

Innenausschuss
Wortprotokoll
95. Sitzung

Öffentliche Anhörung

am Montag, 11. März 2013, von 11.00 Uhr bis 13.00 Uhr
Marie-Elisabeth-Lüders-Haus, Raum 3.101 (Anhörungssaal)
Adele-Schreiber-Krieger-Straße 1, 10117 Berlin

Vorsitz: Wolfgang Bosbach, MdB

Öffentliche Anhörung von Sachverständigen
zum

Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Änderung des Telekommunikationsgesetzes und zur
Neuregelung der Bestandsdatenauskunft

BT-Drucksache 17/12034

	<u>Seite</u>
I. Anwesenheitsliste	
• Mitglieder des Deutschen Bundestages	4
• Bundesregierung, Bundesrat, Fraktionen	
II. Sachverständigenliste	6
III. Sprechregister der Sachverständigen und Abgeordneten	7
IV. Protokollierung der Anhörung Bandabschrift	8
V. Anlage A:	
Schriftliche Stellungnahmen der Sachverständigen - Ausschussdrucksachen-Nr.: 17(4)680 A ff -	
• Ernst Wirth Bayerisches Landeskriminalamt – 17(4)680 A	35
• Prof. Dr. Kyrill-Alexander Schwarz Julius-Maximilians-Universität Würzburg – 17(4)680 B	37
• Prof. Dr. Matthias Bäcker, LL.M. Universität Mannheim – 17(4)680 C	40
• Wilhelm Achelpöhler Rechtsanwalt, Fachanwalt für Verwaltungsrecht, Münster – 17(4)680 D	47
• Prof. Dr. Dieter Kugelmann Deutsche Hochschule der Polizei, Münster – 17(4)680 E(neu)	56
• Dr. Alexander Dix Berliner Beauftragter für Datenschutz und Informationsfreiheit – 17(4)680 F	64
• Peter Schaar Der Bundesbeauftragte für den Datenschutz und die Informations- freiheit, Bonn/Berlin – 17(4)680 G	67

Anlage B:

Weitere Stellungnahmen

- **BITKOM e.V.**, Berlin – 17(4)621 69
- **Arbeitskreis Vorratsdatenspeicherung** – 17(4)686 73

I. Anwesenheitsliste Mitglieder des Deutschen Bundestages

Bundesregierung

Bundesrat

Fraktionen und Gruppen

II. Liste der Sachverständigen für die Öffentliche Anhörung am 11. März 2013

1. Wilhelm Achelpöehler Rechtsanwalt, Münster

2. Prof. Dr. Matthias Bäcker, LL.M. Universität Mannheim

3. Dr. Alexander Dix Berliner Beauftragter für Datenschutz und Informationsfreiheit, Berlin

4. Prof. Dr. Dieter Kugelmann Deutsche Hochschule der Polizei, Münster

5. Peter Schaar Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Bonn/Berlin

6. Prof. Dr. Kyrill-Alexander Schwarz Julius-Maximilians-Universität Würzburg

7. Ernst Wirth Bayerisches Landeskriminalamt, München

III. Sprechregister der Sachverständigen und Abgeordneten

<u>Sprechregister der Sachverständigen</u>	Seite
Wilhelm Achelpöhler	8, 27, 32
Prof. Dr. Matthias Bäcker, LL.M.	9, 22, 28, 33
Dr. Alexander Dix, LL.M.	11, 24, 31, 34
Prof. Dr. Dieter Kugelman	12, 23, 27
Peter Schaar	14, 25, 31, 34
Prof. Dr. Kyrill-Alexander Schwarz	15, 20
Ernst Wirth	17, 19, 32

Sprechregister der Abgeordneten

Vors. Wolfgang Bosbach	8, 18, 23, 25, 32, 34
BE Armin Schuster (Weil am Rhein)	18, 19
BE Michael Hartmann (Wackernheim)	21
BE Gisela Piltz	25
BE Jan Korte	30
BE Dr. Konstantin von Notz	33

IV. Protokollierung der Anhörung

Vors. **Wolfgang Bosbach**: Meine sehr verehrten Damen und Herren, herzlich willkommen zur 95. Sitzung des Innenausschusses, der Sachverständigenanhörung über den Gesetzentwurf zur Änderung des Telekommunikationsgesetzes – kurz Bestandsdatenauskunft. Ich danke den Herren Sachverständigen, dass Sie unserer Einladung nachgekommen sind, um uns bei den anstehenden Beratungen mit Ihrer Expertise zu unterstützen und die Fragen der Kolleginnen und Kollegen am heutigen Tage zu beantworten. Ich begrüße die Gäste auf der oberen Etage, für die Bundesregierung wird später noch der Parlamentarische Staatssekretär Dr. Ole Schröder zu uns kommen. Ich bedanke mich auch für die schriftlichen Stellungnahmen, die uns erreicht haben. Das war nicht selbstverständlich, denn die Zeit war relativ kurz, umso dankbarer sind wir Ihnen. Die Stellungnahmen werden an die Mitglieder des Ausschusses und der mitberatenden Ausschüsse verteilt und werden dann Bestandteil einer Gesamtdrucksache über dieses Gesetzgebungswerk. Für die heutige Anhörung wird von dem Wortprotokoll eine Bandabschrift gefertigt, das Protokoll wird Ihnen zur Korrektur übersandt. Die Gesamtdrucksache besteht aus dem Protokoll und Ihren schriftlichen Stellungnahmen und wird auch in das Internet eingestellt.

Zeit haben wir bis maximal 13.00 Uhr, d. h., wir müssen nicht so lange, wir dürfen aber so lange tagen. Zum Einstieg hat jeder Sachverständige die Gelegenheit, das Gesetzgebungsvorhaben aus seiner Sicht zu bewerten in einer Länge von bitte nicht mehr als fünf Minuten, danach beginnt die Fragerunde. Zunächst mit den zuständigen Berichterstattern der Bundestagsfraktionen.

In alphabetischer Reihenfolge darf ich zunächst Herrn Wilhelm Achelpöhler, Rechtsanwalt aus Münster um seine Stellungnahmen bitten.

SV Wilhelm Achelpöhler (Rechtsanwalt, Münster): Herr Vorsitzender, ich bedanke mich für die Einladung. Ich habe die Stellungnahme des Deutschen Anwaltvereins überreicht, ich will mich deshalb auch kurzfassen. Wir haben es hier mit einer Gesetzesinitiative zu tun, die letztlich vom Bundesverfassungsgericht (BVerfG) veranlasst worden ist. Man hat sich in der Vergangenheit an der Grenze des verfassungsrechtlich Zulässigen bewegt, allerdings auf der falschen Seite. Jetzt habe ich den Eindruck, ist es politisch gewollt, sich weiterhin an dieser Grenze des verfassungsrechtlich Zulässigen zu bewegen. Meines Erachtens gelingt es nicht immer, diese Grenze nicht zu überschreiten. Das betrifft insbesondere die fachgesetzlichen Ermächtigungen im Rahmen des Bundeskriminalamtgesetzes (BKAG) und des Bundespolizeigesetzes (BPolG). Das BVerfG hatte in seiner Entscheidung darauf hingewiesen, dass diese Ermächtigungen verfassungsrechtlich noch hinnehmbar seien, da sie an eine konkrete Gefahr anknüpften. In der heutigen Fassung des Gesetzes gibt es diese Anknüpfung an eine konkrete Gefahr in den fachgesetzlichen

Ermächtigungen nicht mehr, sondern die Ermächtigung zur Datenerhebung knüpft nur daran an, dass das zur Aufgabenerfüllung dienen soll. Wenn es der Aufgabenerfüllung dient, dann muss man in den Blick nehmen, dass zu den Aufgaben sowohl der Bundespolizei als auch des Bundeskriminalamts (BKA) gerade auch die Gefahrenvorsorge gehört, so dass im Unterschied zu der früheren Fassung hier der Anwendungsbereich erweitert wird. Die Bundesregierung hatte im Hinblick auf ähnliche Hinweise des Bundesrates darauf hingewiesen, dass eine konkrete Ermächtigung, nämlich die nach § 4a BKAG, eine konkrete Gefahr voraussetze, das ist richtig. Nur, die jetzt im Gesetzentwurf vorgeschlagene fachgesetzliche Regelung knüpft nicht an diese Norm an, sondern generell an die Aufgabenerfüllung des BKA. Das erfasst auch die Gefahrenvorsorge und damit Eingriffe weit im Vorfeld. Wenn man sich vor Augen führt, dass das BVerfG die damalige Fassung angesichts ihrer doch relativen Weite noch als hinnehmbar gehalten hat, weil die konkrete Gefahr gefordert wird, dann wird man sagen können, jetzt ist es noch ein bisschen mehr, was erlaubt worden ist. So dass sich die Frage doch neu stellt, ob hier der Rahmen des verfassungsrechtlich Zulässigen überschritten worden ist. Es findet sich zwar eine Passage in der Entscheidung des BVerfG, wonach eine derartige Übermittlung zur Aufgabenerfüllung nicht beanstandet wird, aber das war konkret bezogen auf die Aufgabenerfüllung im Bereich der Gefahrenabwehr, die eine entsprechende konkrete Gefahr voraussetzte. Da sehe ich ein verfassungsrechtliches Problem.

In anderer Hinsicht meine ich, dass sich da eher rechtspolitische Fragen stellen, bspw. die Frage der Benachrichtigungspflicht oder des Richtervorbehalts. Ich persönlich halte mehr davon, die Rechtsschutzmöglichkeiten der Betroffenen insoweit zu eröffnen, als sie von bestimmten Maßnahmen, jedenfalls soweit es IP-Adressen betrifft, informiert werden, damit sie nachträglichen Rechtsschutz suchen können. Wer ansonsten Erfahrungen mit polizeilichen Maßnahmen unter Richtervorbehalt gemacht hat, der wird durch die Realität einigermaßen ernüchtert sein und sich von diesem Instrument nicht allzu viel versprechen. Das waren kurz zusammengefasst meine Ausführungen.

Vors. **Wolfgang Bosbach**: Vielen Dank, Herr Achelpöbler. Der nächste Sachverständige ist Herr Prof. Dr. Bäcker von der Universität in Mannheim, herzlich willkommen.

SV **Professor Dr. Matthias Bäcker, LL.M.** (Universität Mannheim): Auch ich bedanke mich für die Gelegenheit zur Stellungnahme und kann teilweise an meinen Vorredner anknüpfen. Laut der Einladung zu dieser Anhörung sollen hier prozedurale Sicherungsmaßnahmen für Bestandsdatenabrufe im Vordergrund stehen, insbesondere Richtervorbehalte und Benachrichtigungspflichten. Ich denke aber auch, dass der Entwurf einige grundlegende Fragen aufwirft, die zumindest hier im Rahmen der Einführung erwähnt werden sollten. Das betrifft zum einen die vorgesehenen Übermittlungsermächtigungen in § 113 Telekommunikationsgesetz-Entwurf

(TKG-E) und zum anderen die Abfrageermächtigungen, zu denen Herr Achelpöhler schon etwas gesagt hat.

§ 113 TKG in der Entwurfsfassung leidet unter einem recht gravierenden handwerklichen Fehler: Das BVerfG hat in seinem Beschluss zu dem alten § 113 TKG das sogenannte „Doppeltür-Modell“ eingeführt, nach dem der Transfer von Bestandsdaten zu einer Sicherheitsbehörde zweier Ermächtigungen bedarf: nämlich einer Übermittlungsermächtigung für die TK-Diensteanbieter und einer Abfrageermächtigung für staatliche Stellen. Damit ist die Frage noch nicht geklärt, was in diesen Ermächtigungen jeweils drinzustehen hat. Auch dazu hat sich das BVerfG jedoch verhalten und gesagt, dass die grundrechtliche Rechtfertigungslast für den Bestandsdatenabruf schon in der Übermittlungsermächtigung abzudecken ist. Das bedeutet konkret, dass die Übermittlungsermächtigung bereits den Datentransfer an eine tatbestandliche Schwelle binden muss, die dafür sorgt, dass insgesamt die verfassungsrechtlichen Anforderungen gewahrt sind. § 113 TKG in der Entwurfsfassung tut das nicht, sondern § 113 TKG in der Entwurfsfassung nennt lediglich die Behörden, an die übermittelt werden darf, aber nicht, unter welchen Voraussetzungen dies geschehen darf. Das führt dazu, dass diese Vorschrift die Regelungsverantwortung des Gesetzgebers verfehlt und darum Grundrechte verletzt.

Die Probleme setzen sich fort in den Abfragermächtigungen, die der Gesetzentwurf vorsieht. Herr Achelpöhler hat zum BKAG schon etwas gesagt und hat meiner Ansicht nach damit vollkommen Recht. Die Abrufermächtigungen, die der Gesetzentwurf vorsieht, binden mitnichten den Abruf durchweg an eine konkrete Gefahr oder einen konkreten Tatverdacht, wie das bisher der Fall war, sondern sie erweitern gegenüber dem bisherigen Rechtszustand ganz massiv die Befugnisse der Sicherheitsbehörden, insbesondere des BKA, der Bundespolizei und auch des Zollkriminalamts hin zum Gefahrenvorfeld. Eine besonders auffällige Vorschrift ist § 7 BKAG in der Entwurfsfassung, eine Vorschrift, die dem BKA ergänzende Datenerhebungen im Rahmen seiner Zentralstellentätigkeit ermöglicht. Die Vorschrift soll dem BKA ermöglichen, kriminalstrategische Analysen durchaus weit im Vorfeld von Gefahr und Verdacht durchzuführen. Dazu soll jetzt auch der Bestandsdatenabruf bereitstehen. Das ist mit dem Beschluss des BVerfG nicht zu vereinbaren.

Schließlich möchte ich noch kurz auf die verfahrensrechtlichen Sicherungen eingehen, die ja den Hauptgegenstand der Anhörung bilden sollen: Verfassungsrechtlich geboten sind solche Sicherungen für die Abfrage von Zugangsdaten, mit denen entweder Endgeräte oder Speicherungseinrichtungen im Netz gesichert werden. Denn der Abruf eines Zugangsdatums vertieft den Grundrechtseingriff, der in der Kenntnisnahme der Inhalte liegt, weil der informationelle Selbstschutz des Betroffenen vereitelt wird. Deswegen meine ich, dass hier sowohl ein Richtervorbehalt als auch eine Benachrichtigungspflicht geboten sind, soweit nicht Richtervorbehalt und Benachrichtigungspflicht ohnehin schon für die Kenntnisnahme der Inhalte ange-

ordnet werden, die dann letztlich entschlüsselt werden sollen. Was die Abfrage von IP-Adressen angeht, glaube ich nicht, dass ein Richtervorbehalt verfassungsrechtlich geboten ist, eine generelle Benachrichtigungspflicht wohl auch nicht. Rechtspolitisch erscheint mir eine Benachrichtigungspflicht allerdings angezeigt. Herzlichen Dank!

Vors. **Wolfgang Bosbach**: Als nächster Sachverständiger bitte Herr Dr. Dix, der Berliner Beauftragte für Datenschutz und Informationsfreiheit.

SV **Dr. Alexander Dix, LL.M.** (Berliner Beauftragter für Datenschutz und Informationsfreiheit, Berlin): Vielen Dank, auch für die Einladung zu dieser Anhörung. Ich will mich auf drei Punkte konzentrieren. Ich habe eine schriftliche Stellungnahme übergeben, allerdings so spät, dass sie Ihnen möglicherweise noch nicht vorliegt. Auf diese Stellungnahme verweise ich und ich will drei Punkte hervorheben: Zum einen hat das BVerfG in seinem Beschluss, der durch diesen Gesetzentwurf umgesetzt werden soll, differenziert zwischen der Auskunft über Bestandsdaten – gewissermaßen klassisch über Telefonnummern und die dahinterstehenden Personen – und der Identifizierung von dynamischen IP-Adressen auf der anderen Seite. Bei der Aufdeckung von dynamischen IP-Adressen hat das Gericht ausdrücklich von einer erheblich größeren Persönlichkeitsrelevanz gesprochen, weil man die IP-Adresse gewissermaßen als Generalschlüssel für das Surfverhalten von Internetnutzern ansehen kann. Wenn diese IP-Adresse aufgedeckt wird, liegt darin ein erheblich größerer Eingriff, so dass der Gesetzgeber daran gehindert ist, die bloße Bestandsdatenauskunft und die Aufdeckung von IP-Adressen pauschal gleichzubehandeln. Genau das tut der Entwurf aber. In diesem Punkt sehe ich ihn als verfassungsrechtlich problematisch an. Das betrifft sowohl die erste als auch die zweite Tür, also die Abrufbefugnisse in den Fachgesetzen. Der Gesetzgeber muss hier der erhöhten Persönlichkeitsrelevanz bei der Aufdeckung von IP-Adressen Rechnung tragen. Das sollte er zumindest auch in der Form tun, dass nicht wie bisher für die Verfolgung von Ordnungswidrigkeiten jedweder Art die Aufdeckung von IP-Adressen zugelassen wird. Hier muss auch schon nach dem Urteil des BVerfG zur Vorratsdatenspeicherung mindestens eine Einschränkung, wenn man überhaupt die Verfolgung von Ordnungswidrigkeiten mit diesen Mitteln ausstatten will, auf Ordnungswidrigkeiten von erheblicher Bedeutung erfolgen.

Zum Zweiten: Die Einführung des Internetprotokolls Version 6, die gegenwärtig bereits läuft, ist in ihren Auswirkungen noch nicht vollständig abzusehen. Ich verweise aber darauf, dass das BVerfG auch schon in seinen Ausführungen zu § 112 TKG, der gar nicht Gegenstand dieses Gesetzentwurfs ist, der vom BVerfG in der alten, jetzigen Fassung auch für unbedenklich gehalten wurde, gleichwohl im Hinblick auf die Einführung des Internetprotokolls Version 6 eine Beobachtungs- und Nachbesserungspflicht des Gesetzgebers statuiert. Ich bin der Auffassung, weil gegenwärtig die Auswirkungen dieser technischen Neuerungen – das Internetprotokoll Version 6 wird ja gegenwärtig parallel zu IPv4 genutzt und möglicherweise auch noch

für längere Zeit – der Gesetzgeber seiner Beobachtungs- und Nachbesserungspflicht nur in der Weise gerecht werden kann, indem er jetzt den § 112 TKG mit einer Befristung bis zum 31. Dezember 2014 versieht und dann eine unabhängige wissenschaftliche Evaluation genau mit dieser Frage befasst, welche Auswirkung IPv6 in diesem Bereich hat.

Zum dritten Punkt: Der Gesetzentwurf sieht keinerlei Benachrichtigungspflichten vor. Das Gericht hatte ausdrücklich die Frage offengelassen, ob Benachrichtigungspflichten und eventuell auch der Vorgang der Datenerhebung beim Betroffenen geboten sein könnten, weil die nicht Gegenstand des Verfahrens waren. Der Gesetzgeber sollte diese Fragen aber beantworten, und zwar in der Weise, dass Benachrichtigungspflichten eingeführt werden, um dem Betroffenen zumindest nachträglich Rechtsschutzmöglichkeiten zu geben. Da teile ich die Auffassung, die auch Herr Achelpöehler geäußert hat. Ich habe mich nicht zur Frage des Richtervorbehalts geäußert, dazu wird mein Kollege, Herr Schaar, noch Stellung nehmen. Seine Auffassung zu diesem Punkt teile ich ausdrücklich. Vielen Dank!

Vors. **Wolfgang Bosbach**: Wir danken Ihnen. Als nächster Sachverständiger bitte Herr Prof. Dr. Kugelmann von der Deutschen Hochschule der Polizei in Münster.

SV **Professor Dr. Dieter Kugelmann** (Deutsche Hochschule der Polizei, Münster): Vielen Dank, Herr Vorsitzender, und vielen Dank für die Einladung. Ich gehe auf die Fragen der Anhörung ausgehend vom Richtervorbehalt ein. Bei der Frage des Grundrechtsschutzes durch Verfahren, prozedurale Vorkehrungen, hebt das BVerfG insbesondere auf die Intensität des Eingriffes ab. Da spielt insbesondere eine Rolle, ob der Eingriff heimlich ist, ob Daten besonders sensibel sind, welche Daten damit gesammelt werden und ob die Zonen der Privatheit, die besonders geschützt sind, tangiert werden. Ich würde die drei unterschiedlichen Fallgruppen, die § 113 TKG enthält, insoweit einzeln kurz ansprechen wollen.

Das eine ist die Frage der Zuordnung dynamischer IP-Adressen: Bedarf es eines Richtervorbehalts? Meine Antwort darauf ist: ja. Das BVerfG hat hier gesagt, Art. 10 Grundgesetz (GG) ist einschlägig, d. h., wir haben eine heimliche Maßnahme, eine Maßnahme, die dem Betroffenen nicht bekannt wird, die einen Eingriff in die Telekommunikationsfreiheit bedeutet. Das löst verfassungsrechtlich zwingend die Notwendigkeit eines Richtervorbehalts aus.

Die zweite Fallgruppe ist die der Zugangssicherungs-codes, die PIN- und PUK-Vorkehrungen, die der Einzelne ja deshalb trifft, um seine Privatsphäre selbstbestimmt zu schützen. Genau das, was das BVerfG im Volkszählungsurteil gesagt hat: Jeder soll selbst darüber bestimmen können, ob jemand Zugang zu seinen Daten hat oder nicht. Wenn dann jemand Zugangsmechanismen einrichtet, bedeutet das, er errichtet eine selbst definierte Zone der Privatheit, in die der Staat nur unter

hohen Voraussetzungen eingreifen darf; also auch insoweit die Notwendigkeit eines Richtervorbehaltes, weil diese Zone der Privatheit besonders schützenswert ist.

Die dritte Fallgruppe wäre der normale Zugriff auf die Daten, die die Provider, die Telekommunikationsunternehmen, nach den §§ 95 und 111 des TKG sammeln. Inso- weit sehe ich keine verfassungsrechtliche Gebotenheit eines Richtervorbehaltes. Hier geht es überwiegend um die Vertragsdaten, um die Daten, die mit Einwilligung des Betroffenen vom Telekommunikationsunternehmen erhoben werden. Das ist nicht heimlich und es ist nicht so nah an der selbst bestimmten Privatheit, dass die er- höhten Schwellen aufgerufen werden.

Zum nächsten Punkt, den Mitteilungspflichten: Auch diese Mitteilungspflichten, übrigens wie auch den Richtervorbehalt, würde ich in den Fachgesetzen verorten, also nicht im TKG. Das ist ein technisches, ein wirtschaftliches Gesetz, das sich eher an die Diensteanbieter wendet. Mitteilungspflichten sind Mittel der nachträglichen Kontrolle im Unterschied zum Richtervorbehalt, der ein Mittel vorbeugender Kontrolle ist. Mitteilungspflichten der nachträglichen Kontrolle sollten in die Fachgesetze integriert werden, insbesondere wieder für Fallgruppe 1 bei den dynamischen IP-Adressen. Wenn ein Zugriff einer der abschließend genannten Behörden auf die Daten des Betroffenen heimlich erfolgt und dabei konkrete Kommunikationsvorgänge betroffen sind, ist verfassungsrechtlich eine Mitteilungspflicht zwingend erforderlich, um nachträglich Rechtsschutz für den Einzelnen zu ermöglichen.

Die zweite Fallgruppe: PINs, PUKs – Zugangssicherungs-codes. Auch hier wieder der Punkt, dass der Betroffene aus eigenem Willen und eigener Entscheidungsmacht eine Zone der Privatheit errichtet. Diese Zone der Privatheit wird verletzt, indem wir die PINs abfragen, dann kennt sie der Staat. Dann muss man dem Betroffenen min- destens hinterher mitteilen: „Du kannst wieder eine neue PIN einrichten“, damit er wieder eine Zone errichten kann, denn jetzt ist seine PIN ja bekannt, also die Zone der Privatheit gerade geöffnet. Ein Selbstbestimmungsargument, Schutz der infor- mationellen Selbstbestimmung schafft meines Erachtens die zwingende Notwendig- keit Mitteilungspflichten.

Zur letzten Fallgruppe – Bestandsdaten nach den §§ 95 und 111 TKG: Da würde ich parallel zum Richtervorbehalt sagen, die Eingriffstiefe ist nicht so erheblich, dass wir hier von einer derart starken Berührung der Privatheit ausgehen müssen, dass eine Mitteilungspflicht geboten wäre. Ob sie verfassungspolitisch sinnvoll ist, liegt im Spielraum des Gesetzgebers.

Zum letzten Punkt – die Technik: IPv6, da stehen wir, wie in so vielen technisch geleiteten Dingen, vor der Situation der Unsicherheit. Der Unsicherheit deshalb, weil es noch unsicher ist, wie in welcher Bandbreite diese neuen Internetprotokolle ange- wendet werden. Insbesondere wie und in welcher Bandbreite die sogenannten

Privacy Extensions, die Möglichkeit dann doch wieder teils zu verschlüsseln, angewendet würden. Wenn ich davon ausgehe, bisher sind es dynamische, immer neu zugewiesene Adressen, künftig können es statische sein, dann ist das mit Sicherheit eine Verletzung oder eine Berührung des Rechts auf informationelle Selbstbestimmung, das hat auch das BVerfG in seinem Urteil ausdrücklich gesagt. Damit stellt sich die Frage, wenn es so wäre, wie 2011 zumindest die Deutsche Telekom oder Vodafone angekündigt hatten, dass sie von Providerseite die Privacy Extensions standardmäßig einführen wollten, dann würde wieder eine gewisse Dynamik hineinkommen. Das heißt, man hätte eine Annäherung an die dynamischen IP-Adressen. Die Konsequenz wäre rechtliche Gleichstellung in diesem Fall mit dem, was dynamische IP-Adressen betrifft. Das ist ein Punkt, der von der Technik abhängt, der sich auch nicht letztlich abschließend bewerten lässt, jedenfalls beim Datenschutz. Aber ich würde entgegen dem BVerfG auch dazu neigen, bei der Einführung und Anwendung von IPv6 das gleichzustellen mit dynamischen IP-Adressen. Mit der Konsequenz, dass ich befürworten würde, in den Fachgesetzen jeweils zu dem Absatz, in dem die dynamischen IP-Adressen geregelt sind, einen weiteren Satz anzuhängen, in dem steht: „Satz 1 gilt auch bei festen Internetprotokollen“, um einen möglichst hohen Grundrechtsschutz des Betroffenen zu gewährleisten. Danke schön!

Vors. **Wolfgang Bosbach**: Wir danken Ihnen. Der nächste Sachverständige ist der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Herr Schaar.

SV **Peter Schaar** (Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Bonn/Berlin): Vielen Dank, Herr Vorsitzender. Ich denke, es ist auch schon bei den Vorrednern deutlich geworden, dass wir hier hinsichtlich der Eingriffsintensität abstufen müssen. Aus meiner Sicht sind die Zugangs-sicherungs-codes, die abgefragt werden, am sensibelsten – die PINs und PUKs. Dann kommen die Zuordnungsdaten hinsichtlich der dynamischen IP-Adressen. In vergleichbarer Weise würde ich auch die IPv6-Adressen bewerten. Bei IPv6 handelt es sich um ein Protokoll, das es ermöglicht, nicht nur den Nutzer zu identifizieren, sondern ggf. auch in seinem Bereich befindliche Gerätschaften oder Dienste, die eine eigene IP-Adresse bekommen. Wir wissen noch nicht genau, wie diese Zuordnung erfolgen wird. Aber gerade bei diesen Geräten wie Kühlschränken, Heizungen, Garagentore usw. ist es so, dass diese Informationen im Zweifel nicht dynamisch, sondern fest zugeordnet werden, damit die entsprechenden Funktionen kontrolliert werden können. Das würde bedeuten, dass die auslösenden Aktivitäten damit dann auch dem Zugriff unterliegen würden, wenn eine Abfrage erfolgt. Deshalb würde ich die Beauskunftung von IPv6-Adressen, jedenfalls der Zuordnung der dynamischen IP-Adressen bei IPv4 gleichstellen. Am wenigsten sensibel, das ist schon genannt worden, ist die normale Bestandsdatenauskunft. Das hat Konsequenzen für die Benachrichtigungspflicht. Hier denke ich, dass, wie vom BVerfG in seiner Vorratsdatenspeicherungsentscheidung auch explizit gefordert, eine Benachrichtigungspflicht, bezogen auf die Zuordnung der IPv4-Adressen erfolgen muss.

Bei PINs und PUKs gibt es bisher keine Rechtsprechung des BVerfG. Aber im Hinblick auf den Sensitivitätsgrad und entsprechend der Eingriffstiefe sehe ich auch hier eine Benachrichtigungspflicht als geboten an. Hinsichtlich der einfachen Bestandsdatenauskunft sehe ich diese Notwendigkeit nicht.

Im Hinblick auf den Richtervorbehalt würde ich diese Abstufung genauso vornehmen und für die IP-Beauskunftung sowie die PIN- und PUK-Beauskunftung einen Richtervorbehalt vorschlagen. Auch wenn das BVerfG in seinem Urteil das so nicht explizit vorgesehen hat.

Ein wichtiger Punkt ist die Frage: Für welche Zwecke dürfen solche Daten abgefragt werden? Das ist auch schon von verschiedenen Sachverständigen angesprochen worden. Hier sehe ich insbesondere bei den Ordnungswidrigkeiten Nachbesserungsbedarf. Nicht jede Ordnungswidrigkeit rechtfertigt eine Bestandsdatenauskunft, das hat das BVerfG auch deutlich gemacht. Dementsprechend sollte eine Beschränkung in diesem Bereich auf besonders schwere Ordnungswidrigkeiten vorgenommen werden. Vielen Dank!

Vors. **Wolfgang Bosbach**: Wir danken Ihnen. Der vorletzte Sachverständige ist Herr Prof. Dr. Schwarz von der Julius-Maximilians-Universität in Würzburg.

SV Professor Dr. Kyrill-Alexander Schwarz (Julius-Maximilians-Universität Würzburg): Herr Vorsitzender, meine sehr verehrten Damen und Herren, haben Sie ganz herzlichen Dank für die Gelegenheit hier zur Sachverständigenstellungnahme. Ich möchte zunächst einleitend auf einige Punkte hinweisen und mich dann einzelnen Aspekten des Gesetzgebungsvorhabens näher zuwenden.

Ein erster ganz zentraler Punkt, meine Damen und Herren, ist tatsächlich eine Vergewisserung über die Eingriffsintensität und Eingriffsqualität, über die wir hier reden. Wenn man sich das gesamte sicherheitsrechtliche Instrumentarium etwas genauer ansieht, dann wird man sagen können, dass wir uns in Anbetracht dessen, was sonst möglich ist, hier zunächst einmal auf einer relativ geringen Stufe bewegen. Diese relativ geringe Stufe führt dann aber im Ergebnis auch dazu, dass die Rechtfertigungsanforderungen an entsprechende Eingriffe deutlich tiefer sind als bei anderen möglichen sicherheitsrechtlichen Instrumentarien. Darüber hinausgehend, und das ist ein ganz zentraler Punkt, das ist auch bei allen bisherigen Sachverständigenstellungnahmen deutlich geworden, es ist deutlich zu differenzieren zwischen dem, was verfassungspolitisch vielleicht gewünscht ist, und dem, was verfassungsrechtlich tatsächlich geboten ist. Verfassungsrechtlich geboten ist deutlich weniger als das, was verfassungspolitisch möglicherweise erwünscht wird.

Ich will mich auf einige Bereiche etwas näher konzentrieren. Der erste Punkt ist die Frage: Reicht das, was wir in § 113 TKG-E geregelt haben, momentan aus? Es ist zutreffend darauf hingewiesen worden, dass diese Regelung des § 113 TKG-E im Wesentlichen drei Teilregelungselemente enthält. Man kann sagen, das mag man möglicherweise noch weiter ausdifferenzieren, und man mag sagen, das sind von der Eingriffsintensität doch unterschiedliche Dinge, die es vielleicht auch verdienen, dass sie jeweils eine einzelne gesetzliche „Hausnummer“ bekämen. Auf der anderen Seite kann man sagen, es sind insgesamt Daten, die abgefragt werden, die von der Intensität des Eingriffs her deutlich geringer sind und es ist nicht die Vorschrift alleine, die rechtsstaatlich vielleicht Bauchschmerzen bereiten könnte. Sondern man muss sehen, diese Vorschrift, und das ist genau die Systematik, mit der die Rechtsprechung des BVerfG umgesetzt wird, das Doppeltür-Modell knüpft immer an eine fachspezifische Ermächtigung an und das Vorliegen hier in dieser fachspezifischen Ermächtigung ist das, was letzten Endes den Eingriff rechtfertigen kann oder nicht. Das bedeutet aber auch, dass wir die jeweils fachspezifischen Ermächtigungen und die Rechtfertigungen nach Maßgabe des Fachrechts nicht eins zu eins übertragen müssen in die generelle Ermächtigung des § 113 TKG.

Was ebenfalls im Vorfeld geäußert wurde und was nach meiner Meinung nicht zutreffend ist, ich habe das auch in der schriftlichen Stellungnahme ausgeführt, ist die Vorstellung, dass hiermit ein allgemeines Überwachungsszenario ermöglicht würde. Es handelt sich um Maßnahmen, die im Einzelfall erfolgen sollen. Das heißt, ein generelles Gefühl der Überwachung, um ein altes Zitat aus der Rechtsprechung des BVerfG hier noch einmal aufleben zu lassen, ist mit Maßnahmen nach § 113 TKG und den entsprechenden fachspezifischen Ermächtigungen sicherlich nicht zu befürchten.

Der sicherlich entscheidende Punkt ist die Frage von Richtervorbehalten und Benachrichtigungspflichten. Richtervorbehalte als Instrument präventiver Kontrolle, Benachrichtigungspflichten als Instrument einer ex-post-Kontrolle. Wenn man sich jüngere rechtswissenschaftliche Arbeiten anschaut, dann wird sehr deutlich, dass bei beiden Instrumenten erhebliche Bedenken hinsichtlich ihrer Tauglichkeit und ihrer Wirksamkeit mittlerweile im Schrifttum geltend gemacht werden. Da ist in sehr schöne Worte gekleidet worden, dass bspw. die Strahlkraft des Richtervorbehaltes doch deutlich nachgelassen hat, wenn man sich tatsächlich ansieht, was dort passiert. Man mag über andere Dinge sprechen, die das kompensieren mögen. Man mag darüber sprechen, ob man Mitwirkungspflichten von Datenschutzbeauftragten oder anderes einführt. Das ist bisher alles nicht passiert. Aber rechtspolitisch oder verfassungsrechtlich zwingend ist weder der Richtervorbehalt noch eine Benachrichtigungspflicht. Ich will das noch einmal verdeutlichen: Wenn man sich ansieht, für welche Fälle ursprünglich das GG einen Richtervorbehalt vorgesehen hat, dann waren das Eingriffe in Art. 13 GG – die Unverletzlichkeit der Wohnung – und zwar wegen der besonderen Intensität der entsprechenden Eingriffe. Dann ist es die

Rechtsprechung des BVerfG gewesen, die zunehmend zum Schutz durch entsprechendes Verfahren Richtervorbehalte und Benachrichtigungspflichten aufgebaut hat. Was man aber ganz deutlich sagen muss, diese entsprechenden Instrumentarien von Schutz durch Verfahren sind für massive Grundrechtseingriffe gedacht, die wir hier im Ergebnis nicht haben. Das heißt, wir müssen auch zur Kenntnis nehmen, Sie können das rechtspolitisch gerne machen, aber es ist verfassungsrechtlich nicht geboten, entsprechende Benachrichtigungspflichten oder Richtervorbehalte aufzunehmen. Das ist eine Frage dessen, was man politisch durchsetzen möchte oder auch nicht. Herzlichen Dank!

Vors. **Wolfgang Bosbach**: Vielen Dank, Herr Prof. Schwarz. Als letzter Sachverständiger vom Bayerischen Landeskriminalamt in München, Herr Wirth.

SV **Ernst Wirth** (Kriminalrat, Bayerisches Landeskriminalamt, München): Herr Vorsitzender, meine Damen und Herren, ich bedanke mich recht herzlich für die Einladung und die Möglichkeit, hier Stellung zu beziehen. Ich habe in meinen schriftlichen Ausführungen Stellung zum Thema der Benachrichtigungspflicht und des Richtervorbehaltes genommen, deshalb möchte ich hier mündlich nicht mehr darauf eingehen. Grundsätzlich ist es aus unserer Ansicht so, dass das vorliegende Gesetzesvorhaben, insbesondere die geplante Einführung von § 100j Strafprozessordnung (StPO) als handhabbar, positiv und umsetzbar bewertet wird. Es beinhaltet klarstellende Regelungen und Befugnisse, ohne diese durch Formvorschriften zu überfrachten. Wir leiden derzeit wiederholt darunter, dass Gesetzesvorhaben und -initiativen mit Formvorschriften überfrachtet werden, die es in der praktischen Umsetzung nahezu verunmöglichen, aus polizeipraktischer Sicht diese noch umzusetzen. Als besonders positiv werten wir die Verpflichtung der Telekommunikationsdiensteanbieter zur Einführung einer gesicherten elektronischen Schnittstelle zur Entgegennahme der Auskunftsverlangen sowie für die Erteilung der Auskünfte. Damit wird eine moderne und transparente Kommunikationsform zu den Verpflichteten geschaffen. Nach den mir vorliegenden Informationen arbeiten die großen Netzbetreiber auch bereits mit großem Nachdruck daran, diese elektronische Schnittstelle alsbald umzusetzen, weil sie hier erhebliches Einsparpotenzial sehen. Auch wir stehen in ständigem Dialog mit den Netzbetreibern, um bei unserer Behörde das Gegenstück abbilden zu können. Um Bedenken eines nicht sachgerechten Vorgehens bei der Einführung der gesicherten elektronischen Schnittstelle zu begegnen, weise ich darauf hin, dass wir im Bayerischen Landeskriminalamt neben den technischen Bestrebungen auch organisatorische Maßnahmen getroffen haben. In meinem Sachgebiet installierte ich einen von der Leitungsfunktion gestärkten Monitoring-Verantwortlichen, der nicht auf Ebene der Sachbearbeitung tätig ist und losgelöst von meiner Führungsfunktion die Rechtmäßigkeit des Vorgehens prüft, sowie qualitätssichernde Maßnahmen ergreift. Dieser Monitoring-Sachbearbeiter oder -Verantwortliche steht in einem ständigen Dialog mit

den behördlichen Datenschutzbeauftragten, um auch hier dessen Belange eins zu eins berücksichtigen zu können.

Der Vollständigkeit halber weise ich noch darauf hin, dass wir einen Anpassungsbedarf sehen im Justizvollzugsentschädigungsgesetz (JVEG) und zwar in der Anlage 3 zum § 23. Hier ist bisher eine Kostenreduzierung von 20 % vorgesehen, wenn bestimmte Sachverhalte über zentrale Stellen angefordert oder angefragt und abgerechnet werden. Hiervon sind bisher die Kostenziffern 200 und 201 ausgenommen. Sollte die elektronische Schnittstelle in Betrieb genommen werden, sehen wir hier Nachbesserungsbedarf dahingehend, dass auch hier die 20 %-Regelung für uns zutreffen könnte. Ich bedanke mich bei Ihnen.

Vors. **Wolfgang Bosbach**: Wir danken Ihnen, Herr Wirth. Wir kommen jetzt zur Runde mit den Berichterstattern der Fraktionen. Ich darf darum bitten, die Fragen nicht nur zu formulieren, sondern auch mitzuteilen, an wen diese gerichtet werden. Es beginnt für die Fraktion der CDU/CSU der Kollege Schuster.

BE Armin Schuster (Weil am Rhein) (CDU/CSU): Vielen Dank, Herr Vorsitzender. Meine Herren Sachverständigen, herzlichen Dank für die wirklich prompte Lieferung. Wir versuchen, den Zeitplan einzuhalten, deswegen sind Sie auch etwas unter Druck geraten. Aber uns war diese Anhörung wichtig.

Ich möchte beginnen mit einer Frage an Herrn Wirth und weil das hier noch gar nicht zur Sprache kam. Sie können hier am besten etwas aus der Praxis schildern zum Thema PIN, PUK, dynamische IP-Adressen und Bestandsdaten. In welchen Fällen macht eine Polizeibehörde davon Gebrauch? Was sind das für Fälle und wie läuft es bei Ihnen ab? Welche Schlüsse können Sie aus diesen Daten ziehen, um dann Aufklärung zu betreiben?

Die weitere Frage: Wie sähe das bei Ihnen in der Praxis aus, wenn wir die Prozedur eines Richtervorbehaltes jetzt machen würden und was hätte das für Auswirkungen? Sie haben nur angedeutet, Sie würden überfrachtet mit Formvorschriften. Der Richtervorbehalt ist für mich etwas mehr als eine Formvorschrift, aber ich habe es verstanden. Mich würde interessieren, wie sich das bei Ihnen vor Ort auswirkt.

Meine weiteren Fragen gehen an Herrn Prof. Dr. Schwarz, zwei einfache Fragen, aber ich würde es gerne hören: Werden wir mit dem jetzt vorliegenden Gesetzentwurf die Vorgaben des BVerfG erfüllen? Noch konkreter: Werden wir in Karlsruhe erfolgreich sein, sollte es dort zu einer Prüfung kommen, angesichts dessen, was jetzt vorliegt?

Die zweite Frage an Sie, denn Sie haben das sehr schön formuliert – verfassungsrechtlich nicht geboten, aber es könnte politisch gewünscht sein. Wenn wir dem

politischen Wunsch nachkämen, welche Folgewirkungen sehen Sie dann hinsichtlich des Verschiebens verfassungsrechtlicher Maßstäbe, denn das Gericht hat uns dazu ja nicht aufgefordert? Was hat das für Folgewirkungen, wenn wir damit anfangen? Ist das unter Umständen auch so etwas wie ein „Dammbruch“, der dann auf den Praktiker, der links von Ihnen sitzt, wieder die Folgen haben könnte, die er schon beschrieben hat?

Vors. **Wolfgang Bosbach**: Herr Wirth, bitte.

SV **Ernst Wirth** (Kriminalrat, Bayerisches Landeskriminalamt, München): Drei Fragestellungen, einmal PIN, PUK und Anwendungsbeispiele. Ich wurde beim Hinflug über einen aktuellen Sachverhalt informiert, der sich über das Wochenende in Nordbayern zugetragen haben soll. Es wurde eine 33-jährige Frau erstochen in ihrer Wohnung aufgefunden, neben sich liegend war ihr nicht aktives Mobiltelefon. Es ist für die Ermittler von zentraler Bedeutung festzustellen, mit wem hat diese Frau als Letztes telefoniert und es ist zeitnah zu erheben oder zu realisieren die Aktivierung des Mobiltelefons. Dieses Mobiltelefon war gesichert mit PIN und PUK. Wir benötigen somit umgehend die Nummern PIN und PUK, um auf diese Mobiltelefone zugreifen zu können, um die letzten ein- oder abgehenden Gespräche erheben zu können. Das sind typische Anwendungsbeispiele.

Anwendungsbeispiele für IP-Adressen: Sie werden nahezu alle davon in Kenntnis gesetzt sein, dass vor 14 Tagen der FIS-Worldcup in Garmisch-Partenkirchen im alpinen Bereich ausgetragen wurde, und die Ski-Rennläuferin Tina Maze mit dem Tode bedroht wurde. In einem Internetforum hat ein bisher nicht identifizierter Täter mitgeteilt, er würde Tina Maze töten, nachdem sie ins Ziel einläuft. Wenn es nicht gelingt, dann wird er ihr die Knie mit einer Eisenstange zertrümmern, er führt eine Eisenstange bei sich. So war der Inhalt dieser Androhung. Es ist für uns erforderlich, hier sofort reagieren zu können, um die Person zu identifizieren, welche hinter dieser IP-Adresse des Absenders steht.

Zur letzten Frage, die Auswirkungen zum Richtervorbehalt: Wir sehen das grundsätzliche Problem, dass wir in der Umsetzung von Maßnahmen überfrachtet werden mit Anordnungsvorbehalten, die uns sehr viel Zeit kosten. Es stellt sich für mich die Frage bei Bestandsdaten, in welcher Form auch immer, ob ein Richtervorbehalt dieser Maßnahme aus praktischer Sicht gerecht wird. Ich sehe das mit großem Bedenken.

BE **Armin Schuster (Weil am Rhein)** (CDU/CSU): Können Sie etwas zu der Zahl der Fälle sagen, wie viele Fälle haben Sie?

SV **Ernst Wirth** (Kriminalrat, Bayerisches Landeskriminalamt, München): Wir können die Anzahl der Fälle nicht benennen. Es gibt Rauschgiftermittlungsverfahren, da wird

bei einem Mittäter ein Telefonbuch sichergestellt, dann ist es erforderlich, die in dem Notizbuch vorhandenen Daten zu klären. Fälle zu benennen ist schwierig, es geht immer um die Anzahl der Anfragen. Letztlich ist es ein Instrument der Ermittlung von Kontaktpersonen, das sich zu einem Standardinstrument entwickelt. Danke schön!

Vors. **Wolfgang Bosbach**: Herr Prof. Schwarz, bitte.

SV Professor Dr. Kyrill-Alexander Schwarz (Julius-Maximilians-Universität Würzburg): Herr Schuster, herzlichen Dank für die Frage. Was ich Ihnen nicht beantworten kann, ist, wie das BVerfG etwas entscheiden wird, das ist nur schwer möglich. Aber ich denke, was den Gesetzgeber mit dem hier vorliegenden Entwurf gelungen ist, dass die Vorgaben des BVerfG umgesetzt worden sind. Was darüber hinausgeht, ist etwas, was durch die Rechtsprechung nicht zwingend vorgezeichnet ist. Man kann darüber streiten, ob man sich am Rande dessen bewegt, was verfassungsrechtlich zulässig ist. Ich bin der Meinung, Sie sind auf der verfassungsrechtlich zulässigen Seite mit diesem Gesetzentwurf. Ich will allerdings auch darauf hinweisen, dass die zentrale Frage, über die wir hier sprechen, nämlich die Frage von Richtervorhalten und Benachrichtigungspflichten, jedenfalls dann an deutlichen Schwierigkeiten verliert, wenn man sich über eines im Klaren ist: Es muss sichergestellt sein, das ist aber auch unstreitig, dass unter dem Stichwort „Gebot effektiven Rechtsschutzes“ gegen die abschließende behördliche Maßnahme Rechtsschutz grundsätzlich, auch als ex-post-Rechtsschutz, möglich sein muss. Das setzt ggf. voraus, dass man sich über Benachrichtigungspflichten nach Maßgabe des jeweiligen Fachgesetzes und nach Maßgabe der jeweiligen Ermittlungsmaßnahmen dann auch Gedanken macht, wenn es dort vorgeschrieben ist. In der allgemeinen Ermächtigungsnorm des § 113 TKG ist das mitnichten erforderlich.

Zum zweiten Punkt: Wozu würde das verfassungsrechtlich führen, wenn man hier bei Maßnahmen dieser Eingriffsintensität generell Benachrichtigungspflichten und einen Richtervorbehalt einführen würde? Zum einen glaube ich, wenn man das überhaupt verfassungspolitisch machen möchte, differenzieren sollte nach den jeweiligen fachspezifischen Maßnahmen, um die es geht. Das heißt, das ist der richtige Regelungs-ort, um sich zu überlegen, ob wir Richtervorbehalt und Benachrichtigungspflichten brauchen. Ein genereller Richtervorbehalt und generelle Benachrichtigungspflichten halte ich für falsch. Es geht immer um die Frage: Was machen Sie mit den entsprechenden Maßnahmen? Dann muss es im Einzelfall ggf. auch erforderlich sein. Wozu führt das? Das ist, wenn ich es etwas überspitzt formuliere, weitaus mehr als vorauseilender Gehorsam gegenüber einer Rechtsprechung, die das nicht verlangt. Sie verschieben tatsächlich die Gewichte, weil Sie letzten Endes dann irgendwann in der Pflicht sein werden, auch politisch begründen zu müssen, warum haben Sie es nicht bei allen anderen sicherheitsrechtlichen Maßnahmen ebenfalls und warum bieten Sie nicht einen entsprechenden Schutz durch Verfahren. Dass das dann unter Umständen eine Bürde auch für die operierenden Behörden sein mag, das will ich

hier nur andeuten. Ich glaube, dazu würde Herr Wirth als Praktiker deutlich mehr sagen können.

Vors. **Wolfgang Bosbach**: Für die SPD-Fraktion Michael Hartmann bitte.

BE **Michael Hartmann (Wackernheim)** (SPD): Vielen Dank, Herr Vorsitzender. Auch von unserer Seite ein Dankeschön an die Sachverständigen. Eine Vorbemerkung: Wir sitzen ja jetzt nicht zusammen, weil wir nicht gewusst hätten, was wir an diesem winterlichen Märztag tun sollen, sondern weil uns das BVerfG noch einmal „Hausaufgaben“ mit auf den Weg gegeben hat. Es ist keineswegs so, dass wir in einem Bereich sind, den man so oder so sehen kann, sondern wir haben strenge und begründete Vorgaben und müssen versuchen, uns sehr genau an dem zu orientieren, was uns das BVerfG vorgegeben hat, um nicht erneut eine Pleite zu erleben. Gut finde ich bei allen Sachverständigen, dass Sie die grundsätzliche Erforderlichkeit nicht infrage gestellt haben. Wir brauchen dieses Gesetz, die Sicherheitsbehörden müssen arbeitsfähig sein und bleiben in einem Feld, das ganz wichtig ist und welches mit fortschreitender Technisierung auch immer heikler wird nach beiden Seiten hin. Was können die Behörden überhaupt noch effektiv erreichen und wie kann andererseits das, was uns an Bürgerrechten hoffentlich gemeinschaftlich wichtig ist, geschützt und gewahrt bleiben?

Vor diesem Hintergrund habe ich drei Fragen. Zunächst an Herrn Prof. Bäcker. Das Beispiel von Herrn Wirth war ja durchaus einleuchtend und eindrucksvoll. Aber geht es wirklich im Wesentlichen um solche Anwendungsbeispiele? Ist nicht vielmehr ein solcher Fall durchzudenken, dass ein Handy, das einer dritten Person gehört, bei einem lebenden Straftäter vorgefunden wird. Ein lebender Straftäter, der das Handy z. B. von Frau Gisela Piltz hat. Sie wollen im Interesse des Schutzes von Frau Piltz und vielleicht auch zur Aufklärung des Sachverhaltes versuchen, an PIN und PUK und andere Sicherungsdaten zu kommen. Ist das nicht ein typischerer Fall, wenn auch konstruiert?

Zum Zweiten: Wäre es dann nicht unbedingt erforderlich, dass die Betreffende, nennen wir sie auch hier Frau Gisela Piltz, auch darüber informiert wird, dass ihre Daten ausgelesen wurden und werden mussten? Da bin ich im Bereich der Benachrichtigungspflichten.

Ich bin der Überzeugung, dass wir dahinter auf keinen Fall zurückgehen können, dass das nicht einfach ein „nice to have“ ist, sondern eine unbedingte Erforderlichkeit.

Meine zweite Frage geht an Herrn Prof. Kugelmann und an Herrn Dr. Dix. Herr Dr. Dix und Herr Prof. Kugelmann, die Frage IPv6 ist wirklich eine höchst heikle, weil wir vieles noch nicht voraussehen können, wenn es denn wirklich so weit ist. Sie haben uns beide für diesen Punkt sensibilisiert, aber unterschiedliche Antworten gefunden.

Die eine Antwort war: Befristet und evaluiert dann. Die andere Antwort war: Zieht Sicherungen jetzt schon ein, so gut wie möglich. Das müssten wir unbedingt zusammenbekommen. Da wir bestimmte Entwicklungen noch nicht absehen können, die Entwicklung aber in die Grundrichtung gehen wird, so viel wissen wir heute, müssen wir versuchen, auch da schon eine entsprechende Begrenzung vorzusehen. Wie könnte die aussehen? Ist es tatsächlich nur die Evaluierung, die Befristung, oder wo könnte wirklich ein gemeinsamer Standard gefunden werden?

Ein weiterer Punkt, den ich gerne noch einmal an Herrn Schaar richte: Sie haben für mich nachvollziehbar die Frage gestellt: Abfrage, aber zu welchem Zweck? Dann waren wir bei dem Beispiel der Ordnungswidrigkeiten, das uns auch Bauchschmerzen bereitet, denn vieles ist Ordnungswidrigkeit. Welchen Vorschlag können Sie aus Ihrer Fachsicht unterbreiten? Gibt es wirklich die Möglichkeit, einen abschließenden Katalog zu erstellen, um dann alles erfasst zu haben? Geht das und wo fängt man an? Ordnungswidrigkeit ist auch das Überfahren einer roten Ampel. Wo hört man auf? Ordnungswidrigkeiten mit gravierender Auswirkung sind z. B. im Bereich der Wirtschaftskriminalität statuiert. Ich würde bitten, das von Ihnen noch ein bisschen konkreter als Hilfe für unsere weiteren Beratungen zu bekommen. Vielleicht können auch Sie, Herr Prof. Kugelman, zu der Frage noch etwas sagen. Danke sehr!

Vors. **Wolfgang Bosbach**: Herr Prof. Bäcker, bitte.

SV **Prof. Dr. Matthias Bäcker** (Universität Mannheim): Wenn Sie mich fragen, was ein praktisch typischer Anwendungsfall ist, bringen Sie mich natürlich auf Glatteis, weil ich mich als Wissenschaftler immer dem Vorwurf aussetze, dass ich davon ja keine Ahnung habe. Mit dieser Vorrede würde ich sagen, wenn Sie typische Anwendungsfälle für die Bestandsdatenabfrage suchen, dann müssen Sie danach differenzieren, welche Behörde im Rahmen von welchem Rechtsregime solche Abrufe vornimmt. Es macht einen Unterschied, ob das nach der Strafprozessordnung oder nach einem Landespolizeigesetz oder nach einem der bundesrechtlichen Sicherheitsgesetze geschieht, die im Entwurf behandelt werden. Man kann sicher fragen, ob im Bereich des Strafprozesses der typische Fall wirklich der ist, dass das Mobiltelefon des Opfers eines Tötungsdelikts entsperrt und ausgewertet werden soll, oder ob es insbesondere bei der Abfrage von IP-Adressen vielleicht doch etwas um bagatellarische Kriminalität geht. Was an den Angaben von Herrn Wirth nicht ganz zusammenpasst, ist dass er einerseits sagt, hier entwickle sich ein neues Standardinstrument der Strafverfolgungsbehörden, andererseits aber ein Tötungsdelikt als typischen Anwendungsfall darstellt. Nach meinem Kenntnisstand sind Tötungsdelikte nicht so häufig, dass man sie als typische Beispiele ansehen könnte. Bei § 7 BKA-Gesetz wird man jedenfalls von ganz anderen Anwendungsfällen ausgehen müssen, auch von ganz anderen als denen, die in der Entwurfsbegründung stehen. In der Entwurfsbegründung werden als einschlägige Fälle eine

Suizidankündigung oder eine Drohung mit einem Amoklauf genannt. Da muss man klar sagen: Suizide zu verhindern, ist nicht Aufgabe des BKA. Amokläufe sind nur ein recht randständiger Bereich der Aufgabe des BKA. Bei der Zentralstellen-tätigkeit, zu der § 7 BKA-Gesetz gehört, geht es vielmehr darum, kriminalstrategisch Beziehungsgeflechte zu analysieren, und zwar zu einem Zeitpunkt, wo man nur relativ vage Vorstellungen davon hat, was man eigentlich sucht. Da geht es darum, gefährliche Strukturen herauszuarbeiten, denen man sich dann in einer recht breit angelegten kriminalstrategischen Überwachung nähern möchte. Das wäre meiner Ansicht nach ein typischer Anwendungsfall von § 7. Mit dem, was das Bundesverfassungsgericht zu beurteilen hatte – Abwehr einer konkreten Gefahr, Verfolgung einer konkreten Straftat – hat das nicht viel zu tun. Aus meiner Sicht ist es ein zentraler Punkt, über den ich Sie als Parlamentarier auch gerne bösgläubig machen möchte, dass das Gesetz hier nicht nur fortschreibt, was die bisherige Rechtslage ist, sondern dass dieses Gesetz die Möglichkeit der Bestandsdatenauskunft gegen-über dem, was wir bisher haben, ganz weitgehend erweitern wird.

Eine Benachrichtigungspflicht bei der Abfrage von PIN und PUK – ich habe es bereits gesagt – ist verfassungsrechtlich geboten. Bei der Zuordnung von IP-Adres-sen habe ich ein bisschen Bauchschmerzen, eine Benachrichtigungspflicht all-gemein als verfassungsrechtliches Gebot anzusehen. Ich halte sie aber für allemal sinnvoll und ich bin ganz bei meinen Kollegen, die sagen: Irgendeine Rechtsschutz-möglichkeit, die auch faktisch wahrnehmbar ist, muss jedenfalls bestehen. Vielen Dank!

Vors. **Wolfgang Bosbach**: Wir danken Ihnen. Ich weiß nicht, ob ich der Einzige bin, aber ich habe Herrn Wirth jedenfalls nicht so verstanden, dass er den von ihm geschilderten Fall als typischen Fall der Alltagskriminalität betrachtet, sondern dass es ein aktueller Fall ist, der erst auf der Hinfahrt an ihn herangetragen worden ist und dass es für die Aufklärung und Überführung des Täters von überragender Bedeutung ist, dass rasch Erkenntnisse gewonnen werden und vielleicht auch mithilfe des dann geöffneten Handys zu sehen, welche Anrufe getätigt worden sind. So habe ich ihn jedenfalls verstanden. Herr Prof. Dr. Kugelmann, bitte.

SV **Prof. Dr. Dieter Kugelmann** (Deutsche Hochschule der Polizei, Münster): Das „Doppeltürmodell“ lässt Spielräume bei der zweiten Tür. Deshalb hatten wir dahingehend überlegt, Richtervorbehalte und Mitteilungspflichten auf der Abruf-ebene, also in den Fachgesetzen zu verankern, d. h. aber auch, dass man dort durchaus differenzieren kann, was auch die Zwecke der Abrufe bedeutet. Man muss durchaus auf das konkrete Gesetz gucken – und ich stimme dem Kollegen Bäcker vollkommen zu, die Zentralstellen sind da durchaus der problematischere Fall, während sich beim BKA-Gesetz die Bekämpfung des internationalen Terrorismus und dazu eine Abfrage ohne Weiteres vertreten lässt. Es heißt aber nicht, dass in beiden Vorschriften zwingend identische Voraussetzungen errichtet werden

müssen. Ich weise daraufhin, dass auch die Landesgesetzgeber aktiv sind, weil in den Polizeigesetzen der Länder auch die entsprechenden Abfrageregulungen dementsprechend geändert werden müssen. Zum Beispiel der erste Entwurf aus Schleswig-Holstein sieht sowohl einen Richtervorbehalt wie eine Mitteilungspflicht in den zwei von mir angesprochenen Fällen, die er enthält, vor und er stellt auch IPv6 den dynamischen Internetprotokollen gleich. Das ist letztlich auch von Bedeutung unter dem Gesichtspunkt der Technikoffenheit. Das Bundesverfassungsgericht hat diese Technikoffenheit in einem Urteil mit drin. Es ist jedenfalls bei künftigen Techniken das Recht auf informationelle Selbstbestimmung betroffen. Wir agieren natürlich nicht im grundrechtsfreien Raum, wir müssen uns nur überlegen, was wir dann damit machen und da würde ich das, Herr Hartmann, in einer Zeit der Unsicherheit im Handeln und der Unsicherheit, die dem Gesetzgeber dann im gewissen Maße obliegt, ein bisschen zusammenführen. Ich würde tendenziell bundesrechtspolitisch die strengere Regelung erst einmal einführen, d. h. dass gerade dann Evaluationspflichten, wie sie gefordert sind, sinnvoll sind und dann nach zwei, drei Jahren fragen: Ist das sinnvoll, ist die Technik gelaufen? Oder ist es vielleicht möglich, das an der und der Stelle zu lockern? Ich würde aber von der strengeren allenfalls hin zur weniger strengen Regelung tendieren. Der gemeinsame Standard, den man hätte, wäre ein hoher Standard angesichts der gesicherten Technik, mit der Option, das durch Sunshine-Clauses, durch Evaluationen entsprechend zu modifizieren, denn – auch da gebe ich den Kollegen Recht – wir sind mit dieser Regelung hier zur Bestandsdatenauskunft im Bereich informatorischer Eingriffe in Grundrechte. Der Staat nutzt die Informationstechnik, um Zugriff auf Daten zu bekommen, und hier braucht er Telekommunikationsdienstleister und nutzt die auch noch mit, die für ihn die Daten erheben, die er dann kriegt. Das ist eine Gesamt-tendenz, dass wir zusehends schwierige Tatbestandsmerkmale fassen können müssen; zusehends schwieriger jenseits der Zwecke, auch die konkreten tatbestandlichen Voraussetzungen eng fassen können; zusehends eine weniger konkrete Gefahr als Anforderungen in den Vorschriften alleine haben, in das Gefahrenvorfeld vorverlagern. Deshalb würde ich es in der Gesamttendenz auch für sinnvoll erachten, gerade deshalb die verfahrensrechtlichen Vorkehrungen eher auszubauen als abzubauen, weil wir die materiellen Vorkehrungen alleine ganz schwer so konkret fassen können, so dass wir die Sicherheitsbedürfnisse nicht verraten. Vielen Dank!

Vors. **Wolfgang Bosbach**: Vielen Dank! Jetzt kommt Herr Dr. Dix und danach Herr Schaar.

SV **Dr. Alexander Dix, LL.M.** (Berliner Beauftragter für Datenschutz und Informationsfreiheit, Berlin): Herr Hartmann, ich würde Herrn Prof. Dr. Kugelman völlig darin zustimmen, dass man die Probleme, die durch die Einführung von IPv6 entstehen, schon jetzt durch verfahrensrechtliche Sicherungen abfangen sollte. Ich bin dezidiert der Auffassung, dass sowohl ein Richtervorbehalt als auch nach-

trägliche Benachrichtigungspflichten schon jetzt geboten sind, aber ich würde zusätzlich für die Einführung einer Evaluation sowohl für den § 112 TKG, der bisher gar nicht im Gesetzentwurf enthalten ist, als auch für den § 113 TKG plädieren – ich würde beide Forderungen aufrecht erhalten und gestatten Sie mir noch eine Bemerkung zur Frage der Einschränkung der Erhebungsbefugnisse in den Fachgesetzen, also bei der zweiten Tür: Da könnte man sich vorstellen, dass auch die Nachrichtendienste und das BKA unbegrenzt den Zugriff auf IP-Adressen nur erhalten, indem die Vorschriften zu besonderen Formen der Datenerhebung im Bundesverfassungsschutzgesetz und auch im BKA-Gesetz auf die Aufdeckung von IP-Adressen erstreckt werden.

Vors. **Wolfgang Bosbach**: Danke! Herr Schaar, bitte.

SV **Peter Schaar** (Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Bonn/Berlin): Vielen Dank! Die Forderung, die Zugriffe jedenfalls, hinsichtlich der Zuordnungsdaten zu den IP-Adressen auf Ordnungswidrigkeiten von besonderer Schwere zu beschränken, ist vom Bundesverfassungsgericht selbst formuliert worden und zwar in der Vorratsdatenspeicherungsentscheidung in Randnummer 262. Dort sagt das Gericht, dass es sich auch hier um im Einzelfall besonders gewichtige Ordnungswidrigkeiten handeln muss, die der Gesetzgeber zudem ausdrücklich benennen muss. Der sauberste Weg wäre, in den jeweiligen Fachgesetzen eine entsprechende Differenzierung vorzunehmen. Ich sehe das quasi als geboten an. Allerdings bin ich mir bewusst, dass das eine ziemlich anspruchsvolle und aufwendige Aufgabe wäre, weil eine Vielzahl von Fachgesetzen angefasst werden müsste und dementsprechend zu überlegen wäre, ob man einen entsprechenden Hinweis – allerdings spezifiziert auf die entsprechenden Sachverhalte – an zentraler Stelle, möglicherweise auch im Telekommunikationsgesetz oder in der Strafprozessordnung, vornimmt. Die Kriterien, die man anlegen kann, sind vermutlich die gleichen wie bei der Differenzierung von Straftaten. Da gibt es verschiedene Anknüpfungspunkte. Ein Anknüpfungspunkt ist sicherlich die Höhe des Bußgeldrahmens, der hier vorgesehen ist, aber gleichwohl – das muss man sich noch einmal sehr genau anschauen, inwieweit das hier tatsächlich übertragbar ist. Der Aspekt der wiederholten Verstöße könnte ebenfalls ein Kriterium sein. Allerdings scheue ich mich hier, Ihnen das als fertige Lösung vorzuschlagen.

Vors. **Wolfgang Bosbach**: Frau Kollegin Piltz von der FDP erhält jetzt die Gelegenheit, einen Fall zu bilden, bei dem der Kollege Hartmann dringend tatverdächtig ist.

BE **Gisela Piltz** (FDP): Herr Vorsitzender, meine Herren Sachverständigen, auch im Namen meiner Fraktion herzlichen Dank dafür, dass Sie versuchen, mit uns gemeinsam dieses Gesetz besser zu machen. Das ist jedenfalls das Ziel, das wir

haben. Wir sind auch schon ein Stück weiter vorangekommen und zu Beginn möchte ich sagen, Herr Kollege Hartmann, ich bin weder Täterin noch Opfer einer Straftat. Im Hinblick auf das Beispiel: Wir sind hier nicht vor Gericht und nicht bei der Staatsanwaltschaft in der rechtsstaatlichen Vorlesung. Ich habe allerdings noch meine Zweifel am Beispiel in diesem konkreten Zusammenhang, weil es sich um eine Tote handelt und insofern möglicherweise nicht um eine heimliche Abfrage; aber das ist bei Beispielen so, mal passen sie und mal passen sie nicht. Was Sie uns sagen wollten, haben wir, glaube ich, verstanden, aber dennoch habe ich da meine Zweifel. Ich möchte nur für das Protokoll sagen: Herr Hartmann, Sie wollten mich hier keiner Straftat verdächtigen. Es gibt mehrere zentrale Punkte, um die es hier heute geht. Es geht um die Frage der Benachrichtigungspflichten, wie, wo, warum und an welcher Stelle. Bis auf zwei Sachverständige – das habe ich jetzt gelernt – sind alle anderen der Auffassung, dass man Benachrichtigungspflichten braucht, insbesondere bei den dynamischen IPs, PINs, PUKs und Passwörtern. Manche gehen sogar darüber hinaus. Die Frage, die wir uns stellen müssen, ist, wie man mit dieser technischen Frage umgeht. Deshalb meine Frage an die Sachverständigen Prof. Dr. Bäcker, Prof. Dr. Kugelmann und Herrn Achelpöhler: Können Sie uns einen Rat geben, wie eine Norm mit Abfragebefugnis, z. B. im BKA-Gesetz, aussehen könnte, durch die die Benachrichtigungspflichten dann wenigstens den nachträglichen Rechtsschutz sichern oder garantieren könnten? Meine weitere Frage in diesem Zusammenhang geht an Herrn Prof. Dr. Bäcker: Das Bundesverfassungsgericht hat in seiner Entscheidung darauf hingewiesen, dass die polizeilichen Generalklauseln eigentlich zu weit gehen, um darauf die Abfrage von Bestandsdaten zu stützen. Wenn ich das richtig sehe, ist es im Entwurf der Bundesregierung die vorgelegte Befugnisnorm für die Abfrage durch die Sicherheitsbehörden. Er liest sich eigentlich wie duplizierte Generalklauseln. Halten Sie das mit dem Tenor des Bundesverfassungsgerichts für vereinbar? Wenn nicht, wo könnten wir es noch konkretisieren, so dass es besser wird? Der zweite Bereich, mit dem wir uns beschäftigen, ist die Frage des Richtervorbehalts. Auch da teilt die Mehrzahl der Sachverständigen meine persönliche Auffassung: Es wäre klug, wenn wir das immer hätten. Dabei sagen die meisten aber, dass kein doppelter Richtervorbehalt erforderlich sei. Daher meine Fragen an Prof. Dr. Bäcker und Prof. Dr. Kugelmann: Wäre die Verankerung eines subsidiären Richtervorbehaltes bei der Abfrage von PINs, PUKs und Passwörtern in den jeweiligen Abfragebefugnisnormen klar möglich? Wäre es an dieser Stelle ausreichend, dies nur für Fälle vorzusehen, in denen die Maßnahme ohne Wissen und Kenntnis des Betroffenen geschieht oder ist ein Richtervorbehalt auch in den Fällen nötig, in denen etwa eine offene Sicherstellung bei Anwesenheit des Betroffenen erfolgt. Das sind durchaus unterschiedliche Sachverhalte, die man vielleicht unterschiedlich regeln möchte. Das würde ich gerne wissen. Können Sie uns da einen Rat mit auf den Weg geben? Es ist ja eine Sache, – und ich glaube, das ist auch unumstritten – das wir überlegen müssen, was sozusagen nach dem Urteil des Bundes-

verfassungsgerichts geboten ist, aber es ist auch immer eine Frage, was für uns rechtsstaatlich geboten ist und das kann durchaus auch ein Unterschied sein.

Vors. **Wolfgang Bosbach**: Herr Achelpöhler, bitte.

SV **Wilhelm Achelpöhler** (Rechtsanwalt, Münster): Zum Richtervorbehalt: Ich meine, dass verfassungsrechtlich kein Richtervorbehalt gegeben ist. Da bewegen wir uns im Bereich des Politischen. Der Kollege Schwarz hat darauf hingewiesen, dass es andere Maßnahmen mit einer deutlich höheren Eingriffsintensität gibt, z. B. die Rasterfahndung. Da gibt es verfassungsrechtlich keine Form des Richtervorbehalts. Das kann man auch ohne Richtervorbehalt machen. Da gibt es dann die entsprechenden Benachrichtigungspflichten und diese Benachrichtigungspflichten wären aus meiner Sicht das, was hier das Mittel der Wahl ist. Auf der anderen Seite gibt es immer dann die Bedenken der Praktiker, die sagen, dass das ein Aufwand ist. Diesen Aufwand wollen wir doch vermeiden. Das muss doch praktisch sein. Das Bundesverfassungsgericht hat in der Entscheidung, über die wir hier die ganze Zeit reden, auf den freiheitssichernden Charakter dieses Aufwands hingewiesen, denn das Bundesverfassungsgericht hat gesagt, dass diese manuelle Abfrage immer einen gewissen Verfahrensaufwand verursacht, der dazu beitragen dürfte, dass die Behörde nur die Auskunft bei hinreichendem Bedarf einholt. Der Aufwand ist für den Praktiker bei der Polizei und den Sicherheitsbehörden ein Nachteil, für den Bürger hat es einen freiheitssichernden Aspekt. Wenn wir dann sehen, dass wir mit der Möglichkeit der elektronischen Schnittstelle alles dafür tun, diesen Aufwand zu reduzieren, dann würde ich sagen, ist ein Äquivalent zu diesem reduzierten Aufwand die entsprechende Benachrichtigungspflicht. Diese kann man ganz einfach den entsprechenden Regelungen der Länder im Polizeirecht entnehmen, die eben auch bei bestimmten Maßnahmen, wie z. B. der polizeilichen Rasterfahndung, die Information der Betroffenen nach Durchführung der Maßnahme vorsieht, soweit der Zweck der Maßnahme dadurch nicht gefährdet wird. Das ist eine Benachrichtigungspflicht, die aus meiner Sicht hier ohne Weiteres eingeführt werden könnte und auch letztlich sinnvoll wäre.

Vors. **Wolfgang Bosbach**: Danke! Herr Prof. Dr. Kugelmann, bitte.

SV **Professor Dr. Dieter Kugelmann** (Deutsche Hochschule der Polizei, Münster): Zunächst zur Benachrichtigungspflicht im Bundeskriminalamt-Gesetz: Vielleicht wäre es gesetzestechnisch eine Idee, an die vorhandenen Vorschriften des BKA-G anzuknüpfen. Da gibt es in § 20a) bis w) BKA-G – Terrorismusbekämpfung – viele Vorbilder. Das würde genau in den Bereich „besondere schwere Eingriffe in das Recht auf informationelle Selbstbestimmung und ähnliche Grundrechte“ passen. Die Regelungsmodelle könnte man da auch übernehmen, ggf. durch einen Verweis. Das würde für den § 20b BKA-G am einfachsten gehen, weil er schon als Mittel der Datenerhebung enthalten ist. Eine gewisse Schwierigkeit ist da vielleicht der § 7

BKA-G, den Kollege Bäcker schon zu Recht angemahnt hat. In der Zentralstellenfunktion des Bundeskriminalamts, also in der Auswertung der überwiegend aus den Ländern stammenden Daten, die man zusammenfasst und ggf. anreichert, müsste man in der Tat vielleicht einen Extrapassus mit hineinnehmen. Ich weiß nicht, ob da ein bloßer Verweis auf eine Buchstabenvorschrift genau passen würde. Da müsste man noch einmal genauer drauf gucken. Das kann ich Ihnen leider jetzt nicht abschließend in die Feder diktieren. Gleiches gilt für den Richtervorbehalt. Die Frage des Richtervorbehaltes ist insbesondere dann von Relevanz, wenn heimlich Eingriffe vorliegen. Sie haben es zu Recht angedeutet. Das ist auch der Grund, weshalb es bei Art. 10 GG beim Eingriff aus grundrechtssystematischen Erwägungen zum Richtervorbehalt kommt, wenn Art. 10 eben Eingriffe auf dynamische IP-Zuordnung zulässt, dann ist es für mich relativ zwingend ein Richtervorbehalt, wie man ihn ausgestaltet. Beim Bundesamt für Verfassungsschutz ist eine Einführung eines § 8d BVerfSchG geplant. Da gibt es ja schon einen § 8b BVerfSchG und da steht eben nicht Richtervorbehalt drin, sondern vorbeugende Kontrolle durch die G10-Kommission. Da ist der Vorteil der Differenzierung in den Fachgesetzen, dass man darauf abheben kann, also bei dem Richtervorbehalt in den weiteren Maßnahmen im Zusammenhang besonderer Mittel der Datenerhebung. Es ist nun mal nicht so, dass es keine Richtervorbehalte gibt, sondern es bei besonders schweren Telekommunikationsüberwachungen, natürlich aber auch in Art. 13 GG, das schon alles gibt. Da gibt es auch den 24-Stunden-Notdienst oder notfalls die Möglichkeiten, unverzüglich die richterlichen Entscheidungen nachzuholen. Ich sehe da keine rechtsstaatliche, nicht verkraftbare Beeinträchtigung der Handlungsfähigkeit und ich würde auf diese Vorbilder entsprechend dann abheben, um diese dort in den entsprechenden Vorschriften einzufügen.

Vors. **Wolfgang Bosbach**: Vielen Dank! Herr Prof. Dr. Bäcker.

SV **Professor Dr. Matthias Bäcker** (Universität Mannheim): Sie haben mich nach der generalklauselartigen Weite der Abfragevorschriften gefragt. Ich glaube, hier muss man zwei Punkte differenzieren: Das Bundesverfassungsgericht hat jedenfalls für die Zuordnung von IP-Adressen eine Abfragevorschrift verlangt, die spezifisch darauf zugeschnitten ist. Eine solche Norm muss also die Zuordnung einer IP-Adresse unter bestimmten Voraussetzungen erlauben. Wir haben damit gegenüber der polizeilichen Generalklausel jedenfalls den Fortschritt erzielt, dass es eine besondere Regelung gibt, die das betreffende Ermittlungsinstrument erst einmal beschreibt. Eine andere Frage ist, an welche Voraussetzungen der Datenabruf geknüpft wird. Ich glaube nicht, dass man von Verfassung wegen für den Bestandsdatenabruf im Strafverfahren generell höhere Voraussetzungen braucht als den Anfangsverdacht einer Straftat. Im Polizeibereich ist die konkrete Gefahr als noch hinnehmbare Zugriffsvoraussetzung anerkannt worden. Das Problem bei den präventivpolizeilichen Regelungen des Entwurfs ist aber, dass sie hinsichtlich des Eingriffstatbestands sogar noch über die polizeiliche Generalklausel hinausgehen,

indem sie Eingriffe im Vorfeld der konkreten Gefahr zulassen. Das ist ein neues Problem, das dieser Entwurf mit sich bringt und wo er zumindest sehr heikel wird.

Was das Erfordernis und die Gestaltung von Richtervorbehalt und Benachrichtigungspflicht angeht, kann man die Erörterungen ein wenig systematisieren, wenn man sich den Zweck dieser Vorkehrungen und das Wechselwirkungsverhältnis zwischen ihnen anschaut. Sowohl die Benachrichtigungspflicht als auch der Richtervorbehalt kompensieren zunächst einmal Heimlichkeit von Ermittlungsmaßnahmen. Heimlichkeit bedeutet, dass der Betroffene im Vorhinein nichts gegen die Maßnahme machen kann, weil er nichts davon weiß, möglicherweise nachher auch nicht. Darum soll er benachrichtigt werden, um nachträglich Rechtsbehelfe einlegen zu können, und ein Richtervorbehalt soll gewährleisten, dass die Belange des Betroffenen schon vor der Maßnahme im Verfahren berücksichtigt werden. Der Richtervorbehalt erfasst noch eine weitere Fallgruppe, für die die Benachrichtigungspflicht nicht relevant ist, nämlich überraschende Maßnahmen. Der klassische Fall ist die Wohnungsdurchsuchung. Die Wohnungsdurchsuchung als solche erfolgt nicht heimlich, Sie können sich trotzdem vorher nicht dagegen wehren, weil Sie vorher nichts davon wissen, und wenn Sie dann von der Wohnungsdurchsuchung erfahren, in dem Moment, wo die Polizei im Haus steht, können Sie keinen Rechtsschutz mehr erlangen. In den Fällen heimlicher Maßnahmen besteht nun ein gewisses Wechselwirkungsverhältnis zwischen Benachrichtigung und Richtervorbehalt, zumindest dann, wenn es sich um einen Eingriff minderer Intensität handelt. Ich glaube, dass es dann trotz der Heimlichkeit ausreicht, eines der beiden Instrumente vorzusehen. Das ist aus meiner Sicht der Fall bei der Zuordnung der IP-Adresse, nicht bei dem Abruf von Zugangsdaten, weil das ein Eingriff von recht erheblichem Gewicht ist, wo meiner Ansicht nach beides geboten ist. Herr Kugelmann hat völlig zu Recht darauf hingewiesen, dass die Lähmung der Praxis durch Richtervorbehalte mit der hoffentlich inzwischen flächendeckenden Einführung des auch verfassungsrechtlich gebotenen richterlichen Eilendienstes ein beherrschbares Problem sein sollte.

Letzter Punkt: Wie gestaltet man die verfahrensrechtlichen Sicherungen sinnvoll aus? Hier muss man auf eine Besonderheit Rücksicht nehmen, die sowohl bei der IP-Zuordnung als auch bei der Erhebung der Zugangsdaten besteht. Das sind Maßnahmen, die auf weitere Ermittlungsmaßnahmen bezogen sind. Die IP-Zuordnung dient dazu, Daten einer bestimmten Person zuzuordnen, die schon durch eine andere Maßnahme bekannt geworden sind. Der Abruf von Zugangsdaten soll Daten entschlüsseln, die man schon hat, oder den Zugriff auf Daten vorbereiten, die man noch erlangen möchte, z. B. in dem Fall des aufgefundenen Mobiltelefons. Wenn jetzt eine Benachrichtigungspflicht und ein Richtervorbehalt schon für die jeweilige andere Maßnahme besteht – z. B. wenn das Mobiltelefon im Rahmen einer Hausdurchsuchung erlangt wird, für die ohnehin ein Richtervorbehalt besteht –, dann ist es aus meiner Sicht entbehrlich, einen weiteren Richtervorbehalt

für die Datenzuordnung vorzusehen. Insofern bietet sich an, eine Subsidiaritätsklausel in die jeweiligen Regelungen aufzunehmen. Wo dagegen für die Bezugsmaßnahme keine Sicherungen bestehen, sollte der Richtervorbehalt bzw. die Benachrichtigungspflicht wenigstens bei der Zuordnungsmaßnahme aufleben.

Ich würde an der Stelle gerne noch einen Punkt betonen, der insbesondere für die Zuordnung von IP-Adressen relevant ist, wo bestimmte Kommunikationsdaten auf eine bestimmte Person bezogen werden. Da stehen wir im Moment gerade im Strafprozess vor dem Problem, dass die Erlangung dieser Kommunikationsdaten völlig unzureichend weil unspezifisch geregelt ist. Die Erlangung von komplexen Datenbeständen, die bei Unternehmen vorhanden sind, wird im Wesentlichen auf die Ermittlungsgeneralklausel des § 161 StPO gestützt, garniert mit einer angeordneten Hausdurchsuchung. Diese Norm soll dann auch decken, dass ein Unternehmen seine eigenen Datenbestände nach kriminalistischen Kriterien durchforstet und danach die Treffer an die Strafverfolgungsbehörden auswirft. Das ist funktional so etwas ähnliches wie die Rasterfahndung, nur dass es sich gesetzes-technisch nicht um eine Rasterfahndung handelt, weshalb die Maßnahme auf völlig unspezifische und tatbestandlich sehr weit gefasste Regelungen gestützt wird. Dieses Problem ist nicht unmittelbar Gegenstand dieses Entwurfs. Aber das Bedürfnis, wenigstens die Zuordnung der IP-Adresse prozedural abzusichern, entsteht ganz wesentlich daraus, dass wir im vorgelagerten Schritt der Datenerlangung bei Unternehmen keine hinreichenden Schutzvorkehrungen haben. Vielen Dank!

Vors. **Wolfgang Bosbach**: Wir danken Ihnen! Für die Fraktion DIE LINKE. hat jetzt der Kollege Korte das Wort.

BE **Jan Korte** (DIE LINKE.): Schönen Dank, Herr Vorsitzender! Vielleicht nur soviel: Der Kollege Schuster hat eingangs gefragt, ob wir mit dem Gesetz erfolgreich sein werden. Das Problem bei diesen ganzen Gesetzesvorhaben, gerade im Bereich der Innenpolitik, ist, dass Sie meistens nicht erfolgreich gewesen sind, weswegen wir ja ständig etwas Neues machen müssen, weil das Bundesverfassungsgericht gesagt hat, dass das so nicht geht. Deswegen sollte man es in Zukunft vielleicht gar nicht so weit kommen lassen, sondern gleich grundrechtserfolgreiche Gesetze vorlegen. Ganz konkret hätte ich drei Fragen. Zum einen an Herrn Schaar und Herrn Dr. Dix: Sie haben eben die Frage nach der Verfolgung von Ordnungswidrigkeiten erwähnt. Wäre es nicht eigentlich, wenn wir uns nicht nur im Grenzbereich des verfassungsmäßig Zulässigen bewegen wollen, per se eine Überlegung, diese grundsätzlich auszuschließen? Solche massiven Eingriffe dürfen nicht zur Verfolgung von Ordnungswidrigkeiten angewandt werden. Das wäre die erste Frage. Die zweite Frage an Herrn Achelpöhl: Sie haben in Ihrer Stellungnahme folgendes pointiert beschrieben. Das Bundesverfassungsgericht hielt die in § 113 Abs. 1 Satz 1 TKG normierten Schwellen der Übermittlungsbefugnis für „ver-

fassungsrechtlich noch hinnehmbar.“ Und dann – und das ist, glaube ich, das Entscheidende, was wir diskutieren: Der Gesetzentwurf senkt sie mit seiner Anknüpfung an die Aufgaben der Sicherheitsbehörden weiter ab, indem auch die „Gefahrenvorsorge“ eine Datenübermittlung rechtfertigt. Das ist eigentlich das zentrale Problem, was wir diskutieren. Vielleicht dazu noch etwas ausführlicher Ihre Einschätzung. Die letzte Frage richtet sich an den Kollegen Wirth. Ich kann logischerweise voll nachvollziehen, dass man als Kriminalbeamter des LKA im Allgemeinen und als bayerischer LKA-Beamter im Speziellen möglichst viele Befugnisse haben möchte und möglichst viele Auflagen haben möchte, aber bei dem Stichwort Richtervorbehalt, was Sie angesprochen haben, glaube ich, dass es eher umgekehrt ist. Erstens haben wir eine Personalunteraustattung, gerade in der Frage von Richtervorbehalten. Die kommen gar nicht hinterher, das alles abzuarbeiten und wenn, dann wird es ja fließbandartig abgearbeitet und ich finde, das sollte eigentlich mehr Zeit kosten und nicht weniger Zeit. Das zumindest noch als eine Frage getarnte Erwiderung.

Vors. **Wolfgang Bosbach**: Vielen Dank! Herr Schaar, bitte.

SV **Peter Schaar** (Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Bonn/Berlin): Herr Korte, ich würde nicht so weit gehen, hier Ordnungswidrigkeiten generell auszunehmen. Zum einen sind wir als Datenschützer auch für die Verfolgung von Ordnungswidrigkeiten im Datenschutzrecht zuständig. Wir [Anm.: der BfDI] müssen das zwar über die Bundesnetzagentur machen, jedenfalls die Datenschutzbehörden der Länder sind selber Bußgeldbehörden. Es kann dabei durchaus um gravierende Fälle gehen, die nur entsprechend nachzuvollziehen sind, wenn man weiß, von welcher Stelle z. B. ein Telefonanruf ausgegangen ist oder wer da ggf. bestimmte Informationen missbraucht hat. Ich würde es insofern nicht generell ausschließen. Allerdings denke ich schon, dass man hier Erheblichkeitsschwellen definieren sollte, wie das vom Bundesverfassungsgericht auch gefordert worden ist.

Vors. **Wolfgang Bosbach**: Danke! Herr Dr. Dix, bitte.

SV **Dr. Alexander Dix, LL.M.** (Berliner Beauftragter für Datenschutz und Informationsfreiheit, Berlin): Ich teile die Auffassung, die Herr Schaar geäußert hat. Ich würde aber schon sagen, wie ich es auch in meiner schriftlichen Stellungnahme gesagt habe, dass der Gesetzgeber durchaus die Option hat, bei der Verfolgung vom Verwaltungsunrecht, – und darum geht es ja bei Ordnungswidrigkeiten – zumindest die Aufdeckung von IP-Adressen für unzulässig zu erklären. Die Option hat der Gesetzgeber. Eine andere Möglichkeit wäre dann, enumerativ tatsächlich bestimmte besonders schwere Ordnungswidrigkeiten zu benennen.

Vors. **Wolfgang Bosbach**: Vielen Dank! Herr Achelpöhler, bitte.

SV Wilhelm Achelpöbler (Rechtsanwalt, Münster): Zu der Frage der Gefahrenvorsorge, den Eingriffsbefugnissen, die auch Bestandteil des Gesetzentwurfs sind, waren in der alten Fassung im § 113 TKG enthalten. Jetzt wird das entsprechend aufgegliedert. Da hat das Bundesverfassungsgericht ausdrücklich darauf hingewiesen, dass der Gesetzgeber wörtlich § 177 Randnummer [...]. Der Gesetzgeber hat die Gefahrenvorsorge gerade nicht einbezogen und stellt dann im Weiteren dar, dass seinerzeit nach der damaligen Fassung das Erfordernis einer konkreten Gefahr gegeben sei und dekliniert dann diese materiellen tatbestandlichen Voraussetzungen für alle Bereiche durch, für das BKA-Gesetz, für das Polizeigesetz, für den Nachrichtendienst usw. und fragt immer, ob wir hier eine hinreichende tatbestandliche Normierung der Eingriffsvoraussetzung haben. Nach der gegenwärtigen Fassung ist es nur noch erforderlich, dass das zur Aufgabenerfüllung oder zur Erforschung des Sachverhalts erforderlich ist und nichts anderes. Man kann sich eigentlich die Frage des Richtervorbehalts angesichts dieser tatbestandlichen Weite auch fast sparen, weil man sich die Frage stellen muss, was der Richter überprüfen muss und ob jetzt die Einholung einer bestimmten Auskunft bei dem Telekommunikationsanbieter zur Aufgabenerfüllung des BKA erforderlich ist. Das ist eine derartige Weite. Wer da keine Begründung für liefern würde, hätte, glaube ich, seinen Beruf verfehlt. Die ganze Diskussion um Rechtsschutz macht keinen Sinn, wenn man keine tatbestandlichen Hürden auf der anderen Seite hat. Diese Hürden hatte das Bundesverfassungsgericht in seiner Entscheidung angemahnt. Es hat eben gesagt, – mit dem, was wir gerade festgestellt haben – dass der Gesetzgeber ausdrücklich die Gefahrenvorsorge ausgenommen und eine konkrete Gefahr gefordert hat. Damit bewegen wir uns an der Grenze des verfassungsrechtlich Hinnehmbaren, also an der äußersten Grenze und die gegenwärtige Fassung, nicht beim § 113 TKG, aber bei den entsprechenden Regelungen – Bundespolizeigesetz und BKA-Gesetz – erweitern diesen Rahmen auf die gesamte Aufgabenerfüllung des BKA und das ist eben auch die Gefahrenvorsorge und im Prinzip daher ein mögliches Eingreifen weit im Vorfeld einer Gefahr und damit eine verfassungsrechtliche Gefahr des Scheiterns vor dem Bundesverfassungsgericht

Vors. **Wolfgang Bosbach**: Danke! Herr Wirth, bitte.

SV Ernst Wirth (Kriminalrat, Bayerisches Landeskriminalamt, München): Vielen Dank! Das war jetzt wohl eine generelle Fragestellung von Ihnen, Herr Korte. Eine Minderausstattung mit Richtervorbehalten sehe ich grundsätzlich nicht, sondern ich sehe eine angemessene Ausstattung mit Richtervorbehalten. Ich sehe nur das Risiko, dass Richtervorbehalte inflationär vorgegeben werden. Welche Maßnahmen soll es denn künftig noch geben, die keinem Richtervorbehalt unterliegen?

Vors. **Wolfgang Bosbach**: Vielleicht ist an dieser Stelle, nicht als Belehrung, sondern nur als Hinweis, zu sagen, dass auch die Nicht-Richter an Recht und

Gesetz gebunden sind, weil manchmal der Eindruck erweckt wird, wenn kein Richter drüber guckt, kann es nichts sein, kann es nichts werden und ist rechtswidrig, weil die Polizei in erster Linie an das dran, drauf und drüber denkt und nicht an die Verteidigung des Rechtsstaates, aber das würde Herr Korte niemals unterschreiben. Er ist mittlerweile auch korrekt geworden. Herr Dr. von Notz, für BÜNDNIS 90/DIE GRÜNEN, bitte.

BE Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank, Herr Vorsitzender! Vielleicht auch Bezug nehmend auf das, was Herr Schuster zu Anfang gesagt hat: Ich finde es großartig, dass wir diese Anhörung machen, nicht nur, weil die Zeit so drängt und das so wichtig ist, sondern eben auch, weil deutlich wird, dass es offensichtlich starken Korrekturbedarf an dem gibt, was wir hier diskutieren und dafür sind ja Anhörungen auch da. Da bin ich gespannt. Bei dem Richtervorbehalt kann ich mir die Anmerkung auch nicht verkneifen. Es gibt keine Widersprüchlichkeit in Ihrer Argumentation, sondern in der Sache, wie wir allgemein darauf gucken. Bei den Fällen, die Sie beschrieben haben, wird niemand sagen, dass da nicht dringender Handlungsbedarf besteht oder dass da auch zügigst ein Richterentscheid herbeizuführen ist. Das Problem ist, dass wir krasseste Massenfälle haben, bei denen Richter mit Arbeit zuge deckt werden, wo diese Angemessenheit nicht mehr gegeben ist, und die führt dann in der faktischen Arbeitssituation dazu, dass der Richtervorbehalt leerläuft und damit ist dem Rechtsstaat und den Menschen überhaupt nicht geholfen. Eine Frage an Herrn Prof. Dr. Bäcker: Es gibt ja ein Argumentationspapier des BMJ, das kursiert und in dem steht, dass die hier vorliegende Regelung keine Erweiterung der Befugnisse für Abfragen mit sich bringt. Würden Sie dieser Aussage zustimmen, ja oder nein? Die zweite Frage geht an Herrn Dr. Dix und Herrn Schaar. Wenn ich die Frage teile, darf ich, glaube ich, nur noch eine stellen. Die Regierung entscheidet sich ja für eine Prüfpflicht der Provider in dem Entwurf, gewissermaßen ein kleines „Doppeltürmodell“, neben der gesetzlichen Prüfpflicht für die Sicherheitsbehörden, was ich grundsätzlich schon einen guten Gedanken finde. Die Frage: Kann man sozusagen diese zweite Kontrollebene normenklarer stärken oder ausbauen, damit daraus tatsächlich noch eine weitere Hürde entsteht? Wie schauen Sie darauf? Vielen Dank!

Vors. **Wolfgang Bosbach:** Danke! Herr Prof. Dr. Bäcker.

SV Professor Dr. Matthias Bäcker (Universität Mannheim): Herzlichen Dank, Herr Dr. von Notz! Ich wiederhole mich gerne. Ich halte diese Auffassung in dem mir nicht bekannten Diskussionspapier – die bisherigen Befugnisse würden nicht erweitert – in dieser Allgemeinheit für unzutreffend. Sie werden im präventivpolizeilichen Bereich ganz massiv erweitert. Im Bereich der Strafverfolgung und der Nachrichtendienste trifft die Aussage hingegen zu.

Vors. **Wolfgang Bosbach**: Danke! Herr Dr. Dix, bitte.

SV **Dr. Alexander Dix, LL.M.** (Berliner Beauftragter für Datenschutz und Informationsfreiheit, Berlin): Es ist richtig, dass sowohl die Telekommunikationsdiensteanbieter als auch die abfragenden Behörden einer Prüfpflicht unterworfen werden. Insofern teile ich auch nicht die Auffassung des Bundesrates, der hier offenbar in seinen Einwänden die Telekommunikationsdiensteanbieter tendenziell entlasten will. Man kann und sollte sehr wohl auch die Prüfpflicht bei den Diensteanbietern präzisieren. Da ist durchaus eine Schärfung der Normenklarheit vorstellbar, ohne dass ich einen konkreten Formulierungsvorschlag hätte.

Vors. **Wolfgang Bosbach**: Vielen Dank! Herr Schaar, bitte!

SV **Peter Schaar** (Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Bonn/Berlin): Vielen Dank, Herr Vorsitzender! Herr Dr. Dix hat es ausgeführt. Man kann diese Prüfverpflichtung der Provider sicherlich noch verbessern, allerdings können die Provider nicht das Vorliegen der rechtlichen Bedingungen bei der abfragenden Stelle, bei dem Bedarfsträger, prüfen. Es ist letztlich immer nur eine formale Prüfmöglichkeit, die man den Providern aufbürden kann. Das sollte man auch tun, das geschieht auch schon in einem gewissen Umfang, aber es entlastet letztlich auch nicht die Behörden, die diese Informationen bekommen wollen, hier gründliche Prüfungen vorzunehmen. Gestatten Sie mir in diesem Zusammenhang auch noch einmal eine ganz kurze Bemerkung zum Richtervorbehalt: Ich denke, dass auch hier Lösungen denkbar sind, wie wir sie z. B. im § 100b StPO haben, beispielsweise verweist § 100g StPO, Verkehrsdatenauskunft, auch auf § 100b StPO. Da gibt es die Rechtsfigur der Gefahr im Verzuge, wo dann von einer richterlichen Entscheidung abgesehen werden kann. Das wäre bei der Bestandsdatenauskunft dort, wo ein Richtervorbehalt eingeführt werden sollte, natürlich genauso denkbar.

Vors. **Wolfgang Bosbach**: Vielen Dank! Weitere Fragen liegen jetzt – zumindest bei den Berichterstatern – nicht vor. Gibt es darüberhinaus noch Fragen an die Sachverständigen? Das ist nicht der Fall. Dann darf ich mich bei Ihnen bedanken, insbesondere bei den Herren Sachverständigen, die nach Berlin angereist sind, bei den Kolleginnen und Kollegen sowie bei den Gästen.

Ende: 12:30 Uhr