

z.V. v. m. 17

An das
Bundesverfassungsgericht
Postfach 1771
76006 Karlsruhe

- bei G1 -

Bundesverfassungsgericht	
Eing. 02.11.17	9-10
<i>9</i> Doppel	<i>14-15</i>
<i>2</i> Anlage	<i>2</i> Doppel

Finig 1

BvR 1732/14 (Beer, Breyer, Dudda et. alt. gegen § 180a LVwG u.a.)

In dem Verfassungsbeschwerdeverfahren BvR 1732/14 zeige ich an, dass mich die Landesregierung von Schleswig-Holstein sowie der Schleswig-Holsteinische Landtag gemeinsam mit ihrer Vertretung betraut haben,

Anlage Bet. 1 und 2.

Aus Sicht der Landesregierung von Schleswig-Holstein sowie des Schleswig-Holsteinischen Landtags ist die Verfassungsbeschwerde unzulässig, zumindest aber unbegründet.

Dies lege ich in der folgenden Stellungnahme dar.

Inhalt

A. Einleitung	4
B. Zulässigkeit der Verfassungsbeschwerde.....	5
I. Beschwerdefähigkeit (Grundrechtsträgerschaft)	5
II. Beschwerdebefugnis.....	6
III. Zwischenergebnis	9
C. Begründetheit der Verfassungsbeschwerde.....	10
I. Einleitung	10
II. Maßstabsbildung.....	11
III §§ 180a, 180b Landesverwaltungsgesetz	12
1. Zu 3.1.1.: Eingriffsschwelle der „bevorstehenden Gefahr“	12
2. Zu 3.1.2.: Fehlende Beschränkung von Auskunftersuchen auf Einzelfälle	14
3. Zu 3.1.3.: Fehlende Beschränkung auf polizeilich Verantwortliche	16
4. Zu 3.1.4.: Fehlende Pflicht zur Benachrichtigung	17
5. Zu 3.1.5.: Mangelnde Kontrolle durch fehlende Statistik.....	18
6. Zu 3.1.6.: Fehlende Subsidiarität des Zugriffs auf Zugangssicherungs-codes (PINs, Passwörter)	19
7. Zu 3.1.7.: Mangelnde Sicherheit erhobener Zugangssicherungs-codes.....	20
8. Zu 3.1.8.: Ausufernde Identifizierung von Internetnutzern	21
9. Zu 3.1.9.: Soziale Netzwerke und Internetdienste (Telemedien).....	26
IV. § 8a Abs. 1 Landesverfassungsschutzgesetz	29
1. Zu 3.2.1.: Eingriffsschwelle der Erforderlichkeit zur Aufgabenerfüllung.....	29
2. Zu 3.2.2.: Fehlende Beschränkung auf Einzelfälle	30
3. Zu 3.2.3.: Fehlende Beschränkung auf polizeilich Verantwortliche	31
4. Zu 3.2.4.: Mangelnder Rechtsschutz wegen fehlender Benachrichtigung.....	31
5. Zu 3.2.5.: Mangelnde Kontrolle durch fehlende Statistik.....	32
6. Zu 3.2.6.: Mangelnde Klarheit der Befugnisse zur Abfrage von Zugangssicherungs-codes.....	32

7. Zu 3.2.7.: Fehlende Subsidiarität des Zugriffs auf Zugangssicherungs-codes (PINs, Passwörter)	33
8. Zu 3.2.8.: Mangelnde Sicherheit erhobener Zugangssicherungs-codes	34
9. Zu 3.2.9.: Unzureichende Eingriffsschwellen für Identifizierung von IP- Adressen.....	34
10. Zu 3.2.10.: Soziale Netzwerke und Internetdienste (Telemedien).....	35
D. Ergebnisse	36

A. Einleitung

Die mit der Verfassungsbeschwerde angegriffenen landesrechtlichen Vorschriften, zu denen aus der Sicht des schleswig-holsteinischen Landtags und der Landesregierung allein Stellung zu nehmen ist, hat der Gesetzgeber Schleswig-Holsteins zur Anpassung an technische und verfassungsrechtliche Entwicklungen in dem Bereich des Grundrechts auf informationelle Selbstbestimmung sowie des Fernmeldegeheimnisses erlassen.

Anlass für diese gesetzgeberische Initiative war insbesondere die Entscheidung des Bundesverfassungsgerichts vom 24. Januar 2012 u.a. zu § 113 TKG. Das Bundesverfassungsgericht hatte mit seiner Entscheidung eine Verfassungsbeschwerde gegen die bundesrechtlichen Regelungen über die Verpflichtung geschäftsmäßiger Anbieter von Telekommunikationsdiensten zur Speicherung (§ 111 TKG) und Verwendung von Kundendaten (Bestandsdaten), insbesondere zu ihrer Beauskunftung im Wege des automatisierten oder manuellen Auskunftsverfahrens (§§ 112, 113 TKG) nicht voll umfänglich, aber im Wesentlichen zurückgewiesen. Das Gericht hat dabei einige materielle Anforderungen an derartige Grundrechtseingriffe entwickelt, die die Nutzung der gespeicherten Daten regelnden Gesetzgeber zu beachten haben.

Aufgrund der in der Entscheidung entwickelten „Doppeltürenlehre“

BVerfGE 130, 151 (184),

müssen oftmals verschiedene Gesetzgeber bei der Regelung einer Datennutzung zusammenwirken: Erst die Gesamtschau einer Regelung zur Speicherung und einer Regelung über den Abruf persönlicher Daten ermöglicht deren Nutzung zu einem konkreten Zweck (Gefahrenabwehr, Strafverfolgung etc.). Der schleswig-holsteinische Gesetzgeber hat für seine Kompetenzbereiche –Gefahrenabwehr und Verfassungsschutz – Normen in Anlehnung an die Vorgaben des Bundesverfassungsgerichts,

so das ausdrückliche Motiv: Gesetzentwurf der Landesregierung, LT-Drs. SH 18/713, S. 1,

geschaffen. Diese Regelungen erlauben den Abruf von auf bundesrechtlicher Grundlage gespeicherten und bereitgestellten Daten. Im Einklang mit der sonstigen Rechtsprechung des Bundesverfassungsgerichts zu dem Grundrecht auf informationelle Selbstbestimmung (und auch Art. 10 GG) galt es dabei insbesondere, verhältnismäßige und normenklare Vorschriften zu formulieren, die eine rechtssichere Nutzung der aufgrund bundesrechtlicher Verpflichtung zu speichernden Normen erlauben. Dies ist durchweg gelungen.

Die Verfassungsbeschwerde ist daher unbegründet. Sie ist aber auch bereits unzulässig.

B. Zulässigkeit der Verfassungsbeschwerde

Es bestehen erhebliche Zweifel an der Zulässigkeit der Verfassungsbeschwerde.

Die Beschwerdebefugnis der Beschwerdeführer steht in Frage. Es ist angesichts des Vortrags sehr zweifelhaft, dass diese tatsächlich eine Möglichkeit der Betroffenheit in eigenen Grundrechten geltend machen. Die Ausführungen der Beschwerdeführer können aber auch mangels unmittelbarer Selbstbetroffenheit nicht überzeugen.

I. Beschwerdefähigkeit (Grundrechtsträgerschaft)

Eine Verfassungsbeschwerde kann von „jedermann“ eingelegt werden (§ 90 BVerfGG), der Träger von Grundrechten ist. Die Beschwerdeführer sind sicherlich *auch* Grundrechtsträger, allerdings legen die äußere Gestaltung der Verfassungsbeschwerde und die auf ihre Zulässigkeit bezogene Argumentation nahe, dass die Beschwerdeführer in dem anhängigen Verfahren *nicht* als Träger von Grundrechten auftreten.

Es ist nicht unüblich, dass parlamentarische Mandatsträger als Bürger eine Verfassungsbeschwerde einlegen. Vorliegend ist aber Verfassungsbeschwerde auf dem Briefbogen einer (nicht mehr bestehenden) Fraktion des schleswig-holsteinischen Landtags eingereicht worden. Die Beschwerdeführer bezeichnen sich als „Abgeordnete“ und sie geben keine Privatadressen, sondern vielmehr ihre (gemeinsame) dienstliche Anschrift beim Landtag an.

Die Beschwerdeführer wollten ihre Verfassungsbeschwerde also ersichtlich nicht als Grundrechtsträger, sondern als Inhaber eines öffentlichen Amtes einreichen. In dieser Eigenschaft wird ihr Rechtskreis allerdings im vorliegenden Zusammenhang nicht durch (Bundes-) Grundrechte, sondern durch Statusrechte der Landesverfassung geschützt.

Dass es sich bei der Einreichung der Verfassungsbeschwerde als Fraktion bzw. als eine Gruppe von Landtagsabgeordneten nicht um einen Zufall oder ein Versehen handelt, wird auch anhand der Argumente deutlich, mit denen Beschwerdeführer zu unterstreichen suchen, dass sie durch die angegriffenen Normen „unmittelbar“ betroffen sind. Hier wird ausdrücklich darauf verwiesen, dass die Beschwerdeführer als

„Abgeordnete im schleswig-holsteinischen Landtag ... darauf angewiesen [sind], anonyme und nicht rückverfolgbare Hinweise beispielsweise über Missstände im Land erhalten zu können, In diesem Zusammenhang müssen sie auch selbst geschützt und kommunizieren und im Internet recherchieren können“; Beschwerdeschrift, S. 2.

An dieser Aussage wird deutlich, dass die Beschwerdeführer die maßgeblichen Berührungspunkte mit den streitbefangenen Regelungen und die entscheidende Exposition gegenüber staatlichen Eingriffen nicht als Grundrechts-, sondern als Mandatsträger befürchten. In dieser Eigenschaft und mit dieser Begründung fehlt es den Beschwerdeführern aber bereits an einer Beschwerdefähigkeit in dem hier angestregten Verfahren.

II. Beschwerdebefugnis

Des Weiteren ist die Verfassungsbeschwerde gem. § 90 Abs. 1 BVerfGG nur zulässig, wenn die Beschwerdeführer behaupten, in einem ihrer Grundrechte oder in einem der diesen gleichgestellten, dort genannten Rechte aus der Verfassung verletzt zu sein.

Soweit man die oben bereits geäußerten Bedenken zu der Grundrechtsträgerschaft der Beschwerdeführer in dem konkreten Zusammenhang ignoriert, kommen als durch die streitbefangenen Regelungen betroffene Grundrechte Art. 10 GG sowie das Grundrecht auf informationelle Selbstbestimmung in Betracht.

Allerdings müssen die angegriffenen Regelungen geeignet sein, den Beschwerdeführer selbst, unmittelbar und gegenwärtig in seiner grundrechtlich geschützten Rechtsposition zu beeinträchtigen,

BVerfGE 1, 97 (101 ff.); 109, 279 (305); 115, 118 (137 ff.).

Diese Voraussetzungen sind bei einer Verfassungsbeschwerde gegen eine Norm selten gegeben. Hier wird eine „unmittelbare Betroffenheit“ nur unter engen Voraussetzungen angenommen, die hier nicht vorliegen. Denn durch eine Rechtsnorm ist ein Beschwerdeführer nur dann unmittelbar betroffen, wenn diese in ein Grundrecht eingreift, ohne dass es rechtsnotwendig oder auch nur nach der tatsächlichen Verwaltungspraxis eines besonderen, vom Willen der vollziehenden Gewalt beeinflussten Vollziehungsakts bedarf,

z.B. BVerfGE 1, 97 (102 f.); 110, 141 (152).

Die mit der Verfassungsbeschwerde angegriffenen Normen erlauben Behörden unter engen Voraussetzungen den Zugriff auf von Dritten gespeicherte Daten.

Die für diesen Zugriff erforderlichen Ermächtigungsgrundlagen wirken nicht aus sich heraus, sondern entfalten erst auf der Grundlage weiterer Vollzugsakte – insbesondere aufgrund der Entscheidung, eine Abfrage durchzuführen bzw. aufgrund der Abfrage selbst – Wirkung.

Derzeit steht aber noch gar nicht fest, ob und inwieweit gerade Daten der Beschwerdeführer von einer solchen Abfrage betroffen sein werden. Die Beschwerdeführer behaupten auch nicht

einmal, dass ihre Daten bereits auf der Grundlage der streitbefangenen Normen abgefragt worden sind. Ergibt sich eine Betroffenheit aber erst bei Anwendung des Gesetzes, so können Verfassungsbeschwerden grundsätzlich nicht schon gegen das Gesetz selbst, sondern nur gegen den auf dessen Grundlage erfolgenden Vollzugsakt gerichtet werden,

BVerfGE 1, 97 (102 f.); 109, 279 (306); 122, 63 (78).

Nach der Rechtsprechung des Bundesverfassungsgerichts kann sich eine Verfassungsbeschwerde in einer solchen Konstellation nur ganz ausnahmsweise gegen das vollziehungsbedürftige Gesetz selbst richten,

BVerfGE 100, 313 (354 ff.); 109, 279 (306 f.); 125, 260 (305).

Dies ist insbesondere dann der Fall, wenn dem Beschwerdeführer die Möglichkeit genommen wird, den Vollzugsakt anzugreifen – etwa, weil der Betroffene von diesem typischerweise keine Kenntnis erlangt.

Sowohl Maßnahmen nach § 180a LVwG als auch solche nach § 8a Abs. 1 LVerfSchG sind zwar als zunächst verdeckte Maßnahmen ausgestaltet. Aber die Normen sehen grundsätzlich eine Pflicht vor, den Betroffenen von dem Grundrechtseingriff zu benachrichtigen (180b Abs. 1 Satz 8, Abs. 2 LVwG, § 8a Abs. 7 Satz 3 LVerfSchG), so dass sichergestellt ist, dass den Beschwerdeführern ein Vorgehen gegen den Grundrechtseingriff möglich ist und diese den Vollzugsakt daher abwarten können. Es ist nicht geboten, eine Verfassungsbeschwerde unmittelbar gegen die angegriffenen Normen zu eröffnen, weil die sich aus dem Gesetz ergebende Mitteilungspflicht für die grundrechtsintensiven Konstellationen der angegriffenen Normen eine unmittelbare Betroffenheit der Beschwerdeführer durch die Norm selbst ausschließt.

Hiergegen spricht auch nicht, dass das Gesetz Möglichkeiten vorsieht, von einer Benachrichtigung des Betroffenen abzusehen. Das Bundesverfassungsgericht hat festgestellt, dass effektiver Rechtsschutz nicht gewährleistet wird (und damit eine unmittelbare Betroffenheit bereits durch die Norm gegeben ist), wenn eine nachträgliche Bekanntgabe des Eingriffs zwar grundsätzlich vorgesehen ist, von dieser aber aufgrund weitreichender Ausnahmetatbestände (ggfs. auch langfristig) abgesehen werden kann,

BVerfGE 109, 279 (307); 120, 378 (395 f.).

Dies ist grundsätzlich verfassungsrechtlich zulässig,

BVerfGE 100, 313 (397 f.).

Bei den streitbefangenen Normen sind Ausnahmen von der Mitteilungspflicht vorgesehen, soweit deren Verwirklichung dem Eingriffszweck zuwiderliefe oder andere Rechte und Interessen

das Interesse des Betroffenen überwiegen (§§ 180b Abs. 1 Satz 9 und Satz 10 LVwG, § 8a Abs. 7 Satz 3 a.E. LVerfSchG). Bei der am wenigsten intensiven Eingriffskonstellation des § 180a Abs. 1 LVwG ist unmittelbar durch die Norm keine Benachrichtigung vorgesehen. Im Sinne der Rechtsprechung des Bundesverfassungsgerichts dürften diese Ausnahmen auch als weitreichend eingestuft werden,

vgl. insbesondere BVerfGE 109, 279 (307).

In einer solchen Situation genügt nach der Rechtsprechung des Bundesverfassungsgerichts die Darlegung des Beschwerdeführers, mit einiger Wahrscheinlichkeit durch die auf den angegriffenen Rechtsnormen beruhenden Maßnahmen in seinen Grundrechten berührt zu werden, um eine unmittelbare Betroffenheit allein aufgrund der streitbefangenen Norm behaupten zu können,

BVerfGE 100, 313 (354 ff.); 109, 279 (307 f.); 125, 260 (305).

Maßgeblich ist hierfür insbesondere, ob die Maßnahmen auf einen tatbestandlich eng umgrenzten Personenkreis zielen oder eine große Streubreite haben und Dritte auch zufällig erfassen können,

BVerfGE 109, 279 (308); 125, 260 (305).

Allerdings ermöglichen die angegriffenen Normen aufgrund ihrer tatbestandlichen Struktur weder Maßnahmen mit großer Streubreite, noch werden sie Personen erfassen, die hierzu keinen Anlass gegeben haben. Dies erscheint angesichts der Ausgestaltung von § 180a LVwG und § 8a Abs. 1 LVerfSchG als gefahrenabwehrrechtliche Einzelfallbefugnisse fraglich.

§ 180a LVwG erfordert das Vorliegen einer konkreten Gefahr für bestimmte Schutzgüter und stellt Auskunftersuchen der Polizei unter den Vorbehalt einer Erforderlichkeitsprüfung im Einzelfall. Insoweit ermächtigt § 180a LVwG lediglich zur Abfrage von Daten eines begrenzten Personenkreises. So müssen beispielsweise bei Auskunftersuchen nach § 180a Abs. 2 Satz 1 Nr. 1 LVwG die Tatbestandsvoraussetzungen des § 185a LVwG vorliegen und damit gemäß § 185a Abs. 1 Satz 2 i.V.m. § 185 Abs. 2 Satz 2 LVwG Tatsachen dafür sprechen, dass die von der Datenerhebung betroffenen Personen als Verantwortliche in Anspruch genommen werden können.

§ 8a Abs. 1 LVerfSchG ermächtigt ebenfalls lediglich zur Einholung von Auskünften im Einzelfall und stellt diese Abfrage unter den Vorbehalt einer Erforderlichkeitsprüfung. Zudem sind Abfragen gem. § 7 Abs. 1 LVerfSchG nur zulässig, wenn tatsächliche Anhaltspunkte für den Verdacht von Bestrebungen oder Tätigkeiten i.S.v. § 5 Abs. 1 LVerfSchG vorliegen. Damit kann eine solche Maßnahme nur dann durchgeführt werden, wenn sich aufgrund tatsächlicher

Umstände Verdachtsmomente ergeben, die eine Zuordnung des jeweiligen Betroffenen zu einer beobachtungsbedürftigen Bestrebung oder Tätigkeit im Sinne von § 5 Abs. 1 LVerfSchG erlauben. Somit ist sichergestellt, dass keine Personen erfasst werden, die keinerlei Anlass zu Maßnahmen gegeben haben.

Beide Regelungen schließen somit eine Bestandsdatenabfrage mit großer personeller Streubreite aus und schützen den Einzelnen vor einer zufälligen Betroffenheit. Jedenfalls aber bestünde bei dem nur zufällig Betroffenen auch keinerlei Grund, eine Ausnahme von der Mitteilungspflicht anzunehmen, weil entgegenstehende Belange einem solchen Fall nicht ersichtlich sind.

Maßnahmen nach § 180a LVwG und § 8a LVerfSchG unterscheiden sich damit auch wesentlich von der von den Beschwerdeführern zur Begründung ihrer unmittelbaren Betroffenheit zitierten Rechtsprechung in Angelegenheiten der Vorratsdatenspeicherung. Dort hatte das Bundesverfassungsgericht die Wahrscheinlichkeit der Betroffenheit der Beschwerdeführer von der verdeckten Maßnahme mit der erheblichen, wohl umfassenden Streubreite der von der Vorratsdatenspeicherung erfassten Daten begründet,

BVerfGE 125, 260 (305).

Hierbei bestand die konkrete Gefahr, dass Daten ohne Anknüpfung an ein vorwerfbares Verhalten abgerufen werden,

so ausdrücklich BVerfGE 125, 260 (318).

Diese Befürchtungen bestehen angesichts des Wesens der Bestandsdatenabfrage sowie angesichts der oben dargestellten Ausgestaltungen der Regelungen als Einzelfallbefugnisse zur Abwehr besonders qualifizierter Gefahren unter dem Vorbehalt besonderer prozeduraler Sicherungen nicht.

III. Zwischenergebnis

Die Verfassungsbeschwerde ist unzulässig, weil es den Beschwerdeführern zum einen als Mandatsträgern an der erforderlichen Grundrechtsberechtigung mangelt; zum andern weisen sie nicht die erforderliche Beschwerdebefugnis auf.

C. Begründetheit der Verfassungsbeschwerde

Die Verfassungsbeschwerde ist auch unbegründet.

I. Einleitung

Der schleswig-holsteinische Gesetzgeber hat sich bei der Gestaltung der angegriffenen Ermächtigungsgrundlagen eng an der maßgeblichen Entscheidung des Bundesverfassungsgerichts vom 24. Januar 2012 orientiert.

Dies wurde trotz rechtspolitischer Distanz zu dem Vorhaben auch durch das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD)

Umdruck Schleswig-Holsteinischer Landtag 18/1245, S. 2: „Damit entspricht der Entwurf in wesentlichen Punkten den verfassungsrechtlichen Anforderungen an Bestimmtheit und Verhältnismäßigkeit von Eingriffsermächtigungen. In anderen Punkten besteht allerdings noch Nachbesserungsbedarf“; diese erweisen sich dann aber in erster Linie als rechtspolitische Anregungen.

sowie die Neue Richtervereinigung (NRV) Schleswig-Holstein,

Umdruck Schleswig-Holsteinischer Landtag 18/1250, S. 1: das Gesetzesvorhaben „verbessert den gesetzlichen Schutz von Telekommunikationsnutzerdaten und zielt darauf ab, den Anforderungen des Bundesverfassungsgerichts u.a. aus dem Beschluss vom 24. Januar 2012 - 1 BvR 1299/05 - Rechnung zu tragen. Bis auf einzelne Aspekte ist dies aus Sicht der NRV auch gelungen“,

im Rahmen der parlamentarischen Anhörung zu dem Gesetzesvorhaben weitgehend (mit einigen Abstrichen) bestätigt. Weitere Verschärfungen der Ermächtigungsgrundlagen – etwa im Hinblick auf die Präzisierung der Eingriffsschwelle – wurden dann noch auf Anregung des Innen- und Rechtsausschusses in das Gesetz eingebracht,

Bericht und Beschlussempfehlung des Innen- und Rechtsausschusses, LT-Drs. 18/928.

Die verfassungsrechtliche Kritik der Beschwerdeführer an den angegriffenen Normen nährt sich zum einen aus einem Fehlverständnis der in dem Beschluss vom 24. Januar 2012 entwi-

ckelten Maßstäbe und zum andern aus dem Willen, die Maßstäbe dieses Beschlusses noch weiter zu verschärfen, weil das Bundesverfassungsgericht nach Ansicht der Beschwerdeführer mit Blick auf den Grundrechtsschutz nicht weit genug gegangen ist.

II. Maßstabsbildung

Die Speicherung, Abfrage und Verwendung von Daten, die durch Nutzung von Telekommunikation und Telemedien anfallen, berührt entweder das Telekommunikationsgeheimnis (Art. 10 GG) oder aber das Grundrecht auf informationelle Selbstbestimmung. Während einfache Bestandsdaten, Daten zur Zugangssicherung oder statische IP-Adressen durch das letztgenannte Grundrecht geschützt sind, fallen Informationen über die Zuordnung dynamischer IP-Adressen wegen ihrer Nähe zu konkreten Kommunikationsvorgängen in den Schutzbereich des Telekommunikationsgeheimnisses,

siehe i.E. die jeweiligen Zuordnungen in BVerfGE 130, 151 (179 ff.).

Im Ergebnis ist diese Abgrenzung aber für die Intensität des Grundrechtsschutzes nicht von zentraler Bedeutung, da die Anforderungen, die das Bundesverfassungsgericht mit Blick auf das letztgenannte Grundrecht ermittelt hat, weitgehend auf die speziellere Garantie des Art. 10 GG zu übertragen sind,

BVerfGE 100, 313 (359 f.); 125, 260 (310).

In beiden Fällen sind Grundrechtseingriffe möglich, wenn sie in verhältnismäßiger Art und Weise das staatliche Anliegen und die Sensibilität eines bestimmten Datums in einen Ausgleich bringen. Dabei ist es nicht nur erforderlich, mit der Schwere des Grundrechtseingriffs die tatbestandliche Eingriffsschwelle zu verschärfen, sondern auch prozedurale Absicherungen des Eingriffs zu gewährleisten, die es dem Grundrechtsträger ermöglichen, sich gegen den Eingriff zur Wehr zu setzen. Der heimliche Eingriff wiegt schwerer als der offene, der indirekte Zugriff wiegt schwerer als der direkte. Auch die Persönlichkeitsrelevanz der in Anspruch genommenen Daten wirkt auf die gebotene Strenge der Eingriffsermächtigung zurück.

Dies alles führt dazu, dass die Rechtfertigung von Eingriffen in das Grundrecht auf informationelle Selbstbestimmung (und in das Telekommunikationsgeheimnis) eine Beurteilung der Eingriffsschwere voraussetzt, von der ausgehend dann die materiellen und prozeduralen Anforderungen an die Rechtfertigung des Eingriffs entwickelt werden müssen.

Die wesentlichen Eckpfeiler der insoweit gebotenen Erwägungen wurden durch das Bundesverfassungsgericht hauptsächlich in zwei jüngeren Entscheidungen entwickelt,

BVerfGE 125, 260; 130, 151.

Deren Wertungen sind durch den schleswig-holsteinischen Landesgesetzgeber nachvollzogen worden.

III §§ 180a, 180b Landesverwaltungsgesetz

§ 180a Abs. 1 und 2 LVwG enthalten Ermächtigungen zur Auskunft über Bestandsdaten. § 180a Abs. 1 LVwG bezieht sich auf „einfache“ Bestandsdaten und damit nach der in § 3 Nr. 3 TKG enthaltenen Legaldefinition auf „Daten eines Teilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden“, umfasst. Eine genauere Benennung der fraglichen Daten enthalten die in Bezug genommenen §§ 95 und 111 TKG.

§ 180a Abs. 2 LVwG ermächtigt zu der Abfrage solcher Bestandsdaten, „mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird“. Des Weiteren ermöglicht die Norm die Abfrage statischer und dynamischer IP-Adressen. § 180 Abs. 4 LVwG erlaubt den Behörden die Abfrage von Telemedien-Bestandsdaten.

§ 180b LVwG enthält die prozeduralen Sicherungen für Abfragen nach § 180a LVwG.

Die Betrachtung dieser Normen macht deutlich, dass der Gesetzgeber die zunehmende Persönlichkeitsrelevanz und die damit einhergehende wachsende Intensität eines Grundrechtseingriffs durch Abfrage durch ebenfalls immer strenger werdende materielle Eingriffsschwellen sowie prozeduraler Absicherungen würdigt. Das Vorbringen der Beschwerdeführer lässt sich zumeist auf den Vorwurf mangelnder Verhältnismäßigkeit oder fehlender Normenklarheit der streitbefangenen Vorschriften zurückführen.

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

Alle Abfragen nach § 180a LVwG dürfen nur bei Vorliegen einer „im einzelnen Falle bevorstehenden Gefahr für die öffentliche Sicherheit“ erfolgen. Mit dieser Formulierung knüpft der Gesetzgeber an die verfassungsrechtliche Vorgabe an, dass eine Datennutzung nicht ausufernd und anlasslos erfolgen darf,

BVerfGE 125, 260 (316 ff.),

und bewegt sich dabei auf dem gesicherten Grund altbekannter polizeirechtlicher Dogmatik und Terminologie. Ungeachtet dessen rügen die Beschwerdeführer eine Verletzung der Gebote der Verhältnismäßigkeit und der Normenklarheit im Hinblick auf die in § 180a Abs. 1 und 2 LVwG geregelten Auskunftsermächtigungen über Bestandsdaten.

Der Kern der Rüge besteht darin, dass die Eingriffsschwelle der „im einzelnen Falle bevorstehenden Gefahr für die öffentliche Sicherheit“ als zu niedrig und der verwendete Gefahrenbegriff als unklar angesehen werden. Die Beschwerdeführer legen dar, dass nach der Rechtsprechung des Bundesverfassungsgerichts eine konkrete Gefahr im Sinne der polizeilichen Generalklauseln Mindestvoraussetzung einer verhältnismäßigen staatlichen Bestandsdatenerhebung ist,

BVerfGE 130, 151 (205 ff.).

Die Formulierung der „im einzelnen Falle bevorstehenden Gefahr“ ist mit dem Begriff der konkreten Gefahr, wie ihn das Bundesverfassungsgericht verwendet, identisch.

Dies folgt bereits aus einer systematischen Auslegung der Begrifflichkeit vor dem Hintergrund der im LVwG verwendeten Gefahrbegriffe. Das LVwG nennt an bislang keiner Stelle den Begriff der konkreten Gefahr. Vielmehr wird für deren Beschreibung durchweg der Begriff der im einzelnen Fall bevorstehenden Gefahr verwendet (vgl. §§ 176 Abs. 1 Nr. 2, 179 Abs. 1, 180 Abs. 2 Satz 1, 180a Abs. 1 Satz 1, Abs. 2 Satz 2 und Abs. 4, 181 Abs. 1, 191 Abs. 1 Satz 1 Nr. 1, 193 Abs. 1 Satz 2, 193 Abs. 2 Nr. 1, 199 Abs. 3 Nr. 1, 201 Abs. 1 Satz 1, 259 Abs. 1 Satz 2 LVwG).

Daneben kennt das LVwG qualifizierte Gefahrbegriffe, wie die gegenwärtige Gefahr (vgl. §§ 180a Abs. 2 Satz 2 und Abs. 4, 185 Abs. 3, 185 a Abs. 1 Satz 1, 186a Abs. 4 Satz 1, 201a Abs. 1 Satz 1, 210 Abs. 1 Nr. 1, 220 Abs. 1, 229 Abs. 2 Nr. 1, 230 Abs. 1 Satz 1, 258 Abs. 2 Nr. 1, 259 Abs. 2 LVwG), die Gefahr im Verzuge (vgl. §§ 180b Abs. 1 Satz 4, 186 Abs. 1 Satz 2, 208 Abs. 5 Satz 1 LVwG) sowie die erhebliche Gefahr (vgl. §§ 179 Abs. 4 Satz 1 Nr. 2, 193 Abs. 2 Nr. 2, 195a Abs. 1, 208 Abs. 1, Abs. 3 Nr. 3 und Abs. 4 Satz 1 LVwG).

Dass der Begriff der im einzelnen Fall bevorstehenden Gefahr dabei mit dem der konkreten Gefahr identisch ist, wird insbesondere durch die Formulierung der polizei- und ordnungsrechtlichen Generalklausel der §§ 174, 176 LVwG gestützt. Diese setzt in § 176 Abs. 1 Nr. 2 LVwG ebenso das Vorliegen einer im einzelnen Fall bevorstehenden Gefahr voraus und wird in der Literatur durchweg als eine konkrete Gefahr verstanden,

Becker/Brüning, Öffentliches Recht in Schleswig-Holstein, 2014 (München) § 3, Rn. 89.

Die Charakterisierung einer Gefahr als „bevorstehend“ dient v.a. ihrer Differenzierung von der Störung (§ 176 Abs. 1 Nr. 1 LVwG; polizeirechtlich auch: Schaden), mithin von der bereits realisierten Gefahr. Ein anderes Verständnis dieses Tatbestandsmerkmals wäre bei der polizeilichen Generalklausel aus dogmatischen, historischen, aber auch aus rechtsvergleichenden

Gründen völlig undenkbar. Dann muss dasselbe Verständnis bei § 180a LVwG zugrundegelegt werden.

Auch die Gesetzesbegründung zu dieser Norm weist ausdrücklich darauf hin, dass Bestandsdatenabfragen tatbestandlich an das Vorliegen einer konkreten Gefahr geknüpft sind und schließt eine Anwendung der Befugnis im Gefahrenvorfeld ausdrücklich aus,

Gesetzentwurf der Landesregierung, LT-Drs. SH 18/713, S. 13.

Dieses Verständnis des in § 180a LVwG verwendeten Gefahrbegriffs dürfte von niemandem außer den Beschwerdeführern bestritten werden,

Martens, in: PdK, Kommentar zum LVwG SH, § 180a, Rn. 410 e, f; Stellungnahme des ULD, Umdruck Schleswig-Holsteinischer Landtag 18/1245, S. 1; Stellungnahme der NRV, Umdruck Schleswig-Holsteinischer Landtag 18/1250, S. 2).

Anwendungsschwierigkeiten aufgrund einer von den Beschwerdeführern geltend gemachten Unbestimmtheit des Begriffs der im einzelnen Fall bevorstehenden Gefahr ergeben sich aus diesem Grunde nicht.

§ 180a LVwG knüpft staatliche Bestandsdatenerhebungen somit an das Vorliegen einer konkreten Gefahr und setzt insoweit die auch diese Vorgaben des Bundesverfassungsgerichts aus dem Beschluss vom 24. Januar 2012 vollumfänglich um. Folglich genügt die Regelung insoweit dem Gebot der Verhältnismäßigkeit und dem Gebot der Normenklarheit.

Zudem hat der Gesetzgeber in § 180a Abs. 2 Satz 1 LVwG die Vorgabe des Bundesverfassungsgerichts umgesetzt, dass für den Zugriff auf diese Daten auch die gesetzlichen Voraussetzungen für die Nutzung der auf den Endgeräten gespeicherten Daten gegeben sein müssen,

BVerfGE 130, 151 (208 ff.),

und auf diese Weise durch die Bezugnahme auf weitere Ermächtigungsgrundlagen das Erfordernis der konkreten Gefahr gleich ein zweites Mal normiert.

Der Gesetzgeber hat durch die Einführung der „im einzelnen Falle bevorstehenden Gefahr für die öffentliche Sicherheit“ einen ausreichenden Eingriffsanlass normiert.

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

Die Ausführungen der Beschwerdeführer, § 180a Abs. 1 und Abs. 2 LVwG ermächtigten aufgrund des fehlenden Tatbestandsmerkmals „im Einzelfall“ zu routinemäßigen und massenhaften Bestandsdatenabfragen und verletzen daher das Verhältnismäßigkeitsgebot, überzeugen nicht.

Die notwendige Verhinderung einer flächendeckenden Abfrage wird bereits dadurch sichergestellt, dass sowohl nach § 180a Abs. 1 LVwG als auch nach § 180a Abs. 2, der auf Abs. 1 aufbaut und dessen Bedingungen verschärft, ein Einzelfallbezug durch die „im Einzelfall bestehende Gefahr“ hergestellt wird. So kann es höchstens geschehen, dass zu einem einzelnen Gefahrenvorgang die Daten mehrerer Personen abgefragt werden. Die Begrenzung der Abfrage liegt daher in der Benennung ihres Anlasses. Hierdurch wird eine massenhafte und gleichsam auf Vorrat erfolgende Datenerhebung ausgeschlossen.

„Aus verfassungsrechtlicher Perspektive ist die Zahl der Bestandsdatenauskünfte als solche kein relevantes Kriterium. Maßgeblich ist vielmehr stets die Abwägung der verfassungsrechtlich maßgeblichen Positionen, sodass auch ganz vereinzelt ausgeführte Maßnahmen bei nicht tragfähiger Interessenabwägung rechtswidrig, eine Vielzahl von Maßnahmen mit tragfähiger Begründung hingegen rechtmäßig sein kann. ... Sicherzustellen ist lediglich, dass die Abfrage von Bestandsdaten in jedem Einzelfall auch tatsächlich geprüft wird“,

Stellungnahme *Buermeyer* zu dem Antrag der Fraktion Piraten (LT-Drs. NRW 16/1467), NRW Landtag Stellungnahme 16/639, S. 7 f.

Neben der Eingrenzung behördlicher Abfragemöglichkeiten durch das Tatbestandsmerkmal der im Einzelfall bevorstehenden Gefahr, ergibt sich auch aus dem in § 180a Abs. 1 Satz 1 und Abs. 2 LVwG genannten Erfordernis der Erforderlichkeit die weitere Pflicht des Rechtsanwenders, in jedem Einzelfall zu prüfen, ob die Bestandsdatenauskunft für den jeweils aktuell zu beurteilenden Gefahrensachverhalt tatsächlich notwendig ist,

Gesetzentwurf der Landesregierung, LT-Drs. SH 18/713, S. 13.

Ferner garantiert das einzuhaltende Verfahren nach § 180a Abs. 1 Satz 2 und § 180b LVwG eine tatsächliche Prüfung des im Einzelnen vorzunehmenden Datenabrufs. Gemäß § 180a Abs. 1 Satz 2 LVwG i.V.m. § 113 Abs. 2 Satz 1 TKG sind Auskünfte dabei explizit auf den Einzelfall beschränkt. Über die Verweisung des § 180a Abs. 1 Satz 2 LVwG werden die Tatbestandsvoraussetzungen des § 113 Abs. 2 Satz 1 TKG auch Voraussetzung für die Erhebungsbefugnis der Polizeibehörden.

Darüber hinaus sorgt bereits die tatbestandliche Fassung der § 180a Abs. 1 und 2 LVwG dafür, dass in jedem der – ggf. auch zahlreichen – Einzelfälle die Datenübermittlung tatsächlich verhältnismäßig ist. Die Behörde muss zudem im Rahmen des ihr eingeräumten Ermessens eine

dem Verhältnismäßigkeitsgrundsatz Rechnung tragende Entscheidung darüber treffen, wessen Daten in welchem Umfang anzufordern sind.

Da der Gesetzgeber somit hinreichend Sorge für eine Beschränkung von Auskunftersuchen auf Einzelfälle getragen hat, liegt ein Verstoß gegen den Grundsatz der Verhältnismäßigkeit des Grundrechtseingriffs nicht vor.

3. Zu 3.1.3.: Fehlende Beschränkung auf polizeilich Verantwortliche

Die von den Beschwerdeführern gerügte fehlende Beschränkung des § 180a Abs. 1 LVwG auf Störer vermag in Anbetracht der Ausführungen des BVerfG zu § 113 Abs. 1 Satz 1 TKG a.F. und vor dem Hintergrund der geringen Eingriffstiefe der Bestandsdatenabfrage eine Verfassungswidrigkeit der Norm nicht zu begründen.

Das Bundesverfassungsgericht hat in seinem Beschluss vom 24. Januar 2012 die Regelung des § 113 Abs. 1 Satz 1 TKG a.F., die Auskünfte ebenfalls nicht von vornherein auf Polizeipflichtige im Sinne des allgemeinen Ordnungsrechts beschränkte, vor dem Hintergrund des geringen Eingriffsgewichts der Bestandsdatenauskunft als verhältnismäßig angesehen,

BVerfGE 130, 151 (206 f.).

Eine Einschränkung des möglichen Adressatenkreises der Maßnahmen nach § 180a Abs. 1 und 2 LVwG gründet außerdem auf dem Übermaßverbot,

Bär, Die Neuregelung des § 100j StPO zur Bestandsdatenauskunft, Auswirkungen auf die Praxis der Strafverfolgung, MMR 2013, S. 700 ff. (702).

Zudem ergibt sich bei den eingriffsintensiveren Maßnahmen nach § 180a Abs. 2 Satz 1 Nr. 1 LVwG eine Begrenzung der Abfrage auf Personen, bei denen Tatsachen dafür sprechen, dass sie als Verantwortliche in Anspruch genommen werden können, §§ 180a Abs. 2 Satz 1 Nr. 1, 185a Abs. 1 Satz 2, 185 Abs. 2 Satz 2 LVwG. Bei Maßnahmen nach § 180a Abs. 2 Satz 1 Nr. 2 LVwG gelangen die Normen über die polizeiliche Verantwortung (§§ 218 ff. LVwG) über §§ 180a Abs. 2 Satz 1 Nr. 2, 210 LVwG zur Anwendung: Da der Eingriff nur zulässig ist, wenn auch die weitergehende Maßnahme vorgenommen werden kann, wirkt die bei dieser erforderlichen Störereigenschaft ebenso auch auf den datenrechtlichen Eingriff zurück wie die stark eingrenzenden Normen der Nichtstörerhaftung.

Während also bei § 180a Abs. 1 LVwG eine Begrenzung auf Störer nicht erforderlich ist, liegt bei § 180a Abs. 2 LVwG durch die Weiterverweisung auf die dort genannten Eingriffsermächtigungen eine Begrenzung nach Maßgabe polizeilicher Verantwortlichkeit vor. Dies genügt dem Grundsatz der Verhältnismäßigkeit.

4. Zu 3.1.4.: Fehlende Pflicht zur Benachrichtigung

Die Beschwerdeführer rügen die fehlende Pflicht zur Benachrichtigung des Betroffenen bei Auskunftsverlangen nach § 180a Abs. 1 LVwG. Allerdings ist eine solche Benachrichtigungspflicht aufgrund der niedrigen Eingriffsintensität des Abrufens von Bestandsdaten nach § 180a Abs. 1 LVwG – im Gegensatz zu den sensibleren Daten, die nach § 180a Abs. 2 LVwG abgerufen werden können (vgl. § 180b Abs. 1 LVwG) – verfassungsrechtlich nicht geboten.

Ob verfahrensrechtliche Vorkehrungen in der Form von nachträglichen Mitteilungspflichten verfassungsrechtlich geboten sind, um die Verhältnismäßigkeit eines Grundrechtseingriffs zu sichern, bemisst sich nach der jeweiligen Intensität des Eingriffs. Wenn diese gering ist, besteht nach Ansicht des Bundesverfassungsgerichts kein umfassendes Erfordernis einer Benachrichtigung der von der Auskunft Betroffenen,

BVerfGE 130, 151 (210); s.a. *Kugelman/Dalby*, Die Neuregelung der Bestandsdatenauskunft gem. § 113 TKG und die Notwendigkeit des Grundrechtsschutzes durch Verfahren, in: FS Kutscha, 2013 (Baden-Baden), S. 105 ff. (114).

Das Gewicht der Datenabfrage hängt zunächst davon ab, welche Inhalte von der Abfrage erfasst werden und welche Persönlichkeitsrelevanz diese Informationen für sich und in Verknüpfung mit anderen Informationen haben,

Petri, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 2012 (5. Aufl., München), Kapitel G Rn. 46; *Kugelman/Dalby*, Die Neuregelung der Bestandsdatenauskunft gem. § 113 TKG und die Notwendigkeit des Grundrechtsschutzes durch Verfahren, in: FS Kutscha, 2013 (Baden-Baden) S. 105 ff. (114)).

Die Auskunft nach § 180a Abs. 1 LVwG stellt nur einen Eingriff von geringer Intensität in das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) des Betroffenen dar. Die gemäß § 180a Abs. 1 LVwG abgerufenen Daten sind solche, die im Rahmen von Verträgen üblicherweise übermittelt werden. Sie stellen keine höchstpersönlichen Daten dar und sind nicht als besonders sensibel zu bewerten,

BVerfGE 130, 151 (205 f.); *Kugelman/Dalby*, Die Neuregelung der Bestandsdatenauskunft gem. § 113 TKG und die Notwendigkeit des Grundrechtsschutzes durch Verfahren, in: FS Kutscha, 2013 (Baden-Baden) S. 105 ff. (116, 119)); *Dalby*, CR 2013, S. 361 ff. (366).

Der Bundesgesetzgeber hat eine ähnliche Wertung der Datensensibilität in bundesrechtlichen Abrufvorschriften vorgenommen. Auch dort besteht für die Auskunft über Daten i.S.d. §§ 95, 111 TKG keine Mitteilungspflicht (vgl. bspw. § 100j Abs. 1 StPO, § 7 Abs. 3 S. 1 BKAG,

zur Verfassungsmäßigkeit der dort fehlenden Mitteilungspflicht s. *Kugelman*, in: ders., BKAG, 2014, § 7 Rn. 45.

Der Gesetzgeber ist somit von Verfassungs wegen nicht gezwungen, Mitteilungspflichten für Bestandsdatenabfragen nach § 180a Abs. 1 LVwG einzuführen, um die Verhältnismäßigkeit dieser Maßnahme sicherzustellen.

5. Zu 3.1.5.: Mangelnde Kontrolle durch fehlende Statistik

Die Beschwerdeführer rügen eine fehlende Regelung zur statistischen Erfassung der staatlichen Bestandsdatenabfragen. Eine solche sei erforderlich, um eine Überprüfung und Evaluierung der Maßnahmen nach § 180a LVwG zu ermöglichen und folge aus dem Verhältnismäßigkeitsgrundsatz.

Diese Forderung wurde – allerdings wohl eher im Sinne einer rechtspolitischen „best practice“ und ohne ausdrückliche Einordnung als verfassungsrechtliche Notwendigkeit – im Gesetzgebungsverfahren sowohl vom Unabhängigen Landeszentrum für Datenschutz als auch von der Neuen Richtervereinigung erhoben,

Schleswig-Holsteinischer Landtag, Umdrucke 18/1245, S. 4 bzw. 18/1250, S. 4.

Die Neufassung des § 186b Abs. 1 Satz 2 LVwG schafft für die Landesregierung allerdings bereits eine jährliche Berichtspflicht für Maßnahmen nach § 180a Abs. 2 und 4 LVwG. Gemäß § 186b Abs. 1 Satz 2 i.V.m. Abs. 1 Satz 1 LVwG müssen Anlass, Umfang, Dauer und Ergebnis der entsprechenden Eingriffe gegenüber dem Landtag offengelegt werden. Diese Angaben gewährleisten damit eine öffentliche Transparenz des staatlichen Handelns,

Martens, in: PdK Kommentar LVwG SH, 2014, § 186b, Rn. 424.

Für die weniger eingriffsintensiven Maßnahmen nach § 180a Abs. 1 LVwG ist eine Evaluation hingegen nicht erforderlich. Allenfalls bei besonders eingriffsintensiven Maßnahmen sowie bei

Regelungen mit einem hohen experimentellen Charakter kann eine Evaluation als grundrechtssicherndes Verfahrensrecht verfassungsrechtlich geboten sein,

Kilian/Heussen, Computerrecht, 2017, 1. Abschnitt. Erläuterungen Teil 13: Datenschutz Grundrechtsschutz durch Verfahren, Rn. 63.

Wie bereits dargelegt, stellen Abfragen nach § 180a Abs. 1 LVwG jedoch lediglich einen Grundrechtseingriff von leichtem Gewicht dar (s. oben, zu 3.1.4.).

Unabhängig davon trifft den Gesetzgeber unter bestimmten Voraussetzungen eine verfassungsunmittelbare Beobachtungs- und Korrekturpflicht bei Gesetzen, die in Grundrechte eingreifen,

BVerfGE 112, 304 (316),

sodass es keiner besonderen und ausdrücklichen Normierung entsprechender Beobachtungspflichten und erst recht keiner ausdrücklichen Festlegung auf eine bestimmte Methode der Beobachtung und Evaluierung („Statistik“) bedarf.

6. Zu 3.1.6.: Fehlende Subsidiarität des Zugriffs auf Zugangssicherungs-codes (PINs, Passwörter)

Die Beschwerdeführer fordern, dass zur Wahrung des Verhältnismäßigkeitsgrundsatzes der Staat Zugangssicherungs-codes allenfalls dann erheben darf, wenn die damit bezweckte Datenerhebung auf andere Weise, insbesondere durch Inanspruchnahme des Telekommunikationsanbieters, nicht erfolgen kann.

Die Ansicht der Beschwerdeführer, nach der die Inanspruchnahme des Telekommunikationsanbieters prinzipiell einen milderen Grundrechtseingriff darstellt als der unmittelbare staatliche Zugriff auf die Speichereinrichtungen, kann aber nicht überzeugen. Für die Beurteilung der Eingriffsintensität beim Betroffenen ist es unerheblich, ob zunächst der Telekommunikationsanbieter die Daten sichtet und im Anschluss daran relevante Daten an die Polizei weiterleitet oder ob der Telekommunikationsanbieter den Zugriffscode übermittelt und so die Polizei nach relevanten Daten sucht. Im Ergebnis kommt es bei beiden Vorgehensweisen zu einem heimlichen Zugriff auf Daten, die der Betroffene zuvor gegen fremden Zugriff gesichert und damit als besonders schutzwürdig festgelegt hat,

Stellungnahme *Buermeyer* zu dem Antrag der Fraktion Piraten (LT-Drs. NRW 16/1467), NRW Landtag Stellungnahme 16/639, S. 9.

Es mag auch offenbleiben, ob Private grundsätzlich vertrauenswürdiger als staatliche Behörden sind, wenn es darum geht, Daten zu speichern und zu sichten.

Für den Betroffenen ist in einem solchen Fall vielmehr relevant, wann er von dem Eingriff Kenntnis erlangt, damit er neue Zugangssicherungen erstellen und gegebenenfalls nachträglichen Rechtsschutz suchen kann,

Buermeyer, a.a.O., S. 10.

Dass eine nachträgliche Kenntnisnahme durch § 180b Abs. 1 Satz 8 LVwG hinreichend abgesichert ist und dass eine eventuelle Nichtbenachrichtigung nur unter engen Voraussetzungen verfassungsrechtlich zulässig ist, wurde bereits dargelegt.

Daneben kann eine über den Grundsatz der Verhältnismäßigkeit hinausgehende Subsidiarität der Abfrage keine eigenständige Bedeutung entfalten; keinesfalls ist sie verfassungsrechtlich geboten. Insgesamt obliegt es der Gestaltungsfreiheit des Gesetzgebers, mit welchen Mitteln er die Verhältnismäßigkeit einer Maßnahme sichert. Hier hat der Gesetzgeber eine erhebliche Eingriffsschwelle, einen Richtervorbehalt sowie eine Benachrichtigungspflicht eingeführt, die im Zusammenwirken die Verhältnismäßigkeit der Maßnahme sicherstellen.

7. Zu 3.1.7.: Mangelnde Sicherheit erhobener Zugangssicherungs-codes

Die Beschwerdeführer rügen, dass das Gesetz keinerlei Vorkehrungen zur Gewährleistung der Sicherheit erhobener Zugangssicherungs-codes trifft. Allerdings bedarf es zur Wahrung der Verhältnismäßigkeit keiner besonderen Schutzvorschriften. Nutzung und Speicherung des Codes unterliegen den allgemeinen Regeln des staatlichen Datenschutzrechts. Es ist nicht dargelegt, warum es verfassungsrechtlich geboten ist, hier *leges speciales* allein für Zugangssicherungs-codes zu schaffen, da der Staat auch in anderen Zusammenhängen sensible Daten verwaltet, die auf der Grundlage des allgemeinen Datenschutzrechts vor missbräuchlichem Zugriff geschützt werden.

Es ist zwischen dem erlangten Zugangssicherungscode selbst und den mithilfe des Zugangssicherungs-codes erlangten Daten zu differenzieren.

Bezüglich der Inhalte, die mithilfe von erlangten Zugangssicherungs-codes ausgelesen werden können, bestimmen die Rechtsgrundlagen, die die Nutzung der Zugangssicherungs-codes regeln (§§ 185 a, 210 LVwG), auch die Vorkehrungen zur Gewährleistung der Sicherheit dieser Daten. So verpflichtet § 186 Abs. 3 LVwG die Polizei zur unverzüglichen Vernichtung der Daten, sobald diese nicht mehr erforderlich für die dort aufgezählten Zwecke sind. § 186 Abs. 6 LVwG bestimmt, unter welchen Voraussetzungen die Daten anderweitig verwertet werden dürfen. Sofern auf die Daten gemäß § 210 LVwG zugegriffen wurde, bestimmt § 210 Abs. 2 LVwG, dass die Daten gelöscht werden müssen, sofern die Voraussetzungen der Sicherstellung weggefallen sind oder der Zweck erreicht ist.

Ausdrücklich findet sich mit Blick auf die nach § 180a Abs. 2 LVwG erlangten Zugangssicherungscodes selbst keine vergleichbare Regelung, die bestimmt, wie dieser nach Abschluss der Maßnahmen aufzubewahren ist oder wann dieser vernichtet werden soll. Allerdings gelten auch hier die allgemeinen Regeln des Datenschutzrechts im LVwG. Insoweit enthält § 196 Abs. 2 LVwG eine allgemeingültige Löschungsverpflichtung für in Dateien gespeicherte Daten, wenn die Daten nicht mehr zu dem konkreten Zweck benötigt werden, der Anlass für die Abfrage war.

Weiterhin erscheint fraglich, ob solche Regelung – wie sie von den Beschwerdeführern als Grundlage der Verhältnismäßigkeit der Maßnahme gefordert werden – überhaupt erforderlich ist. Es ist zu berücksichtigen, dass § 180b Abs. 1 Satz 8 LVwG anordnet, dass die betroffene Person nach Abschluss der Maßnahmen von der Polizei zu unterrichten ist. Mit Kenntnis von dem Zugriff auf seinen Zugangssicherungscode hat der Betroffene sodann die Möglichkeit, den entsprechenden Zugangscode zu ändern. Dass der ursprüngliche Code dann unter Umständen bei der Polizei verbleibt, ist dann belanglos, da dieser nach der Erstellung einer neuen Zugangssicherung durch den Betroffenen keinen Persönlichkeitsbezug mehr aufweist. Der Code als solcher ist kein sensibles Datum – nur der dadurch mögliche Zugriff auf andere Daten macht einen Zugangssicherungscode zu einem sensiblen Datum. Insoweit besteht dann auch keine Gefahr, dass der Zugriffscode zu anderen Zwecken weitergegeben wird, da der Code nach Änderung des Passwortes durch den Betroffenen ohnehin seinen Zweck, auf die dadurch gesicherten Daten zuzugreifen, nicht mehr erfüllt.

8. Zu 3.1.8.: Ausufernde Identifizierung von Internetnutzern

Zentraler Aspekt der Verfassungsbeschwerde ist die behauptete Unverhältnismäßigkeit der Identifikationsmöglichkeiten von Internetnutzern auf der Grundlage von § 180a Abs. 1, Abs. 2 Satz 2 LVwG.

In seiner auf die Speichernorm („erste Tür“) bezogenen Entscheidung vom 24. Januar 2012 hatte das Bundesverfassungsgericht wegen der Bedeutung der Information über die Zuordnung einer dynamischen IP-Adresse festgelegt, dass die entsprechende Auskunft eine normenklare Regelung erfordert, da es sich hierbei um einen Eingriff in Art. 10 Absatz 1 GG handelt. Diese Daten sind hinsichtlich ihrer Sensibilität in der Nähe von Verkehrsdaten anzusiedeln, bei denen es sich nach § 3 Nr. 30 TKG um solche handelt, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden. Die in § 180a Abs. 1, Abs. 2 Satz 2 LVwG angesprochenen Bestandsdaten zu Name und Anschrift kann der Diensteanbieter nur anhand der bei ihm gespeicherten Telekommunikationsverkehrsdaten feststellen, die dem Schutz des Fernmeldegeheimnisses unterliegt. Allerdings hat das Gericht in seiner Entscheidung

dung festgestellt, dass trotz der Rückschlüsse, die von diesen Daten auf eine dann deanonymisierte Kommunikation im Internet gezogen werden können, wegen des besonderen staatlichen Interesses an einer sich in das Internet verlagernden Kommunikation solche Auskünfte „auch unabhängig von begrenzenden Rechtsgüter- und Straftatenkatalogen für die Verfolgung von Straftaten, für die Gefahrenabwehr und die Aufgabenwahrnehmung der Nachrichtendienste auf Grundlage der allgemeinen fachrechtlichen Ermächtigungen“ möglich sein müssen. Allerdings muss es das Anliegen des Eingriffs sein, Güter zu schützen, denen auch sonst von der Rechtsordnung ein besonderes Gewicht beigemessen wird. Ein Richtervorbehalt zur prozeduralen Absicherung des Telekommunikationsgeheimnisses ist hingegen nicht erforderlich,

BVerfGE 125, 260 (342 f.).

Die Beschwerdeführer sind von diesen Aussagen des Bundesverfassungsgerichts aus dem Jahr 2010, von denen das Gericht auch noch im Jahr 2012 nicht abgerückt zu sein scheint,

BVerfGE 130, 151 (205 f.) verlangt lediglich, dass Eingriffe auf der Grundlage klarer Ermächtigungsgrundlagen zu erfolgen haben,

nicht überzeugt. Sie erläutern, dass die Identifizierung von Internetnutzern über dynamische IP-Adressen eine erheblich größere Persönlichkeitsrelevanz aufweist und damit einen schwereren Grundrechtseingriff darstellt, als die Identifizierung einer Telefonnummer. Die Kenntnis der IP-Adressen ermöglicht in weitem Umfang eine Deanonymisierung von Kommunikationsvorgängen im Internet,

so auch BVerfGE 130, 151 (204).

Dass die aus diesem Umstand resultierende besondere Persönlichkeitsrelevanz klare Voraussetzungen für den Grundrechtseingriff erfordert ist unstreitig. Daher hat der Landesgesetzgeber die Bedeutung des Grundrechtseingriffs zum Anlass genommen, nicht nur den Gegenstand der Abfrage zu begrenzen, sondern auch durch eine Normierung anspruchsvoller materieller Voraussetzungen und prozeduraler Sicherungen, die über die Vorgaben des Bundesverfassungsgerichts hinausgehen, die Zulässigkeit entsprechender Abfragen zu begrenzen und damit die Verhältnismäßigkeit der Norm sicherzustellen,

vgl. hierzu auch Erwägungen in dem Gesetzentwurf der Landesregierung, LT-Drs. SH 18/713, S. 9.

Diese Begrenzung erfolgt durch materielle wie auch durch prozedurale Sicherungen.

Zunächst wird die im Vergleich zu den einfachen Bestandsdaten des § 180a Abs. 1 LVwG größere Sensibilität und Persönlichkeitsrelevanz dadurch deutlich, dass § 180a Abs. 2 Satz 2 LVwG die identifizierende Zuordnung dynamischer IP-Adressen auf Fälle begrenzt, in denen

die Auskunft zur Abwehr einer im einzelnen Fall bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person sowie zur Abwehr einer gegenwärtigen Gefahr eines gleichgewichtigen Schadens für Sach- oder Vermögenswerte oder für die Umwelt erforderlich ist. Es reicht also nicht jedwede Gefahr für das Schutzgut der öffentlichen Sicherheit aus (vgl. § 180a Abs. 1 LVwG), sondern es muss eine Gefahr für eines der genannten Rechtsgüter vorliegen. Insoweit ist der Gesetzgeber im Laufe des Gesetzgebungsverfahrens,

vgl. Bericht und Beschlussempfehlung des Innen- und Rechtsausschusses, LT-Drs. SH 18/928, S. 3,

den Forderungen des ULD im Gesetzgebungsverfahren,

Umdruck Schleswig-Holsteinischer Landtag 18/1245, S. 2,

umfassend nachgekommen. Bereits durch diese erhöhte Eingriffsschwelle verdeutlicht der Gesetzgeber die besondere Sensibilität für diese Form der Datenabfrage und führt eine Differenzierung gegenüber der einfachen Bestandsdatenabfrage, die schon bei Vorliegen einer konkreten Gefahr ohne ausdrückliche Begrenzung auf bestimmte polizeiliche Schutzgüter zulässig ist.

Das in § 180a Abs. 2 Satz 2 LVwG verwendete Tatbestandsmerkmal der im einzelnen Fall bevorstehenden Gefahr ist dabei – entgegen den Ausführungen der Beschwerdeführer – mit dem Begriff der konkreten Gefahr identisch (dazu oben, zu 3.1.1.).

Diese materiellen Anforderungen gehen über die Forderung des Bundesverfassungsgerichts hinaus, nach der solche Auskünfte „auch unabhängig von begrenzenden Rechtsgüter- und Straftatenkatalogen für die Verfolgung von Straftaten, für die Gefahrenabwehr und die Aufgabenerfüllung der Nachrichtendienste auf Grundlage der allgemeinen fachrechtlichen Ermächtigungen“ möglich sein müssen und allein solche Güter zu schützen haben, denen auch sonst von der Rechtsordnung ein besonderes Gewicht beigemessen wird,

BVerfGE 125, 260 (342 f.).

Im Hinblick auf die polizeilichen Schutzgüter halten die Beschwerdeführer die Regelung des § 180a Abs. 2 Satz 2 LVwG insoweit für widersprüchlich, als dass ein Schaden für Sach- oder Vermögenswerte oder für die Umwelt nie einer Verletzung von Leib, Leben oder Freiheit einer Person gleichgewichtig sein könne. Die Beschwerdeführer verkennen jedoch, dass § 180a Abs. 2 Satz 2 LVwG das Bestehen einer *gegenwärtigen* Gefahr eines gleichgewichtigen Schadens für Sach- oder Vermögenswerte oder für die Umwelt voraussetzt und somit für diese Rechtsgüter besondere Anforderungen an die zeitliche Nähe des Schadenseintritts stellt. Die Einbeziehung von Sach- und Umweltschäden als solche ist entgegen den Ausführungen der Be-

schwerdeführer dabei auch nicht grob unverhältnismäßig. Das Bundesverfassungsgericht fordert lediglich eine Rechtsgutbeeinträchtigung, der von der Rechtsordnung auch sonst ein hervorgehobenes Gewicht beigemessen wird,

BVerfGE 125, 260 (344); so auch Ansicht des ULD, Umdruck Schleswig-Holsteinischer Landtag 18/1245, S. 2).

Aber auch in prozeduraler Hinsicht verschärft der Gesetzgeber den Zugriff auf diese Daten gegenüber der Abfrage einfacher Bestandsdaten deutlich und geht dabei über die Vorgaben des Bundesverfassungsgerichts hinaus:

So sieht § 180b Abs. 1 Satz 1 LVwG für Personenauskünfte zu dynamischen IP-Adressen einen Richtervorbehalt und damit eine vorbeugende Kontrolle durch eine unabhängige und neutrale Instanz vor. Zudem sichern Benachrichtigungspflichten die Kenntnis des Betroffenen von der Maßnahme, § 180b Abs. 1 Satz 8 LVwG. Daneben ordnet § 186b Abs. 1 Satz 2 LVwG eine parlamentarische Kontrolle der Abfragen an.

Die landesrechtlichen Vorschriften über die Identifizierung von Internetnutzern mittels dynamischer IP-Adressen berücksichtigen somit vollumfänglich die erhöhte Eingriffsintensität dieser Maßnahme im Vergleich zu einfachen Bestandsdatenabfragen nach § 180a Abs. 1 LVwG, indem sie diese von gesteigerten materiellen Anforderungen abhängig machen und die verhältnismäßige Anwendung im Einzelfall durch Verfahrenssicherungen gewährleisten.

Die Beschwerdeführer fordern darüber hinaus jedoch eine Anpassung der Voraussetzungen der Identifizierung eines Internetnutzers anhand einer dynamischen IP-Adresse an die Eingriffsschwellen für Verkehrsdatenabfragen, namentlich an die Tatbestandsmerkmale des § 185a LVwG, um eine „Diskriminierung“ von Internetverbindungen zu vermeiden. Indes ist nicht zu übersehen, dass die beiden Ermächtigungsgrundlagen einander hinsichtlich der Eingriffsstrenges in materieller und prozeduraler Hinsicht durchaus ähneln. Auch gehen die Beschwerdeführer bei ihren Ausführungen offenbar (aber fälschlicherweise; vgl. § 180b Abs. 1 LVwG) davon aus, dass die Abfrage der dynamischen IP-Adressen ohne richterliche Ermächtigung zulässig ist,

Beschwerdeschrift, S. 12,

sodass der Vorwurf der Diskriminierung insoweit auf einem Missverständnis beruht.

Insgesamt überspitzen die Beschwerdeführer aber die von ihnen geforderten Anforderungen an den Eingriff und übersehen dabei die verschiedenen, der Verhältnismäßigkeit der Maßnahme dienenden Sicherungen, derer der Gesetzgeber sich bedient hat. Deren Gebotenheit richtet sich

grundsätzlich nach der Schwere des Eingriffs in das Telekommunikationsgeheimnis. Das Bundesverfassungsgericht hat die in Rede stehenden Auskünfte insoweit zwar als schwer und an besondere Voraussetzungen zu knüpfen, dennoch nicht aber als gleich eingriffsintensiv wie die Abfrage von Verkehrsdaten bewertet,

BVerfGE 125, 260 (340 f.).

Dass eine Gleichstellung der hier relevanten Bestandsdaten mit Verkehrsdaten nicht aufgrund Verhältnismäßigkeitsgrundsatzes verfassungsrechtlich geboten ist, ergibt sich nach einer Abwägung zwischen dem Gewicht der durch eine Bestandsdatenabfrage mittels dynamischer IP-Adresse beeinträchtigten Grundrechte einerseits sowie der durch sie verfolgten Gemeinwohlinteressen andererseits. Diese Abwägung hat das Bundesverfassungsgericht bereits in seiner o.a. Entscheidung zur sog. Vorratsdatenspeicherung und zu § 113 TKG in dem Sinne vorgenommen, den der schleswig-holsteinische Gesetzgeber in seinen Regelungen nachvollzogen hat. Insbesondere die vom Bundesverfassungsgericht bemängelten Defizite in dem Bereich der Normenklarheit,

BVerfGE 130, 151 (200 ff.),

hat der schleswig-holsteinische Gesetzgeber auch bei der Abfrage der Zuordnung von IP-Adressen beseitigt. Ein Eingriff in Art. 10 GG liegt zwar vor, weil zur Beantwortung der Abfrage einer IP-Adresse auf die gespeicherten Verkehrsdaten zugegriffen werden muss und diese ausgewertet werden müssen,

BVerfGE 130, 151 (183, 204).

Dies gilt sowohl für die Auskunft über dynamische IP-Adressen als in ihrer Gestalt als Auskunft über die Nutzer bereits bekannter dynamischer Adressen,

BVerfGE 125, 260 (341 f.),

als auch in ihrer Form als Mitteilung der noch unbekannten dynamischen IP-Adresse als solcher,

BVerfGE 130, 151 (181 f.).

Dennoch ist indes nach Ansicht des Gerichts dieser interne Rückgriff auf Verkehrsdaten zur Vorbereitung der Auskunft nicht als ebenso eingriffsintensiv wie die Abfrage von Verkehrsdaten zu bewerten,

BVerfGE 125, 260 (340 f.); dieser Ansicht folgend: *Dalby*, CR 2013, S. 361 ff. (365); ebenso Stellungnahme des ULD, Umdruck Schleswig-Holsteinischer Landtag 18/1245, S. 2.

„Da die Brücke zwischen den mit der bekannten IP-Adresse und den als Auskunft zu übermittelnden Bestandsdaten nur durch eine Auswertung der Verkehrsdaten hergestellt werden kann, liegt die Eingriffsqualität der Personenauskunft letztlich zwischen beiden Befugnissen“,

Bär, MMR 2013, S. 700 ff. (703).

Insbesondere wird durch die Bezugnahme auf die „zu einem bestimmten Zeitpunkt [zugewiesene] Internet-Protokoll Adresse“ sichergestellt, dass eine generelle Abfrage zur Verwendung einer IP-Adresse ohne Begrenzung ausgeschlossen ist, um die Grenze zur Verkehrsdatenabfrage zu respektieren,

so zu § 100j StPO *Bär*, MMR 2013, S. 700 ff. (703).

Insgesamt bleibt daher festzuhalten, dass der Landesgesetzgeber mit der Normierung der materiellen und prozeduralen die für die Abfrage einer Zuordnung dynamischer IP-Adressen, über die Anforderungen, die das Bundesverfassungsgericht in seiner Entscheidung zur Vorratsdatenspeicherung bestimmt hat, hinausgeht. Den rechtspolitischen Wünschen der Beschwerdeführer könnte vermutlich nur entsprochen werden, wenn der Gesetzgeber eine solche Abfrage gänzlich unterbinden würde. Dass eine solche Ignoranz gegenüber der Nutzung des Internets als Medium zur Gefährdung von Rechtsgütern weder geboten noch erforderlich ist, hat das Bundesverfassungsgericht aber ebenfalls deutlich gemacht,

BVerfGE 125, 260 (342 f.).

9. Zu 3.1.9.: Soziale Netzwerke und Internetdienste (Telemedien)

Die Beschwerdeführer beanstanden die durch den in § 180a Abs. 4 LVwG enthaltenen Verweis auf die Voraussetzungen der Abs. 1 - 3 herbeigeführte Gleichstellung der Auskunftsvoraussetzungen über Bestandsdaten von Telemediendiensten mit den Voraussetzungen für die Auskunft über Bestandsdaten von Telekommunikationsdiensten. Der durch § 180a Abs. 4 LVwG eröffnete Zugriff auf Telemedien-Bestandsdaten stelle einen erheblich intensiveren Grundrechtseingriff dar als der bloße Zugriff auf Telekommunikations-Bestandsdaten,

Beschwerdeschrift, S. 16 f.

Informationen über Telemedien-Bestandsdaten können durchaus aufschlussreicher sein als die Bestandsdaten eines Telekommunikationsdienstes, da sie zugleich Rückschlüsse auf den Inhalt des genutzten Telemedienangebots zulassen,

vgl. hierzu insbes. die Stellungnahme des ULD, Umdruck Schleswig-Holsteinischer Landtag 18/1245, 2 f.; ebenso Stellungnahme der Neuen Richtervereinigung, Umdruck Schleswig-Holsteinischer Landtag 18/1250, S. 2).

Während sich Telekommunikationsdienste auf Verträge mit Telefon-, Mobilfunk-, E-Mail- oder vergleichbaren Anbietern beschränken, umfassen Telemediendienste Verträge mit Online-Shops, Informationsdiensten, Internetportalen, Suchmaschinen, Chatrooms, Dating-Communitys, Blogs oder vergleichbaren Diensten. Bei bestimmten Telemedien-Angeboten können bereits die Bestandsdaten Rückschlüsse auf die Gesundheit, politische oder religiöse Überzeugungen oder ähnlich sensible Sachverhalte ermöglichen. Dies betrifft etwa Gesundheitsportale, Internet-Angebote von Kirchen oder politischen Parteien oder Angebote von Beratungsstellen,

Stellungnahme des ULD, Umdruck Schleswig-Holsteinischer Landtag 18/1245, S. 2 f.

Allerdings lassen die Beschwerdeführer unbeachtet, dass der Gesetzgeber diese Eingriffsintensität durchaus berücksichtigt und an den Abruf von Telemedien-Bestandsdaten nach § 180a Abs. 4 LVwG im Gegensatz zu einfachen Bestandsdatenabfragen nach § 180a Abs. 1 LVwG sehr deutlich erhöhte Anforderungen gestellt hat.

Zum einen muss eine konkrete Gefahr für besonders bedeutsame Schutzgüter vorliegen. Eine bloße Gefahr für das Schutzgut der öffentlichen Sicherheit ist also nicht ausreichend. Diese Verschärfung ist im Laufe des Gesetzgebungsverfahrens durch den Innen- und Rechtsausschuss in den Entwurf eingefügt worden,

Bericht und Beschlussempfehlung des Innen- und Rechtsausschusses, LT-Drs. SH 18/928, S. 4.

Durch diese erhöhte Eingriffsschwelle verdeutlicht der Gesetzgeber die besondere Sensibilität für diese Form der Datenabfrage und nimmt eine Differenzierung gegenüber der einfachen Bestandsdatenabfrage vor.

Zum andern gelten nach § 180b Abs. 2 LVwG strengere Verfahrensvorschriften als bei der einfachen Bestandsdatenauskunft nach § 180a Abs. 1 LVwG, da die prozeduralen Voraussetzungen wie bei der qualifizierten Bestandsdatenabfrage (v.a. Richtervorbehalt und Benachrichtigungspflicht) einzuhalten sind. Dies ist den Beschwerdeführern offenbar entgangen,

Beschwerdeschrift, S. 16: „ohne richterliche Anordnung“.

Ferner unterliegt die Landesregierung einer Berichtspflicht gegenüber dem Landtag, § 186b Abs. 1 Satz 2 LVwG.

Diese strengeren Voraussetzungen und prozeduralen Absicherungen lassen den Zugriff auf Telemedien-Bestandsdaten insgesamt als verhältnismäßig erscheinen, da der Gesetzgeber mit ihnen zum Ausdruck gebracht hat, dass ihm die Sensibilität der fraglichen Daten durchaus bewusst war.

Die Beschwerdeführer verlangen indes, dass Telemedien-Nutzungsdaten nur unter denselben Voraussetzungen erhoben werden dürfen wie § 185a LVwG es für die Abfrage von Verkehrsdaten der Telekommunikation vorsieht. Dies folge aus der erhöhten Eingriffsintensität des Abrufens von Telemedien-Nutzungsdaten, die mit der Eingriffsintensität des Abrufens von Verkehrsdaten der Telekommunikation vergleichbar sei. Aus diesem Grunde zweifeln die Beschwerdeführer an der Verhältnismäßigkeit der Vorschrift.

In der Tat weisen diese Nutzungsdaten eine deutliche Nähe zu den Verkehrsinformationen der Telekommunikation und damit einen ähnlichen Schutzbedarf auf,

Karg, Zugriff von Ermittlungsbehörden auf Nutzungsdaten bei der Strafverfolgung, DuD 2015, S. 85 ff. (86); *von der Grün*, BeckOK Polizeirecht BW, 2015, § 23a PolG Rn. 42; Stellungnahme des ULD, Umdruck Schleswig-Holsteinischer Landtag 18/1245, 2.

Allerdings wird der Abruf der Nutzungsdaten durch § 180a Abs. 4 LVwG dahingehend begrenzt, dass nur Angaben zur Identifikation des Nutzers sowie Datum und Uhrzeit der entsprechenden Nutzung des Telemediendienstes erhoben werden dürfen. Somit richten sich die Auskunftsbefugnisse gerade nicht auf Angaben über den Umfang der jeweiligen Nutzung und Angaben über die vom Nutzer in Anspruch genommenen Telemedien. Ebenso wenig sind darüber hinaus von den Telemediendiensten erfasste Nutzungsdaten von der Ermächtigung des § 180a Abs. 4 LVwG erfasst. Hierdurch wird die Sensibilität der in Anspruch genommenen Daten deutlich herabgesetzt und damit die Verhältnismäßigkeit des Eingriffs hergestellt.

Die Beschwerdeführer rügen zudem, § 180a Abs. 4 LVwG stelle durch die Erwähnung der „Identifikation der Nutzer“ einen Verstoß gegen das Gebot der Normenklarheit dar. Diese Rüge kann allerdings durch eine systematische Auslegung vor dem Hintergrund der Begrifflichkeiten des § 15 TMG entkräftet werden.

§ 180a Abs. 4 LVwG verweist auf Daten i.S.d. § 15 TMG, beschränkt die Auskunftsbefugnis allerdings auf die Identifikation der Nutzer und auf das Datum und die Uhrzeit des Beginns und

Endes der Nutzung. Damit übernimmt § 180a Abs. 4 LVwG die im Katalog des § 15 Abs. 1 TMG aufgeführten Begrifflichkeiten nahezu wortwörtlich. Von § 180a Abs. 4 LVwG sind somit eindeutig lediglich die Nutzungsdaten nach § 15 Abs. 1 Satz 2 Nr. 1 und Nr. 2 Alt. 1 TMG umfasst. Welche Daten das sind, ist der einschlägigen Literatur zum TMG zu entnehmen. Die Vorschrift genügt somit dem Bestimmtheitsgebot.

Soweit § 180 Abs. 4 LVwG von „Identifikation der Nutzer“ handelt, während das TMG die „Identifikation des Nutzers“ benennt, scheint dies ein Redaktionsversehen zu sein. Zumindest deuten die Gesetzesbegründungen auf kein anderes Verständnis hin. Insbesondere wäre es angesichts einer systematischen Auslegung abwegig, davon auszugehen, dass hier eine Ermächtigungsgrundlage zur Auskunft über *alle* Nutzer eines Telemediendienstes geschaffen werden soll.

Die Beschwerdeführer rügen darüber hinaus zu Unrecht, dass sich aus dem Verweis in § 180a Abs. 4 LVwG auf die § 180a Abs. 1 bis 3 LVwG nicht ergibt, welche dieser Vorschriften auf welche Anfrage Anwendung finden sollen. Die Tatbestandsvoraussetzungen für den Eingriff (insbesondere der Gefahrbegriff und die betroffenen Schutzgüter) sind bereits in Absatz 4 selbst aufgeführt. Der Verweis auf Absatz 1 ist damit nur noch ein Verweis auf das anzuwendende Verfahren nach § 180a Abs. 1 Satz 2 LVwG. Der Verweis auf Absatz 2 bezieht sich auf die zusätzlichen Voraussetzungen in § 180a Abs. 2 Satz 1 LVwG beziehen („wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen“) und findet beim Abrufen von Passwörtern Anwendung.

Damit bleibt im Ergebnis festzuhalten, dass der Gesetzgeber auch bei der Normierung von § 180a Abs. 4 LVwG eine Regelung gefunden hat, die die Eingriffstiefe durch materielle wie prozedurale Sicherungen in verhältnismäßiger Weise rechtfertigt.

IV. § 8a Abs. 1 Landesverfassungsschutzgesetz

1. Zu 3.2.1.: Eingriffsschwelle der Erforderlichkeit zur Aufgabenerfüllung

Die Beschwerdeführer rügen die Eingriffsschwelle in § 8a Abs. 1 LVerfSchG, welche Zugriffe auf Bestandsdaten durch den Verfassungsschutz zulässt, soweit dies zur Erfüllung der Aufgaben der Verfassungsschutzbehörde erforderlich ist.

Dieser Verweis in § 8a Abs. 1 LVerfSchG auf die Aufgaben nach § 1 LVerfSchG entspricht nach Auffassung der Beschwerdeführer nicht den Anforderungen, die sich aus der Rechtsprechung des BVerfG hinsichtlich der Möglichkeit von Bestandsdatenabfragen durch Verfas-

sungsschutzbehörden ergeben. Danach ist Voraussetzung einer verhältnismäßigen Bestandsdatenabfrage, dass diese „zur Aufklärung einer bestimmten, nachrichtendienstlich beobachtungsbedürftigen Aktion oder Gruppierung geboten sein muss“,

BVerfGE 130, 151 (206).

Die in dem von den Beschwerdeführer angeführten Beschluss des Bundesverfassungsgerichts auf ihre Verfassungsmäßigkeit überprüfte Norm (§ 113 TKG a.F.) benannte diese Voraussetzung allerdings ebenfalls nicht ausdrücklich. Das Gericht leitete sie dennoch im Wege der Auslegung ab. § 113 Abs. 1 Satz 1 TKG a.F. sah als Eingriffsschwelle für die Übermittlung von Bestandsdaten durch die Auskunftspflichtigen vor, dass die Daten im Einzelfall „für die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder“ erforderlich sein müssen.

Obwohl § 113 Abs. 1 Satz 1 TKG a.F. also lediglich auf die Aufgaben der Verfassungsschutzbehörden als Eingriffsschwelle verwies, urteilte das Bundesverfassungsgericht, dass sich bereits aus dem Erfordernis der Erforderlichkeit im Einzelfall ergebe, dass eine Auskunft „zur Aufklärung einer bestimmten, nachrichtendienstlich beobachtungsbedürftigen Aktion oder Gruppierung geboten sein muss“ (s.o.).

Entsprechend ist auch die Regelung des § 8a Abs. 1 LVerfSchG auszulegen. Aus dem Tatbestandsmerkmal der Erforderlichkeit im Einzelfall ergibt sich die von den Beschwerdeführern geforderte Eingriffsschwelle.

Zudem legt § 7 Abs. 1 LVerfSchG fest, dass – soweit das LVerfSchG nichts anderes bestimmt – die Verfassungsschutzbehörde bei der Wahrnehmung ihrer Aufgaben nach § 5 Abs. 1 LVerfSchG nur tätig werden darf, wenn tatsächliche Anhaltspunkte für den Verdacht der dort genannten Bestrebungen oder Tätigkeiten vorliegen. § 7 Abs. 2 LVerfSchG sichert darüber hinaus die Verhältnismäßigkeit der Maßnahme im Einzelfall. Somit trägt das LVerfSchG den Anforderungen des Bundesverfassungsgerichts durch Anwendung § 7 Abs. 1 und 2 LVerfSchG Rechnung.

2. Zu 3.2.2.: Fehlende Beschränkung auf Einzelfälle

Die Beschwerdeführer rügen eine fehlende Beschränkung der Maßnahmen nach § 8a Abs. 1 LVerfSchG auf Einzelfälle. Allerdings sehen § 8a Abs. 1 Satz 1 und Satz 2 LVerfSchG ausdrücklich eine Befugnis der Verfassungsschutzbehörde „im Einzelfall“ vor. Darüber hinaus kann auch an dieser Stelle auf die Ausführungen zu Gliederungspunkt 3.1.2. verwiesen werden. Die dort angestellten Erwägungen lassen sich auf die Bestandsdatenauskünfte nach § 8a Abs. 1 LVerfSchG übertragen.

3. Zu 3.2.3.: Fehlende Beschränkung auf polizeilich Verantwortliche

Die von den Beschwerdeführern mit Blick auf § 180a Abs. 1 LVwG ebenso wie hier gerügte fehlende Beschränkung des Tatbestands auf Störer vermag in Anbetracht des Regelungszusammenhangs der §§ 8a Abs. 1, 7 Abs. 1 LVerfSchG und vor dem Hintergrund der geringen Eingriffstiefe der Bestandsdatenabfrage eine Verfassungswidrigkeit der Norm nicht zu begründen.

Zum einen stellt sich angesichts des geringen Eingriffsgewichts bereits die Frage, ob eine Beschränkung in Anlehnung an die polizeirechtliche Verantwortlichkeit überhaupt erforderlich ist,

ablehnend insoweit in ähnlichem Zusammenhang BVerfGE 130, 151 (206 f.).

Zum andern kann die Verfassungsschutzbehörde gem. § 7 Abs. 1 LVerfSchG 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 ist Voraussetzung für eine Bestandsdatenabfrage gemäß § 8a Abs. 1 LVerfSchG, dass sich aufgrund tatsächlicher Umstände Verdachtsmomente ergeben, die eine Zuordnung des Betroffenen zu einer beobachtungsbedürftigen Bestrebung oder Tätigkeit im Sinne von § 5 Abs. 1 LVerfSchG erlauben.

Eine weitere Einschränkung des möglichen Adressatenkreises der Maßnahmen nach § 8a Abs. 1 LVerfSchG ergibt sich auch hier aus dem Übermaßverbot,

Bär, Die Neuregelung des § 100j StPO zur Bestandsdatenauskunft, Auswirkungen auf die Praxis der Strafverfolgung, MMR 2013, S. 700 ff. (702).

Damit stellt der Gesetzgeber in hinreichendem Maße sicher, dass kein Grundrechtsträger ohne jeden zurechenbaren Anlass Adressat einer entsprechenden Maßnahme wird.

4. Zu 3.2.4.: Mangelnder Rechtsschutz wegen fehlender Benachrichtigung

Die Beschwerdeführer rügen, dass bei Maßnahmen nach § 8a Abs. 1 LVerfSchG eine verfassungsrechtlich gebotene Benachrichtigung Betroffener von Datenauskünften nicht vorgesehen ist.

Dieser Anwurf blendet aus, dass § 8a Abs. 7 Satz 3 LVerfSchG durchaus die Benachrichtigung Betroffener in einer Vielzahl der Fälle verlangt. Lediglich im Hinblick auf Auskunftsverlangen nach § 8a Abs. 1 Satz 1 und Satz 2 LVerfSchG sieht § 8a Abs. 7 Satz 2 LVerfSchG keine

Benachrichtigungspflicht gegenüber den Betroffenen vor. Dies gründet jedoch auf der niedrigeren Eingriffsintensität des bloßen Abrufens von einfachen Telemedien- und Telekommunikations-Bestandsdaten. Das vom Gesetz vorgesehene Verfahren, das nach dem Kriterium der Eingriffsintensität differenziert, ist damit verhältnismäßig (vgl. dazu ausführlich die zu dem Gliederungspunkt 3.1.4. angestellten Erwägungen).

5. Zu 3.2.5.: Mangelnde Kontrolle durch fehlende Statistik

Die Beschwerdeführer rügen das Fehlen einer Regelung zur statistischen Erfassung der Bestandsdatenabfragen nach § 8a LVerfSchG. Eine solche sei erforderlich, um eine Überprüfung und Evaluierung der Maßnahmen zu ermöglichen und folge aus dem Verhältnismäßigkeitsgrundsatz.

Neben den bereits oben unter 3.1.5. dargelegten allgemeinen Ausführungen ist insoweit darauf hinzuweisen, dass § 8a Abs. 8 LVerfSchG für die grundrechtsintensiven Anordnungen nach § 8a Abs. 2 LVerfSchG eine Unterrichtungspflicht des Parlamentarischen Kontrollgremiums vorsieht. Für Maßnahmen nach § 8a Abs. 1 LVerfSchG ist eine Unterrichtung des Parlamentarischen Kontrollgremiums hingegen nicht vorgesehen, da diese deutlich weniger eingriffsintensiv sind.

Zudem trifft den Gesetzgeber auch hier unter bestimmten Voraussetzungen eine verfassungsunmittelbare Beobachtungs- und Korrekturpflicht bei Gesetzen, die in Grundrechte eingreifen,

BVerfGE 112, 304 (316),

sodass es einer besonderen und ausdrücklichen Normierung entsprechender Beobachtungspflichten nicht bedarf.

6. Zu 3.2.6.: Mangelnde Klarheit der Befugnisse zur Abfrage von Zugangssicherungs-codes

Im Gegensatz zu § 180a Abs. 2 Satz 1 LVwG, der einen abgeschlossenen Katalog von Maßnahmen vorsieht, für die Zugangssicherungs-codes verwendet werden dürfen und bestimmt, dass die Voraussetzungen für die Durchführung dieser Maßnahmen bereits bei entsprechenden Auskunftsverlangen vorliegen müssen, verweist § 8a Abs. 1 Satz 3 LVerfSchG lediglich darauf, dass die Auskunft nur verlangt werden darf, sofern auch die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen.

Die Beschwerdeführer rügen diesbezüglich einen Verstoß gegen das Gebot der Normenklarheit.

Allerdings setzt § 8a Abs. 1 Satz 3 LVerfSchG die Vorgaben des Bundesverfassungsgerichts aus dem Beschluss vom 24. Januar 2012 vollumfänglich um. Das Gericht hatte gefordert, dass Behörden Zugangssicherungs_codes nur dann abfragen dürfen, wenn sie im Einzelfall auch zur Nutzung der durch sie geschützten Daten berechtigt sind,

BVerfGE 130, 151 (207 ff.).

Dadurch wollte das Gericht eine Umgehung von im Einzelfall strengeren Voraussetzungen der fachrechtlichen Befugnisnorm für den Zugriff auf die hinter den Zugangssicherungsdaten liegenden Inhalte verhindern.

Der Gesetzgeber hat für das LVerfSchG den von dem Bundesverfassungsgericht verwendeten Passus („wenn die gesetzlichen Voraussetzungen für die Nutzung vorliegen“) übernommen und stellt damit sicher, dass die Zugangssicherungs_codes nicht unter leichteren Voraussetzungen erlangt werden können als es die einschlägigen Befugnisnormen für den Zugriff auf die zugangsgeschützten Inhaltsdaten vorsehen. Durch die offene Formulierung wird sichergestellt, dass die Voraussetzung für die Herausgabe des Zugangssicherungs_codes mit der Eingriffstiefe der jeweiligen Anschlussmaßnahme korreliert,

Dalby, CR 2013, S. 361 ff. (365).

Es mag zwar rechtspolitisch vorbildlich sein, wenn Ermächtigungsgrundlagen zur Datenabfrage – wie etwa § 180a Abs. 2 Satz 1 LVwG – eine abschließende Aufzählung der zulässigen Nutzungszwecke durch Benennung weiterer Ermächtigungsgrundlagen regelt. Es darf aber nicht vergessen werden, dass dies in den gesetzlichen Regelungen zu Bestandsdatenabfragen eher eine Seltenheit darstellt. Die meisten bundes- und landesrechtlichen Normen verwenden ebenfalls den abstrakten Passus des Bundesverfassungsgerichts (bspw. § 100j Abs. 1 Satz 2 StPO, § 8d Abs. 1 Satz 2 BVerfSchG, § 22 Abs. 2 Satz 2 BKAG, § 24b Abs. 1 Satz 2 LVerfSchG M-V).

Ein Verstoß gegen die Normenklarheit liegt daher nicht vor, da die Eingriffsvoraussetzungen durch die Zusammenführung der hier in Streit stehenden Norm mit einer weiteren Ermächtigungsgrundlage ermittelt werden können.

7. Zu 3.2.7.: Fehlende Subsidiarität des Zugriffs auf Zugangssicherungs_codes (PINs, Passwörter)

Der von den Beschwerdeführern geforderten Subsidiaritätsklausel bedarf es nicht (vgl. dazu ausführlich die zu dem Gliederungspunkt 3.1.6. angestellten Erwägungen).

8. Zu 3.2.8.: Mangelnde Sicherheit erhobener Zugangssicherungscodes

Die Beschwerdeführer rügen, dass § 8a Abs. 1 Satz 3 LVerfSchG keinerlei Vorkehrungen zur Gewährleistung der Sicherheit erhobener Zugangssicherungscodes trifft. Derartige Vorkehrungen sind jedoch dann nicht erforderlich, wenn der Betroffene nachträglich Kenntnis von der Datenabfrage erlangt und somit dazu in der Lage ist, neue Zugangssicherungen zu erstellen. Der ursprünglich im Rahmen der Datenabfrage erlangte Zugangssicherungscode weist in der Folge keinen Personenbezug mehr auf, da er keinen Zugriff auf personenbezogene Daten mehr erlaubt (vgl. dazu ausführlich die zu dem Gliederungspunkt 3.1.7. angestellten Erwägungen). Die Kenntnis des Betroffenen von Maßnahmen nach § 8a Abs. 1 Satz 3 LVerfSchG sichert § 8a Abs. 7 Satz 3 LVerfSchG.

Daneben ergibt sich aus § 14 Abs. 1 Nr. 2 LVerfSchG, dass die Zugangssicherungscodes zu löschen sind, wenn ihre Kenntnis für die Aufgabenerfüllung nicht mehr erforderlich ist.

9. Zu 3.2.9.: Unzureichende Eingriffsschwellen für Identifizierung von IP-Adressen

Die Beschwerdeführer fordern, dass angesichts der größeren Eingriffsintensität der Identifizierung von Internetnutzern über dynamische IP-Adressen die Verfassungsschutzbehörde Abfragen nach § 8a Abs. 1 Satz 4 LVerfSchG nur bei Vorliegen einer konkreten Gefahr tätigen dürfe. Ferner rügen die Beschwerdeführer, dass die rechtlichen und tatsächlichen Grundlagen entsprechender Auskunftsbegleichen aktenkundig zu machen sind.

Bei diesen Forderungen handelt es sich jeweils um Elemente der Verhältnismäßigkeit des Grundrechtseingriffs, deren konkrete Anforderungen durch die Intensität des Grundrechtseingriffs determiniert werden.

Das Bundesverfassungsgericht hat indes ausdrücklich klargestellt, dass Nachrichtendienste grundsätzlich unabhängig von konkreten Gefahren in deren Vorfeld tätig werden. Angesichts ihrer beschränkten Aufgaben, die nicht unmittelbar auf polizeiliche Maßnahmen ausgerichtet sind, ist eine niedrigere Eingriffsschwelle für Bestandsdatenabfragen aber dennoch rechtlich zulässig,

BVerfGE 130, 151 (205 f.).

Das Erfordernis der konkreten Gefahr findet aber auch durch die Regelung des § 7 Abs. 1 LVerfSchG Berücksichtigung. Danach ist Voraussetzung für ein Tätigwerden der Verfassungsschutzbehörde bei der Wahrnehmung ihrer Aufgaben nach § 5 Abs. 1 LVerfSchG, dass tatsächliche Anhaltspunkte für den Verdacht der dort genannten Bestrebungen oder Tätigkeiten vorliegen.

Der Landesgesetzgeber hat der größeren Eingriffsintensität der Identifizierung von Internetnutzern über dynamische IP-Adressen zudem durch die in § 8a Abs. 7 LVerfSchG normierten, erhöhten Anordnungs- und Unterrichtungspflichten Rechnung getragen, die jeweils zur Verhältnismäßigkeit der Maßnahme beitragen,

Gesetzentwurf der Landesregierung, LT-Drs. SH 18/713, S. 16.

Dabei sehen §§ 8a Abs. 7 Satz 1, 8b Abs. 1 Satz 2 LVerfSchG auch vor, dass in einem schriftlichen Antrag die rechtlichen und tatsächlichen Grundlagen der Abfrage nach § 8a Abs. 1 Satz 4 LVerfSchG dargelegt werden. Ferner besteht durch die Unterrichtung der G10-Kommission über derartige Maßnahmen eine weitere Kontrollbefugnis. Eine solche Inanspruchnahme des Parlaments zum Zwecke der Kontrolle von Tätigkeiten des Verfassungsschutzes, auch wenn sie Auswirkung auf die individuelle Grundrechtsausübung hat, ist durchaus üblich und auch zum Schutz der Funktionsfähigkeit dieser Dienste erforderlich,

Zumindest hinsichtlich der Anordnungs- und Unterrichtungspflichten besteht damit eine Gleichstellung dieser Bestandsdaten mit den Verkehrsdaten,

Gesetzentwurf der Landesregierung, LT-Drs. SH 18/713, S. 16.

Des Weiteren fordern die Beschwerdeführer, dass an die Identifizierung von Internetnutzern auch materiell dieselben Anforderungen gestellt werden wie an sonstige Eingriffe in das Fernmeldegeheimnis. Eine derartige Gleichsetzung ist nach der Rechtsprechung des Bundesverfassungsgerichts hingegen nicht erforderlich. Zur Begründung wird auf die Ausführungen zum Gliederungspunkt 3.1.8. verwiesen.

10. Zu 3.2.10.: Soziale Netzwerke und Internetdienste (Telemedien)

Wie von den Beschwerdeführern dargelegt, kann der Zugriff auf Telemedien-Nutzungsdaten durch den Verfassungsschutz nicht mehr in zulässiger Weise durch die vorliegende Verfassungsbeschwerde angegriffen werden.

D. Ergebnisse

Die Verfassungsbeschwerde ist weder zulässig noch begründet.

1. Unzulässigkeit der Verfassungsbeschwerde:

- a. Die Beschwerdeführer treten nicht als Grundrechtsträger, sondern als (ehemalige) Abgeordnete des Schleswig-Holsteinischen Landtags auf und machen bei ihrem Vortrag zur Zulässigkeit nicht Grundrechte, sondern Statusrechte geltend und
- b. sie verfügen – unabhängig von (1.a.) – zudem nicht über die erforderliche Beschwerdebefugnis, weil sie durch die angegriffenen Normen nicht unmittelbar in Grundrechten betroffen sind.

2. Unbegründetheit der Verfassungsbeschwerde

- a. Der schleswig-holsteinische Gesetzgeber ermöglicht den Polizeibehörden sowie dem Verfassungsschutz auf der Grundlage der streitbefangenen Normen Eingriffe in das Grundrecht auf informationelle Selbstbestimmung sowie das Telekommunikationsgeheimnis.
- b. Hierzu hat der Gesetzgeber in Anlehnung an die Entscheidung des Bundesverfassungsgerichts vom 24. Januar 2012 ein abgestuftes, an der jeweiligen Persönlichkeitsrelevanz und Intensität des Eingriffs ausgerichtetes, ausdifferenziertes System von Ermächtigungsgrundlagen geschaffen.
- c. Diese begrenzen bereits den Zugriff auf einfache Bestandsdaten, die keine schwere Persönlichkeitsrelevanz aufweisen, anhand althergebrachter polizeirechtlicher Eingriffsvoraussetzungen.
- d. Im Hinblick auf die Abfrage sensiblerer Daten hat der Gesetzgeber durch erhöhte Eingriffsschwellen und prozedurale Absicherungen bis hin zu einem Richtervorbehalt klare und verhältnismäßige Eingriffsmöglichkeiten geschaffen, um den schleswig-holsteinischen Behörden Instrumente zur Erfüllung fundamentaler staatlicher Aufgaben an die Hand zu geben.

Dänischenhagen, den 25. Oktober 2017



Professor Dr. Florian Becker