Deutscher Bundestag

Protokoll Nr. 75

16. Wahlperiode
Rechtsausschuss
(6. Ausschuss)

P r o t o k o l l *)

der 75. Sitzung

am 21. September 2007, 12.00 Uhr
Berlin, Paul-Löbe-Haus, Raum E 400

Beginn der Sitzung: 12.10 Uhr

Vorsitz: Vorsitzender Andreas Schmidt (Mülheim), MdB

Öffentliche Anhörung

Teil II: Telekommunikationsüberwachung, Vorratsdatenspeicherung

a) Gesetzentwurf der Bundesregierung **S. 1 - 59**

Entwurf eines Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG

BT-Drs. 16/5846

b) Gesetzesentwurf der Abgeordneten Jerzy Montag, Hans-Christian Ströbele, Wolfgang Wieland, weitere Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Entwurf eines Gesetzes zur Reform der Telekommunikationsüberwachung
(… Gesetz zur Änderung der Strafprozessordnung)

BT-Drucksache 16/3827

c) Antrag der Abgeordneten Jörg van Essen, Sabine Leutheusser-Schnarrenberger, Mechthild Dyckmans, weiterer Abgeordneter und der Fraktion der FDP

Reform der Telefonüberwachung zügig umsetzen

BT-Drucksache 16/1421

---

*) redigiertes Wortprotokoll

Vorsitzender Andreas Schmidt (Mülheim): Meine sehr geehrten Damen und Herren, liebe Kolleginnen und Kollegen. Ich darf Sie sehr herzlich begrüßen zu unserer heutigen Sachverständigenanhörung zum Thema Telekommunikationsüberwachung/ Vorratsdatenspeicherung, zum zweiten Teil unserer Anhörung. Ich heiße insbesondere die Herren Sachverständigen herzlich willkommen und darf Sie bitten, Platz zu nehmen. Herr Prof. Dr. Ronellenfitsch wird etwas später kommen. Ich schlage vor, trotzdem schon zu beginnen. Wir haben uns darauf verständigt, dass wir diese Anhörung handhaben wie im Rechtsausschuss üblich, d. h. wir werden mit einer kurzen Statementrunde der Sachverständigen beginnen, wobei jedes Statement maximal fünf Minuten nicht übersteigen sollte, damit wir auch noch genügend Zeit für die Fragen haben.

Ich bitte Herrn Dr. Breyer, Neue Richtervereinigung e.V., Arbeitskreis Vorratsdatenspeicherung, Berlin, mit seinem Statement zu beginnen. Herr Dr. Breyer, Sie haben das Wort.

SV Dr. Patrick Breyer: Vielen Dank Herr Vorsitzender. Nicht nur der Bundesdatenschutzbeauftragte hat die Vorratsdatenspeicherung einen Dammbruch genannt. In der Tat ist eine anlass- und verdachtsunabhängige Speicherung personenbezogener Daten ein Bruch mit Grundsätzen des Datenschutzes und des Verfassungsrechts. Ein Bruch unter anderem des Erforderlichkeitsgebots, der Datensparsamkeit, des Verbots der Speicherung personenbezogener Daten auf Vorrat zu noch unbestimmten Zwecken und ein Bruch des Verhältnismäßigkeitsgebots. Wir haben daneben auch einen quantitativen Dammbruch in der Hinsicht, dass erstmals über die gesamte Bevölkerung Informationen über unser tägliches Leben und unser Verhalten gesammelt werden. Meines Erachtens ist das die größte Informationssammlung überhaupt, die in Deutschland über die Bevölkerung existiert. Was ist nun der Anlass dafür, dass sich der Deutsche Bundestag mit diesem Vorschlag beschäftigt, nachdem er sich mehrere Male – zuletzt im Jahre 2005 – fraktionsübergreifend gegen eine Vorratsdatenspeicherung ausgesprochen hatte? Anlass ist eine EU-Richtlinie aus dem letzten Jahr. Die wird allerdings, wie ich gleich noch näher ausführen werde, meiner Überzeugung nach in wenigen Monaten von dem Europäischen Gerichtshof aufgehoben werden, und zwar weil sie einer Rechtsgrundlage entbehrt.

Zwischenzeitlich hat nämlich die große Kammer des Gerichtshofs mit Urteil vom 30. Mai 2006 zwei EG-Rechtsakte zur Fluggastdatenübermittlung in die USA für nichtig erklärt, die auch auf Artikel 95 des EG-Vertrages gestützt waren. Der Gerichtshof hat zur Begründung angeführt, es handele sich um eine Datenverarbeitung, *„die nicht für die Erbringung einer Dienstleistung erforderlich ist, sondern zum Schutz der öffentlichen Sicherheit und zu Strafverfolgungszwecken“* als erforderlich angesehen wird. Und wenn man dieses Abgrenzungskriterium auf die Vorratsdatenspeicherung überträgt, liegt auf der Hand, dass auch das eine Datenverarbeitung ist, die nicht für die Erbringung einer Dienstleistung erforderlich ist, sonst müsste sie nicht angeordnet werden, sondern eben für Strafverfolgungszwecke für erforderlich angesehen wird. Deswegen kann auch diese Richtlinie nicht auf Artikel 95 EG-V gestützt werden und wird mangels Rechtsgrundlage für nichtig erklärt werden.

Dann stellt sich die Frage, was bedeutet das für die Rechtslage in Deutschland? Falls die Richtlinie schon umgesetzt worden sein sollte zu diesem Zeitpunkt, bedeutet das, dass das Bundesverfassungsgericht freie Hand haben wird, dieses Gesetz am Grundgesetz, an den Grundrechten zu messen und da ist die Rechtsprechung ebenso deutlich. Ich will nur zwei Entscheidungen zitieren. Einmal den Beschluss des Ersten Senats des Bundesverfassungsgerichts vom 4. April letzten Jahres zur Rasterfahndung. Dort heißt es in Rdnr. 137: *„Verzichtet der Gesetzgeber auf begrenzende Anforderungen an die Wahrscheinlichkeit des Gefahreneintritts sowie an die Nähe der Betroffenen zur abzuwehrenden Bedrohung und sieht er gleichwohl eine Befugnis zu Eingriffen von erheblichem Gewicht vor, so genügt dies dem Verfassungsrecht nicht“*. Zum anderen das Urteil des Ersten Senats vom 12. März 2003. Es konkretisiert das für den Bereich der Telekommunikationsdaten. Dort heißt es in Rdnr. 75: *„Insofern genügt es verfassungsrechtlichen Anforderungen nicht, dass die Erfassung der Verbindungsdaten allgemein der Strafverfolgung dient. Vorausgesetzt sind vielmehr eine Straftat von erheblicher Bedeutung, ein konkreter Tatverdacht und eine hinreichend sichere Tatsachenbasis“* usw. Das heißt, auf der Grundlage dieser Rechtsprechung ist auch eindeutig, dass eine allgemeine verdachtsunabhängige Vorratsdatenspeicherung, die ja keinerlei Nähe der Betroffenen zu einer Gefahr oder

Straftat voraussetzt, nicht mit den Grundrechten, mit der Verfassung, vereinbar ist und vor dem Bundesverfassungsgericht keinen Bestand haben kann.

Jetzt ist aber die Frage, wie der Gesetzgeber zum jetzigen Zeitpunkt reagieren kann? Das ist keine ganz einfache Frage. Der Königsweg und meines Erachtens der einzig verfassungsrechtlich gangbare Weg ist im Moment derjenige, den der Gesetzgeber in richtiger und verantwortungsvoller Weise auch bei der so genannten Online-Durchsuchung gewählt hat, nämlich zu sagen, wir warten ab, wie die Gerichte entscheiden. Auch bei der Vorratsdatenspeicherung steht ja die Entscheidung des Europäischen Gerichtshofs über die Nichtigkeitsklage Irlands an. Sie ist Mitte nächsten Jahres zu erwarten. Ferner steht eine Entscheidung des Bundesverfassungsgerichts über eine Verfassungsbeschwerde gegen die Vorratsspeicherung von Bestandsdaten an, die im Telekommunikationsgesetz festgelegt ist. Diese Verfassungsbeschwerde hat das Bundesverfassungsgericht zugestellt. Es geht also offenbar auch davon aus, dass sie Aussicht auf Erfolg hat, was nach den genannten Kriterien der Fall ist. Und deswegen ist hier der Königsweg der, zu sagen, dieser Artikel 2 des vorliegenden Gesetzentwurfs wird ausgeklammert und von einer Umsetzung zum jetzigen Zeitpunkt zunächst abgesehen. Vielen Dank.

Vorsitzender Andreas Schmidt (Mülheim): Vielen Dank, Herr Dr. Breyer. Das Wort hat jetzt Herr Dr. Fiedler. Rechtsanwalt, Verband Deutscher Zeitschriftenverleger e.V., Berlin.

SV Dr. Christoph Fiedler: Herr Vorsitzender, sehr geehrte Damen und Herren. Die Medien würden es auch begrüßen, wenn vor einer Umsetzung der Ausgang der Klage vor dem EuGH abgewartet würde. Dennoch beschränke ich mich hier auf einzelne problematische Punkte des Umsetzungsentwurfs.

Die Vorratsdatenspeicherung würde aus Sicht der Medien selbst im Falle einer engen Umsetzung, also Zweckbindung beispielsweise hinsichtlich terroristischer Straftaten, und selbst im Falle eines zusätzlichen spürbaren Schutzes journalistischer Quellen die Pressefreiheit schwächen. Von einer solchen grundrechtsschonenden Minimalumsetzung ist der Entwurf aber weit entfernt. Er gibt sehr weite Zugriffsermächtigungen und ein praktisch wirksamer Informantenschutz ist auch aus

unserer Sicht nicht gegeben. Der Entwurf wird deshalb, sollte er so in Kraft treten, die Pressefreiheit massiv schädigen. Journalisten, Medien sind darauf angewiesen, dass Informanten zwar nicht absolut, aber doch im Regelfall tatsächlich auf die zugesicherte Vertraulichkeit auch vertrauen können. Ohne die Möglichkeit eines solchen Vertrauens läuft die Pressefreiheit gerade in politisch relevanten Fällen leer, denn potenzielle Informanten bleiben für sich, sagen nichts, das Geschehen bleibt unbekannt oder ungeklärt. Die Vorratsdatenspeicherung beeinträchtigt die Möglichkeit eines solchen für die Presse essentiellen Vertrauensverhältnisses mit bislang nicht gekannter Intensität. Obwohl die Eingiffs- bzw. Zugriffsermächtigungen, § 100g StPO-RegE, die gleichen sind wie bei den anlassbezogenen Einzelfallmaßnahmen, erlangen sie eine ganz neue Dimension. Es werden alle Telefon-, Mobilfunk-, E-Mail- und Internetverbindungsdaten sowie Mobilfunkstandortdaten für sechs Monate gespeichert. Das heißt, dass der Staat erstmals Zugriff erhält auf alle elektronischen Kontakte von und mit allen Journalisten für das jeweils vergangene halbe Jahr. Allein diese Tatsache wird Informanten massiv abschrecken und hat es – wie Beispiele gezeigt haben – in Belgien auch schon getan. Die Informanten müssen ihre Enttarnung befürchten, wenn der Journalist innerhalb eines halben Jahres nach der Kontaktaufnahme in das Visier der Staatsanwälte gerät. Und wie geschieht das? Nun, es geschieht einmal durch die Veröffentlichung oder durch die bestimmungsgemäße Verwendung der Insiderinformation im Rahmen der Recherche. Der Informant muss die Enttarnung aber auch dann befürchten, wenn der Journalist innerhalb der nächsten sechs Monate wegen irgendwelcher anderer Recherchen oder Veröffentlichungen für die Staatsanwaltschaft interessant wird. Die Vorratsdatenspeicherung fixiert die komplette elektronische Kommunikationshistorie des Journalisten und multipliziert damit das Enttarnungsrisiko für alle Informanten, und zwar auch aufgrund von Vorgängen, von denen sie nichts wissen und nichts wissen können. Dieses Risiko, als Zufallsfund enttarnt zu werden, ist tatsächlicher Natur und wird sicherlich dadurch gesteigert, dass im Rahmen der Auswertung der Kommunikationsgeschichte fast schon notwendigerweise häufig Begleitfunde anfallen werden, die Zufallsfunde zu nennen vielleicht schon Euphemismus ist. Dieses tatsächliche Risiko wird dadurch gesteigert, dass die Verwendung solcher Begleitfunde nach dem Regierungsentwurf legal ist. Ist so das vermehrte intensivierte Risiko einer Enttarnung und der Zerstörung oder Nichtbegründung des Vertrauensverhältnisses beschrieben, wird das gesteigert durch die weiten

Zugriffsmöglichkeiten. Wir meinen deshalb, dass die Vorratsdatenspeicherung – und beziehen das zunächst einmal auf die Journalistenkommunikation, nehmen aber nur zu den anderen Bereichen einfach keine Stellung – auf die Verfolgung wirklich schwerer Straftaten begrenzt werden sollte. Sie wurde politisch mit Terrorismusgefahren begründet und sollte dann auch auf terroristische Gefahren und Straftaten beschränkt bleiben. Zudem sollte die Verwendung von Zufallsfunden untersagt werden, wobei man sehen muss, dass das natürlich umso wichtiger ist, je weiter die Zugriffsmöglichkeiten bleiben. Da eine derartige Minimalumsetzung der Richtlinie zudem fraglos europarechtskonform wäre, greift hier auch das Grundgesetz und man kann der Meinung sein, eine solche enge Umsetzung sei grundrechtlich geboten. Wir gehen davon aus, jedenfalls für den Bereich der Presse.

Der abschreckende Effekt auf Informanten wird aber unabhängig von der beschriebenen Problematik – Zufallsfunde, weite Ermächtigung – dadurch ins Unverhältnismäßige gesteigert, dass ein spürbarer, praktikabler Quellenschutz nicht stattfindet. Erhebung und Verwertung der Journalistenkontakte, also dieser Kommunikationsgeschichte, setzen lediglich voraus, dass der Eingriff nicht unverhältnismäßig erscheint. Der Zugriff ist insbesondere auch ohne jeden Verdacht strafbarer Beteiligung des Journalisten möglich. Die Verstrickung, wie das am Mittwoch wahrscheinlich versehentlich von jemandem gesagt wurde, kann nicht nur leicht erfolgen, sie ist gar nicht nötig.

Ein Quellenschutz, ein Informantenschutz, der beschränkt ist auf die Verhältnismäßigkeitsprüfung, der sich darin erschöpft, ist unkalkulierbar und keine geeignete Vertrauensgrundlage. Eine bloße Verhältnismäßigkeitsprüfung bleibt aber darüber hinaus sogar noch hinter dem unzureichenden Niveau des Schutzes zurück, das für den Schutz gegen Durchsuchung und Beschlagnahme vor der Cicero-Entscheidung praktiziert wurde. Denn § 97 Abs. 5 StPO nennt zwei einengende Voraussetzungen, erstens Verstrickung, also Verdacht der strafbaren Beteiligung, nach dem Regierungsentwurf sogar Einleitung eines Verfahrens, und zweitens muss zusätzlich zu dem Verdacht die Beschlagnahme verhältnismäßig sein. Das Cicero-Urteil hat das noch weiter eingeschränkt, nämlich gesagt, in der Konstellation der Veröffentlichung des Dienstgeheimnisses kann das allein nicht ausreichen, um die Aufhebung des Quellenschutzes durch Durchsuchung und Beschlagnahme zu

begrenzen. Soweit also am Mittwoch gesagt wurde, es ginge im Wesentlichen um materiellrechtliche Fragen, ist das nicht ganz richtig. Wir meinen, dass der Gesetzestext auch bei dem Zugriff auf die Vorratsdaten wenigstens die beiden ersten Begrenzungen, also den Strafbarkeitsverdacht und die Verhältnismäßigkeit, kumulativ benennen muss. Wenn man das nicht macht, dann wird der bei Durchsuchung und Beschlagnahme geltende Vertrauensschutz bei der Überwachung der elektronischen Kommunikation und dem Zugriff auf die Kommunikationshistorie aus der Vorratsdatenspeicherung ausgehebelt und umgangen. Das ist – und das erscheint uns wichtig – zunächst einmal eine Frage des angemessenen Schutzniveaus und nicht der Ungleichbehandlung oder Gleichbehandlung mit anderen Berufsgeheimnisträgern. Und auch, das ist ein weiterer Punkt, wenn wir einen solchen Schutz für verfassungsrechtlich geboten halten, ist es zunächst einmal eine Frage der Erfüllung des gesetzgeberischen Auftrags zur Schaffung eines angemessenen Ausgleichs zwischen Pressefreiheit und Geheimnisschutz. Der erschöpft sich nämlich entgegen manch' anders lautenden Äußerungen – und zuweilen klingt auch die Begründung so – nicht in der Nachzeichnung des verfassungsrechtlichen Minimums. So würden Sie übrigens auch die Koalitionsvereinbarung deuten, wenn sie sagt, dass die Regierung insbesondere den *„besonderen Schutz der Journalisten sichern"* wolle. Nach dem jetzigen Entwurf bleibt dem Informanten kaum noch eine Möglichkeit der vertraulichen Kontaktaufnahme mit Journalisten. Allein das Ausmaß der Trockenlegung der Quellen ist nicht prognostizierbar. Mit der Postkutsche vorzufahren oder Treffen im Wald ohne Akku im Mobiltelefon sind keine praktikablen Alternativen. Versiegen aber die Quellen, sind Presse und Rundfunk blind, wird mit ihnen die Demokratie beschädigt. Die Vorratsdatenspeicherung wird die Medien in jedem Fall beeinträchtigen. Unterbleibt aber, wie bislang vorgesehen, ein effektiver Quellenschutz, werden die Medien in ihrem Kern getroffen.

Ein letzter Hinweis, der auch verfassungsrechtlichen Gehalt haben kann. Man hört das Argument, in Zeiten gesteigerter Terrorismusgefahr müsse auch die Presse zurückstecken. Das erscheint uns, insbesondere in der Frage des Quellenschutzes, unzutreffend. Denn gerade in Zeiten des Terrorismus, in denen der Staat Bürgerrechte vermehrt beschränkt und vermehrt geheim agiert, ist jede Demokratie auf eine effektive und robuste Pressefreiheit angewiesen. Vielen Dank.

Vorsitzender Andreas Schmidt (Mülheim): Vielen Dank Herr Dr. Fiedler. Jetzt hat das Wort Herr Dr. Graf, Richter am Bundesgerichtshof Karlsruhe.

SV Dr. Jürgen-Peter Graf: Vielen Dank, Herr Vorsitzender. Lassen Sie mich mit einem persönlichen Beispiel beginnen. Vor einigen Monaten wurde mein Account eines Bezahlsystems eines Auktionshauses geknackt, wobei ich gleich sagen kann, es war weder eine Phishing-Attacke – das wäre mir aufgefallen – noch war ein Trojaner auf meinem Rechner. Es war also ein ganz normales Knacken des Accounts. Das führte dazu, dass innerhalb von 48 Stunden etwa 40 Transaktionen durchgeführt wurden mit diesem Account. Es wurde virtuelles Gold für ein Spiel bei chinesischen Profi-Händlern gekauft und der Schaden lag insgesamt immerhin im vierstelligen Bereich. Mag sein, dass man sagt, das kann ein Bundesrichter gut aushalten. Das habe ich auch ausgehalten, aber einige Bürger würden dadurch sicherlich schon sehr stark beeinträchtigt. Ich habe das natürlich nicht sofort entdeckt, weil man so einen Account nicht täglich anschaut wie auch das Konto, sondern erst nach etwas mehr als zwei Wochen und ich ahnte schon damals und so war es auch, dass die Täter nicht entdeckt werden können, weil die IP-Nummern, bei einer norddeutschen Verwaltung gespeichert, inzwischen gelöscht waren. Es ergibt sich auf diese Art und Weise gerade bei Taten, die mit Telekommunikation begangen sind, ein gewisser rechtsfreier Raum, weil man doch sehr genau weiß, sobald die IP weg ist, gibt es praktisch keine Chance mehr zu ermitteln. Das ist so ähnlich, wie wenn Sie ein Warenhaus abends nach Geschäftsschluss einfach offen lassen, die Mitarbeiter alle nach Hause schicken und hoffen, dass am nächsten Morgen noch alles da ist. Der einzige Unterschied ist, beim Warenhaus kann es passieren, dass ein Passant es sieht, wenn jemand reingeht, und dann die Polizei ruft. Im Internet sieht es eben niemand. Sobald die IP gelöscht ist, ist sie weg. Wie charakterfest müssen eigentlich deutsche Verkäufer und Verkäuferinnen sein, wenn sie nur von einer Kreditkarte, die ihnen vorgelegt wird, die Verifikationsnummer aufschreiben müssten – der Rest ist ohnehin bei ihnen im Rechner – sie könnten nach zwei, drei Wochen, wenn niemand mehr weiß, dass da bezahlt wurde, munter mit dem Einkaufen beginnen und sich die Produkte elektronisch liefern lassen. Softwareprodukte sind leicht einige 100 Euro wert und schon kann kein Mensch mehr

nachweisen, wer der Besteller war, den Täter kann man nicht feststellen, weil eben die Daten gelöscht sind.

Auf der anderen Seite, wie groß sind die Gefahren? Es wird darauf hingewiesen, dass es hier Einschränkungen geben kann. Zunächst einmal will ich sagen, wenn es um das Speichern von Internetdaten geht, also IP-Nummern, dann haben Sie eine Sammlung von IP-Nummern, mit denen eigentlich weder eine Firma noch ein Privater irgend etwas anfangen kann. Auch die Zeiten, in denen man ins Internet gegangen ist, was früher vielleicht entscheidend war, ist heutzutage kein Problem mehr. Sie werden im Regelfall 24 Stunden Online sein, dann kommt die Zwangsunterbrechung, dann geht es wieder aufs Neue los. Das heißt, auch da können Sie keine Gewohnheiten erkennen. Es wird bei den meisten Flatrate-Besitzern das gleiche sein. Mit der IP-Nummer ist es nicht anders, als wenn Sie auf einer CD-ROM die Geburtsdaten aller deutschen Bürger ohne Namensangaben haben. Damit können Sie auch relativ wenig anfangen. Im Übrigen ist es so, die Daten werden da gespeichert, wo sie angefallen sind. Das heißt, der Provider oder der Kommunikationsdienstleister hatte ohnehin die Möglichkeit, die Daten zur Kenntnis zu nehmen. Und wenn sie dann bei ihnen gespeichert sind, sind sie ja zunächst noch nicht weitergegeben. Das heißt, es ist nicht sehr viel anders, als wenn irgendwo ein Speicher mitläuft und das gab es in der Vergangenheit oftmals genug, bis vor einigen Jahren die Gerichte eingeschritten sind. Man hat nie gehört, dass hier die Daten irgendwo weiter verwendet worden sind. Das wäre sicherlich, denke ich, durch die Presse gegangen. Ich gehe davon aus, dass die Sicherheit durchaus überprüft wird, so wie es auch bei Telekommunikationsüberwachungsanlagen und -einrichtungen der Fall war, dass also die Regulierungsbehörde und auch die Datenschutzbeauftragten sicherlich ein Auge darauf haben werden, dass da wenig passiert. An den Staat können sie eben nur dann herausgeben, wenn eine entsprechende Anordnung da ist. Auch das werden die Provider hier genauestens beobachten. Bei den Handy-Daten mag es etwas anderes sein, aber auch da haben Sie nur die Bewegungsdaten. Natürlich die Anrufe, das könnte gewisse Unterschiede darstellen, aber auch hier verweise ich darauf, dass man ja immerhin den Verdacht einer erheblichen Straftat haben muss, um diesen Bereich hier aufzulösen und Daten zu erhalten. Solange also keine Inhaltsdaten gespeichert werden – und das ist ja nicht die Absicht – gehe ich davon aus, dass diese damit verbundenen theoretischen

Gefahren jedenfalls vom Bürger nicht als solche empfunden werden und der Bürger es vorziehen wird, dass ein gewisser Datensatz, der für Außenstehende wenig aussagekräftig ist, gespeichert wird, als dass nachher Straftaten begangen werden, die mangels Zuordnung nicht mehr aufgeklärt werden können. Vielen Dank.

Vorsitzender Andreas Schmidt (Mülheim): Vielen Dank Herr Dr. Graf. Jetzt hat das Wort Herr Dr. Grützner, Geschäftsführer des Verbandes der Anbieter von Telekommunikations- und Mehrwertdienste e.V., Köln.

SV Jürgen Grützner: Ganz herzlichen Dank, Herr Vorsitzender. Meine Damen und Herren erlauben Sie mir, Ihren Blick ein wenig auf die Sichtweise derjenigen Unternehmen zu lenken, die das Ganze irgendwo im Griff halten und in den Griff bekommen sollen. Das sind die Anbieter der Telekommunikationsdienste sowohl für das Festnetz als auch für den Mobilfunk. Wir haben uns den Gesetzentwurf genau angeschaut und es gibt aus unserer Sicht hier einige ganz erhebliche Bedenken, die wir auch schon lange im Vorfeld den politisch Verantwortlichen mitgeteilt haben. Nach wie vor ist das, was uns hier vorliegt, aus unserer Sicht, aus Sicht der Unternehmen, nicht praktikabel umzusetzen. Es ist in wesentlichen Punkten unklar, wie die Unternehmen hier vorgehen sollen, was von den Unternehmen konkret verlangt wird. Ich gehe gleich im Detail noch darauf ein. Wir haben festgestellt, dass durch diesen Gesetzentwurf der Bundesregierung aus unserer Sicht absolut unnötig hohe Kosten verursacht würden. Dabei könnte durch einen effizienteren Umgang, durch Schnittstellen – auch dazu komme ich noch – die Kostenbelastung der Unternehmen gesenkt und damit letztendlich der Bürger oder Steuerzahler deutlich entlastet werden. Letztlich haben wir aber auch ganz erhebliche verfassungsrechtliche Bedenken. Ich kann mich da nicht nur meinen Vorrednern anschließen, sondern ich möchte hier einen neuen, ganz wesentlichen Aspekt, der Ihnen aber auch bekannt ist, einbringen. Aus unserer Sicht ist es nicht zulässig, verfassungsrechtlich nicht zulässig, die Unternehmen ohne eine ganz klare Entschädigungsregelung mit derartigen Pflichten zu betrauen. Wir halten es für unverzichtbar, dies zeitgleich mit dem hier vorgelegten Gesetzentwurf zu tun.

Darüber hinaus sehen wir, und auch das ist aus unserer Sicht eine durchaus rechtliche Problematik, dass die Gründe, deretwegen Daten gespeichert,

insbesondere nachher auch abgerufen werden können, deutlich über das hinausgehen, was ursprünglich mit dem Gesetzentwurf einmal vorgesehen war, oder was eigentlich die Intention auch der EU gewesen ist. Also, wir sind zum Teil weit von der Diskussion einer Terrorabwehr entfernt. Wir nehmen aus verschiedenen politischen Richtungen wahr, dass man nicht nur in Fällen von Betrug, sondern auch in Fällen, in denen es darum geht, wer z. B. unzulässig Klingeltöne geladen oder Musikdownloads gemacht hat, also wo es um das geistige Eigentum geht, speichert. Das sind Bereiche, in denen ich nicht sehen und nicht erkennen kann, dass sie noch angemessen in irgendeinem Zusammenhang zur Terrorismusabwehr stehen.

Ich will ein paar Punkte aufgreifen, die konkret auf die Normen hinweisen sollen, die wir für problematisch halten. Zunächst ist das der § 100 g Abs. 1 Satz 3 StPO-RegE. Hier geht es um Verkehrsdaten, um die Echtzeitüberwachung. Diese Verkehrsdaten und diese Echtzeitüberwachung haben das gleiche Schutzbedürfnis wie das Fernmeldegeheimnis es für alle Daten vorsieht. Diese spezielle Datensammlung, eine Echtzeitüberwachung, verstößt aus unserer Sicht gegen die Auffassung des Bundesverfassungsgerichts, das hier die Daten gleichstellt und unter einen gleichen Schutz stellt.

Das Zweite ist, dass eine Erfassung der E-Mails aus unserer Sicht unpraktikabel ist. Es ist mit leichtesten Mitteln, zum Teil schon mit Handys möglich, die E-Mail-Adresse zu ändern. Es geht nicht einmal um das Fälschen einer E-Mail, sondern nur um das Ändern einer E-Mail, wie wir jetzt technisch festgestellt haben. Eine Nummer mit hohem technischen Aufwand und hohen Kosten zu speichern, die ein Kunde selber ändern kann, macht aus unserer Sicht überhaupt keinen Sinn. Das ist Bürokratie vom Feinsten, die da aufgebaut wird, die in der Strafverfolgung, gerade bei den kriminellen Fällen und in den kriminellen Anwendungen keinerlei zusätzliche Sicherheit gibt. Eine Speicherverpflichtung der Dienstanbieter und nicht nur der Carrier, also nicht nur der Netzbetreiber, sondern auch der Serviceprovider, z. B. von Debitel, halten wir für völlig überflüssig, weil dies eine doppelte Datensammlung bedeuten würde. Alle zur Verfügung stehenden Daten liegen bereits bei den Netzbetreibern. Ich brauche hier nicht noch eine weitere Belastung für weite Teile der Wirtschaft auszusprechen.

Es gibt noch einen wesentlichen Punkt, der wurde hier schon mehrfach angesprochen, das ist die Beschränkung auf die schweren Straftaten. Aus unserer Sicht sind alle Hinweise – auch seitens der EU – eindeutig, dass es sich hier nur um schwere Straftaten handeln soll. Eine Ausweitung auf andere Straftaten bis hin zu Ordnungswidrigkeiten ist aus unserer Sicht nicht akzeptabel.

Ein wichtiger Punkt ist aus Sicht der Unternehmen natürlich die Frage der Übergangsfristen. Wenn eine auch enge und besser überarbeitete Version zum Tragen kommen soll, dann ist es unmöglich, eine Umsetzung zum 1. Januar nächsten Jahres herbeizuführen. Die Spielregeln stehen bis heute nicht fest. Die Anforderungen stehen bis heute nicht fest. Es gibt in erheblichem Umfang noch Möglichkeiten, hier Kosten einzusparen und effizientere Abfragen, z. B. über gleiche Schnittstellen der Behörden, über besondere Verfahren, über gleiche Datenformate noch ganz erhebliche Kosteneinsparungen zu realisieren. Dann muss man sich über eine Umsetzung unterhalten und wir halten hier die Vorgaben, die man für einzelne Bereiche vorgesehen hat, nämlich den 15. März 2009 für die Internet-Daten für einen ggf. erreichbaren Zeitpunkt. Wir sehen auch, dass die Bundesregierung selber weiß, dass eine schnelle Umsetzung eigentlich gar nicht in der vom Gesetz vorgesehenen Zeit erfolgen kann. Die Bußgeldtatbestände sollen erst ab dem 1. Januar 2009 greifen. Das halten wir für richtig. Das Zwangsgeld, das aber nach den allgemeinen Regeln des TKG jedem Unternehmen auferlegt werden kann, würde aber schon ab dem 1. Januar 2008 greifen und das ist aus unserer Sicht – wahrscheinlich ungewollt – ein deutlicher Hinweis darauf, dass die Bundesregierung selber weiß, dass es zum 1. Januar nächsten Jahres nicht funktionieren kann. Ich möchte es an dieser Stelle erst einmal bei diesen Anmerkungen belassen.

Vorsitzender Andreas Schmidt (Mülheim): Vielen Dank Herr Grützner. Jetzt hat das Wort Herr Dr. Liedtke, Datenschutz- und Sicherheitsbeauftragter E-Plus Mobilfunk GmbH & Co. KG, Düsseldorf.

SV Dr. Rainer Liedtke: Dankeschön Herr Vorsitzender. Herr Vorsitzender, meine Damen und Herren, ich möchte einfach noch einmal ein bisschen Revue passieren lassen, was wir insgesamt in diesem Feld überhaupt vor uns sehen. Wir haben in der Vergangenheit als TK-Industrie an vielen Stellen bereits Informationen über unsere

Kunden an Polizei und Sicherheitsbehörden übermittelt. Angefangen von der klassischen TK-Überwachung über viele andere Maßnahmen. Ich denke, dass die Zugriffe, die Polizei und Sicherheitsbehörden an der Stelle haben, oft durchaus gerechtfertigt sind und sich durch den zunehmenden Zugriff auf diese Daten darin ein Wandel in der Art und Weise, wie Kriminalität stattfindet, widerspiegelt. Bislang galt aber einfach der Grundsatz, dass wir die Daten herausgegeben haben, die wir in unserem Bereich zu Abrechnungszwecken in der Regel – sofern es sich nicht um die Inhaltsdaten bei der Telekommunikationsüberwachung handelte – erhoben hatten, gespeichert haben. Diesen Pfad verlassen wir jetzt. Wir sollen jetzt, begonnen hat es ja bereits 2004 mit der TKG-Novelle für die Bestandsdaten, aber nunmehr auch für die durch das Fernmeldegeheimnis geschützten Daten, eine Vorratsdaten-speicherung einführen. Das heißt, wir sollen hier Daten erheben und speichern, die wir zum Teil zu eigenen Zwecken gar nicht erheben und speichern würden, und das insbesondere auch für Zeiträume, für die wir normalerweise diese Daten gar nicht speichern würden. In der Diskussion wird immer wieder angebracht, dass es sich ja hier nur um die Verbindungsdaten handele und dass man sehr wohl die Inhaltsdaten außen vor ließe. Wenn man sich das TKG anschaut, dann sieht man dort sehr deutlich, dass durch das Fernmeldegeheimnis nicht nur der Inhalt der Telekommunikation, sondern eben auch die näheren Umstände, also sprich in diesem Fall die Verbindungsdaten geschützt sind. Das TKG geht ein Stück weit darüber hinaus und sagt nun auch eindeutig, dass die gesprächsbegleitenden Daten von nicht erfolglosen Gesprächen auch dem Fernmeldegeheimnis unterliegen. Also, diese Diskussion, die versucht, verschiedene Schutzniveaus zu installieren, greift einfach nicht, liegt einfach schief und sie ist auch sachlich nicht gerechtfertigt. Wenn ich mir ansehe, wie sich Kommunikation heute entwickelt, muss man einfach feststellen, dass die persönliche Kommunikation Aug' in Aug', unter vier Augen, mehr und mehr der elektronischen Telekommunikation weicht und dass mit diesem Instrument der Vorratsdatenspeicherung mehr und mehr die Möglichkeit besteht, am Ende des Tages ein vollständiges Kommunikationsprofil jedes einzelnen Bürgers zu erheben und zu speichern. Und das geht weit über das hinaus, was bislang in der Vergangenheit durch Maßnahmen, durch gerechtfertigte Art und Weise durch Polizei und Justiz umgesetzt worden ist. Es geht wirklich so weit, dass wir künftig für sämtliche Bundesbürger – um beim Mobilfunk, um bei dem Beispiel zu bleiben, jedes etwas ältere Kind hat ja heutzutage bereits ein solches Gerät – am Ende des Tages

dahin kommen, dass wir für jeden Bundesbürger ein vollständiges Kommunikationsprofil und auch ein Bewegungsprofil für das letzte halbe Jahr erstellen können. Da ist es für mich eigentlich nur ein schwacher Trost, dass diese Daten nicht in dem Bereich der Sicherheitsbehörden oder der Justiz sind, sondern dass sie in dem Bereich der Privaten bleiben. Das, glaube ich, behebt das Problem nicht. Denn die Daten sind einfach erhoben und sie sind da und wie die Vergangenheit bei vielen anderen Beispielen zeigt, wenn Daten da sind, werden sie auch genutzt.

Ich denke, dass an diesem Beispiel auch schon deutlich wird, dass hier an der Stelle nicht nur das Fernmeldegeheimnis jedes einzelnen Bundesbürgers betroffen ist, sondern auch das aus Art. 2 GG abgeleitete Recht auf informationelle Selbstbestimmung. Denn hier ist der ganz persönliche Umgang mit den ganz persönlichen Daten betroffen und man darf sich wirklich fragen, inwieweit eigentlich das Recht besteht, solche Daten von jedem Bundesbürger zu erheben, wohl wissend, dass doch nur in ganz wenigen Fällen diese Daten tatsächlich für Ermittlungszwecke am Ende des Tages benötigt werden. Das ist aus meiner Sicht klassische Vorratsdatenspeicherung. Wenn man sich dann noch überlegt, ob diese Maßnahmen auch wirksam und angemessen sind vor dem Hintergrund der Bekämpfung von Terrorismus, dann muss man doch klar sagen, dass bereits heute – auch auf EU-Ebene – darüber diskutiert wird, dass viele der Dinge, die in der EU-Richtlinie und letztendlich auch dann in unserem Gesetzentwurf enthalten sind, zahnlose Tiger sind. Das Beispiel IP-Daten wurde schon angesprochen. Ich glaube nicht, dass das Fälschen von IP-Daten ein so aufwendiger technischer Prozess ist, dass insbesondere terroristische Kreise sich dieser Maßnahme nicht bedienen werden. Einen ähnlichen Punkt haben wir bei der Speicherung der Endgerätenummern von Mobilfunktelefonen. Auch hier ist eine Fälschung relativ einfach möglich und das zeigt, dass Zielgruppe dieser ganzen Vorratsdatenspeicherung eben nicht die Terroristen sein können, denn die werden sich häufig diesen Möglichkeiten entziehen. Hinzu kommt auch noch die Möglichkeit, dass die Daten gefälscht oder verfälscht werden können. Dadurch können in beliebiger Weise auch einfach falsche Spuren gelegt werden. Wenn man sich überlegt, welchen Umfang an Daten, welchen Umfang an Datenspeicherung wir durch die Vorratsdatenspeicherung bekommen, möchte ich bezweifeln, dass Bürger

in den Fällen, in denen sie ungerechtfertigt in Ermittlungen einbezogen werden, überhaupt in der Lage sind, die einzelnen Daten, die ihnen dann vorgehalten werden, wirklich zu interpretieren. Sie werden nämlich oft gar nicht wissen, dass diese Daten existieren und sie werden sie dann selber auch gar nicht zuordnen können – mit der Konsequenz, dass sie letztendlich diese Vorwürfe schwer werden entkräften können.

Es wurde versprochen und es gibt auch entsprechende Stellungnahmen des Bundestages, dass die Umsetzung in nationales Recht sich an den Minimalanforderungen der EU-Richtlinie orientieren soll. Das sehe ich, wie meine Vorredner das auch schon angesprochen haben, an diversen Punkten nicht wirklich erfüllt. Ich möchte darauf auch nicht im Detail eingehen, aber ich möchte noch einmal auf das Thema § 100 g StPO-RegE eingehen. Will § 100 g StPO-RegE im Gegensatz zu den früheren Regelungen, die aus § 12 FAG erwachsen sind – wo es wirklich nur um die Übermittlung von Verbindungsdaten ging, die z. B. aus der Vergangenheit da waren oder die in den nächsten Wochen anfallen, die dann beispielsweise im Wochenrhythmus ermittelt wurden –, jetzt auch unter den abgesenkten Eingriffsvoraussetzungen gegenüber §§ 100 a und b StPO-RegE die Echtzeitübermittlung von Verbindungsdaten ermöglichen, wenn auch ohne Standortdaten? Das sehe ich als eine sehr drastische Ausweitung der Vorgaben der EU-Richtlinie. Wie gesagt, ich möchte auf die Einzelheiten im Detail nicht weiter eingehen. Dazu gibt es auch genügend Stellungnahmen, die das angesprochen haben.

Vielleicht einen Punkt noch: Verwendungszweck. Da ist nun im Regierungsentwurf neuerdings enthalten, dass auch zum Zwecke der Gefahrenabwehr – also sprich die klassischen Polizeigesetze der Länder – Möglichkeiten geschaffen werden, auf diese Daten zuzugreifen. Auch da möchte ich sagen, dass das natürlich deutlich über das hinausgeht, was die EU in ihrer Richtlinie vorsieht und auch da muss man natürlich aufpassen und sehen, dass in der Vergangenheit bereits Landesgesetze in diesem Umfeld durchaus nicht als ganz verfassungskonform eingestuft worden sind.

Zum Thema Inkrafttreten auch noch ein kurzes Wort. Die Bundesregierung hat seinerzeit bei der Verabschiedung der EU-Richtlinie noch einmal darauf gedrungen, dass der gesamte IP-Bereich eben nicht schon zum 1. Januar 2008 mit Inkrafttreten

des normalen Voice-Geschäftes umgesetzt werden muss, sondern erst zum 15. März 2009. Diese Regel, wenn auch nicht der 15. März, sondern ich glaube der 1. Januar 2009, war noch im Referenten-Entwurf enthalten. Dieser Termin ist nunmehr vorverlegt worden auf den 1. Januar 2008. Es tut mir leid, das ist technisch einfach nicht machbar, und ich halte es eigentlich für einen Skandal, wenn der Gesetzgeber eine Frist festschreibt, von der ganz klar ersichtlich ist, dass sie nicht umsetzbar ist. Und da helfen auch die Hilfestellungen, dass beispielsweise die Ordnungswidrigkeiten, die Sanktionierungen erst ab dem 1. Januar 2009 greifen sollen, nicht weiter, weil letztendlich die Netzagentur über Verwaltungszwang auch Zwangsgelder bei uns eintreiben kann. Nicht zu vergessen ist bitte auch die Tatsache, dass es durchaus Fälle gibt, in denen Mitarbeiter, die vor Ort diese Daten sammeln und an die Behörden übermitteln, z. T. mit Verfahren wegen Strafvereitelung bedacht werden können und letztendlich persönlich damit umgehen müssen. Diese Gefahr besteht natürlich auch in den Fällen, wo wir nicht gesetzeskonform Daten bereitstellen können.

Abschließend möchte ich noch kurz zum Thema Kosten Stellung nehmen. Entgegen unserer Hoffnung ist ja auch in diesem Gesetzespaket das Thema Kosten in keiner Weise geregelt, obwohl wir bereits seit 2004 im TKG eine entsprechende Ermächtigungsnorm für Entschädigungen haben. Es wird hier sozusagen nochmals oben draufgesattelt auf die ganzen Tätigkeiten, die wir als TK-Industrie heute bereits für die öffentlichen Behörden leisten, ohne dass auch nur mit einem Wort das Thema Entschädigung angesprochen wird. Das halte ich für einen nicht gangbaren Weg. Hier werden von der Industrie Dinge gefordert, die einfach nicht umsetzbar sind. Ich weiß, dass in den vergangenen Tagen Gespräche statt gefunden haben, um eine Entschädigungsregelung auf den Weg zu bringen. In dem Zusammenhang ist auch davon berichtet worden, dass die Unternehmen insbesondere durch die Abrechnung von Gesprächskosten bei der Ausleitung von Überwachungsmaßnahmen riesige Gewinne oder überhaupt Gewinne machen. Ich kann Ihnen für unser Haus sagen, dass wir bei E-Plus die Gesprächskosten, die Gesprächsgebühren bei der Ausleitung bei TÜ-Maßnahmen, überhaupt nicht bepreisen, weil es uns einfach viel zu aufwendig ist, die Daten zu erheben und anschließend dann mit den paar Cent vergüten zu lassen, die uns da zustehen. Im Übrigen, abschließend vielleicht noch, ich kenne keinen in der TK-Industrie, der mit diesem „Geschäft" wirklich etwas

verdient. Am Ende des Tages legen wir alle massiv zu an der Stelle und ich kann wirklich nur hoffen, dass das, was im Moment diskutiert wird, nämlich eine pauschale Entschädigungsregelung, dass das nun wirklich möglichst kurzfristig, spätestens mit der Umsetzung dieses Gesetzes, auch greift. Danke schön.

Vorsitzender Andreas Schmidt (Mülheim): Vielen Dank Herr Dr. Liedtke. Jetzt begrüße ich Herrn Prof. Dr. Michael Ronellenfitsch. Universität Tübingen, Juristische Fakultät, Lehrstuhl für Öffentliches Recht und Verwaltungsrecht. Wir haben uns vorhin, Herr Prof. Ronellenfitsch, auf ein fünfminütiges Eingangsstatement verständigt. In diesem Rahmen haben Sie, bitte schön, jetzt das Wort.

SV Prof. Dr. Michael Ronellenfitsch: Herr Vorsitzender, meine Damen und Herren Abgeordnete. Ich bin eingeladen als Inhaber eines Lehrstuhls für Öffentliches Recht und nicht als hessischer Datenschutzbeauftragter. Ich maße mir also an, eine freie Position zu vertreten ohne Solidaritätsdruck im Zusammenhang mit der Konferenz der Datenschutzbeauftragten. Aber aus Solidaritätsdruck, nicht um Sie zu brüskieren, habe ich darauf verzichtet, irgendwelche Präjudizien der schriftlichen Statements zu machen. Denn es geht hier um Fragen, die noch sehr kontrovers – selbst in Kreisen der Datenschützer – diskutiert werden. Ich möchte nur einen Punkt sagen, ich maße mir nicht an, Ihnen irgendwelche Ratschläge zu erteilen, wie Sie sich politisch entscheiden. Aber ich möchte, dass, wenn Sie Regelungen treffen, Sie sie handwerklich optimal treffen.

Zur Vorratsdatenspeicherung zunächst einmal die Unterscheidung zwischen der Datenspeicherung der Kunden zu Abrechnungszwecken. Dazu wurde ja schon das Erforderliche gesagt. Ich möchte nur davor warnen: Was als Datum in der Welt ist, unterliegt dem Zugriff der Überwachungsbehörden. Ob Sie es rechtlich regeln oder nicht, ist eine ganz andere Frage. Aber wenn man hier großzügig argumentiert und sagt, das betrifft nur das individuelle Verhältnis zwischen dem Telekommunikations-dienstleister und seinem Kunden und dann können zu Überwachungszwecken relativ lange Zeit Daten vorgehalten werden, dann haben Sie das Datum in der Welt und dann entsteht das Problem, wie kanalisiere ich den Zugriff in diese Richtung? Begehrlichkeiten sollte man nicht unnötig wecken. Das vorsichtig formuliert.

Jetzt das Überwachungsverhältnis. Da geht es um die Abwägung von verschiedenen Rechtspositionen. In der gegenwärtigen Terrorismusdiskussion ist es ja völlig klar, dass man mit dem Terrorismusargument alle andere Argumente totschlägt. Sie werden immer ein Argument finden, dass es hochwertige Rechtsgüter als Eingriffsermächtigung gibt, dass es höchstwertige Rechtsgüter gibt und dass der Bestand der Bundesrepublik gefährdet ist. Dann stehen Sie gegen die Bevölkerung, wenn Sie gefragt werden, warum haben Sie nicht alle Überwachungsmöglichkeiten ausgeschöpft, die es technisch gab? Aber das ist ein Abwägungsfaktor, den man in die Debatte bringen muss. Ich möchte die Gegenposition vertreten. Was von den Datenschützern immer wie eine Monstranz vor sich hergetragen wird, ist dieses Grundrecht auf informationelle Selbstbestimmung. Jetzt bitte ich Sie, was nützt Ihnen das Grundrecht auf informationelle Selbstbestimmung, wenn man damit dann nichts verbindet. Das ist vom Bundesverfassungsgericht erfunden worden als Abwägungsfaktor zwischen der Menschenwürde und der allgemeinen Handlungsfreiheit. Die ganze Palette der Beschränkungsmöglichkeiten ist gegeben. Mit anderen Worten, das Grundrecht auf Selbstbestimmung hat ein völlig unterschiedliches Gewicht, je nachdem, in welchem Zusammenhang in die informationelle Selbstbestimmung eingegriffen wird. Und das hat mein Vorredner schon gesagt, es geht bei der Vorratsdatenspeicherung nicht nur um die Verbindungsdaten, sondern es geht um das Kommunikationsprofil und das Kommunikationsprofil ist ein einheitliches Grundrecht. Wir haben nicht isolierte Grundrechte, wir haben in Art. 5 GG in der Summe ein gewichtiges Grundrecht der individuellen Lebensgestaltung und da gehört einfach die Kommunikation dazu. Um das nicht noch verworrener klingen zu lassen: Wenn Sie eine gleitende Skala haben bei der informationellen Selbstbestimmung zwischen Menschenwürdebereich – laut Bundesverfassungsgericht Kernbereich privater Lebensgestaltung, was immer man darunter verstehen will – bis hin zur Mobilität – Kommunikation im öffentlichen Raum, im öffentlichen Bereich mit weiten Handlungsspielräumen – da ist die Frage, wo positioniere ich die Vorratsdatenspeicherung? Die Vorratsdatenspeicherung positioniere ich umso mehr in den Kernbereich privater Lebensgestaltung, je mehr Daten gespeichert werden. Wenn Sie bloß Verbindungsdaten speichern, ohne Adresse des Angewählten oder dergleichen, dann bitte ich Sie, dann ist es eine läppische Angelegenheit, hier den Überwachungszugriff zu ermöglichen. Das Problem ist das Gesamtbild – das haben Sie ja angedeutet – der Kommunikation. Sie

haben zu Recht auf die Teenager, auf die Kinder und Jugendlichen hingewiesen. Aber Erwachsene sind genau so handyfreundlich. Und wenn Sie sich überlegen, wie oft wir am Tag telefonieren und kommunizieren und mit anderen in Kontakt, in Verbindung treten, dann ist unser Lebensprofil weitgehend durch Kommunikation bestimmt. Und in diesem Bereich muss man fragen, wie kann ich zugreifen, mit welcher Legitimation? Ich möchte nicht sagen, dass man gar nicht zugreifen kann, aber es ist ein Rechtfertigungsgrund erforderlich. Die Erforderlichkeit ergibt sich nicht allein aus der Europäischen Richtlinie. Da bitte ich Sie, Sie werden sich ein Armutszeugnis ausstellen, wenn Sie diesem albernen Gerede folgen, Eins-zu-eins-Umsetzung und solche Sachen. Das kommt immer wieder an, ja, was heißt Eins-zu-eins-Umsetzung? Das heißt doch Abschreiben. Dazu sind Sie nicht da. Sie sind dazu da, politisch zu gestalten, umzusetzen und die Richtlinie braucht man nicht sklavisch zu befolgen, man kann sie sinngemäß und sachgerecht zu Ende denken. Da bin ich im Gegensatz zu meinem Vorredner – ich habe leider nur ihn aus Zeitgründen hören können – der Meinung, Sie haben einen großen Gestaltungsspielraum und im Rahmen der Gefahrenabwehr kann sehr wohl eine Überwachungsnotwendigkeit bestehen und die Gefahrenabwehr ist mir persönlich immer wichtiger als die repressive polizeiliche Verfolgungsmaßnahme. Ob ich einen Terroristen bestrafe oder nicht, ist mir im Grunde gleichgültig. Natürlich hat man ein Strafbedürfnis, aber mir ist es viel wichtiger, zu verhindern, dass ein Terrorist überhaupt etwas anstellt. Der Schutz der Bevölkerung im Rahmen der Gefahrenabwehr, der muss eingebaut werden, wenn die Europäische Richtlinie aus Kompetenzgründen das nicht ausformuliert hat. Dann heißt es nicht, dass man das nicht auf nationaler Ebene machen sollte.

Letzter Punkt. Ich habe vermutlich die fünf Minuten schon überschritten. Der Eingriff in den Gewerbebetrieb der betroffenen Unternehmen ist massiv. Das ist einleuchtend – das haben Sie auch dargestellt – aber das kann man ausgleichen, das ist keine Enteignung oder so etwas Ähnliches. Das ist eine Inhaltsbestimmung des Eigentums und diese Inhaltsbestimmung des Eigentums ist verhältnismäßig, wenn sie zumutbar und erträglich gestaltet wird und sie ist verhältnismäßig, wenn sie wirklich zu krass sein sollte, wenn man in der Übergangszeit, in der Übergangsphase eine Entschädigungsregelung trifft. Und dann hat man dieses Problem weg und in der Summe kann man eine Gesamtabwägung durchführen, die zum Ergebnis kommt,

dass die Vorratsdatenspeicherung der Kontrolle unterliegt mit moderaten Einschränkungen des Inhalts, was man alles an Vorratsdaten ermittelt. Sie sehen es mir nach, dass ich jetzt nicht den Datenschützer rausgehängt habe, denn das wird mein Nachredner ohne weiteres für mich tun. Vielen Dank.

Vorsitzender Andreas Schmidt (Mülheim): Vielen Dank, Herr Prof. Dr. Ronellenfitsch. Jetzt hat der Datenschützer das Wort. Herr Dr. Weichert, Landesbeauftragter für den Datenschutz, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel.

SV Dr. Thilo Weichert: Herr Vorsitzender, sehr geehrte Damen und Herren. Jetzt kommt es schon so weit, dass ich also eine Monstranz vor mir hertragen darf, das Recht auf informationelle Selbstbestimmung. Ich beschränke mich nicht auf das Recht auf informationelle Selbstbestimmung, sondern beziehe auch die Grundrechte der Telekommunikationsfreiheit, Art. 10 GG, Art. 8 EMRK ein. Auch die Europäische Grundrechtecharta enthält diese Regelung, die die Privatsphäre und die Kommunikationsfreiheit von uns Menschen gewährleisten soll. Ich möchte den ganz dringenden Appell an den Bundestag richten, von der Vorratsdatenspeicherung insgesamt Abstand zu nehmen. Wenn das jetzt von Ihnen nicht gewollt und gekonnt wird, möchte ich Sie hilfsweise bitten, zumindest die Entscheidung des EuGH, die zu diesem Thema getroffen werden wird, abzuwarten und dann mit der größeren Weisheit, insbesondere was Kompetenzrechte und Grundrechtsinterpretation angeht, an den Gesetzgebungsauftrag zu gehen, sollte dann wirklich noch etwas übrig bleiben, was gesetzlich geregelt werden soll. Das Bundesverfassungsgericht hat in ständiger Rechtsprechung klar gemacht, dass es ein verfassungsrechtliches Verbot der Verarbeitung personenbezogener Daten auf Vorrat gibt. Dieser Begriff wurde vom Verfassungsgericht ausdrücklich verwendet, ohne dass die Betroffenen eigenen Anlass gegeben haben, ins Blaue hinein. Das sind die Begriffe, die vom Verfassungsgericht verwendet werden, ohne eine absehbare Erforderlichkeit, und zwar nicht allgemein, sondern in Bezug auf den jeweiligen Datensatz. Also muss bezüglich jeder einzelnen Person, die jetzt hier gespeichert wird, eine Erforderlichkeit gegeben sein, und zwar für ganz konkrete Zwecke. Diese Anforderung des Verfassungsgerichtes ist meines Erachtens nicht erfüllt. Daneben hat das Bundesverfassungsgericht seit 1969, also schon seit langem und in ständiger

Rechtsprechung bis zum heutigen Tag auch klar gemacht, dass es verboten ist, Persönlichkeitsprofile zu erstellen. Wenn wir immer mehr im Internet kommunizieren und Kommunikationsprofile über diese Daten erstellt werden können, dann sind diese Kommunikationsprofile auch Persönlichkeitsprofile und wir bewegen uns hier im verfassungsrechtlich unzulässigen Bereich. Das Bundesverfassungsgericht hat außerdem in einer jüngeren Entscheidung gesagt, dass eine Rundumüberwachung verhindert werden muss. Auch diese Argumentation spricht hundertprozentig gegen die Pläne, die von der Bundesregierung verfolgt werden.

In jedem Fall ist das, was hier geplant ist, nicht verhältnismäßig. Es ist viel zu unbestimmt geregelt. Es sind unüberschaubare Nutzungsmöglichkeiten in dem Gesetz vorgesehen, nicht nur eine Beschränkung auf die Strafverfolgung, auf Verfolgung schwerer Straftaten. Das, was Sie, Herr Dr. Graf, jetzt hier dargestellt haben, so leid es mir tut, da Sie selbst betroffen sind, ist keine schwere Straftat, das ist ein Vermögensdelikt. Daher dürfte also schon aus Verhältnismäßigkeitsgründen nicht genutzt werden, was hier geplant ist, aber natürlich bestehen die Begehrlichkeiten auch gerade in diesem Bereich. Darüber hinausgehend hat der Gesetzgeber bisher die Planung, die Daten auch noch für Zwecke der Nachrichtendienste zu nutzen. Nachrichtendienste werden tätig, ohne dass eine konkrete Gefahr bestehen muss und ohne dass eine Straftat überhaupt begangen sein soll – im Vorfeld. Überlegen Sie sich genau, ob Sie wirklich dem Nachrichtendienst den Zugriff auf diese Daten geben wollen. Und sogar für die Durchführung von Zivilverfahren, das heißt, für den Streit von Zivilpersonen, auch dafür sind diese Daten gedacht. Das kann doch nicht sein. Das sind wirklich unbestimmte Regelungen, die dann auch unbestimmte Zwecke darstellen und verfassungsrechtlich nicht akzeptabel sind. Ich bin mir sicher, dass die Datenspeicherung auch nicht erforderlich ist zur Verhinderung von terroristischen Anschlägen. Terroristische Straftäter haben das technische Know-how, sich dieser Vorratsspeicherung zu entziehen. Wir haben bisher keine Evaluation bezüglich der Regelungen in anderen Ländern. In anderen Ländern gibt es schon Vorratsdatenspeicherung. Wenn Sie analysieren würden, was in diesen Ländern an Daten gespeichert wird und welche Effekte sich daraus jetzt für die Kriminalitätsbekämpfung ergeben, würden Sie feststellen, dass hier diese Maßnahme absolut unverhältnismäßig und uneffektiv ist. Es gibt auch keine

erkennbare Prüfung von milderen Mitteln, was vom Verfassungsgericht dringend gefordert wird. Wir als Datenschützer haben immer vorgeschlagen, auch ein Quick Freeze zu regeln, d. h. also ein schnelles Zugreifen auf diese Daten, Einfrieren dieser Daten und Zugreifen auf diese Daten. Ich kann als Beispiel das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) nennen. Wir betreiben schon seit mehreren Jahren den vom Wirtschaftsministerium geführten Anonymisierungsdienst, der ja auch von dieser Regelung betroffen sein wird. Wir sind mit diesem Anonymisierungsdienst stark in der Kritik der Strafverfolger gewesen, weil uns vorgeworfen wurde, wir würden jetzt Kriminellen ein Forum oder ein Mittel geben, um ihre Straftaten unbeobachtet zu begehen. Wir haben daraufhin ein Strafverfolgungstool eingebaut, so dass innerhalb von wenigen Stunden für die Zukunft mitgelogged werden kann, welche Personen bezüglich einer IP- oder eines sonstigen Adressdatums welche Internetkommunikation vornehmen. Wir waren sehr verblüfft – das ist vielleicht auch eine empirische Erfahrung – wir haben irre viele Anfragen von Strafverfolgungsbehörden gehabt und haben sie auch weiterhin, seitdem wir das eingerichtet haben. Wenn Sie einen richterlichen Beschluss – den können Sie relativ schnell bekommen, das ist in der Zwischenzeit auch in der Justiz gewährleistet – vorlegen, dann kriegen Sie innerhalb von wenigen Minuten ein entsprechendes Mitloggen und Sie können solche Straftäter dann weiter verfolgen. Wir haben bisher in diesen vier Jahren einen einzigen richterlichen Beschluss bekommen und der hat nichts gebracht. Ich möchte damit nur zeigen, dass, wenn diese Daten mal vorhanden sind, sie natürlich genutzt werden. Aber der Aufwand, selbst ein rechtstaatliches Verfahren, was so ein Richterbeschluss darstellt, im Verhältnis zum Nutzen, der ist so groß, dass dann die Strafverfolger davon Abstand nehmen. Das ist jetzt nur unsere Erfahrung im ULD. Ich glaube, die wird aber bestätigt durch viele andere Erfahrungen in diesem Bereich. Die Strafverfolger haben sehr viele Möglichkeiten der Strafverfolgung. Die sollten sie effektiv nutzen und dann glaube ich, bleibt nicht mehr viel übrig für diese Regelungen.

Ich sehe noch einen weiteren Punkt, den ich ansprechen möchte, weil der hier von den anderen Kollegen noch nicht thematisiert worden ist. Wenn wir eine Vorratsdatenspeicherung bekommen und alle Menschen wissen, dass ihre Verbindungsdaten gespeichert sind über lange Zeit, werden sie sich genau überlegen, ob sie das Internet in der Zukunft noch so unbefangen nutzen, wie sie es

derzeit tun. Das hat ganz massive Konsequenzen für die IT-Wirtschaft. Das hat ganz massive Konsequenzen auch für die Pläne der Bundesregierung, E-Government-Anwendungen zu praktizieren und so eine einfache Kommunikation mit dem Bürger über das Internet zu ermöglichen. Das hat ganz massive Beeinträchtigungen zur Folge für das Vertrauen der Bürgerinnen und Bürger in Bezug auf E-Commerce und alles, was mit Online-Handel und Online-Kommunikation zu tun hat.

Herr Dr. Graf, erlauben Sie mir zum Schluss noch eine kleine Replik. Ich hätte viel zu dem zu sagen, was Sie gesagt haben. Aber es gibt die Möglichkeit, sicher im Internet Online-Banking zu betreiben. Da ist zunächst einmal jeder selbst gefragt. Die Bank ist gefragt und der Bankkunde ist gefragt, sichere Verfahren zu nutzen, und solche Verfahren können so sicher gemacht werden, dass irgendwelche Hacker – ich weiß nicht, wem Sie jetzt hier aufgesessen sind – dass solche Hacker keine Chance mehr haben. Zu den anderen Ideen von Herrn Dr. Graf würde ich gerne nachher noch was sagen, wenn entsprechend gefragt wird. Vielen Dank.

Vorsitzender Andreas Schmidt (Mülheim): Vielen Dank. Jetzt hat abschließend in dieser Runde das Wort Herr Wirth, Bayerisches Landeskriminalamt, München. Bitteschön, Herr Wirth.

SV Ernst Wirth: Sehr geehrter Herr Vorsitzender, meine Damen und Herren. Ich bedanke mich. Als letzter Redner in der Runde hat man es entweder ganz einfach oder ganz schwer. Die vorliegende Regelung zur Mindestspeicherfrist von TK-Verkehrsdaten, umgangssprachlich Vorratsdatenspeicherung, enthält aus polizeipraktischer Sicht überwiegend begrüßenswerte Regelungen und ist als sehr gelungen zu bewerten. § 113 a TKG-RegE enthält als Kernpunkt die Regelung über die Speicherung von Verkehrsdaten, die unterschiedlichen technischen Ausgangsparameter zur Speicherung und ist trotz der umfangreichen Ausführungen praxistauglich, insbesondere was die Auswertung von Mobilfunkdaten betrifft. Der Auswertung von Mobilfunktelefonie, sprich Funkzellenauswertung, kommt aus unserer Sicht zentrale Bedeutung zu. Verdeutlicht wird dies anhand der Klärung des Mordes von Rudolph Moshammer, Mord zum Nachteil von der Wohnungsprostituierten I. in München, Mord zum Nachteil des Asylbewerbers A. in

München. Geklärt werden konnten diese Taten durch DNA-Abgleich und als zweitwichtigstes Instrument in der Beweiskette durch Auswertung der Funkzellen und der TK-Verkehrsdaten. In der Beweiskette im Rahmen von Ermittlungsverfahren bei Kapitaldelikten bewerten wir zwischenzeitlich die Verbindungs- und Verkehrsdaten als elektronische DNA. Sie hat bei uns einen sehr hohen Stellenwert und wir vertreten die Ergebnisse aus der Funkzellenauswertung als Gutachter regelmäßig vor Gericht.

Zum Stichwort der Echtzeitauskunft folgende Sachlage: Ich wurde um zehn vor zwölf heute informiert, dass sich ein Angehöriger der Bundeswehr in Bad Reichenhall aus der Kaserne abgesetzt und einen Amoklauf angekündigt hat. Der Soldat führt 350 Schuss Munition und ein Gewehr G 3 mit sich sowie ein Mobiltelefon. Es gilt, sofort festzustellen, wo sich das Mobiltelefon des vermeintlichen Täters befindet. Hierzu ist die Echtzeitauskunft zwingend notwendig. Wir brauchen hier direkte und unmittelbare Auskunft über den Standort des Mobiltelefons. Gerne wird den Polizei- und Sicherheitsbehörden unterstellt, dass wir am Ende eines jeden Tages ein Bewegungsprofil der Staatsbürger erstellen wollen. Wir wollen ausschließlich eines, nämlich die Klärung von Straftaten. Dazu sind wir verpflichtet und dazu brauchen wir wirksame Instrumentarien. Und ein äußerst wirksames Instrumentarium im Rahmen der modernen Kommunikationsgesellschaft ist, Verbindungsdaten auszuwerten. Ich bedanke mich.

Vorsitzender Andreas Schmidt (Mülheim): Vielen Dank Herr Wirth. Damit haben wir die Statementrunde abgeschlossen. Wir beginnen jetzt die erste Fragerunde. Ich will noch einmal unser bewährtes Verfahren darstellen. Jede Kollegin, jeder Kollege hat die Möglichkeit, zwei Fragen zu stellen. Eine Frage an maximal zwei Sachverständige oder zwei Fragen an einen Sachverständigen. Ich empfehle Ihnen, sich eine kurze Notiz zu machen, wenn Sie Adressat einer Frage sind, weil wir die Fragen sammeln und erst nach Abschluss der Fragerunde in die Antwortrunde eintreten. Es hat sich bereits der Kollege Kauder gemeldet. Bitte schön.

Siegfried Kauder (Villingen-Schwenningen) (CDU/CSU): Ich habe eine Frage an Herrn Prof. Dr. Ronellenfitsch und an Herrn Dr. Graf. Dr. Fiedler hat durchaus bemerkenswerte Argumente vorgetragen. Er sieht die Pressefreiheit nicht nur

angeknabbert, sondern regelrecht in Gefahr durch die Vorratsdatenspeicherung. Dr. Fiedler, in einem Punkt kann man Ihnen sicherlich entgegenkommen, was Zufallsfunde anbelangt. Das haben wir vor zwei Tagen bei der TKÜ-Anhörung miteinander debattiert. Nun gibt es ja gewisse Vorgaben der Verfassung. Die Pressefreiheit bewegt sich ja nicht im rechtsfreien Raum, sondern sie ist begrenzt durch die allgemeinen Gesetze. Deswegen meine Bitte an Dr. Graf und Prof. Dr. Ronellenfitsch klarzustellen, was im Zusammenhang mit der Vorratsdatenspeicherung die Verfassung im Interesse der Pressefreiheit fordert, wo Korrekturen zwingend notwendig erscheinen oder nicht.

Jörg van Essen (FDP): Meine erste Frage geht auch an Prof. Dr. Ronellenfitsch, weil Sie Lehrstuhlinhaber für Öffentliches Recht sind. Ich finde, Dr. Breyer hat hier gut nachvollziehbar die Fragwürdigkeit des Vorhabens sowohl nach Europarecht als auch nach Verfassungsrecht vorgetragen. Da Sie ja insbesondere auch mit datenschutzrechtlichen Fragen befasst sind, würde mich Ihre Beurteilung sowohl des europarechtlichen als auch des verfassungsrechtlichen Zusammenhangs interessieren. Insbesondere vor dem Hintergrund, dass ja die Vorratsdaten-speicherung nicht nur, wie es ursprünglich beabsichtigt war, bei schwersten Straftaten mit terroristischem Hintergrund, sondern auch bei einfachen Straftaten, bei Begehung mittels Telekommunikation in Zukunft in Deutschland vorgesehen ist.

Die gleiche Frage richtet sich auch an Dr. Fiedler. Sie haben sich im Wesentlichen auf den jetzigen Entwurf gestützt und den Schwerpunkt, das ist auch Ihre Aufgabe aufgrund Ihrer beruflichen Funktion, auf den Schutz von Journalisten gesetzt. Aber mich würde auch die Beurteilung dieser Frage interessieren. Denn ich hatte aus Ihrem Vortrag eigentlich den Eindruck, dass Sie sich schon damit abgefunden hatten, dass das Ganze rechtmäßig ist und nur noch Journalisten geschützt werden müssen.

Jan Korte (DIE LINKE.): Herr Vorsitzender, meine erste Frage geht an Herrn Dr. Breyer. Der Wissenschaftliche Dienst der Verwaltung des Deutschen Bundestages hat vor einem halben Jahr ein Gutachten erstellt, in dem er schon die Eins-zu-eins-Umsetzung der Richtlinie für nicht kompatibel mit dem Grundgesetz eingeschätzt hat. Ich würde jetzt gerne noch einmal dazu Ihre Einschätzung hören und auch dazu, inwieweit der jetzt vorgelegte Entwurf der Bundesregierung eigentlich noch darüber

hinausgeht oder weit darüber hinausgeht, wo Sie dort eigentlich die entscheidenden Verschärfungen sehen, die damit einhergehende Problematik.

Und zum Zweiten an Herrn Dr. Weichert eine Frage. Sie haben an einem Beispiel eben dargestellt, wie sich Menschen in einer Gesellschaft bei einem stetig steigenden Überwachungsdruck verhalten, zum Beispiel ganz konkret in der Nutzung des Internets. Da würde mich eine allgemeinere Einschätzung von Ihnen interessieren. Wie sich erstens Kommunikation verändert und wie sich auch demokratisches Verhalten und Partizipation in einer Gesellschaft sukzessive verändern und, wenn Sie von einem Dammbruch sprechen, ob hier auch vielleicht ein Quantensprung zu erwarten ist. Wie Menschen eigentlich ihr Verhalten ändern und vielleicht auch anfangen, den aufrechten Gang nicht mehr zu gehen oder ihn auch weniger zu gehen. Das würde mich interessieren.

Jerzy Montag (BÜNDNIS 90/DIE GRÜNEN): Zwei Fragen. Die erste an Herrn Dr. Graf. Herr Dr. Graf, zuallererst ganz ernst mein Bedauern, dass Sie Opfer einer Straftat geworden sind. Aber Sie haben jetzt sozusagen aus dieser Opfersituation heraus die Behauptung in Ihrem Statement aufgestellt: Wenn die Bevölkerung zu entscheiden hätte, ob sie mehr Schutz ihrer Kommunikation haben will oder eine größere Möglichkeit, Straftaten aufzuklären, dann würden sich die Menschen selbstverständlich für die Aufklärung der Straftaten entscheiden. Ich weiß, dass die Fragestellung weh tut. Das Bundesverfassungsgericht – ich würde Sie dann auch um eine Bewertung als Bundesrichter bitten – vertritt eine andere Auffassung. Nämlich diejenige, dass, wenn im Staat die Möglichkeiten einer Kontrolle im Sinne einer Verbundkontrolle steigen, sich daraufhin das Kommunikationsverhalten der Bevölkerung ändert, und zwar von einem freien Kommunikationsverhalten zu einem gesteuerten. Bereits die Gefahr, dass sich das Verhalten der Bevölkerung verändern könnte, sieht das Bundesverfassungsgericht als einen schwerwiegenden Grundrechtseingriff an. Wenn man sich jetzt noch überlegt, dass von dieser Vorratsdatenspeicherung 500 Millionen Menschen betroffen sind, in Deutschland 80 Millionen. Von diesen 500 Millionen Menschen sind zum Glück die allerallerwenigsten Opfer und die allerallerwenigsten Täter. Dann ist doch das Verhältnis des Eingriffs gegenüber allen, gegenüber dem möglichen Erfolg in den Einzelfällen, also dass man hier den Täter aufspürt und Sie die 4.000 Euro

wiederkriegen – wenn überhaupt – und der Täter eine Strafe erhält, ein Missverhältnis. Dazu wollte ich gern von Ihnen eine Einschätzung haben.

Meine zweite Frage richtet sich an Herrn Grützner und an Herrn Dr. Weichert. Ich würde Sie herzlich bitten, dass Sie die Position von Herrn Dr. Graf, den ich als Juristen sehr schätze, aber heute als Techniker kennen gelernt habe, dass Sie die Position von Herrn Dr. Graf bewerten aus Ihrer Sicht, wonach die IP-Adressen völlig ungefährliche, nichtssagende Informationen sind, deren Festhalten und Verarbeiten unter keinen Umständen irgend etwas Besonderes sein könnte.

Joachim Stünker (SPD): Herr Dr. Liedtke, Sie haben ja zu Recht darauf hingewiesen, dass der überwiegende Teil dieser Daten heute schon zu Zwecken der Abrechnung usw. vorhanden ist. Sie haben dann gesagt, dass eine ganze Reihe von Daten, die wir ansonsten gar nicht speichern würden, jetzt zusätzlich erhoben werden sollen. Ich will Sie nur bitten, zu schildern, welche Daten Sie damit meinen, das ein bisschen näher zu präzisieren.

Herr Prof. Dr. Ronellenfitsch, Sie haben ja auch die Abwägung noch einmal sehr deutlich gemacht. Der Staat ist immer im Spannungsfeld, auf der einen Seite die Fragen der inneren Sicherheit, die Fragen der Strafverfolgung und auf der anderen Seite die persönlichen Freiheitsrechte der Einzelnen. Bei den Verkehrsdaten, bei dem ganzen TKÜ-Bereich, bei der Wohnraumüberwachung ist der Einsatz sicherlich wesentlich schwieriger, aber diese ganzen Verkehrsdaten setzen Menschen zunehmend freiwillig durch ihr Kommunikationsverhalten. Die Entwicklung, bei diesen Möglichkeiten der Informationsmedien und der Mitteilungsmedien, die wird sicherlich rasant sein, also noch fortschreiten. Wo würden Sie bei der Verhältnismäßigkeitsabwägung – oder kann man das überhaupt – eine Grenze ziehen? Kann man eine rote Linie ziehen, wo Sie sagen würden, die darf auf jeden Fall nicht überschritten werden bei den Möglichkeiten, dort präventiv oder repressiv tätig zu werden.

Klaus Uwe Benneter (SPD): Herr Prof. Dr. Ronellenfitsch, das wollte ich noch ergänzen. Sie sind ein bisschen darüber hinweggegangen bei der informationellen Selbstbestimmung. Das Gesamtbild, von dem auch Dr. Liedtke sprach, was sich ja

durch diese vielen Daten, von denen jetzt ja auch der Kollege Stünker sprach, dann ergeben könnte: Wo ist dann eigentlich die Grenze, ab der es in einen Bereich geht, der die informationelle Selbstbestimmung so treffen könnte, dass man andere Regelungen finden müsste? Wo ist da der Grenzbereich?

Eine Frage an Sie, Herr Dr. Weichert, Sie sprachen von den Erfahrungen in anderen Ländern. Wenn Sie uns da das eine oder andere Beispiel nennen könnten, wie lange da welche Erfahrungen gemacht wurden?

Herr Dr. Graf, das Beispiel mit dem offenen Warenhaus habe ich nicht richtig mitgekriegt. Also, was soll uns das sagen? Das ist mir nicht klar geworden.

Sabine Leutheusser-Schnarrenberger (FDP): Ich hätte zunächst eine Frage an Herrn Dr. Breyer und Herrn Dr. Weichert, und zwar noch mal zu der grundlegenden Frage bei der Vorratsdatenspeicherung und der Zweckbestimmung. Gerade aufgrund der durch die Rechtsprechung des Bundesverfassungsgerichts konkretisierten Anforderungen ist es ja notwendig, bei der Datenspeicherung eine konkrete Zweckbestimmung zu haben. Ich bitte doch nochmals aus Ihrer Sicht darzulegen, wo Sie Gründe für, aber auch Bedenken dagegen sehen, bei einer Vorratsspeicherung in dem hier vorgeschlagenen Sinne. Ich bitte Sie, auch die jüngste Rechtsprechung von 2007, bei der es um die Bankkontenabfrage gegangen ist, in Ihre Bewertung einzubeziehen. Meine Frage ist, ob das, was in der Begründung des Gesetzentwurfs ausgeführt wird, dass es ja dann Strafverfolgungszwecken diene, hier bei der Vorratsspeicherung zum Tragen kommen kann? Ist das aus Ihrer Sicht eine Rechtfertigung, die auch verfassungsrechtlich trägt?

Die zweite Frage richtet sich an Herrn Dr. Liedtke und an Herrn Grützner. Ich möchte Sie bitten, aus Ihrer Erfahrung doch einmal zu dem Stellung zu nehmen, was Herr Wirth gesagt hat. Herr Wirth hat dargelegt, welche Informationen wichtig sind für die Tätigkeit des Landeskriminalamts, für die Polizei. Was denn da jetzt schon geht, in welchem Umfang und wie denn da schon Nachfragen im Rahmen des geltenden Rechts erfolgen? Ferner bitte ich dazu Stellung zu nehmen, mit welchem Anfragevolumen Sie aufgrund bisheriger Erfahrungen rechnen, wenn das, was im Gesetzentwurf enthalten ist, dass ja nicht nur zu Strafverfolgungszwecken, sondern

auch zur Gefahrenabwehr abgefragt werden darf und auch die Verfassungsschutzbehörden jeweils auf Bund- und Länderebene aus Ihren millionenfachen Datenbeständen abfragen dürfen, Gesetz wird. Was bedeutet das für Sie aus unternehmerischer Sicht insgesamt und wie schätzen Sie das ein?

Vorsitzender Andreas Schmidt (Mülheim): Vielen Dank. Ich habe jetzt keine weiteren Wortmeldungen in dieser ersten Fragerunde. Dann starten wir mit der ersten Antwortrunde und es beginnt jetzt Herr Dr. Weichert. Ihnen liegen Fragen der Kollegen Korte, Montag, Benneter und der Kollegin Leutheusser-Schnarrenberger vor.

SV Dr. Thilo Weichert: Die Frage von Herrn Korte, wie die Bevölkerung sich verhält, ist schwierig zu beantworten, weil wir da noch keine Erfahrungswerte haben und ich glaube, die Verhaltensweisen in Deutschland werden sicherlich andere sein als in anderen Ländern, weil wir ja eine andere IT-Kultur haben und auch eine andere Datenschutzkultur als in anderen Ländern. Man kann feststellen, wenn man es etwa mit anderen Ländern vergleicht, dass dort die Kriminalität zumindest aufgrund der Vorratsspeicherung und auch sonstiger Überwachungsmaßnahmen definitiv nicht abgenommen hat, im Gegenteil, erheblich höher ist. Großbritannien ist das beste Beispiel, wo sehr viel mehr Überwachungsmaßnahmen stattfinden, auch schon eine Vorratsdatenspeicherung, und die Kriminalität erheblich höher ist als in der Bundesrepublik. Also Deutschland ist insofern Sicherheitsweltmeister und Datenschutzweltmeister und es scheint sich nicht gegenseitig auszuschließen. Was wir aber erleben würden, glaube ich, ist, dass die Bevölkerung Ausweichstrategien finden würde. Und eine dieser Ausweichstrategien wird die sein, dass sie Angebote außerhalb der Europäischen Union in Anspruch nähme. Dass sie dann unter Umständen in anderer Hinsicht rechtstaatlich sehr fragwürdige, vielleicht auch nicht vertrauenswürdige Angebote in Anspruch nähme, weil sie dann die Hoffnung hat, dass sie zumindest hier z. B. auch beim Runterladen von irgendwelcher Musik und ähnlichem nicht mitgeloggt werden kann und dann vielleicht irgendein Abmahnkönig ihr dann eine entsprechende Abmahnung zuschickt. Also, ich denke, so etwas kann passieren. Es wird auf jeden Fall ein Hindernis sein für die Nutzung von IT, die Nutzung von E-Government und E-Commerce. Wir können feststellen, dass alle Anbieter im IT-Bereich, die jetzt mit Internet zu tun haben, also Google, Microsoft

usw., dass die ganz große Anstrengungen unternehmen, damit die Vertraulichkeit ihrer Datenverarbeitung auch gegenüber dem Staat, gegenüber staatlichen Einrichtungen, also insbesondere auch in den USA gegenüber dem Homeland-Security-Department, gewahrt ist. Google sollte z. B. Millionen Datensätze an das Homeland-Security-Department herausgeben, hat aber gesagt: Das machen wir nicht, denn wir befürchten, wenn wir das machen, dann wird es bei den Nutzungszahlen unserer Suchmaschine und bei unseren sonstigen Diensten einen GAU geben. Deswegen glaube ich, dass es noch nicht deutlich erkennbare, aber absehbare Entwicklungen bei der Bevölkerung gibt. Und dort, wo etwas Sensibles passiert, dort wird man es eher unterlassen, über das Internet zu kommunizieren oder man würde Ausweichstrategien anwenden. Es gibt zwar sehr viele Menschen, die meinen, sie hätten nichts zu verbergen. Das ist zweifellos richtig, aber ich bin mir sicher, dass gerade in der Internetkommunikation von jedem von uns etwas ist, was er vor anderen, vor Strafverfolgungsbehörden, vor Nachrichtendiensten oder auch vor zivilen Fahndern geheim gehalten wissen möchte.

Die zweite Frage. Wenn wir theoretisch Milliarden von Datensätzen haben, dann sind wir als Datenschutzaufsichtsbehörden absolut überfordert. Die Hoffnung von Herrn Dr. Graf, dass wir hier noch eine effektive Kontrolle durchführen können, ist illusorisch. Herr Wirth hat schon auf diese Funkzellenabfrage hingewiesen. Wir hatten einmal einen solchen Fall in Schleswig-Holstein. Einen einzigen Fall. Das hatte für uns einen Ermittlungsaufwand von etwa einer Woche für zwei Leute bedeutet. Weil man nämlich wirklich die ganzen Datensätze durchgehen musste, wir uns anschauen mussten, wo die von wem übermittelt und wie sie benutzt worden sind usw. Das ist ein riesig aufwendiges Verfahren. Soll das jetzt bundesweit so implementiert werden, dann wäre die zwangsläufige Konsequenz, wenn man verfahrensrechtliche Sicherung auch effektiv haben möchte, dass die Datenschutzbehörde massiv ausgebaut werden müsste. Das ist auch eine Kostenfrage, auch eine Frage, ob denn das überhaupt sein muss. Also in dem Bereich würde ich sagen, ist das definitiv nicht notwendig.

Zur Frage von Herrn Montag, wie es denn mit der IP-Adresse ist. IP-Adresse und Geburtsdatum sind völlig unterschiedliche Daten. Ich teile mein Geburtsdatum durchschnittlich mit 5 Millionen Bundesbürgern. Aber die IP-Adresse, die ich heute

um soundsoviel Uhr verwende, die ist eindeutig und über den jeweiligen Provider kann festgestellt werden, dass Thilo Weichert mit dem Bundestag eine E-Mail ausgetauscht hat oder mit irgendjemand anderem, welchen Dienst er verwendet hat und welche Dinge er bei der Gelegenheit getan hat. Das ist absolut ein Unterschied und an der IP-Adresse, Herr Dr. Graf, das können Sie mir als Datenschützer glauben, haben sehr viele ein riesiges Interesse. Wir hatten gestern eine Diskussion zur Suchmaschine mit Google. Die sagen natürlich, die IP-Adresse, das ist für uns die Wunderwaffe mit der wir Werbung betreiben können, mit der wir Nutzungsprofile erstellen können, mit der wir eben alle möglichen Interessenprofile erstellen können, um auch alle möglichen Konsequenzen, Persönlichkeitsprofile daraus abzuleiten. Und genau das ist auch der Hintergrund, weshalb die Strafverfolgungsbehörden an diesen Daten ein so großes Interesse haben. Weil es effektive Informationen sind, mit denen etwas erreicht werden kann. Also, zu behaupten, es handele sich hier um eine Banalität, zeugt nicht unbedingt von Kenntnis.

Das Beispiel von anderen Ländern. Ich weiß, dass sehr viele andere Länder darüber diskutieren, es teilweise auch schon praktizieren. Irland z. B. hat ja vor dem Europäischen Gerichtshof geklagt. Ich kenne keine empirischen Untersuchungen, also vergleichende empirische Untersuchungen. Aber Ergebnisse, die mir von Kollegen aus den anderen Ländern mitgeteilt werden, belegen, dass sehr sehr wenig Gebrauch davon gemacht wird, weil es im Augenblick auch technisch noch wahnsinnig schwierig ist. Je einfacher aber dann diese Daten zur Verfügung gestellt werden, desto schneller werden diese Daten auch genutzt werden, desto umfangreicher werden diese Daten genutzt und dann denke ich, wird vielleicht auch der eine oder andere Betrug damit aufgeklärt werden. Aber im Verhältnis zu der Gesamtkriminalität hat das in keinem der Länder auch nur ansatzweise erkennbar einen Effekt gehabt.

Zur Zweckbindung: Die Kontodatenentscheidung des Bundesverfassungsgerichts ist mir wohl bekannt und ich bin auch nicht ganz, muss ich Ihnen ehrlich sagen, glücklich über das, was das Verfassungsgericht insofern – insbesondere was die Transparenz angeht – entschieden hat. Aber bei den Kontodaten hat das Bundesverfassungsgericht gesagt, ist ganz klar eine Beschränkung auf definierte Zwecke notwendig. Diese definierten Zwecke, die finde ich in dem Gesetzentwurf,

den ich heute hier zu beurteilen habe, leider nicht. Da heißt es eben nicht „schwere Straftaten“. Das heißt es auch, aber nicht alleine. Sondern es wird noch eine Vielzahl von weiteren Nutzungszwecken dazu aufgeführt. Ich habe es schon in meinem Eingangsstatement genannt. Und da kann man definitiv nicht mehr von hinreichend definierten Zwecken sprechen und es ist nicht nur die Zweckbindung, die vom Verfassungsgericht gefordert wird. Es sind auch die Bestimmtheit der Regelung und die Erforderlichkeit der Daten für diesen Zweck nicht gegeben, auch diese Anforderung des Verfassungsgerichts sehe ich bei diesem Gesetzentwurf nicht erfüllt.

SV Prof. Dr. Michael Ronellenfitsch: Alle Fragenden bitte ich, mir zu gestatten, dass ich die Fragen, die im Zusammenhang stehen, einheitlich behandele. Es ist der Komplex des Abwägungsgebots und der Pressefreiheit. Das, was isoliert ist, ist die Frage der europarechtlichen Würdigung und der verfassungsrechtlichen Würdigung, die zum anderen Komplex überleitet. Aber ich bemühe mich, alle Fragen, um abzukürzen, zusammenhängend zu behandeln.

Was den europarechtlichen Aspekt betrifft, so ist einzuräumen, dass ein Nichtigkeitsverfahren vor dem europäischen Gerichtshof stattfindet. Aber bis dieses Verfahren durchgeführt worden ist, ist die Richtlinie für uns verbindlich und es besteht eine Umsetzungspflicht. So, wie ich Ihre Frage verstanden habe, war die Konstellation eigentlich mehr die, ob die Vorratsdatenspeicherung europarechtswidrig ist. Europarechtswidrigkeit ist im Augenblick in der Diskussion. Dann müssten Sie das vergleichen mit der Datenschutzrichtlinie in Relation zu der Richtlinie, die die Vorratsdatenspeicherung vorsieht. Und da fällt es mir sehr schwer, zu begründen, warum das europarechtswidrig ist, denn es sind zwei gleichrangige Richtlinien. Sie müssten dann höchstens sagen, es gibt höherrangiges Primärrecht, das entgegensteht, europäische Grundrechte, die zu beachten sind. Und das sind Dinge, die mir – ehrlich gesagt – zu heikel sind, vor einer Entscheidung des Europäischen Gerichtshofs abschließend zu beurteilen. Ich kann Ihnen meine Beurteilung sagen, was nützt Ihnen das?

Jörg van Essen (FDP): Ich würde die schon ganz gerne wissen. Das Urteil kann ich später lesen, jetzt interessiert mich Ihre Beurteilung, Herr Professor.

SV Prof. Dr. Michael Ronellenfitsch: Nach meiner Beurteilung ist es europarechtskonform – genauso, wie es verfassungskonform ist. Das, was unsere gemeinsame europäische Rechtskultur ist, das Zentrum, das über allem steht, ist das Bekenntnis zur Menschenwürde, zur individuellen Selbstentfaltung, zur informationellen Selbstbestimmung und das werde ich jetzt beantworten im Zusammenhang mit der Abwägung, ob die beeinträchtigt ist oder nicht. Ich habe ja vorhin versucht anzudeuten, dass die Abwägung im Ergebnis ein Mosaik ergibt. Sie ergibt ein Bild und das besteht aus vielen Einzelteilen und auf der Waagschale liegt auf der einen Seite alles das, was grundrechtsrelevant ist, und das, was ich mit Monstranz bezeichnet habe, mit der informationellen Selbstbestimmung, das war nicht, um sie abzuwerten, sondern um zu sagen, es nützt nichts, wenn ich mich nur auf dieses Schlagwort berufe, sondern ich muss alle Grundrechte, die hier einschlägig sind, in die Waagschale werfen. Das leitet über zu Ihrer Frage, Herr Stünker. Sie haben ja gesagt, es betrifft nicht unmittelbar den Kernbereich der Menschenwürde, der Lebensgestaltung. Es betrifft den externen Bereich. Aber es geht nicht um die Frage nur allein, was Sie mit jemandem besprochen haben, um den Inhalt. Von fundamentaler Bedeutung ist natürlich auch, mit wem Sie wann wo gesprochen haben. Und der Kommunikationsvorgang insgesamt ist so essentiell für die menschliche Lebensgestaltung, dass wir uns ja nicht irgendwie einfrieren oder einbunkern können in Häusern, sondern wir müssen kommunizieren und immer mehr kommunizieren und da sind noch eine Fülle von Grundrechten berührt. Herr Dr. Weichert hat zu Recht das Telekommunikationsgeheimnis angesprochen. Die ganze Art sich zu artikulieren, die Lebensgestaltung, ist stark kommunikationsgeprägt. Wir sind soziale Wesen, das brauche ich nicht zu vertiefen, aber ich hoffe, dass klar ist, dass die Vorgänge, die die Kommunikation als Gesamtbild ergeben, in der Summe bei der Abwägung so gewichtig sind auf der einen Seite der Waagschale, dass auf der anderen Seite der Waagschale mindestens gleichrangige Rechtsgüter stehen müssen. Und das ist für mich das Entscheidende. Die Zweckbindung ist ein datenschutzrechtlicher Grundsatz. Klar, aber bei der verfassungsrechtlichen Abwägung kommt es darauf an, welche Rechtsgüter ich schütze. Bei Höchstkriminalität und bei terroristischen Anschlägen muss ich zugestehen, trotz meiner Funktion als Datenschützer, dass mir die Abwägung reicht. Der Kommunikationsbereich auf der einen Seite und auf der anderen Seite der Bereich

der Schwerstkriminalität. Bei der Gefahrenabwehr ist die Frage, ob ich jede läppische Gefahrenabwehr für die öffentliche Ordnung ausreichen lasse. Das reicht natürlich nicht. Aber bei Gefahrenabwehr geht es ja auch um die Sicherheit des Ganzen und es geht um höchstwerte Rechtsgüter. In dem Fall reicht mir auch die Gefahrenabwehr. Und ich muss Ihnen auch sagen, Herr Dr. Weichert, im Gegensatz zu Ihrer Position, die Straftaten, die mit Mitteln der Telekommunikation begangen werden, die man noch präzisieren könnte, genau gegen die richtet sich ja meine Überwachungstendenz. Die reichen aus, man darf nur nicht eine Generalklausel einführen oder so Larifari-Worte wie „Straftaten von erheblicher Brisanz“ oder so etwas Ähnliches. Das reicht nicht. Wenn jemand am Feiertag irgendwo mit dem Ghettoblaster herummarschiert, ist das nicht irgendwie signifikant.

Aber ich meine, Herr Benneter, ich hoffe, wir sind uns einig, wie ich es konzeptionell verstehe bei der Abwägung. Ich kann Ihnen jetzt keine feste Grenze markieren, dann wäre ja das Ergebnis der Abwägung vorweggenommen. Die Abwägung ist nur das Ziel zu einer Grenze und es muss gleichrangig sein: Auf der einen Seite das Gewicht der informationellen Selbstbestimmung, die Kommunikationsfreiheit, die ein Höchstwert von Verfassungsrang ist und auf der anderen Seite die genau gleichrangigen Höchstwerte, die die Einschränkung rechtfertigen. In diesem Bereich, und das ist schwer zu formulieren, aber in diesem Bereich muss ich natürlich auch die zusätzliche Argumentationsschiene einführen, die Berufsgeheimnisträger. Das war die Frage zur Pressefreiheit. Die Presse hat ja keinen Freibrief, alles machen zu dürfen, was der Normalbürger nicht darf. Die Schranken der Pressefreiheit sind nur gezielt gegen die Presse, gezielte Grundrechtseinschränkungen gegen eine bestimmte Meinung, aber diese Annextätigkeiten, die Informantengeheimnisse und dergleichen mehr, sind nicht völlig unaushöhlbar. Wenn ich als Presseorgan einen Informanten habe, der mir sagt, an dem oder dem Tag kommt ein Selbstmordattentäter und versucht, ein Kernkraftwerk in die Luft zu jagen, ja dann muss ich Ihnen ehrlich sagen, dann ist mir die Pressefreiheit in dem Fall nachrangig. Das ist das, was ich mit der Abwägung darzustellen versucht habe. Sie müssen sammeln, was an Abwägungsbelangen eine Rolle spielt, gewichten und einander gegenüberstellen. Ich hoffe, dass ich damit die Fragen abschließend beantwortet habe.

Vorsitzender Andreas Schmidt (Mülheim): Vielen Dank, Herr Prof. Dr. Ronellenfitsch. Jetzt bitte Herr Dr. Liedtke auf die Fragen der Kollegen Stünker und Leutheusser-Schnarrenberger.

SV Dr. Rainer Liedtke: Herr Stünker, zunächst zu Ihren Fragen, welche Daten wir künftig zusätzlich speichern müssen. Das, was wir im Moment speichern, ist ja in der Tat nur das Abrechnungsrelevante, d. h. im Wesentlichen die Gespräche, die Sie selber führen. Da brauchen wir natürlich die Daten, um Ihnen hinterher die Rechnung zu schreiben. Was wir künftig im Rahmen der Vorratsdatenspeicherung zusätzlich erheben müssen, ist im Bereich der Bestandsdaten schon einmal die Endgerätenummer. Vielleicht noch einmal ganz kurz der Hinweis dazu, dass bereits heute 40% der Endgeräte eben nicht im Zusammenhang mit Mobilfunkverträgen verkauft werden, sondern auf ganz anderen Wegen. Damit stellt sich auch schon die Frage, inwieweit dort eine Wettbewerbsverzerrung zwischen den Point-of-Sale-Geschäften besteht, die die Mobilfunkverträge mitverkaufen, und den Geschäften, die nur reinen Zubehörhandel betreiben. Dann kommt natürlich der gesamte sogenannte Incomingverkehr dazu, also die ganzen Gespräche, die in unser Netz hineinkommen, die wir im Moment nur in ganz seltenen Fällen, eben dann, wenn sie auch abrechnungsrelevant sind, z. B. bei Roaming etc., auch speichern müssen. Die müssten wir jetzt versuchen, vollständig zu speichern. Wenn Sie selber telefonieren, dann haben wir natürlich Ihre Daten, mit wem Sie wann wie lange telefoniert haben, die speichern wir natürlich, um Ihnen eine vernünftige Rechnung zu stellen. Wenn Sie aber ein Gespräch bekommen, dann kriegen Sie normalerweise dafür keine Rechnung. Wir sind ja nicht in China, in China werden auch solche Gespräche vergebührt, aber bei uns wird das nicht gemacht. Es sei denn, Sie befinden sich im Ausland, dann wird ja der Anteil, der dadurch entsteht, dass das Gespräch ins Ausland geleitet wird, Ihnen in Rechnung gestellt und diese Gespräche müssen wir natürlich auch erfassen. Die erhalten wir aber in der Regel erst mit deutlicher Verzögerung, weil wir von unseren Partnern, den Netzbetreibern, die Daten erst mit deutlicher Verzögerung bekommen. Die Daten müssten wir zusätzlich speichern. Dann gibt es so ein paar Kleinigkeiten, die technisch ziemlich brisant sind. Wir müssten nämlich nicht nur die Verbindungsdaten speichern von den eingehenden Verkehren, sondern auch zusätzliche Daten, wie Endgerätenummer und IMSI-Nummern, alles Daten, die wir eigentlich technisch gar nicht zur Verfügung

haben, die müssten wir auch noch speichern. Hinzu kommen noch die Daten für eventuelle Um- und Weiterleitungen. Wenn Sie jetzt z. B. Ihren Partner anrufen und dieser hat sein Gespräch weitergeleitet, umgeroutet auf irgendein anderes Endgerät, dann müssten wir das, auch wenn das in unserem Netz nicht unbedingt nachvollziehbar ist, wahrscheinlich auch speichern. Hinzu kommt das Thema Standortdaten. Wir müssen jetzt noch viel deutlicher auch dokumentieren, welchen Zustand das Netz im Moment hat, um letztendlich dann auch im Zweifel nachweisen zu können, was vor einem halben Jahr über welche Zelle gelaufen ist. Das müssen wir ja auch nach einem halben Jahr noch nachvollziehen können. Das sind Dinge, die wir heute überhaupt nicht nachhalten. Sie müssen davon ausgehen, dass so ein Mobilfunknetz ein sehr dynamisches Netz ist, d. h. wenn Sie heute ein Netz aufbauen, dann sieht das in drei, vier Wochen ganz ganz anders aus. Dann haben auch die Zellennamen gewechselt. Alle diese Dinge müssten wir nachvollziehen, um die im Zweifel dann auch für ganz alte Daten noch einmal in irgendeiner Art und Weise aufrechterhalten zu können.

Wir haben den gesamten Bereich des IP-Verkehrs. Wir sind ja nebenbei letztendlich auch Access-Provider, Sie können über Mobilfunk auch auf das Internet zugreifen. Damit kommen wir auch in die ganzen Speicherpflichten bezüglich des IP-Verkehrs, wobei wir, was die IP-Nummern angeht, noch ein ganz besonderes Schmankerl haben. Der Nummernraum der öffentlichen IP-Adressen ist sehr stark eingegrenzt, was zur Folge hat, dass wir als E-Plus-Mobilfunk auch nur eine geringe Anzahl von IP-Adressen im öffentlichen Raum haben. Intern federn wir das dadurch ab, dass wir private IP-Adressen, also IP-Adressen, die nicht nach außen sichtbar sind, nutzen, aber sobald sie über eines unserer Gateways in das öffentliche Internet wandern, bekommen sie von uns auf temporärer Basis eine IP-Nummer zugeordnet. Da diese Anzahl der IP-Nummern, die wir haben, nicht ausreichen, müssen wir auch noch auf Port-Basis runter, sozusagen auf eine Untergruppierung. Das alles geschieht temporär, d. h. in diesem Moment haben Sie die IP-Adresse XY mit dem Port sowieso und zwei Sekunden später hat ein ganz anderer Kunde diese Nummer. Das ist natürlich auch so ein Punkt, wo man sich fragen kann, wie greift das Ganze überhaupt? Es dürfte fraglich sein, ob Sie im freien Internet auf den Servern überhaupt diese Portadressen, -informationen mitgespeichert haben, so dass am Ende wahrscheinlich Anfragen auf uns nach IP-Adressen zu einem bestimmten

Zeitpunkt zukommen. Und da können wir nur sagen, einer von dieser Gruppe von 785.000 Kunden war es. Das ist eine zusätzliche Problematik. Ich denke, das reicht erstmal zu dem Thema. Es ist wirklich ein ganzer Haufen von Daten, es ist eben nicht damit getan, dass man mal eben ein paar mehr Platten in die entsprechenden Server reinschraubt und damit dann die verlängerte Speicherfrist realisiert.

Zum zweiten Thema von Frau Leutheusser-Schnarrenberger. Da ging es darum, welche Daten wir heute schon liefern, welche Auswertungen möglich sind. Die Ausführungen von Herrn Wirth – die Mordfälle, die er ansprach – haben ja gezeigt, dass er heute schon in der Lage ist, mittels genau dieser Daten auch die entsprechenden Schlüsse zu ziehen und diese Mordtaten aufzuklären. Auch die sogenannten Funkturmbeschlüsse, also gesamte Verkehrsdaten zu bestimmten Bereichen zu übermitteln. Das geht mit tatsächlich ganz konkreten Punkten los, endet dann im Zusammenhang damals mit den Terrorattentaten oder versuchten Attentaten auf den Regionalexpress in Nordrhein-Westfalen, dass man die Verkehrsdaten für den gesamten Weg dieses Zuges von A bis Z heraussuchen sollte, wo man einfach auch technisch an die Grenzen stößt. Aber wenn man das vernünftig eingrenzt, kann man das auch heute machen. Auch die unverzügliche Standortausleitung ist mit einem entsprechenden Beschluss natürlich möglich. Dazu brauche ich nicht die abgesenkten Eingriffsschranken des § 100 g StPO-RegE. Auch wenn Herr Wirth vielleicht darauf abzielen wollte, nach § 100 g StPO-RegE würde er ja auch diese Standortdaten nicht in Echtzeit bekommen, denn gerade da sind sie ja nach dem Gesetzestext ausgeschlossen. Die Echtzeitdaten über den Standort bekommt er auch heute schon und wir haben ja diese Daten, die ich eben kurz skizziert habe, auch für einen ganz erheblichen Zeitraum bei uns im Hause, ca. ein Vierteljahr, vorrätig, und es gibt ganz selten Anforderungen, die über diesen Zeitraum hinausgehen.

Vorsitzender Andreas Schmidt (Mülheim): Vielen Dank. Jetzt hat das Wort Herr Grützner zur Beantwortung der Fragen der Kollegen Montag und Leutheusser-Schnarrenberger.

SV Jürgen Grützner: Herzlichen Dank. Zunächst einmal muss man wissen, dass IP-Adressen wirklich zu den sensibelsten Identifikationsmöglichkeiten gehören, die

wir heute haben. Ich kann daraus komplette Profile erstellen. Sie würden bei mir heute feststellen können, dass ich um 7.15 Uhr angefangen habe, im Internet die ersten Mails abzurufen und dort Mails abzusenden. Das war in Düsseldorf, dann habe ich mich in Düsseldorf am Flughafen das zweite Mal eingeloggt. Das dritte Mal würden Sie sehen, dass ich mich in Berlin eingeloggt habe. Sie können aus diesen IP-Adressen komplette Bewegungsprofile generieren. Die EU sieht eine Speicherung der IP-Adresse wohl auch aus diesem Grunde nicht vor. Das ist eine Eingriffstiefe, die nach unserer Kenntnis rechtlich, was die EU-Vorgaben angeht, nicht vorgegeben ist, so dass hier das deutsche Gesetz über die Anforderungen der EU hinausgeht. Das entspricht aus unserer Sicht nicht dem, was die ursprüngliche Beschlusslage auch im Deutschen Bundestag gewesen ist. Wir haben zusätzliche Probleme, was den Mobilfunkbereich angeht. Es gibt weitere erhebliche technische Probleme, hier die Daten zusammenzufassen. Die Speicherung der Daten an sich ist nicht das Problem, wie so oft, sondern nachher die Zusammenfügung dieser Datensätze mit den jeweiligen Betreibern zu den jeweiligen Personen. Das erfordert nicht irgendeinen Speicheraufwand, sondern das erfordert sozusagen Arbeitsspeicher, das erfordert aktives Equipment, was bei den Unternehmen mit erheblichen Kosten zu Buche schlägt. Insofern ist das also auf der einen Seite ein sehr relevanter Faktor, was die Inhalte angeht, auf der anderen Seite ein sehr teurer Faktor für die Unternehmen. Dies vielleicht zu der Frage der dynamischen IP-Adressen. Im Übrigen werden im Festnetz natürlich IP-Adressen auch für eigene Zwecke z. T. über eine bestimmte Frist, nämlich zu Abrechnungszwecken, gespeichert. Wenn man dies jetzt auf ein halbes Jahr ausdehnt, kommen Mengen auf die Unternehmen zu. Nicht wiederum was die Speicherung angeht, sondern was die Auswertung nachher angeht und das Zusammenfügen der Daten, die die Unternehmen vor völlig neue Probleme stellen. Da geht es nicht mehr darum, ein paar Speicherchips einzusetzen, sondern sie brauchen, wenn sie zeitnah ein Ergebnis produzieren wollen, ein völlig anderes Softwareequipment, um hierauf zugreifen zu können.

Der zweite Punkt. Ich kann meinem Vorredner nur zustimmen. Ich glaube, die Fälle, die Herr Wirth gebracht hat, sind mit den heutigen Mitteln lösbar gewesen. Das hat er selber gesagt, das finde ich ganz beeindruckend, wir brauchen deswegen keine Erweiterung dieser Möglichkeiten. Die Unternehmen helfen den Strafverfolgungsbehörden in vielen Fällen oft in Minutenschnelle und arbeiten in

hervorragender Weise mit den Strafverfolgungsbehörden zusammen. Erschwert wird die Arbeit mit den Strafverfolgungsbehörden dadurch, dass es unterschiedliche Datenformate gibt, die verwendet werden, unterschiedliche Schnittstellen, die verwendet werden. Das Problem ist seit langem bekannt. Es wäre, was die Qualität und den Preis sowohl für uns als auch für die Strafverfolgungsbehörden angeht, ein Leichtes, hier Millioneneinsparungen vorzunehmen, wenn man sich ein paar Gedanken über eine bessere Zusammenarbeit machen würde und das nicht an Kommunal- oder Landesgrenzen enden lassen würde, denn hier haben die Länder auch wiederum ihre ganz besonderen Befugnisse, die sie weidlich ausnützen. Telekommunikation ist kein Landesrecht und Telekommunikation ist keine Landestechnologie. Also wenn wir hier auf beiden Seiten deutlich einsparen wollen, dann gibt es dazu noch enormes Potenzial. Bevor man so ein Gesetz macht, sollte man auch erstmal schauen, dass beide Seiten ihre Hausaufgaben machen und hier zu vernünftigen Regelungen untereinander kommen. Die wirtschaftliche Belastung der Unternehmen ist durch das Vorhalten der Technologie, die ich für die Speicherung und für die nachfolgende Abfrage brauche, enorm. Und zwar völlig unterschiedlich, die Unternehmen haben hier sehr unterschiedliche Kosten und sie haben vor allem ganz unterschiedliche Abfragemengen. Das Beispiel aus der letzten Anhörung finde ich eklatant. QSC ist ein mittelständisches Unternehmen, das 400.000 Euro für das Equipment im Jahr gezahlt hat, um die Technik bereitstellen zu können, etwa 100.000 Euro an Personalkosten. Es hat im ganzen letzten Jahr eine einzige Abfrage gegeben. Das ist auf Seiten der Deutschen Telekom vielleicht ein Problem, das kann man noch auf ein paar Hundert Euro runterrechnen, weil die Zahl der Abfragen entsprechend groß ist, immer noch kein Vergleich zu dem, was heute die Entschädigung hergibt. Aber da habe ich eine ganz andere Größenordnung, da komme ich vielleicht auf 300 Euro oder so etwas, statt auf 17 Euro. Aber für ein Unternehmen, das für eine Abfrage 500.000 Euro zur Verfügung stellen muss, ist dies außerhalb dessen, was aus meiner Sicht auch aus verfassungsrechtlichen Gründen noch unter dem Gesichtspunkt Sozialpflichtigkeit gesehen werden kann. Wenn der Staat dies von einem Unternehmen verlangt, muss es hier in Anwendung des Verhältnismäßigkeitsgrundsatzes aus unserer Sicht eindeutig zu einer angemessenen Entschädigung kommen.

Vorsitzender Andreas Schmidt (Mülheim): Vielen Dank, Herr Grützner. Jetzt hat das Wort Herr Dr. Graf auf die Fragen der Kollegen Kauder, Montag und Benneter.

SV Dr. Jürgen-Peter Graf: Zunächst zur Frage des Abgeordneten Kauder nach der Einschränkung der Journalisten durch solche Aufzeichnungen. In dem Gesetzentwurf der Bundesregierung, der die Speicherung vorsieht, ist ja auch § 53 b StPO-RegE enthalten, den wir am Mittwoch ausgeklammert haben. Ich gehe davon aus, dass der dann genau so Gesetz wird und dass hier die Journalisten in diesem Bereich durchaus geschützt sind. Natürlich kann so eine Abfrage in einem konkreten Fall dazu führen, dass auch der Journalist mit einem Europol-Mitarbeiter gesprochen hat. Das räume ich ohne weiteres ein, aber damit ist doch nicht automatisch der Verdacht einer Straftat gegeben und damit dürfte diese Information auch hier nicht verwertbar sein. Es sei denn, man hätte aus anderen Randinformationen Hinweise, dass auch im Europol möglicherweise ein solcher Verdacht vorliegt, der strafrechtlich relevant wäre. Also, insofern denke ich, dass hier im Zusammenhang mit den Vorschriften des § 53 b StPO-RegE ein ausreichender Schutz gegeben ist.

Zur Frage des Abgeordneten Montag. Herr Montag, mit der Erzählung meines persönlichen Falles wollte ich natürlich auch etwas provozieren und das scheint mir gelungen zu sein. Es ist so, dass Sie völlig Recht haben. Natürlich kann durch den Umstand der Speicherung von Daten ein Verhalten geändert werden. Das Verhalten kann aber auch dadurch geändert werden, dass ich das Gefühl habe, dass ich mich in einem unsicheren Bereich bewege. Nicht umsonst hat es etwa acht Jahre gedauert, seit 1995, wenn wir da etwa den Startpunkt setzen, bis E-Commerce sich überhaupt durchsetzen konnte. Es gibt heute noch sehr viele Leute, die sagen, ich mache kein E-Banking, weil ich Angst habe, dass da etwas passiert und ich bezahle auch nicht mit einer Kreditkarte im Internet. Wenn allerdings bekannt wird, dass es hier Bereiche gibt, in denen Straftaten schlichtweg nicht aufklärbar sind, dann denke ich, wird auch das zu einer Verhaltensänderung führen und es könnte sein, dass dann sehr schnell das Pendel in die andere Richtung ausschlägt. Deswegen bleibe ich bei meiner Auffassung, dass hier die Speicherung eher dazu beiträgt, das Vertrauen ins Internet zu steigern. Es ist auch so, was die Bevölkerung betrifft – ich erlebe es zwar nicht täglich, aber doch in monatlichem Abstand – dass beispielsweise im Strafverfahren, wenn man einen Beweis mangels Verwertungsverbot nicht

berücksichtigen kann und es dann möglicherweise zu einem Freispruch führt, dass die Betroffenen mit großem Unverständnis reagieren. Sie können es kaum nachvollziehen, dass hier ein Nachweis nicht gelungen ist und man unter Umständen einen Straftäter freisprechen muss. Das ist aber hinzunehmen, denn sonst hätten wir ja kein Beweisverwertungsverbot. Wenn ich aber Beweismittel, die keinem Verwertungsverbot unterliegen, durch Löschung vernichte, ist es etwas anderes. Denn hier liegt ja kein Grundrechtsverstoß, auch kein Verstoß gegen die Rechte Betroffener vor, wenn ich, was Prof. Dr. Ronellenfitsch sagte, es hinnehmen kann, dass die Speicherung als solche vorgenommen wird. Daher denke ich, es ist durchaus, da beharre ich darauf, für die normalen Bürger hinnehmbar, dass ich sage, ich sichere mich ab, dass eine individuelle Straftat auch aufgeklärt werden kann, wenn ich solche Mittel zur Verfügung habe.

Nun zu dem, was der Abgeordnete Benneter zum offenen Warenhaus sagt. Es war natürlich ein drastisches Beispiel, aber wenn ich tatsächlich rechtsfreie Räume im Internet schaffe, weil ich nicht mehr in der Lage bin, hier zu ermitteln und wenn für einen Täter keinerlei Gefahr besteht, ermittelt zu werden, weil eben, bis die Straftat bekannt wird, die IP-Adresse weg ist, dann fragt sich natürlich auch, inwieweit ich dann noch mit Recht Straftaten im so genannten „real life“ bestrafen kann, dann kann man auch sagen, dann muss der Warenhausdieb oder ähnliches in diesem Bereich eigentlich auch nicht mehr bestraft werden oder er kann einwenden, das wäre nicht so. Also, das ist ein sehr komplexer Bereich, aber man muss doch schon sehen, dass Betroffene ganz anders reagieren, als wenn sie eben nicht betroffen sind und wie gesagt, das Ganze kann auch Auswirkungen auf das Verhalten haben. Und, Herr Vorsitzender, gestatten Sie mir eine Bemerkung, nur zwei Sätze zum Vorwurf von Herrn Weichert. Herr Weichert, Sie haben ganz geschickt das IP-Datum mit Inhaltsdaten verknüpft, da aber Inhaltsdaten nicht gespeichert werden dürfen, ist es einfach schlichtweg falsch.

(Unverständliche Zwischenbemerkungen)

SV Dr. Christoph Fiedler: Die Frage des Abgeordneten van Essen bezog sich auf die Europarechtskonformität, die Verfassungsmäßigkeit der Vorratsdatenspeicherung. Bei der Europarechtskonformität geht es wohl um die Richtlinie. Wir unterscheiden

hier zwischen formeller und materieller Seite. Bei allen unterscheiden wir, wie Herr Prof. Ronellenfitsch das schon zutreffend gemacht hat, zwischen der Ansicht, die man natürlich für die richtige hält und dem, was Richter irgendwann sagen werden, worauf man dann Ansichten revidiert oder nicht. Meine Ansicht bei der formellen Seite ist die, dass die Richtlinie auf die falsche Ermächtigungsgrundlage gestellt wurde. Art. 95 EG-Vertrag ist absolut nicht die richtige Ermächtigungsgrundlage. Würde man noch Europarechtswidrigkeitspunkte für die Unwürdigkeit eines Gesetzgebungsverfahrens hinzunehmen, dann würde auch das noch mehr für die formelle Nichtigkeit der Richtlinie sprechen. In dem Punkt meine ich auch, dass es berechtigte Aussichten gibt, dass der EuGH in diesem Fall ausnahmsweise mal konsequent bleiben wird und, dass er diese Richtlinie für nichtig erklären wird.

Hinsichtlich der materiellrechtlichen Vereinbarkeit beantworte ich nur die Frage nach der Vereinbarkeit mit Primärrecht. Das wären hier im Wesentlichen Grundrechte, die sich einmal ergeben können aus der Bindung auch des europäischen Sekundärrechts an die europäische Menschenrechtskonvention und an die Grundrechte des Primärrechts, die da ja als ungeschriebene Rechtssätze stehen. Ob sie effektiv sind, ist eine andere Frage. Das hängt natürlich davon ab, welchen Inhalt man diesen Grundrechten gibt. Der Europäische Gerichtshof ist bislang, das zweite Tabakwerbeurteil hat es gezeigt, nicht besonders erpicht darauf, europäische Grundrechte materiell auszufüllen und gegenüber den beiden anderen Organen Europas durchzusetzen. Dennoch meine ich, kann man gut vertreten, dass auf der dritten Stufe der Verhältnismäßigkeit der Vorteil durch die Vorratsdatenspeicherung angesichts der Schwere der Eingriffe in die Grundrechte von fast 500 Millionen Europäern zu gering ist. Wobei ich dazu sagen muss, dass auf dieser dritten Stufe, anders als auf der Erforderlichkeitsstufe, nach verbreiteter Ansicht – und ich glaube auch nach zutreffender Ansicht – des Bundesverfassungsgerichts und auch der europäischen Gerichte mildere Mittel einbezogen werden dürfen. Um es klar zu machen, auf der Erforderlichkeitsstufe scheitert die Vorratsdatenspeicherung nicht am Quick-Freeze-Verfahren, weil man immer sagen kann, die Vorratsdatenspeicherung ist ja noch ein Stück effektiver als das Quick-Freeze-Verfahren. Aber auf der dritten Stufe, wenn man da das Quick-Freeze-Verfahren hinzunimmt, kann man sagen, die Vorteile der Vorratsdatenspeicherung mit ihrer allumfassenden rückwirkenden Erfassung der Kommunikationsgeschichte aller

Bürger im Verhältnis zum Quick-Freeze-Verfahren sind zu gering im Verhältnis zu den massiven Nachteilen, die die verdachtlose Speicherung der Kommunikationshistorie für alle 450 Millionen Europäer mit sich bringt.

Wenn man das so sieht, wird man sich nicht wundern, wenn ich das gleiche auch für den grundgesetzlichen Maßstab sage. Bei dem grundgesetzlichen Maßstab gibt es aber noch andere Angriffspunkte, die sich auch dann ergeben, wenn man dem Schluss nicht folgt. Die ergeben sich daraus, dass die Umsetzung des Regierungsentwurfs natürlich konkret wird. Die Richtlinie sagt eigentlich nur „schwere Straftaten“. Das könnte man, wie wir das für allein richtig halten, als grundrechtsschonende Minimalumsetzung übernehmen, also wirklich beschränken beispielsweise auf terroristische Straftaten oder eben vergleichbar schwere Straftaten. Man kann es auch so machen, wie das die Bundesregierung jetzt macht, also Gefahrenabwehr, Verfassungsschutz und ein weites Feld an Straftaten, ein Großteil der Straftaten. In dem Fall lässt sich gut vertreten und auch dem würde ich persönlich als Jurist zuneigen, dass die Weite der Zugriffsermächtigungen auch die Quantität der Zugriffe auf diese gespeicherten Daten so erhöht wird, dass man von unverhältnismäßigen Beeinträchtigungen sprechen kann. Das wird noch verschärft, wenn es Fälle geben sollte, von denen es wahrscheinlich viele gibt, von denen die Bürger gar nichts erfahren. Das ist ein wichtiger Aspekt, ein verfahrensrechtlicher Aspekt, der besonders für Journalisten gilt. Wenn ihre Kommunikationshistorie, die – wie ausgeführt wurde – teilweise ja schon zu einem Lebensprofil werden kann, wenn die gespeichert wird, verdachtslos, ohne dass sie einen Anlass geben, und es wird dann darauf zugegriffen und der Staat verwertet sie, aber sie erfahren es gar nicht, dann steigert das den Eingriff noch mehr.

Ich habe jetzt einen Punkt übersprungen, der bei der verfassungsrechtlichen Prüfung sicherlich eine Rolle spielen wird und der auch schon angesprochen wurde. Man kann natürlich sagen – und das ist vielleicht der Paradigmenwechsel und ist vielleicht eine der spannendsten Fragen einer verfassungsmäßigen Entscheidung: Ist es überhaupt zulässig für einen grundrechtlich gebundenen Rechtstaat, die Kommunikationsverbindungshistorie aller seiner Bürger auch ohne konkreten Anlass gegenüber dem einzelnen Bürger aufzuzeichnen? Hat also ein grundrechtlich gebundener Rechtstaat das Recht zu sagen, dass meine Kommunikations-

verbindungshistorie gespeichert wird? Er muss ja einen Grund angeben, einen Grund mir gegenüber, obwohl ich keinen Anlass gebe für irgendein verdächtiges Verhalten, für eine Gefahr: Ich bin kein Gefährder, auch kein potenzieller Gefährder. Er muss einen Grund angeben für den Fall, dass ich irgendwann doch noch einmal etwas Böses mache oder dass, auch ohne etwas Böses zu machen, diese Daten im Kontext mit einer Straftat relevant werden. Das ist eine sehr interessante Frage, auf deren Antwort man gespannt sein kann. Aber die Sachen, die ich davor nannte, sind davon unabhängig.

Ich möchte als letzten Punkt auf die Presse zu sprechen kommen. Einfach deshalb, weil die verfassungsrechtlichen Anforderungen jedenfalls mit dem Regierungsentwurf u. E. unterschritten sind. Die bloße Verhältnismäßigkeit ist, wie gesagt, nicht geeignet, Vertrauen zu bilden. Es geht nicht um einen absoluten Schutz, den gibt es auch gar nicht. Aber es geht doch um einen Schutz, der jedenfalls in der Regel und tatsächlich praktikabel erscheint. Da meinen wir, auch im Licht der Cicero-Entscheidung, die ja noch weiter geht, dass zumindest der Verstrickungsverdacht plus die Verhältnismäßigkeit auch hier bei der Vorratsdatenspeicherung vor dem Zugriff auf die journalistische Kommunikationsgeschichte im Gesetz stehen müssen. Hinzukommen muss jedenfalls auch die Benachrichtigung. Es kann nicht sein, dass sozusagen die Presse auch noch ohne die Möglichkeit gerichtlicher Kontrolle kontrolliert wird. Da gibt es dann auch, und das berührt die Verfassungsmäßigkeit insgesamt und nicht nur meinen beruflichen Background, da gibt es auch schon eine Besonderheit. Zur Demokratiebedeutung der Presse kann man viel erzählen. Aber in dem Fall stimmt sie, glaube ich, schon. Das Vertrauensverhältnis zwischen demjenigen, der seine Dienstgeheimnisverpflichtungen bricht und der Presse ist ja etwas Merkwürdiges. Der Staat hat ein legitimes Interesse daran, das Dienstgeheimnis zu schützen. Er hat sogar auch ein legitimes Interesse daran, Strafverfolgung einzuleiten. Dennoch sagt man nicht ohne Grund mit großem Streit immer wieder einfachrechtlich und verfassungsrechtlich, wir müssen, was ja eine Straftat ist, im Verhältnis zum Journalisten als Vertrauen schützen. Und der Grund dafür ist, dass – wenn das nicht so wäre – die Geschichte der Bundesrepublik sehr wahrscheinlich eine andere wäre. Man könnte ja mal hingehen und all die Fälle aufzählen, die zu durchaus gewichtigen und auch positiven politischen Veränderungen geführt haben, bei denen es um solche Vertrauensbrüche ging.

SV Dr. Patrick Breyer: Danke schön. Im Rahmen der Beantwortung der Fragen der Abgeordneten Korte und Leutheusser-Schnarrenberger wollte ich noch mal kurz auf die IP-Adressen eingehen, die hier sehr oft genannt und diskutiert worden sind. Es ist gesagt worden, die EU-Richtlinie sieht deren Speicherung nicht vor. Das muss man insofern klarstellen, als die Zugangsanbieter nach der EU-Richtlinie sehr wohl die IP-Adressen speichern sollen. Aber nicht die E-Mail-Anbieter, wie das hier im Gesetzentwurf erstmals drin ist. Im Referentenentwurf war das noch nicht enthalten. Herr Dr. Graf hat gesagt, in seinem Fall sei die IP-Adresse gelöscht gewesen, und es hätte deswegen keine Ermittlung stattfinden können. Da muss ich sagen, wenn der Straftäter einen chinesischen Dienst eingesetzt hat, um das Geld irgendwie bei Seite zu schaffen, war er sicherlich so versiert, auch einen internationalen Anonymisierungsdienst einzusetzen, so dass selbst wenn die deutschen Provider gespeichert hätten, sie da nicht weiter gekommen wären. Sie haben auch gesagt, im Internet bestünde derzeit eine Art rechtsfreier Raum, in dem Straftaten von vornherein nicht aufklärbar wären. Da kann ich nur sagen, das Internet oder die Telekommunikationsnetze sind genauso ein rechtsfreier Raum wie die Post, bei der ja auch nicht protokolliert wird, wer wem Briefe schreibt. Genauso rechtsfrei wie persönliche Gespräche, bei denen ja auch nicht protokolliert wird, wer mit wem wann spricht. Genauso wie der Straßenverkehr, bei dem nicht protokolliert wird, wer sich wann wo aufhält. Man muss sich immer vor Augen halten, dass der Anteil von Fällen, in denen wirklich Telekommunikation missbraucht wird, bei 0,001 % liegt, das heißt, dass die weitaus meisten Nutzer, Millionen von Menschen, sich wirklich keine Straftat zuschulden kommen lassen. Im Verdachtsfall ist sehr wohl gezielt ermittelbar und das Ergebnis zeigt die Aufklärungsquote. Wir haben bei den Straftaten eine durchschnittliche Aufklärungsquote von 55 % in allen Bereichen. Wir haben eine Aufklärungsquote von 80 % im Bereich Internetbetrug, im Bereich Urheberrechts-verletzung, im Bereich kinderpornografischer Materialien. Das heißt, im Internet sind schon jetzt mit den heute verfügbaren Daten sehr viel mehr Straftaten aufklärbar als bei allgemeinen Straftaten. Und das Bundeskriminalamt hat in einer Studie 381 Straftaten ermittelt, in denen Verbindungsdaten nach der bisherigen Rechtslage gefehlt hätten. Das ist – gemessen an der Gesamtzahl der jährlich nicht aufgeklärten Straftaten, das sind einige Millionen – gerade einmal 0,01 %. Das heißt, selbst wenn

man davon ausgeht, dass diese 381 Straftaten jährlich mehr aufgeklärt werden könnten, fällt das nicht ins Gewicht.

Sie haben auch gesagt, eine IP-Adresse sei nicht aussagekräftig. Da kann ich nur sagen, seit dem Urteil zur Volkszählung steht fest, dass Sie nicht auf das Datum selbst abstellen dürfen, sondern auf seine Nutzungs- und Verwendungsmöglichkeiten. Da ist es bei der IP-Adresse so, dass im Internet verbreitet protokolliert wird, welche IP-Adresse was bei Google sucht, welche Seiten Sie sich bei Amazon anschauen usw. usw. Das heißt, wenn Sie die IP-Adresse haben und die Verknüpfung mit der Person des Nutzers, können Sie das gesamte Internet-Nutzungsverhalten aufdecken. Und deswegen ist es zu kurz gegriffen, zu sagen, die IP-Adresse ist für sich genommen nicht aussagekräftig. Wenn Sie Telefongespräche abhören, ist es auch für sich genommen nicht aussagekräftig, wenn Sie nicht wissen, wer daran beteiligt ist. Also, das muss man schon im Zusammenhang sehen. Sie haben gesagt, die IP-Adresse sei nie missbraucht worden in der Vergangenheit. Da kann ich nur auf die Bonusmeilen-Affäre hinweisen, da hat ein Mitarbeiter von einem Unternehmen Daten mit sehr schwerwiegenden Folgen für die betroffenen Abgeordneten herausgegeben. Das heißt, es passiert durchaus, dass Mitarbeiter solche Daten illegal herausgeben. Es hat Durchsuchungen gegeben, irrtümlich, weil jemand ein offenes WLAN-Netz von einem Herrn benutzt hatte oder weil ein Straftäter Kreditkarten von jemand anderem missbraucht hatte und die Polizei bei dem Eigentümer durchsuchte und das war natürlich nicht der Täter. In England hat es Fälle gegeben, in denen die Menschen in Verdacht geraten sind, Kinderpornografie genutzt zu haben. Hinterher stellte sich heraus, dass nur jemand deren Kreditkartendaten missbraucht hatte. Aber es hat zu Suiziden geführt. Da haben sich Menschen umgebracht, weil sie sich von allen Seiten dem Verdacht ausgesetzt sahen – zu Unrecht – solche Kinderpornografie genutzt zu haben. Ich gebe Ihnen aber auch Recht, wenn Sie sagen, das sind Einzelfälle. Das kann man sicherlich sagen. Aber was kein Einzelfall ist, ist die allgemeine Befürchtung eines Missbrauchs, von der schon das Bundesverfassungsgericht sagt, die alleine schon sei zu berücksichtigen und das trifft jeden. Das ist kein Einzelfall. Sie haben das Beispiel des belgischen Journalisten genannt, der uns berichtet hat, seit Einführung der Vorratsdatenspeicherung in Belgien seien Kontakte gekappt worden, zu

Informanten in einer Partei, zu Regierungsbehörden. Das heißt, schon die Befürchtung des Missbrauchs von Jedermann hat ganz konkrete Auswirkungen.

Ihre letzte These war, dass die Bürger vermutlich damit einverstanden sind, verbesserte Strafverfolgung gegen die Aufgabe ihrer Privatsphäre einzutauschen. Da kann ich nur sagen, es gibt eine Forsa-Umfrage aus dem Juni 2007 genau zu dieser Frage. Dort hat eine Mehrheit eine sechsmonatige Speicherung der Verbindungsdaten als unangemessenen Eingriff abgelehnt. Übrigens auch eine Mehrheit der SPD-Wähler und auch unter den CDU-Wählern waren es 49 %. Also, es kann hier empirisch gesehen nicht die Rede davon sein, dass die Bürger mit dieser Maßnahme einverstanden wären.

Jetzt möchte ich aber auch gern auf die juristischen Fragen zu sprechen kommen. Herr Korte, Sie haben das Gutachten des Wissenschaftlichen Dienstes des Deutschen Bundestages vom letzten Jahr angeführt. In der Tat hat der Wissenschaftliche Dienst sehr schwerwiegende Zweifel geäußert, ob die Richtlinie europarechtskonform ist, ob sie sich überhaupt umsetzen lässt in Vereinbarkeit mit dem Grundgesetz. Ich habe vorhin anhand der Rechtsprechung dargelegt, dass das nicht der Fall ist. Ich habe das Rasterfahndungsurteil genannt. Und dann muss ich auch Ihnen, Herr Prof. Ronellenfitsch, widersprechen, wenn Sie sagen, es gebe Werte, die es aufwiegen können, das Telekommunikationsverhalten der gesamten Bevölkerung aufzuzeichnen. Sie haben gesagt, im Bereich schwerer Terrorismusstraftaten sei das geeignet, das aufzuwiegen. Da möchte ich kurz eben diese Rasterfahndungsentscheidung zitieren. Drei Sätze daraus, die darauf eingehen. Die besagt nämlich auch im Ausgangspunkt, dass es abgewogen werden muss, und sagt, der Verdachtsgrad kann herabgesenkt werden bei schweren Straftaten. Aber dann heißt es wörtlich: *Die Anforderungen an den Wahrscheinlichkeitsgrad und die Tatsachenbasis der Prognose dürfen allerdings nicht beliebig herabgesenkt werden. Selbst bei höchstem Gewicht der drohenden Rechtsgutbeeinträchtigung kann auf das Erfordernis einer hinreichenden Wahrscheinlichkeit nicht verzichtet werden.* Und im Bereich der Vorratsdatenspeicherung haben Sie keinerlei Wahrscheinlichkeit, dass die betroffenen Nutzer in irgendeinem Zusammenhang zu einer

Rechtsgutsbeeinträchtigung stehen. Deswegen gibt es keine Werte, die es rechtfertigen könnten, die gesamte Bevölkerung zu erfassen.

Dann haben Sie, Herr Korte, die Richtlinie angesprochen. Inwiefern geht das deutsche Umsetzungsgesetz darüber hinaus? Das Bundesverfassungsgericht hat im Urteil zum Europäischen Haftbefehl sehr deutlich gesagt, dass der Gesetzgeber zumindest verpflichtet war, den Grundrechtseingriff auf das vorgegebene Maß zu beschränken. Das ist bei diesem Gesetzentwurf sicherlich nicht der Fall. Um nur einige Punkte zu nennen: Einmal die Verwendungsmöglichkeiten der Verbindungsdaten. Die Richtlinie sieht das nur in schweren Straftaten vor. Das heißt, das könnte man etwa beschränken auf die Fälle des § 139 Abs. 3 StGB. Sehr schwere Straftaten. Hier soll die Nutzung bei jeder erheblichen Straftat möglich sein, bei jeder mittels Telekommunikation begangenen Straftat. Das heißt, Beleidigungen im Internet, Gefahrenabwehr, Nachrichtendienste, es geht also ganz schwerwiegend darüber hinaus. Es ist ein praktisches Verbot von Anonymisierungsdiensten enthalten. Das ist in der EU-Richtlinie nicht vorgesehen. Es ist eine Identifizierungspflicht enthalten, die schon heute in Deutschland besteht, die aber Gegenstand einer Verfassungsbeschwerde ist. Es ist die Speicherung auch von IP-Adressen der Nutzer von E-Mail enthalten. Es ist keine Entschädigung vorgesehen, die in Übereinstimmung mit der Richtlinie eingeführt werden könnte. Also in sehr vielen Punkten geht dieser Gesetzentwurf weit über das hinaus, was die Richtlinie vorgegeben hat. Insbesondere, was die Verwendung und die Menge der Daten im Internetbereich anbetrifft. Im Übrigen hat auch die Generalanwältin am Europäischen Gerichtshof in einer Stellungnahme letzthin Zweifel angemeldet, ob die Richtlinie überhaupt verhältnismäßig ist. Sie konnte das in dem Fall offenlassen. Ich habe in meiner schriftlichen Stellungnahme auch zu der Frage der Umsetzungspflicht Stellung genommen. Ich bin, wie gesagt, der Überzeugung, dass keine Umsetzungspflicht besteht. Das hat auch das Gutachten des Wissenschaftlichen Dienstes ausgeführt. Wenn der europäische Gesetzgeber über seine Kompetenzen hinausgeht, ist Deutschland völkerrechtlich nicht verpflichtet, eine kompetenzwidrige Richtlinie umzusetzen. Das hat auch das Bundesverfassungsgericht gesagt. Und wenn Sie einen schwerwiegenden offensichtlichen Verstoß haben, sagt auch der Europäische Gerichtshof, dass ein solcher Rechtsakt unwirksam ist. Nach dem Urteil des Europäischen Gerichtshofs aus dem letzten Jahr zu Art. 95 EG-Vertrag ist es

m. E. offensichtlich, dass auch die Vorratsdatenspeicherung dem gleichen Schicksal unterliegen wird, weil auch diese Datenspeicherung nicht zum Erbringen einer Dienstleistung erforderlich ist.

Frau Leutheusser-Schnarrenberger hat das Urteil zur Bankkontenabfrage angesprochen, ob das etwas an der verfassungsrechtlichen Beurteilung ändert. Man muss sehen, dass dieses Urteil anders gelagert ist. Es betrifft erstens die Abfrage von Stammdaten von Bankkonten. Es betrifft zweitens den Bereich der Finanzdaten, wobei ich meine, dass der finanzielle Verkehr sehr viel weniger sensibel ist als mein gesamtes Kommunikationsumfeld, als mein Bewegungsprofil. Also, das Urteil hat daher andere Qualitäten. Drittens muss man sagen, es war eine Befugnis zur Abfrage im Einzelfall, während es hier so ist, dass Daten überhaupt erst gespeichert werden sollen. Über Monate hinweg. Das heißt, es ist schon eine andere Konstellation. Deshalb würde ich sagen, bedeutet dieses Urteil auch keine Änderung der Rechtsprechung, sondern es fügt sich ein in die Rechtsprechung des Bundesverfassungsgerichts, die ich skizziert habe. In die ständige Rechtsprechung, wonach ein Verbot der Speicherung personenbezogener Daten auf Vorrat zu noch unbestimmten Zwecken besteht. Diese Bankkontenabfrage bedeutet ja keine Speicherung auf Vorrat. Von daher würde ich sagen: Keine Änderung. Unverändert ist das mit der Rechtsprechung des Bundesverfassungsgerichts nicht in Einklang zu bringen. Danke.

Vorsitzender Andreas Schmidt (Mülheim): Vielen Dank. Wir haben jetzt noch weitere Wortmeldungen für eine zweite Fragerunde. Es beginnt der Kollege Dr. Gehb.

Dr. Jürgen Gehb (CDU/CSU): Wenn ich geahnt hätte, dass die Antworten so lange dauern, hätte ich möglicherweise meine Frage zurückgezogen. Ich will dennoch Herrn Dr. Graf etwas fragen. Ich gehe davon aus, Herr Dr. Graf, wir haben Sie hier als Sachverständigen bestellt, dass Sie auch sachverständig sind. Dass Sie vom Präsidium des Bundesgerichtshofs in den Senat für Computerkriminalität eingesetzt worden sind, zeigt, dass Sie Sachkenntnis haben und wir sollten den Sachverständigen nicht gegenseitig die Sachkenntnis absprechen. Das will ich mal vorausschicken. Ich habe eine Frage, Herr Dr. Graf. Wir haben ja eben von Herrn Liedtke gehört und das wissen wir ja auch alle, früher sind die Daten, als es eine

Flatrate noch nicht gab, zu Abrechnungszwecken gespeichert worden. Das wurde von den Providern gemacht, weil sie abrechnen wollten. Hat denn das verfassungsrechtlich eine andere Qualität? Da hätte man ja auch schon drauf zugreifen können. Bei der Vorratsdatenspeicherung wird, wie der Name schon sagt, nur auf Vorrat ein Datum gespeichert und erst in Verbindung mit § 100 g StPO-RegE oder überhaupt den strafprozessualen Ermittlungsbefugnissen wird doch dieses Datum zu irgendeinem Zweck jetzt auch verwendet. Sonst schlummert es doch eigentlich, so gefährlich oder so ungefährlich wie ein eingemachtes Glas Erdbeeren oder so wie es bei Ihnen früher war, als Sie die Daten nur zu Abrechnungszwecken erhoben haben. Worin liegt also der verfassungsrechtlich qualitative Unterschied? Weil die eigentliche Zweckbestimmung ja erst in § 100 g StPO-RegE kommt und überhaupt virulent wird. Im Übrigen speichert der Staat ja Daten gar nicht. Er greift darauf zurück und konstruiert jetzt eine Pflicht.

Und noch eine Frage an Herrn Wirth. Herr Wirth, würde es die Polizei eigentlich interessieren, wann Herr Grützner heute Morgen aufgestanden ist, wohin er gefahren ist? Das haben Sie uns vorhin alles freiwillig gesagt oder ist es nicht so, dass es Sie erst interessieren würde, wenn Herr Grützner sich verdächtig gemacht hätte einer der Straftaten, die Sie nahezu – nicht enumerativ – hier beschrieben haben? Also käme denn irgendeiner auf die Idee, einfach mal so ein Bewegungsbild zu erstellen, ohne Anlass? Ich finde, dass sollte man vielleicht einmal klarstellen, weil hier ja viele Zuhörer sind und durch einige Beiträge der Sachverständigen der Eindruck erweckt wird, als müsse man immer den Argwohn haben, jeder betreibe damit Missbrauch. Dass polizeiliche Ermittlungsmethoden missbrauchsanfällig sind, das ist doch ganz klar. Selbst derjenige, der eine Blutprobe abnimmt nach einer harmlosen Alkoholfahrt, könnte damit auch zu dem Arbeitgeber des Fahrers gehen und damit nachweisen, dass der Fahrer ein Bluter ist oder die Mehlstaupe hat oder sonst was. Also, ich finde, wir sollten nicht nur die Sabotageanfälligkeit und die individuelle Fehlsamkeit sehen, sondern das, was Herr Ronellenfitsch – das hätte mir eigentlich schon nach seinen zwei Ausführungen gereicht und ich hätte den Saal verlassen können – gesagt hat, nachvollziehen: Es ist verfassungsmäßig und europarechtstauglich. Und jetzt wollte ich dennoch die zwei Fragen gestellt haben. Eine an Herrn Dr. Graf. Und eine an Herrn Wirth.

Jerzy Montag (BÜNDNIS 90/DIE GRÜNEN): Ich habe eine Frage an Herr Dr. Breyer und auch noch eine Frage an Herrn Dr. Graf. Wobei ich Herrn Dr. Graf bitten würde, um meine Frage beantworten zu können, die Bedingung, die ich hier vorweg stelle, zu unterstellen, auch wenn Sie da einer anderen Auffassung wären. Als der Europäische Gerichtshof die Übereinkommen zur Weitergabe von Fluggastdaten kassiert hat, hat die Bundesjustizministerin bezogen auf die Vorratsdatenspeicherung erklärt: Jetzt ist die Tür zum Europäischen Gerichtshof im Sinne einer Klage offen. Bevor es die europäische Richtlinie zur Vorratsdatenspeicherung gegeben hat, hat in Deutschland nicht einmal auf Seiten der Konservativen, der Union jemand ernsthaft den Wunsch gehabt, national eine Vorratsdatenspeicherung einzuführen. Alle reden mehr oder minder darüber, wir seien jetzt dazu gezwungen. Jetzt müssen wir es machen, weil es Europa gemacht hat. Ich persönlich bin nicht einer solch festen Überzeugung wie Herr Dr. Breyer, dass die Sache beim Europäischen Gerichtshof auffliegen wird. Aber dennoch habe ich eine berechtigte Hoffnung, wenn ich mir so die Rechtsprechung anschaue. Würden Sie es für möglich halten und würden Sie uns zuraten können, in das Gesetz eine Verfallklausel einzusetzen mit dem Inhalt, dass, wenn der Europäische Gerichtshof die europäische Richtlinie kassiert, dann auch das deutsche Umsetzungsgesetz entfällt? Weil wir sonst in die Gefahr hineinlaufen, dass wir jetzt irgendetwas machen, zu dem wir angeblich mehr oder minder gezwungen werden, und dann stehen wir vor dem Problem, wenn die Grundlagen europarechtlich evtl. entfallen sollten. Also meine ganz konkrete Frage, ob das eine Möglichkeit wäre, wie Sie das einschätzen würden.

Meine zweite Frage richte ich an Herrn Dr. Weichert und Herrn Grützner. Zu den Beispielen von Herrn Wirth über die Aufklärung der Mordfälle in Bayern haben schon Sachverständige Stellung genommen in dem Sinne, dass man das ja ohne das neue Gesetz hat aufklären können. Was mich aber noch berührt hat und zu dem noch nicht Stellung genommen worden ist, ist dieser Fall eines Amokläufers. Ich hoffe sehr, Herr Wirth, dass das jetzt nur ein theoretisches Beispiel war und dass Sie nicht wirklich heute eine Nachricht bekommen haben, dass ein Soldat um 12.00 Uhr mittags usw. Aber wenn das wirklich passiert wäre, was ja schrecklich wäre, wollte ich gerne wissen, Herr Weichert und Herr Grützner, kann man da nicht schon nach geltendem Recht helfen? Oder braucht man dazu die Vorratsdatenspeicherung und...

Zwischenruf: Könnte es sein, Herr Kollege, dass die Frage schon gestellt und auch schon beantwortet worden ist?

Jerzy Montag (BÜNDNIS 90/DIE GRÜNEN): Ach so. Auch bezüglich des Amoklaufs? Dann bitte ich um Nachsicht. Dann müssten nur noch die Sachverständigen, damit ich voll im Bild bin, noch mal ganz kurz die Antwort skizzieren.

Sabine Leutheusser-Schnarrenberger (FDP): Ich hätte die Bitte an Herrn Dr. Breyer und an Herrn Dr. Fiedler, im Zusammenhang mit dem hier vorliegenden Gesetzentwurf kurz etwas zu sagen und juristisch zu bewerten. Nämlich: Welchen Unterschied es machen kann, ob die Vorratsdaten gespeichert sind, und zwar gesetzlich verpflichtend bei einem Unternehmen, also bei einem Privaten, oder bei der Behörde. Eine weitere Frage geht an Herrn Grützner und an Herrn Dr. Liedtke. Könnten Sie bitte etwas zu der derzeitigen Bedeutung von Anonymisierungsdiensten sagen, zu dem Umfang der Anwendungen, wie Sie den einschätzen. Vorhin kam so eine kleine Bemerkung, die würden natürlich gerade gezielt angewendet, um sich dann auch mit der Anonymisierung entsprechend zu schützen und um kriminelle Handlungen zu begehen. Welche Rolle spielen die überhaupt bei Ihrer Tätigkeit? Dies, um einfach hier eine gewisse Einschätzung vornehmen zu können. Danke.

Vorsitzender Andreas Schmidt (Mülheim): Ich sehe keine weiteren Fragesteller und gehe davon aus, dass wir mit dieser zweiten Antwortrunde abschließen können. Wir beginnen mit der Antwortrunde, mit Herrn Dr. Breyer auf die Fragen der Kollegen Montag und Leutheusser-Schnarrenberger.

SV Dr. Patrick Breyer: Danke schön. Zunächst ist gesagt worden, dass die Daten bereits früher zu Abrechnungszwecken gespeichert worden sind. Das muss man relativieren. Bis zu den 90er Jahren gab es ja keine digitalen Verbindungsstellen im deutschen Telefonnetz und deswegen sind bis zu den 90er Jahren auch gar keine Verbindungsdaten in Deutschland gespeichert worden. Zum zweiten durfte auch früher die IP-Adresse, die vergeben worden ist, nicht gespeichert werden, weil von der IP-Adresse die Abrechnung nicht abhängt. Das ist höchstrichterlich geklärt worden, vom Landgericht Darmstadt bis hin zum Bundesgerichtshof und obwohl die Unternehmen sich nicht daran halten, haben sie auch früher nur wenige Wochen

lang gespeichert und nicht sechs Monate, wie das jetzt geschehen soll. Andere Daten sollen jetzt überhaupt erstmals gespeichert werden, die nie gespeichert worden sind. Z. B. sind der ganze Bereich E-Mail und der ganze Bereich Bewegungsprofile bisher nicht gespeichert worden.

Herr Montag hat mich zu dem Urteil des Europäischen Gerichtshofs zu den Fluggastdaten gefragt und den sehr interessanten Vorschlag unterbreitet, in das Umsetzungsgesetz eine Verfallklausel aufzunehmen, wonach das Gesetz verfällt, sobald die Richtlinie vom Europäischen Gerichtshof für nichtig erklärt worden ist. Das ist ein sehr guter Vorschlag, dem ich mich ausdrücklich anschließen kann. Denn wenn tatsächlich nur die Richtlinie jetzt die Ursache dafür ist, eine Vorratsdatenspeicherung in Deutschland einzuführen – und auch nur sie kann ja vielleicht verfassungsrechtlich noch gegen die Rechtsprechung des Bundesverfassungsgerichts ins Feld geführt werden, weil die Richtlinie natürlich Vorrang hat vor nationalem Verfassungsrecht –, wenn das wirklich so ist, ist es in der Tat konsequent zu sagen, sobald die Richtlinie gekippt wird, tritt diese Vorratsdatenspeicherung wieder außer Kraft. Denn wie ich eingangs erwähnt habe, wird danach das Gesetz in vollem Umfang am Grundgesetz gemessen werden und kann hier mit Sicherheit keinen Bestand haben. Von daher kann ich den Vorschlag ausdrücklich begrüßen.

Frau Leutheusser-Schnarrenberger hat gefragt, welchen Unterschied es mache, ob die Daten bei den Unternehmen oder bei einer Behörde selbst gespeichert werden. Dazu muss ich sagen, dass es aus meiner Sicht kein geringerer Grundrechtseingriff ist, das ist eine Art bloßes Out-Sourcing, denn auch wenn der Staat selbst speichern würde, wie das, glaube ich, in England angedacht war, könnte er ja sagen, wir greifen auf die Daten nur mit richterlichem Beschluss zu. Und in einem Rechtsstaat gehe ich natürlich davon aus, dass das dann auch passieren würde. Das heißt, inhaltlich macht das gar keinen Unterschied. Im Gegenteil, es ist noch ein zusätzlicher Eingriff, wenn Privatunternehmen ohne Entschädigung herangezogen würden, diese Daten vorzuhalten. Es ist aber auch ein zusätzlicher Eingriff in die Rechte der Betroffenen, weil die natürlich der Gefahr ausgesetzt sind, dass die Daten bei den einzelnen Unternehmen missbraucht werden. Das sind ja etwa – ich weiß es nicht – tausende von Unternehmen, die speichern sollen, auch die ganzen kleinen

E-Mail-Anbieter. Es besteht natürlich eine sehr große Gefahr, dass da Missbrauch vorkommt, wenn so viele Unternehmen, auch kleine, beteiligt sind. Insofern ist es aus meiner Sicht kein geringerer Eingriff, sondern ein tieferer Eingriff.

SV Dr. Christoph Fiedler: Ich kann bestätigen, was mein Vorredner gesagt hat, und will nur einen Punkt ergänzen. Zu der grundrechtdogmatischen Frage muss man wohl ziemlich eindeutig sagen, dass es auch ein Eingriff ist und nicht von geringerem Gewicht. Das Entscheidende ist hier der gesetzliche Zwang des Staates, dass diese Daten gespeichert werden, ob er das selber macht oder durch Private, kann insoweit keinen Unterschied machen. Das gilt sogar, das nur als Ergänzung, wenn Sie sich die verfassungsrechtliche Rechsprechung ansehen, bei privatgesetzlichen Zwängen, bei einem durch öffentlich-rechtlichen Zwang wie hier durch das TKG dürfte es im Ergebnis also gar keinen Unterschied machen.

SV Dr. Jürgen-Peter Graf: Zunächst zur Frage von Herrn Dr. Gehb, Speicherung zu Abrechnungszwecken. Ich kann es vielleicht ergänzen. Bis vor einem Jahr wurde vielmals von den Unternehmen nicht nur zu Abrechnungszwecken, sondern auch aus Sicherheitserwägungen gespeichert. Da gibt es eine Vorschrift im TKG, die mir jetzt nicht wortwörtlich vorliegt, aber das war eigentlich der Grund, warum sehr viele Unternehmen gespeichert haben und auch bei T-Online ist es ja bekannt geworden durch entsprechende Urteile, teilweise wurde mehrere Wochen, sechs bis acht Wochen gespeichert. Das heißt also, wir hatten damals schon eine Situation, die der heutigen durchaus ähnlich ist. Und da konnten dann die Ermittlungsbehörden auf diese Daten zurückgreifen und deswegen konnten in diesem Zusammenhang auch relativ viele Taten aufgeklärt werden. Es gab Provider, die haben sich immer schon bei den Flatrates daran gehalten. Nur gab es früher relativ wenige Flatrates. Das hat sich auch erst in den letzten drei, vier Jahren durchgesetzt. Da gab es also keinen so großen Unterschied. Erst seitdem die Urteile in den letzten zwei, drei Jahren mit der Löschungsverpflichtung ergangen sind, ist es nahezu durchgängig, d.h. innerhalb von 24 bis 48 Stunden sind die Daten regelmäßig gelöscht. Manche sogar noch schneller.

Zu dem, was Sie, Herr Montag, gesagt haben. Ich habe mit einer Verfallklausel grundsätzlich keine Probleme. Sie muss allerdings bestimmt sein. Und ob eine

Verfallklausel, die lauten würde „falls ein Gericht eine solche Entscheidung trifft“, ob die bestimmt genug wäre, das scheint mir zumindest fragwürdig.

(Unverständlicher Zwischenruf)

Ja, wenn das Gericht konkret entscheidet. Falls die Aussage eindeutig ist. Also, mir scheint eine datumsmäßige Verfallklausel im Sinne einer Evaluierung sicherlich viel klarer, aber ich bin kein Verfassungsrechtler. Insofern vermag ich nicht zu sagen, ob diese Vorschrift dann so halten würde. Aber denkbar wäre so etwas schon.

Noch eine abschließende Bemerkung zur Frage IP. Es ergibt sich eindeutig aus § 113 a Abs. 4 TKG-RegE, was bei einer IP zu speichern ist. Nämlich nur Beginn und Ende sowie die Nennung des Teilnehmeranschlusses und nicht mehr und nicht weniger. Also weder, ob der Teilnehmer bei Google oder ob er bei Ebay war oder sonst wo. Das wird alles nicht gespeichert. Das wird allenfalls im Zusammenhang mit einer Verknüpfung anderer Datennetze herauskommen. Es wurde ja vorhin schon gesagt, Google weigert sich, Daten herauszugeben und ich denke, Ebay wird es genauso machen. Von daher besteht diese Gefahr sicherlich nicht. Also, die IP-Speicherung als solche ist vollkommen inhaltsneutral.

Vorsitzender Andreas Schmidt (Mülheim): Vielen Dank. Der Kollege Benneter hat dazu eine Zusatzfrage.

Klaus Uwe Benneter (SPD): Nein, ich wollte Prof. Ronellenfitsch etwas fragen, zu der Frage des Kollegen Montag, zur Verfallklausel.

SV Prof. Dr. Michael Ronellenfitsch: Ich halte die Verfallklausel für unglücklich. Sie haben ja nicht die Richtlinie unmittelbar eins zu eins umgesetzt, sondern Sie haben eine eigene gestalterische Regelung getroffen. Und rein von der Kosmetik her, unabhängig vom verfassungsrechtlichen, stellen Sie sich ein Armutszeugnis aus, wenn Sie reinschreiben, „unter der Bedingung, dass die europäische Richtlinie nicht von einem Gericht kassiert wird, halten wir unser Gesetz aufrecht“. Wenn Sie das Gesetz für europarechtswidrig und für verfassungswidrig halten, dann sollten Sie den Mut haben, zu sagen, wir machen jetzt gar kein Gesetz. Das wäre dann konsequent,

aber rein von der Verfassungsästhetik ist es unglücklich, sich abhängig zu machen von der Entscheidung des Europäischen Gerichtshofs.

Vorsitzender Andreas Schmidt (Mülheim): Vielen Dank. Jetzt in der Reihenfolge weiter. Herr Grützner auf die Fragen der Kollegen Montag und Leutheusser-Schnarrenberger.

SV Jürgen Grützner: Vielen Dank, Herr Vorsitzender. Wir hatten eben schon darauf hingewiesen, dass eigentlich aus unserer Sicht alle Tatbestände, die von Herrn Wirth genannt worden sind, von den Unternehmen nach heute geltendem Recht hätten verhindert werden können, da nämlich die Daten, die hierfür von ihnen benötigt würden, oft in Minutenschnelle heute schon bereits von den Unternehmen zur Verfügung gestellt werden. Gerade in den von Ihnen genannten schweren Fällen passiert das auf eine sehr sehr unbürokratische Art und Weise, wobei häufig auf die eigentlich vorgesehenen Prüfungen in vollem Umfange verzichtet wird und die Prüfungen nachträglich durchgeführt werden. Dabei stellt sich in aller Regel heraus, dass es eben ordentlich gelaufen ist. Aber hier wird nach heute geltendem Recht alles getan, dass eben diese Dinge nicht geschehen und dass man einen solchen Amoklauf nicht mit Datensammlungen „rückwärts“, sondern mit der Beantwortung der Frage, wo sich der Täter mit seiner Pumpgun befindet, herausfindet, das ergab sich eigentlich schon aus dem Fall.

Zu den Anonymisierungsdiensten. Die spielen eigentlich im alltäglichen Leben nach meinem Kenntnisstand eine noch sehr untergeordnete Rolle. Was sehr viel häufiger, wenn man in den kriminellen Bereich hinein geht, ge- und benutzt wird, das sind ungesicherte Netzzugänge, gerade bei WLAN. Gerade bei Technologien, die es mir völlig anonym gestatten, auf dem Rücken eines anderen Zugangsnutzers in ein Netz hinein zu kommen. Ich brauche zu gut deutsch diese Anonymisierungsdienste heutzutage nicht. Ich kann mich mit dem Auto an jede Ecke stellen und kann mir drei WLAN-Netze aussuchen, über die ich reingehen kann. Und ich kann natürlich auch Buchungen und Abbuchungen durchführen, wenn ich mich dieser Netze bediene. Dafür brauche ich überhaupt keinerlei Zusatztechnik. Und ich brauche überhaupt keine illegale Technik. Ich brauche dazu nichts. Insofern gibt es da einen gewissen Hang zu einem rechtsfreien Raum, wenn man das als rechtsfreien Raum sehen will.

Bitte gestatten Sie mir noch eine Anmerkung zur Bedeutung von Datensammlungen. Es erscheint mir gerade vor dem Hintergrund einer ganz aktuellen Entscheidung der USA, die wir gerade selber auswerten – die ist erst einige Tage alt – erwähnenswert, dass es den US-Behörden gestattet wird, in vollem Umfang auf sämtliche gespeicherten Daten von Drittstaaten, ausdrücklich nicht der USA selbst, sondern von Drittstaaten, zuzugreifen. Nach dem Motto, alles, was ich kriegen kann und was gespeichert wird, darf ausgewertet werden. Nicht nur mit staatlicher Erlaubnis, sondern mit staatlichem Auftrag. Wenn wir an unsere Kunden denken, denn letztlich sind es nicht nur Bürger, sondern auch Kunden, wenn wir denen nicht mehr erklären können, dass ihre Daten auch nur halbwegs sicher sind, dann wird das Geschäft nicht nur für die Politiker schwierig, sondern auch für uns. Denn wir vermitteln im Mobilfunk immer noch den Eindruck, als würde jemand – und so verhält sich die Bevölkerung heute – der von A nach B telefoniert, wirklich von A nach B telefonieren. Die, die das Geschäft betreiben, wissen längst, dass ohne große Probleme, ohne großen technischen Aufwand, längst Dritte mithören können und dass das auch häufig geschieht. Aber insgesamt ist der Eindruck so, dass kein Missbrauch geschieht, und ich sage noch mal ganz vorsichtig, die Bevölkerung weiß, dass Daten bei Privaten gespeichert werden. Wir haben auch angeregt, mal zu überlegen, ob es nicht richtig wäre, diese heikle Datensammlung bei einer staatlichen Stelle unterzubringen. Ich kann nur davor warnen, wirklich davor warnen, dass hier Privatunternehmen derart sensible Daten speichern, die derart weitgehend zu Missbräuchen über Google und Internetanbieter verführen, die nicht nur Bewegungsprotokolle nachhalten, wo ich gerade bin, an welchem Flughafen, das ist es nicht. Aber vielleicht, mit welcher Fluglinie ich fliege und was ich gerade im Internet abgerufen habe. Das sind wirtschaftsrelevante Daten, die einen Wert darstellen und die in der Zukunft einen sehr hohen Wert darstellen werden. So zu tun, als sei das alles irrelevant, als gäbe es hier gar kein Interesse an diesen Daten, die da in Millionenhöhe gespeichert werden von unseren Unternehmen, und zwar von tausenden von Unternehmen. Der Kunde kann nachher nicht einmal nachvollziehen, wo er sich eingeloggt hat, bei welchem Unternehmen, wenn er in irgendeinem Hotel war. Er hat nicht einmal selber mehr den Überblick, bei welchem Unternehmen welche Daten gespeichert sind. Das ist aus meiner Sicht ein völlig unhaltbarer Zustand, der von dem Gesetzentwurf überhaupt nicht in Erwägung

gezogen wird. Also aus meiner Sicht ist, gerade bei der zukünftigen Internetnutzung eine geradezu verheerende Wirkung auf die Vertraulichkeit der Korrespondenz und der Korrespondenz unter Menschen gegeben.

SV Dr. Rainer Liedtke: Ich kann mich auf die Frage der Abgeordneten Leutheusser-Schnarrenberger eigentlich nur dem anschließen, was Herr Grützner gerade gesagt hat, was die Anonymisierungsdienste angeht. Die spielen eigentlich nur eine minimale Rolle. In der Tat sind die Missbrauchsmöglichkeiten durch nichtberechtigte Zugänge im Wireless-Lan-Bereich oder wo auch immer viel einfacher und kostengünstiger zu realisieren für jemanden, der dort wirklich Missbrauch betreiben will. Ich denke, das führt zu größeren Problemen und da muss man einfach dafür sorgen, dass auch diese Netzbereiche, die immer mehr in privater, in ganz persönlicher Obhut von Kunden sind, dass die eine stärkere Absicherung erfahren. Was die Datensammlungen bei den Unternehmen angeht – vielleicht auch noch mal kurz zu dem, was Herr Grützner gesagt hat – auch das kann man, denke ich, nur unterschreiben. Im Grunde genommen ist es wahrscheinlich eine sauberere Lösung, wenn tatsächlich ein Data-Retention-Programm käme, so dass man diese Daten in der Tat unter staatlicher Obhut speichern würde. Das wäre eine wirklich saubere Angelegenheit. Das, denke ich, würde das Problem sicherlich nicht entschärfen. Die Problematik ist ja eben auch schon mal diskutiert worden, inwieweit das überhaupt Unterschiede macht, ob das bei Privaten gespeichert wird oder in staatlicher Obhut. Also ich glaube, von daher gesehen sind die Dinge, die bisher angesprochen sind, nach wie vor in aller Schärfe auch so zu bewerten. Allerdings wäre es für uns in der Tat eine Entlastung und möglicherweise auch für die Sicherheitsbehörden eine gewisse Vereinfachung des Zugangs, weil sie dann genau wüssten, wo sie sich hinwenden müssten und sich so die eine oder andere Suche nach dem zuständigen Netzbetreiber sparen könnten.

SV Dr. Thilo Weichert: Nach dem, was Herr Grützner gesagt hat, und nachdem eigentlich alles schon gesagt worden ist, muss ich auf die Frage des Abgeordneten Montag nur noch ganz wenige Sätze ergänzen. Der Amoklauf kann natürlich nach der augenblicklichen Rechtslage so weit aufgeklärt werden. Die notwendigen Daten sind zu beschaffen und bei Gefahr in Verzug, die liegt hier offensichtlich vor, auch ohne richterliche Anordnung, also in Sekundenschnelle, wie Sie das darstellen. Das

Problem der aktuellen Regelung besteht darin, dass wir eine gesetzliche Grundlage bekommen und Google in der Zukunft verpflichtet werden kann, gesetzlich verpflichtet werden kann, diese Daten zur Verfügung zu stellen. In den USA bestand damals die rechtliche Grundlage zur Bereitstellung von diesen Millionen Datensätzen nicht. Also genau das, was die USA damals versuchten, das soll heute in Deutschland legalisiert werden. Insofern muss man sich da auch schon ansehen, wo diese Daten sind, und was der Private dann wirklich auch noch in eigener Entscheidungsfreiheit hat. Er hat eben keine Entscheidungsfreiheit, wenn er gesetzlich verpflichtet wird, und das ist hier ausdrücklich vorgesehen.

Vorsitzender Andreas Schmidt (Mülheim): Vielen Dank. Abschließend hat jetzt das Wort Herr Wirth zur Beantwortung der Frage des Kollegen Gehb.

SV Ernst Wirth: Die Frage war, ob wir daran interessiert sind, das Kommunikationsverhaltensprofil von Herrn Grützner zu Beginn des Tages zu analysieren. Wir sind nicht daran interessiert. Erlauben Sie mir den Hinweis, verdachtsunabhängige Rechercheüberprüfungen scheiden aus. Es wurde angesprochen, es fehle an einer standardisierten Übertragung, an Zusammenarbeit mit Betreibern, Verpflichteten und den Behörden. Sie kennen den Beschluss der Innenminister vom November 2006, der dringend die Einführung einer standardisierten Technik zum Austausch von Kommunikationsverkehrsdaten empfiehlt, Elektronische Schnittstelle Behörden (ESB). Wir haben es in Bayern mit Pilotprojekten seit Frühjahr 2006 umgesetzt.

Mehrfach wurde die Amoklage angesprochen. Es ist eine tatsächliche Lage. So eine Lage kommt im Regelfall immer freitags. Das wissen wir. Natürlich bekommen wir die Daten der Netzbetreiber bereits jetzt unverzüglich auf freiwilliger und unbürokratischer Basis in hervorragender Form. Gleichwohl herrscht Handlungsbedarf, dass man es normiert. Es muss festgeschrieben werden. Der Gesetzestext lautet jetzt: *Sind unverzüglich zur Verfügung zu stellen.* Unverzüglich. Es ist nicht geregelt, in welcher Art und Weise. Jetzt ist die Echtzeit gefordert und es muss die ESB normiert werden. Dann haben wir ein Komplettpaket und dann kann man sauber arbeiten.

Vorsitzender Andreas Schmidt (Mülheim): Vielen Dank, Herr Wirth. Vielen Dank, meine Herren Sachverständigen, dass Sie uns Rede und Antwort gestanden haben, dass Sie uns Ihren Sachverstand zur Verfügung gestellt haben. Ich schließe die Sitzung und wünsche Ihnen einen guten Heimweg und ein schönes Wochenende.

Ende der Sitzung: 14.45

Andreas Schmidt (Mülheim), MdB
Vorsitzender