzungen des § 210 LVwG für die Sicherstellung von Gegenständen. Es ist nicht ersichtlich und von den Beschwerdeführern auch nicht dargetan, dass die in Bezug genommenen Eingriffsermächtigungen nicht den verfassungsrechtlichen Anforderungen genügen.

Durch die Bezugnahme auf § 185a LVwG werden die auf diese Eingriffsermächtigung gestützten Abfragen auf Störer beschränkt. Denn § 185a Abs. 1 Satz 2 LVwG verweist auf § 185 Abs. 2 Satz 2 LVwG. Letzterer beschränkt die Zulässigkeit von Maßnahmen auf Personen, bei denen Tatsachen dafür sprechen, dass sie „als Verantwortliche in Anspruch genommen werden können“. Die Inanspruchnahme anderer Personen im Sinne des § 220 LVwG ist damit ausgeschlossen.

Für die Eingriffsschwelle der Sicherstellung nach § 210 LVwG ist eine Beschränkung auf Verantwortliche im Sinne der §§ 218 und 219 LVwG gesetzlich nicht festgelegt. Nach unserem Verständnis ist eine solche Beschränkung verfassungsrechtlich nicht zwingend erforderlich. Das Bundesverfassungsgericht hat eine Anknüpfung der Voraussetzungen für die Abfrage von Zugriffssicherungs-codes an die Voraussetzungen für den Zugriff auf die Daten selbst geknüpft (BVerfG, Beschluss vom 24.1.2012 Rn. 185). Sofern die Befugnis für den Zugriff auf die Daten auch für Dritte gilt, ist aus der Rechtsprechung des Bundesverfassungsgerichts kein Erfordernis erkennbar, die Abfrage von Zugriffssicherungs-codes weiter einzuschränken.

Für das **Auskunftersuchen über Inhaber von IP-Adressen** fehlt eine Beschränkung auf Störer ebenfalls. Hier könnte eine solche Beschränkung durchaus angebracht sein. Das ULD hat in seinen Stellungnahmen im Gesetzgebungsverfahren stets darauf hingewiesen, dass eine deutliche Unterscheidung der Eingriffsschwellen für die reine Bestandsdatenauskunft und die Bestandsdatenauskunft unter Nutzung von dynamischen IP-Adressen erforderlich ist. Dem ist der Gesetzgeber schließlich, entsprechend dem Vorschlag des ULD, durch eine Anhebung der Gefahrenschwelle in § 180a Abs. 2 Satz 2 LVwG gefolgt. Eine Beschränkung auf Störer würde die Schwelle nochmals anheben. Inwieweit ein fachlicher Bedarf dafür besteht, auch Dritte im Sinne des § 220 LVwG mithilfe einer Bestandsdatenabfrage unter Nutzung ihrer IP-Adresse ermitteln zu können, kann von hier aus nicht beurteilt werden. Nähere Kenntnisse über solchen fachlichen Bedarf wären aber erforderlich, um einschätzen zu können, ob der Adressatenkreis der Maßnahme so weitreichend sein muss, wie er in § 180a Abs. 2 Satz 2 LVwG definiert ist, oder ob aus Gründen der Verhältnismäßigkeit Einschränkungen geboten sind.

#### **4. Zu 3.1.4 Fehlende Benachrichtigung**

Die Beschwerdeführer rügen das Fehlen einer Benachrichtigungspflicht für die Erhebung von Bestandsdaten nach § 180a Abs. 1 LVwG. Für die eingriffsintensiveren Maßnahmen des § 180a Abs. 2 LVwG ist in § 180b Abs. 1 Satz 8 ff. LVwG eine Benachrichtigung vorgesehen. Angesichts der verhältnismäßig geringen Eingriffsintensität, die das Bundesverfassungsgericht der Bestandsdatenabfrage zugemessen hat (BVerfG, Beschluss vom 24.1.2012 Rn. 177, 187) dürfte eine Benachrichtigung verfassungsrechtlich nicht zwingend geboten sein.

### **5. Zu 3.1.5 Mangelnde Kontrolle durch fehlende Statistik**

Eine statistische Erfassung der Anwendung der neu eingeführten Vorschriften hatte das ULD im Gesetzgebungsverfahren empfohlen, damit nachträglich die Inanspruchnahme dieser neuen Befugnisse überprüft und evaluiert werden kann (siehe Stellungnahme vom 31. Mai 2013, LT-Umdruck 18/1245). Ob eine solche Statistik verfassungsrechtlich zwingend geboten ist, ist unseres Erachtens angesichts der verhältnismäßig geringen Eingriffsintensität, die das Bundesverfassungsgericht den Maßnahmen zugemessen hat (BVerfG, Beschluss vom 24.1.2012 Rn. 177, 187), fraglich.

### **6. Zu 3.1.6 Fehlende Subsidiarität des Zugriffs auf Zugangssicherungscodes**

Die Beschwerdeführer rügen, dass das Gesetz für den Zugriff auf Zugangssicherungscodes keine ausdrückliche Subsidiarität in der Weise vorsieht, dass „der Staat Zugangssicherungscodes allenfalls dann erheben darf, wenn dies damit bezweckte Datenerhebung auf andere Weise - insbesondere durch Inanspruchnahme des Anbieters – nicht erfolgen kann“. Eine mildere Maßnahme sei das Auskunftersuchen beim Anbieter über bestimmte eingegrenzte Daten. Dies ist nachvollziehbar. Die Beschwerdeführer gehen jedoch nicht darauf ein, dass es für den Zugriff auf die gesicherten Daten eigene Ermächtigungsnormen gibt, auf die § 180a Abs. 2 Satz 1 LVwG verweist und die ihrerseits zum Teil Subsidiaritätsklauseln enthalten. Die in der Verfassungsbeschwerde angesprochene Frage der Subsidiarität ist daher eher eine Frage der Eingriffsschwelle für den Zugriff auf die Daten – der durch die angegriffenen Vorschriften nicht geregelt wird – als für die Abfrage der Zugangssicherungscodes.

### **7. Zu 3.1.7 Mangelnde Sicherheit erhobener Zugangssicherungscodes**

Für die Sicherung der Zugangssicherungscodes bei den Polizeibehörden gelten die allgemeinen Anforderungen aus §§ 5 ff. des Landesdatenschutzgesetzes an die Gewährleistung der Datensicherheit. Diese Vorgaben gelten für alle öffentlichen Stellen des Landes gleichermaßen, also auch für die Polizei. Maßstab für die Anforderungen an die zu ergreifenden Maßnahmen ist jeweils der Schutzbedarf der Daten. Damit legt auch das allgemeine Recht für besonders schutzwürdige Daten hohe Anforderungen an Sicherungsmaßnahmen fest. Es ist kein Grund ersichtlich, warum für die Sicherung von Zugangssicherungscodes bereichsspezifisch spezielle Anforderungen geregelt werden sollten. Vielmehr wäre zu befürchten, dass für andere Daten, für die keine bereichsspezifischen Sicherungsmaßnahmen vorgesehen sind, der Umkehrschluss gezogen wird, dass für diese kein besonderer Schutz erforderlich ist.

### **8. Zu 3.1.8 Ausufernde Identifizierung von Internetnutzern**

Die Beschwerdeführer halten für Auskunftersuchen unter Verwendung von IP-Adressen, die der Identifizierung von Internetnutzern dienen, höhere Eingriffsschwellen und Verfahrenssicherungen für geboten. Dies hat unter Bezugnahme auf die Rechtsprechung des Bundesverfassungsgerichts und in Anbetracht des Eingriffs in Artikel 10 GG (BVerfG, Urteil vom 2. März 2010 – 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 - Rn. 254 ff.; BVerfG, Beschluss vom 24.1.2012 Rn. 173) auch das ULD im Gesetzgebungsverfahren gefordert (Stellungnahme vom 31. Mai 2013, LT-Umdruck 18/1245). Die Voraussetzungen des § 180a Abs. 2 Satz 2 LVwG stehen nach unserer Auffassung nunmehr mit diesen Anforderungen im Einklang. Nach der

Rechtsprechung des Bundesverfassungsgerichts ist die Auskunft über die Identität von Internetnutzern weder mit der reinen Bestandsdatenabfrage noch mit der Verkehrsdatenabfrage gleichzusetzen (BVerfG, Urteil vom 2.3.2010 Rn. 254 ff.). Nach dieser Rechtsprechung „darf der Gesetzgeber solche Auskünfte auch unabhängig von begrenzenden Rechtsgüter- und Straftatenkatalogen für die Verfolgung von Straftaten, für die Gefahrenabwehr und die Aufgabenwahrnehmung der Nachrichtendienste auf der Grundlage der allgemeinen fachrechtlichen Eingriffsermächtigungen zulassen“ (BVerfG, Urteil vom 2.3.2010 Rn. 261). Auch ein Richtervorbehalt ist danach nicht erforderlich. Über diese Maßstäbe geht die Eingriffsermächtigung im LVwG hinaus, indem sie die materielle Eingriffsschwelle auf den Schutz bestimmter Rechtsgüter beschränkt und als Verfahrenssicherung in § 180b LVwG einen Richtervorbehalt sowie eine Benachrichtigungspflicht vorsieht.

## **9. Zu 3.1.9 Soziale Netzwerke und Internetdienste (Telemedien)**

Die Beschwerde rügt außerdem § 180a Abs. 4 LVwG, der die Abfrage von Daten bei Telemedien-Diensteanbietern erlaubt. Zutreffend weisen die Beschwerdeführer darauf hin, dass Bestandsdaten über Telemediendienste aufgrund ihres weitaus größeren Aussagegehalts nicht mit Bestandsdaten über Telekommunikationsdienste gleichgesetzt werden können (vgl. auch die Stellungnahme des ULD vom 31. Mai 2013, LT-Umdruck 18/1245). Dem trägt § 180a Abs. 4 LVwG Rechnung, indem er höhere Eingriffsschwellen als § 180a Abs. 1 LVwG und zudem nach § 180b Abs. 2 LVwG Verfahrenssicherungen wie Richtervorbehalt und Benachrichtigungspflichten vorsieht.

Es ist jedoch fraglich, ob diese Einschränkungen verfassungsrechtlich ausreichend sind. Zum einen erfasst § 180a Abs. 4 LVwG nicht nur Telemedien-Bestandsdaten, sondern auch Telemedien-Nutzungsdaten nach § 15 TMG. Die Intensität dieses Eingriffs dürfte insoweit die der in § 180a Abs. 1 und 2 LVwG vorgesehenen Eingriffe sowie der Abfrage von Telemedien-Bestandsdaten übersteigen. Fraglich ist, ob hierfür nicht auch entsprechend höhere Eingriffsschwellen vorgesehen werden müssten (so die Stellungnahme des ULD vom 31. Mai 2013, LT-Umdruck 18/1245; insgesamt kritisch zur Einbeziehung von Telemediendaten die Stellungnahme der Neuen Richtervereinigung vom 3. Juni 2013, LT-Umdruck 18/1250). Es ist zum anderen auch fraglich, ob die Regelungen des Telemediengesetzes - die im Sinne der Rechtsprechung des Bundesverfassungsgerichts eine der Türen im Doppeltürenmodell darstellen - insoweit den Anforderungen der Rechtsprechung des Bundesverfassungsgerichts entsprechen. Dies gilt insbesondere für die Auskunft über Telemedien-Nutzungsdaten, die in § 15 TMG nicht geregelt ist. Schließlich ist auch fraglich, ob den schutzwürdigen Interessen der Betroffenen ausreichend Rechnung getragen wird, soweit die Nutzung von Telemedien Aufschluss über besondere Arten personenbezogener Daten im Sinne des § 11 Abs. 3 des Landesdatenschutzgesetzes geben, insbesondere wenn Telemedien genutzt werden, die von Berufsgeheimnisträgern angeboten werden.

## **II. Zu § 8a Landesverfassungsschutzgesetz (LVerfSchG)**

### **1. Zu 3.2.1 und 3.2.2. Eingriffsschwelle der Erforderlichkeit zur Aufgabenerfüllung und Fehlende Beschränkung auf Einzelfälle**

Die Beschwerdeführer rügen wie auch bei der Befugnis zur Bestandsdatenabfrage in § 180a Abs. 1 LVwG eine fehlende Beschränkung auf Einzelabfragen (dazu bereits oben zu 3.1.2).

Nach unserem Verständnis entspricht die Befugnis für die Verfassungsschutzbehörde zur Abfrage von Telekommunikations-Bestandsdaten denjenigen Voraussetzungen, die das Bundesverfassungsgericht in seiner Entscheidung vom 24.1.2012 (Rn. 177) als „verfassungsrechtlich noch hinnehmbar“ (Rn. 178) akzeptiert hat.

## **2. Zu 3.2.3 Fehlende Beschränkung auf Störer**

Die Verfassungsbeschwerde hält eine Beschränkung der Bestandsdatenabfrage auf Zielpersonen im Sinne des § 6 Abs. 3 Satz 2 Nr. 1 LVerfSchG für verfassungsrechtlich geboten. Das Bundesverfassungsgericht hat für die Bestandsdatenabfrage zur polizeilichen Gefahrenabwehr hingegen Eingriffsschwellen akzeptiert, die „nicht von vornherein auf Polizeipflichtige im Sinne des allgemeinen Polizei- und Ordnungsrechts“ beschränkt war, solange sich eine Begrenzung der Eingriffsbefugnis aus anderen Merkmalen ergibt (BVerfG, Beschluss vom 24.1.2012 Rn. 177). Solche anderen eingriffsbeschränkenden Voraussetzungen im Sinne dieser Entscheidung dürften sich aus der Erforderlichkeit im Einzelfall in § 8a Abs. 1 Satz 2 LVerfSchG und aus der Anknüpfung an die in § 5 LVerfSchG definierten Aufgaben der Verfassungsschutzbehörde ergeben. Somit entsprechen die Voraussetzungen auch insoweit denjenigen, die das Bundesverfassungsgericht in der genannten Entscheidung als „verfassungsrechtlich noch hinnehmbar“ (Rn. 178) akzeptiert hat.

## **3. Zu 3.2.4 Mangelnder Rechtsschutz wegen fehlender Benachrichtigung**

Soweit die Beschwerdeführer die fehlende Benachrichtigungspflicht für die Bestandsdatenauskunft rügen, gelten die obigen Ausführungen zum LVwG entsprechend (siehe oben zu 3.1.4).

## **4. Zu 3.2.5 Mangelnde Kontrolle durch fehlende Statistik**

Soweit die Beschwerdeführer die fehlende Statistikpflicht für die Bestandsdatenauskunft rügen, gelten die obigen Ausführungen zum LVwG entsprechend (siehe oben zu 3.1.5).

## **5. Zu 3.2.6 Mangelnde Klarheit der Befugnisse zur Abfrage von Zugangssicherungs-codes**

Die von den Beschwerdeführern vorgebrachte Kritik an dem pauschalen Verweis auf die „gesetzlichen Voraussetzungen für eine Nutzung der Daten“, ohne dass diese Voraussetzungen genannt werden oder sonst aus dem Gesetz selbst erkennbar wird, in welchen anderen Vorschriften diese Voraussetzungen geregelt sind, hat auch das ULD im Anhörungsverfahren gegenüber dem Innen- und Rechtsausschuss des Schleswig-Holsteinischen Landtages geäußert (Stellungnahme des ULD vom 31. Mai 2013, LT-Umdruck 18/1245).

Zugangssicherungs-codes wie PIN/PUK oder Passwörter weisen gegenüber den Bestandsdaten einen höheren Schutzbedarf auf. Diese Daten schützen den Zugang zu Endgeräten und Speichereinrichtungen und damit die Betroffenen vor einem Zugriff auf die entsprechenden Telekommunikationsvorgänge und Inhaltsdaten. Daher sind erhöhte Anforderungen an eine präzise und normenklare Beschränkung der Auskunftersuchen zu stellen.

Durch die Formulierung „darf die Auskunft nur verlangt werden, wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen“ werden die Anforderungen nicht erfüllt. Der Entwurf übernimmt hier die vom Bundesverfassungsgericht in der Entscheidung vom 24.1.2012 (Rn. 185) abstrakt formulierten Anforderungen, ohne dass eine spezifische Prüfung erkennbar ist. An dieser Stelle ist aus unserer Sicht der Gesetzgeber aufgefordert, abschließend zu prüfen und festzulegen, für welche Zwecke und unter welchen Voraussetzungen die zugangsgeschützten Inhaltsdaten durch die Verfassungsschutzbehörde genutzt werden dürfen. Diese Zwecke und Voraussetzungen müssen - wie in § 180a Abs. 2 Satz 1 LVwG - als Eingriffsschwelle für Auskunftersuchen über die Zugangssicherungs\_codes festgelegt werden. Gerade für die Nutzung der Inhaltsdaten durch die Verfassungsschutzbehörde ist eine Präzisierung erforderlich, da es sich nicht ohne weiteres erschließt, unter welchen Voraussetzungen die Verfassungsschutzbehörde Besitz an Endgeräten erlangen und die darauf gespeicherten Daten nutzen darf. Dies wird nicht einmal in der Entwurfsbegründung (LT-Drs. 18/713) erläutert.

Es ist aus unserer Sicht daher zweifelhaft, ob § 8a Abs. 1 Satz 3 LVerfSchG den verfassungsrechtlichen Ansprüchen an die Normenklarheit und Bestimmtheit genügt.

#### **6. Zu 3.2.7 Fehlende Subsidiarität des Zugriffs auf Zugangssicherungs\_codes**

Hinsichtlich der Frage der Subsidiarität von Abfragen über Zugangssicherungs\_codes gegenüber Anfragen über Inhalts- und Verkehrsdaten an die Diensteanbieter gelten die obigen Ausführungen (zu 3.1.6) entsprechend. Allerdings gilt dies hier mit der Einschränkung, dass eine Prüfung der in Bezug genommenen Voraussetzungen für den tatsächlichen Zugriff auf die Daten nicht möglich ist, da diese im Gesetz nicht genannt werden (siehe oben zu Ziff. 3.2.6).

#### **7. Zu 3.2.8 Mangelnde Sicherheit erhobener Zugangssicherungs\_codes**

Hier gelten die obigen Ausführungen zu 3.1.7 entsprechend.

#### **8. Zu 3.2.9 Unzureichende Eingriffsschwellen für Identifizierung von IP-Adressen**

Die Beschwerdeführer halten die gleichartige Ausgestaltung der materiellen Eingriffsschwelle für die reine Bestandsdatenabfrage und die Abfrage zur Identifizierung von Inhabern dynamischer IP-Adressen für verfassungsrechtlich unzulässig. Es müssten an die letztgenannten Abfragen dieselben Anforderungen gestellt werden wie an die Abfrage von Verkehrsdaten. Diese Auffassung findet jedoch in der bisherigen Rechtsprechung des Bundesverfassungsgerichts keine Stütze. Denn danach ist die Auskunft über die Identität von Internetnutzern weder mit der reinen Bestandsdatenabfrage noch mit der Verkehrsdatenabfrage gleichzusetzen (BVerfG, Urteil vom 2.3.2010 Rn. 254 ff.). Nach dieser Rechtsprechung „darf der Gesetzgeber solche Auskünfte auch unabhängig von begrenzenden Rechtsgüter- und Straftatenkatalogen für die Verfolgung von Straftaten, für die Gefahrenabwehr und die Aufgabenwahrnehmung der Nachrichtendienste auf der Grundlage der allgemeinen fachrechtlichen Eingriffsermächtigungen zulassen“ (BVerfG, Urteil vom 2.3.2010 Rn. 261). „Das Erfordernis einer auf Anhaltspunkte im Tatsächlichen gestützten konkreten Gefahr gilt dabei für die Nachrichtendienste ebenso wie für alle zur Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung zuständigen Behörden“ (Rn. 261). Diese Voraussetzungen erfüllt § 8a Abs. 1 Satz 3 LVerfSchG. Diese Vorschrift, aus der sich nach Satz 1 bereits das Erfordernis des Einzelfallbezugs ergibt, ist im

294

Zusammenhang mit § 7 Abs. 1 LVerfSchG zu sehen, der eine Einschränkung für die Ausübung sämtlicher Befugnisse der Verfassungsschutzbehörde enthält. Danach darf, soweit dieses Gesetz nichts anderes bestimmt, die Verfassungsschutzbehörde bei der Wahrnehmung ihrer Aufgaben nach § 5 Abs. 1 LVerfSchG nur tätig werden, wenn tatsächliche Anhaltspunkte für den Verdacht der dort genannten Bestrebungen oder Tätigkeiten vorliegen. Damit dürfte die vom Bundesverfassungsgericht beschriebene Eingriffsschwelle (s.o.) erreicht sein.

Wir hoffen, dass diese Einschätzungen für die Prüfung der Verfassungsbeschwerde hilfreich sind und stehen für nähere Erläuterungen selbstverständlich gern zur Verfügung.

Mit freundlichen Grüßen

In Vertretung

  
Barbara Körffer