Landtag von Baden-Württemberg **Drucksache 15 / 4421**

15. Wahlperiode **03. 12. 2013**

Gesetzentwurf

der Landesregierung

Gesetz zur Änderung des Polizeigesetzes und des Landesverfassungsschutzgesetzes

A. Zielsetzung

Das Bundesverfassungsgericht hat mit Beschluss vom 24. Januar 2012 (BVerfGE 130, 151 ff.) festgestellt, dass die Ermächtigung zur Bestandsdatenauskunft in § 113 des Telekommunikationsgesetzes sowie in den Fachgesetzen der Sicherheits- und Verfassungsschutzbehörden unzureichend ist. Erforderlich sei eine qualifizierte Rechtsgrundlage zur Auskunftspflicht der Telekommunikationsunternehmen und zur Zuordnung dynamischer Internetprotokoll-Adressen. Die Voraussetzungen für eine Auskunft über Zugangssicherungscodes seien zudem dahingehend zu ergänzen, dass zugleich die Bedingungen für die Datennutzung vorliegen müssen. Das Gericht hat jedoch festgestellt, dass die beanstandeten Regelungen übergangsweise bis längstens Ende Juni 2013 angewendet werden dürfen. Der Bundesgesetzgeber hat für seinen Kompetenzbereich die Normen den verfassungsrechtlichen Vorgaben bereits angepasst. Mit dem Gesetz zur Änderung des Polizeigesetzes und des Gesetzes über den Verfassungsschutz in Baden-Württemberg soll die Entscheidung des Bundesverfassungsgerichts nun auf Landesebene umgesetzt werden.

B. Wesentlicher Inhalt

Mit der Gesetzesänderung sollen den Vorgaben des Bundesverfassungsgerichts entsprechende Ermächtigungsgrundlagen für materielle Anforderungen

- an die Datenerhebung durch Polizei und Landesamt für Verfassungsschutz mittels identifizierender Zuordnung dynamischer Internetprotokoll-Adressen,
- an die Auskunftserteilung über Zugangssicherungscodes von Mobilfunkendgeräten und Speichereinrichtungen sowie

Eingegangen: 03. 12. 2013 / Ausgegeben: 12. 12. 2013

- an die Erhebung von Bestandsdaten durch das Landesamt für Verfassungsschutz

geschaffen werden. Gleichzeitig wird klargestellt, dass die Befugnis zur Erhebung von Bestands- und Nutzungsdaten (Nutzungsdaten nur im Polizeibereich) auch solche nach dem Telemediengesetz umfasst.

C. Alternativen

Keine.

D. Wesentliche Ergebnisse der Regelungsfolgenabschätzung und Nachhaltigkeitsprüfung

Durch die Änderung des Polizeigesetzes und des Landesverfassungsschutzgesetzes sind keine erheblichen Auswirkungen auf die ökonomischen, ökologischen und sozialen Verhältnisse zu erwarten. Auch nennenswerte Kosten für die öffentlichen Haushalte oder für Private entstehen durch die Gesetzesänderungen nicht.

Staatsministerium
Baden-Württemberg
Ministerpräsident

Stuttgart, 3. Dezember 2013

An den
Präsidenten des Landtags
von Baden-Württemberg

Sehr geehrter Herr Landtagspräsident,

in der Anlage übersende ich gemäß Artikel 59 Absatz 1 der Landesverfassung den von der Landesregierung beschlossenen Entwurf eines Gesetzes zur Änderung des Polizeigesetzes und des Landesverfassungsschutzgesetzes mit Begründung und Vorblatt. Ich bitte, die Beschlussfassung des Landtags herbeizuführen. Federführend ist das Innenministerium zuständig.

Mit freundlichen Grüßen

Kretschmann
Ministerpräsident

Der Landtag wolle beschließen,

dem nachstehenden Gesetzentwurf seine Zustimmung zu erteilen:

Gesetz zur Änderung des Polizeigesetzes und des Landesverfassungsschutzgesetzes

Artikel 1

Änderung des Polizeigesetzes

§ 23 a des Polizeigesetzes in der Fassung vom 13. Januar 1992 (GBl. S. 1), zuletzt geändert durch Artikel 13 des Gesetzes vom 23. Juli 2013 (GBl. S. 233, 239), wird wie folgt geändert:

1. In Absatz 1 Satz 1 werden nach dem Wort „Telekommunikationsgesetzes“ die Wörter „und Nutzungsdaten im Sinne des § 15 Absatz 1 Satz 2 Nummer 2 und 3 des Telemediengesetzes“ eingefügt.

2. Absatz 2 wird wie folgt geändert:

   a) In Satz 5 werden nach dem Wort „wird“ die Wörter „oder eine Bezeichnung des Nutzers der Telemedien, dessen Daten erhoben werden“ eingefügt.

   b) In Satz 6 werden nach dem Wort „Telekommunikation“ die Wörter „oder Telemediennutzung“ eingefügt.

3. Absatz 5 wird wie folgt geändert:

   a) In Satz 1 werden nach dem Wort „Telekommunikationsdienste“ die Wörter „oder Telemediendienste“ eingefügt.

   b) In Satz 2 werden nach dem Wort „Verkehrsdaten“ die Wörter „und Nutzungsdaten“ eingefügt.

   c) In Satz 3 werden nach dem Wort „Telekommunikations-Überwachungsverordnung“ die Wörter „sowie dem Telemediengesetz“ eingefügt.

4. Absatz 9 wird wie folgt gefasst:

   „(9) Der Polizeivollzugsdienst kann ohne Wissen des Betroffenen Daten im Sinne der §§ 95 und 111 des Telekommunikationsgesetzes und der §§ 14 und 15 Absatz 1 Satz 2 Nummer 1 des Telemediengesetzes über die in §§ 6 und 7 sowie unter den Voraussetzungen des § 9 über die dort genannten Personen erheben, soweit dies zur Abwehr einer Gefahr für die öffentliche Sicherheit erforderlich ist. Die Auskunft nach Satz 1 darf zur Abwehr einer Gefahr für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicher-

heit des Bundes oder eines Landes oder einer gemeinen Gefahr auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse sowie weiterer zur Individualisierung erforderlicher technischer Daten verlangt werden. Bezieht sich das Auskunftsverlangen nach Satz 1 auf Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird, darf die Auskunft zur Abwehr der in Satz 2 genannten Gefahren nur verlangt werden, wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen. Absatz 1 Satz 4 sowie Absatz 5 Satz 1, 3 und 4 gelten entsprechend. Die betroffenen Personen sind von Maßnahmen nach Satz 2 und 3 zu unterrichten, soweit und sobald hierdurch der Zweck der Maßnahme nicht vereitelt wird. Die Unterrichtung unterbleibt, wenn ihr überwiegende schutzwürdige Belange Dritter oder der betroffenen Person selbst entgegenstehen oder wenn seit Beendigung der Maßnahme fünf Jahre verstrichen sind. Wird die Unterrichtung zurückgestellt oder von ihr abgesehen, sind die Gründe aktenkundig zu machen."

Artikel 2

Änderung des Landesverfassungsschutzgesetzes

Das Landesverfassungsschutzgesetz in der Fassung vom 5. Dezember 2005 (GBl. 2006 S. 1) wird wie folgt geändert:

1. Nach § 5 a wird folgender § 5 b eingefügt:

„§ 5 b

Weitere Auskunftsverlangen

(1) Soweit dies zur Erfüllung der Aufgaben des Landesamtes für Verfassungsschutz erforderlich ist, darf von demjenigen, der geschäftsmäßig Telekommunikationsdienste, Telemediendienste oder beides erbringt oder daran mitwirkt, Auskunft über die nach den §§ 95 und 111 des Telekommunikationsgesetzes sowie nach § 14 des Telemediengesetzes erhobenen Daten verlangt werden. Bezieht sich das Auskunftsverlangen nach Satz 1 auf Daten, mittels derer der Zugriff auf Endgeräte oder Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird, darf die Auskunft nur verlangt werden, wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen.

(2) Die Auskunft nach Absatz 1 darf auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse sowie weiterer zur Individualisierung erforderlicher technischer Daten verlangt werden.

(3) Auskunftsverlangen nach Absatz 1 Satz 2 und Absatz 2 sind aktenkundig zu machen.

(4) Der Betroffene ist in den Fällen des Absatzes 1 Satz 2 und des Absatzes 2 spätestens fünf Jahre nach Erteilung der Auskunft über diese zu benachrichtigen. Die Benachrichtigung unterbleibt, solange eine Gefährdung des Zwecks der Auskunft und der Eintritt übergreifender Nachteile für das Wohl des Bundes oder eines Landes nicht ausgeschlossen werden können oder wenn ihr überwiegende schutzwürdige Belange Dritter oder der betroffenen Person selbst entgegenstehen. Die Benachrichtigung unterbleibt endgültig, wenn die in Satz 2 genannten Gründe auch fünf Jahre nach Erteilung der Auskunft noch vorliegen. Die Entscheidung über das Absehen von einer Benachrichtigung erfolgt durch die Amtsleitung. Die Gründe für das Absehen von einer Benachrichtigung sind aktenkundig zu machen.

(5) Aufgrund eines Auskunftsverlangens nach Absatz 1 oder 2 hat derjenige, der geschäftsmäßig Telekommunikationsdienste, Telemediendienste oder beides erbringt oder daran mitwirkt, die zur Auskunftserteilung erforderlichen Daten unverzüglich, vollständig und richtig zu übermitteln.

(6) Das Landesamt für Verfassungsschutz hat für ihm erteilte Auskünfte eine Entschädigung zu gewähren, deren Umfang sich nach § 23 und Anlage 3 des Justizvergütungs- und -entschädigungsgesetzes bemisst; die Vorschriften über die Verjährung in § 2 Absatz 1 und 3 des Justizvergütungs- und -entschädigungsgesetzes finden entsprechend Anwendung.“

2. Die Inhaltsübersicht ist entsprechend anzupassen.

Artikel 3

Einschränkungen von Grundrechten

Durch Artikel 1 und 2 wird das Fernmeldegeheimnis (Artikel 10 des Grundgesetzes) eingeschränkt.

Artikel 4

Inkrafttreten

(1) Dieses Gesetz tritt am 1. März 2014 in Kraft.

(2) Die Befugnisse zur Erhebung von Bestandsdaten sind spätestens fünf Jahre nach ihrem Inkrafttreten zu evaluieren.

Begründung

A. Allgemeiner Teil

I. Änderung des Polizeigesetzes

Mit Beschluss vom 24. Januar 2012 (BVerfGE 130, 151 ff.) hat das Bundesverfassungsgericht zu § 113 Telekommunikationsgesetz (TKG) festgestellt, dass

a) Telekommunikationsbestandsdaten durch die Sicherheitsbehörden nur mittels einer qualifizierten Rechtgrundlage für den Datenabruf erhoben werden dürfen,

b) die bislang nach überwiegender Auffassung den §§ 111 ff. TKG zugeordneten dynamischen Internetprotokoll-Adressen nicht der Abrufermächtigung des § 113 TKG unterfielen, sondern hierfür eine normenklare Regelung, die den Eingriff in das Fernmeldegeheimnis beachtet, erforderlich sei und

c) der bisher durch § 113 Absatz 1 Satz 2 TKG eröffnete Zugriff auf Zugangssicherungscodes unverhältnismäßig sei, da nicht zugleich festgelegt werde, wann und in welchem Umfang die Behörden von den Daten Gebrauch machen dürfen.

Um eine Anpassung der gesetzlichen Regelungen zu ermöglichen, hatte das Bundesverfassungsgericht eine Übergangsfrist bis zum 30. Juni 2013 festgesetzt.

Die unter a) erwähnte qualifizierte Ermächtigungsgrundlage für die polizeiliche Erhebung von Bestandsdaten wurde bereits mit Gesetz vom 20. November 2012 (GBl. S. 625) in § 23 a Absatz 9 Polizeigesetz (PolG) geschaffen.

Die Änderung des Polizeigesetzes aufgrund der unter b) und c) genannten Feststellungen des Bundesverfassungsgerichts setzte dagegen zunächst die Anpassung durch den Bundesgesetzgeber voraus, wie sie mit dem Gesetz zur Änderung des TKG und zur Neuregelung der Bestandsdatenauskunft vom 20. Juni 2013 erfolgt ist (BGBl. I S. 1602). Hierzu korrespondierend soll § 23 a Absatz 9 PolG hinsichtlich der Zuordnung dynamischer Internetprotokoll-Adressen sowie für den Zugriff auf Zugangssicherungscodes ergänzt werden.

Der Beschluss des Bundesverfassungsgerichts zum TKG ist sinngemäß auf das Telemediengesetz (TMG) übertragbar. Hinzu treten Überschneidungen und Abgrenzungsschwierigkeiten zwischen TKG und TMG für einzelne Internetdienste. Jedoch hat die Polizei auf gleichartige Gefahren zu reagieren. Zum Beispiel bedarf es bei Androhung eines Suizids in einem Internetforum zur Identifizierung des Nutzers der Auskunft über dessen selbstgewählte Kennung (Nickname) durch den Telemediendiensteanbieter. Wenn dabei nicht der tatsächliche Name, sondern nur die genutzte dynamische Internetprotokoll-Adresse übermittelt werden kann, muss als zweiter Schritt beim Telekommunikationsdiensteanbieter die Zuordnung der IP-Adresse zu dem Anschlussinhaber und dessen Adresse folgen. Deshalb ist klarzustellen, dass die Bestands- und Nutzungsdaten des TMG ebenfalls erhoben und genutzt werden dürfen. Dabei werden die Daten zur Identifizierung des Nutzers (§§ 14 und 15 Absatz 1 Satz 2 Nummer 1 TMG) wegen der Vergleichbarkeit zu Telekommunikationsbestandsdaten an diese Erhebungsvoraussetzungen geknüpft. Demgegenüber dürfen die Daten, die Telekommunikationsverkehrsdaten gleichzusetzen sind (§ 15 Absatz 1 Satz 2 Nummer 2 und 3 TMG, z. B. Dauer oder Umfang einer Telemediennutzung), nur unter den erhöhten Voraussetzungen aus § 23 a Absatz 1 PolG erhoben werden.

Die Möglichkeit, unter den Voraussetzungen von § 112 TKG durch die Bundesnetzagentur Auskunft über Bestandsdaten zu erhalten, besteht fort. Das Bundesverfassungsgericht hatte im Beschluss vom 24. Januar 2012 die Regelung in § 112 TKG als verfassungsgemäß bestätigt.

II. Änderung des Gesetzes über den Verfassungsschutz in Baden-Württemberg

Zum Beschluss des Bundesverfassungsgerichts vom 24. Januar 2012 (BVerfGE 130, 151 ff.) sowie der aktuellen Gesetzgebung des Bundes wird auf die Ausführungen unter I. verwiesen.

Mit der Neufassung des § 5 b Landesverfassungsschutzgesetz (LVSG) wird die unter I. a) benannte qualifizierte Ermächtigungsgrundlage für die Erhebung von Bestandsdaten (Daten eines Nutzers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste oder Telemediendienste erhoben werden, etwa Name, Anschrift, Rufnummer etc.) geschaffen.

Da die Forderung des Bundesverfassungsgerichts nach qualifizierten Rechtsgrundlagen für den Abruf von Bestandsdaten nicht nur für die Abfragen nach dem TKG gilt, sondern auch auf die Abfragen nach dem TMG übertragbar ist, wird mit der ausdrücklichen Nennung der Anbieter von Telekommunikationsdiensten und Telemediendiensten diese qualifizierte Rechtsgrundlage geschaffen.

Bislang hat man die Abfragen von Bestandsdaten bei Anbietern von Telekommunikationsdiensten auf § 5 Absatz 1 LVSG in Verbindung mit § 113 Absatz 1 Satz 1 TKG und bei Anbietern von Telemediendiensten auf § 5 Absatz 1 LVSG in Verbindung mit § 14 Absatz 2 TMG gestützt. Neue Befugnisse für den Verfassungsschutz werden daher nicht begründet.

Die Änderungen des LVSG aufgrund der unter I. b) und I. c) genannten Feststellungen des Bundesverfassungsgerichts setzten eine Anpassung der entsprechenden Vorschriften durch den Bundesgesetzgeber voraus. Diese sind im Gesetz zur Änderung des TKG und zur Neuregelung der Bestandsdatenauskunft vom 20. Juni 2013 (BGBl. I S. 1602) erfolgt. § 5 b LVSG n. F. nimmt die Regelungen hinsichtlich der Zuordnung dynamischer Internetprotokoll-Adressen und der Regelungen für den Zugriff auf Zugangssicherungscodes auf. Die Änderungen beschränken sich dabei auf die Umsetzung der Vorgaben des Bundesverfassungsgerichts.

B. Einzelbegründung

I. Zu Artikel 1 (§ 23 a PolG)

Zu Nummer 1) (§ 23 a Absatz 1 Satz 1)

Durch die Regelung wird klargestellt, dass auch die den Verkehrsdaten im Sinne des § 96 Absatz 1 des Telekommunikationsgesetzes gleichzusetzenden Nutzungsdaten gemäß § 15 Absatz 1 Satz 2 Nummer 2 und 3 des Telemediengesetzes unter denselben Voraussetzungen wie Telekommunikationsverkehrsdaten erhoben werden dürfen. D. h., diese Telemediennutzungsdaten dürfen nur unter den in Absatz 1 benannten qualifizierten Voraussetzungen erhoben werden. Die dadurch definierte Gefahrenschwelle wäre nach der Rechtsprechung des Bundesverfassungsgerichts selbst für eingriffsintensivere Datenerhebungen von vorsorglich anlasslos gespeicherten Telekommunikationsverkehrsdaten zulässig (BVerfGE 125, 260, 329 f).

Zu Nummer 2 Buchstabe a) (§ 23 a Absatz 2 Satz 5)

Es handelt sich um eine redaktionelle Folgeänderung zu Nummer 1.

Zu Nummer 2 Buchstabe b) (§ 23 a Absatz 2 Satz 6)

Es handelt sich um eine redaktionelle Folgeänderung zu Nummer 1.

Zu Nummer 3 Buchstabe a) (§ 23 a Absatz 5 Satz 1)

Es handelt sich um eine redaktionelle Folgeänderung zu Nummer 1.

Zu Nummer 3 Buchstabe b) (§ 23 a Absatz 5 Satz 2)

Es handelt sich um eine redaktionelle Folgeänderung zu Nummer 1.

Zu Nummer 3 Buchstabe c) (§ 23 a Absatz 5 Satz 3)

Es handelt sich um eine redaktionelle Folgeänderung zu Nummer 1.

Zu Nummer 4 (§ 23 a Absatz 9)

Es wird klargestellt, dass Identifikationsmerkmale eines Telemediennutzers unter denselben Voraussetzungen erhoben werden dürfen wie die Bestandsdaten zur Identifikation des Nutzers eines Telekommunikationsvertrags. Die Daten werden beispielsweise benötigt, um bei Ankündigung einer Amoktat, eines Suizids oder einer anderen Gefahr in einem Chat oder ähnlichen Internetmedium den unter einem Kurz- oder Phantasienamen (Nickname) auftretenden Betroffenen identifizieren und die Gefahr abwehren zu können.

Die Zulässigkeit von Auskunftsverlangen wird auf Gefahren für die öffentliche Sicherheit beschränkt.

Mit Absatz 9 Satz 2 und 3 wird, korrespondierend zu § 113 des Telekommunikationsgesetzes (TKG), die Erhebung der Daten zu Internetprotokoll-Adressen sowie für den Zugriff auf Endgeräte geregelt. Für das ebenfalls betroffene Telemedienrecht gilt dies entsprechend.

In Satz 2 wird die polizeiliche Datenerhebungsbefugnis definiert und geregelt, dass die Auskunft nach Satz 1 auch anlassbezogen zu bekannten Internetprotokoll-Adressen, die zu einem bestimmten Zeitpunkt zugewiesen waren oder noch sind, zu erteilen ist (vgl. auch § 113 Absatz 1 Satz 3 TKG). Die Befugnis ist auf die Abwehr konkreter Gefahren für die benannten hochrangigen Rechtsgüter – entsprechend deren Nennung in § 23 a Absatz 1 – beschränkt. Die Telekommunikations- und Telemediendiensteanbieter sind, ausgesprochen durch Verweis auf § 23 a Absatz 5, zur Auskunft verpflichtet.

Die technische Entwicklung kann es bedingen, dass zusätzlich zu der zu einem bestimmten Zeitpunkt zugewiesenen dynamischen Internetprotokoll-Adresse weitere technische Daten für die Zuordnung zu der betroffenen Person erforderlich sind. Dies ist u. a. bei der Verbreitung findenden Network Address Port Translation-Technologie der Fall, bei der dynamische Internetprotokoll-Adressen zeitgleich mehrfach an verschiedene Nutzer vergeben werden und daher die Auskunft über einen Nutzer der Einbeziehung zusätzlicher Daten bedarf.

Der Eingriff in das Fernmeldegeheimnis ist durch den mit der Ermächtigung verfolgten Zweck gerechtfertigt. Die Daten werden insbesondere zur Fahndungsunterstützung bei der Ermittlung von Personalien und Standort bei Amok- und Suizidankündigungen benötigt.

Satz 3 regelt die Datenerhebungsbefugnis für Auskünfte der Diensteanbieter über Zugangssicherungscodes wie z. B. Passwort, Persönliche Identifikationsnummer (PIN) oder Personal Unblocking Key (PUK) von Mobilfunkendgeräten oder Spei-

chereinrichtungen (vgl. auch § 113 Absatz 1 Satz 2 TKG). Die Befugnis ist, ebenso wie in Satz 2, auf die Abwehr konkreter Gefahren für die hochrangigen Rechtsgüter Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder eine gemeine Gefahr beschränkt. Damit wird dem Umstand Rechnung getragen, dass der damit verbundene Eingriff in das Grundrecht auf informationelle Selbstbestimmung wegen der Überwindung der durch den Zugangssicherungscode gesetzten Barriere von den Betroffenen als besonders gravierend empfunden wird.

Satz 3 beinhaltet zudem die zusätzliche Einschränkung, dass für solche Daten die Auskunft nur verlangt werden darf, wenn zugleich die gesetzlichen Voraussetzungen für die Datennutzung vorliegen. Eine Behörde darf nach der Rechtsprechung des Bundesverfassungsgerichts nur dann die Möglichkeit zur Erhebung eines Zugangssicherungscodes haben, wenn sie diesen in der konkreten Abfragesituation zur Erfüllung ihrer Gefahrenabwehraufgabe benötigt (BVerfGE 130, 151, 207 ff.). Die materiellen und formellen Voraussetzungen für die Nutzung sind in eigenständigen Rechtsgrundlagen, z. B. § 20 PolG, geregelt.

Zur Gefahrenabwehr kann der Zugriff auf einen derartigen Zugangssicherungscode beispielsweise erforderlich werden, wenn die Daten auf einem aufgefundenen Mobiltelefon, das nur über PIN oder PUK reaktiviert werden kann, Hinweise zum Aufenthaltsort einer vermissten Person enthalten können. Die Nutzung dieser Daten, d. h. Anrufkontakte oder versandte Kurzmitteilungen, wäre dann nach §§ 20, 37 PolG zulässig.

Der Zugangssicherungscode ist aufgrund von §§ 46, 37 Absatz 1 Satz 1 PolG unverzüglich nach dessen Nutzung zu löschen.

Die in den Sätzen 5 bis 7 geregelte Unterrichtung des Betroffenen trägt dem Grundsatz der Transparenz Rechnung und eröffnet die Möglichkeit nachträglichen Rechtsschutzes. Sie korrespondiert mit der Neuregelung der Bestandsdatenauskunft durch den Bundesgesetzgeber etwa in § 100 j Absatz 4 Strafprozessordnung (StPO).

Wie bei anderen ohne Wissen des Betroffenen durchgeführten Maßnahmen (vgl. §§ 22 Absatz 8, 23 Absatz 6 PolG) unterbleibt die Unterrichtung, wenn seit Beendigung der Maßnahme fünf Jahre verstrichen sind.

II. Zu Artikel 2 (§ 5 b LVSG)

Zu Nummer 1 (§ 5 b neu)

In der Vergangenheit wurden die Abfragen von Bestandsdaten (z. B. Rufnummern und andere Anschlusskennungen, Name und Anschrift des Anschlussinhabers etc.) bei Anbietern, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken, auf § 5 Absatz 1 LVSG in Verbindung mit § 113 Absatz 1 Satz 1 TKG gestützt. Diese Rechtsgrundlage entspricht jedoch nicht den Vorgaben der o. g. Entscheidung des Bundesverfassungsgerichts. Mit § 5 b Absatz 1 wird nunmehr die geforderte qualifizierte Rechtsgrundlage zur Erhebung der Bestandsdaten geschaffen.

Wenngleich Gegenstand des Beschlusses des Bundesverfassungsgerichts vom 24. Januar 2012 nur die Regelungen des TKG waren, soll aus Klarstellungsgründen auch der Abruf von Bestandsdaten nach dem TMG in einer spezifischen Rechtsgrundlage erfasst werden. § 14 Absatz 2 TMG legt, vergleichbar § 113 Absatz 1 Satz 1 TKG, insoweit bereits fest, in welchen Fällen die Diensteanbieter zur Übermittlung der betreffenden Daten berechtigt sind. Die Rechtsprechung des Bundesverfassungsgerichts ist insoweit übertragbar auf Auskunftsverlangen gemäß § 14 Absatz 2 TMG, die Bestandsdaten der Nutzerinnen und Nutzer von Telemedienangeboten (u. a. Videoplattformen, Online-Auktionen sowie soziale Netzwerke) betreffen.

In Absatz 1 Satz 1 wird die Berechtigung der Verfassungsschutzbehörde zur Abfrage von Bestandsdaten im manuellen Verfahren erteilt. Die Beauskunftung von Bestandsdaten ist nur im Einzelfall zulässig. Die Abfrage von Bestandsdaten ist für die gesetzliche Aufgabenerfüllung der Verfassungsschutzbehörde unerlässlich, weil nur anhand dieser Auskünfte die Absender oder sonstige Beteiligte an Kommunikationsvorgängen identifizierbar sind. Diese Informationen können wiederum das Erkenntnisbild von relevanten Personen erheblich vervollständigen. Darüber hinaus erhält die Verfassungsschutzbehörde durch die Abfrage von Bestandsdaten wesentliche Informationen und Daten für die Durchführung von Maßnahmen nach dem Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz – G 10).

Die Abfrage von Bestandsdaten bei Anbietern von Telemediendiensten im Sinne des Absatzes 1 Satz 1 kommt z. B. dann in Betracht, wenn die Verfassungsschutzbehörde bei der Beobachtung eines extremistischen Versandhandels überprüfen möchte, ob der Betreiber des Versandhandels auch auf Verkaufsplattformen im Internet aktiv ist. Sie ist aber auch in den Fällen relevant, in denen der Urheber eines Videos, z. B. bei einem Spendenaufruf für eine legalistische extremistische Organisation, auf einem Videoportal zu identifizieren ist.

In Erfüllung der durch das Bundesverfassungsgericht aufgestellten Erfordernisse regelt Absatz 1 Satz 2, dass Abfragen von Bestandsdaten, sofern diese Passwörter oder sonstige Zugangsberechtigungen umfassen (insbesondere PIN und PUK für den Zugriff auf Mobilfunkendgeräte), nur zulässig sind, sofern die gesetzlichen Voraussetzungen für die Nutzung dieser erlangten Passwörter etc. vorliegen.

Die Regelungen zu dem Auskunftsverlangen aufgrund einer dynamischen Internetprotokoll-Adresse wurden in Absatz 2 aufgenommen. Die technische Entwicklung kann es bedingen, dass weitere technische Daten für die Zuordnung einer dynamischen Internetprotokoll-Adresse erforderlich sind. Dies ist u. a. bei der Verbreitung findenden Network-Address-Port-Translation-Technologie der Fall, bei der dynamische Internetprotokoll-Adressen zeitgleich mehrfach an verschiedene Nutzer vergeben werden und daher die Auskunft über einen Nutzer der Einbeziehung zusätzlicher Daten zur Individualisierung bedarf. Andernfalls würden auch die Daten der anderen Nutzer herausgegeben, denen zeitgleich die Internetprotokoll-Adresse zugewiesen wurde, die aber nicht im Fokus der Verfassungsschutzbehörde stehen. Daher wurde eine entsprechende Ergänzung in Absatz 2 vorgenommen.

Die Daten über die Zuordnung der Internetprotokoll-Adressen werden z. B. in den Fällen benötigt, in denen der Verfassungsschutzbehörde als Ermittlungsansatz lediglich eine Internetprotokoll-Adresse bekannt ist. Dies ist u. a. dann der Fall, wenn Personen über Internettelefonie verschlüsselt miteinander kommunizieren und die Verfassungsschutzbehörde im Rahmen einer Überwachungsmaßnahme nach dem Artikel 10-Gesetz lediglich die Internetprotokoll-Adresse des Kommunikationspartners der überwachten Person erlangt.

Um die Nachvollziehbarkeit von Auskunftsverlangen zu gewährleisten, wird in Absatz 3 eine Dokumentationspflicht normiert.

Für Abfragen von Bestandsdaten, sofern diese Passwörter oder sonstige Zugangsberechtigungen umfassen (Absatz 1 Satz 2) oder die Zuordnung einer dynamischen Internetprotokoll-Adresse betreffen (Absatz 2), wird mit Absatz 4 eine Pflicht zur Benachrichtigung des von der Abfrage Betroffenen geregelt. Die Benachrichtigung darf nur dann und solange unterbleiben, wie eine Gefährdung des Zwecks der Auskunft und der Eintritt übergreifender Nachteile für das Wohl des Bundes oder eines Landes nicht ausgeschlossen werden können oder wenn ihr überwiegende schutzwürdige Belange Dritter oder der betroffenen Person selbst entgegenstehen. Über das endgültige Absehen von der Benachrichtigung aus diesen Gründen muss die Amtsleitung entscheiden. Die hierfür maßgeblichen Gründe müssen dokumentiert werden.

Mit der Regelung in Absatz 5 werden die Diensteanbieter ausdrücklich zur Auskunftserteilung verpflichtet. Dies entspricht den Vorgaben des Bundesverfassungsgerichts.

In Absatz 6 wird eine Regelung über den Anspruch der zur Auskunft verpflichteten Anbieter von geschäftsmäßigen Telekommunikationsdiensten und Telemediendiensten auf eine Entschädigung für die Auskunftserteilung geschaffen. Diese Regelung beinhaltet Entschädigungen für Auskünfte zu Bestandsdaten. Hinsichtlich der Höhe wird auf die entsprechende Anwendung des § 23 des Justizvergütungs- und -entschädigungsgesetzes (JVEG) verwiesen. Diese Regelung entspricht derjenigen im Bundesverfassungsschutzgesetz. Auch die Telemediendiensteanbieter, die das JVEG nicht ausdrücklich erwähnt, werden auf der Grundlage des § 23 JVEG entschädigt.

Zu Nummer 2 (Inhaltsübersicht)

Die Inhaltsübersicht wird entsprechend angepasst.

III. Zu Artikel 3

Die Bestimmung trägt dem Zitiergebot Rechnung.

IV. Zu Artikel 4

Die Bestimmung in Absatz 1 regelt das Inkrafttreten.

Die Befugnisse zur Bestandsdatenerhebung durch die Polizei in § 23 a Absatz 9 PolG und durch die Verfassungsschutzbehörde in § 5 b LVSG werden spätestens fünf Jahre nach dem Inkrafttreten evaluiert.

Die Bundesregierung berichtet zum 31. Dezember 2015 dem Bundestag über den Stand der Einführung des Internetprotokolls Version 6 durch Diensteanbieter und die Auswirkungen auf den Schutz der Grundrechte und die Ermittlungsmöglichkeiten der in § 113 des Telekommunikationsgesetzes benannten Stellen (Artikel 10 des Gesetzes zur Änderung des Telekommunikationsgesetzes und zur Neuregelung der Bestandsdatenauskunft). Eine Evaluation der neuen landesrechtlichen Regelungen vor diesem Zeitpunkt ist untunlich.

C. Wesentliches Ergebnis der Anhörung

Zu dem Entwurf haben Gemeinde- und Landkreistag, der Landesbeauftragte für den Datenschutz, der Anwaltsverband Baden-Württemberg, die Arbeitsgemeinschaft Verwaltungsrecht im Deutschen Anwaltsverein sowie der Verein der Verwaltungsrichterinnen und -richter Stellung genommen. Die beiden kommunalen Landesverbände sowie die Arbeitsgemeinschaft Verwaltungsrecht im Deutschen Anwaltsverein und der Verein der Verwaltungsrichterinnen und -richter haben gegen die vorgeschlagenen Regelungen keine Einwendungen erhoben.

I. Zum Vorblatt

Landesbeauftragter für den Datenschutz

Der Landesbeauftragte für den Datenschutz hält es für erforderlich, angesichts des Verstreichens der vom Bundesverfassungsgericht gesetzten Übergangsfrist (30. Juni 2013) die Erforderlichkeit der Wiedereinführung statt der Fortführung der Befugnisse zur Bestandsdatenauskunft zu begründen. Ebenso müsse die Entschädigungspflicht gegenüber den Diensteanbietern als neue Zahlungs-

verpflichtung klargestellt werden und auf deren Kostenaufwand eingegangen werden.

Die Sichtweise des Landesbeauftragten für den Datenschutz trifft bei rein formaler Betrachtung zu. Die im Rahmen der Vorbereitung des Gesetzentwurfs erforderlichen Abstimmungen, namentlich mit der Gesetzgebung des Bundes (Gesetz zur Änderung des Telekommunikationsgesetzes und zur Neuregelung der Bestandsdatenauskunft vom 20. Juni 2013) sowie der Abstimmungsbedarf auf Landesebene haben dazu geführt, dass in der Zeit zwischen diesem Datum und dem Inkrafttreten der Neuregelung keine Bestandsdatenerhebung erfolgen kann. Inhaltlich erhalten Polizei und Verfassungsschutz aber keine neuen Befugnisse. Die Erforderlichkeit der Befugnisse für Polizei und Verfassungsschutz ist in der Gesetzesbegründung dargelegt. Diese wird nicht dadurch beeinflusst, dass die Ermächtigungsnormen zur Bestandsdatenerhebung durch Polizei und Verfassungsschutz nicht lückenlos fortgeführt werden konnten, sondern formal neu zu regeln sind.

Für manuelle Auskunftsersuchen wurden die Diensteanbieter bereits in der Vergangenheit grundsätzlich entschädigt. Der Entschädigungsanspruch erhält nunmehr eine eigenständige Rechtsgrundlage im Polizei- und Verfassungsschutzgesetz. Er wird weiterhin aus dem Haushalt von Polizei und Verfassungsschutz gedeckt.

Die Auskunftspflicht der Diensteanbieter wurde durch den Bund mit dem „Gesetz zur Änderung des Telekommunikationsgesetzes und zur Neuregelung der Bestandsdatenauskunft“ vom 20. Juni 2013 begründet und deren daraus folgender Erfüllungsaufwand beschrieben (BT-Drucksache 17/12034).

II. Zu Artikel 1 Nummer 1 (§ 23 a Absatz 1 Satz 1 PolG)

Anwaltsverband Baden-Württemberg

Der Anwaltsverband hegt Zweifel an der Bestimmtheit der polizeilichen Eingriffsbefugnisse aufgrund des Verweises auf § 15 Absatz 1 Satz 2 des Telemediengesetzes (TMG), der die Nutzungsdaten mit dem Zusatz „insbesondere“ definiert und damit eine Erweiterung um andere als die benannten Nutzungsangaben ermögliche.

In § 23 a Absatz 1 und 9 PolG wird durch die Bezugnahme auf die Nummern 1 bzw. 2 und 3 des § 15 Absatz 1 Satz 2 TMG eine Einschränkung der Nutzungsdaten, die erhoben werden dürfen, vorgenommen. Durch die Bezugnahme ist eine Erweiterung um weitere Nutzungsdaten (die als Nummern 4 ff. definiert werden könnten) gerade nicht möglich. Dass die in der Aufzählung benannten Nutzungsdaten selbst abstrakt formuliert sind, ist für Rechtsbegriffe typisch und gerichtlich voll überprüfbar.

III. Zu Artikel 1 Nummer 4 (§ 23 a Absatz 9 PolG)

1. Landesbeauftragter für den Datenschutz

a) Der Landesbeauftragte für den Datenschutz erachtet die Gleichstellung von Nutzungsdaten gemäß § 15 Absatz 1 Satz 2 Nummer 1 TMG mit Bestandsdaten gemäß § 14 TMG in § 23 a Absatz 9 PolG als nicht konsequent. Dazu verweist er auf fließende Übergänge zu § 15 Absatz 1 Satz 2 Nummern 2 und 3 TMG und die abweichende Umsetzung in § 5 b LVSG. Für alle Telemediennutzungsdaten sollte die einheitliche Eingriffsschwelle des § 23 a Absatz 1 PolG gelten. Denn die niedrigeren Voraussetzungen nach § 23 a Absatz 9 Satz 1 PolG könnten vor allem die Auskunft über IP-Adressen sowie sog. „Session-IDs“ und „persistente Cookies“ betreffen.

In der Gesetzesbegründung wurde dargelegt, dass die Daten zur Identifizierung des Nutzers (§§ 14 und 15 Absatz 1 Satz 2 Nummer 1 TMG) wegen der Vergleichbarkeit zu Telekommunikationsbestandsdaten an die Erhebungsvoraussetzungen nach § 23 a Absatz 9 PolG geknüpft werden. Demgegenüber sollen die Daten, die Art und Umfang der Nutzung des Telemediums betreffen (§ 15 Absatz 1 Satz 2 Nummer 2 und 3 TMG) und daher wie Telekommunikationsverkehrsdaten über die tatsächliche Kommunikation Auskunft geben, nur unter den erhöhten Voraussetzungen aus § 23 a Absatz 1 PolG erhoben werden. Dies ist verfassungsrechtlich gut vertretbar. So werden etwa in Schleswig-Holstein sogar Nutzungsdaten nach § 15 Absatz 1 Nummer 2 TMG (Beginn und Ende der Telemediennutzung) der polizeilichen Bestandsdatenauskunft zugeordnet (vgl. § 180 a Landesverwaltungsgesetz SH).

Der IP-Adresse kommt im Rahmen des Telemediengesetzes als Identifikationsmerkmal eine andere Qualität zu als dies für die Telekommunikation der Fall ist. Denn Rückschlüsse auf Standorte, von denen die Nutzung ausging, und auf Kommunikationspartner (ggf. zusammengeführt zu „Bewegungsprofilen“) sind aus der Erhebung einer IP-Adresse nach dem TMG nicht möglich. Die IP-Adresse hat vielmehr nur die Zuordnungsfunktion wie eine Telefonnummer bei der Telekommunikation. Die Erhebung der IP-Adresse ist für die polizeiliche Gefahrenabwehr auch erforderlich, da Telemediendienste typischerweise kostenlos sind und die Nutzer sie deshalb ohne Angabe ihrer echten, als Bestandsdaten erhebbaren Personalien gebrauchen. Demgegenüber wird bei der Erhebung von Bestandsdaten anhand einer dynamischen IP-Adresse der damit verbundenen mittelbaren Verkehrsdatenauswertung durch § 23 a Absatz 9 Satz 2 Rechnung getragen.

Die vom Landesbeauftragten für den Datenschutz daneben als individualisierende Daten benannten sog. „Session-IDs“ und persistenten, d. h. beständigen Cookies können von der Polizei nicht erhoben werden. „Session-IDs“ bestehen nur temporär bis zur Schließung des Webbrowsers durch den Nutzer (z. B. während der Zusammenstellung eines Warenkorbs). Die Cookies sind allein beim Nutzer zur Erleichterung des nächsten Telemedienkontakts gespeichert, aber nicht beim Diensteanbieter vorhanden und damit durch die Polizei dort nicht erhebbar.

Durch die bereits bestehende Regelung in § 5 a LVSG zu Telemediennutzungsdaten wurde für das Landesverfassungsschutzgesetz eine abweichende Zuordnung vorgenommen.

b) In § 23 a Absatz 9 PolG sollte nach Auffassung des Landesbeauftragten für den Datenschutz wie in § 23 a Absatz 1 PolG ausdrücklich eine konkrete Gefahr als Voraussetzung benannt werden.

Für Maßnahmen des Polizeivollzugsdiensts ist, auch ohne ausdrückliche Benennung, stets eine konkrete Gefahr erforderlich. Die Formulierung der Gefahrenschwelle in § 23 a Absatz 1 PolG erfolgte in Abgrenzung zur zuvor geltenden Fassung von § 23 a PolG „unmittelbar bevorstehende Gefahr“ sowie orientiert an der Bundesverfassungsgerichtsentscheidung vom 2. März 2010 (BVerfGE 125, 260, 329 f.). Ansonsten ist ein die „konkrete“ Gefahr nochmals betonender Zusatz für das Polizeigesetz nicht üblich.

c) Der Landesbeauftragte für den Datenschutz fordert unter Verweis auf die Entscheidung des Bundesverfassungsgerichts vom 2. März 2010, eine Regelung zur Aktenkundigmachung der Auskunftsbegehren für IP-Adressen zu ergänzen und dies beispielsweise wie in § 20 a des Polizeigesetzes Nordrhein-Westfalen in Form einer schriftlichen Behördenleiteranordnung umzusetzen. Das gleiche müsse für die Erhebung eines Zugangssicherungscodes gelten.

Die Normierung einer Aktenpflicht, die den bereits bestehenden Grundsatz der Aktenführung wiederholt, ist nicht geboten.

Das Bundesverfassungsgericht hatte die Forderung, die rechtlichen und tatsächlichen Gründe für Auskunftsbegehren aktenkundig zu machen, für die (mittelbare) Nutzung von vorsorglich anlasslos gespeicherten Verkehrsdaten aufgestellt. Die systematische sog. Vorratsdatenspeicherung müsse wegen des hohen Eingriffs in die Betroffenengrundrechte besonderen förmlichen Voraussetzungen unterliegen. Diese Rechtsprechung lässt aber nicht den Schluss zu, dass für die hier betroffene Verarbeitung anderer Verkehrsdaten – gespeichert aus Anlass der Vertragserfüllung oder Störungsbeseitigung – dieselben Maßnahmen erforderlich sind. Die Aktenkundigmachung wurde vom Bundesverfassungsgericht auch für die Erhebung eines Zugangssicherungscodes nicht nochmals besonders gefordert.

d) Die Einschränkung zur Unterrichtung des Betroffenen in § 23 a Absatz 9 Satz 6 PolG, wenn dieser das Auskunftsverlangen kennt oder kennen muss, erachtet der Landesbeauftragte für den Datenschutz als Verstoß gegen das Transparenzgebot und fordert deren Streichung.

Die Anregung wird aufgegriffen und die Einschränkung gestrichen.

In Anlehnung an die Unterrichtungspflichten bei anderen ohne Wissen des Betroffenen durchgeführten Maßnahmen (vgl. §§ 22 Absatz 8, 23 Absatz 6 PolG) wird eine zeitliche Grenze von fünf Jahren nach Beendigung der Maßnahme neu geregelt.

2. Anwaltsverband Baden-Württemberg

a) Der Anwaltsverband stellt in Frage, ob eine IP-Adresse für sich bereits ein personenbezogenes Datum ist und weist zur Zuordnung der IP-Adresse zu der sie nutzenden Person auf die Grundrechtsrelevanz aus der mittelbaren Auswertung von Verkehrsdaten hin. Daneben fragt der Anwaltsverband an, ob unter den Zusatz in § 23 a Absatz 9 Satz 2 „weitere zur Individualisierung erforderliche Daten“ auch vom Diensteanbieter vergebene Pseudonyme für Nutzungsprofile gemäß § 15 Absatz 3 Satz 1 TMG fallen.

Die Erhebung der IP-Adresse als Nutzungsdatum nach § 15 Absatz 1 Satz 2 Nummer 1 TMG darf mit der Erhebung von Name und Adresse des Betroffenen (Bestandsdaten) anhand einer bekannten IP-Adresse nicht vermischt werden. Für die Erhebung der Bestandsdaten des Nutzers anhand der dynamischen IP-Adresse wurde durch § 23 a Absatz 9 Satz 2 dem Eingriff in das Fernmeldegeheimnis Rechnung getragen (vgl. BVerfGE 130, 151, 180 ff.).

Unter den Begriff „weitere zur Individualisierung erforderliche Daten“ fallen die technischen Angaben, die die Zuordnung einer mehrfach vergebenen IP-Adresse zu deren Nutzern anhand der sogenannten „Ports“ ermöglichen. Nutzungsprofile nach § 15 Absatz 3 Satz 1 TMG werden nicht entpseudonymisiert.

b) Zur Erhebung eines Zugangssicherungscodes wirft der Anwaltsverband die Frage auf, ob unter die „gesetzlichen Voraussetzungen für die Nutzung“ auch Datenübermittlungsvorschriften wie §§ 42, 48 a PolG fallen.

Zu der in § 23 a Absatz 9 Satz 3 PolG geregelten Voraussetzung, dass die Datennutzung zulässig sein muss, wurde der typische Anwendungsfall der Entschlüsselung eines Mobiltelefons zur Ermittlung von Hinwendungsorten eines Vermissten genannt. Eine Datenübermittlung stellt dagegen keine Nutzung des Zugangssicherungscodes dar. Dem Übermittlungsempfänger muss als Grundlage der Nutzung auch die Befugnis zur Erhebung des Zugangssicherungscodes zustehen.

c) Der Anwaltsverband ist zu § 23 a Absatz 9 Satz 6 der Auffassung, dass nur bei positiver Kenntnis vom Auskunftsverlangen eine Unterrichtung des Betroffenen unterbleiben kann. Unterrichtungen sollten zudem immer schriftlich erfolgen.

Zur Streichung der Einschränkung gilt das oben unter III. 1. d) Gesagte. Eine Form der Unterrichtung ist, wie in bestehenden Unterrichtungsregelungen des Polizeigesetzes, nicht vorgeschrieben. Dass immer die Schriftform eingehalten werden muss, ergibt sich auch nicht aus dem Grundsatz der Aktenkundigmachung des polizeilichen Handelns.

IV. Zu Artikel 2 (§ 5 b LVSG)

1. Landesbeauftragter für den Datenschutz

a) Die Schaffung eines neuen § 5 b LVSG erachtet der Landesbeauftragte für den Datenschutz als gesetzessystematisch unbefriedigend. Die Zugehörigkeit zu den bestehenden Regelungen über Telekommunikations- und Telemediendaten in § 5 a LVSG sowie die systematische Trennung in Auskünfte durch öffentliche oder nicht-öffentliche Stellen werde durch die Nachstellung als eigener Paragraf unter der Überschrift „Weitere Auskunftsverlangen“ nicht deutlich.

Das Gesetz beschränkt sich auf die verfassungsgerichtlich veranlasste Neuregelung der Rechtsgrundlage für die Bestandsdatenauskunft. Von einer Änderung bestehender Normen wurde daher bewusst abgesehen. Hinzu kommt, dass Eingriffe gemäß § 5 a LVSG abweichenden Voraussetzungen folgen. Die Bestandsdatenabfragen richten sich nur zum Teil an die von § 5 a LVSG Verpflichteten, betreffen andere („weitere“) Auskunftsgegenstände und folgen anderen rechtlichen Voraussetzungen. Dass der gewählte Weg vor dem Hintergrund der Normenklarheit angemessen ist, belegen die in dieser Weise durchgeführten Novellierungen sowohl des Bundesverfassungsschutzgesetzes als auch anderer Landesverfassungsschutzgesetze.

b) Unter Verweis auf die Entscheidung des Bundesverfassungsgerichts vom 2. März 2010 fordert der Landesbeauftragte für den Datenschutz, die Eingriffsschwelle um die Voraussetzung zu ergänzen, dass eine „auf Anhaltspunkte im Tatsächlichen gestützte konkrete Gefahr“ vorliegt.

Die Bezugnahme auf eine konkrete Gefahr widerspricht dem Wesen des Verfassungsschutzes. Zu dessen Aufgaben hat das Bundesverfassungsgericht vielmehr ausgeführt, er habe „Aufklärung bereits im Vorfeld von Gefährdungslagen zu betreiben“ sowie „mannigfaltige Bestrebungen auf ihr Gefahrenpotenzial hin allgemein zu beobachten und sie gerade auch unabhängig von konkreten Gefahren in den Blick zu nehmen“ (Urteil vom 24. April 2013, 1 BvR 1215/07 – Antiterrordatei). Entsprechend ziele auch die Aufklärung der Verfassungsschutzbehörden nicht unmittelbar auf die Verhütung und Verhinderung von konkreten Straftaten oder Gefahren.

Die vom Landesbeauftragten für den Datenschutz zitierten Eingriffsvoraussetzungen bezogen sich auf den schweren Eingriff in das Fernmeldegeheimnis durch Verarbeitung vorsorglich anlasslos gespeicherter Verkehrsdaten. Ein solcher Eingriff liegt bei der Bestandsdatenauskunft nicht vor. Daher kann diese Rechtsprechung nicht unmittelbar auf den zu regelnden Sachverhalt übertragen werden.

c) Der Landesbeauftragte für den Datenschutz erachtet es, ebenfalls unter Verweis auf das Urteil des Bundesverfassungsgerichts vom 2. März 2010, für erforderlich, eine Regelung zur Aktenkundigmachung der Auskunftsbegehren für IP-Adressen sowie für die Erhebung eines Zugangssicherungscodes zu regeln und dies beispielsweise durch die schriftliche Anordnung des Behördenleiters umzusetzen.

Die Anregung wird aufgegriffen und § 5 b LVSG um die Formulierung ergänzt: „Auskunftsverlangen nach § 5 b Absatz 1 Satz 2 und Absatz 2 LVSG sind aktenkundig zu machen.“ Dadurch wird die Nachvollziehbarkeit von Auskunftsverlangen gewährleistet.

d) In Fortführung seiner Argumentation zu c) beanstandet der Landesbeauftragte für den Datenschutz das Fehlen von Benachrichtigungspflichten gegenüber dem Betroffenen.

Die Anregung wird ebenfalls aufgegriffen und § 5 b LVSG um eine Regelung zur Benachrichtigung des Betroffenen ergänzt.

2. Anwaltsverband Baden-Württemberg

a) Der Anwaltsverband bittet zu dynamischen IP-Adressen darum, in § 5 b LVSG deren Zuordnung zu den Nutzungsdaten gemäß § 15 Absatz 1 Satz 2 Nummer 1 TMG klarzustellen. Der Verweis nur auf § 14 TMG sei insofern irreführend.

Die Erhebung der IP-Adresse als Nutzungsdatum nach § 15 Absatz 1 Satz 2 Nummer 1 TMG darf mit der Erhebung von Name und Adresse des Betroffenen (Bestandsdaten nach § 14 TMG) anhand einer bekannten IP-Adresse nicht vermischt werden. Für die Erhebung der Bestandsdaten des Nutzers anhand der dynamischen IP-Adresse wurde durch § 5 b LVSG dem Eingriff in das Fernmeldegeheimnis Rechnung getragen (vgl. BVerfGE 130, 151, 180 ff.). Für darüber hinausgehende Auskunftsverlangen über Nutzungsdaten gelten die Voraussetzungen des § 5 a LVSG.

b) Der Anwaltsverband ist der Auffassung, dass dem Verhältnismäßigkeitsgrundsatz und der verdeckten Tätigkeit des Verfassungsschutzes durch eine Qualifizierung der Voraussetzung „zur Erfüllung der Aufgaben erforderlich“ sowie durch die Aufnahme einer Unterrichtungspflicht der Betroffenen Rechnung getragen werden muss.

Auf die Stellungnahmen zu den gleichgerichteten Anregungen des Landesbeauftragten für den Datenschutz unter IV. 1. b) und d) wird verwiesen.

V. Zu Artikel 4

Landesbeauftragter für den Datenschutz

Nach Ansicht des Landesbeauftragten für den Datenschutz sollte sich angesichts der vom Bundesverfassungsgericht im Beschluss vom 24. Januar 2012 benannten Beobachtungs- und Nachbesserungspflicht die Evaluationsregelung auch auf den Verfassungsschutz erstrecken.

Die Anregung wird umgesetzt. Die Evaluation der Befugnis zur Erhebung von Bestandsdaten soll auch für das Landesverfassungsschutzgesetz gelten.

VI. Weitere Stellungnahmen

1. Landesbeauftragter für den Datenschutz

Der Landesbeauftragte für den Datenschutz kritisiert, dass anlässlich der Neuregelung von § 5 b LVSG nicht zugleich eine Änderung von § 6 Absatz 3 LVSG vorgenommen wird und fordert dessen Ergänzung. Diese Änderung der gemäß Urteil des Bundesverfassungsgerichts vom 3. März 2004 unzureichenden Regelung zur akustischen Wohnraumüberwachung habe er bereits mehrfach angemahnt.

Die Gesetzesnovelle bezweckt ausschließlich die rechtskonforme Regelung der Bestandsdatenabfrage. Weitergehende Änderungen des LVSG bleiben einer späteren Novellierung vorbehalten. Maßnahmen aufgrund dieser Rechtsgrundlage werden vom Landesamt für Verfassungsschutz nicht durchgeführt.

2. Anwaltsverband Baden-Württemberg

Nach Auffassung des Anwaltsverbands sollte die Neuregelung der Bestandsdatenauskunft zum Anlass für weitere Polizeigesetzänderungen genommen werden. Dazu bittet er, seine Stellungnahmen zu vorausgegangenen Änderungen des Polizeigesetzes vom Mai 2008 sowie August 2012 nochmals zu prüfen. Wegen einer aktuellen Presseveröffentlichung sollte der Schutz von Telefonaten zwischen Strafverteidigern und ihren Mandanten vor polizeilicher Abhörung erhöht werden.

An den Stellungnahmen vom 2. Oktober 2012 (LT-Drucksache 15/2434) und 25. August 2008 (LT-Drucksache 14/3165) wird festgehalten. Die Befugnisse zur Erhebung von Telekommunikationsdaten sind im Polizeigesetz eindeutig geregelt. Eine Erhebung der Inhalte von Telefongesprächen ist unzulässig. Regelungsbedarf besteht daher nicht.