Deutscher Bundestag
16. Wahlperiode

Protokoll Nr. 16/94

Innenausschuss

Wortprotokoll

94. Sitzung

Öffentliche Anhörung

am Montag, 11. Mai 2009, von 14.00 Uhr bis 17.00 Uhr
Paul-Löbe-Haus, Raum E 200
10557 Berlin, Konrad-Adenauer-Str. 1

Vorsitz: Sebastian Edathy, MdB

Öffentliche Anhörung von Sachverständigen
zum

Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes

BT-Drucksache 16/11967

Seite

Anlage B:

Nicht angeforderte Stellungnahmen
Ausschussdrucksachen-Nr. 16(4)588 ff

I. Anwesenheitsliste Mitglieder des Deutschen Bundestages

Bundesregierung

Bundesrat

Fraktionen und Gruppen

II. Liste der Sachverständigen für die Öffentliche Anhörung am 11. Mai 2009

1.	Dr. Patrick Breyer	Arbeitskreis Vorratsdatenspeicherung
2.	Annette Brückner	Eurasburg
3.	Dr. Udo Helmbrecht	Bundesamt für Sicherheit in der Informationstechnik, Bonn
4.	Prof. Dr. Andreas Pfitzmann	Technische Universität Dresden
5.	Prof. Dr. Hartmut Pohl	Hochschule Bonn-Rhein-Sieg, St. Augustin
6.	Prof. Dr. Ralf Poscher	Ruhr-Universität Bochum
7.	Peter Schaar	BfDI, Bonn
8.	Prof. Dr. Jörg Schwenk	an der Teilnahme kurzfristig verhindert

III. Sprechregister der Sachverständigen und Abgeordneten

IV. Protokollierung der Anhörung

Vors. **Sebastian Edathy**: Liebe Kolleginnen und Kollegen, sehr geehrte Damen und Herren, ich darf hiermit die 94. Sitzung des Innenausschusses des Deutschen Bundestages in der laufenden Wahlperiode eröffnen und Sie alle sehr herzlich begrüßen. Die Ausschusssitzung findet in Form einer öffentlichen Anhörung statt zu einem Gesetzentwurf der Bundesregierung betreffs der Stärkung der Sicherheit in der Informationstechnik des Bundes. Ich denke, viele der Kolleginnen und Kollegen haben dazu in den vergangenen Wochen auch zahlreiche Bürgereingaben bekommen. Ich habe zwischenzeitlich glaube ich mehr Eingaben zum vermeintlich geplanten Verbot des so genannten Paintball-Spiels bekommen, aber auch dieses Thema bewegt viele Menschen. Der Sinn der heutigen Anhörung ist, die Beratungen im Ausschuss über die vorliegenden Vorschläge weiter zu befördern. Mein Name ist Sebastian Edathy, ich bin Vorsitzender des Innenausschusses und werde die heutige Anhörung leiten. Ich bedanke mich sehr herzlich bei den Herren Sachverständigen, dass Sie zum einen der Anhörung nachgekommen sind und zum anderen, dass Sie uns schriftliche Stellungnahmen übermittelt haben. Diese schriftlichen Stellungnahmen sind verteilt worden und werden zu einem späteren Zeitpunkt dem Protokoll über die heutige Anhörung beigefügt. Ich gehe davon aus, dass die Bereitschaft der Sachverständigen zur öffentlichen Durchführung der Anhörung auch beinhaltet, dass wir ihre schriftlichen Stellungnahmen später in eine Gesamtdrucksache mit aufnehmen. Das Protokoll wird den Sachverständigen in der Rohfassung mit der Möglichkeit zugeleitet, ggf. noch Korrekturen vorzunehmen. Wenn das alles überarbeitet ist, wird das Protokoll mit den schriftlichen Stellungnahmen veröffentlicht und zudem auch im Internetauftritt des Deutschen Bundestages eingestellt.

Wie Sie der Einladung für die heutige Anhörung entnehmen konnten, ist als zeitlicher Rahmen eine Dauer von drei Stunden, längstens bis 17.00 Uhr vorgesehen. Die Obleute haben sich im Vorfeld darauf verständigt, dass den Sachverständigen jeweils 5 Minuten Zeit gegeben werden soll, um noch einmal ihre Schwerpunkte zum Gesetzentwurf der Bundesregierung mündlich darlegen zu können. Anschließend würden wir mit der Befragung der Sachverständigen durch die Berichterstatterinnen und Berichterstatter im Ausschuss beginnen bzw. durch weitere interessierte Ausschussmitglieder. Ich darf wie üblich vorab die Kolleginnen und Kollegen darum bitten, dass Sie diejenigen Sachverständigen konkret benennen, an die Ihre Fragen gerichtet sind.

Ich muss leider darauf hinweisen, dass einer der Sachverständigen kurzfristig aus gesundheitlichen Gründen absagen musste, obwohl er schon auf der Anreise war. Das ist Prof. Dr. Schwenk, der uns heute leider auch zu seinem eigenen Bedauern nicht zur Verfügung stehen kann.

Wir beginnen mit den mündlichen Vorträgen in der alphabetischen Reihenfolge, so dass zunächst Herr Dr. Breyer das Wort hat.

SV **Dr. Patrick Breyer** (Arbeitskreis Vorratsdatenspeicherung): Vielen Dank, Herr Vorsitzender. Mein Name ist Patrick Breyer, ich bin Mitglied im Arbeitskreis Vorratsdatenspeicherung und wie Sie schon richtig erwähnt haben, bewegt dieses Thema „Surfprotokollierung“ sehr viele Menschen. Wir haben den Prozess der Einführung des Gesetzes zur Vorratsdatenspeicherung mit vielen Demonstrationen, bei denen Zehntausende auf der Straße waren, mit Verfassungsbeschwerden – der größten Verfassungsbeschwerde in der Geschichte der Bundesrepublik – begleitet und waren entsprechend schockiert, dass wenige Tage, nachdem die letzte Stufe der Vorratsdatenspeicherung Anfang des Jahres in Kraft getreten ist, nun ein Gesetzentwurf vorgelegt worden ist, der letztlich das legalisieren würde, was eigentlich nie passieren sollte, nämlich auch Inhalte auf Vorrat zu speichern: welche Seiten im Internet aufgerufen worden sind, nach welchen Suchworten man gesucht hat, was man im Internet geschrieben und gelesen hat. Das sind sehr sensible Daten. Es geht im Unterschied zu § 100 Telekommunikationsgesetz (TKG), der in der Gesetzesbegründung genannt wird, nicht nur um die Person der Kontaktpartner, sondern darum, wofür wir uns interessieren, wonach wir suchen, in welcher Lebenssituation wir gerade sind. Es informiert sich jemand in einer Notlage über Drogen oder Eheprobleme, oder er sucht vielleicht auf Google nach bestimmten Sachen, oder er sieht sich auf eBay bestimmte Erotikprodukte an. Es sind äußerst sensible Daten, wer sich wofür im Internet interessiert und wonach er sucht. Deswegen ist die vorgesehene Ermächtigung im Telemediengesetz (TMG), solche Daten zur Störungsbeseitigung speichern zu dürfen, eine sehr schwerwiegende Änderung. Ebenso die Änderung in § 5 des beabsichtigten BSI-Gesetzes, die eine ganz ähnliche Vorratsdatenspeicherung ermöglichen würde, nämlich dem Bundesamt für Sicherheit in der Informationstechnik (BSI) erlauben würde, zu speichern, auf welchen Seiten man sich bei Bundesbehörden auf deren Portalen informiert hat. In der Sache ist eine solche Vorratsdatenspeicherung nicht geeignet zur Abwehr von Angriffen oder Gefahren. Man kann Angriffe nur verhindern, indem man Sicherheitslücken schließt, die Systeme auf dem aktuellen Stand hält, Firewalls installiert und ähnliche Maßnahmen ergreift, aber nicht, indem man Daten ansammelt. Aus der Praxis kann man anführen, dass selbst das Bundeskriminalamt (BKA), ebenso wie das Bundesjustizministerium (BMJ) oder der Bundesbeauftragte für den Datenschutz (BfDI), auf solche Speicherungen verzichtet und damit keineswegs häufiger Störungen hat als Seiten, die solches auf Vorrat speichern. Was die verfassungsrechtliche Frage angeht, meine ich, dass diese Vorschriften nicht zu rechtfertigen sind, denn wir haben in den Entscheidungen zur Videoüberwachung, zur Rasterfahndung, zum Kfz-Massenabgleich und jetzt auch zur Vorratsdatenspeicherung gehört, dass eine flächendeckende und anlasslose Erfassung personenbezogener Daten nicht verfassungsmäßig ist. Deswegen bitte ich darum, diese beiden Vorschriften aus dem Gesetzentwurf zu streichen. Danke schön!

Vors. **Sebastian Edathy**: Vielen Dank! Das Wort hat Frau Brückner, bitte.

BE **Frank Hofmann (Volkach)** (SPD): Ich halte es für sinnvoll und bin mit Herrn Binninger einig, dass wir bei § 15 TMG den Artikel 3 in diesem Gesetzgebungsverfahren, nicht weiterverfolgen werden und dass es sinnvoll ist, dies jetzt schon in der Anhörung zu berücksichtigen, so dass dazu nicht mehr vorgetragen werden muss.

Vors. **Sebastian Edathy**: Vielen Dank für den Hinweis, Herr Hofmann. Frau Brückner, bitte.

SV **Annette Brückner** (Intelligents, Gesellschaft für strategische Unternehmensberatung mbH): Vielen Dank, Herr Vorsitzender. Sehr geehrte Damen und Herren, ich möchte mich zunächst kurz vorstellen: Ich bin Gründungsgesellschafterin und langjährige Geschäftsführerin eines Unternehmens, das vom BSI-Gesetzentwurf betroffen sein könnte, nämlich eines deutschen Softwarehauses. Das Unternehmen habe ich vor 30 Jahren gemeinsam mit meinem Mann gegründet, wir waren anfangs auf Datenübertragungsprotokolle spezialisiert, wie sie auch hier eine Rolle spielen, haben u.a. für den Deutschen Bundestag Kommunikationskomponente geliefert und später z. B. das Informationssystem für den Schalck-Golodkowski-Untersuchungsausschuss entwickelt. Im Auftrag des Bundesministeriums des Innern (BMI) haben wir anschließend polizeiliches Informationssystem nach Ungarn, in die Slowakei und in die Ukraine geliefert. Heute wird dieses System z. B. im Land Brandenburg als landesweites Analyse- und Auswertungssystem für die Kriminalpolizei eingesetzt und unterstützt dort polizeiliche Fachverfahren im Bereich des Staatsschutzes bei der Bekämpfung organisierter Kriminalität, der Kinderpornographie oder auch von schweren Kapitalverbrechen. Ich wollte Ihnen dies eingangs mitteilen, um deutlich zu machen, dass mir sowohl der IT-Markt als auch das Geschäft mit Bundesbehörden und anderen Behörden aus jahrelanger Erfahrung bekannt ist.

Ergänzend zu meiner schriftlichen Stellungnahmen möchte ich auf zwei Aspekte des vorliegenden Gesetzentwurfs hinweisen: Erstens: Den so genannten Dual-Use. Zweitens: Die globale Strategie des BMI, die sich in den Ergebnissen der so genannten „Future-Group“ manifestiert.

Zum Ersten – Dual-Use: Das BMI hat in der laufenden Wahlperiode wichtige sicherheitsrelevante Gesetze unter Dach und Fach gebracht. Ich erinnere an das Gesetz über die Antiterrordatei bzw. die Gemeinsamen Dateien, die Vorratsdatenspeicherung sowie das BKA-Gesetz. Nicht unberücksichtigt bleiben dürfen Vorhaben, die zunächst nicht nur sicherheitsrelevant erscheinen, nämlich das Passgesetz, das Gesetz zur Einführung des neuen elektronischen Personalausweises oder das erst im April dieses Jahres in den Bundestag eingebrachte Bürgerportalgesetz. Die mit dem Gesetzesvorhaben verbundenen und von der Bundesregierung explizit artikulierten Absichten sind die eine Seite der Medaille. Doch besitzen die zuletzt genannten Gesetzesvorhaben einen möglichen zweiten Nutzen, weshalb ich sie Dual-Use nenne. Er besteht darin, dass Bürger und Vertreter von Unternehmen immer mehr gedrängt und, wie zu befürchten ist, in der Zukunft

zunehmend verpflichtet werden, sich in der Online-Kommunikation und bei Rechtsgeschäften im Online-Verkehr eindeutig zu identifizieren. Es dient dies, wie die Gesetzesvorhaben ausdrücken, zwar durchaus auch der Sicherheit im Rechtsverkehr, vor allem aber schafft es die Möglichkeit, dass der Handelnde automatisiert durch entsprechende Auswerteprogramme als Individuum erkannt, in Datenbanken eingestellt und mit den Beständen aus anderen Datensystemen abgeglichen werden kann. Dass ich weiß, wovon ich rede, möchte ich mit einem kurzen Beispiel deutlich machen: Ich habe selbst ein Patent für ein solches Informationssystem entwickelt und auch zum Patent angemeldet und erteilt bekommen.

Zweitens, zur globalen Strategie: Sollten Sie der Meinung sein, dass ich das Risiko des Dual-Use überzeichne, so möchte ich Ihnen ein Zitat zur Kenntnis bringen aus einem Konzeptpapier über öffentliche Sicherheit, Datenschutz und Technologie in Europa. Es handelt sich um einen im Jahr 2007 veröffentlichten Bericht einer informellen hochrangigen Beratergruppe über die Zukunft der inneren Sicherheit in der Europäischen Union, der so genannten „Future-Group“. Diese Gruppierung kam auf Initiative von Bundesinnenminister Dr. Schäuble zustande, und zwar zu Zeiten der deutschen Ratspräsidentschaft im gleichen Jahr. Die Arbeiten der „Future-Group“ bilden den Arbeitsplan für innere Sicherheit und Justizangelegenheiten für den nächsten Vierjahreszeitraum, also von 2010 bis 2014. In diesem Dokument wird der Begriff vom „Digitalen Tsunami“ eingeführt. Dazu heißt es, ich zitiere: „Was den Digitalen Tsunami weiter anschwellen lässt, ist das Onlineverhalten. Soziale Netzwerke wie MySpace, Facebook und Second Life und darüber hinaus alle Formen von Onlineaktivitäten generieren Berge von Informationen, die von staatlichen Sicherheitsorganisationen genutzt werden können. Jedes Objekt, das ein Mensch benutzt, jede Transaktion, die er macht und beinahe jeder Geschäftsgang oder jede Reise, die er unternimmt, erzeugt einen detaillierten digitalen Datensatz. Dies generiert einen wahren Schatz an Informationen für öffentliche Sicherheitsorganisationen und eröffnet gigantische Möglichkeiten zur Steigerung der Effektivität und Produktivität der öffentlichen Sicherheit.“ Der BSI-Gesetzentwurf würde einen wesentlichen Beitrag leisten, um den digitalen Tsunami noch weiter anwachsen zu lassen. Er würde dafür sorgen, dass die gesamte Kommunikation von Bürgern und Unternehmen mit Behörden sowie der Verkehr von Behörden untereinander Teil dieser gigantischen Flutwelle wird. Bürger und Unternehmen müssten somit befürchten, dass erstens immer mehr Anfragen, Anträge, Bescheide, Reiseaktivitäten, Finanztransaktionen und Kommunikationsvorgänge in Datenbanken eingespeist werden. Zweitens, dass Daten umfassend ausgetauscht bzw. Datenbanken zusammengeführt werden und drittens, dass daraus Dossiers über jeden Einzelnen von uns entstehen. Es erscheint mir wichtig, diesen globalen Aspekt der aktuellen Sicherheitspolitik auch bei zunächst isolierter Betrachtung des BSI-Gesetzentwurfes nicht aus den Augen zu verlieren. Vielen Dank!

Vors. **Sebastian Edathy**: Vielen Dank, Frau Brückner. Das Wort hat Dr. Helmbrecht, bitte.

SV **Dr. Udo Helmbrecht** (Präsident des Bundesamtes für Sicherheit in der Informationstechnik - BSI): Vielen Dank, Herr Vorsitzender. Das Statement von mir haben Sie schriftlich vorliegen und insofern will ich nur einige Punkte daraus noch einmal hervorheben. Das BSI-Gesetz stammt aus dem Jahr 1990, einer Zeit, in der noch nicht daran zu denken war, wie das Internet heute unser Privat- und Geschäftsleben vernetzt. Was wir heute feststellen müssen, ist, dass wir in unserer Gesellschaft von der Informationstechnik abhängig sind. Wir haben, wenn es um die Gefährdungslage im Internet geht, drei Punkte zu betrachten. Der erste Punkt ist, dass heute Produkte im Umlauf sind, die von Soft- und Hardware-Firmen hergestellt und geliefert werden, die Schwachstellen enthalten. Schwachstellen sind sicherlich technisch etwas ganz Normales, man kann mit diesen umgehen. Aber das Problem ist, dass in dieser Branche – das ist der zweite Punkt und das gibt es in keiner anderen Branche – Schwachstellen von Produkten kriminell ausgenutzt werden. Das heißt, heute wird von kriminell organisierten Menschen global das Internet missbraucht, um Schaden im Sinne von Informations- sowie Geldabfluss – denken Sie an Phishing etc. – anzurichten und hieraus Nutzen zu ziehen.

Darüber hinaus gibt es drittens, wie das früher auch war und das ist heute im Internet nicht anders, nachrichtendienstliche Spionage. Das heißt, was wir in unserer Gesellschaft grundsätzlich feststellen, ist, dass das, was wir bisher in der Vergangenheit in unserem realen Leben erlebt haben, in das Internetgeschäft und in das private Leben wandert und dass wir uns damit auseinander setzen müssen, wie wir uns im Internet, in diesem virtuellen Raum gegen Missbrauch, gegen kriminelle Energie und Spionage schützen wollen. Das heißt, die klassischen Schutzmaßnahmen, die wir bisher hatten, reichen nicht aus. Da wir hinterher noch „Fragen und Antworten“ haben, möchte ich jetzt nicht auf Teilaspekte meiner Vorredner eingehen, aber das, was wir heute als Virenschutz und Firewalls kennen, reicht für das, was wir heute in unserem Regierungsnetz sehen, nicht mehr aus. Das Internet kann darüber hinaus auch durch kriminelle Energie oder politische Interessen zu Sabotageakten missbraucht werden, wie wir das in den letzten Jahren in Estland und in Georgien gesehen haben, oder denken Sie an den Conficker-Wurm, der die Armeen Deutschlands, Frankreichs und Englands betroffen hat, oder die letzten Fälle, die in den USA aufgetreten sind. Deutschland, sowohl die Verwaltung als auch die Wirtschaft wird täglich über das Internet angegriffen, da brauchen wir nur in die Presse zu schauen. Die Regierungsnetze werden täglich angegriffen und die Regierung und deren Handlungsfähigkeit sind damit bedroht. Staatlich geheim zu haltende Informationen sind täglich Spionageangriffen ausgesetzt. Aber auch die Informationen der Bundesbürgerinnen und -bürger, die in der Bundesverwaltung verarbeitet werden, sind ebenso Manipulation und Spionage ausgesetzt. Wir benötigen einen ausreichenden Schutz im Interesse des Bürgers bezüglich seiner personenbezogenen Daten und den Schutz seiner Kommunikation mit den Bundesbehörden. Das heißt, wir müssen das BSI-Gesetz nach ca. 20 Jahren den tatsächlichen Gegebenheiten anpassen.

Insofern komme ich kurz auf die wesentlichen Paragraphen. Gemäß § 4 des Gesetzentwurfs soll das BSI als zentrale Meldestelle für IT-Sicherheit, Information über Sicherheitslücken und neue Angriffsmuster auf die Sicherheit der Informationstechnik zentral sammeln und auswerten.

§ 7 soll dem BSI ermöglichen, Informationen und Warnungen vor Sicherheitslücken in informationstechnischen Produkten und Diensten sowie vor Schadprogrammen an die betroffenen Stellen oder die Öffentlichkeit weiterzugeben.

In § 5 geht es um die Abwehr konkreter informationstechnischer Angriffe. Lassen Sie mich das, weil es dort im Detail beschrieben ist, an einem Beispiel deutlich sagen: Es ist ein völliges Missverständnis, wenn hier diskutiert wird, dass es um Überwachung, Speicherung oder Abgleich anderer Informationen geht, ein völliges Missverständnis! Ich glaube, man muss die Begriffe Kontrolle und Überwachung sorgfältiger benutzen. Wenn ein Bundesbürger aus dem Urlaub einreist, seinen Personalausweis an der Grenzkontrolle vorweist, dann kontrollieren wir, wer hineinkommt. Wenn jemand auf der Fahndungsliste steht, dann muss er mit Konsequenzen rechnen. Dort handelt es sich auch nicht um Überwachung. Wenn jemand aus Mexico kommt und wir am Flughafen sehen, ob er einen roten Kopf oder Fieber hat, dann ist das keine Überwachung, sondern Kontrolle. Darum geht es uns beim BSI: wir wollen die Bundesverwaltung schützen und kontrollieren, was an Datenverkehr in die Bundesverwaltung hineingeht. Wenn Sie das Gesetz genau lesen, ist es so geregelt, dass wir niemals ohne Anlass in die Informationen hineinsehen. Denn wir sind nicht an personenbezogenen Daten interessiert, sondern es geht uns nur darum, zu erkennen, ob Schadprogramme in das Bundesnetz hineinkommen.

Ein anderer Punkt ist § 8, die Sicherheitsstandards. Hier geht es darum, dass wir in der Bundesverwaltung Einfluss darauf nehmen können, welches Sicherheitsniveau wir haben, d. h., wir wollen in der Bundesverwaltung sichere IT-Produkte einsetzen und durch Standards, Zertifizierung und weitere Maßnahmen erreichen, dass wir sichere Produkte in der Bundesverwaltung auch zum Schutz der Bundesbürgerinnen und -bürger einsetzen können. Vielen Dank!

Vors. **Sebastian Edathy**: Vielen Dank, Herr Sachverständiger. Das Wort hat Prof. Dr. Pfitzmann, bitte.

SV **Prof. Dr. Andreas Pfitzmann** (Technische Universität Dresden): Ich möchte das, was ich Ihnen sage, unter das Motto stellen: Was wir tun müssen, ist Sicherheitslücken schließen und nicht in erster Linie Schadprogramme analysieren oder die Benutzung von Infrastrukturen des Bundes protokollieren. Es muss darum gehen, Sicherheitslücken zu schließen. Alles andere ist Kosmetik, wenn es darum geht, Sicherheit zu steigern.

Ich möchte auch darauf hinweisen, dass Sicherheitslücken schließen nicht ganz einfach ist. Man muss sicherlich auch an den IT-Herstellern Kritik üben. Aber es ist auch nicht einfacher geworden mit dem, was in den letzen Jahren innenpolitisch diskutiert wurde. Wir haben in dem Bereich inzwischen eine Interessenkollision im Amts- und Geschäftsbereich des BMI, wo einerseits das BSI die Aufgabe hat, Sicherheit zu befördern und Sicherheitslücken zu schließen, und das BKA die Befugnis erhalten hat, Sicherheitslücken auszunutzen, und von daher auch ein Interesse hat, dass diese erhalten bleiben.

Ich gehe einige wesentliche Paragraphen durch. Zunächst einmal § 5: Da habe ich hergeleitet, dass so, wie die Formulierungen jetzt sind, es letztlich darauf hinausläuft, dass man, wenn man Schadprogramme in der entsprechenden Form schreibt, damit dem BSI eine Befugnis verschaffen würde, alles für unbegrenzte Zeit zu speichern. Ich weiß, dass das nicht das ist, was sich Herr Dr. Helmbrecht wünscht. Wenn es aber darum geht, über ein Gesetz zu reden, dann geht es nicht darum, was man sich wünscht, sondern was in diesem Gesetz steht. Das wäre ggf. auch das, was das Bundesverfassungsgericht (BVerfG) dann interessieren würde. Aus den Überlegungen zu § 5 leiten sich drei wichtige Forderungen her. Das eine ist, wenn man dem BSI auch nur annähernd so weitreichende Befugnisse gibt, wie es jetzt im Gesetzentwurf steht, die Frage: Wer kontrolliert das BSI? Aus den Gründen Interessenkollision und Transparenz denke ich, dass die Vorstellung, dass das BMI allein oder hauptsächlich das BSI kontrolliert, dann sicher nicht mehr reicht. Es wäre zu überlegen, inwieweit eine parlamentarische Kontrollkommission nötig ist, um ein BSI mit auch nur annähernd den Befugnissen, wie sie jetzt im Gesetz stehen, zu kontrollieren, da mit diesen Befugnissen Gefährdungen auch für Bürger heraufbeschworen werden könnten, die durchaus dem, was von Geheimdiensten ausgehen kann, nahe kommen.

Die zweite Forderung wäre, dass, wenn Dinge gespeichert werden, dafür richterliche Anordnungen einzuholen sind, möglichst vorher, spätestens aber drei Tage nach Ergreifen einer Maßnahme. Eine Formulierung, dass das jemand im BSI absegnen muss, der die Qualifikation zum Richteramt hat, wäre aus meiner Sicht bei weitem nicht hinreichend.

Zum Dritten: Bitte § 5 deutlich restriktiver und klarer fassen. Wenn man gegen diesen Paragraphen so einfach Gegenbeispiele gegen das Gemeinte konstruieren kann, wie das zurzeit der Fall ist, dann ist das ein schlecht geschriebener Gesetzestext.

In § 7 wird in das nicht näher spezifizierte Ermessen des BSI gestellt, welche Sicherheitslücken und wann es diese veröffentlicht und welche nicht. Ich hatte schon angedeutet: Es gibt eine Interessenkollision im Dienstbereich des BMI. Da es aus meiner Sicht darum geht, die Sicherheitslücken zu schließen und nicht in erster Linie, Schadprogramme oder Nutzung von IT zu analysieren, bin ich sehr dafür, in das Gesetz hineinzuschreiben, dass Sicherheitslücken, die dem BSI bekannt werden, grundsätzlich zu veröffentlichen sind. Man muss dann über die Details reden. Bei „grundsätzlich“ mag

es Ausnahmen geben und man muss darüber reden, wann sind sie zu veröffentlichen, aber für das Vertrauen des Bürgers in das BSI ist dies absolut notwendig. Wenn von dieser Veröffentlichung abgewichen wird, dann stellt sich an der Stelle auch wieder die Frage: Wer kontrolliert das? Man braucht an der Stelle eine Kontrolle außerhalb des BMI. An der Stelle würde sich auch anbieten, eine parlamentarische Kontrollkommission zu nehmen. Es sei an der Stelle darauf hingewiesen, dass, wenn man Sicherheitslücken nicht veröffentlicht, die Geschichte uns erzählt, dass sie dann besonders lange nicht geschlossen werden und damit könnte man, wenn man keine Pflicht zur Veröffentlichung von Sicherheitslücken hat, die Probleme und den Bedarf für Speicherung, den § 5 lösen soll, erst auch anheizen und schaffen. Also bitte diese beiden Paragraphen im Zusammenhang reformieren.

Der nächste Paragraph, der kritisch ist, ist § 9...

Vors. **Sebastian Edathy**: Herr Sachverständiger, darf ich auf die Zeit hinweisen.

SV **Prof. Dr. Andreas Pfitzmann**: Ja, das ist der letzte Paragraph, zu dem ich etwas sage. An der Stelle wird dem BMI die Befugnis eingeräumt, zu sagen, dass irgendwelche Produkte aus politischen Erwägungen das Sicherheitszertifikat nicht bekommen sollen, oder dass Zertifikate aus dem Ausland nicht anerkannt werden. Mein Vorschlag ist, diese Befugnisse ersatzlos zu streichen. Das BSI sollte in seiner fachlichen Arbeit in keiner Form weisungsgebunden an irgendwelche politischen Erwägungen des BMI gebunden sein – wegen der Interessenkollision. Als meine Studenten diesen Entwurfstext gelesen haben, fingen sie an zu lachen und sagten: Okay, sicherheitszertifizierte Dinge vom BSI haben dann sozusagen den Bundestrojaner schon eingebaut, sonst würden sie das Zertifikat nicht bekommen. Das ist genau das, was man nicht will, aber es ist so, wie Leute den vorgelegten Gesetzestext lesen. Danke schön!

Vors. **Sebastian Edathy**: Vielen Dank! Das Wort hat Prof. Dr. Pohl, bitte.

SV **Prof. Dr. Hartmut Pohl** (Hochschule Bonn-Rhein-Sieg): Das erste ist: Das Gesetz erweckt den Eindruck, als würden diese Schadprogramme vom Himmel fallen und würden uns überfluten. Das ist ein völlig falscher Eindruck. Schadprogramme können nur Schaden anrichten, wenn sie tatsächlich eine Sicherheitslücke ausnutzen. Wenn die Sicherheitslücke geschlossen ist, dann nutzt auch ein Schadprogramm nichts. Ein aktuelles Beispiel ist der schon erwähnte Conficker-Wurm, der eine Sicherheitslücke, die längst gepatcht und korrigiert war, ausnutzte und deswegen Schaden anrichten konnte, weil viele Anwender die Fehlerkorrekturen nicht eingefahren haben. Eine Diskussion von Schadprogrammen, wie sie im Gesetzentwurf vorgesehen ist, die Untersuchungen und der Versuch, sie abzuwehren, ist aus meiner Sicht völlig nutzlos und kratzt an der Oberfläche der Informationssicherheit. Wir müssen uns an die Ursachen halten. Die Ursache ist jeweils eine Sicherheitslücke, zu der eine ganze Reihe von Schadprogrammen zugeordnet werden können und die Schadprogramme können dann diese Sicherheitslücke ausnutzen. Die Diskussion über Schadprogramme

ist überflüssig. Wir müssen uns auf die Sicherheitslücken konzentrieren. Das ist auch der Stand der Technik in Unternehmen, die sich nicht dazu verleiten lassen zu protokollieren, wer greift auf unsere Systeme wann zu und sendet etwas, sondern, wenn ein Angriff stattgefunden hat, wird nicht eruiert, wer der Täter ist, es wird eruiert, wo liegt die Sicherheitslücke, und die wird geschlossen. Das ist der Stand der Technik.

Wenn ich ein Beispiel aus dem Brandschutz bringen darf: Wenn Sie sich hier umsehen, es werden Sicherheitsmaßnahmen ergriffen, im Schrank ist ein Feuerlöscher, es gibt eine Sprinkleranlage, die Decke ist schwer entflammbar – selbst wenn es hier brennt, geht der Brand nicht aus dem Raum hinaus. Ganz wichtig, Sie sehen auch die Hinweise auf die Fluchtwege, wir kommen noch hinaus – auch wenn es hier brennt, der Brand geht nicht in die anderen Räume. Sie würden sehr lachen, wenn jemand fordert, wir wollen vor dem Raum eine Videokamera aufstellen und kontrollieren, protokollieren, auswerten und speichern, wer in den Raum hinein- und wer hinausgeht. Das ist kein Brandschutz, das ist Überwachung. So formuliert das Gesetz, vergleichbar in § 5, und deswegen muss § 5 aus meiner Sicht völlig gestrichen werden. Wir sollten im Gegenteil die Bundesregierung verpflichten, ab Ende 2009 ausschließlich zertifizierte Produkte einzusetzen, um wenigstens ein gewisses Sicherheitsniveau bei der Bundesverwaltung zu erreichen.

Zum Zweiten: Ich möchte etwas zu den Sicherheitslücken sagen. Es ist schon schlimm genug, dass die Fehler nicht korrigiert werden in vielen Bereichen und sich z. B. der Conficker-Wurm ausbreiten konnte. Viel schlimmer ist, dass es unveröffentlichte Sicherheitslücken gibt und dass es eine ganze Szene auf dieser Welt an bestimmten Orten gibt – in Vorderasien, in Osteuropa –, die systematisch gezielt neue Sicherheitslücken sucht. Das klingt erst einmal überraschend und etwas akademisch, aber tatsächlich gibt es auch einen Markt von Käufern und Interessenten für diese unveröffentlichten Sicherheitslücken, die je nach Schwere in der Größenordnung von bis zu 500.000 Dollar verkauft werden. Wer sind die Interessenten? Das liegt auf der Hand, das sind Nachrichtendienste, Wirtschaftsunternehmen, die Wirtschaftsspionage betreiben wollen, und das ist die organisierte Kriminalität. Wenn Sie sich dafür interessieren, gehen Sie in ein Internet-Versteigerungshaus – z.B. mit dem schönen Namen „WabiSabiLabi“ –, dort kann man unveröffentlichte Sicherheitslücken einstellen. Das ist so etwas wie eBay für Sicherheitsleute oder für Nachrichtendienste. Das ist mein zweiter Punkt, denn im Gesetzentwurf wird gesagt, das BSI kann (muss aber nicht!) solche unveröffentlichten Sicherheitslücken, die der Bundesregierung bekannt geworden sind, veröffentlichen. Was wird die Folge sein? Das BSI ist natürlich nicht die einzige Institution, die diese Sicherheitslücken kennt, es gibt andere, fremde Nachrichtendienste, es gibt Wirtschaftsunternehmen. Diese fremden Wirtschaftsunternehmen nutzen unveröffentlichte Sicherheitslücken aus – für den BND habe ich das in einem Aufsatz veröffentlicht –, nicht gegen deutsche Unternehmen, aber gegen andere. Fremde Nachrichtendienste und fremde Unternehmen treiben Wirtschaftsspionage gegen deutsche Unternehmen unter Ausnutzung von unveröffentlichten Sicherheitslücken. Der Schaden für Deutschland ist dann der Wegfall von Arbeitsplätzen. Der Wirtschaftsstandort

Deutschland wird massiv geschädigt, nur deswegen, weil unveröffentlichte Sicherheitslücken unveröffentlicht bleiben und sie das BSI nach diesem Entwurf auch gar nicht veröffentlichen muss. Das Gegenteil muss gefordert werden. Die Bundesregierung muss alle ihre bekannten Sicherheitslücken veröffentlichen, damit sich die Unternehmen und auch die Bürger dagegen schützen können. Wenn sie nicht veröffentlicht werden, ist der Bestand der Bundesrepublik Deutschland gefährdet.

Ein Beispiel dazu: Sie werden das aus der „Spiegel"-Veröffentlichung kennen, „Chinesen im Bundeskanzleramt". Die Chinesen, das ist die Gruppe „Titan-Rain", haben seit 2003 die US-Regierung erfolgreich angegriffen, sie haben die englische Regierung seit 2003 angegriffen, in Deutschland ist das im Jahre 2007 entdeckt worden. Schönen Dank!

Vors. **Sebastian Edathy**: Vielen Dank! Herr Prof. Dr. Poscher, bitte.

SV **Prof. Dr. Ralf Poscher** (Ruhr-Universität Bochum): Vielen Dank, Herr Vorsitzender. Meine Damen und Herren, meines Erachtens geht es bei diesem Entwurf auch noch um etwas Grundsätzlicheres. Zunächst hat der Entwurf ein wichtiges sicherheitspolitisches Anliegen, nämlich den Schutz der Informationstechnik des Bundes vor gezielten Angriffen krimineller ausländischer Dienste, Terroristen u.ä. Die Sicherheit der Informationssysteme ist auch international eines der großen Themen der defensiven aber auch offensiven Sicherheitspolitik. Gerade am heutigen Tage führt die „International Harold Tribune" den Leitartikel über die Cyberwar-Strategien des US-Militärs auf der Titelseite. Das ist ein großes Thema und der Gesetzgeber und die Ministerien haben sich zu Recht Gedanken dazu gemacht, wie man die Sicherheit der Informationssysteme des Bundes gewährleisten kann. Das Instrument, das der Gesetzgeber dazu wesentlich entwickelt hat, findet sich in § 5 BSI-Gesetz. Dieser Mechanismus, der installiert werden soll, ist mit einer ganzen Reihe von Grundrechtseingriffen verbunden und birgt auch selbst beachtliche Risiken für den Datenschutz und die Datensicherheit. Das ist als solches verfassungsrechtlich nicht zu kritisieren, weil es der allgemeinen Dialektik von Sicherheitsmaßnahmen entspricht, dass sie selbst immer auch Risiken für die Rechtsgüter schaffen, die sie andererseits aber zu schützen bezwecken.

Auch im Bereich der Sicherung von Informationstechnik des Bundes wird es unvermeidbar sein, dass dieser Schutz mit Grundrechtseingriffen und Risiken für den Datenschutz sowie Missbrauchsgefahren verbunden ist. Das Verfassungsrecht – und ich sitze hier als Verfassungsrechtler – reagiert auf diese Dialektik nicht so, dass es diese Sicherheitsmaßnahmen grundsätzlich untersagt. Aber das Verfassungsrecht fordert, dass so eingriffsintensive und mit so erheblichen Risiken und Missbrauchsgefahren behaftete Überwachungs- oder Kontrollsysteme, wie das in § 5 vorgeschlagene, mit ausreichenden Schutzmechanismen versehen sind, die die Eingriffsintensität der Maßnahmen sowie die Risiken und die Missbrauchsgefahren minimieren, verfassungsrechtlich kompensieren und begrenzen. Das bedeutet, dass in die Instrumente zur Sicherung der Informationstechnik des Bundes bereits durch den

Gesetzgeber selbst Elemente des Datenschutzes eingearbeitet werden müssen. An diesem Punkt sehe ich neben einer ganzen Reihe von Einzelpunkten das strukturelle Hauptproblem des Entwurfs. Er bemüht sich nicht in demselben Maße um die Implementation eines effektiven Datenschutzkonzeptes, wie er sich um die Installation eines Sicherheitssystems bemüht. Das ist aber genau der Zug, der jetzt im Wechselspiel zwischen Sicherheitspolitik und Verfassungsrecht im Bereich des Datenschutzes ansteht. Das Verfassungsrecht kann angesichts der immer weiter steigenden Eingriffs- und Gefährdungspotenziale der Informationstechnik nicht weiter tatenlos zusehen, sondern muss verlangen, dass die Befugnisse zur Kommunikationsüberwachung und zur Datensammlung mit ausreichenden datenschutzrechtlichen Sicherungen versehen sind. Es ist nur die Frage, wer diesen Zug macht: Entweder Sie, der Gesetzgeber, oder das Bundesverfassungsgericht. Dazu brauchen Sie auch keinen Verfassungsrechtler zu befragen, es reicht mittlerweile, wenn Sie die Bild-Zeitung lesen.

Es ist auch nicht so, dass der Entwurf keinerlei Ansätze enthielte, die in die richtige Richtung weisen. Ich denke, das gestufte Auswertungssystem, das sich die Verfasser des Entwurfs überlegt haben, um eine nicht-automatisierte Auswertung möglichst zu vermeiden, ist ein wichtiger Beitrag zur Minimierung der Eingriffsintensität, die mit diesem Überwachungs- oder auch „Kontroll“system verbunden ist. Doch das reicht allein nicht aus. Es fehlen wichtige Regelungselemente zum Ausschluss des Missbrauchs und zur Begrenzung der gesellschaftlichen und demokratischen Risiken, die von solchen Systemen ausgehen.

Ich habe in der schriftlichen Stellungnahme drei Regelungsbausteine zu diesem Punkt vorgeschlagen, die dabei Abhilfe schaffen können. Erstens: Müsste eine Pseudonymisierung der erhobenen Protokolldaten einschließlich eines gesetzlich geregelten Mechanismus zur Entpseudonymisierung geregelt werden, wenn diese im Einzelfall aus Sicherheitsgründen einmal erforderlich sein sollte. Was aber nach allen Auskünften äußerst selten der Fall sein soll.

Zweitens: Die Dokumentation der Überprüfungssignaturen und ihre effektive, d. h., unter Umständen unangemeldete Kontrolle durch eine unabhängige Stelle, etwa durch den Bundesdatenschutzbeauftragten.

Drittens: Die Sicherung einer besonderen demokratischen Kontrolle des Bundesamtes durch das Parlament, ein parlamentarisches Gremium oder durch die Veröffentlichung von Tätigkeitsberichten nach dem Muster der Regelung der Strafprozessordnung zur Telekommunikationsüberwachung.

Mit der gesetzlichen Vorgabe eines solchen Systems datenschutzrechtlicher Sicherungen, die in die Regelung der Sicherheitsinstrumente eingelassen sind, würde nicht nur ein Gewinn für das Sicherungskonzept der Bundesverwaltung verbunden sein, sondern die Bundesverwaltung würde auch ein Zeichen setzen. Der Gesetzgeber würde ein Modell schaffen, dass sich auf andere Bereiche der Verwaltung und modi-

fiziert auf den Datenschutz im Rahmen der Privatwirtschaft ausdehnen ließe. Es würde auch einen Anreiz für Softwarehersteller geschaffen, sich nicht nur mit Sicherheitslösungen zu beschäftigen, sondern, wenn sie sich mit Sicherheitslösungen beschäftigen, zugleich an Datenschutzlösungen zu denken. Nach allen Gesprächen, die ich im Zusammenhang mit dieser Anhörung geführt habe, ist deutlich geworden, dass das nicht immer in dem Maße geschieht, wie es möglich wäre.

Meiner Einschätzung nach steht der Gesetzgeber hier an einer Weggabelung. Er kann den Entwurf ein bisschen kosmetisch überarbeiten – das ist meiner Ansicht nach ein verfassungsrechtlich sehr riskanter Weg; oder er kann politische, und ich denke auch verfassungsrechtliche, Führungsstärke dadurch zeigen, dass er den Datenschutz ebenso ernst nimmt wie das Sicherheitskonzept und dass er Datenschutz und Sicherheit nicht in eine falsche Opposition bringt. Danke schön!

Vors. **Sebastian Edathy**: Vielen Dank! Das Wort hat Herr Schaar.

SV **Peter Schaar** (Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit): Vielen Dank, Herr Vorsitzender. Was bedeutet Datenschutz im Zusammenhang mit den vorgesehenen Maßnahmen zur Abwehr von Schadprogrammen und Gefahren für die Kommunikationstechnik des Bundes? Datenschutz bedeutet zunächst, dass der Eingriff in Persönlichkeitsrechte minimiert wird, insbesondere in das Recht auf informationelle Selbstbestimmung. Das wiederum bedeutet, dass so wenig personenbezogene Daten wie möglich erhoben, verarbeitet und ausgewertet werden. Man kann dieses Hauptkriterium, diesen Grundsatz auf verschiedenen Ebenen anwenden. Einmal im Hinblick auf die Frage, wie überhaupt die Gefährdungssituation ist. Da ist schon einiges gesagt worden, Herr Prof. Pohl hat dazu einige grundlegende Ausführungen gemacht. Der beste Schutz gegen Schadprogramme und gegen Sicherheitsgefährdungen, die aus dem Internet kommen, besteht darin, dass man die Sicherheitssysteme und die IT-Systeme insgesamt so sicher gestaltet, dass diese Schadprogramme nicht ihre Schadwirkung entfalten können. Das ist der erste Schritt. Der zweite Schritt ist die Bewertung der tatsächlichen Gefährdungssituation. Auch hier ist in den Stellungnahmen, die ich von einigen Gutachtern gelesen habe, insbesondere von Frau Brückner, einiges in Frage gestellt worden. Gleichwohl gehe ich aufgrund der mir vorliegenden Informationen davon aus, dass eine steigende Gefahr für die Informationstechnik des Bundes besteht. Herr Dr. Helmbrecht hat darauf hingewiesen, dass es hier zunehmende Gefährdungen gibt. Ich würde das nicht in Frage stellen, es erscheint mir nicht nur plausibel, sondern es wird auch durch Informationen gedeckt, die ich von anderer Seite erhalten habe, die ich aber hier im Detail nicht darlegen kann. Wenn es entsprechende Gefährdungslagen gibt, denen man mit klassischen Maßnahmen der IT-Sicherheit nicht wirklich effektiv und auf Dauer begegnen kann, dann muss man zusätzliche Maßnahmen treffen. Auch dann stellt sich aber die Frage: Wie kann man die Eingriffsintensität dieser Maßnahmen minimieren? In diesem Zusammenhang möchte ich darauf hinweisen, dass es außer der personenbezogenen Kontrolle, wie sie an den Grenzen stattfindet, die aus meiner Sicht auch eine Form von

Überwachung ist, auch Mechanismen gibt, die ohne personenbezogene Daten auskommen können. So hat die Fachhochschule Gelsenkirchen seit langem in Zusammenarbeit mit dem BSI an einem System gearbeitet, das eine automatisierte, aber nicht personenbezogene Auswertung der Kommunikationsvorgänge ermöglicht. Das heißt, falls man tatsächlich eine völlig anonyme Auswertung bewerkstelligen könnte, wäre das der minimal mögliche Eingriff. Insofern stellt sich die Frage, ob diese Ansätze überhaupt weiter verfolgt worden sind, oder warum man dann umgeschwenkt ist auf eine Lösung, die auf einer personenbezogenen Auswertung des Kommunikationsverkehrs beruht. Wenn man diese Frage beantwortet hat, dann kann man gleichwohl auch noch einiges für den Datenschutz tun und ich bin da mit Herrn Prof. Poscher völlig einer Meinung, man kann und man sollte die Daten möglichst anonym bzw. pseudonym auswerten. Ich denke, es ist zumindest in dieser ersten Phase der Analyse möglich, die Daten, die an den Gateways zum Internet anfallen – möglicherweise auch innerhalb des Netzes der Bundesverwaltung – so auszuwerten, dass ein direkter Rückbezug auf die Personen, die an diesem Datenverkehr beteiligt sind, unterbleibt. Das heißt, eine zentrale Forderung meinerseits ist dabei die nach einer möglichst anonymen und pseudonymen Auswertung. Die Pseudonymisierung muss möglicherweise stattfinden, um im Nachhinein eine Verknüpfung zu den konkreten Schadensereignissen herzustellen. Als Beispiel: Mittels einer E-Mail sind Daten in einen Rechner der Bundesverwaltung gelangt, also muss es irgendwo möglich sein, den Empfänger ausfindig zu machen. Das ist aber nur dann notwendig, wenn man konkrete und tatsächliche Anhaltspunkte hat für das Vorhandensein entsprechender Schadsoftware, die man dann bekämpfen bzw. beseitigen muss. Dazu muss man möglicherweise den Empfänger kennen. In einem solchen Fall den Personenbezug herzustellen, hielte ich dann für vertretbar unter der Voraussetzung, dass die anderen Prüfschritte auch erfolgt sind. Allerdings sollten diese tatsächlichen Anhaltspunkte dann auch dokumentiert werden müssen. Das könnte man im Gesetz auch aufnehmen.

Neben der Pseudonymisierung und Anonymisierung von Daten kommt auch der Transparenz der Verfahren besondere Bedeutung zu. Ich denke, dass hier die Benachrichtigungspflicht ein Mittel ist. Die Benachrichtigungspflicht von Betroffenen ist in § 5 Abs. 3 BSI-Gesetz doch etwas schwach ausgebildet. Ich könnte mir vorstellen, dass man da noch einmal nachbessert.

Im Hinblick auf § 5 Abs. 4 des BSI-Gesetzentwurfs denke ich, dass die Übermittlungsbefugnisse doch etwas weitgehend sind, insbesondere im Hinblick darauf, dass hier vorgesehen ist, dass einer Strafverfolgungsbehörde nicht nur bei Hinweisen auf schwere Straftaten die Daten übermittelt werden sollen, sondern auch in den Fällen, in denen diese Straftaten mittels Telekommunikation begangen werden. Ich gehe davon aus, dass sämtliche Straftaten, die auf diese Art und Weise aufgedeckt werden können, mittels Telekommunikation begangen werden, weil es sich hierbei um Telekommunikation handelt, die ausgewertet wird. Insofern würde man praktisch jegliche Information, die auf Straftaten hinweist, auswerten können. Hier wäre eine Begrenzung auf tatsächlich schwere Straftaten sehr sinnvoll.

Im Hinblick auf die in § 5 Abs. 6 BSI-Gesetzentwurf vorgesehenen Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung rege ich an, dass man sich hier stärker beschränkt. Entweder verzichtet man generell auf die Auswertung derartiger Daten bzw. solcher Daten, bei denen die Möglichkeit besteht, dass sie diesem Kernbereich zuzuordnen sind, oder man führt zumindest einen Richtervorbehalt ein, um eine unabhängige Entscheidung zu gewährleisten und es nicht dem BMI zu überlassen zu entscheiden, was gehört zu diesem Kernbereich und was nicht. Auf Ausführungen zu § 15 TMG verzichte ich im Hinblick auf die erfreuliche Entscheidung der Koalitionsfraktionen, das nicht weiter zu verfolgen.

Vors. **Sebastian Edathy**: Vielen Dank, Herr Schaar. Da Herr Prof. Dr. Schwenk leider nicht hier ist, sind wir damit am Ende der mündlichen Stellungnahmen der Sachverständigen angelangt. Wir könnten jetzt mit den Fragen der Abgeordneten beginnen und das Fragerecht für die Unionsfraktion hat zunächst Herr Abg. Binninger, bitte.

BE **Clemens Binninger** (CDU/CSU): Herr Vorsitzender, vielen Dank. Meine Herren, ich darf vielleicht die freudige Botschaft gleich noch um einen weiteren Punkt ergänzen, dass wir uns auch in den Verhandlungen dem Grunde nach bereits auf die Regelung der Anonymisierung und Pseudonymisierung verständigt haben, so dass wir auch bei diesem Punkt keinen vertieften Expertenstreit beginnen müssen und uns auf die noch offenen Fragen konzentrieren können.

Ich habe drei kurze Fragen an drei Sachverständige, an Herrn Dr. Helmbrecht, Herrn Pohl und Herrn Prof. Poscher. Zunächst meine Frage an Dr. Helmbrecht: Es wird teilweise, und das war in den Sachverständigenanhörungen auch zu entnehmen, ein bisschen der Eindruck erweckt, als ob die Bedrohungslage für die IT-Sicherheit relativ gering sei und auf das, was die Bundesregierung – das BSI – vorhat, sehr intensiv eingreifen würde, also alles überwachen, alles speichern. Könnten Sie dazu noch etwas sagen, was wirklich vorgesehen ist und was das BSI wirklich überhaupt erkennt bei seiner automatisierten Auswertung von Daten bzw. was überhaupt nur gespeichert werden darf.

Mir erschien bei dem einen oder anderen auch der Eindruck zu sein, es reicht, wenn wir uns auf zertifizierte Produkte konzentrieren. Wenn die gesichert im Einsatz sind, dann kann uns nichts mehr passieren. Reicht es angesichts der heutigen Organisationsmöglichkeiten von Hackern und von organisierter Kriminalität, wirklich aus, um sich auch vor solchen Angriffen zu schützen, indem man sagt, wir setzen ganz auf zertifizierte Produkte, dann kann uns nichts mehr passieren? Das wären meine zwei Fragen an Dr. Helmbrecht.

Herr Prof. Pohl, zwei kurze Fragen an Sie: Sie hatten ja eingangs erwähnt, dass Unternehmen es in der Wirtschaft so handhaben, dass sie bei Angriffen erst einmal abwarten bis sie passieren und dann die Lücke schließen, aber nichts weiter dagegen

unternehmen. Könnten Sie uns da konkret die Unternehmen benennen, zumindest die Branche? Ich frage deshalb, weil ich IT-Weltmarktführer in meinem Wahlkreis habe und ich es mir nicht vorstellen kann, dass die sich alles gefallen lassen. Es interessierte mich, aus welchen Bereichen diese Unternehmen sind.

Die zweite Frage: Hatten Sie Gelegenheit, im Vorfeld der Anhörung den Lagebericht zur IT-Sicherheit des BSI zu bekommen, in dem sehr detailliert die Gefährdungsszenarien beschrieben sind?

Meine letzte Frage geht an Prof. Poscher: Der Schwerpunkt der Kritik, und ich glaube auch der Schwerpunkt unserer Arbeit ohne Frage, ist der § 5 BSI-Gesetzentwurf. Er ist sicher das Herzstück des Gesetzes und er ist nicht einfach, das räume ich ein. Ich glaube auch nicht, dass er einfach zu haben ist, wenn er alle Bedürfnisse berücksichtigt, die gefordert werden. Aus dem Gesetzestext, den wir haben, ungeachtet der Ergebnisse der Verhandlungen, sehe ich schon ein abgestuftes Vorgehen – automatisierte Auswertung, Protokolldaten unverzüglich zu löschen, erst wenn Anhaltspunkte auf eine Schadstoffware vorhanden sind darf mehr passieren. Wo würden Sie uns konkret und an welcher Stelle sagen, da muss eine weitere Stufe für den Datenschutz hinein, ohne dass das Instrument wirkungslos wird, und wie könnte dies aussehen?

Vors. **Sebastian Edathy**: Vielen Dank! Zur Beantwortung zunächst Herr Dr. Helmbrecht, bitte.

SV **Dr. Udo Helmbrecht**: Vielen Dank! Ich möchte noch einmal ein Beispiel geben, damit deutlich wird, wo heute unsere Bedrohung liegt. Wenn Sie morgen eine E-Mail von mir bekommen, in der steht, „Sehr geehrte Damen und Herren, anbei meine Ausführungen von gestern. Klicken Sie auf den Anhang und sehen sich ihn an.“ Da kann die E-Mail-Adresse gefälscht sein und der Anhang kann ein Trojaner sein. Das soll nicht heißen, dass Sie jetzt nichts mehr aufmachen dürfen, aber die Problematik ist, wie wir damit im Internet umgehen. Das Problem, das dahinter steckt, gilt nicht nur für die Bundesverwaltung, das gilt für jeden Privatmann, für jedes Privatunternehmen, für jeden Mittelständler. Wenn jemand durch Social Engineering das Umfeld des Opfers ausspioniert und eine ganz dedizierte E-Mail schickt, dann öffnet man diese. Das entdecken die gängigen Viren und Trojaner und Firewalls nicht. Wenn Sie selber ein Virenschutzprogramm auf dem PC haben und sich die Häufigkeit automatischer Updates von Virensignaturen ansehen, dann geschieht das im Stunden-, manchmal im Minuten- oder manchmal im Tagestakt. Das heißt, dass die Kriminellen, die das für wirtschaftliche oder Spionageinteressen ausnutzen, uns in dem Moment einen Schritt voraus sind.

Der zweite Punkt sind die Websites. Nachdem Kriminelle erkannt haben, dass man mit den E-Mails vielleicht nicht mehr so einfach an die Zielperson herankommt, werden jetzt Websites im Internet angegriffen. Es sind schon – Statistiken gehen in die Richtung – zahlreiche Websites infiziert. Allein wenn Sie die Website anklicken, haben Sie schon

das Risiko, dass Sie ein Schadprogramm auf Ihrem Rechner haben. Wir suchen nach einem Ausweg, wie wir mit diesem Phänomen umgehen. Natürlich wäre es schön, wenn unsere Produkte besser, d.h. sicherer wären. Wir haben hier eine schnelllebige Branche. Zum Vergleich: Es kommt kein Flugzeug in die Luft, kein Waggon auf die Schiene, kein Auto auf die Straße, ohne dass es durch eine Behörde zugelassen wird. Etwas Vergleichbares gibt es in der IT-Branche nicht. Es ist auch nicht möglich zu fordern, dass nur zertifizierte Produkte eingesetzt werden, davon gibt es gar nicht genügend. Wenn wir morgen den Einsatz nicht-zertifizierter Produkte verbieten würden, welche Produkte wollten wir dann einsetzen? Zu sagen, wir wollen ausschließlich zertifizierte Produkte einsetzen, ist in einer globalen Weltwirtschaft nicht umsetzbar. Wir können die Welt nicht zwingen, nur Produkte nach unserem Sicherheitsstandard in Deutschland importieren oder exportieren zu dürfen. Ich hätte das auch gerne und habe in meiner Amtszeit immer den Einsatz zertifizierter Produkte unterstützt, aber es gibt nicht genügend zertifizierte Produkte, um alle Anwendungsgebiete abzudecken. Wir dürfen auch die Marktmechanismen nicht vergessen. Wenn Sie sich beispielsweise die neuen IT-Produkte Mobilkommunikations-Branche ansehen, z. B. Handys und PDAs, dann macht die Branche den gleichen Fehler wieder wie bei den PCs. Wenn der Hersteller sagt, Sie müssen auf einem Handy oder PDA ein Virenschutzprogramm einsetzen, dann wissen Sie genau, wo das Problem ist, nämlich, dass der Hersteller nicht ein sicheres Produkt, sondern ein schickes, billiges Produkt liefert. Insofern bleibt uns als BSI für die Bundesverwaltung in diesen Fällen nur die Möglichkeit, mit eigenen Entwicklungen verschlüsselte Sprachübertragung oder sichere E-Mail-Kommunikation selbst anzubieten und damit als Antwort auf die Frage der Zertifizierung: Wir wollen zertifizierte, sichere Produkte. Nur, der Markt ist dafür heute noch nicht für alle Anwendungsgebiete da.

Zur Frage, wie wir mit der E-Mail Kommunikation umgehen: Ich sagte es, wir sind nicht an personenbezogenen Daten interessiert. Die Schwierigkeit ist, dass wir mit der verfügbaren Technik nicht alle Schadprogramme entdecken. Die Frage ist, wie können wir Datenströme, die in unser Netz hineingehen, kontrollieren? Wir wollen dies weitestgehend automatisiert tun. Was wir heute machen, weil wir noch keine rechtlichen Befugnisse haben, ist, dass wir in zehn Behörden das Schadprogrammerkennungssystem (SES) einsetzen, um Erfahrungen zu sammeln. Dazu haben wir Dienstvereinbarungen mit den betroffenen Behörden abgeschlossen. Damit es ganz deutlich wird: wir speichern heute noch nichts. Was wir heute tun, ist, dass wir uns mit Einverständnis der Behörden automatisiert den Verkehr zu diesen Behörden ansehen. Um Ihnen eine Zahl zu nennen, wir haben etwa 50 Mio. E-Mails pro Monat, davon sind etwa 99,5 % Spam, das ist „der Schrott“, der von außen geschickt wird, und wir haben nur 0,001 – ein Tausendstel – Prozent aller E-Mails, die nach Abstimmung mit den Behörden in die manuelle Auswertung kommen. Es interessiert uns nicht der Inhalt der E-Mail, sondern, ob ein Schadprogramm, z.B. Trojaner vorhanden ist, oder ob jemand von innen heraus Schadprogramme automatisch nachladen will. Das heißt, die große Masse der E-Mails soll automatisiert durch Technik analysiert werden. Lediglich sofern ein Verdacht besteht, werden entsprechende weitergehende Maßnahmen ergriffen. Im

Anschluss können wir eine Anzeige erstatten oder Websites sperren lassen, damit diese nicht mehr aufgerufen werden. Insofern hoffe ich, Ihre Fragen beantwortet zu haben.

Vors. **Sebastian Edathy**: Vielen Dank! Herr Prof. Dr. Pohl, bitte.

SV **Prof. Dr. Hartmut Pohl**: Ich habe nicht sagen wollen, dass die Unternehmen abwarten, Angriffe zulassen und sich etwas gefallen lassen. Ich habe gesagt, dass sie Sicherheitsmaßnahmen realisieren, dass sie die Sicherheitslücken schließen, aber nicht eruieren, wer sie angegriffen hat. Das ist völlig unerheblich, sie wollen ihre Daten und Informationswerte schützen und deswegen realisieren sie Sicherheitsmaßnahmen. Unerheblich ist, wer angegriffen hat, und das ist im Tenor des Gesetzes ganz anders. Ein tatsächlicher Angreifer kommt natürlich nicht mit einer E-Mail-Adresse von 1&1 oder von der Telekom wie ein ordentlicher Bürger. Ein Angreifer würde eine Adresse wie wolfgang.terrorist@taliban.af für Afghanistan oder @pa für Pakistan benutzen und dann hat die Bundesregierung erhebliche Schwierigkeiten, den Absender festzustellen. Sie kann ihn praktisch nicht feststellen. Das ist irgendein Provider irgendwo in Afghanistan.

Zum Zweiten: Wenn es kein E-Mail-Angriff ist – und das ist gleichzeitig eine Antwort auf den Lagebericht. Es ist international bekannt, wie man angreift. Die Angriffe laufen nicht von Punkt zu Punkt, der Angreifer hat einen Rechner und greift dann das Innenministerium an, sondern der Angreifer greift einen Rechner in Korea an, hüpft von dem Server in die USA und treibt Server Hopping, und dann irgendwann, nachdem er 50 mal gehüpft ist, greift er das Innenministerium an – auch meine Hochschule ist von solchen Hüpfversuchen betroffen. Wenn man das rückverfolgen, überwachen, protokollieren und speichern will, kann man das gerne. Nur, den Täter kann man natürlich nicht rückverfolgen. Es sei denn, man besucht diese Orte, man analysiert die Protokolle auf den Servern etc. Es ist ein Riesenaufwand und dann stelle ich, was hier noch keiner gemacht hat, die Frage nach den Kosten der Überwachung, Auswertung und Protokollierung.

Zusammengefasst zu Ihrer ersten Frage: Es wird nicht eruiert, wer es war. Das ist mit einem angemessenen Aufwand nicht leistbar. Wenn es Ihnen trotzdem im Einzelfall einmal gelingen sollte, einen Täter zu packen, z. B. einen dieser bekannten Chinesen – vielleicht Herrn Wu Han –, dann haben Sie tatsächlich einen Chinesen von insgesamt mehr als 1,3 Mrd. erwischt, der Sie angegriffen hat. Dann gehen Sie einmal nach China und greifen Sie sich ihn. Was haben wir davon, dass wir wissen, Herr Wu Han hat die Bundesregierung angegriffen? Nichts! Entscheidend ist, die Sicherheitslücke zu schließen...

BE **Clemens Binninger**: Ich finde es ein bisschen zu gelassen, wenn wir sagen, wir können es nicht nachverfolgen, also was haben wir davon. Dafür können die Angriffe zu viel Schaden anrichten.

SV **Prof. Dr. Hartmut Pohl**: Sie haben mich gefragt, wie die Unternehmen reagieren. Die Unternehmen besitzen diese Gelassenheit und sagen, uns interessiert nicht, wer angreift, sondern welche Sicherheitslücken wir haben. Das ist es.

Sie haben mich nach den Gutachten für unterschiedliche Branchen gefragt. Herzlichen Dank für die Gelegenheit, dass ich das sagen darf. Ich berate Versorger, Pharmaindustrie, Automobilindustrie, kleine und mittelständische Unternehmen, die natürlich erhebliche Risiken im Ausfall ihres Geschäfts sehen, wenn die Produktion unterbrochen ist.

Der Lagebericht des BSI ist mir bekannt. Ich habe ausdrücklich darauf hingewiesen, dass diese Gruppe „Titan-Rain“ ganz gut analysiert ist und international seit 2003 die Regierungen der Welt angreift. Das ist auch der Bundesregierung bekannt – nach dem „Spiegel“-Bericht seit 2007.

Vors. **Sebastian Edathy**: Vielen Dank! Herr Prof. Dr. Poscher, bitte.

SV **Prof. Dr. Ralf Poscher**: Gefragt war nach den Stufen, die man einziehen kann. Ich denke, das knüpft einmal daran an, was Herr Prof. Dr. Pohl gerade gesagt hat und hängt mit der Pseudonymisierung zusammen. Wenn Sie das System, mit den jetzt bestehenden Stufungen, pseudonymisiert laufen lassen würden, würden bis zur Aufhebung der Pseudonymisierung keine personenbezogenen Daten anfallen. Die nächste Stufe, nach der Sie fragen, die im Gesetz noch nicht enthalten ist, wäre die der Aufhebung der Pseudonymisierung. Diese hat aber, wie Herr Prof. Dr. Pohl anschaulich gemacht hat, nur in sehr, sehr seltenen Fällen – das haben auch alle Rechenzentrumsleiter, mit denen ich mittlerweile gesprochen habe, gesagt – irgendeine Relevanz, weil man in der Regel weiß, dass die Angriffe nicht zurückverfolgbar sind, da sie so angelegt sind, dass der Aufwand zu groß ist. Sie brauchen die Entpseudonymisierung, jedenfalls des Absenders, in den seltensten Fällen. Und die nächste Stufe wäre zu sagen: Gut, selbst das lassen wir noch zu, aber dann unter besonderen Bedingungen. Das ist noch einmal wichtig: Wenn Sie jetzt noch überlegen, an dem Gesetzentwurf etwas zu ändern, dass Sie es nicht bei einem blassen Verweis auf das Bundesdatenschutzgesetz belassen, der jetzt in der Begründung steht, sondern Sie müssen in der Sache regeln, was genau zu geschehen hat. Sie müssen ein organisatorisches Regime schaffen, das die Sicherheit schafft, dass zum einen eine Pseudonymisierung stattfindet und dass ihre Aufhebung zum anderen auch rechtlich und politisch zuordbar bleibt: Etwa durch einen Behördenleitervorbehalt, bei dem der Behördenleiter nicht nur wichtige Fälle abzeichnet, sondern jedes Mal, wenn die Pseudonymisierung aufgehoben werden soll, dafür auch gerade stehen muss und dies dokumentiert wird. Das wäre die nächste Stufe, nach der Sie gefragt haben.

BE **Clemens Binninger**: Herr Vorsitzender, darf ich eine kurze Nachfrage stellen? Aufgreifend, dass was Herr Prof. Dr. Pohl und Sie, Herr Prof. Dr. Poscher, gesagt

haben: Jetzt unterstellen wir einmal die Pseudonymisierung – wie selten es auch überhaupt nötig sein wird, dann im konkreten Fall personenbezogen nachzuforschen – wäre es dann nicht aber angezeigt, dass wir insgesamt in der Bewertung dieses Gesetzes etwas zurückfahren, was hier „Überwachung“ und „Eingriffe“ angeht, wenn wir es doch so gut wie nie können. Erst haben wir es automatisiert; solange wir keine Anhaltspunkte haben, wird gelöscht. Wenn wir Anhaltspunkte haben, machen wir es pseudonymisiert und erst in ganz wenigen Fällen greifen wir dann zu. Dann ist das, glaube ich, nach meinen Dafürhalten eher falsch zu sagen: Hier wird gigantisch alles überwacht, was Bürger mit Behörden kommunizieren, inklusive Eingriffe in personenbezogene Daten.

Vors. **Sebastian Edathy**: Eine Nachfrage von Herrn Abg. Clemens Binninger. Herr Prof. Dr. Poscher, bitte.

SV **Prof. Dr. Ralf Poscher**: Auch dazu die Antwort. Zurzeit ist es eben nicht so, dass das Gesetz die Pseudonymisierung vorschreibt. Es kennt auch kein organisatorisches Instrumentarium für diese Pseudonymisierung. Daher werden die Daten eben nicht pseudonymisiert gespeichert. Und Sie haben dann die ganzen Daten gerade derjenigen, die nicht „hacken“, das sind Klardaten. Diese können Sie zurückverfolgen. Sie legen unter Umständen einen großen Pool von Daten an, mit dem dann alles Mögliche geschehen kann. Es geht nicht darum, dass man das jemandem unterstellen würde. Aber wir haben jetzt Erfahrungen gemacht, dass, wenn solche datenschutzrechtlichen Verlockungen offen stehen, diese auch genutzt werden.

– Zwischenrufe nicht rekonstruierbar –

SV **Prof. Dr. Ralf Poscher**: Aber auch ehemalige Teile der Bundesverwaltung, die Bundesbahn, die Telekom… Das soll auch niemandem unterstellt werden. Wenn Sie aber solche Instrumente anlegen, wenn Sie solche Datenreservoirs schaffen, dann gehört es dazu, dass Sie auch entsprechende Sicherungsmechanismen installieren. Ohne Pseudonymisierung haben Sie einen ungesicherten Datenbestand. Sie können ihn durch die Pseudonymisierung sichern. Das ist der Unterschied.

Vors. **Sebastian Edathy**: Herr Dr. Helmbrecht möchte kurz ergänzen.

SV **Dr. Udo Helmbrecht**: Ich möchte nur noch einmal ergänzen und deutlich machen, worum es uns geht. Es geht uns nicht um personenbezogene Daten, wie das manchmal unterstellt wird.

– Zwischenrufe nicht rekonstruierbar –

Der Punkt ist: Wenn Sie eine E-Mail im Verdachtsfall analysiert haben, kann diese eine Web-Adresse enthalten, die von Nachrichtendiensten oder organisierten Kriminellen missbraucht wird. Für uns geht es nicht darum, dass wir am Ende irgendjemanden im

Ausland finden. Aber es geht uns darum, dass wir diese Web-Adressen herausbekommen, damit wir verhindern können, dass diese wiederum benutzt werden, um uns anzugreifen. Das sind keine personenbezogenen Daten im Sinne meiner Adresse, meines Geburtstags oder meines Geschlechts.

Vors. **Sebastian Edathy**: Bevor die Ungeduld zunimmt hat jetzt Frau Abg. Gisela Piltz für die FDP-Fraktion das Wort.

BE **Gisela Piltz** (FDP): Es ist auch interessant: Wenn die Opposition hier nicht diese Anhörung beantragt hätte, wäre das Gesetz, das Sie hier fast alle verrissen haben, verabschiedet worden. Es ist schön, dass wir hier Rechtsberatung für die Bundesregierung machen können. Aber ein bisschen dramatisch finde ich das schon. Und Herr Binninger, bei allem Respekt, aber nur weil Sie hier sagen: Wir ziehen Anonymisierung … das machen wir anders, heißt es noch lange nicht, dass das a) so passiert und b) dass wir wissen, wie es geht und ob das klug gemacht ist oder nicht. Das werden wir dann mal sehen. Ich bin überzeugt davon, dass die CDU mir auch sagen würde: Wir haben den Kernbereichsschutz hier, weil ja das BMI entscheidet. Das müssen wir noch einmal sehen. Und im Übrigen gibt es noch genügend andere Kritikpunkte. Das kommt jetzt. Meine erste Frage an Herrn Schaar. Der Präsident des BSI hat hier – manche Vergleiche hinken doch sehr – einen Unterschied zwischen Kontrolle und Überwachung versucht herzustellen, auch für dieses Gesetz. Auch die letzte Diskussion ging darum, dass man eigentlich diese Daten gar nicht haben wolle. Was mich dann aber wundert ist, warum man dann Zufallsfunde weitergeben kann? Da würde ich gerne noch einmal ihre Meinung dazu haben. Inwieweit das denn aus ihrer Sicht tatsächlich auch so ist, wie das hier dargestellt worden ist. Und das Zweite: Die Regelung, die jetzt quasi nur ansatzweise den Kernbereich schützt, die ist ja aus meiner Sicht sehr originell. Dass wir den Datenschutzbeauftragten – einen Juristen aus dem Haus im BKA… Das war auch schon originell, fand ich. Aber ist Ihnen ein anderes Gesetz bekannt, wo man den Kernbereichsschutz doch eher eigenmächtig strickt und sich nur im eigenen Saft bewegt? Meine zweite Frage geht an Frau Brückner und Herrn Prof. Dr. Pohl. Hier ist viel von Zertifizierung gesprochen worden. Und wenn man sich anschaut, dann geht es schon z.B. im Gesetz zum Personalausweis und auch zum Reisepass, aber insbesondere zum Personalausweis, um die Zertifizierung, die bei dem Personalausweis dabei sein soll, und auch darum, dass möglichst nur vom BSI zertifizierte Produkte benutzt werden sollen. Da könnte man auch rein wirtschaftlich auf die Idee kommen, dass hier eine Marktmacht, eine marktbeherrschende Stellung des BSI geschaffen werden soll. Nach dem Motto: „Das BSI entscheidet wer gut ist und wer nicht.“ Sehen sie darin vielleicht auch eine Gefahr für den IT-Markt? Und meine zweite Frage an Herrn Prof. Dr. Pohl: Es wird hier viel darüber gesprochen, dass das so nicht geht. Welche konkreten, sinnvolleren Möglichkeiten gäbe es denn eigentlich, das zu schützen, was uns hier allen schützenswert erscheint, nämlich die IT-Sicherheit des Bundes. Dass man da etwas tun muss – und im Übrigen nicht erst seit gestern und nicht nach dem Motto: Wir haben seit 20 Jahren kein neues Gesetz gemacht – das haben Sie eben schon eindrucksvoll geschildert. Das Problem ist eben schon etwas

länger bekannt. Meine nächste Frage geht an Herrn Prof. Dr. Poscher und Herrn Dr. Breyer. Heute, gleichzeitig oder zeitversetzt, hat es hier im Haus eine Anhörung zum Arbeitnehmerdatenschutz gegeben und überhaupt zu Fragen, die Arbeitnehmer angehen. Wenn ich das jetzt richtig verstehe, könnte man mit diesem Gesetzentwurf auch alle Arbeitnehmer, zumindest des Bundes, überwachen oder alles aufzeichnen. Sie wollen das nicht, überwachen, das ist nur ein zufälliges Abfallprodukt und deshalb meine Frage: Ist das ein wirkliches Problem dieses Gesetzentwurfes und wenn ja, wie könnte man dem begegnen? Eine weitere Frage an Herrn Prof. Dr. Poscher und auch an Herrn Prof. Dr. Pfitzmann. Die Berufsgeheimnisträger sind in diesem Gesetzentwurf überhaupt nicht geregelt und das finde ich persönlich sehr mutig. Weil ich natürlich auch als Anwalt oder als Arzt oder als Abgeordnete, meinetwegen auch als Seelsorger, schon ein Interesse daran habe, Kommunikation, ohne das sie aufgezeichnet wird, zu vollziehen. Und auch da meine Frage: Inwieweit Sie das als Problem dieses Gesetzentwurfes sehen und wie man das lösen könnte. Und meine letzte Frage an Sie, Herr Dr. Helmbrecht: Sie haben, apropos Schwachstellen, uns eben noch einmal beschrieben, wie das so ist im Internet, wenn man Mails verschickt. Und deshalb meine konkrete Frage: Sie haben uns eine Mail geschickt mit Ihrer Stellungnahme als Word-Datei mit der Funktion aktiviert „Änderungen verfolgen“. Halten Sie das für sinnvoll im IT-Kommunikationszeitalter?

Vors. **Sebastian Edathy**: Also, als ich vorhin gebeten habe, die Sachverständigen zu benennen, an die sich eine Frage richtet, bin ich nicht davon ausgegangen, dass einzelne Kolleginnen und Kollegen dazu übergehen, Fragen an alle Sachverständigen zu stellen. Ich bitte doch im Sinne der Möglichkeit, dass alle Fraktionen sich hier beteiligen können, ein bisschen Maß zu halten. Wir hatten früher einmal Anhörungen, wo ich die Zahl der Fragen vorgegeben habe. Das möchte ich eigentlich nicht wieder einführen müssen. Aber es gibt auch die Möglichkeit, Frau Abg. Piltz, eine zweite oder dritte Runde zu machen. Herr Kollege Abg. Binninger hat sich auf drei Sachverständige bezogen und bei Ihnen bin ich jetzt bei sieben. Das also nur als geschäftsleitende Anregung: Aber in der Reihenfolge der Fragen von Frau Abg. Piltz. Herr Schaar, bitte.

SV **Peter Schaar**: Vielen Dank, Herr Vorsitzender. Sie haben ja noch einmal feinsinnige Differenzierung von Dr. Helmbrecht zwischen Kontrolle und Überwachung aufgegriffen. Ich denke, es gibt schon Kontrollen, die erst einmal nicht Überwachungscharakter im Sinne einer persönlichen Überwachung haben können. Wenn man tatsächlich den Datenstrom, d.h., die Bits und Bytes nach bestimmten Mustern durchsucht, ohne dass die Inhalte, die Urheber oder die Adressaten bekannt werden, dann könnte man sagen, ist das tatsächlich keine Überwachung. Das ist übrigens der Mechanismus, der zugrunde gelegt wird bei diesem „Gelsenkirchener Modell“, d.h., dass man versucht, auf einer technisch gesprochen sehr niedrigen Protokollebene – der Begriff Protokoll ist doppeldeutig, im Sinne von Kommunikationsprotokoll oder -standard. Wenn auf dieser sehr niedrigen Ebene bestimmte Muster als Schadprogramme oder als Schadsoftware identifiziert werden können, dann würde ich sagen, ist das noch keine Überwachung im engeren Sinne. Wenn allerdings diese Daten verbunden bleiben mit den Personen, von

denen sie stammen bzw. an die sie gerichtet sind, dann macht das schon einen riesigen Unterschied. Dann wird das zu einer Form von Überwachung, zumal wenn diese Daten dann auch noch gespeichert bleiben. Die Frage des Personenbezugs ist ja durchaus in Bezug auf sehr unterschiedliche Kreise von Personen, die dann ggf. Gegenstand von Überwachung werden könnten, zu sehen. Einmal geht es um die Mitarbeiterinnen und Mitarbeiter der öffentlichen Verwaltung – das ist eine Frage, die Sie an andere Sachverständige auch noch gestellt haben –, deren Surfverhalten bzw. deren Kommunikationsverhalten ggf. nachvollzogen werden kann. Es kann daneben um Bürgerinnen und Bürger gehen, die mit der Verwaltung kommunizieren, und „last but not least“ kann es um sonstige Dritte gehen, deren Inhalte über diese Gateways übermittelt werden. Das müssen nicht unbedingt dieselben Personen sein. Wenn der Autohändler bspw. im Rahmen des Kfz-Zulassungsverfahrens, das demnächst auch automatisiert stattfindet, eben auch bestimmte Daten von Personen, die eine Abwrackprämie beantragt haben, oder die ein Kfz zulassen wollen, übermittelt, fallen auch personenbezogene Daten dieser Dritten an. Und auf alle diese Kategorien muss man die Anforderung einer anonymen Auswertung anwenden und einer Pseudonymisierung, wenn man dann den Datenschutz entsprechend gewährleisten will.

Sie haben auch noch die Frage gestellt nach einer vergleichbaren Regelung der Selbstkontrolle der Einhaltung des Kernbereichs, der privaten Lebensgestaltung. Nein, mir ist kein anderes Gesetz bekannt, wo das vorgesetzte Ministerium diese Aufgabe zugewiesen bekommt.

Vors. **Sebastian Edathy**: Vielen Dank. Frau Brückner, bitte.

SV **Annette Brückner**: Ja, Frau Abg. Piltz, Sie hatten gefragt nach der Zertifizierung durch das BSI einerseits und ob die Gefahr besteht, dass das BSI eine ihm vielleicht nicht zustehende Marktmacht gewinnt. Was die Zertifizierung angeht, möchte ich zunächst darauf eingehen, dass das BSI sich ja – in meinen Augen vollkommen zu Recht – im Gesetzentwurf die Möglichkeit vorbehält, Standards und technische Richtlinien zu setzen. Das ist absolut nichts Neues, denn das tut es bisher auch schon und war bisher auch sehr erfolgreich. Wir sollten uns vielleicht einmal darüber unterhalten, was eigentlich Standards sind. Und da gibt es eine ganze Bandbreite. Das können allgemein oder international anerkannte tatsächliche Standards sein, die auch Normencharakter haben, und von entsprechenden Normungsorganisationen verabschiedet sind. Das kann das Widerspiegeln des Stands der Technik sein. Es kann sich handeln um „best practices“, wie sie gerade eben im Bereich der Informationssicherheit von einer Organisation der englischen Regierung unter der Kurzbezeichnung ITIL herausgegeben worden sind. Und sie sind auch deswegen positiv, weil erstens sehr viele Leute darin mitarbeiten und weil zweitens sichergestellt ist, dass technische Weiterentwicklungen in diese Standards hineinfließen. Was ich allerdings bedenklich finde bei den Standards, wie sie das BSI vorsieht, ist, dass im Unterschied zum BSI-Errichtungsgesetz alles gestrichen worden ist, was diese Standards offen und transparent macht. Früher hieß es im Gesetz – nicht in dem des Gesetzentwurfes,

sondern im BSI-Errichtungsgesetz von 1990 – dass es sich entweder um Standards des BSI handelt oder um allgemein anerkannte Standards. Das ist ersatzlos gestrichen worden. Und da frage ich mich als potenzieller Hersteller: Woher soll ich denn wissen, was das BSI an technischen Richtlinien herausgibt? Bevor ich hier weitermache, sollte ich vielleicht noch auf zwei Dinge eingehen, die an der Stelle eine Rolle spielen. Das eine ist die Tatsache, dass so etwas nicht absolut neu ist. Wir haben vor 25 Jahren bereits Datenübertragungskomponenten entwickelt. Das war Hardware und Software. Und da war es vollkommen normal, dass man sich an das sog. Zentralamt für Zulassungen im Fernmeldewesen (ZZF) wenden musste, um da seinen entsprechenden Sticker zu bekommen – diesen Aufkleber, den Sie alle kennen, das Posthörnchen – damit das Gerät an das entsprechende Telekommunikationsnetz angeschlossen werden durfte. Und von daher ist für mich nicht ganz nachvollziehbar, was Herr Dr. Helmbrecht vorhin gesagt hat, dass der Markt dem nicht folgen würde, dass es einfach keine zertifizierten Geräte gäbe. Denn bis jetzt war es immer so: Wo ein Geschäft zu holen ist, ist der Markt auch da. Und man richtet sich nach den entsprechenden Standards. Also dafür würde ich gerne einmal harte Fakten sehen. Das ist das eine. Aber um jetzt weiterzumachen bei der Zertifizierungsinstanz BSI. Es ist doch zunächst einmal zu sagen, dass, was die Standards und technischen Richtlinien angeht, wir hier einen Mangel auf drei Ebenen zu beklagen haben. Das eine ist: Wir haben keine Transparenz. Das zweite ist: Wir haben keine Offenheit, weil wir nicht wissen, welche Standards eigentlich angewendet werden sollen. Und das dritte ist: Die Allgemeingültigkeit ist gestrichen. Wenn also diese drei Dinge wieder ins Gesetz hineinkommen könnten, dann wäre aus meiner Sicht dem absolut Genüge getan, was notwendig wäre, wenn auch noch die anderen Dinge mit ins Spiel kommen. Und das betrifft jetzt die Marktmacht, die potenzielle Marktmacht des BSI. Da sehe ich eine gewisse Gefährdung darin, dass das BSI eine Mehrfachrolle einnimmt. Zum einem definiert es, was eigentlich geleistet werden soll, ohne offenzulegen. Zum zweiten ist es die Prüf-, Zertifizierungs- und Akkreditierungsinstanz. Also man stellt selbst die Standards auf und sagt dann: Jetzt entscheide ich selbst, ob ich oder ob du als Anbieter mit dem konform gehst oder nicht. Das dritte ist, dass das BSI in einem sehr weitgehenden Rahmen auch faktischer Entscheider über Beschaffungen ist. Einmal über die Beschaffungen, die im eigenen Bereich getätigt werden. Aber wenn das BSI seine Standards vorgibt, ist es auch automatisch so, dass sich dann eine Landesbehörde oder eine Kommunalbehörde, wohl als Kommunikationspartner, an diesen Standards orientieren muss. Und das prädeterminiert deren Beschaffungsvorgänge. Das ist also die dritte Rolle, die das BSI hier faktisch einnimmt. Und das vierte betrifft die Tatsache, dass sich das BSI in dem Gesetzentwurf hier vorbehält, auch aktiv Wettbewerber zu werden, weil es ja Komponenten selbst entwickeln und anbieten will. Das soll so weit gehen, dass per Verwaltungsvorschrift geregelt wird, dass die Bundesstellen das zu übernehmen haben. Damit haben wir in meinen Augen einen „closed shop“, einen Markt, der vollkommen bestimmt wird von BMI und BSI. Und das kann meiner Ansicht nach so nicht hingehen. Danke.

Vors. **Sebastian Edathy**: Vielen Dank. Herr Prof. Dr. Pohl.

SV **Prof. Dr. Hartmut Pohl**: Sie haben gefragt, wie die IT-Sicherheit bei der Bundesregierung aus meiner Sicht hergestellt werden könnte. Dazu eine Anmerkung: Wir sprechen hier über Angriffe und gleichzeitig sprechen wir über Spam. Das ist eine Werbemail, das ist kein Angriff in dem harten Sinne. Angriffe sind für mich nur zielgerichtete Aktivitäten gegen Systeme, im Fall dieses Gesetzes gegen die Systeme der Bundesregierung, und nicht Mails, die an jedermann in der Welt, dessen E-Mail man nun kennt, geschickt werden. Das ist Spam. Den filtert man heraus. Das ist zeitaufwendig, aber es ist nicht weiter der Rede wert. Auch Viren werden relativ leicht herausgefischt. Ich würde sagen: „nachrangige Angriffchen“. Die Virensuchprogramm-Hersteller liefern in ein bis zwei Tagen eine Funktion, so dass man solche Viren erkennt, spätestens meist nach ein bis zwei Tagen. Also den letzten Virus, den wir im Institut hatten, der datiert von vor sieben Jahren. Man erreicht mit diesen Virensuch-Programmen schon ein hohes Maß an Sicherheit. Das sind nicht die Angriffe, die ich meine. Mit Angriffen meine ich, wenn jemand zielgerichtet einen bestimmten Server der Bundesregierung, des Bundeskanzleramtes, des Verteidigungsministeriums oder des Wirtschaftministeriums angreift und hier Informationen rausholt, also Spionage, oder Informationen verfälscht, also Sabotage. Und dazu – abgesehen von den Standardmaßnahmen Viren – Würmersuche und Firewall etc., das ist der Grundschutz, wie er vom BSI bezeichnet wird, solche Maßnahmen sind Standard, Intrusion-Protection-Systeme, das kann man alles machen – zu diesem Grundschutz muss natürlich auch gehören, ausschließlich zertifizierte Systeme einzusetzen. Die US-Regierung hat das, aus meiner Sicht, wenn ich mich recht erinnere, schon für 1991 gefordert. Und wir haben das immer noch nicht in der Bundesregierung. Es darf nicht der Eindruck entstehen, dass es da vielleicht ein System gibt, was zertifiziert ist, oder eine Hand voll, das sind Tausende. Die Amerikaner, die Engländer, die Franzosen, die Niederländer und die Kanadier, nur um die ursprünglichen Staaten zu nennen, die an diesen gemeinsamen Kriterien mitgearbeitet haben, haben alle auf der Grundlage dieser einheitlichen Kriterien Systeme zertifiziert. Also es sind z.B. alle bedeutenderen Betriebssysteme zertifiziert, in unterschiedlichen Sicherheitsniveaus, natürlich. Es ist Standardsoftware zertifiziert. Diese allgemeinen „Common Criteria“, sind inzwischen ein ISO-Standard und gelten weltweit. Die Japaner haben zertifiziert. Ich habe sicherlich gleich eine ganze Reihe von Staaten jetzt nicht nennen können, weil ich sie nicht im Kopf habe, die Systeme zertifiziert haben. Es ist nicht eine Hand voll, die Ihnen an zertifizierten Systemen zur Verfügung steht, sondern sicherlich tausend. Das ist eine, aus meiner Sicht, Grundschutzmaßnahme, die die Regierung sehr leicht durchsetzen könnte. Das zweite sind natürlich Sicherheitslücken. Die, die man kennt, muss man sofort schließen. Wenn der Hersteller eine Fehlerkorrektur veröffentlicht hat, das fordert im Übrigen auch das BSI, dann muss diese Fehlerkorrektur unverzüglich eingefahren werden. Anderenfalls ist man nicht sicher, dass ein Angreifer diese Systeme nicht doch angreift. Also, die Bundesregierung sollte natürlich diese Sicherheitslücken sofort schließen. Damit ist implizit schon gesagt, dass man auch alle nicht veröffentlichten Sicherheitslücken kennen sollte, also sie veröffentlichen muss, wenn man eine kennt. Damit die Behörden in die Lage versetzt werden, sich zu

schützen. Wenn das BSI eine Sicherheitslücke geheim halten würde, wie das ja nach dem Gesetzentwurf möglich ist, dann würden wir Gefahr laufen, dass die Bundesregierung sich nicht gegen Angriffe und Sicherheitslücken schützen könnte. Es sei denn, das BSI informiert Punkt für Punkt die Kanzlerin oder den Wirtschaftminister. Schönen Dank.

Vors. **Sebastian Edathy**: Vielen Dank. Herr Sachverständiger Prof. Dr. Poscher, bitte.

SV **Prof. Dr. Poscher**: Zu der Frage der Überwachung der Arbeitnehmer, praktisch der Bundesverwaltung. Es ist ganz klar – und insofern verstehe ich auch, dass das Bundesamt das zurückweist –, das System ist natürlich nicht auf eine Überwachung aller Mitarbeiter angelegt. Der Punkt ist aber, dass dieses System und die Datenmengen, die erstellt werden, sich zu solchen Zwecken missbrauchen ließen. Es geht jetzt darum, einen Schutz davor zu schaffen. Das ist das eine. Das andere ist, dass dieses System, so wie das System angelegt ist, eben auch für die Mitarbeiter der Bundesverwaltung und alle, die mit ihm kommunizieren, das Risiko von Zufallsfunden birgt. Dass ihre Kommunikation, weil sie zufällig mit irgendwelchen Dingen belastet ist, in die Auswertung gerät. Ich denke, die beiden Mechanismen, die davor schützen können, sind zum einen die Pseudonymisierung, sowohl der Erhebung als auch der Datenbestände, zum anderen wesentlich höhere Verwendungsschranken für die ganz wenigen Fälle, in denen die Pseudonymisierung aufgehoben werden muss und Zufallsfunde gemacht werden. Für diese Fälle sind deutlich höhere Verwendungsschranken zu finden, als der Gesetzentwurf sie vorsieht. Nach dem Gesetzentwurf können auch wegen Bagatellkriminalität die Daten an die Verfolgungsbehörden weitergereicht werden. Der dritte Punkt knüpft daran an. Alle diese Mechanismen würden natürlich auch Berufsgeheimnisträger schützen. Ich denke, man sollte überlegen, diese sowohl in diesem Gesetz als auch in anderen Gesetzen noch einmal besonders zu schützen und ich habe auch auf die entsprechende Regelung etwa der Strafprozessordnung hingewiesen. An diesen Schutz, den Berufsgeheimnisträger in der Strafprozessordnung vor Zufallsfunden haben, angelehnt, könnte man das Gesetz ausgestalten. Dahin geht mein Vorschlag.

Vors. **Sebastian Edathy**: Vielen Dank. Herr Dr. Breyer, bitte.

SV **Dr. Patrick Breyer**: Danke. Die Frage, die Sie an mich gerichtet hatten, war, inwiefern dieser § 5 BSIG-Entwurf auch eine Arbeitnehmerüberwachung vorsieht oder was er für die Arbeitnehmer der Bundesverwaltung bedeuten würde. Insofern bin ich dankbar, dass Sie darauf aufmerksam machen, dass nicht nur die Nutzer betroffen sind, d.h. diejenigen, die sich die Internetportale des Bundes anschauen, sondern auch diejenigen, die aus dem Bund heraus auf das Internet zugreifen. Und da ist in der Tat eine gravierende Auswirkung in diesem § 5 enthalten: Bisher ist es so, wenn E-Mails ankommen bei einer Behörde, können die natürlich gefiltert werden, können Virenscanner eingesetzt werden etc., nach Maßgabe der Mitbestimmungsgesetze. Sie haben auch erläutert, wie das BSI das bisher schon macht in Abstimmung mit der

Behörde und in Abstimmung mit der Mitarbeitervertretung. Nach diesem § 5 soll das ganz anders laufen. Da soll eine zentrale Stelle, nämlich das BSI, für die gesamte Informationstechnik des Bundes in eigener Verantwortung und ohne Abstimmung mit den Mitarbeitervertretungen zuständig sein, nach Abs. 1 Nr. 1 Protokolldaten zu sammeln, d.h. insbesondere auch Surfprotokolle, also was die Mitarbeiter aufgerufen haben im Internet. Nach Nr. 2 soll es den Inhalt automatisch rastern können, d.h. das, was bisher bei den Behörden selbst passiert. Und nach Abs. 2 sollen die Protokolldaten auch aufbewahrt werden, noch länger als es nach Abs. 1 vorgesehen ist. Das würde für die Mitarbeiter eine Durchbrechung des Fernmeldegeheimnisses bedeuten. Denn das BSI steht noch nicht beim Empfänger, sondern vor dem Empfänger, deswegen ist das Fernmeldegeheimnis anwendbar. Erst recht natürlich bei privaten Telefonaten oder E-Mails ist ein Eingriff in das Fernmeldegeheimnis da. Da bringt auch eine Pseudonymisierung nichts. Denn die Protokolle sind schon pseudonym. Sie haben ja in Surfprotokollen nicht drinstehen: Herr XY hat zugegriffen, sondern die IP-Adresse. Deswegen ist eine Pseudonymisierung ohne zusätzlichen Wert. Man muss auf jeden Fall anonyme Daten nutzen. Dazu ist auch schon viel gesagt worden, wie gut das bisher in der Praxis funktioniert. Von daher – ausgehend von den Ausführungen von Herrn Dr. Helmbrecht – frage ich mich, warum die bisherige Praxis nicht reichen soll. Sie haben geschildert wie viel das BSI schon macht und dass es nur ganz seltene Fälle offenbar sind, in denen weitere Daten benötigt werden. Deswegen schafft diese Regelung, meines Erachtens, Risiken auch für die informationelle Selbstbestimmung der Mitarbeiter, setzt sie den Risiken von Datenpannen aus, von versehentlichen Veröffentlichungen. Man kann die Sicherheit von Informationssystemen nicht schützen, indem man noch mehr Daten Sicherheitsrisiken aussetzt.

Vors. **Sebastian Edathy**: Herr Prof. Dr. Pfitzmann, bitte.

SV **Prof. Dr. Andreas Pfitzmann**: Ich würde nicht in erster Linie für Berufsgeheimnisträger versuchen, wiederum etwas Spezielles zu machen. Sondern ich würde allgemein versuchen den Personenbezug und die Erfassung, ggf. auch Erfassbarkeit, zu senken. Herr Prof. Dr. Pohl hat sehr deutlich gesagt: Wer angreifen will, macht es über so viele Zwischenstufen, dass der sich alleine pseudonymisiert. D.h. also das, was wir hier einfach erfassen, das sind die Daten von den Arglosen. Und deswegen würde ich jetzt nicht sagen, Berufsgeheimnisträger bitte eine gesonderte Behandlung, sondern nein, Personenbezug generell weg.

Vors. **Sebastian Edathy**: Herr Dr. Helmbrecht, bitte.

SV **Dr. Udo Helmbrecht**: Sie fragten nach der Word-Datei. Das ist eine geschickte Frage, das gebe ich zu. Normalerweise würde ich auch nur eine PDF-Datei versenden. Aber es war leider gewünscht, dass wir eine Word-Datei schicken. Also hat die brave Mitarbeiterin, als Beamtin, das als Word-Dokument geschickt. Zwei kurze Bemerkungen zum Thema „Common Criteria“ will ich kurz anschließen. Unser Problem bei

den „Common Criteria“ ist: Es gibt nicht genügend Produkte für den alltäglichen Bedarf. Jeder, der hier oder zu Hause einen PC hat: Schauen Sie mal, ob das, was Sie auf Ihrem PC haben, ein zertifiziertes Produkt ist. Der Markt liefert das nicht. Wenn Sie ein Gesetz verabschieden, nach dem in der Bundesverwaltung nur zertifizierte Produkte eingesetzt werden dürfen, wäre ich glücklich darüber. Aber dies wird nicht passieren. Unser Problem ist, dass wir die Maßnahmen, die wir heute diskutieren, bis dato als BSI nicht wahrnehmen können: Wir speichern nichts willkürlich. Wir arbeiten gerade an der Oberfläche, wenn Herr Schaar sagte, dass wir das Schadprogrammerkennungssystem (SES) einsetzen. Dies geschieht mit gerade mal zehn Bundesbehörden mit Dienstvereinbarungen. Wir wollen auf der einen Seite Sicherheit für die Bediensteten hier im BSI, in meiner Behörde sowie in der Bundesverwaltung. Und wir wollen nicht zahlreiche Dienstvereinbarungen für alle Bundesbehörden schließen müssen. Unser Ziel ist letztlich Rechtssicherheit, auch für die Bürgerinnen und Bürger. Daher benötigen wir die Befugnisse im BSI-Gesetz.

Vors. **Sebastian Edathy**: Vielen Dank. Das Fragerecht hat jetzt die SPD-Fraktion. Herr Abg. Hofmann, bitte.

BE **Frank Hofmann** (Volkach) (SPD): Vielen Dank, Herr Vorsitzender. Herr Dr. Helmbrecht, ich möchte in dem Bereich die erste Frage gleich einmal an Sie richten. Bei der Lagedarstellung, bei der Gefährdungsanalyse, nach dem, was man öffentlich hört, hat alles mit China zu tun. Gehen Sie davon aus, dass das Hell- und Dunkelfeld in etwa gleich ist? Oder sind da strukturelle Mängel vorhanden, dass wir auch mit Angriffen natürlich von anderen Staaten auf die Bundesbehörden zu rechnen haben, bzw. dass sie auch erfolgt sind, ohne dass Sie das jeweils festgestellt haben? Das wäre für mich eine wichtige Sache. Und eine zweite Frage noch dazu. Sicherheitslücken veröffentlichen, das war die Forderung hier. Wie sehen Sie das oder wo könnte darin das Problem liegen? Eine andere Frage, die richtet sich insbesondere an Herrn Dr. Breyer, Herrn Prof. Dr. Pfitzmann und Herrn Prof. Dr. Pohl. Sie haben dafür plädiert, sich nicht so sehr um die Schadprogramme zu kümmern, sondern die Sicherheitslücken zu schließen. Und Herr Dr. Breyer, Sie haben den Kopf geschüttelt, als es hieß: Mit zertifizierten Produkten, das würde nicht funktionieren. Da möchte ich nur einmal wissen, was ihre Reaktion darauf ist. Ich denke, dass das die erste Entscheidung ist. Kann ich sagen, wir können die Sicherheitslücken schließen, dann müssen wir uns um das andere nicht kümmern. Aber gibt es zumindest ein „time lag“, wo ich doch an Schadprogramme heran gehen muss und mich darum kümmern muss? Das ist für mich die entscheidende Frage für dieses Gesetz hier. Es ist über die gefährdeten Berufsgruppen, wie Journalisten, Ärzte usw., schon gesprochen worden. Ich wollte bei Ihnen, Herr Prof. Dr. Poscher, noch einmal nachfassen mit der Benachrichtigungspflicht durch eine unabhängige Stelle. Ist es verfassungsrechtlich erforderlich, dass wir eine unabhängige Stelle nehmen oder ginge dies auch anders?

Vors. **Sebastian Edathy**: Vielen Dank, Herr Abg. Hofmann. Herr Dr. Helmbrecht zunächst, bitte.

SV **Dr. Udo Helmbrecht**: Vielen Dank. Zunächst zu der Frage: Veröffentlichung von Sicherheitslücken. Die Problematik ist, das haben wir mehrfach gehört, dass es heute Schwachstellen in Systemen gibt. Es gibt zu einem bestimmten Zeitpunkt nicht bekannte Schwachstellen. Und die Frage, die keiner von uns im Detail beantworten kann, ist: Wie viele Kriminelle gibt es, die diese Schwachstelle schon ausnutzen, die wir als BSI oder die Hersteller von Viren-Suchprogrammen oder von sonstigen Produkten noch nicht kennen? Wird eine Schwachstelle bekannt, sprechen wir natürlich zunächst einmal mit dem Hersteller und fragen: Gibt es dazu schon einen sog. „Patch“, also eine Korrektur, um diese Schwachstelle zu beheben? Und dann hängt es von dem Hersteller ab. Es kann sein, dass der Hersteller sagt: Ich habe schon ein Patch, dies wird in Kürze veröffentlicht. Oder der Hersteller sagt: Tut mir leid, es dauert noch zwei oder vier Monate, bis eine Schwachstelle behoben wird. Und genau darum geht es, dass in diesen Fällen, in denen die Schwachstelle nicht sofort behoben werden kann, im Falle einer Veröffentlichung das Risiko besteht, dass wir es in die ganze Welt hinausposaunen: Bei dem Hersteller, bei dessen Produkt gibt es eine Schwachstelle und gegen diese Schwachstelle kann man im Moment nichts tun, weil der Hersteller einige Wochen benötigt, um sie zu beheben. Und bis andere sog. „workarounds“, also Umgehungen, gefunden haben, kann auch einige Zeit vergehen. Und dann kann jeder kriminelle Trittbrettfahrer diese Schwachstelle auch ausnutzen. Also insofern ist das für uns eine Abwägung des Risikos, wann wir das veröffentlichen. Die zweite Frage war: Was wissen wir? Da muss ich Ihnen heute ehrlich sagen, da wir dieses Gesetz noch nicht haben: Ich weiß es nicht. Insofern kann ich auch nicht sagen, ob die Bundesregierung jetzt ausreichend geschützt ist, oder ob wir mehr tun müssen. Wir können das bisher nur aus Indizien ableiten. Was wir aus dem Umfeld unseres Regierungsnetzes wissen, ist Folgendes: Alles, was an Spam in der Welt herumgeistert, kommt auch bei uns an. Wir sehen die Schadprogramme, die bei uns ankommen. Wir haben im Schnitt pro Tag etwa fünf bis sechs Trojaner, die bei den oben erwähnten Bundesbehörden ankommen. Dadurch, dass wir mit anderen Behörden in Dialog treten und sich die Computer Emergency Response Teams mit der Industrie austauschen, haben wir eine gewisse Erfahrung, wie wir es in unserem Lagebericht dargestellt haben. Aber sichere Auskünfte darüber geben, wie das Dunkelfeld aussieht, können wir erst, wenn wir entsprechend den Vorgaben des § 5 analysieren dürfen, was sich dort wirklich abspielt.

Vors. **Sebastian Edathy**: Vielen Dank. Herr Dr. Breyer, bitte.

SV **Dr. Patrick Breyer**: Dankeschön. An mich war die Frage gerichtet, wie das Verhältnis von Sicherheit und Überwachung ist, d.h. Sicherheit der Informationstechnik im Verhältnis zu der Protokollierung und Auswertung, wie sie hier vorgesehen ist. Das Verhältnis ist relativ leicht darzustellen: Die Surfprotokollierung, wie sie hier in dem § 5 vorgesehen ist, hat nichts mit einem Schutz der Informationstechnik zu tun. Sie ist dazu ungeeignet. Das liegt schon an dem Wesen der Protokollierung. Bei einer Protokollierung schreiben Sie mit. Sie können damit nichts verhindern. Deswegen hat

beides miteinander nichts zu tun. Auch Ihre Frage, ob es vielleicht für Fälle erforderlich ist, in denen eine Sicherheitslücke ausgenutzt worden ist, die noch nicht geschlossen ist, das sog. „time lag“, ob es in diesen Fällen erforderlich ist, da sage ich auch da: Nein. Denn in diesen Fällen bringt eine Protokollierung nichts, um diese Sicherheitslücke zu schließen. Es ist auch nicht dazu erforderlich, wie in der Begründung des Gesetzentwurfs steht, damit man jetzt nachschaut, wer die Sicherheitslücke in der Vergangenheit ausgenutzt hat. Sondern, wenn ein Schadprogramm aufgetreten ist, muss die gesamte Bundesverwaltung natürlich daran gehen, ihre Systeme zu überprüfen und Virenscanner updaten, was auch immer man da ergreift. Da nützt es nichts, nachträglich nachzuverfolgen, was da vielleicht gemacht worden ist, was auch im Fall der meisten Schadprogramme gar nicht funktioniert, das anhand von Protokolldaten nachzuvollziehen. Sie haben gefragt, warum ich den Kopf geschüttelt habe, als gesagt worden ist: Sichere Produkte sind nicht machbar. Da ist sehr wohl sehr viel zu machen, was der Gesetzgeber noch tun könnte. Ich gehe ein paar Ideen einmal durch: Zum einen gibt es im Bereich der Automobiltechnik den TÜV, der ab und zu einmal routinemäßig überprüft, wie es um die Sicherheit des Autos bestellt ist. So etwas könnte man vielleicht auch für national wichtige Informationstechnik einführen. Zum zweiten die Produkthaftung. Wir haben im Bereich der Produkthaftung ein sehr erfolgreiches Gesetz, das dazu geführt hat, dass die Zahl der Unfälle und der unsicheren Produkte sehr zurückgegangen ist. Dadurch, dass die Hersteller einfach dafür haften, wenn sie unsichere Produkte in die Welt gesetzt haben. Die Produkthaftung gilt aber bisher nur für Vermögensschäden. Wenn man das ausweiten würde, dass die Hersteller etwa auch für Datenpannen, für nicht materielle Schäden haften oder für nicht körperliche Schäden, könnte das auch etwas bringen. Oder wenn man eine Haftung der Anbieter vorsehen würde, die unsichere Systeme betreiben und deswegen plötzlich personenbezogene Daten im Internet veröffentlichen. Also, das Haftungsrecht ist ein sehr effizientes Instrument, das noch nicht ausreichend ausgeschöpft ist. Und was den Bereich der Datensicherheit angeht: Da ist die beste Sicherheit die Datensparsamkeit. Es freut mich, wenn Herr Dr. Helmbrecht vorhin gesagt hat: Ziel dieses Gesetzentwurfes ist auch, personenbezogene Daten zu schützen. Nur, der beste Schutz, sichere Daten, sind nur nicht gespeicherte Daten. Die können dann auch nicht versehentlich veröffentlicht oder angegriffen oder sonst Gegenstand von Datenpannen werden. Man müsste im Telemediengesetz durchsetzen, dass wir anonym surfen können, natürlich auch auf Behördenwebsites. Deshalb ist diese Regelung genau das Gegenteil von dem, was es bräuchte, um die Sicherheit in der Informationstechnik zu gewährleisten.

Vors. **Sebastian Edathy**: Herr Prof. Dr. Pfitzmann, bitte.

SV **Prof. Dr. Andreas Pfitzmann**: Aus meiner schriftlichen Stellungnahme wäre der Vorschlag: Das BSI soll alle seine Erkenntnisse über Sicherheitslücken und Schadprogramme umgehend an Betroffene weitergeben, also bspw. an die Hersteller oder die Leute, die das System mit Sicherheitslücken betreiben, und zeitnah veröffentlichen. Also es ist klar, dass man da einen gewissen Abstand braucht. Erst

einmal warnt man die Hersteller, die Betroffenen, aber am Schluss, denke ich, muss veröffentlicht werden. Und zwar nicht irgendwann, sondern da gehört an die Stelle auch eine Frist in das Gesetz, bspw. drei Monate, weil sich manche Hersteller viel Zeit lassen, wenn es nicht ein wirkliches Druckmittel gibt, dass sie sich beeilen müssen. Die zweite Sache. Kann man sichere Systeme bauen? Wie sicher sind die Systeme in der Verwaltung? Die erste Antwort lautet: Ja, wir könnten wirklich sichere Systeme bauen. Und da weiß ich, worüber ich rede. Es laufen bei einem Kollegen von mir Projekte, wo auch zusammen mit dem BSI Mikrokerne gebaut werden, da werden Systeme gehärtet. Da geht sehr viel. Aber wenn die öffentliche Verwaltung meint, dass alle Leute mit der „eierlegenden Wollmilchsau“ arbeiten müssen, mit Featuritis ohne Ende, dann kriegen sie es natürlich nicht in den Griff. Und die Frage ist jetzt, wie machen Sie die Güterabwägung? Was klar ist, ist, wenn Sie jeden mit der „eierlegenden Wollmilchsau“ arbeiten lassen, dann kriegen Sie die Sicherheit nie in den Griff. Und jetzt haben Sie eine Güterabwägung. Wollen Sie in der öffentlichen Verwaltung, bei der Beschaffungspolitik der öffentlichen Verwaltung sagen, Priorität hat die Beschaffung der „eierlegenden Wollmilchsau“? Und dann macht im Nachgang das BSI, oder wer auch immer, eine möglichst umfassende Protokollierung und Auswertung der Schäden, die dabei entstehen? Oder machen Sie vorbeugend einen Schritt, dass Sie sagen, es darf nicht Jeder beliebige Technik beschaffen und in Betrieb nehmen. „Eierlegende Wollmilchsau“ ist nicht das Standardprodukt in der öffentlichen Verwaltung und an der Stelle wird es substanziell. Es ist klar, Sie können nicht „everybody’s darling“ sein. Sie können nicht jedem Mitarbeiter alles ermöglichen auf seiner „Kiste“, ob er sie jetzt anfassen darf oder nicht, und dann Sicherheit garantieren. Man muss sich entscheiden. Aus meiner Sicht, denke ich mal, muss man eher der öffentlichen Verwaltung Auflagen machen, was sie darf, als jetzt die Bürger mit ihren Daten die Zeche bezahlen zu lassen. Dankeschön.

Vors. **Sebastian Edathy**: Sie haben Herrn Prof. Dr. Pohl und Herrn Prof. Dr. Poscher auch gefragt.

SV **Prof. Dr. Hartmut Pohl**: Vielen Dank, Herr Vorsitzender. Ich bin zu den Sicherheitslücken noch einmal gefragt worden. Bei den unveröffentlichten Sicherheitsrisiken besteht das ungeheure Risiko, dass ich sie gar nicht kenne, dass ich die zugrunde liegenden oder ausnutzenden Schadprogramme also auch nicht erkennen kann. Ich bin Opfer, ohne es zu wissen. Als Unternehmen und als Bundesregierung, wenn die Sicherheitslücke nicht veröffentlicht ist, ist man völlig offen für einen Angreifer. Also das ist eine Situation, die man aus meiner Sicht vermeiden muss. Es müssen die Sicherheitslücken veröffentlicht werden. Ein Risiko bei der Veröffentlichung einer Sicherheitslücke besteht aus meiner Sicht nur sehr nachrangig. Es gibt eine Reihe von Unternehmen im Markt, Softwareunternehmen, die sehr gern Fehlerkorrekturen erstellen für erkannte Sicherheitslücken großer Hersteller, bei denen die Hersteller sich nicht entschließen können, diese Lücken zu schließen. Also finden wir Drittanbieter, die sehr wohl bereit sind, Fehlerkorrekturen herzustellen, also bleibt diese Sicherheitslücke, wenn überhaupt, nur kurze Zeit bestehen. Da könnte man dem

BSI zumuten und den Hersteller, wie Herr Prof. Dr. Pfitzmann sagte, informieren und unter Zeitdruck setzen. Drei Monate wäre mir viel zu lange. Sechs Wochen ist eine sehr lange Zeit. Es hängt aber natürlich von der Schwere der Sicherheitslücke ab. Wenn der Hersteller keinen „Patch“ in der Hinterhand hat und sich nicht bereit erklärt diese Fehlerkorrektur zu erstellen, dann könnte man sich vorstellen, dass das BSI Drittanbieter fragt: Sind Sie bereit, dafür eine Fehlerkorrektur herzustellen? Im Übrigen, es ist unverzichtbar, dass die Sicherheitslücke veröffentlicht wird. Dann kann die Regierung, das Unternehmen darüber entscheiden: Lasse ich meine Systeme weiterlaufen und setze mich dem Risiko aus, oder schalte ich doch meine Systeme ab? Ich fahre nicht auf allen meinen Systemen diese spezielle Software mit dieser Sicherheitslücke. Wir haben heute überhaupt noch nicht über Parametrisierung gesprochen. Man muss nicht immer das gesamte Softwarepaket, was einem der Hersteller anbietet, installieren, sondern man kann es, der Begriff fiel, „härten“, nur bestimmte Komponenten nehmen, nur ausgewählte, die vielleicht sicherer sind, und andere, die unsicher sein könnten, weglassen. Also hat die Bundesregierung oder ein Unternehmen einen großen Spielraum zwischen völligem Abschalten und Härten eines Systems. Wichtig ist, dass ich die Sicherheitslücke kenne. Sonst bin ich unwissendes Opfer und weiß das gar nicht.

Vors. **Sebastian Edathy**: Herr Prof. Dr. Poscher, bitte.

SV **Prof. Dr. Ralf Poscher**: Die Frage richtete sich auf die Benachrichtigungspflicht und ich habe den Punkt so verstanden, eine unabhängige Stelle darüber entscheiden zu lassen, ob die Benachrichtigung erfolgt oder nicht. Ich denke, verfassungsrechtlich notwendig ist erst einmal die Benachrichtigung. Denn nur die Benachrichtigung gewährleistet, dass individueller Rechtsschutz stattfindet. Rechtsschutz heißt nicht einfach nur, dass irgendwann einmal irgendein Richter irgendwie mit der Sache befasst ist, sondern Rechtsschutz heißt, dass rechtliches Gehör gewährt wird. Denn ohne dieses rechtliche Gehör werden Sie nur selten beurteilen können, ob eine Datenverwendung für den Betroffenen erheblich ist, ob er Gründe vorzutragen hat, die einen eventuellen Verdacht entkräften könnten etc. Alles das kann auch eine Kontrolle durch eine unabhängige Stelle bei der Benachrichtigungspflicht nicht leisten. Ich könnte mir das als ein zusätzliches verfahrensrechtliches Instrument vorstellen, um die Ausnahmen zu kontrollieren. Da wäre es vielleicht sinnvoll, dass eine unabhängige Stelle kontrolliert, ob wirklich ein unverhältnismäßiger Aufwand vorliegt, oder ob durch die Benachrichtigung oder die Ermittlung Rechtsverletzungen oder Rechtseingriffe, entweder bei den Betroffenen oder bei Dritten noch einmal vertieft würden. Aber auch mit einer unabhängigen Stelle, die dazwischen geschaltet ist, kann ich mir eine Ausnahme, wie sie jetzt im Gesetz steht, wonach eine unabhängige Stelle darüber entscheidet, ob der Betroffene einen Eingriff für erheblich erachtet, oder ob er ein Interesse daran haben könnte, die Sache weiter zu verfolgen, nicht vorstellen. Das würde diesen Mangel nicht beheben. Deshalb müsste dieser Satz gestrichen werden.

Vors. **Sebastian Edathy**: Wenn ich das richtig sehe Herr Dr. Helmbrecht, ist noch die

Frage bezüglich China und Hell- und Dunkelfeld offen? Nein Abg. Hofmann ist zufrieden mit der Beantwortung. Dann hat das Fragerecht jetzt die Fraktion DIE LINKE. Frau Abg. Jelpke, bitte.

BE **Ulla Jelpke** (DIE LINKE.): Danke, Herr Vorsitzender. Ich würde gerne Frau Brückner noch einmal fragen. Sie haben in Ihrer Stellungnahme beschrieben, dass Sie bereits eine Unklarheit einerseits mit dem Begriff „Protokolldaten“ sehen und andererseits sagen Sie aber auch, dass es die Probleme bei der automatisierten Auswertung der Protokolldaten gebe. Vielleicht können Sie das noch einmal erläutern auch im Hinblick auf die Möglichkeiten, dass Kommunikationsinhalte sichtbar gemacht werden können. Meine zweite Frage geht noch einmal an Frau Brückner und an Herrn Dr. Helmbrecht. Ich würde doch ganz gern noch einmal genauer nachfragen wollen, was eigentlich gegenwärtig zum Kommunikationsnetz des Bundes gehört und welche Schnittstellen es zu Nichtbundesinstitutionen gibt. Und von Herrn Prof. Dr. Pfitzmann und Herrn Dr. Breyer würde ich ganz gerne eine verfassungsrechtliche Würdigung des § 5 im Regierungsentwurf haben wollen und Sie bitten, wenn es denn eine ersatzlose Streichung gäbe, auszuführen, was denn die Alternativen wären.

Vors. **Sebastian Edathy**: Zur Beantwortung zunächst Frau Brückner, bitte.

SV **Annette Brückner**: Zu Ihrer Frage, Frau Abg. Jelpke, was Protokolldaten eigentlich sind, ist schon der Gesetzentwurf selbst zumindest ambivalent. Denn er spricht einmal von Protokolldaten im Zusammenhang mit sog. „Logfiles“ und einmal von Protokolldaten im Zusammenhang mit Datenübertragungsprotokollen. Beides muss natürlich unterschiedlich ausgewertet werden. Das muss gleich im Vorhinein gesagt werden. Um es kurz aus halbwegs technischer Sicht zu erklären, was eigentlich Protokolldaten von „Logfiles“ sind, so können Sie sich die so vorstellen, wie zeitlich sortierte Listen, in denen enthalten ist, welche Aktivitäten von Nutzern oder auch von Systemen durchgeführt werden. Solche Protokolldaten gibt es von Betriebssystemen. Das können Sie auf Ihrem eigenen Rechner nachschauen, wenn Sie ein Windows-System oder ein anderes System haben. Solche Protokolldaten kann man sich vorstellen bei Datenbanken, wo protokolliert wird, wann ein Benutzer sich dort anmeldet und abmeldet bis hin, zu welchen Daten er möglicherweise einpflegt und abfragt. Aber das sind alles diese Protokolldaten, die eigentlich nur zeitlich sortierte Aktivitätslisten liefern, und insofern zunächst einmal etwas Unkritisches sind, außer, dass sie natürlich, wenn es um die Auswertung geht, durchaus Bezug haben zu dem Fragekomplex, den Herr Dr. Breyer vorhin beantwortet hat, was nämlich in den Bereich der möglichen Leistungskontrolle von Mitarbeitern von Behörden geht, wenn man solche Protokolldaten auswertet. Das ist in dem Bereich, in dem ich arbeite, ein Dauerbrenner. Das kann man wirklich so sagen. Aber zurück noch einmal zu dem unterschiedlichen Begriff „Protokolldaten“. Ich habe diese kleine Puppe hier nicht unabsichtlich mitgebracht. Sie kennen die alle. Das ist eine russische Matroschka. Und damit komme ich auf den Begriff der Datenübertragungsprotokolldaten. Und diese Datenübertragungsprotokolldaten haben mit dem Protokollieren im Sinne von

Aktivitäten und zeitlich sortierten Listen an dieser Stelle überhaupt nichts zu tun. Sondern da kommt der Begriff „Protokoll“ mehr eigentlich aus dem semantischen Umfeld: Ich halte mich an ein Protokoll, ich halte mich an ein Regelwerk. Ich bin höflich genug oder auch konform mit den Regeln, indem ich als Sender bzw. Empfänger einer Kommunikationsnachricht die entsprechenden Regeln einhalte. Daher kommt Datenübertragungsprotokoll. Und was hat es nun mit dieser Matroschka zu tun? Das kommt jetzt zu Ihrer dritten Frage. Nämlich, was haben die Datenübertragungsprotokolle eigentlich mit der Möglichkeit zu tun, Kommunikationsinhalte auszuwerten? Man muss sich dazu vorstellen, dass Datenübertragungsprotokolle nach einem sog. Schichtenprinzip aufgebaut sind. Und jede dieser Schichten ist zuständig für eine ganz bestimmte Aufgabe, die zu erledigen ist. Wir gehen also einmal von dem Beispiel aus, dass Sie eine E-Mail irgendwo hinschicken, dann ist diese E-Mail hier die kleinste Puppe. Und diese kleinste Puppe, die Sie lesen können und die dann hoffentlich auch ihr Kommunikationspartner auf der anderen Seite lesen kann, wird auf dem Weg der Datenübertragung verpackt. Man spricht auch aus dem Grund von „Paketvermittlung“. Da kommt also eine weitere Puppe drum herum. Die sorgt bspw. dafür, dass die Adresse, die Sie eingegeben haben, irgendwas Linksfraktion.de, weil Sie zu Hause arbeiten, bis die aufgelöst und umgesetzt wird in die sog. IP-Adresse. IP-Adresse heißt also, die numerische, die auf dem technischen Datenübertragungsweg verständlich ist. Und diese IP-Adresse wird eingeführt in das Datenpaket oder in die vielen Datenpakete, die Sie wegschicken. Dann kommt die nächste Schicht, also die nächste Matroschkapuppe, die packt da etwas anderes drum herum. Die Pakettierung, das tut jetzt aber nichts zur Sache, was das ist. Wichtig ist nur, es findet hier eine fortgesetzte Pakettierung statt und dann auf dem Weg zum Empfänger auch wieder ein Entpacken, so dass der Empfänger nur noch liest, was Sie ihm in der E-Mail geschickt haben. Das kann man am besten damit vergleichen, wenn Sie eine CD in Ihren CD-Player einlegen, dann interessiert Sie nicht die Bohne, was da an digitalen Signalen irgendwo von irgendwelchen technischen Komponenten abgestrahlt, empfangen oder ausgewertet wird, sondern Sie wollen Mozart oder Pink Floyd oder was auch immer hören. Und das ist das Einzige, was Sie interessiert. Und ähnlich ist das auch mit diesen Datenübertragungsprotokollen mit entsprechenden Protokollgeräten, sog. „Protocol Analizern“, mit denen man sichtbar machen und nachvollziehen kann, was auf diesen verschiedenen Ebenen der Datenübertragung technisch geschieht. Und damit kann man auch ohne weiteres nachvollziehen, welche IP-Adressen tatsächlich betroffen sind, denn man kann sie auch „faken“, also verfälschen. Und man kann nachvollziehen, welche Daten dort enthalten sind. Und das ist das Gefährliche an der Sache.

Vors. **Sebastian Edathy**: Herr Abg. Dr. Dieter Wiefelspütz, Sie haben nicht das Wort. Vielen Dank. Herr Dr. Helmbrecht.

SV **Dr. Udo Helmbrecht**: Vielen Dank. Ich finde das Beispiel sehr schön, weil es die Schwierigkeit besonders verdeutlicht. Wenn jetzt irgendwo in dieser Puppe ein Schadprogramm steckt, stellt sich die Frage: Wie kommen wir daran? Und dann interes-

sieren uns eben nicht die personenbezogenen Daten, die sich auf anderen Ebenen dieser Puppe befinden. Zu Ihrer Frage, wo Kommunikation stattfindet: Ich gebe Ihnen ein paar Beispiele, ich glaube dann bekommt man eine Vorstellung davon. Eine wesentliche Aufgabe für uns ist der Betrieb des Regierungsnetzes, der sog. Informationsverbund Bonn-Berlin (IVBB). Dieser wurde zwischen Bonn und Berlin vor zehn Jahren aufgebaut, und an ihn sind die meisten Ministerien und Bundesoberbehörden angeschlossen. Dann gibt es eine ganze Reihe von Beziehungen zu anderen Landesbehörden, so dass Kommunikation von Bundes- zu Landesbehörden stattfindet. Des Weiteren gibt es Verbindungen, z. B. von jeder Botschaft zum Auswärtigen Amt in Berlin. Insofern handelt es sich um ein weit verzweigtes Netz. Die Bundeswehr betreibt eigene Netze. Also ist das BSI im Wesentlichen verantwortlich für das Regierungsnetz Bonn-Berlin, aber natürlich auch für die Schnittstellenübergänge zuständig. Eine große Schwierigkeit ist, dass es noch viele „Stand-alone"-Systeme gibt, wo bspw. in Behörden oder Liegenschaften Rechner direkt am Internet angeschlossen sind, die keine Beziehungen zum Netz auf direktem Wege haben. Aber wenn Sie an das Schadprogramm Conficker denken, können Sie mit einen USB-Stick Daten von A nach B tragen, und damit können Sie natürlich auch Schadprogramme in das Regierungsnetz übertragen. Also insofern gibt es eine Vielzahl von Schnittstellen. Darüber hinaus, im Gesetz ist von informationstechnischen Systemen die Rede: Wenn der Bund Portale betreibt, in denen er Angebote für den Bürger anbietet, bedeutet dies, dass der Bürger damit auch eine Beziehung Bürger-Portal-Bundesverwaltung eingeht. Beispielsweise wenn Sie auf sozialversicherungspflichtige Daten zugreifen, oder mit anderen Behörden kommunizieren etc. Auch in diesen Fällen müssen wir für die Sicherheit der Daten der Bürger sorgen.

Vors. **Sebastian Edathy**: Beantwortet das Ihre Fragen, Frau Jelpke?

Abg**. Ulla Jelpke**: Frau Brückner hat mir das noch nicht beantwortet.

SV **Annette Brückner**: Ich bedaure das. Ich habe tatsächlich die Frage übersehen. Auch ich kann es mehr als Frage denn als Feststellung formulieren. Es ist im März dieses Jahres ein Beschaffungsvorhaben entschieden worden, so muss man es wohl sagen, über das sog. DOI-Netz. Dieses DOI-Netz, wenn man die Beschreibungen richtig liest, ist ein Vorhaben im Bereich des Gesamtvorhabens des Bundes über „Deutschland Online Infrastruktur". Wenn man diese Beschaffungsentscheidung liest, ergibt sich daraus, dass da ein „Backbone", also eine Art Rückgrat, installiert werden soll, das in Zukunft die Netze sämtlicher Verwaltungen miteinander verbinden soll. Und daraus kann man eigentlich nur interpretieren, dass die erwähnten Kommunikationsnetze des Bundes, wie das IVBB-Netz, das Herr Dr. Helmbrecht erwähnte, auch das Bundeswehrnetz und ähnliches, und eben auch Landesnetze für Länderverwaltungen und von Kommunalverwaltungen an dieses DOI-Netz angeschlossen werden. Jedenfalls liest es sich so in geradezu euphorischen Werbeschriften, die man dazu im Internet findet. Und wenn das so ist und wenn das so stimmt, stellt sich die Frage, welche Auswirkungen die Maßnahmen, die für das BSI in

diesem Gesetzentwurf beschlossen werden sollen, dann auch auf Länder- und Kommunalverwaltungen haben werden. Danke sehr.

Vors. **Sebastian Edathy**: Vielen Dank. Herr Prof. Dr. Pfitzmann, bitte. Herr Dr. Helmbrecht war noch nicht fertig, bitte.

SV **Dr. Udo Helmbrecht**: Ich möchte das noch einmal mit einem Satz ergänzen. Das Gesetz macht deutlich, dass es um die Informationssicherheit des Bundes geht. D.h., wir kommunizieren natürlich an vielen Stellen. Beispielsweise zum weltweiten Internet, zu Landesbehörden und zu Firmen, die weitere Kommunikationsbeziehungen haben. Das Wesentliche ist, dass wir hier über den Schutz der Kommunikationstechnik des Bundes reden. Und es gibt im Gesetz Ausnahmen für das Parlament, den Bundestag etc. Unter die Befugnisnorm fallen auch die Netzübergänge von der Bundesverwaltung in andere Netze.

Vors. **Sebastian Edathy**: Herr Prof. Dr. Pfitzmann, bitte.

SV **Prof. Dr. Andreas Pfitzmann**: Sie fragen mich nach einer verfassungsrechtlichen Würdigung von § 5. Ich bin kein Verfassungsrechtler. Ich bin nicht einmal Jurist. Ich bin einfach Informatiker. Wenn ich den Text lese und mir überlege, welche Schadprogramme oder Rahmen für Schadprogramme könnte man schreiben, dann lesen wir in Abs. 3: „Eine über die Absätze 1 und 2 hinausgehende Verwendung personenbezogener Daten ist nur zulässig, wenn bestimmte Tatsachen den Verdacht begründen“. Da kann ich jetzt als Informatiker kreativ werden und mir solch ein Rahmenprogramm einfallen lassen, das habe ich in den schriftlichen Unterlagen auch getan, „dass, ... 3. sich aus ihnen Hinweise auf ein Schadprogramm ergeben können“, ist dann sicherlich unbeschränkt möglich. Und ich kann den Rahmen auch so schreiben, dass das über einen beliebig langen Zeitraum möglich wäre. Und dann merkt man natürlich, dass diese Regelung, so wie ich das als juristischer Laie lese, aber ich versuche sie wirklich gründlich zu lesen, dass sie ins Uferlose geht. Meine Vermutung wäre, dass das Verfassungsrechtlern nicht gefallen wird, wenn ich das ganz vorsichtig äußern darf als Informatiker.

Vors. **Sebastian Edathy**: Herr Dr. Breyer, bitte.

SV **Dr. Patrick Breyer**: Danke. Sie hatten zwei Fragen an mich gerichtet. Die verfassungsrechtliche Würdigung dieses § 5 und Alternativen, wenn wir ihn streichen würden. Was die verfassungsrechtliche Würdigung angeht. Es ist erst einmal wichtig, sich im Klaren zu sein, was der überhaupt bedeutet, was da drinsteht. Und da hatte ich vorhin schon ein paar Worte dazu gesagt. Meines Erachtens würde die Nummer 1, Protokolldaten zu erheben, es ermöglichen, das gesamte Surfverhalten auf Bundesportalen in personenbezogener Form zu speichern, und die Daten müssten dann „unverzüglich“ ausgewertet werden. Es ist von Gerichten schon dahingehend ausgelegt worden, dass „unverzüglich“ sieben Tage heißen soll. D.h., schon diese

Nummer 1 würde eine Vorratsdatenspeicherung des Surfverhaltens ermöglichen. Bei Nummer 2 soll eine automatisierte Auswertung mit Hilfe von Software erfolgen, um Datenströme auf Schadsoftware zu überprüfen, und bei Absatz 2 soll eine Vorratsspeicherung der Protokolldaten noch für einen Zeitraum von bis zu drei Monaten erfolgen, und zwar unter Voraussetzungen, die so niedrig sind – Herr Prof. Dr. Pfitzmann hat es schon gesagt –, dass flächendeckend und permanent eine Aufzeichnung des Surfverhaltens möglich wäre. Verfassungsrechtlich kann ich ein paar Entscheidungen des Bundesverfassungsgerichts dazu anführen: Wir haben einmal die Entscheidung zur Videoüberwachung in Bayern, aus der hervor geht, dass das Merkmal „erforderlich“ nicht reicht, um solch eine Eingriffsermächtigung zu begrenzen. Wir haben die Entscheidung zur Rasterfahndung, aus der hervor geht, dass bestimmte Gefahrenstufen vorhanden sein müssen und dass man nicht ins „Blaue“ hinein solche Maßnahmen zulassen darf. Wir haben die Entscheidung zum Kfz-Massenabgleich gerade vom letzten Jahr, in der es ausdrücklich im Leitsatz heißt, dass solche Maßnahmen nicht flächendeckend und auch nicht anlasslos vorgenommen werden dürfen. Damit kollidiert diese Bestimmung massiv. Und wir haben letztlich die einstweiligen Anordnungen zur Vorratsdatenspeicherung, die deutlich machen, dass das Einzige, was diese Regelungen stützt, das zwingende Europarecht ist, welches die Vorratsdatenspeicherung vorgibt. Hier, bei diesem § 5, haben Sie kein Europarecht, das sich anführen lässt. D.h., die Norm würde der umfassenden Kontrolle des Bundesverfassungsgerichts unterliegen und in dieser Fassung mit Sicherheit keinen Bestand haben, weil sie nicht anlassbezogen ist und weil sie keine enge und konkrete Zweckbindung vorsieht und weil sie im Übrigen, ich hatte das vorhin schon näher ausgeführt, aus meiner Sicht auch nicht geeignet ist, um Sicherheitslücken überhaupt durch eine Protokollierung zu schließen. Was wären die Alternativen, wenn man diesen § 5 streichen würde, der übrigens bisher in dieser Form nicht besteht und bisher kommen die Bundesbehörden auch ohne diese Vorschrift gut zurecht?

– Zwischenrufe, nicht rekonstruierbar –

SV **Dr. Patrick Breyer**: Die Alternative zur Protokollierung des Surfverhaltens ist eben, keine Protokollierung vorzunehmen, und zwar keine personenbezogene. Ich hatte eingangs schon genannt, dass etwa das BMJ, der Bundesdatenschutzbeauftragte oder selbst das Bundeskriminalamt das Surfverhalten auf ihren Seiten nicht protokollieren und das offensichtlich auch nicht erforderlich ist, um Störungen zu beheben. Stattdessen muss eben die Software regelmäßig aktualisiert, Sicherheitslücken geschlossen und ein Grundschutz vorgesehen werden, wie Herr Prof. Dr. Pohl auch schon näher ausgeführt hat. Und die Alternative zur automatisierten Auswertung auf Schadprogramme ist eben, dass dies, wie bisher, bei den Behörden passiert oder in Abstimmung mit den Behörden, die Empfänger der Nachrichten sind, und auch in Abstimmung dann ggf. mit deren Personalräten, und nicht dass das zentral das BSI erledigt. Aus meiner Sicht ist auch eine zentralisierte Infrastruktur anfälliger für Angriffe und ist daher eine dezentrale Lösung vorzuziehen. Hier sind

bisher zwei konkrete Beispiele genannt worden in der Anhörung. Herr Dr. Helmbrecht hat eine E-Mail angeführt, an die ein Trojaner angehängt ist. Dafür brauchen Sie diese Norm überhaupt nicht, denn in der E-Mail sind alle Daten sowieso vorhanden, auch die IP-Adresse des Absenders. Da brauchen Sie keine Protokollierung. Das zweite Beispiel war, dass man infizierte Webseiten erkennen will. Wenn wirklich eine Webseite mit einem Sicherheitsrisiko verbunden ist, müssen Sie sofort die Software aktualisieren, damit der Browser sich nicht auf diese Art und Weise ausnutzen lässt. Sie können die Webseite bis dahin auch für Zugriffe sperren. All das ist bisher schon möglich, da braucht es keinen § 5 und insbesondere keine Protokollierung des Surfverhaltens.

Vors. **Sebastian Edathy**: Vielen Dank. Das Wort hat der Kollege Abg. Wolfgang Wieland, Fraktion BÜNDNIS 90/DIE GRÜNEN.

BE **Wolfgang Wieland** (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank, Herr Vorsitzender. Es ist immer etwas Besonderes hier als Letzter fragen zu dürfen. Aber heute ist es ganz besonders schön, weil man zu Beginn gehört hat – da gab es zwar schon eine Vorankündigung, es könnte so kommen –, dass das Telemediengesetz nun kein Thema mehr ist. Wäre nett gewesen, es auch den Sachverständigen zu sagen, dann hätten sie nicht gegen offene Türen angeschrieben, wobei auch die Frage ist, inwieweit sie Prokura haben, meine Herren, mir das zu erklären.

– Zwischenrufe, nicht rekonstruierbar –

BE **Wolfgang Wieland**: Nein, das würden wir gerne wissen. Inwieweit das auch verbindlich bleiben wird. Weil wir hier schon ausgehandelte Gesetzentwürfe hatten, von den es dann hieß, die dürfen wir dann doch nicht einbringen. Es wäre besser gewesen, es förmlicher zu machen. Und nun hier ad hoc zu hören, auch die Anonymisierung und Pseudonymisierung einführen zu wollen. Was soll man denn damit anfangen. Wir können es doch gar nicht beurteilen. Gleichzeitig fragt der Kollege Abg. Hofmann weiter nach Benachrichtigungen. Wenn ich konsequent anonymisiere, dann muss ich doch niemanden benachrichtigen: „Wir haben Ihre Daten anonymisiert“. So konsequent soll es offenbar nicht erfolgen. Eigentlich müssten wir jetzt eine Befragungsrunde der beiden Koalitionsvertreter machen, um zu wissen, welche Fragen dann noch sinnvoller Weise an die Sachverständigen zu stellen sind. Bei aller Liebe für Progressivität und dass Sie hier Auszeiten nehmen und miteinander tuscheln. So ist das kein Vorbild, Herr Kollege Abg. Hofmann und Herr Kollege Abg. Binninger, wirklich nicht, auch nicht gegenüber den Sachverständigen.

– Zwischenrufe, nicht rekonstruierbar –

BE **Wolfgang Wieland**: Schreiben Sie weiter an ihren Kommentaren. Sichern Sie alle Texte ab und gehen Sie offline, wer weiß, was kommt, die Warnungen haben Sie gehört, Herr Kollege. Die rudimentär nur noch möglich sind. Also wenn ich nicht weiß,

was kommt, weiß ich wirklich nicht, ob das alles die Gefahren sind. Wir haben nun sehr ernstzunehmende Zuschriften bekommen von Anwaltsvereinen, von Presseorganisationen etc. Da muss man ein bisschen verantwortlicher mit umgehen. Dennoch die Frage an Herrn Dr. Helmbrecht: Warum müssen Sie eigentlich, um die Aufgaben Ihrer Behörde wahrzunehmen, Daten an Dritte weitergeben, an Strafverfolgungsbehörden oder an Nachrichtendienste? Warum ist das notwendig? Das wird hier immer als Zufallsfund bezeichnet. Meines Erachtens lässt das Gesetz sogar ein systematisches Anfragen dieser Strafverfolgungsbehörden und der Nachrichtendienste an Sie zu, dann hat das mit Zufall gar nichts zu tun, sondern dann werden die Dateien, die Sie anlegen, angezapft. Zweite Frage, die Formulierung des § 7: Kann es auch sein, dass man sie so lesen muss, solange die Bundesregierung selber Sicherheitslücken nutzt, z.B. der Bundesnachrichtendienst, wollen wir sie nicht veröffentlichen. Oder ist das nur bösartig gedacht. Bei Herrn Prof. Dr. Pohl hörte ich das ein bisschen in diese Richtung heraus. Wenn man es nicht so will, warum formuliert man das dann nicht? Sie werden in dem Moment veröffentlicht, wo man Abhilfemöglichkeiten zur Verfügung stellen kann oder wo man sie in absehbarer Zeit nicht zur Verfügung stellen kann, aber warnen muss man damit nicht, dass eintritt, was Herr Prof. Dr. Pohl geschildert hat. Eine Frage an Herrn Dr. Breyer: Sie haben uns ein schönes Schema zur Verfügung gestellt, was der Bundesrat will, was der Innenausschuss des Bundesrates zum Telemediengesetz will. Was kann man denn da auf das BSI-Gesetz übertragen? Mir ist z.B. die fehlende Bußgeldmöglichkeit aufgefallen. Wir reden hier immer, die öffentlich Bediensteten werden sich demnächst wie die Bahn- und wie die Telekom-Beschäftigten behandeln lassen müssen, dann ist auch die Frage spannend, was kann man denn gegen die tun, die möglicherweise verstoßen gegen die Möglichkeiten, die dieses Gesetz hier schafft? Und last but not least die letzte Frage an den Datenschutzbeauftragten Peter Schaar, ob er irgendeine Notwendigkeit sieht, die Aufgaben dieses Gesetzes tatsächlich nur auf Abwehr von Angriffen zu beschränken und keine weiteren Zwecke wie Strafverfolgung, wie Übermittlung nachrichtendienstlichen Wissens damit zu verbinden. Also eine geschlossene Regelung, wie wir sie, ich ziehe jetzt einmal einen Vergleich, bspw. bei der Autobahn-Maut hatten, hier zu schaffen.

Vors. **Sebastian Edathy**: Herr Dr. Helmbrecht, bitte.

SV **Dr. Udo Helmbrecht**: Vielen Dank. Warum müssen wir Daten weitergeben? Eine Vorbemerkung dazu: Das BSI ist eine präventive Behörde, die Vertrauen genießt, diese Reputation müssen wir uns immer wieder erarbeiten. Wenn wir beispielsweise Kryptographie zur Verschlüsselung entwickeln, wenn wir Informationen an die Wirtschaft, den Bürger etc. weitergeben, dann dient dies unserem präventiven Image. Insofern können wir uns als BSI gar nicht leisten, an der einen oder anderen Stelle nicht mit diesem Bewusstsein umzugehen, weil sich das in der Szene schnell genug herumsprechen würde. Wenn wir aber nun ein Schadprogramm entdeckt haben und von diesem eine andere Behörde betroffen ist, das kann eine Bundes- oder eine Landesbehörde sein, dann wollen wir diese Informationen weitergeben. Insofern dient

es dazu, dass die anderen sich auch schützen können, wenn sie betroffen sind. Wenn Sie dieses Beispiel nehmen, dann ist es heute naiv zu glauben, dass man mit den gängigen Mitteln, die es am Markt gibt, sich genügend schützen kann. Daher müssen wir in der Bundesverwaltung mehr tun. Am Ende brauchen wir bessere Virenschutzprogramme und Firewalls für uns selber, als das am Markt gängig und üblich ist.

BE **Wolfgang Wieland**: Das Thema, ob Sie auf die Lücken deswegen nicht sofort hinweisen müssen nach dem Gesetzestext, weil bspw. der Bundesnachrichtendienst sie nutzt in den Rechnern anderer Regierungen?

SV **Dr. Udo Helmbrecht**: Also wir als BSI tun das nicht. Das machen wir weder in der Diskussion mit dem BKA noch in dieser Diskussion hier. Wir wollen in der Szene mit unserem guten Ruf als präventive Behörde erscheinen, wir können uns das gar nicht leisten, solche Dinge zu tun. Dann würden die anderen Dinge, wie Zertifizierung, Information der Gesellschaft oder Zusammenarbeit mit der Forschung sowie Industrie gar nicht funktionieren.

BE **Wolfgang Wieland**: Herr Dr. Helmbrecht, das war auch nicht die Frage.

Vors. **Sebastian Edathy**: Herr Abg. Wieland melden Sie sich doch bitte, wenn Sie weitere Nachfragen haben.

BE **Wolfgang Wieland**: Beide Nachfragen, sorry, wurden nicht beantwortet. Die erste zielte auf die Weitergabe personenbezogener Daten an Strafverfolgungsbehörden und an Nachrichtendienste, nicht, dass er andere Behörden vor Schadware warnt, das ist seine Aufgabe. Meine Frage war, ob er zur Wahrnehmung dieser Abwehr vor Schadware Aufgaben, Daten zu diesen Zwecken weitergeben muss. Ob da irgendein Zusammenhang besteht. Ich will mir nur erklären, warum das in einen Gesetzentwurf gelandet ist.

SV **Dr. Udo Helmbrecht**: Die Problematik ist ja, dass mit solchen Fragen am Ende unterstellt würde, der einzige Zweck dieses Gesetzes wäre, dass wir personenbezogene Daten sammeln wollen. Der Prozess der Auswertung ist weitestgehend automatisiert. Wenn man feststellt, dass der Verdacht auf ein Schadprogramm besteht, dann soll dieses weiter untersucht werden. Und wenn sich am Ende herauskristallisiert, dass eine strafbare Handlung mit einem Schadprogramm zur Ausnutzung einer Schwachstelle durchgeführt worden ist, dann hat man ganz am Ende mit all diesen Mitteln, die wir hier diskutiert haben, bis dahin nur wirklich den gefunden, der wirklich kriminell oder nachrichtendienstlich gehandelt hat. Wenn man ganz am Ende nun weiß, diese E-Mail, als Beispiel, kommt von dem Herrn X aus dem Land Y, dann muss man sich fragen, ist das in Deutschland, ist das strafverfolgungsrechtlich relevant? Und muss man das zur Anzeige bringen? Und wenn es dann am Ende eine nachrichtendienstliche Spionageaktivität war, dann muss man das doch auch weitergeben. D. h., ganz am Ende dieser Kette, wenn alles berücksichtigt ist, Automati-

sierung, Pseudonymisierung etc. und man eine E-Mail gefunden hat, die kriminellen Ursprungs ist, dann geht es doch darum, diese Daten weiterzugeben, um das auch strafrechtlich zu verfolgen.

Vors. **Sebastian Edathy**: Vielen Dank. Herr Dr. Breyer, bitte.

BE **Wolfgang Wieland**: So steht das wirklich nicht im Gesetz.

Vors. **Sebastian Edathy**: Herr Abg. Wieland. So geht es nicht. Herr Dr. Breyer, bitte.

SV **Dr. Patrick Breyer**: An mich hatten Sie die Frage gerichtet, inwiefern das Schema, was ich auf Seite 2 meiner Stellungnahme entwickelt hatte, auch auf das BSI-Gesetz übertragbar ist. Ich will gerne versuchen, da auch § 5 BSI-Gesetz eine Surfprotokollierung einschließt, diese Kriterien einmal darauf anzuwenden. Also der § 5 legt erstens nicht fest, aus welchem Anlass die Nutzungsprotokolle erstellt werden dürfen. Und legalisiert deswegen, meiner Befürchtung nach, eine permanente flächendeckende Surfprotokollierung. Und wenn Sie die Stellungnahmen anderer Verbände oder des Anwaltsvereins sehen, ist nicht nur meine Auslegung so, sondern auch andere lesen das so, dass tatsächlich eine permanente und flächendeckende Protokollierung damit erfolgen würde. Zweitens ist die Protokollierung auch nicht auf den Einzelfall beschränkt. Drittens ist die maximale Aufbewahrungsdauer zwar festgelegt, aber nur im Absatz 2 und auf drei Monate, was natürlich völlig inakzeptabel ist. Wenn man im Einzelfall tatsächlich konkret protokollieren will, weil ein aktueller Angriff oder eine aktuelle Sicherheitslücke vorhanden ist, reicht es natürlich, das am folgenden Tag jeweils zu bearbeiten. Es wäre auch viel zu spät, darauf erst nach Tagen oder Wochen zu reagieren. Viertens ist eine Zweckbindung nicht vorgesehen, sondern, wie Sie schon gesagt hatten, eine Öffnung für ganz andere Zwecke. Fünftens ist auch die Weitergabe von Nutzungsprotokollen nicht ausgeschlossen und die Vertraulichkeit der Internetnutzung nicht garantiert. D.h., wenn ich auf der Seite des Bundesamt für gesundheitliche Aufklärung mich über Drogen oder ähnliches informiere, ist nicht gewährleistet, dass das anonym bleibt und dass das auch wenigstens bei der Zentrale bleibt. Sechstens, die Bußgeldpflicht wäre natürlich wenig sinnvoll für das BSI, wenn also der Bund an sich selbst ein Bußgeld zahlen muss. Hier müsste man etwa mit einem Schadenersatzanspruch der Betroffenen arbeiten. Wir fordern schon lange, dass diejenigen, die von Datenmissbrauch betroffen sind, eine Pauschalsumme auch für ihre immateriellen Schäden bekommen. Vielleicht 100 oder 200 Euro. Das könnte durchaus eine Abschreckungswirkung auch beim Bund entfalten. Und der siebte Punkt, dass Internetprotokolladressen dem Datenschutz und diesen Regelungen unterliegen, ist nicht ausdrücklich vorgesehen. Man sollte das im Telemediengesetz klarstellen, weil im Moment es leider noch Anbieter gibt, die sagen, unsere Surfprotokolle unterfallen gar nicht dem Datenschutz, weil die nicht personenbezogen seien. Darüber herrscht Streit, und es wäre wichtig, wenn man das gesetzlich klarstellen würde.

Eine letzte Anmerkung: Vor wenigen Wochen ging durch die Medien, dass das Bundeskriminalamt seine Praxis eingestellt hat, die Besucher von Fahndungsseiten nachzuverfolgen, und dabei wohl Dutzende und Hunderte von Pressevertretern und sonstige unschuldige Menschen, die sich einfach dafür interessiert haben, ermittelt hat. Mit diesem § 5 würde genau das wieder eingeführt: Es wird alles protokolliert, worauf man surft, auch auf die Fahndungsseiten des Bundeskriminalamts. Und wie Sie gesagt haben, könnte das Bundeskriminalamt die Daten auch anfordern. Und sie könnten dann übermittelt werden nach diesem Absatz 4. Und deswegen wäre es aus meiner Sicht ein Rückschritt.

Vors. **Sebastian Edathy**: Herr Schaar, bitte.

BE **Peter Schaar**: Vielen Dank. Herr Abg. Wieland, Sie haben nach der Notwendigkeit der Übermittlung der Daten gefragt, und zwar der personenbezogenen Daten an andere Behörden. Das ist erst einmal eine Zweckänderung. Es geht hier nicht um die Abwehr von Schadprogrammen und Gefahren für die Kommunikationstechnik des Bundes, sondern es geht um andere Zwecke, die damit verfolgt werden sollen. Insofern handelt es sich um eine ganz klassische Zweckerweiterung. Ob diese Zweckerweiterung einmal erforderlich ist, ist eine Frage, die man fachlich diskutieren muss. Die zweite Frage ist, inwieweit sie verfassungsrechtlich vertretbar ist. Und dieses ist wiederum abhängig einerseits von der Schutzbedürftigkeit der Daten. Denn es handelt sich um einen weiteren Eingriff in den Datenschutz, also in das Recht auf informationelle Selbstbestimmung. Dieses wiederum legt die Frage nahe, was sind das für Daten, die dort übermittelt werden. Und das muss abgewogen werden gegen die berechtigten öffentlichen Interessen, die eine entsprechende Übermittlung rechtfertigen könnten. Die Daten, um die es sich hier handelt, können einerseits Protokolldaten der Kommunikation sein, also Telekommunikationsverkehrs- oder Nutzungsdaten von Telemedien. Es können aber auch Inhalte sein. D.h., wenn sich bspw. das Schadprogramm in einer E-Mail befindet, als Anhang bspw., Herr Dr. Helmbrecht schickt mir eine E-Mail und ohne dass er das weiß, ist der Anhang der E-Mail infiziert mit einem ganz gefährlichen Trojaner. Gleichwohl kann das ein hochsensibler Text sein. Die Privatnutzung ist bei uns auch zugelassen. Vielleicht haben wir auch private Kontakte. Das können auch höchst sensible Daten sein, die den Kernbereich der Privatsphäre betreffen. D.h., das Fernmeldegeheimnis wäre in einem solchen Falle betroffen. Die Hürden müssten, um einmal eine Vergleichbarkeit zu machen, praktisch genauso hoch sein, wie sie bei sonstigen Eingriffen in das Fernmeldegeheimnis angebracht sind. Die Regelung ist hier etwas undifferenziert, muss ich sagen, weil sie hier nicht dieser unterschiedlichen Sensibilität der verschiedenen Daten, die hier in Frage kommen, Rechnung trägt. Im Hinblick auf die Inhalte ist sicherlich die Hürde noch wesentlich höher als im Hinblick auf die Verkehrsdaten, und bei den Nutzungsdaten ist es irgendwo dazwischen. Man müsste das noch einmal sehr genau anschauen. Wichtig ist für mich allerdings die Aussage, dass für den Primärzweck des Gesetzes diese Übermittlung nicht erforderlich ist. Zumal die Sekundärgefahren, die aus diesen Schadprogrammen ausgehen können,

bspw. für die Funktionsfähigkeit irgendeiner technischen Anlage, auch ohne personenbezogen zur Kenntnis gebracht werden können. Wenn es sich um personenbezogene Daten handelt, dann stellt sich aber auch die Frage nach der Erforderlichkeit. Ich habe das anfangs erst einmal unterstellt. Man muss also fragen, wessen personenbezogene Daten werden dort übermittelt. Da hat die Anhörung einiges für mich klargemacht, was ich so vorher nicht in der Deutlichkeit gesehen habe, dass jedenfalls die Angreifer praktisch nicht zu identifizieren sein werden, wenn es sich um solche gezielten Angriffe handelt, die hier speziell abzuwehren sind. Das hat nicht nur Herr Prof. Dr. Pohl ausgeführt, sondern auch Herr Dr. Helmbrecht hat dem zugestimmt, dass das nicht das Ziel sein kann. Dann stellt sich mir die Frage, wenn es gar nicht darum geht, den Angreifer ausfindig zu machen, sondern nur einen Dritten, der möglicherweise Empfänger dieser E-Mail ist, also im Grunde Opfer, ob das tatsächlich angemessen ist. Ich weiß es nicht. Ich denke, das müsste man noch einmal vertieft diskutieren.

Vors. **Sebastian Edathy**: Vielen Dank! Ich würde vorschlagen, dass wir jetzt eine offene Fragerunde machen, zumal wir maximal noch 30 Minuten zur Verfügung haben. Insofern bitte ich um Wortmeldungen. Abg. Wieland hat sich bereits gemeldet.

BE **Wolfgang Wieland**: Ich habe eine Frage an Prof. Poscher, weil der Kollege Binninger eben dazwischenrief: „Die Stelle müssen Sie mir zeigen“. Zwingt nicht § 5 Abs. 4 BSI-Gesetzentwurf, so wie er hier in der Formulierung vorgelegt wird, gerade dazu, die Möglichkeit anzunehmen, neben personenbezogenen Daten, die sich auf den Schadware-Angriff beziehen, auch Daten, die sich auf davon völlig abstrahierte andere Straftaten oder auf Bestrebungen gegen die freiheitlich demokratische Grundordnung beziehen, zur Verfügung zu stellen. Wobei möglicherweise offen ist, ob aktiv, passiv, oder auch beides. Jedenfalls, dass es hier ganz eindeutig um personenbezogene Daten geht, die über den Angriff hinausgehen.

SV **Prof. Dr. Ralf Poscher**: Ja, das war auch eine Frage, die ich mir gestellt habe. Ich bin auch davon ausgegangen, dass das Gesetz selber natürlich davon ausgeht, dass es nicht nur Protokolldaten sind. Die ganze Regelung zum Kernbereichsschutz würde ja sonst keinen Sinn machen. Deshalb habe ich danach gefragt, wie das technisch abläuft. Man hat mir das so erklärt, dass zunächst eine automatisierte Auswertung und dann eine Auswertung durch einen Beamten stattfindet. Da kann es sein, dass dann etwa eine E-Mail geöffnet werden muss. Der Beamte sieht sich die E-Mail natürlich nicht daraufhin an, ob irgendwelche geheimdienstlichen, betrügerischen, terroristischen oder sonstigen Aktivitäten besprochen werden. Er muss aber unter Umständen unweigerlich den Inhalt der E-Mail zur Kenntnis nehmen, oder er sieht das kinderpornographische Foto, in dem sich etwa ein Schadprogramm verbergen könnte. Das sind die Zufallsfunde, die bei solchen Verfahren auftauchen. Diese können auch Kernbereichsdaten enthalten. Insofern ist der Entwurf dem tatsächlichen Vorgehen angemessen und reflektiert dies auch, indem er eine Schutzregelung dafür vorsieht. Das ist im Grunde nicht anders als bei einer Wohnungsdurchsuchung, bei der man nach einer bestimmten

Sache sucht und noch andere findet. Die Frage, wie geht man mit diesen Zufallsfunden um, stellt sich in unserer Rechtsordnung an vielen Stellen. Wir beantworten sie im Bereich der Telekommunikation so, dass wir sehr hohe Hürden dafür ansetzen, wann wir diese Zufallsfunde für andere Zwecke verwenden dürfen. Die Hürden, die hier formuliert sind, sind aber erstens nicht ausreichend bestimmt formuliert und zweitens erreichen sie auch nicht die Schwelle, die auch verfassungsrechtlich dafür vorgesehen ist.

Vors. **Sebastian Edathy**: Frau Piltz, bitte.

BE **Gisela Piltz**: Der Kollege Wieland hatte Herrn Dr. Helmbrecht gefragt, warum genau man das eigentlich so machen müsse. Wenn ich mich richtig erinnere, haben Sie gesagt, weil es auf dem Markt so nichts gibt, was die Behörden bräuchten, bzw. sie brauchen mehr als das, was es bisher gibt. Deshalb meine Frage an die Professoren Pfitzmann und Pohl, ob sie diese Auffassung teilen. Wir haben uns mittlerweile eingearbeitet und wissen schon, was paketgebundene Verkehre sind und dass man dafür nicht mehr zur Post gehen muss, aber manchmal braucht man den Rat von Sachverständigen und deshalb wollte ich das noch einmal hinterfragen. Vielen Dank!

Vors. **Sebastian Edathy**: Herr Prof. Pfitzmann, bitte.

SV **Prof. Dr. Andreas Pfitzmann**: Wenn man die Frage so versteht: Kann die Verwaltung ohne irgendwelche Umschulungsaufwände und ohne, dass sich für den einzelnen Sachbearbeiter etwas ändert, umgestellt werden auf sichere Produkte jetzt und heute? So lautet die Antwort: Nein, das geht nicht. Wenn die Frage lautet: Ist es zumutbar für den einzelnen Sachbearbeiter, sich eventuell ein bisschen umzustellen, gewisse Abläufe zu ändern, können wir die Technikbeschaffung – wir können das, was wir haben, nicht einfach wegwerfen – und können wir die Softwarebeschaffung so ausrichten, dass wir innerhalb von zwei Jahren einen vernünftigen Zustand haben? Dann lautet die Antwort definitiv: Ja. Wer an der Stelle nein sagt und Verantwortung trägt, der muss sich fragen lassen, ob er seinem Amt gerecht wird.

Vors. **Sebastian Edathy**: Herr Prof. Pohl, bitte.

SV **Prof. Dr. Hartmut Pohl**: Ich habe die Frage so verstanden, dass das BSI unter Sicherheitsaspekten qualitativ bessere Produkte für die Bundesregierung entwickeln muss, als markterhältlich sind. Mir ist nicht bekannt, dass so etwas bisher vom BSI erstellt worden ist. Das muss es auch nicht, es kann ja im Verschlusssachenbereich, im Hochsicherheitsbereich für Verschlusssachen sein und es können Geräte sein, die nicht veröffentlicht sind. Allerdings würde ich mir dann wünschen, dass die deutschen Sicherheitsunternehmen über diese Aktivitäten informiert werden, damit auch die Unternehmen von diesen Erkenntnissen des BSI profitieren können. Schönen Dank!

Vors. **Sebastian Edathy**: Frau Jelpke, bitte.

BE **Ulla Jelpke**: Das Ziel: erkennen, eingrenzen, beseitigen von Störungen oder Fehlern – auch für mich hat die Anhörung bisher nicht das Ziel belegt, sondern eher das Gegenteil. Meine Frage richtet sich an Frau Brückner, die auf Seite 13 ihres Gutachtens diesen Punkt in Abs. 5.1.1 auch aufgegriffen hat. Wieso folgen daraus Onlinedurchsuchung oder Vorratsdatenspeicherung, auch von Webseiten, die keinerlei Bezug zur Kommunikationsstruktur des Bundes haben?

Vors. **Sebastian Edathy**: Frau Brückner, bitte.

SV **Annette Brückner**: Verstehe ich Sie richtig, dass Sie sich auf den Abs. 3.2.2 beziehen: „Auswertung der Inhalte, insbesondere enthaltener Links und „Absurfen" dieser Links"? Das mag ein Interpretationsproblem sein, aber was ich aus dem Gesetzentwurf bzw. aus der Begründung zum Gesetzentwurf entnehme, wird dort in der Begründung beschrieben, dass man sich Folgendes vorstellt. Das Szenario ist, ein Bundesbeamter surft irgendwo im Internet. Warum er das in der Dienstzeit tut, das bleibt außen vor, er tut es auf jeden Fall. Er gerät dann auf Seiten, die Links enthalten. Dann sieht diese Begründung vor, dass diese Links gespeichert und dann automatisiert abgesurft werden, um zu untersuchen, ob diese Links Schadprogramme enthalten, die ihrerseits Angriffe gegen Einrichtungen des Bundes starten könnten. So habe ich das verstanden. Wenn ich das falsch verstanden habe, dann machen Sie mir bitte klar, wie ich das richtig verstehen soll. Aber wenn Sie es auch so verstanden haben, dann finde ich es doch einigermaßen abenteuerlich, weil es Seiten sein können, die irgendwo sind. Ich stelle mir vor, dass eine Instanz des BSI auf Seiten auf irgendeinem Web-Rechner geht und dort erst einmal untersucht, ob es sich um Schadprogramme handelt. Ich frage mich unter anderem, wo ist da eigentlich die rechtliche Grundlage dafür, aber auch, wo ist die technische Grundlage? Vor allem, was soll dabei herauskommen? Man stellt dann fest, dass in Neuseeland irgendwo ein Link ist, den das BSI für sicherheitsrelevant hält...

- Einwand Abg. Gisela Piltz - nicht rekonstruierbar -

SV **Annette Brückner**: Ja, das auch. Ich meine, damit ist auch noch gar nicht erwiesen, ob dieser Link, der potenziell virulent ist, tatsächlich virulent geworden wäre. Mir erscheint das sehr weit hergeholt zu sein, aber vielleicht ist das ja auch ein Missverständnis.

Vors. **Sebastian Edathy**: Vielen Dank! Gibt es weitere Fragen? Herr Wieland, bitte.

BE **Wolfgang Wieland**: Ich habe noch einmal eine Frage an Herrn Prof. Poscher. Ich bleibe bei Ihrem Beispiel: der fleißige Beamte findet im Anhang Kinderpornographie. Er ist doch weder Polizist noch Staatsanwalt, er unterliegt nicht dem Legalitätsprinzip. Weshalb soll er die Möglichkeit haben, das weiter zu geben. Wenn man davon ausgeht, und Sie beschwören es ja selber in Ihrer schriftlichen Stellungnahme, dass hier in bisher nicht gekannter Weise Kommunikationsverhalten sämtlicher in Behörden arbei-

tender Bediensteter beispielsweise abgespeichert werden kann. Ich sage nicht, die beim BSI wollen das, aber die Möglichkeit besteht. Wenn ein so neuer Datenberg geschaffen wird, warum brauche ich zum Schutz der Datensicherheit diese Möglichkeit in Richtung Strafverfolgung und Nachrichtendienste?

Vors. **Sebastian Edathy**: Herr Prof. Poscher, bitte.

SV **Prof. Dr. Ralf Poscher**: Um die letzte Fragte zuerst zu beantworten: Sie brauchen die Zweckänderung, wie Herr Schaar das richtig beschrieben hat, bei der Verwendung der Daten nicht, um Gefahren für die Sicherheit der Informationssysteme abzuwehren. Das Problem bei diesen Zufallsfunden ist nur, wenn Sie das Wissen einmal haben – wie gehen Sie damit um. Das mag im Fall der Repression noch leichter erträglich sein. Stellen Sie sich aber vor, der Zufall will es, Sie entdecken den Anschlagsplan. Wollen Sie dann wirklich, dass die Beamten sich dumm stellen müssen, dass das Aufgefundene an niemanden weitergeleitet werden kann? Sie haben mit diesen Zufallsfunden immer ein schwieriges Problem. Die Lösung, die man bislang dafür gefunden hat – und jedenfalls das, was verfassungsrechtlich zulässig wäre – ist, dass bei bestimmten besonders schweren Straftaten, bei der Abwehr besonders dringlicher und weit reichender Gefahren die Verwertung der Zufallsfunde zugelassen wird. Allerdings liegt das Gesetz in der jetzigen Fassung weit unterhalb dieses Standards. An dieser Stelle muss man das Gesetz diesem verfassungsrechtlichen Standard erst einmal anpassen. Das Problem der Zufallsfunde kann man aber nicht wegdiskutieren. Wenn Sie es generieren, müssen Sie die Frage entscheiden, wie Sie damit umgehen wollen. Zu sagen, wir tun so, als wüssten wir von nichts, ist jedenfalls im präventiven Bereich kaum durchzuhalten.

Vors. **Sebastian Edathy**: Vielen Dank! Weitere Wortmeldungen liegen nicht vor, so dass wir am Ende der heutigen Anhörung angelangt sind. Ich darf mich sehr herzlich bedanken insbesondere bei den Herren Sachverständigen und bei der Sachverständigen Frau Brückner für das Kommen und dafür, dass Sie uns hier zur Beantwortung von Fragen zur Verfügung gestanden haben. Ich wünsche noch einen angenehmen weiteren Tagesverlauf. Die Sitzung ist geschlossen.

Ende der Sitzung: 16.40 Uhr