Anwaltsverband Baden-Württemberg
im Deutschen **Anwalt**Verein e. V.

Anwaltsverband Baden-Württemberg – Postfach 1221 70808 Korntal-Münchingen

Innenministerium Baden-Württemberg
Herrn MR Dr. Matthias Strohs
Frau Petra Kaciuba
Willy-Brandt-Straße 41

70173 Stuttgart

Hasenbergsteige 5
70178 Stuttgart

Geschäftsstelle:
Johannes-Daur-Straße 10
70825 Korntal-Münchingen

Postfach 1221
70808 Korntal-Münchingen

Telefon 0711 / 2 36 59 63
Telefax 0711 / 2 55 26 55

info@av-bw.de
www.av-bw.de

22. Oktober 2013

Az. 3-0260.0
Entwurf eines Gesetzes zur Änderung des Polizeigesetzes und des Landesverfassungsschutzgesetzes
- Stellungnahme des Anwaltsverbandes Baden-Württemberg -

Sehr geehrter Herr Strohs,
sehr geehrte Frau Kaciuba,

für Ihr Anhörungsschreiben vom 11. September 2013 danken wir Ihnen. Der Anwaltsverband Baden-Württemberg e. V. ist der freiwillige Zusammenschluss der Rechtsanwältinnen und Rechtsanwälte im Land Baden-Württemberg. Er repräsentiert über 9.000 Kolleginnen und Kollegen und vertritt als größte Anwaltsorganisation die Interessen der Anwaltschaft in unserem Bundesland und – in Zusammenarbeit mit dem Deutschen Anwaltverein (DAV) – auch auf nationaler und internationaler Ebene.

Die Gelegenheit zur Stellungnahme zum Gesetzentwurf zur Änderung des Polizeigesetzes und des Landesverfassungsschutzgesetzes nehmen wir nach Beteiligung unserer 25 örtlichen Mitgliedsvereine gerne wahr.

1. Allgemeine Bewertung

Der Gesetzentwurf ist – soweit er Neuregelungen im Polizeigesetz vorsieht – grundsätzlich zu begrüßen. Wir bedauern jedoch, dass diese Neuregelung nicht zum Anlass genommen wird, weitere überfällige Änderungen bzw. Ergänzungen des Polizeigesetzes vorzunehmen, die wir bereits bei früherer Gelegenheit angemahnt hatten. Insoweit verweisen wird auf unsere Stellungnahmen vom 14. Mai 2008 und vom 13. August 2012, die wir dieser Stellungnahme vorsorglich noch einmal als PDF-Dateien beifügen.

Aus gegebenem Anlass regen wir dringend an, die von uns dort angesprochenen Punkte im Laufe des jetzigen Gesetzgebungsverfahrens noch einmal zu überprüfen und einer Regelung zuzuführen. Seinerzeit war seitens Ihres Hauses vielfach kein Regelungsbedarf erkannt worden, weil sich – so Ihre Positionierung zu mehreren Änderungs- bzw. Ergänzungsvorschlägen seitens anderer zu beteiligender Stellen und unsererseits – aus der Gesetzesbegründung hinreichend ergebe, was vom Gesetzgeber gewollt sei, weshalb es nicht erforderlich sei, dies in den Normtext aufzunehmen.

Aktuellen Veröffentlichungen im Nachrichtenmagazin „Der Spiegel“ (Heft 41/2013 bzw. Online-Meldung vom 06.10.2013) zeigen, dass Ermittlungsbehörden über Jahre hinweg Telefonate zwischen Strafverteidigern und deren Mandanten abgehört, diese Mitschnitte protokolliert, ausgewertet und zum Teil jahrelang aufbewahrt haben. Es bedarf keiner Vertiefung, dass eine derartige Praxis evident rechtswidrig ist. Wenn solche Behörde aber – davon muss ausgegangen werden – keinen Respekt vor gesetzlich ausdrücklich normierten Grenzen ihrer Eingriffsbefugnisse haben, so ist erst recht anzunehmen, dass sie der jeweiligen Gesetzesbegründung keinerlei Bedeutung beimessen. Aus diesem Grund ist es keinesfalls ausreichend, etwaige Begriffsbestimmungen, Beschränkungen behördlicher Eingriffsbefugnisse im Wege der Auslegung usw. allein in die jeweilige Gesetzesbegründung aufzunehmen. Vielmehr sind ausdrückliche gesetzliche Regelungen dringend geboten.

2. Einzelfragen

a) Änderungen im Polizeigesetz

aa) § 23a Abs. 1 Satz 1 PolG-E

In der Regel begründen Vorschriften, die zum Umgang mit personenbezogenen Daten ermächtigen, verschiedene, aufeinander aufbauende Eingriffe - insbesondere Erhebung, Speicherung und Übermittlung sowie Datenabruf und -übermittlung nach dem sog. „Doppeltürenmodell“,

vgl. BVerfG, Beschluss vom 24.01.2012 – 1 BvR 1299/05 –, BVerfGE 130, 151ff.

Jeder dieser Eingriffe bedarf jeweils einer eigenen qualifizierten Rechtsgrundlage, wobei eine Zusammenfassung mehrerer Rechtsgrundlagen in einer Norm nicht ausgeschlossen ist. Diesen Anforderungen soll offensichtlich durch die Einfügung der Worte „und Nutzungsdaten im Sinne des § 15 Absatz 1 Satz 2 Nummer 2 und 3 des Telemediengesetzes“ genügt werden.

Problematisch ist hierbei jedoch die gleichzeitige Einbeziehung sowohl des Telekommunikations- als auch des Telemediengesetzes insofern, als beide Gesetze nicht von derselben Begrifflichkeit ausgehen; darüber hinaus erfolgt die Definition der Verkehrsdaten i. S. des § 96 TKG durch eine abschließende Aufzählung, während die Bestimmung der Nutzungsdaten i. S. des § 15 Abs. 1 Satz 2 TMg lediglich beispielhaft („insbesondere“) vorgenommen wird. Zwar nennt der Gesetzentwurf ausdrücklich nur Nr. 2 und 3 des § 15 Abs. 1 Satz 2 TMG und nimmt so scheinbar eine Einschränkung bzw. Konkretisierung vor, die bei genauerer Betrachtung jedoch nicht eintritt, da die einleitenden Formulierungen des Satz 2 unverändert, also einschließlich des „insbesondere“, übernommen werden.

Gemäß § 15 Abs. 1 Satz 1 TMG sind Nutzungsdaten alle personenbezogene Daten eines Nutzers, deren Erhebung und Verwendung erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen. Erforderlich ist die Erhebung und Verwendung derjenigen Daten, die den Dienst so ermöglichen, wie er mit dem Nutzer vereinbart wurde. Dies gilt etwa für IP-Adresse, Ziel- und Startseiten der jeweiligen Anfragen, Suchbegriffe oder je nach Funktionalitäten des Angebots auch die ID eines vom Anbieter gesetzten Cookies, ohne die bereits die Durchführung der Interaktion technisch nicht möglich wäre. Daneben können typische und vom Nutzer gewollte Funktionen wie das automatische Sortieren von Suchergebnissen nach Relevanz mithilfe von Informationen durchgeführt werden, die auf ein Interesse des Nutzers schließen lassen, wie etwa die bisher besuchten Einträge anderer Nutzer und die jeweilige Verweildauer auf diesen Seiten. Die relevanten Nutzungsdaten dürfen in der dazu erforderlichen Art und Weise zulässig verwendet werden, sofern diese Funktion zum Nutzungsverhältnis gehört. Ebenfalls zulässig ist die Erhebung und Verwendung von Nutzungsdaten wie der IP-Adresse oder sonstiger typischer Nutzungsmerkmale, soweit sie die Identifizierung von Spammern ermöglichen,

vgl. Lerch/Krause/Hotho/Rossnagel/Stumme, MMR 2010, 454 (456).

Hieraus folgen erhebliche Zweifel an der gefahrenabwehrrechtlich zu fordernden Bestimmbarkeit der Eingriffsbefugnisse. So ist nicht auszuschließen, dass von der Polizeibehörde Daten als Nutzungsdaten beansprucht werden, die weder im Katalog des § 15 Abs. 1 Satz 2 TMG noch in dem des § 96 Abs. 1 TKG enthalten sind. Eine Konkretisierung erscheint deshalb geboten.

So betrifft etwa § 23a Abs. 9 PolG-E dynamische IP-Adressen, deren Erhebung im Fokus der Gesetzesänderung steht; hierin liegt ein gewisser Widerspruch zu dem in § 23a Abs. 1 PolG-E in Bezug genommenen § 15 Abs. 1 TMG, denn für den Anbieter ist die dynamische IP-Adresse des Nutzers für sich allein genommen kein personenbezogenes Datum, da es auf die Möglichkeiten des Anbieters als verantwortliche Stelle ankommt, die Person des Betroffenen zu identifizieren, ihm dazu jedoch regelmäßig nicht die Mittel zur Verfügung stehen, die hinter der IP-Adresse stehende Person zu ermitteln. Nur im Einzelfall wird der Anbieter über diese Informationen verfügen, wird sich die Personenbeziehbarkeit der IP-Adresse über die Verknüpfung mit personenbezogenen Bestands- oder Inhaltsdaten ergeben mit der Folge, dass auch die übrigen Nutzungsdaten als personenbezogene Daten anzusehen sind,

vgl. Lerch/Krause/Hotho/Rossnagel/Stumme, MMR 2010, 454 (456).

Damit besteht die Möglichkeit, dass die Eingriffsnorm entweder leer läuft oder konturenlos ausufert.

bb) § 23a Abs. 9 Satz 1 PolG-E

Hier fällt auf, dass neben in den bereits in Abs. 1 erwähnten Nutzungsdaten auch die Bestandsdaten i. S. des § 14 TMG erhoben werden können sollen. Es trifft zwar zu, dass auf diese Weise Identifikationsmerkmale eines Telemediennutzers unter denselben Voraussetzungen erhoben werden dürfen wie die Bestandsdaten zur Identifikation des Nutzers eines Telekommunikationsvertrags. Es wäre jedoch wünschenswert, dass die Begrifflichkeiten und Unterschiede deutlich gemacht werden. So werden dynamische IP-Adressen vom Bundesverfassungsgericht weder als Bestands- noch als Verkehrsdaten i. S. des TKG angesehen, nach TMG sind sie aber als Nutzungsdaten zu qualifizieren.

Die Telekommunikationsunternehmen müssen für die Identifizierung einer dynamischen IP-Adresse in einem Zwischenschritt die entsprechenden Verbindungsdaten ihrer Kunden sichten, also auf konkrete Telekommunikationsvorgänge zugreifen.

Die jeweiligen Datenzugriffe haben eine **unterschiedliche Grundrechtsrelevanz**, der Rechnung zu tragen ist. Zwar darf der Gesetzgeber solche Auskünfte für die Gefahrenabwehr auf der Grundlage der allgemeinen fachrechtlichen Eingriffsermächtigungen zulassen, wobei wir ausdrücklich begrüßen, dass der konturenlose Begriff der öffentlichen Ordnung als Eingriffsvoraussetzung entfallen soll. Herkömmlich wird hierunter die Summe aller ungeschriebenen Regeln für ein gedeihliches Zusammenleben verstanden, zu der – überspitzt formuliert – auch die schwäbische Kehrwoche zählt. Da hinsichtlich der Eingriffsschwellen sicherzustellen ist, dass eine Auskunft nicht ins Blaue hinein eingeholt werden, sondern nur aufgrund eines hinreichenden Anfangsverdachts oder einer konkreten Gefahr auf einzelfallbezogener Tatsachenbasis erfolgen darf, war eine Beschränkung auf die öffentliche Sicherheit geboten.

Die nachfolgende Konkretisierung auf Gefahren „für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder eine gemeine Gefahr“ stellt nach unserem Verständnis ein zusätzliche Eingriffshürde für die Erhebung dynamischer IP-Adressen dar, die wir als solche ausdrücklich begrüßen. In der Begründung werden die Unterschiede hingegen nicht deutlich, so dass dem Anwender möglicherweise nicht hinreichend vermittelt wird, dass „bloße“ Gesetzesverletzungen, die auch unter den Begriff einer Gefahr für die öffentliche Sicherheit fallen mögen, nicht zur Erhebung dynamischer IP-Adressen berechtigen.

Diese Einschränkung entspricht aber der verfassungsgerichtlichen Rechtsprechung, der zufolge das Erfordernis einer auf Anhaltspunkte im Tatsächlichen gestützten konkreten Gefahr für alle zur Abwehr von Gefahren für die öffentliche Sicherheit zuständigen Behörden in gleicher Weise gilt wie für die Nachrichtendienste. Das erhebliche Gewicht des Eingriffs solcher Auskünfte erlaubt es nicht, diese allgemein und uneingeschränkt auch zur Verfolgung oder Verhinderung jedweder Ordnungswidrigkeiten zuzulassen. Die Aufhebung der Anonymität im Internet bedarf zumindest einer **Rechtsgutbeeinträchtigung**, der von der Rechtsordnung auch sonst ein **hervorgehobenes Gewicht** beigemessen wird,

> vgl. BVerfG, Urteil vom 02.03.2010 – 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 –, BVerfGE 125, 260ff. (Rdnr. 262).

Insofern ist die klarstellende und zugleich einschränkende Regelung zu begrüßen.

cc) § 23a Abs. 9 Sätze 2 und 3 PolG-E

Gemäß § 15 Abs. 3 Satz 1 TMG darf der Diensteanbieter für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung des Bookmarking-Diensts aus Nutzungsdaten **Nutzungsprofile** erstellen, sofern dies unter Pseudonym geschieht und der Nutzer dem nicht widerspricht. Als Pseudonym kann z.B. eine Cookie-ID verwendet werden, sofern organisatorische Vorkehrungen gegen die Zusammenführung mit den Identifizierungsmerkmalen getroffen werden, denn eine solche ist durch § 15 Abs. 3 Satz 2 TMG untersagt. Fraglich ist aber, ob § 23a Abs. 9 Satz 2 PolG-E genau darauf abzielt, wenn danach „weitere zur Individualisierung erforderliche technische Daten verlangt werden" können. Daran, dass Nutzungsdatenprofile zu den Nutzungsdaten zählen, kann grundsätzlich kein Zweifel bestehen; der Zugriff hieraus soll mit Blick auf das Recht auf informationelle Selbstbestimmung jedoch gerade unterbunden werden. Demgegenüber stellt die Begründung zum Gesetzentwurf klar, dass die Identifizierung von Nutzern über deren selbst gewählte Kennung (Nickname) für erforderlich gehalten wird; folglich werden solche Identifizierungsmöglichkeiten gerade angestrebt, und zwar offenbar einschließlich der nicht vom Nutzer selbst gewählten, sondern auch der vom Anbieter vergebenen Kennung. Hiergegen bestehen Bedenken.

Wir verkennen nicht, dass Verweise auf an anderer Stelle geregelte Voraussetzungen gesetzestechnisch üblich und hinreichend bestimmt sind. Unbefriedigend ist hingegen, dass nicht erläutert wird, in welchem Gesetz die hier einschlägigen Voraussetzungen geregelt sind. Wird hier etwa die Verbindung zu § 42 PolG oder § 48a PolG hergestellt, so ist zu fragen, ob auch diese Normen als Grundlage dienen können sollen. Würde etwa § 48a Abs. 2 PolG als ausreichende Ermächtigungsgrundlage angesehen, so wäre § 23a Abs. 9 PolG-E insofern weitgehend konturenlos und damit rechtsstaatlich bedenklich. Eine Klarstellung erscheint deshalb dringend geboten.

dd) § 23a Abs. 9 Sätze 4 und 5 PolG-E

Soweit die Unterrichtung des Betroffenen vorgesehen ist, entspricht dies den verfassungsrechtlichen Anforderungen,

> vgl. BVerfG, Urteil vom 02.03.2010 – 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 –, BVerfGE 125, 260ff. (Rdnr. 263).

Denn es gibt keinen Grund, anlässlich der Identifizierung von IP-Adressen Ausnahmen vom Grundsatz der Transparenz zu machen. Der Betroffene, der in der Regel davon ausgehen kann, das Internet anonym zu nutzen, hat prinzipiell das Recht zu erfahren, dass und warum diese Anonymität aufgehoben wurde. Folgerichtig sind deshalb Benachrichtigungspflichten vorgesehen, soweit und sobald hierdurch der Zweck der Auskunft nicht vereitelt wird oder sonst überwiegende Interessen Dritter oder des Betroffenen selbst nicht entgegenstehen.

Soweit darüber hinaus von einer Unterrichtung abgesehen werden soll, wenn der Betroffene von dem Auskunftsverlangen bereits Kenntnis hat, sollte klargestellt werden, dass eine positive Kenntniserlangung gemeint ist und so Unwägbarkeiten einer nur zufälligen Kenntniserlangung ausgeschlossen sind.

Soweit von einer Benachrichtigung nach Maßgabe entsprechender gesetzlicher Regelungen ausnahmsweise abgesehen wird und der Grund hierfür aktenkundig zu machen ist, entspricht dies den verfassungsrechtlichen Vorgaben. Wir gehen aber davon aus, dass die Unterrichtung des Betroffenen in der Weise aktenkundig gemacht wird, dass diese Unterrichtung schriftlich erfolgt und das entsprechende Schriftstück bzw. eine Kopie desselben ebenfalls zur Akte genommen wird.

Dies folgt nach unserem Verständnis daraus, dass die rechtlichen und tatsächlichen Grundlagen entsprechender Auskunftsbegehren jedenfalls aktenkundig zu machen sind,

> vgl. hierzu BVerfG, Urteil vom 02.03.2010 – 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 –, BVerfGE 125, 260ff. (Rdnr. 261).

b) Änderung des Landesverfassungsschutzgesetzes

Zu § 5b LVSG-E kann im Wesentlichen auf die vorangegangenen Ausführungen verwiesen werden, soweit inhaltsgleiche Ergänzungen der bisherigen Eingriffsbefugnisse erfolgen sollen. Ergänzend ist auf Folgendes hinzuweisen:

§ 5b Abs. 1 LSVG-E verweist auf §§ 95, 111 TKG und § 14 TMG, § 5b Abs. 2 LSVG-E spricht dann aber die dynamische IP-Adresse an, die – wie zuvor ausgeführt – weder unter den Begriff der Bestands- bzw. Verkehrsdaten i. S. des TKG noch unter den der Bestandsdaten des § 14 TMG zu subsumieren ist, sondern unter den der Nutzungsdaten des § 15 TMG; diese Bestimmung wird jedoch nicht zitiert.

Wie wir zuvor bereits ausführten, ist die dynamische IP-Adresse des Nutzers für den Telemediendienste-Anbieter für sich allein genommen kein personenbezogenes Datum, da es auf die Möglichkeiten des Anbieters als verantwortliche Stelle ankommt, die Person des Betroffenen zu identifizieren, ihm dazu jedoch regelmäßig nicht die Mittel zur Verfügung stehen, die hinter der IP-Adresse stehende Person zu ermitteln. Nur im Einzelfall wird der Anbieter über diese Informationen verfügen, wird sich die Personenbeziehbarkeit der IP-Adresse über die Verknüpfung mit personenbezogenen Bestands- oder Inhaltsdaten ergeben mit der Folge, dass auch die übrigen Nutzungsdaten als personenbezogene Daten anzusehen sind. Für die Identifizierung einer dynamischen IP-Adresse muss der Anbieter in einem Zwischenschritt die entsprechenden Verbindungsdaten seiner Kunden sichten, also auf konkrete Verkehrs- bzw. Nutzungsdaten zugreifen.

Dies wird zwar inhaltlich in § 5b Abs. 2 LSVG-E angesprochen, sollte aber im Interesse der Normenklarheit ausdrücklich durch Bezugnahme auf die einschlägigen Bestimmungen des TKG und des TMG geregelt werden.

Wir vermissen in dem Gesetzentwurf eine Regelung über die Unterrichtung des Betroffenen. Der Regelung in § 5a Abs. 7 LSVG, der zufolge dem Betroffenen oder Dritten etwaige Auskunftsersuchen nicht vom Auskunftsgeber mitgeteilt werden dürfen, ist uns bewusst. Sie verbietet jedoch keine Unterrichtung durch die Behörde.

Die verfassungsrechtlichen Anforderungen für die Verwendung der Daten zur Gefahrenabwehr gelten für **alle Eingriffsermächtigungen mit präventiver Zielsetzung**. Sie gelten damit auch für die Verwendung der Daten durch die **Nachrichtendienste**. Da die Beeinträchtigung durch den Eingriff in allen diesen Fällen für die Betroffenen die gleiche ist, besteht hinsichtlich dieser Anforderungen kein Anlass zu behördenbezogenen Differenzierungen, etwa zwischen Polizeibehörden und anderen mit präventiven Aufgaben betrauten Behörden wie Verfassungsschutzbehörden. Dass Polizei- und Verfassungsschutzbehörden unterschiedliche Aufgaben und Befugnisse haben und in der Folge Maßnahmen mit unterschiedlicher Eingriffstiefe vornehmen können, ist für die Gewichtung einer Verwendung von vorsorglich flächendeckend und langfristig gespeicherten Telekommunikationsverkehrsdaten grundsätzlich ohne Belang,

> vgl. BVerfG, Urteil vom 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07 –, BVerfGE 120, 274 (329 f.); BVerfG, Urteil vom 02.03.2010 – 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 –, BVerfGE 125, 260ff. (Rdnr. 232).

Zwar können Differenzierungen zwischen den Ermächtigungen der verschiedenen Behörden mit präventiven Aufgaben vor der Verfassung Bestand haben,

> vgl. BVerfG, Urteil vom 14.07.1999 – 1 BvR 2226/94, 1 BvR 2420/95, 1 BvR 2437/95 –, BVerfGE 100, 313 (383); BVerfG, Urteil vom 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07 –, BVerfGE 120, 274 (330); BVerfG, Urteil vom 02.03.2010 – 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 –, BVerfGE 125, 260ff. (Rdnr. 232).

Jedoch ist der Gesetzgeber auch bei der Regelung der einzelnen Befugnisse von Sicherheitsbehörden, deren Aufgabe in der Vorfeldaufklärung besteht, an die verfassungsrechtlichen Vorgaben gebunden, die sich aus dem **Verhältnismäßigkeitsgrundsatz** ergeben,

> vgl. BVerfG, Urteil vom 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07 –, BVerfGE 120, 274 330 f.); BVerfG, Urteil vom 02.03.2010 – 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 –, BVerfGE 125, 260ff. (Rdnr. 232).

Es fällt bereits schwer, diese Anforderungen der Eingangsformulierung des § 5b Abs. 1 Satz 1 LSVG-E („Soweit … zur Erfüllung der Aufgaben … erforderlich, …“) zu entnehmen. Im Rahmen der danach verfassungsrechtlich gebotenen Verhältnismäßigkeitsprüfung sind sowohl hinsichtlich der zu schützenden Rechtsgüter als auch hinsichtlich der hierbei zu beachtenden Eingriffsschwelle **besondere Anforderungen an die Datenverwendung** zu stellen.

Denn es ist nicht ersichtlich, weshalb diese **Anforderungen für die Aufgabenerfüllung der Nachrichtendienste** nicht gelten sollten. Zwar beschränken sich die Aufgaben der Nachrichtendienste grundsätzlich auf die Sammlung von Informationen zur Unterrichtung der Regierung. Das vermindert das Gewicht des Eingriffs insoweit, als sich damit für den einzelnen Bürger über die Gefahr des Beobachtetwerdens hinaus nicht auch die Gefahr von hieran anknüpfenden weiteren Maßnahmen verbindet. Zugleich verringert sich hierdurch aber auch das Gewicht zur Rechtfertigung solcher Eingriffe, denn durch bloße Informationen der Regierung können Rechtsgutverletzungen nicht verhindert werden. Dies ist erst möglich durch Folgemaßnahmen der für die Gefahrenabwehr zuständigen Behörden, deren verfassungsrechtliche Begrenzungen bei der Datenverwendung nicht durch weitergehende Verwendungsbefugnisse im Vorfeld unterlaufen werden dürfen. Eine **besondere Belastungswirkung** solcher Eingriffe gegenüber den Bürgern liegt im Übrigen darin, dass nicht nur der jeweilige Eingriff in das Telekommunikationsgeheimnis als solcher in der Regel verdeckt geschieht, sondern praktisch die gesamten Aktivitäten der Nachrichtendienste geheim erfolgen. Befugnisse dieser Dienste zur Verwendung der vorsorglich flächen-

deckend gespeicherten Telekommunikationsverkehrsdaten befördern damit das Gefühl des unkontrollierbaren Beobachtetwerdens in besonderer Weise und entfalten nachhaltige Einschüchterungseffekte auf die Freiheitswahrnehmung,

> vgl. BVerfG, Urteil vom 02.03.2010 – 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 –, BVerfGE 125, 260ff. (Rdnr. 233).

Das Bekanntwerden nachrichtendienstlicher Aktivitäten, die aufgrund einschlägiger Veröffentlichungen in den Medien mit dem Schlagwort „NSA-Skandal" gekennzeichnet werden, führt schlaglichtartig vor Augen, dass gerade in diesem Bereich an Datenerhebung und –verwendung einschließlich der Weitergabe an ausländische Nachrichtendienste und andere Behörde hohe Anforderungen zu stellen sind, weil anderenfalls das Grundrecht auf informationelle Selbstbestimmung staatlicherseits ausgehöhlt wird.

Es gibt deshalb keinen Grund, die Datenerhebung und insbesondere die Identifizierung von IP-Adressen vom Grundsatz der Transparenz auszunehmen. Der Betroffene, der in der Regel davon ausgehen kann, das Internet anonym zu nutzen, hat prinzipiell das Recht zu erfahren, dass und warum diese Anonymität aufgehoben wurde. Dementsprechend hat der Gesetzgeber jedenfalls Benachrichtigungspflichten vorzusehen, soweit und sobald hierdurch der Zweck der Auskunft nicht vereitelt wird oder sonst überwiegende Interessen Dritter oder des Betroffenen selbst nicht entgegenstehen. Soweit von einer Benachrichtigung nach Maßgabe entsprechender gesetzlicher Regelungen ausnahmsweise abgesehen wird, ist der Grund hierfür aktenkundig zu machen,

> so BVerfG, Urteil vom 02.03.2010 – 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 –, BVerfGE 125, 260ff. (Rdnr. 263) nicht nur für Gefahrenabwehrbehörde, sondern auch und gerade für Nachrichtendienste.

Der Gesetzentwurf ist deshalb dementsprechend zu ergänzen. Denn selbst wenn die Unterrichtung des Betroffenen aufgrund einer – erst noch zu treffenden gesetzlichen Regelung - unterbleiben dürfte, gäbe erst die Aktenkundigkeit derartiger Vorgänge dem – nach dem erklärten Willen der Koalitionsparteien – einzurichtenden Parlamentarischen Kontrollgremium auf Landesebene die Möglichkeit einer Überprüfung der nachrichtendienstlichen Aktivitäten auf ihre Rechtmäßigkeit, insbesondere auf ihre Übereinstimmung mit der Verfassung.

Für etwaige Rückfragen oder auch Gespräche stehen wir selbstverständlich gerne zur Verfügung. Wir wären dankbar, wenn wir – ebenso wie in der Vergangenheit – informiert würden, in welcher Weise der Landtag vom Er-

gebnis der Anhörung unterrichtet wird. Sollte dies durch eine Landtagsdrucksache geschehen, in der die Äußerungen der Verbände wiederum dokumentiert werden, und sollte diese Drucksache elektronisch verfügbar sein, bitte wir darum uns ein Exemplar zur Verfügung zu stellen. Sollte im Laufe des weiteren Verfahrens der Entwurf geändert werden und/oder eine weitere Anhörung durchgeführt werden, bitten wir um eine Unterrichtung und die Gelegenheit zur Äußerung.

Mit freundlichen Grüßen

Prof. Dr. Peter Kothe
Präsident