Deutscher Bundestag **Protokoll Nr. 17/31**
17. Wahlperiode

Innenausschuss

Wortprotokoll

31. Sitzung

Öffentliche Anhörung

am Montag, 7. Februar 2011, von 15.00 Uhr bis 17.25 Uhr
Paul-Löbe-Haus, Raum E 200
10557 Berlin, Konrad-Adenauer-Str. 1

Vorsitz: Wolfgang Bosbach, MdB

Öffentliche Anhörung von Sachverständigen
zum

Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften

BT-Drucksachen 17/3630, 17/4145

Seite

I. Anwesenheitsliste Mitglieder des Deutschen Bundestages

Bundesregierung

Bundesrat

Fraktionen und Gruppen

II. Liste der Sachverständigen für die Öffentliche Anhörung am 7. Februar 2011

1.	Michael Bobrowski	Verbraucherzentrale Bundesverband e. V., Berlin
2.	Dr. Stefan Brink	Der Landesbeauftragte für den Datenschutz Rheinland-Pfalz, Mainz
3.	Dipl. Inf. Werner Hülsmann	Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V., Konstanz
4.	Dr. Bernhard Rohleder	BITKOM e.V., Berlin
5.	Prof. Dr. Gerald Spindler	Georg-August-Universität Göttingen
6.	Dr. Oliver Vossius	Deutscher Notarverein e. V., Berlin
7.	Harald Welte	Chaos Computer Club, Berlin

III. Sprechregister der Sachverständigen und Abgeordneten

IV. Protokollierung der Anhörung

Vors. **Wolfgang Bosbach**: Meine sehr verehrten Damen und Herren, liebe Kolleginnen und Kollegen, liebe Gäste, liebe Zuhörerinnen und Zuhörer. Ich begrüße Sie zur öffentlichen Anhörung der Sachverständigen zum Gesetzentwurf der Bundesregierung zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften. Ich danke den Herren Sachverständigen, dass Sie unserer Einladung nachgekommen sind. Es sind wiederum nur Herren. Es wird Zeit, dass sich das zuständige Bundesministerium einmal mit dieser Frage beschäftigt. Weiter begrüße ich die Gäste, die Zuhörer und den Parlamentarischen Staatssekretär beim Bundesminister des Innern, Herrn Dr. Schröder. Sie hatten die Gelegenheit, schriftlich eine Stellungnahme abzugeben, wovon gelegentlich auch Gebrauch gemacht wurde. Diese Unterlagen werden verteilt und sie werden auch dem Protokoll als Anlage beigefügt. Wir werden heute ein Wortprotokoll anfertigen, das wird denen, die sich hier äußern, mit der Bitte um Korrektur, sofern notwendig, übersandt.

Wir haben uns den Zeitraum 15.00 Uhr bis 17.30 Uhr vorgenommen, müssen ihn aber nicht ausschöpfen. Nur, wenn es nicht anders geht, dann können wir bis 17.30 Uhr tagen. Jeder Sachverständige hat einleitend die Gelegenheit, fünf Minuten zu dem Anhörungsthema Stellung zu nehmen. Da wir in den letzten Sitzungen damit erhebliche Probleme hatten – das sind 300 Sekunden. Ich weiß, dass man da nicht alles unterbringen kann, was man unterbringen möchte, aber wir laufen Ihnen auch nicht weg. Das heißt, alles das, was Ihnen noch unbedingt auf der Seele liegt, das werden Sie auch noch garantiert im Laufe des Nachmittages los. Entweder indem Sie von den Kolleginnen und Kollegen nach Ihrem Statement gefragt werden, oder indem Sie einfach so tun, als seien Sie gefragt worden.

Nach dieser Runde beginnt die Befragung der Sachverständigen. Ich wäre den Kolleginnen und Kollegen schon jetzt dankbar, wenn man nicht nur eine Frage formulieren, sondern diese auch an die Sachverständigen, die gemeint sind, adressieren würde.

Es beginnt Herr Bobrowski von der Verbraucherzentrale Bundesverband Berlin. Bitte, Sie haben das Wort.

SV **Michael Bobrowski** (Verbraucherzentrale Bundesverband e. V. Berlin): Vielen Dank, Herr Vorsitzender, guten Tag, meine Damen und Herren. Zunächst vielen Dank für die Einladung, hier vor Ihnen sprechen und Rede und Antwort zum De-Mail-Gesetzentwurf geben zu können. Ich möchte nur ganz kurz ein Versehen zurechtrücken. Wir gehören zu denen, die eine schriftliche Kurzstellungnahme abgegeben haben, aber wir haben uns leider auf unserem Titelblatt bei einer Drucksachen-

nummer vertan. Ich bitte, das zu entschuldigen. Die Drucksache, die als Zweite dort aufgeführt ist, ist die Drucksache, die die Gegenäußerung und die Stellungnahme des Bundesrates betrifft, nicht den Änderungsantrag der Fraktionen der CDU/CSU und FDP. Das war jetzt wichtig. Ansonsten möchte ich einleitend gar nicht so viel über unsere seinerzeitige kritische Stellungnahme im Einzelnen reden. Ich möchte hier vielmehr die in unserer aktuellen Stellungnahme angesprochenen wenigen sehr wichtigen Punkte noch einmal ganz kurz ansprechen und Ihnen dann für Fragen zur Verfügung stehen. Das eine ist, dass wir nach wie vor ganz konsequent, und das haben wir von Anfang an getan, dafür plädieren, eine Ende-zu-Ende-Verschlüsselung vorzusehen, also nicht nur eine Transportverschlüsselung auf den beiden Wegen vom Sender zum Provider bzw. vom Provider II zum Empfänger, sondern eine durchgehende Inhaltsverschlüsselung, die bisher nur auf dem Weg von Provider A zu Provider B vorgesehen ist. Dieses muss sich auch deswegen schon ergeben, weil selbst die Bundesregierung in ihrem Gesetzentwurf ein sehr hohes Sicherheits- und Vertrauensniveau fordert. Wenn man es daran misst, kommt man unseres Erachtens um die Ende-zu-Ende-Verschlüsselung nicht herum. Es wird gelegentlich das Gegenargument gebracht, das sei für den Anwender zu kompliziert. Wir sehen das nicht so. Unserer Information nach gibt es heute durchaus Verfahren, die es dem Anwender auch mit weniger Kenntnis ermöglichen, mithilfe des Providers, der so etwas anbieten könnte, eine solche Ende-zu-Ende-Verschlüsselung ohne großartige Installation an seinem häuslichen PC zu realisieren.

Das zweite für uns ganz entscheidende Kriterium ist die Forderung nach einer einheitlichen, verbindlichen und providerunabhängigen Kennzeichnung der De-Mail-Adresse. Nur so ist unserer Meinung nach erstens die klare Erkennung und technische Unterscheidbarkeit von De-Mail-Adressen gegenüber einfachen E-Mail-Adressen gesichert. Zweitens können Sie nur so eine einfache Portierung der De-Mail-Adressen sicherstellen und damit selbstverständlich auch den Wettbewerb, den wir unter den Providern erwarten, die interessiert sind, so etwas anzubieten, entsprechend realisieren.

Abschließend möchte ich kurz auf zwei Punkte im Änderungsantrag der Fraktionen der CDU/CSU und FDP hinweisen: Ich möchte erwähnen, dass wir sowohl die dort gewünschten zusätzlichen Informationen an die Nutzer hinsichtlich der Unterscheidung zwischen Ende-zu-Ende-Verschlüsselung einerseits und Transportverschlüsselung andererseits unterstützen. Das ist das Mindeste, wenn Sie sich jetzt tatsächlich im Gesetzgebungsverfahren nicht für die Ende-zu-Ende-Verschlüsselung entscheiden können, dass zumindest der Nutzer ganz klar im Rahmen der Antragstellung und Erstnutzung darauf hingewiesen wird, dass es hier zwischen diesen beiden Verschlüsselungsformen einen erheblichen Unterschied gibt. Das Zweite, und auch das unterstützen wir ausdrücklich, ist die Forderung, dass es keine automatische Kopplung geben darf, wenn ein Nutzer die Veröffentlichung seiner

De-Mail-Adresse im Verzeichnisdienst wünscht und der Eröffnung des Zugangs im Sinne der Vorschriften des Verwaltungverfahrensgesetzes (VwVfG). Da darf es keine automatische Kopplung geben. Wenn ich meine Adresse im Verzeichnisdienst publizieren lassen möchte, dann möchte ich nicht dadurch einen Automatismus in Gang setzen, dass mir die Verwaltung oder die Behörde daraufhin automatisch entsprechende Bescheide auf elektronischem Weg, d. h. mittels De-Mail, zuschicken kann, sondern ich muss das ausdrücklich noch einmal gesondert wünschen. So viel dazu von meiner Seite. Danke schön!

Vors. **Wolfgang Bosbach**: Vielen Dank, Herr Bobrowski. Als Nächster bitte Herr Dr. Brink, der Landesbeauftragte für den Datenschutz Rheinland-Pfalz.

SV MR **Dr. Stefan Brink** (Der Landesbeauftragte für den Datenschutz Rheinland-Pfalz, Gruppenleiter Datenschutz in der Privatwirtschaft): Herzlichen Dank, Herr Vorsitzender, meine sehr verehrten Damen und Herren. Ich muss leider auch mit einer Korrektur beginnen. Das fällt mir leichter, weil ich mich nicht selbst korrigieren muss, ich bin nicht der Landesbeauftragte, ich bin Mitarbeiter des Landesbeauftragten für den Datenschutz in Rheinland-Pfalz.

Meine sehr verehrten Damen und Herren, der Gesetzentwurf zu den De-Mail-Diensten ist nicht perfekt, aber er ist nützlich. Er ist nützlich, weil er einen Standard setzt, der über das bisherige Sicherheitsniveau elektronischer Kommunikation hinaus geht. Er ist nicht perfekt, weil er auch „nicht-sichere“ Anwendung erlaubt. Er ist auch nicht perfekt, weil er keine durchgängige Verschlüsselung vorsieht. Aber er ist nützlich, weil er ein marktgängiges Modell anbietet. Das unterscheidet ihn voraussichtlich von den bisherigen Angeboten, die wir im Bereich der elektronischen Signatur oder zum elektronischen Personalausweis haben, wo ja auch schon die ersten Meldungen kommen, dass man von der Performance etwas enttäuscht ist. Der Gesetzentwurf ist auch deswegen nützlich, weil er das Niveau der bisherigen elektronischen Kommunikation deutlich anhebt. Aus der Sicht einer deutschen Datenschutzbehörde kann ich Ihnen sagen, dass das, was sich im normalen E-Mail-Verkehr z. B. zwischen Rechtsanwälten, Ärzten, Krankenversicherungen, Versicherungsmaklern oder auch Behörden abspielt, jeder Beschreibung spottet. Das Sicherheitsniveau ist in dem Bereich offensichtlich vollständig aus dem Blick geraten. Was besonders problematisch ist, weil wir es hier regelmäßig mit gesetzlichen Verschwiegenheitsverpflichtungen zu tun haben. Ich verspreche mir von dem Gesetzentwurf, dadurch, dass er einen Standard setzt, dass diese Stofflichkeit im Umgang mit elektronischer Kommunikation in diesen Bereichen zurückgedrängt werden kann.

Die Frage, wie nützlich der Gesetzentwurf ist, wird sich danach richten, welchen Markt er für die De-Mail-Dienste erschließt. Das wird sich bei den gewerblichen

Nutzern durchaus umsetzen lassen. Für die Verbraucher muss man ein Fragezeichen setzen. Für den Verbraucher ist die Nutzung von De-Mail-Diensten mit so vielen Obliegenheiten verbunden, dass man die Frage stellen kann, ob das ein Erfolgsmodell für den Verbraucher sein wird. Er muss nicht nur den Netzzugang sicherstellen – das ist in ländlichen Regionen immer noch ein Problem. Er muss auch das Nutzungsverhältnis zum Diensteanbieter stabil gestalten. Er muss insbesondere regelmäßig den De-Mail-Eingang kontrollieren und er muss einen Netzzugang finden, der vor Schadsoftware sicher ist. Die ganze Diskussion über Ende-zu-Ende-Verschlüsselung geht aus meiner Sicht ein bisschen an der Thematik vorbei, weil die Gefahren, die beim Netzzugang des einzelnen Verbrauchers lauern, aus meiner Sicht wesentlich größer sind. Deswegen auch die besondere Bedeutung der Freiwilligkeit der Nutzung der De-Mail-Dienste, die durch den Änderungsantrag der Fraktionen der CDU/CSU und FDP noch einmal betont wird. Das finde ich sehr begrüßenswert und halte es für den richtigen Weg. Der Gesetzentwurf ist nicht perfekt. In bestimmten Bereichen ist er auch noch verbesserungsfähig. Ich würde anregen, das Konzept der Abholbestätigung noch einmal grundsätzlich zu überdenken. Das, was dort vorgeschlagen wurde, ist in verschiedener Hinsicht problematisch. Das fängt schon mit der Bezeichnung an. Die Abholbestätigung bestätigt nicht die Abholung, sondern die sichere Anmeldung. Sie bestätigt auch nicht die Möglichkeit der Abholung. Er ist nämlich möglich, dass das Konto gesperrt ist. Da sieht der Gesetzentwurf zwar eine Benachrichtigungspflicht vor, aber möglich bleibt es trotzdem, dass der Dienste-Nutzer überhaupt nicht auf entsprechende Benachrichtigungen zugreifen kann. Wenn Sie bei dem Konzept der Abholbestätigung bleiben wollen, schlage ich Ihnen dringend vor, eine entsprechende Hinweispflicht der Dienste-Anbieter vorzusehen. Das ist nämlich weder für den Nutzer selbstverständlich, noch wird der Dienste-Anbieter von sich aus darauf hinweisen, dass auch bei gesperrtem Konto Nachrichten abgeholt werden können.

Meine sehr verehrten Damen und Herren, das Internet ist in vielen Bereichen ein „Sumpf“ und der Versuch, der mit dem Gesetzentwurf unternommen wird, Schienen in diesen „Sumpf“ zu verlegen, lohnt sicher die Mühe. Der Gesetzentwurf hat aus meiner Sicht die Chance, die Sicherheit der elektronischen Kommunikation zu erhöhen und ist deswegen unter dem Strich begrüßenswert. Vielen Dank!

Vors. **Wolfgang Bosbach**: Vielen Dank, Herr Dr. Brink. Der Nächste ist Herr Diplominformatiker Werner Hülsmann vom Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung in Konstanz.

SV **Dipl. Inf. Werner Hülsmann** (Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V., Bremen): Vielen Dank, Herr Vorsitzender. Guten Tag meine Damen und Herren. Auch hier eine kleine Korrektur: Ich selber komme aus Konstanz, das Forum hat seinen Sitz in Bremen, aber das ist nicht so gravierend.

Grundsätzlich ist es aus meiner Sicht zu begrüßen, dass durch das De-Mail-Verfahren oder -Vorhaben die Vertraulichkeit und Verifizierbarkeit, also Authentizität und Integrität gefördert und auch die Kommunikation zwischen Bürgerinnen, Bürgern und Verwaltung vereinfacht werden soll. Allerdings erfüllt der Gesetzentwurf nicht die Erwartungen, die an ihn gestellt worden sind und mit denen auch für das De-Mail-Verfahren geworben wird. Es wird gesagt, die De-Mail-Nutzung spare Geld. Wenn man sich das E-Post-Verfahren ansieht, stellt man fest, dass ein E-Post-Brief, der dem Einschreiben/Rückschein entspricht, deutlich teurer ist, als wenn ich das auf konventionelle Art eingetütet und frankiert versende. De-Mail würde vor Spam und Phishing schützen. Wie es das schaffen soll, ist mir ein Rätsel, weil es sicher nicht so sein wird, dass ich nur noch ein E-Mail-Konto habe, wo mir nur noch Absender und Absenderinnen, die selber auch De-Mail-Konten haben, Mails senden. Ich werde nach wie vor viele Kommunikationspartner haben, die eine normale E-Mail-Adresse haben und von daher werde ich mindestens eine, wenn nicht mehrere normale E-Mail-Adressen haben. Sodass auf diesen E-Mail-Adressen genau dieselben Spam- und Phishing-Mails eingehen werden, wie sie auch heute eingehen. Beim Phishing ist es vielleicht dann so, dass sie als De-Mail-Nutzer sagen, wenn mir die Sparkasse etwas schickt und wenn das nicht über das De-Mail-Konto geht, weil ich mit denen die De-Mail-Verbindung vereinbart habe, dann falle ich vielleicht bei der Sparkasse nicht auf das Phishing herein. Wenn das aber bei Amazon oder irgendeinem anderen Dienstleister ist, wie bei E-Bay und so weiter ist, die zwar in Deutschland aktiv sind, ihren Sitz aber im Ausland haben, da werde ich auf die Phishing-Mails genauso hereinfallen, wie ich jetzt schon auf sie hereinfalle.

Der Selbstdatenschutz werde mit De-Mail gefördert. Das habe ich besonders interessant gefunden. Allerdings kann hiervon keine Rede sein. Selbstdatenschutz wird nicht gefördert, weil eine echte anonyme oder pseudonyme Nutzung von De-Mail gar nicht möglich und auch gar nicht vorgesehen ist. Damit könnte man noch leben, weil De-Mail rechtsverbindliche E-Mail-Kommunikation ermöglichen soll und der Provider in ganz konkreten Fällen das Pseudonym auflösen können muss, das ist nachvollziehbar. Aber die Provider werden entsprechend des Gesetzentwurfes überhaupt nicht verpflichtet, Pseudonyme anzubieten – sie können es. Sie werden auch nicht verpflichtet, mehrere Pseudonyme anzubieten. Um Selbstdatenschutz zu fördern, müsste ich mindestens die Möglichkeit auf fünf verschiedene Pseudonyme haben, um dann bei meinen verschiedenen Aktivitäten mit unterschiedlichen Pseudonymen zu arbeiten. Der Provider dürfte nur, und ausschließlich aufgrund richterlichen Beschlusses, das Pseudonym aufheben, und nicht wie im Gesetzentwurf vorgesehen, auf eine Abwägung, die ein Provider gar nicht treffen kann. Das ist eine absurde Regelung, dass der Provider eine Interessenabwägung machen kann. Ich selber bin externer Datenschutzbeauftragter bei vielen Firmen. Da gibt es ähnliche Formulierungen: „berechtigtes Interesse der verantwortlichen Stelle“, also der Firma, und „schutzwürdige Belange der Betroffenen“. Diese Abwägung ist eine

Gummiformulierung, das darf bei einer Pseudonymauflösung auf keinen Fall sein, da muss ein richterlicher Beschluss her.

„Ende-zu-Ende-Verschlüsselung werde durch De-Mail vereinfacht“, das steht in einer Broschüre mit Stand: Dezember 2010, mit der für De-Mail geworben wird. Diese Aussage kann ich nicht nachvollziehen. Mit der derzeitigen Konstellation oder Konfiguration Gestaltung von De-Mail wird die Ende-zu-Ende-Verschlüsselung eher erschwert als vereinfacht. Sie könnte zwar vereinfacht werden, wenn die Dienstleister, die De-Mail anbieten wollen, verpflichtet werden, entsprechende Apps – früher sagte man Plug-ins oder kleine Anwendungen – anzubieten, damit der Nutzer mit wenigen Klicks die Ende-zu-Ende-Verschlüsselung installieren, seinen Schlüssel generieren und dann die Ende-zu-Ende-Verschlüsselung dort, wo er sie wünscht, nutzen kann.

Die Ende-zu-Ende-Verschlüsselung wäre auch erforderlich, um wirklich dem Post- und Fernmeldegeheimnis Rechnung zu tragen, das in Deutschland ein sehr hohes Gut ist, und ich würde dringend empfehlen, dieses hohe Gut des Post- und Fernmeldegeheimnisses nicht bei De-Mail fallen zu lassen. Vielen Dank!

Vors. **Wolfgang Bosbach**: Wir danken Ihnen. Mal sehen, was jetzt alles richtiggestellt wird. Als Nächster bitte Herr Dr. Rohleder vom BITKOM Berlin. Sie kommen wahrscheinlich aus Hamburg?

SV **Dr. Bernhard Rohleder** (BITKOM e. V., Berlin, Hauptgeschäftsführer): Nein, ich komme gerade aus der Enquete-Kommission und wir sitzen hier um die Ecke in Berlin. Aber ich darf Ihnen, Herr Vorsitzender, zunächst einmal für die präzise Begrüßung danken und ich habe auch nichts zu korrigieren.

E-Mailen heute ist unsicher, ist unverbindlich, hat zweifelhafte Integrität. Es ist darüber hinaus, wenn man das alles umgehen will, relativ teuer verbindlich zu kommunizieren und ist noch relativ kompliziert. Wie hat die Wirtschaft darauf reagiert? Es wurden kommerzielle Verfahren zur Ende-zu-Ende-Verschlüsselung angeboten und die werden etwa in 5 % aller Nicht-Spam-E-Mails eingesetzt. Insbesondere dort, wo Unternehmen unternehmensintern kommunizieren. Sie haben sich nicht im privaten Bereich und kaum in der Kommunikation zwischen Behörden und der Bevölkerung durchgesetzt. Es wird überwiegend auf den elektronischen Kommunikationsweg vollständig verzichtet. Sie haben sich z. B. auch nicht in der Kommunikation zwischen Versicherungsunternehmen und Versicherungsnehmern durchgesetzt. Was dazu führt, dass viele in der Bevölkerung bei jeder Versicherungsgesellschaft und bei vielen anderen Partnern einzelne Postfächer haben, wo entsprechende Dokumente hinterlegt werden. Sie müssen sich Ihre Passwörter merken. Dieses hat zur Folge, dass Sie ein Passwort für viele Postfächer haben. Das

schafft zusätzliche Internetunsicherheit. An der Stelle sehen wir mit dem De-Mail-Gesetz und dem jetzt angedachten Verfahren – wir benutzen den Begriff nur noch zurückhaltend, weil man ihn so oft hört – aber einen echten Quantensprung in eine sichereres, unkompliziertes, preiswerteres, integeres und verbindliches Internet.

Die Frage der Ende-zu-Ende-Verschlüsselung, meinen wir, sollte man an der Stelle durchaus realistisch betrachten. Wir haben einen deutlichen Fortschritt in der Transportverschlüsselung. Bei der Frage, ob auch Ende-zu-Ende verschlüsselt werden muss, würden wir sagen, es sollte sich jedes Unternehmen, jede Privatperson aussuchen können, wie viel Sicherheit sie gerne möchte. Wer die absolute Sicherheit möchte, so sie überhaupt darstellbar ist, der sollte auch die Ende-zu-Ende-Verschlüsselung wählen. Das werden manche tun. Diejenigen, die sich mit der 99,9 %-Sicherheit zufriedengeben, sollten es bei der Standard-anwendung, der Transportverschlüsselung, belassen. Wir bekommen Sicherheit immer nur auf Kosten des Komforts. Es geht nicht anders, das zieht sich wie eine rote Linie durch die IT, die Telekommunikation, die Internetwelt und insofern müssen Sie überlegen, wie Sie Sicherheit und Komfort gegeneinander abwägen.

Die Frage der Integrität wird durch die De-Mail beantwortet, das ist Ihnen klar. Die Frage des Preises ist in der Gesetzesbegründung aufgegriffen worden, da würden wir zur Zurückhaltung mahnen. Wir gehen davon aus, dass die verbindliche Kommunikation mit De-Mail deutlich günstiger ist, als die im normalen Briefverfahren. Wir brauchen hierzu auch einen entsprechenden Wettbewerb im Markt der sicheren Kommunikationsanbieter und wir sollten nicht auf Basis dessen, was jetzt auf dem Markt ist, Entscheidungen darüber treffen, wie sich der Markt in fünf Jahren entwickeln wird. Die Telekommunikation bietet heute vergleichbare Leistungen zu 2 % des Preises an, den wir vor zehn Jahren hatten. Wir sehen hier deutlich eine Preis-Leistungs-Verbesserung im Sinne der Verbraucher.

Wir haben ein Sonderthema, das ist die Domainendung. Hier ist für uns die Situation als BITKOM nicht ganz einfach. Wir haben eine Mehrheit von 90 % der Unternehmen, die sich auch hier für eine verbindliche Klärung im Gesetz im Sinne der Portierbarkeit der entsprechenden Adressen ausspricht. Der Bundesverband der Deutschen Industrie, den ich hier auch vertreten darf, spricht sich ebenfalls im Sinne der Anwender dafür aus, die sagen, wir müssen so einfach wie möglich auch den Anbieter wechseln können, wenn es z. B. neue Leistungen und Preise auf dem Markt gibt. Aber es gibt im BITKOM auch eine anderslautende Meinung, das ist eine Mindermeinung bei uns, die ich aber noch äußern möchte. Diese lautet, dass wir Investitionsschutz in die Markenidentität der Anbieter brauchen, die sich dann umsetzen sollte in einer entsprechenden Regelung, wie sie heute bereits im Entwurf niedergelegt ist.

Zusammengefasst sehen wir Deutschland hier erstmals im Bereich der ITK-Branche in einer internationalen Vorreiterrolle und wollen hier nicht von einem Alleingang sprechen. Es gibt europäische Initiativen, unter anderem die Stork-Initiative, die auf der deutschen Initiative aufsetzen sollten. Wir plädieren dafür, so schnell wie möglich dieses Gesetz zu verabschieden und es zur Grundlage internationaler einschlägiger Regelungen zu machen. Vielen Dank!

Vors. **Wolfgang Bosbach**: Wir danken Ihnen, Herr Dr. Rohleder. Der nächste Sachverständige ist Herr Prof. Dr. Spindler von der Georg-August-Universität in Göttingen.

SV **Prof. Dr. Gerald Spindler** (Georg-August-Universität Göttingen): Vielen Dank, Herr Vorsitzender. Es gibt nichts zu korrigieren und ich werde auch versuchen, die 300 Sekunden einzuhalten.

Zum ersten Punkt: Ich schließe mich dem Kollegen Rohleder an, was die Frage des Verhältnisses von Vorreiterrolle und Insellösung angeht. Allerdings kann man die Befürchtung äußern, dass von Deutschland vielleicht nicht immer genug Impulse für Brüssel bzw. die EU gegeben werden.

Eine Vorbemerkung zum zweiten Punkt: Es wäre wirklich wünschenswert, wenn wir endlich einmal den „Gordischen Knoten“ insgesamt durchschlagen würden, der sich um digitale Signatur, sicherer Transport, E-Mail und IT-Sicherheit rankt. Das ist ein Thema, was in Brüssel auch thematisiert werden muss, das wird allein in Deutschland nicht zu lösen sein. Das als grundsätzliche Vorbemerkung.

Der zweite Punkt: Da würde ich der 90 %-Meinung beim BITKOM widersprechen, dass wir unbedingt eine einheitliche Domain brauchen. Wettbewerb kann sehr wohl hergestellt werden, indem entsprechende Zertifizierungen für Produkte verwendet werden. Wir reden hier über Produktsicherheitsrecht. Die nötige Sicherheit wird an den Markt nicht durch einen einheitlichen Namen signalisiert, sondern durch entsprechende TÜV- oder sonstige Qualitätssiegel. Dafür brauche ich nicht einen einheitlichen Markennamen. Auch im sonstigen Verbraucherschutz kommt man mit einem verlässlichen Qualitätssignal aus. Wir verlangen nicht für den Verbraucherschutz, dass wir einen einheitlichen Markennamen haben, um z. B. einen guten Kakao oder dergleichen an die Verbraucher zu signalisieren. Das brauchen wir nicht. Wir brauchen ein verlässliches Siegel.

Zum Punkt „Datenschutz“: Erstens Kopplungsverbot – da schließe ich mich dem an, was vorher gesagt worden ist. Das sehe ich mitnichten so, dass wir unbedingt das Kopplungsverbot aufweichen sollten.

Zum Punkt 3 b: Etwas was bisher nicht oder nur ansatzweise thematisiert worden ist, das ist das Stichwort „Pseudonym und Auskunftsanspruch“. Da stimme ich ausdrücklich dem Kollegen Hülsmann zu. Es ist verwunderlich, dass wir im Urhebergesetz beim Auskunftsanspruch wesentlich höhere Schwellenwerte haben, wenn es um die Preisgabe von personenbezogenen Daten geht. Das war damals auch Konsens bei der Gesetzesfassung in Umsetzung der Enforcement-Richtlinie, insbesondere hinsichtlich der Notwendigkeit einer richterlichen Anordnung unter verfassungsrechtlichen Aspekten. Deswegen würde ich darum bitten, noch einmal darüber nachzudenken, ob man nicht einen Richtervorbehalt entsprechend wie in § 101 Urhebergesetz und in entsprechenden Parallelnormen einführen sollte.

Der vierte Punkt – Stichwort „Insolvenz“: In § 11 des Gesetzes ist z. B. der Fall angesprochen, dass der akkreditierte Dienstleistungsanbieter seine Tätigkeit einstellt. Es ist aber nirgendwo für die Stellung des Insolvenzverwalters Vorsorge getroffen worden, etwa hinsichtlich von Erfüllungswahlrechten des Verwalters. Oder es wird Insolvenz mangels Masse abgelehnt etc. Es steht im Gesetz, dass dann innerhalb von drei Monaten alles übertragen würde; aber was passiert wenn er in Insolvenz geht? Da sehe ich gar nichts. Ich habe im Gesetz noch einmal gesucht, aber ich habe nichts dazu gefunden. Das ist ein Punkt, den man noch einmal durchdenken sollte. Das mag zwar bei den großen Providern fernliegend sein und Sie haben auch eine Deckungsvorsoge in das Gesetz geschrieben, aber auch diese kann versagen. Außerdem ist die Deckungsvorsorge nicht allzu hoch.

Zum Stichwort „Freiwilligkeit der Benutzung“ ist auch schon das Wesentliche gesagt worden.

Zum nächsten Punkt, „Ende-zu-Ende-Verschlüsselung“: Da ist meines Erachtens die Position von BITKOM die richtige, d. h. wir brauchen ein relativ hohes Maß an Sicherheit. Das fällt in den Beurteilungsspielraum des Gesetzgebers. Persönlich würde ich für Ende-zu-Ende-Verschlüsselung plädieren. Aber das soll der Markt entscheiden. Wenn das zusätzlich vom Markt mit entsprechenden transparenten Informationen angeboten wird, und ich mich dafür entscheiden kann, dann soll es den Leuten überlassen bleiben, ob sie es wollen oder nicht.

Der letzte Punkt, den ich als Wirtschaftsrechtler ein bisschen bedauere: Das Ganze sieht für mich ein bisschen wie ein Verwaltungszustellungsergänzungsgesetz aus. Wir haben aber viele Probleme, die gerade auch in Richtung Versicherung angesprochen worden sind, im allgemeinen Bürgerlichen Gesetzbuch (BGB). Bei Einführung der qualifizierten digitalen Signatur wurden auch Formfragen etc. in § 126a BGB mit geregelt. Aber die Fragen Zugang, Anscheinsbeweis etc., alles was sich darum rankt, und was mit dem De-Mail-Gesetz geregelt werden soll, zumindest indirekt, hätte man vielleicht ausdrücklich im Gesetz auch ansprechen sollen, auch

wenn in den Begründungen steht: Es reicht, wenn man die Zivilprozessordnung (ZPO) hat, und das kann man daraus interpretieren. Es würde auch hier für unsere bürgerlich rechtlichen Richter der Klarstellung halber dienen, wenn man dazu ein paar Takte sagt, wie man „Zugang“ versteht. Vielen Dank!

Vors. **Wolfgang Bosbach**: Der nächste Sachverständige ist Herr Dr. Vossius vom Deutschen Notarverein hier in Berlin.

SV **Dr. Oliver Vossius** (Deutscher Notarverein e.V., Berlin): Vielen Dank, Herr Vorsitzender. Warum bin ich hier? Als Notar bin ich jemand, der den elektronischen Rechtsverkehr mit modernen Sicherheitstechnologien täglich sogar mehrfach nutzt. Ich nenne nur die Schlagworte „Elektronisches Gerichts- und Verwaltungspostfach - EGVP“, „Digitale Signatur“, „Elektronisches Grundbuch- und Handelsregister“, „Zentrales Vorsorgeregister“ und jetzt auch „Testamentsregister“. Mit dem NotarNet verfügen wir Notare über eines der sichersten Netze im nicht-militärischen Sektor. Jetzt kommt die De-Mail und ich habe das Gefühl, man erwartet von mir, dass ich meine schusssichere Kettenweste gegen einen römischen Lederpanzer eintausche. Bei mir zu Hause in Feldafing betreibt eine Frau Oliv einen Schreibwarenladen mit einer Postagentur. Zu ihr kommt ein Herr und legt ihr einen griechischen Pass und einen Handelsregisterauszug aus Nikosia/Zypern vor, wonach er als Direktor für die Amtskasse Limited handelt. Frau Oliv bezeichnet die Identität des Herrn anhand seines griechischen Passes und leitet die Unterlagen an die Post weiter, denn er möchte ein De-Mail-Konto eröffnen. Dort bei der Post wird ihm das De-Mail-Konto eröffnet und der Firma die E-Mail-Adresse: amtskasse@de-post.de zugewiesen. Kurze Zeit später hat der Gründer der Limited die Firma geändert, den Sitz verlegt und ein physisches Büro gab es ohnehin nie. Nunmehr versendet er über diese Adresse im großen Stil amtlich aufgemachte Rechnungen und Bescheide, in denen er von den Nutzern unter Androhung von Zwangsmaßnahmen Gelder verlangt. Dabei bedient er sich zur Legitimierung des Identitätsbestätigungsdienstes nach § 6 des De-Mail-Gesetzes. Das nicht ausrottbare Übel der betrügerischen Handelsregister-rechnungen, die per Post kommen, zeigt, dass sich selbst mit den Kosten für Porto solch ein Geschäftsmodell zu rentieren scheint. Bereits dieses alltägliche Beispiel verdeutlicht: Identifizierungsdienst und Adressvergabe machen De-Mail momentan zur Mogelpackung. Bei der Identifizierung können Vertretungsverhältnisse nicht zuverlässig geklärt werden. Wer von Ihnen weiß, dass eine zypriotische Limited immer von zwei Personen vertreten wird? Der Identitätsbestätigungsdienst bestätigt keine aktuellen Verhältnisse. Der Provider führt keinerlei eigene Recherchen durch, wie sollte er auch? Über seine Vertragsbedingungen verpflichtet er allenfalls den Betrüger, ihn zu informieren. Selbst der ehrliche Bürger wird die Änderungsmeldung oft vergessen. Was ist dann die Bestätigung nach § 6 des Gesetzes als Beweismittel noch wert? Hier bestätigt nur jemand, dass irgendwann einmal irgendwer Frau Oliv seinen Ausweis gezeigt hat. Meine Empfehlung: Streichen Sie den § 6 heraus, denn

diese Vorschrift wird Ihnen nur Ärger machen. Zudem ist unklar, wer für eine falsche Identitätsbestätigung haftet. Mein Beispiel mit der Firmenänderung zeigt aber auch, dass ich mir bei De-Mail Pseudonym-Adressen ergaunern kann, die man als solche gar nicht erkennt. De-Mail bietet damit keinen optimalen Schutz vor Viren, Trojanern, Phishing, Spam und den ganzen anderen Scheußlichkeiten. Mithin: das Gesetz löst sein Sicherheitsversprechen derzeit nicht ein. Für mich ist mehr als eine Mogelpackung der § 5 Abs. 9 des De-Mail-Gesetzes. Der unbedarfte Leser meint, dass die Abholbestätigung die Übermittlung der Nachricht auf den Computer des Empfängers und das Öffnen der Nachricht dort bestätigt. Falsch, die Abholbestätigung ist nur die Bestätigung, dass man sich bei seinem De-Mail-Provider sicher angemeldet hat. Sie besagt noch nicht einmal, dass man unter dem ganzen Werbemüll die Abrissverfügung tatsächlich gefunden, geschweige denn gelesen hat. Unerkannt laufen die Rechtsmittelfristen, der Anspruch auf rechtliches Gehör bleibt auf der Strecke und der Gegenbeweis ist dem Bürger kaum möglich.

Bei allem Respekt, meine Damen und Herren, das ist für mich Bauernfängerei. So etwas zerstört das Vertrauen des Bürgers in den Rechtsstaat. Daher sehen Sie bitte eine Bestätigung vor, die nach dem Öffnen der Nachricht auf den Computer des Nutzers versandt wird. Warum also das Ganze? Hier geht es nicht um gezielte Bevorzugung bestimmter Branchen, sondern bestimmter Anbieter. Letztlich geht es darum, Porto für das E-Mailen einzuführen. Dazu wird ein suboptimales Produkt mit viel Aufwand entwickelt und in den Markt gepuscht. Durch die Vergabe eines staatlichen Gütesiegels soll für ein bestimmtes Produkt ein Oligopol zementiert werden. Andere Technologien wir EGVP, Elster und qualifizierte elektronische Signatur werden als Sonderanwendungen diskriminiert. Ich habe bei der Sache an das mittelalterliche Salz-, Münz- oder Postregal gedacht. Wir sind für moderne Technik, aber wir fordern ein technik- und wettbewerbsneutrales Konzept.

Mein persönliches Fazit: De-Mail werde ich mir freiwillig nicht antun. Ich werde auch meine Klienten entsprechend beraten und gerade meine Klienten aus der IT-Sicherheitsbranche bestärken mich in dieser Ansicht.

Vors. **Wolfgang Bosbach**: Vielen Dank! Jetzt bitte Herr Welte vom Chaos Computer Club.

SV **Harald Welte** (Chaos Computer Club, Berlin): Guten Tag, sehr geehrter Herr Vorsitzender, sehr geehrte Damen und Herren Abgeordnete. Im Zusammenhang mit dem Gesetzentwurf zu De-Mail stellt sich mir vor allem folgende Frage: Warum sollte ein Bürger oder Verbraucher sich ein System angewöhnen, welches ihm verglichen mit herkömmlicher Briefpost rechtlich zahlreiche Nachteile einhandelt? Das Briefgeheimnis ist so in dem De-Mail-Entwurf, wie er heute vorliegt, nicht gegeben. Die Gefahr unbemerkter und ungewollter Zustellungen wird deutlich erhöht, wie mein Vor-

redner bereits erwähnt hat. Das ganze De-Mail-Gesetz sieht für mich danach aus, als ob es ausschließlich nach den Bedürfnissen der Verwaltungen und Behörden geschneidert worden wäre.

Zu den einzelnen Punkten: Die fehlende Ende-zu-Ende-Verschlüsselung ist bereits mehrfach aufgegriffen worden und ist Gegenstand mehrerer Stellungnahmen unterschiedlicher Sachverständiger in dem Verfahren. Was mir persönlich am Herzen liegt, ist, dass der erhebliche technische, organisatorische und letztlich auch finanzielle Aufwand, der auf einen De-Mail-Anbieter zukommt, sich eigentlich nur daraus erschließt, dass keine Ende-zu-Ende-Verschlüsselung vorgesehen ist. Durch die Tatsache, dass die Information innerhalb dieser Nachricht zumindest kurzfristig unverschlüsselt bei den einzelnen Diensteanbietern vorliegt. Wenn man sich die technischen Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zu De-Mail ansieht, da werden Wandstärken vorgegeben, wie aufwendig die Schließmechanismen an Rechenzentren zu sein haben, dass mindestens acht verschiedene Leute einzelne Berechtigungen in diesem kompletten System haben. Das ist ein erheblicher Aufwand, der nur dadurch entsteht, dass man auf die Ende-zu-Ende-Verschlüsselung verzichtet. Meiner Meinung nach könnte man das System deutlich günstiger und mit weniger sicherheitstechnischem Aufwand haben, wenn man die Ende-zu-Ende-Verschlüsselung einführen würde.

Die Argumentation der Bundesregierung in der Antwort auf den Bundesrat in den einschlägigen Drucksachen, dass die Ende-zu-Ende-Verschlüsselung zu kompliziert für den Anwender sei und darüber hinaus Installationen spezieller Software benötigt werden, kann ich nicht teilen. Es ist heute ohne Probleme möglich, mit modernen Webtechniken Ende-zu-Ende-Verschlüsselung im Webbrowser zu realisieren, ohne dass zusätzliche Software seitens des Anwenders installiert werden muss.

Einer meiner Vorredner hat erwähnt, dass jetzt endlich durch dieses Gesetz ein Standard geschaffen wird, mit dem der Transport der Nachrichten zwischen den Anbietern verschlüsselt werden kann. Technisch liegen diese Standards seit vielen Jahren vor. Das technische Verfahren SMTP über TLS, das bei De-Mail verwendet wird, um die Nachricht im Transport zu verschlüsseln, wird in der Industrie bereits genutzt und das kann die Privatwirtschaft mit der gängigen Software auch heute schon verwenden. Dafür brauche ich kein De-Mail-Gesetz, um diese technischen Verfahren, die von gängiger Software unterstützt werden, und bereits in der Privatwirtschaft zum Einsatz kommen, als Übertragungsverschlüsselung einzusetzen.

Seitens der Überwachung hat man das Problem bei De-Mail, dass im De-Mail-Postfach liegende Post, ob sie nun geöffnet ist oder nicht, oder als zugestellt gilt oder nicht, Geheimdiensten und Polizei ohne richterliche Anordnung zugänglich

ist. Das ist gegenüber der klassischen Briefpost eine deutliche Schlechterstellung des Anwenders.

Die Zugangseröffnung ist auch bereits mehrfach zur Sprache gekommen. Auch ich spreche mich deutlich dafür aus, dass die Zugangseröffnung nach Verwaltungszustellungsgesetz deutlich zu trennen ist von der Nutzung einer De-Mail-Adresse oder auch der Veröffentlichung der De-Mail-Adresse im Verzeichnisdienst. Wie bereits erwähnt, ist die Gefahr von ungewollter Zustellung da.

Weiterhin vermisse ich die Freiwilligkeit in einer deutlicheren Verankerung im Gesetz. Ein freiwilliges De-Mail-System an sich, dabei bleibt es dem Bürger überlassen, ob er das nutzt. Was passiert, wenn Behörden oder andere Dienstleister bestimmte Dienstleistungen nur noch anbieten, wenn De-Mail verwendet wird? Das ist etwas, was es zu verhindern gilt. Dann bleibt von der derzeit viel besprochenen Freiwilligkeit nicht mehr viel übrig.

Als letzten Punkt möchte ich die Insellösung und die fehlende Interoperalität ansprechen. Wenn man sich die technischen Richtlinien des BSI zu De-Mail durchliest, es sind 22 und ich habe sie gelesen, sind dort die gleichen Protokolle und Verfahren aufgelistet, die zum E-Mail-Versand verwendet werden. Trotzdem ist das De-Mail-System nicht interoperabel mit der herkömmlichen E-Mail. Es ist von der Technik her absolut einfach möglich, es interoperabel zu machen, aber es wird künstlich ein Riegel vorgeschoben. Dadurch haben wir inkompatible Systeme. Außerdem gibt es auf europäischer Ebene durch das Europäische Komitee für Normung (CEN) die Normen CEN 15121-1 und -2, welche im Jahr 2010 veröffentlicht wurden und eine europäische Norm für elektronische Post und Hybridpostverfahren setzen sollen. Warum wird im gesamten De-Mail-Verfahren nie darauf eingegangen, dass hier die DIN und andere europäische Normierungsgremien, legitimiert durch die Europäische Kommission, an Standardisierungsverfahren arbeiten, die völlig parallel und unabhängig zu De-Mail vonstattengehen? Die Verfahren sind auf einer technischen Ebene nicht kompatibel. Danke schön!

Vors. **Wolfgang Bosbach**: Vielen Dank! Das waren die Sachverständigen. Wir kommen zur ersten Fragerunde, bitte Clemens Binninger.

BE **Clemens Binninger** (CDU/CSU): Herr Vorsitzender, vielen Dank. Ich habe eine Frage an Herrn Dr. Brink und an Herrn Prof. Spindler. Das betrifft die schon ein paar mal angerissene Frage der Abholbestätigung. Wir sind in der Koalition davon ausgegangen, dass wir die Situation haben, dass ein Bürger auf sein Verlangen hin zum Schutz nicht mit Behörden per De-Mail kommunizieren will, weil er als Verbraucher damit schon geschützt ist. Es kann dann zu einem Postverkehr per De-Mail kommen, der durchaus Rechtsfolgen hat, und man in irgendeiner Form im System erkennen

muss, wann er sehen konnte, wann er diese Post oder De-Mail von der Behörde bekommen hat. Vergleichbar zur realen Welt: Wo ihm vielleicht von der Behörde ein Bußgeldbescheid oder irgendetwas zugestellt wird, und es auch nicht darauf ankommt, ob er diesen Bußgeldbescheid öffnet und ihn gelesen hat und sagt: So ein Mist. Es reicht, dass man ihn ihm gibt. Es war für uns die Überlegung, diese Abholbestätigung im De-Mail-Verkehr zwischen Bürgern und Behörden, sonst nicht, so vorzusehen.

Ich wurde darauf hingewiesen, dass man eine technische Regelung finden müsste und das wäre meine Frage, die vielleicht einen Schritt weiter geht als die pure sichere Anmeldung. Wenn man darauf abhebt, dass eine Abholbestätigung vom System erst dann generiert werden kann, wenn quasi der Nutzer nicht nur sich sicher angemeldet, sondern auf seinem Bildschirm auch schon sein Postfach De-Mail mit Posteingang erschienen ist, sodass er quasi sehen konnte, ich habe Post von der Stadt Berlin oder Hamburg. Halten Sie das, die Frage geht an Sie beide, für zusätzlich notwendig? Müsste man so etwas in einer Richtlinie präzisieren? Ich sehe eigentlich nicht, dass man das im Gesetzestext verankern kann, wann welche Bildschirmmaske relevant sein soll. Oder hielten Sie es aus Sicherheitsaspekten und auch aus Aspekten des Verbraucherschutzes heraus für nicht notwendig?

Vors. **Wolfgang Bosbach**: Herr Dr. Brink, bitte.

SV **Dr. Stefan Brink**: Ich würde sogar noch einen Schritt weiter gehen als Sie mit Ihrer Frage andeuten. Ich würde eher dafür plädieren, auf die Abholbestätigung vollständig zu verzichten und mein Augenmerk auf Art. 3 des Gesetzentwurfs mit der Zustellungsfiktion richten. Ich würde eher mit der Fiktion arbeiten, als zu versuchen, zu genau herauszubekommen, wann die Nachricht tatsächlich geöffnet oder gelesen wurde. Meine Kritik in dem Punkt ist keine datenschutzrechtliche im eigentlichen Sinne. Datenschutzrechtlich ist die Abholbestätigung deswegen ein Übel, weil dadurch die andere Seite Informationen bekommt, die sie nicht unbedingt bekommen muss. Sie bekommt die Information, wann der Nutzer tatsächlich an sein Postfach herangegangen ist. Aus Datenschutzrecht wäre eine Lösung schöner, bei der diese personenbezogenen Daten gar nicht fließen. Meine Argumentation bezieht sich ausschließlich auf den Gesetzentwurf selbst und ich behaupte, dass der in dem Punkt inkonsistent ist. Abgesehen von der Fragestellung, dass die Abholbestätigung keine Abholbestätigung ist. Auch abgesehen von der Fragestellung, dass sie nach Gesetzeswortlaut, insbesondere auch mit Blick auf den Änderungsantrag der Fraktionen CDU/CSU und FDP, bei einer unsicheren Anmeldung gar nicht gegeben wird. Wo ich nicht genau weiß, ob das so gewollt ist. Es gibt noch nicht einmal die Bestätigung der Möglichkeit der Abholung, das war Ihr Beispiel im Vergleich zur Briefpost, weil das Postfach inzwischen gesperrt sein kann. Die Sperrung sieht zwar in § 10 Abs. 1 am Ende vor, dass der Abruf auch von einem gesperrten Konto möglich bleiben muss.

Aber davon gibt es in Abs. 2 Ausnahmen, die ich so deute, dass der Diensteanbieter sagen kann: Wenn du, lieber Nutzer, in Zahlungsverzug bist, sperre ich dir die Möglichkeit, eine Leistung von mir, nämlich den Abruf der Nachricht zu bekommen. Sodass wir die Situation haben, wir haben eine sichere Anmeldung des Nutzers am gesperrten Konto. Er muss sich anmelden können, sonst ist die Abholbestätigung gar nicht möglich. Er sieht möglicherweise die Mail sogar, das ist für den Diensteanbieter ein schönes Druckmittel, dass ich dem Nutzer zeige, hier ist etwas ganz Wichtiges für dich, jetzt zahle einmal, du bist im Verzug, aber aufmachen darfst du es nicht. Jedenfalls plädiere ich in dem Zusammenhang dafür, dass dem Nutzer von Seiten des Diensteanbieters ganz deutlich gemacht wird, du kannst die Nachricht abrufen. Das steht bisher nur im Gesetz, das weiß der Nutzer aber gar nicht. Möglicherweise bekommt er durch den Sperrhinweis des Diensteanbieters suggeriert: das Konto ist für dich nicht mehr verfügbar. Dann steigt der Nutzer wieder aus und sagt: Schade! Deswegen plädiere ich ganz an den Anfang zurück dafür, gar keine Abholbestätigung, sondern das Ganze über die Zustellungsfiktion abzuwickeln.

Vors. **Wolfgang Bosbach**: Vielen Dank, Herr Prof. Spindler, bitte.

SV **Prof. Dr. Gerald Spindler**: Ich mache es kurz: Meines Erachtens wird es nicht ausreichen, das nur auf den Zugang des Servers zu beziehen. Ein ganz einfaches Beispiel aus der jetzt-Welt: Wenn Sie mit dem Zug von hier nach Hannover reisen, fahren Sie mit Ihrem Mobilteil durch diverse Funklöcher. Sie sind dann zwar angemeldet, aber haben dennoch keinen Zugang. Es geht hier nicht um Tage oder Wochen, aber wir paraphrasieren einmal die Situation: ich bin zwar angemeldet, gelte sogar noch als eingeloggt, bin aber weg, ich kann überhaupt nichts. Wenn ich meinen guten alten bürgerlich rechtlichen Begriff des „Zugangs“ und des „in den Machtbereich des Empfängers geraten“ nehme, in dem Sinne, dass der Nutzer wirklich die Macht hat, die Sachen zur Kenntnis zu nehmen, da würde ich sagen: Es reicht nicht. Da brauchen wir in der Tat das, was Sie eben angesprochen haben und – als Jurist ist man geneigt, das in eine Verordnung zu packen, aber die ist eventuell zu unflexibel – dass vielleicht eine Richtlinie oder Standardisierung sicherer wäre. Das Problem ist und das sage ich als Jurist noch einmal ganz deutlich: Es ist so, dass das Rechtsfolgen auslöst. Von daher würde es eher für eine Verordnung sprechen.

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

BE **Gerold Reichenbach** (SPD): Ich bleibe bei dem Themenbereich und habe eine Frage an Herrn Dr. Vossius, Herrn Bobrowski und an Herrn Prof. Spindler. Es geht um den Bereich des Verwaltungszustellungsgesetzes. Wie beurteilen Sie die Änderung zwischen der alten Formierung „glaubhaft macht“ und der neuen Formulierung „nachweist“ in § 5 Abs. 7? Wie beurteilen Sie das aus der Sicht des Ver-

brauchers und welche Folgen hat dies für den mit Zustellungsfiktion bzw. bei nicht vorhandener Zustellung, für den, der mit irgendjemandem im Rechtsverkehr ist?

Das Zweite wurde von Herrn Welte und Herrn Prof. Spindler angesprochen, das war die europäische Ebene. Nach meinem Kenntnisstand soll diese europäische DIN-Norm, die auf Vorgaben des Weltpostvereins beruht, ab April Anwendung finden. Meine Frage: Wenn dem so ist, ist diese Norm beim De-Mail-Gesetz berücksichtigt bzw. bei dem, was im Dienst angeboten wird? Wenn dies nicht berücksichtigt ist, welche Konsequenzen hat das z. B. auch für den europäischen Rechts- oder Postverkehr?

Vors. **Wolfgang Bosbach**: Vielen Dank. Herr Dr. Vossius, bitte.

SV **Dr. Oliver Vossius**: Herzlichen Dank! Zunächst einmal das mit dem Nachweis, wo genau ist es geändert? Ich habe sowohl die Gegenäußerung als auch den Änderungsantrag vorliegen.

BE **Gerold Reichenbach**: § 5a Abs. 4 Verwaltungszustellungsgesetz.

SV **Dr. Oliver Vossius**: Verwaltungszustellungsgesetz – da stellt sich für mich eher die Frage: Wie erbringt der Bürger eigentlich den Gegenbeweis? Dass er, wenn er sich angemeldet hat, aus der Nummer wieder heraus kommt. Eine Abholbestätigung ist generiert, die hat quasi die Qualität der alten Zustellungsurkunde. Es ist eine öffentliche Urkunde, da ist an sich nur der Beweis der Fälschung zulässig. Dann müssen Sie beweisen, dass Sie irgendwo im Tunnel bei Fulda und deswegen gerade in einem Funkloch waren. Das irgendwo überzeugend darzustellen, wenn es um einen Entschließungskostenbescheid über einen fünfstelligen Betrag geht, wird wahrscheinlich vor dem Verwaltungsgericht schwerfallen. Ich bin skeptisch, ob das tatsächlich ein Weg ist. Der Bürger trägt letztlich das Risiko, dass zwischen dem Server seines Providers und seinem Computer irgendetwas passiert und das ist qualitativ etwas anderes als zwischen dem eigenen Briefkasten vor dem eigenen Reihenhaus und der Haustür.

SV **Prof. Dr. Gerald Spindler**: Wenn ich das gleich aufgreifen darf, dann ist an sich ein Glaubhaftmachen besser. Ansonsten muss ich den vollen Gegenbeweis führen. Hier habe ich zumindest zivilprozessual gesprochen eine Möglichkeit. De facto findet dasselbe im Verwaltungsprozess statt, dass man sekundäre Darlegungs- und Beweislasten hat. Wenn man sagt, da gibt es einen gewissen Anschein dafür, dass das doch mit dem Tunnel in Fulda so war, dann kippt das sozusagen auf die Gegenseite. Mit dem kompletten Nachweis hätte ich die volle Beweislastnutzung auf der anderen Seite.

Nicht rekonstruierbarer Einwurf aus der Zuhörerschaft

SV **Prof. Dr. Gerald Spindler**: Wenn es mit Nachweis ist, ja. Wollen Sie zuerst? ...

SV **Harald Welte**: Nein, bitte.

SV **Prof. Dr. Gerald Spindler**: Gut, dann zäume ich das Pferd von hinten auf. Herr Welte, bitte helfen Sei mir noch einmal, die Mandatierungsgrundlage an die CEN-Norm habe ich jetzt nicht im Kopf. Ich meine, es müsste aufgrund einer der TK-Richtlinien gewesen sein. Wenn Sie mir bitte kurz helfen würden. Um es vorweg zu nehmen, es dürfte, was die Rechtsfolgen von Zustellung u. ä. angeht, eigentlich keine Auswirkungen haben, weil mir keine Richtlinie bewusst ist, die hier irgendwelche Normungen im Zusammenhang mit solchen Rechtsfolgen setzen würde. Es kann nur im Bereich der eigentlichen Produktsicherheit sein, des traditionellen Ansatzes. Ich bin am Überlegen, gebe den Ball erst einmal weiter.

SV **Harald Welte**: Ich kann Ihnen leider nicht sagen, auf welcher Legitimierungsgrundlage diese Norm entstanden ist. Ich bin kein Jurist, ich bin Techniker und ich weiß, dass die Normen vom Ausschuss CEN/TC 331 geschaffen wurde und dass die DIN daran beteiligt ist, aber mehr kann ich dazu nicht sagen.

Vors. **Wolfgang Bosbach**: Herr Prof. Spindler, ich hoffe, Sie sind einverstanden, dass ich die Wortmeldungen wieder an mich ziehe. Herr Bobrowski war auch noch gefragt worden.

SV **Michael Bobrowski**: Es war in diesem Fall nicht so schlimm, Herr Prof. Spindler. Ich habe mich nicht zurückgesetzt gefühlt, ich würde nämlich Ihnen und Herrn Dr. Vossius beipflichten. Das tue ich umso lieber, als ich von Hause aus kein Jurist bin und mich etwas unsicher fühlen würde, wenn ich das juristisch beurteilen müsste. Herr Reichenbach, ich hoffe, Sie sind mit den Vorrednern und deren Ausführungen einverstanden. Ich kann mich dem anschließen. Auch aus der Sicht der Verbraucher ist das so. Ich sehe da auch eine gewisse Verschlechterung. Danke!

Nicht rekonstruierbare Frage aus der Zuhörerschaft

Vors. **Wolfgang Bosbach**: Was ist mit der? Die Bundesregierung denkt, das ist ihre Hauptaufgabe.

BE **Clemens Binninger** (CDU/CSU): Da es um Abstimmungen von Richtlinien auf internationaler Ebene und um Konkurrenzverhältnisse geht, hatte der Kollege Reichenbach gefragt, ob die Bundesregierung dazu etwas Aufklärung leisten könnte.

MinDir **Martin Schallbruch** (BMI, IT-Direktor): Wir haben uns mit der Frage der Standardisierung der elektronischen Postdienstleistung im Zusammenhang mit dem De-Mail-Gesetz natürlich auseinandergesetzt. Wir haben auch mit den einschlägigen Unternehmen, die solche Dienstleistungen in Deutschland erbringen wollen, gesprochen. Es ist keine verpflichtende Standardisierung, die vorsieht, dass da irgendwelche Rechtsfolgen daran geknüpft werden sollen. Sondern es ist eine Produktstandardisierung, die noch weit davon entfernt ist, dass das marktgängig ist, oder dass es hier Marktangebote gibt, nicht in Deutschland, auch nicht in anderen europäischen Staaten. In dieser Phase der Standardisierung ist es so, dass es sich einfach nicht anbietet, dass man hier an diesen Dienst anknüpft. Die Standardisierung, die de facto im Internet für elektronische Kommunikation vorhanden ist, auch für die E-Mail-Kommunikation, wird, soweit möglich und soweit die Sicherheitsziele von De-Mail erreichbar sind, übernommen. Was auch dazu geführt hat, dass wir uns innerhalb der EU verabredet haben, dass De-Mail in das schon erwähnte STORK-Projekt aufgenommen wird, um dort elektronische Zustellung mithilfe von Technologien wie De-Mail zu erproben.

Vors. **Wolfgang Bosbach**: Herr Reichenbach, ist das klar?

BE **Gerold Reichenbach** (SPD): Wenn die Bundesregierung schon antwortet. Wir haben da sehr lange recherchiert. Es gibt auch eine Vorabfassung, die ich aber technisch nicht verstehe. Ich kann Ihnen die DIN-Nummern nennen, die in die deutsche DIN-Norm übernommen werden. Wenn Sie sagen, das ist unerheblich, dann heißt das, wir machen ein Gesetz, das mit der ab April geltenden deutschen DIN-Norm nicht kompatibel ist. Ich kann Ihnen auch die Nummern nennen, das sind die 1197 und 1198.

MinDir **Martin Schallbruch** (BMI): Das führt jetzt tief in die Standardisierungsprozesse. Die internationalen Standardisierungsorganisationen ISO, CEN und DIN machen unterschiedliche Normungsverfahren. Das sind auch Normungsverfahren, die keine allgemeine Verbindlichkeit beanspruchen, sondern die ein Stück Vornormen zur Diskussion sind. Um so etwas handelt es sich hier. Das ist dann eine DIN-Veröffentlichung in der Tat und da haben sich die Interessenverbände dazu geäußert. Das ist aber kein Abschluss der Diskussion. Solche Normungsprozesse verlaufen immer so. In diesem frühen Stadium der Normung elektronischer Postdienstleistung sind wir im Augenblick.

Vors. **Wolfgang Bosbach**: Herr Reichenbach, ist das so in Ordnung? Lassen wir es so stehen. Herr Höferlin, bitte.

BE **Manuel Höferlin** (FDP): Vielen Dank, Herr Vorsitzender. Ich habe noch einmal eine Frage zum Thema Domains. Was dazu bisher vorgetragen wurde, war im

Wesentlichen ein Punkt, nämlich der der Möglichkeit des Wechsels neben der Erkennbarkeit. Zur Erkennbarkeit wurde schon aus den Reihen der Sachverständigen gesagt, dass sich die Qualität oder die Eigenschaften eines Produkts nicht unbedingt nur über den Namen bestimmt – mir ist sofort das Beispiel mit dem Taschentuch eingefallen; man nennt einen Firmen- oder Markennamen und trotzdem gibt es verschiedene Qualitäten und Arten des Taschentuches. Ich möchte auf die Möglichkeiten und Problemstellungen beim Wechsel kommen. Der trifft ja nur zu, wenn man nicht den privaten Endnutzer sieht, weil der ja, wenn er eine De-Mail-Adresse wechseln wird, den Domainteil mit dem Namen des Providers wechselt, egal ob man eine einheitliche Domain vorgibt oder nicht. Wo es interessant wird, ist die Frage bei Unternehmen. Wir haben dann irgendwelche Namen. und bspw. de-mail.de. Wir haben ja kein Unternehmen, wo sich alle zusammen de-mail.de teilen werden und wenn Sie dann von einem Provider zum anderen wechseln. Das stand auch nie zur Diskussion, soweit ich das weiß. Viel interessanter ist für mich die Frage, wie es bei Unternehmen ist. Wir haben derzeit die Situation, dass nach unserem Vorschlag keine einheitliche Domain genommen wird, d. h. eine Firma A hat eine De-Mail-Domain, ich nenne sie einmal firma-a.de und eine andere Firma hat eine De-Mail-Domain firma-b.de. Jetzt wechselt die Firma A von einem Provider zum anderen und die Firma B auch von einem Provider zum anderen. Wo sehen Sie da ein Problem, wenn mit einer solchen Domain gewechselt wird, oder gibt es da kein Problem, wenn jemand seinen De-Mail-Domain-Namen mit von einem zum anderen Provider nimmt? Ich hätte dies gerne von Herrn Dr. Rohleder gewusst. Sie können das auch differenziert beantworten. Weil es auch eine technische Frage ist, hätte ich sie auch gerne von Herrn Welte beantwortet.

Vors. **Wolfgang Bosbach**: Herr Dr. Rohleder, bitte.

SV **Dr. Bernhard Rohleder**: Wenn es sich so verhält, wie Sie die Situation jetzt beschreiben, nämlich dass sich der Firmenname in der Endung und zwar ausschließlich in der Endung befindet, dann wird es kein Problem geben beim Umzug. Das werden die Provider entsprechend anbieten. Es wird sich allerdings der Firmenname nur bei den sehr großen Unternehmen als solche Endung finden. Kleine Handwerksbetriebe, der Einzelkaufmann, auch die Privaten werden wahrscheinlich nicht in der Situation sein, dass sie ihren Namen auch zum Domain-Namen machen können. An der Stelle wird es durchaus für einen nicht unerheblichen Teil der deutschen Wirtschaft ein Problem geben können.

Das Zweite: Es wird sich natürlich eine Verschlechterung gegenüber dem Status quo in der unverbindlichen, unsicheren und aktuellen E-Mail-Kommunikation ergeben. Insofern sollte das auch noch berücksichtigt werden.

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

SV **Harald Welte**: Zu dem Umzug: Wenn tatsächlich ein so genanntes Sub-Domain, also der Firmenname.de-mail.de zwischen De-Mail-Anbietern umgezogen wird, dann sehe ich auch keine Probleme. Das man keine Portierung von den Accounts einzelner Anwender hat, das ist etwas, was man technisch einfach hätte spezifizieren und auch vom Gesetz fordern können. Wir haben Rufnummern-Portierungen in Mobilfunknetzten in Deutschland seit 2002. Jetzt ist 2011 und wir diskutieren über ein neues Kommunikationsverfahren, wo ich nicht den Anbieter wechseln kann, ohne dass sich meine Kennung ändert. Das ist aus technischer Sicht ein bisschen komisch.

Vors. **Wolfgang Bosbach**: Herr Bobrowski, Sie hatten sich gemeldet.

SV **Michael Bobrowski**: Vielen Dank! Ich kann das, was Herr Welte gesagt hat, noch ein bisschen ergänzen. Einmal hätte ich auch auf diese Möglichkeit, die wir im Mobilfunk seit Jahr und Tag haben, hingewiesen. Die sich bewährt hat und die wir auch damals ausdrücklich gefordert haben.

Zum Zweiten: Ich mache das an einem Beispiel klar. Der Verbraucherzentrale Bundesverband hat nach dem derzeitigen Stand etwa 110 Mitarbeiterinnen und Mitarbeiter. Wir haben eine E-Mail-Adresse, in der kein Providername vorkommt, also nicht der Provider, den wir nutzen, um in das Internet zu gehen, bzw. E-Mail-Verkehr zu realisieren. Unsere E-Mail-Adresse lautet in meinem Fall bobrowski@vzbv.de. Wenn ich das richtig weiß, Herr Höferlin, heißt Ihre Adresse manuel.hoeferlin@bundestag.de. Da kommt auch kein Providername vor. Ich will damit nur ausdrücken, das ist technisch möglich, nicht nur für Großunternehmen, Herr Dr. Rohleder, sondern auch für jedermann. Ich habe auch schon Privatadressen gesehen, worin auch kein Providername vorkommt, den kann man sich wünschen und auch bekommen. Das ist kein Problem, allein von der Organisation solcher Adressen her steht dem nichts im Wege.

Das Dritte: Soweit ich informiert bin, Fachleute können mich da vielleicht noch korrigieren, ich habe das in Wirtschaftskreisen von Technikern gehört, wären unterschiedliche Domain-Bezeichnungen innerhalb eines Unternehmens ein Problem. Ich spreche jetzt nicht nur für unsere Klientel, um deutlich zu machen, was das für Probleme auch technischer Art bedeutet. Wenn ich es richtig verstanden habe, ist zwar das De-Mail-System auch in einem Unternehmen bei der Abwicklung der elektronischen Kommunikation ein in sich geschlossenes System innerhalb des Gesamtsystems der Kommunikation. Aber bevor ein Mitarbeiter in einem Unternehmen oder einem größeren Handwerksbetrieb eine De-Mail oder eine E-Mail alter Art zugestellt bekommt, laufen beide über denselben Mail-Server. Dieser Mail-Server muss dann entscheiden: De-Mail rechts oder E-Mail links, aufgrund der

unterschiedlichen rechtlichen Bedeutung und Folgen einer solchen speziellen Mail. Das heißt, dieser Mail-Server muss, wenn wir keine einheitliche Domain-Bezeichnung hätten, immer auf die Minute genau eine Datenbank haben, um zu entscheiden, diese Endung ist einer De-Mail zugeordnet, also firmen- oder provider-spezifische Endung, oder es ist eine einfache Mail, und die geht dann den anderen Weg. Das ist schon rein technisch ein schwieriges Unterfangen. Diese Datenbank müsste wirklich auf die Minute oder mindestens Stunde pro Tag aktuell sein, um tatsächlich über die richtigen Wege dieser Mail zu entscheiden. Das ist ein schwieriger Punkt und würde durch eine einheitliche Bezeichnung wesentlich vereinfacht werden. Das als zusätzliches Argument, was für uns als Privatnutzer nicht entscheidend ist. Für uns ist entscheidend die freie und einfache Portierungs-möglichkeit einer solchen Adresse, da sie letztendlich dazu dient, den physischen Postkasten elektronisch abzubilden, die namentlich dem Nutzer zugehörig sein muss und nicht irgendeinem Anbieter.

Vors. **Wolfgang Bosbach**: Vielen Dank! Frau Kollegin Wawzyniak, bitte.

Abg. **Halina Wawzyniak** (DIE LINKE.): Ich möchte noch einmal zur Ende-zu-Ende-Verschlüsselung nachfragen: Wenn ich Herrn Dr. Rohleder und auch Herrn Prof. Spindler richtig verstanden habe, haben Sie gesagt, am Ende soll das der Markt entscheiden, es soll keine Verpflichtung bei der Ende-zu-Ende-Verschlüsselung geben. Für mich stellt sich die Frage, denn wir haben auch gehört, dass bei diesem System, wenn es nicht kommt, d. h., wenn es keine Ende-zu-Ende-Verschlüsselung gibt, zumindest die Gefahr besteht, das grundgesetzlich geschützte Post- und Brief-geheimnis anzutasten. Ich formuliere es vorsichtig. Insofern habe ich bisher nicht verstanden, was gegen eine Verpflichtung spricht, diese Ende-zu-Ende-Ver-schlüsselung durchzuführen. Ich stelle die Frage an Herrn Dr. Rohleder. Wenn es tatsächlich um grundgesetzlich relevante Dinge geht, dass das die Bundesregierung vielleicht noch einmal in einer schriftlichen Stellungnahme erklären könnte. In der Drucksache 17/4145 haben Sie gesagt, würde es das ganze System gefährden, wenn es eine Ende-zu-Ende-Verschlüsselung gibt. Ich wüsste gerne noch einmal, was gegen eine Verschlüsselung spricht, ich habe es nicht verstanden.

An Herrn Welte die weitere Frage. Sie haben es in Ihrer schriftlichen Stellungnahme erwähnt, und auch noch einmal mündlich gesagt, dass bei ohne Ende-zu-Ende-Verschlüsselung, und wenn man die BSI-Richtlinien einhalten will, so ca. 8 Rollen notwendig sind. Wenn dem so ist, würde das nicht zu einer Wettbewerbsverzerrung führen, dass das nur eine bestimmte Anzahl von Anbietern machen kann? Würde das darüber hinaus die versprochene Kosteneinsparung, von der hier immer die Rede ist, nicht eigentlich wieder aufheben?

Vors. **Wolfgang Bosbach** Vielen Dank! Herr Dr. Rohleder, bitte.

SV **Dr. Bernhard Rohleder:** Ich glaube, die Frage ist relativ schnell und einfach zu beantworten. Es gibt bereits Ende-zu-Ende-Verschlüsselung seit ewigen Zeiten im Markt, fast so lange, wie es E-Mails gibt. Sie haben im Markt einfach versagt, sie werden nicht eingesetzt. Sie werden primär zur unternehmensinternen Kommunikation eingesetzt, also nur ein ganz geringer Anteil der E-Mail-Kommunikation, der tatsächlich entsprechend Ende-zu-Ende-verschlüsselt wird. Sehen Sie Ihr eigenes E-Mail Verhalten an, wer von Ihnen hat schon einmal eine E-Mail Ende-zu-Ende verschlüsselt und wer verfügt über einschlägige Informationen und einschlägige Software? Wahrscheinlich nur die allerwenigsten hier im Raum. Uns geht es darum, ein System im Markt zu haben, das ganz niedrige Eintrittsbarrieren hat, das bereits ein sehr hohes Maß an Sicherheit darstellt. Wer darüber hinaus die Ende-zu-Ende-Verschlüsselung möchte, der kann sie optional wählen und sie auch entsprechend einsetzen. Aber für den Großteil unserer täglichen E-Mail-Kommunikation, auch dann, wenn sie Verbindlichkeit braucht, brauchen wir diese 100 % aus meiner Sicht nicht, sondern es genügen die 99,9 %. Wir haben die 100 %-Sicherheit auch nicht im traditionellen Brief- und Postverkehr. Auch das reale Leben ist gefährlich, nicht nur das Internet. Die Sicherheit, die wir unter Transportverschlüsselung darstellen können, geht deutlich über das hinaus, was wir ansonsten im traditionellen Brief- und Postverkehr haben.

Vors. **Wolfgang Bosbach**: Bitte direkt dazu Herr Hülsmann, habe ich Sie richtig verstanden?

SV **Dipl. Inf. Werner Hülsmann**: Die Aussage, dass die Ende-zu-Ende-Verschlüsselung in der Wirtschaft kaum genutzt wird, ist so nicht richtig. Ich selber als externer Datenschutzbeauftragter betreue sehr viele Firmen, u. a. auch Callcenter-Dienstleister. Da ist es gang und gäbe, dass Kundendaten, die vom Callcenter in einem rechtlich einwandfreien Verfahren abtelefoniert werden sollen – Stichwort Datenverarbeitung im Auftrag – von den Telekommunikationsdienstleistern, von den Krankenkassen, von Versicherungen an den Callcenter-Dienstleister und auch die Ergebnisse zurück natürlich Ende-zu-Ende verschlüsselt werden. Auch in vielen anderen Bereichen wird firmenübergreifend eine Ende-zu-Ende-Verschlüsselung genutzt. Optional wählbar wäre eine Ende-zu-Ende-Verschlüsselung nur, wenn die De-Mail-Anbieter verpflichtet werden, sie auch anzubieten, sonst kann ich sie nicht optional wählen.

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

SV **Harald Welte**: Ich komme gleich zu dem Punkt mit dem Aufwand, den Kosten und den Rollen. Der Briefumschlag wird bei jedem Anbieter geöffnet, also die Transportverschlüsselung wird beim Anbieter aufgehoben, dann wird von entsprechender

Software in die Kommunikation hineingesehen und schließlich wieder die Kommunikation in einen neuen Umschlag gepackt für die nächste Transportverschlüsselung. Es ist so, dass hier kurzzeitig die Information bei dem Anbieter im Klartext unverschlüsselt vorliegt und daraus erwachsen erhebliche zusätzliche Sicherheitsnotwendigkeiten für den Betreiber einer solchen Anlage. Ich bin mir sicher, dass die Kosten, die für den Anbieter zum Betrieb des Systems entstehen, deutlich geringer würden, wenn Ende-zu-Ende verschlüsselt werde, weil dann die schützenswerte private Kommunikation niemals die Verschlüsselung verlassen würde. Das heißt, jemand, der diese Information in dem Rechenzentrum erlangt, der hätte nur eine verschlüsselte Information. Das Angriffspotenzial wäre nicht da, die Bedrohungslage ist anders, die Gefahrenanalyse ist anders und auch die Verteidigungs- oder Präventionsmaßnahmen wären überhaupt nicht in dem Maße notwendig.

Vors. **Wolfgang Bosbach**: Herr Dr. Vossius, bitte.

SV **Dr. Oliver Vossius**: Frau Wawzyniak, wenn Sie bei namhaften Providern heute einen E-Mail-Account unterhalten, dann bieten die das vielfach schon an. Wenn ich Ihnen von meinem privaten gmx-Account eine E-Mail an Ihr t-online-Account schicke, dann geht die überhaupt nicht über das Netz, weil es zwischen gmx und t-online eine Direktverbindung gibt, ein so genanntes Backbone, da wird die Leitung sozusagen abgekürzt. Diese E-Mail, die ich Ihnen schicke, ist jetzt schon SSL-verschlüsselt von Anfang bis zum Ende.

Vors. **Wolfgang Bosbach**: Herr Dr. von Notz, bitte.

BE **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank, Herr Vorsitzender. Vielen Dank auch an die Experten, die ja sehr kurzfristig hier Stellung nehmen mussten. Ich wollte vorweg schicken, dass ich persönlich wie auch meine Fraktion den ganzen Grundgedanken bei De-Mail als eine gute Sache finde. Auch wenn ich den Aussagen vorhin, dass das Internet ein „Sumpf“ ist, nicht zustimmen würde. Wenn Sie, Herr Dr. Rohleder, mir die Bemerkung erlauben, dafür, dass das alles so unsicher ist, funktioniert es ja ganz gut. Die Branche, die Sie hier vertreten, ist mit diesem unsicheren „Sumpf“ ja groß und mächtig geworden. Trotzdem kann man ja Dinge optimieren. Aber da stellen sich bei mir doch Fragen. Herr Dr. Rohleder, wenn gesagt wird, dass das Kundenverhalten entscheiden soll, ob man das Briefgeheimnis, also die Ende-zu-Ende-Verschlüsselung, bewahren soll, ist es tatsächlich so, dass die Branche glaubt, dass man beim Briefgeheimnis, was ja eine Errungenschaft war und sicher die Grundlage für den Erfolg der Post ist, bei einer Implementierung eines solchen Systems freiwillig auf ein solches Gut verzichten kann, um das den Leuten schmackhaft zu machen? Deswegen sitzen wir hier zusammen. Wissend, dass es bestimmte Sachen gab, die nicht gut gelaufen sind: die

digitale Signatur und auch der nPerso, weil sie irgendwie für die Menschen nicht attraktiv genug waren. Wir sprechen von einer freiwilligen Implementierung. Ergeben Ihre Marktanalysen oder sonst etwas, dass man auf diese Dinge, wie z. B. das Briefgeheimnis verzichten kann, und die Leute sagen: Ja, das mache ich? Das würde mich interessieren, denn die rechtlichen Verpflichtungen und Obliegenheiten, die Zustellungsfiktion und all das, was nachteilig für den Kunden ist, das bekommen sie sozusagen voll geliefert. Den „Sexy-Part“ klammern wir hier aus. Deswegen die Frage: Glauben Sie wirklich, dass das Boot so schwimmt, wenn Sie den entscheidenden Stein herausschlagen? Ich finde, das ist ein Widerspruch und der bestärkt sich auch noch nach den verschiedenen Einlassungen, die ich bisher gehört habe.

Der zweite Punkt ist relativ konkret: Von Herrn Hülsmann würde ich gerne wissen, wie hoch Sie das Risiko eines Drittzugriffs auf De-Mail einschätzen? Wir haben schon aus Notar-Sicht gehört, was für Fälle konstruierbar sind. Überhaupt die Missbrauchsanfälligkeit des Systems aus Ihrer Sicht würde mich sehr interessieren. Vielen Dank!

SV **Dr. Bernhard Rohleder**: Ich habe, glaube ich, nicht von „Sumpf“ gesprochen und würde das auch nicht wagen, aber mit den gewählten Attributen habe ich bei Ihnen vielleicht den Eindruck erweckt. Ich könnte jetzt einfach sagen, ja wir glauben, dass es funktioniert, möchte aber begründend noch hinzufügen, dass wir nicht über die Fragen der Verletzung des Briefgeheimnisses sprechen. Das Brief-, Post- und Fernmeldegeheimnis wird auch jetzt in Telekommunikations- und Internetnetzen nicht verletzt. Es wird speziell beim De-Mail-Verfahren sichergestellt und Herr Welte hat eben das Verfahren beschrieben. Es ist extrem aufwendig sichergestellt, dass das Briefgeheimnis gewahrt bleibt. Wir reden auch nicht darüber, dass jetzt eine E-Mail stunden-, tage- oder auch minutenlang, auch nur sekundenlang irgendwo ungeöffnet auf dem Server liegen würde und dann könnte jeder Mitarbeiter darauf zugreifen. Es geht um Millisekunden, in denen ent- und verschlüsselt wird, im Sinne der Sicherheit. Um nämlich sicherzustellen, dass es keinen Virus gibt, oder eine andere Veränderung dieser E-Mail bei der Übergabe von einem Netz oder von einem Punkt zum anderen. Insofern halten wir das nicht nur für unkritisch, wir halten es auch für dringend notwendig. Ob sich das im Markt durchsetzt, das hängt natürlich auch damit zusammen, wie das Ganze öffentlich kommentiert wird. Ob nämlich aus diesem in Millisekunden stattfindenden Ent- und Verschlüsselungsprozess tatsächlich eine Diskussion gemacht wird, dass die De-Mail das Briefgeheimnis verletzt. Und das tut sie nicht.

SV **Dr. Stefan Brink**: Noch eine ganz kurze Ergänzung. Zum einen zur Frage unterstützt das De-Mail-Gesetz Verschlüsselungen? Ja, das tut es. Im § 7 Abs. 1 wird der akkreditierte Diensteanbieter gerade verpflichtet, entsprechende Informationen über die Verschlüsselung von Nachrichten vorzuhalten. Das geht in die

richtige Richtung und da kann man möglicherweise auch durchaus eine Verpflichtung der Diensteanbieter ablesen, entsprechende Verschlüsselungen zu akzeptieren. Zweiter Gesichtspunkt: Ich glaube, das Apostroph verschiebt sich ein bisschen, wenn man jetzt sagt, De-Mail ist eine Verletzung des Brief- oder Postgeheimnisses. Ich glaube, man muss stärker, und das hatte ich versucht in meiner Stellungnahme deutlich zu machen, darauf abstellen, wie die jetzige Situation aussieht und wie sie nach De-Mail-Gesetz sein wird. Und da sehe ich durchaus einen Fortschritt. Und drittens, das mit dem „Sumpf“ müssen Sie einem Datenschützer verzeihen. Datenschützer sind erst dann zufrieden, wenn gar nicht mehr kommuniziert wird, dann gibt es auch keine personenbezogenen Daten mehr, die verloren gehen können.

Nicht rekonstruierbare Zwischenrufe der Zuhörerschaft

Vors. **Wolfgang Bosbach**: Herr Hülsmann, Sie hatten sich auch gemeldet.

SV **Dipl. Inf. Werner Hülsmann**: Beziehungsweise wurde ich ja auch direkt gefragt. Vielleicht noch eine kleine Ergänzung: Die Information, wie mich Ende-zu-Ende-verschlüsselte Nachrichten erreichen können, ist zwar wirklich der erste Schritt in die richtige Richtung. Aber wenn dem ersten Schritt nicht der zweite folgt, dass der De-Mail-Anbieter verpflichtet wird, einfache Methoden mir anzubieten, dass ich auch auf Knopfdruck dann dem Empfänger eine Ende-zu-Ende verschlüsselte Mail schicken kann, dann nützt dieser erste Schritt nichts. Um auf die Frage, wie hoch ist das Risiko des Drittzugriffs einzugehen. Wenn hier gesagt wird, aus Sicherheitsgründen ist es erforderlich, dass bei dem Provider die E-Mails entschlüsselt, auf Viren und ähnliches gescannt und dann wieder verschlüsselt werden, dann sage ich, ist das System als solches natürlich sehr unzuverlässig, weil dann überhaupt nicht sichergestellt werden kann, dass der Absender, der vorgibt der Absender zu sein und sich angemeldet hat, dann auch tatsächlich diese E-Mail verschickt hat. Weil, wenn sein System korrumpiert ist, dann hilft auch nicht, dass er sich mit Benutzernamen und Passwort anmeldet und ein zweites Sicherheitsmedium, sei es der nPerso, sei es irgendetwas anderes verwendet. Wenn nämlich dort Viren und Würmer auf dem Rechner sind, dann ist keinerlei Sicherheit gegeben, dass der Text, den er glaubt abzuschicken, dass es auch der ist, der beim Provider ankommt. Von daher haben wir hier natürlich schon ein sehr hohes Risiko, was jetzt allerdings nicht diesen kurzen Zeitpunkt der entschlüsselten E-Mails angeht. Da ist natürlich, ich sag mal, wenn wir bei diesen hohen technischen Sicherheitsanforderungen davon ausgehen, dass es sich auf eine Hand voll oder auf zwei Hände voll von Providern konzentrieren wird, wahrscheinlich eher eine Hand voll, dann haben wir natürlich hier fünf Punkte, für die wir ein sehr hohes Angriffsinteresse haben. Wo es Leute gibt, die ein Angriffsinteresse haben und das konzentriert sich auf sehr sehr wenige Punkte, weil es eben nicht Hunderte von De-Mail-Anbietern geben wird. Und wir solche

Singlepoints of Failure oder Singlepoints of Interest haben, auch wenn es fünf oder sechs sind, dann haben wir natürlich ein hohes kriminelles Potential, hohe kriminelle Energie, die darauf zielt, wortgenau anzugreifen. Und Angreifen heißt nicht, dass ich die Wände mit zehn Zentimeter dickem Beton mit einem Stahlbetonbohrer durchbohre, sondern Angreifen heißt, dass ich mir eventuell die richtigen Personen nehme und sie entweder erpressbar mache oder herausfinde, warum sie erpressbar sind und dann dafür sorge, dass dort die entsprechenden Routinen eingebaut werden, so das bestimmte E-Mails automatisch in diesem Millisekundenbereich, wo sie entschlüsselt sind, eben mal kopiert und woanders hin gesendet werden. Das heißt, je weniger solcher Knoten wir haben, um so höher ist natürlich das Risiko, dass die kriminelle Energie auch voll und ganz ausreicht, um dort erfolgreich zu werden.

Vors. **Wolfgang Bosbach**: Direkt dazu, Clemens. Nein.

SV **Prof. Dr. Gerald Spindler**: Ich will es auch nur ganz ganz kurz machen, weil ja auch die juristische Perspektive angesprochen ist. Aber Stichwort Brief- und Fernmeldegeheimnis: Ich glaube, hier muss man zwei Ebenen auseinanderhalten. Erstens, ob dadurch, dass hier mehr oder minder mittelbar vom Staat eine Infrastruktur vorgeschrieben wird, eine staatliche Schutzpflicht im Sinne des Verfassungsrechts besteht, eine Ende-zu-Ende-Verschlüsselung verpflichtend vorzuschreiben?, da würde ich sagen, nein. Hier sind wir noch in dem Bereich des Beurteilungsspielraumes, dass wir es also nicht unbedingt müssen, dass man bis zum Letzten durch verschlüsselt.

Zwischenruf BE Dr. Konstantin von Notz: Weil es freiwillig ist.

SV **Prof. Dr. Gerald Spindler**: Weil der Staat einen gewissen Beurteilungsspielraum genießt, wie weit die Sicherheit in Abwägung mit in unter Umständen konkurrierenden Interessen ausgestaltet wird. Wir sind hier nicht in dem Bereich der Eingriffsverwaltung bzw. nicht im Bereich der Abwehrrechte in dem Sinne. Sondern es wird ein neuer Schutzstandard etabliert, der vorgegeben wird. Das ist der erste Punkt.

Der zweite Punkt ist der, sie haben unter Umständen konkurrierende Schutzinteressen. Das greift allerdings weit über das hinaus, was wir jetzt hier diskutieren und das wäre das, was ich auch vorhin gemeint hatte mit einem grundlegenden Konzept, weil nämlich unter Umständen auch IT-Sicherheitsinteressen insgesamt – Stichwort kritische Infrastrukturen u. ä. – berührt sind. Aber das geht viel, viel weiter, etwa in die Richtung von dem, was Herr Hülsmann angesprochen hatte, mit Knoten usw., usf., ob Viren ermöglicht werden, Bot-Netze usw. Das bedingt unter Umständen manchmal schon, dass man die E-Mails auch beim Provider analysiert. Das können also durchaus konkurrierende Interessen sein. Der dritte Punkt ist die

Frage: Was ist denn das Brief- und Fernmeldegeheimnis? Auch wenn Sie sich die neueren Entscheidungen, gerade des Bundesverfassungsgerichts, dazu näher anschauen, werden Sie sehen, dass das Bundesverfassungsgericht zu Recht langsam aber sicher auch spezifisch auf die Kommunikationsarten abstellt, das heißt, dieses alte Briefgeheimnis wird nicht unbedingt eins zu eins übertragen auf moderne Kommunikationsformen. Also deswegen hier zu sagen, es ist ein verfassungsrechtliches Muss, dass End-zu-End-verschlüsselt wird, das würde ich persönlich nicht unterschreiben wollen.

Vors. **Wolfgang Bosbach:** Ja klar.

BE **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank. Wenn es jetzt verpflichtend wäre, nicht freiwillig, und die Post von Behörden, die sensible Behördenpost, die ich zu Hause führe, die würde über diese De-Mail laufen, dann würden Sie es auch nicht als Problem sehen, dass es keine Ende-zu-Ende-Verschlüsselung ist? Also mit der Freiwilligkeit, das leuchtet mir ein. Dass man sagt, solange die Menschen die Möglichkeiten haben, dass die Dinge in einem Briefumschlag versiegelt mit dem vollen Schutz kommen, solange ist das ein Free Choice irgendwie. Wenn das jetzt verpflichtend wäre, dann würden Sie sagen, sagt der Gesetzgeber, ach Gott…

Vors. **Wolfgang Bosbach**: Also z. B. Abgabe elektronischer Neuerkennung, also nur noch elektronisch.

BE **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Genau.

Vors. **Wolfgang Bosbach**: Nicht mehr im Briefkasten Finanzamt.

BE **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Richtig, verpflichtend. Jeder muss die E-Mail machen und dann kriegst du es halt so und dann sagt der Gesetzgeber oder bzw. sagt dann das Bundesverfassungsgericht, ja Gott, ist halt elektronisch, da wollen wir jetzt mal Fünf gerade sein lassen, ist halt kompliziert, das irgendwie umzusetzen.

SV **Prof. Dr. Gerald Spindler**: Also da würde ich keine Prognose wagen wollen, wie das Bundesverfassungsgericht entscheidet, wenn es, wie gesagt, unter Umständen konkurrierende Interessen gibt, die dann ins Feld geführt werden können. Und die könnte es unter Umständen geben. Ich würde hier insofern einen Weg mitgehen wollen, indem man differenziert. Wenn es wirklich absolut hochsensible Daten sind – wir reden jetzt über § 3, Abs. 9 BDSG – also etwa um medizinische Daten etc., da spricht natürlich viel dafür, dass man eine End-zu-End Verschlüsselung hat. Das wäre unter Umständen eine Möglichkeit, da zu differenzieren.

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

SV **Michael Bobrowski**: Ich würde gerne noch einen Hinweis geben auf das, was in der Begründung zum Gesetzentwurf steht. Ich hatte vorhin in der Einleitung auch schon einmal ganz kurz darauf hingewiesen. Ich möchte es nochmal zitieren, was für uns dann auch den Maßstab darstellt bei der Bewertung, ob Ende-zu-Ende-Verschlüsselung sinnvoll und notwendig ist oder nicht. In der Begründung zu den Regelungen § 5 Abs. 1 des Gesetzentwurfes, das ist Postfach- und Versanddienst, heißt es: Die Vertrauenswürdigkeit des Post- und Versanddienstes beruht darauf – und jetzt zitiere ich wörtlich – „dass die Nachricht vom Diensteanbieter verschlüsselt übermittelt wird, so dass sie auf dem Transportweg weder ausgespäht noch spurenlos verändert werden kann.“ Und wenn ich als Laie, als Computer-Laie, das richtig verstehe, den Unterschied zwischen Transport und Inhalt der Verschlüsselung, kann das, was hier steht – „spurenlos nicht verändert werden kann“ –, nur durch eine Inhalteverschlüsselung gewährleistet werden. Herr Welte, vielleicht können Sie mir da noch beipflichten. So, das war das Ende des Zitates, das will ich der Ordnung halber noch einmal sagen. Das ist für uns der Maßstab. Es mag sein, Herr Prof. Spindler, da kann ich gar nicht wechseln, es mag sein, dass das verfassungsrechtlich eben nicht erforderlich ist, dass der Staat hier sozusagen im jetzigen Stadium eine Verpflichtung erhält. Aber ich messe diese Frage tatsächlich an dem, was die Bundesregierung in ihrem Gesetzentwurf an Hürde, an Niveau setzt, und das ist relativ hoch, meines Erachtens. Und daraus wächst für uns dann doch die Erwartung, die Forderung, eine Ende-zu-Ende-Verschlüsselung definitiv verbindlich im System vorzugeben. Vielen Dank.

Vors. **Wolfgang Bosbach**: Clemens Binninger.

BE **Clemens Binninger** (CDU/CSU): Ich hatte schon Sorge, Sie stellen sich jetzt gegenseitig Fragen und wollte noch darauf hinweisen, dass wir noch da sind. Zu dem letzten Punkt hätte ich einfach die Bitte, dass die Bundesregierung vielleicht dazu kurz Stellung nimmt, um nochmal auf das hohe Sicherheitsniveau, auch der Transportverschlüsselung, abhebt – Stichwort: Veränderung auf dem Transportwege. Ich habe drei Fragen an Herrn Hülsmann, Herrn Rohleder und an Herrn Prof. Spindler. Einfach nur, dass wir nicht mit unterschiedlichen, ganz unterschiedlichen Meinungen, auseinandergehen, davon abgesehen, ich teile die Einschätzung von Herrn Rohleder völlig, dass sich Ende-zu-Ende-Verschlüsselung im gesamten E-Mail-Markt nicht durchgesetzt hat. Natürlich gibt es Firmen, natürlich gibt es Einzelanwender, die das machen, aber wir reden hier von Massenanwendungen. Da ist es nicht a jour das zu machen, da gibt es, glaube ich, keine Zweifel. Die Frage an Sie wäre, weil Sie gesagt haben, Transportverschlüsselungen, also die 99,9 Prozent Sicherheit als Standard, Ende-zu-Ende, die 100 Prozent, optional. Was hilft mir die

Option, wenn der Provider nicht verpflichtet ist. Würden Sie das, was wir im § 7 – wirklich nur als Bewertung von Ihnen – Abs. 1 nicht verlangen vom Provider, würden Sie das nicht doch als Verpflichtung sehen, wo der Nutzer sagen kann: Und ich bestehe darauf, ich will Verschlüsselung, ich habe diese Entscheidung gefällt und da muss der Provider sich auch an meinen Bedürfnissen orientieren. Die Beschreibung, die wir hier im § 7 Abs. 1 genommen haben, beruht nicht darauf eine Verpflichtung abzuleiten, dass, wenn der Nutzer eine Ende-zu-Ende-Verschlüsselung will, er sie vom Provider auch bekommt. Zweite Frage an den Herrn Rohleder geht in eine ganz andere Richtung, war heute Nachmittag noch kein Thema. Wir wurden auch im Laufe der Gesetzgebungsberatungen darauf hingewiesen, dass wir eine Chance finden sollten, mittelständische Unternehmen am weiteren Prozess auch teilhaben zu lassen. Wir haben daraufhin im § 22 vorgesehen, dass die Fortentwicklung von Richtlinien nicht nur zwischen BSI und zertifizierten Providern, die es in Zukunft geben wird, erfolgen soll, sondern auch unter Beteiligung von Verbänden. Sie, als jemand, der einen großen Verband vertritt, deshalb die Frage: Halten Sie das für ausreichend, um eben auch kleineren mittelständischen Unternehmen hier ausreichend Mitsprachemöglichkeiten einzuräumen? Und die dritte Frage geht noch einmal an Herrn Prof. Spindler. Ich könnte es auch, aber wir wollen ja heute die Sachverständigen hören. Ich habe gesehen, dass Sie vorher bei Herrn Bobrowski bei diesem Thema Domain-Name doch, wie wir ja auch gehört haben, dezidiert anderer Meinung sind. Da wäre ich nochmal dankbar für einen Hinweis, weshalb eben aus den verschiedensten Gründen, die wir auch alle abgewogen haben, dieser einheitliche Domain-Name nicht erforderlich ist.

Vors. **Wolfgang Bosbach**: Herr Hülsmann.

SV **Dipl. Inf. Werner Hülsmann**: Also aus meiner Sicht ergibt sich aus § 7 Abs. 1 in keinster Weise, dass der De-Mail-Anbieter verpflichtet ist, mir die Möglichkeit, also die technischen Möglichkeiten, die entsprechenden Tools, zur Verfügung zu stellen, dass ich auf einfache Art und Weise Ende-zu-Ende-verschlüsseln kann. § 7 Abs. 1 verpflichtet den Dienstanbieter nur, dass er eine solche Ende-zu-Ende-verschlüsselte E-Mail auch tatsächlich durch das De-Mail-Postfach, also durch den Transportweg, hindurch zu leiten hat. Und das die Ende-zu-Ende-Verschlüsselung keine so weite Verbreitung hat, liegt ja daran, dass ich momentan noch einen gewissen Aufwand betreiben muss, um Ende-zu-Ende zu verschlüsseln. Deswegen ist ja die Forderung, De-Mail-Anbieter zu verpflichten, dass ich mit – wie ich es vorhin sagte – mit wirklich vier Mausklicks mein De-Mail-Postfach so eingerichtet habe, dass ich a) Ende-zu-Ende verschlüsselte E-Mails empfangen kann und b) auch versenden kann und dann tatsächlich dann bei jeder einzelnen E-Mail, eventuell sogar bei den Empfängern gar nichts mehr machen kann, machen muss, sondern so, wie ich es jetzt bei meinem Thunderbird mit den entsprechenden Plug-ins mache. Bestimmte Empfänger, da brauche ich überhaupt nichts machen, die gehen automatisch verschlüsselt raus. Der

Empfänger kriegt es verschlüsselt und umgekehrt. Da müssen Sie sich keine Gedanken machen, dass kann – bitte sich jetzt niemanden auf den Schlips getreten fühlen – sogar ein 65jähriger Rechtsanwalt, der seinen Rechner nur

Zwischenruf Abg. Clemens Binninger (Berichterstatter): oder Notar…

SV **Dipl. Inf. Werner Hülsmann**: Deswegen die Erweiterung – der seinen Rechner im Prinzip als elektronische Schreibmaschine und als Fernschreiber in Anführungszeichen verwendet. Selbst die Leute schaffen das dann ganz automatisiert zu verschlüsseln. Aber dafür ist es einfach erforderlich, dass der Provider, wenn er seinen De-Mail-Dienst anbietet, z. B. wie es hier ja auch heißt: Web-basiert, dass er da dann auch Web-basiert die entsprechenden Tools-Applikationen anbietet, dass der Nutzer es kann. Das ist das Wichtige und dann kämen wir auch zu einer Verbreitung von einer Ende-zu-Ende-verschlüsselten E-Mail von bis zu 50 Prozent. Ich würde sagen, die transportgesicherte E-Mail, also bei 99,9 Prozent Sicherheit, halte ich für eine hohe Prozentzahl, weil die würde ich höher sehen. 99,9 Prozent Sicherheit und noch ein kleines bisschen mehr haben wir vielleicht bei der Ende-zu-Ende verschlüsselten Mail. Ich würde da eher von 99 Prozent Sicherheit reden, weil wir ja, wie gesagt, das Thema haben, wie geht der User mit seinem Rechner um. Was ist da drauf? Aber solange es nicht angeboten wird, dass wirklich der De-Mail-Anbieter verpflichtet ist, hey, wenn du diese Option nutzen willst, von mir aus für einen Euro Aufpreis im Monat, dann brauchst du da nur so und so machen, kleine Anleitung dazu, dann würden wir auch die Möglichkeit haben, dass der mittelständische Betrieb seine Angebote, die er ja, was weiß ich, beim Bundeswirtschaftsministerium einreicht, dass er die dann Ende-zu-Ende-verschlüsselt einreicht und nicht eventuelle die Gefahr besteht, dass sie irgendwo irgendwann mal mitgelesen werden und irgendwelche anderen Leute billigere Angebote einreichen.

Vors. **Wolfgang Bosbach**: Vielen Dank. Herr Dr. Rohleder.

SV **Dr. Bernhard Rohleder**: Auch wenn ich dazu nicht gefragt wurde, ich halte die Diskussion für eine Phantomdiskussion, ob das verpflichtend gemacht werden muss. Die Anbieter sind ja nicht doof. Die wissen, was ihre Kunden wollen, und ich gehe fest davon aus, dass es jeder Anbieter ohnehin anbieten wird. Und ob das jetzt vier Klicks sind oder drei Klicks, bei dem einen mehr oder weniger kompliziert, das wird man dann einfach sehen. Und es wird sich derjenige bei dem Kunden durchsetzen, der das komfortabelste, einfachste und sicherste Angebot hat. Und wem es gelingt, Komfort und Sicherheit optimal miteinander zu verbinden und dafür auch noch einen guten Preis anzubieten. Ich glaube, an der Stelle wird es eher realiter kein Problem geben. Die an mich gerichtete Frage, ob das Verfahren, ob ich das für ausreichend erachte. Ich halte es für klug, die Anwender mit an den Tisch zu holen, also

diejenigen, die von Änderungen dann letztlich als Kunden betroffen sein werden und wie viele Verbände das sein müssen, ob zwei oder drei, halte ich an der Stelle für nachrangig. Ich halte für wichtig, dass es dann Vertreter wirklich auch des Mittelstandes sind und die einschlägig legitimiert und kompetent für ihre Kunden sprechen können.

Vors. **Wolfgang Bosbach**: Herr Prof. Spindler.

SV **Prof. Dr. Gerald Spindler**: Nochmal zum Stichwort Portierbarkeit: Da ging es um Fragen der Kosten. Ich hatte das Ganze jetzt eigentlich so verstanden, dass es im Prinzip darum geht, möglichst ein verlässliches Signal für Empfänger zu schaffen. Ist das jetzt ein Dienst, der sicher ist, oder ist er nicht sicher. Das ist für mich erst einmal der Ausgangspunkt. Und das ist ein Ausgangspunkt, den wir generell kennen aus dem Bereich des Produktsicherheitsrechts. Egal, wo wir sind, ob das nun irgendwelche Autos sind, oder ob das Fahrstühle sind, oder was auch immer, es geht um die Produktsicherheit. Dann kommt die nächste Frage: Wie kann das gemacht werden? Im Prinzip kann ich eine E-Mail relativ einfach auch mit einem kleinen Flag ausgestalten, indem signalisiert wird, die E-Mail ist technisch sicher. Wo ich das nun unterbringe, ist unerheblich. Und jedes Programm kann das einfach nach diesem Flag unterscheiden. Deswegen brauche ich keine einheitliche Domain und muss umständlich hin- und her sortieren, sondern ich bekomme halt eine Mail, auf der dieser Flag sitzt, der sofort automatisch vom E-Mail-Programm erkannt wird, genau so, wie Sie es gerade eben mit dem Plug-in so schön beschrieben haben. Und die E-Mail ist in dem richtigen Postfach drin. Deswegen verstehe ich ehrlich gesagt nicht, warum ein einheitlicher Domain-Name nun unbedingt erforderlich sein soll. Ich sehe ehrlich gesagt die Notwendigkeit dafür, im Sinne eines Muss, nicht ein. Zudem besteht ein Beurteilungsspielraum, konkurrierende Interessen einzubeziehen, etwa geschützte Markennamen oder Namensinteressen, die auch durchaus verfassungsrechtlich geschützt sind. Man kann es genauso gut ohne einheitlichen Domain-Namen lösen, wenn die technische Sicherheit, darum geht es ja bloß, signalisiert wird.

Vors. **Wolfgang Bosbach**: Herr Dr. Vossius.

SV **Dr. Oliver Vossius**: Herr Binninger, zu den Domain-Namen: Minimum scheint mir zu sein, dass in einer De-Mail die Toplevel-Domain de-mail.de drin ist. Das hat zwei Gründe. Zum einen gehört diese Toplevel-Domain der Aufsichtsbehörde, die kann damit auch ran und kann notfalls einen Provider von der Teilnahme ausschließen - Stichwort Insolvenz. Zum Zweiten übt diese Toplevel-Domain auf die Nutzer eine Warnfunktion aus. Wenn ich eine E-Mail von andreameier@generali.de bekomme, solch eine Andrea Meier kenne ich nicht, ist wahrscheinlich Werbemüll, klicke ich weg. Es hätte aber auch die Kündigung des Versicherungsverhältnisses drin sein können oder die Änderungen der Vertragsbedingungen. Wenn ich weiß,

andreameier@generali.de-mail.de, das könnte was Wichtiges sein, darauf, glaube ich, sollten achten.

Nicht rekonstruierbare Zwischenrufe der Zuhörerschaft.

Vors. **Wolfgang Bosbach**: Jetzt werde ich aber langsam unruhig.

Nicht rekonstruierbare Zwischenrufe der Zuhörerschaft.

Vors. **Wolfgang Bosbach**: Ich gucke auf den Inhalt, so unterscheiden sich die Leute. Herr Welte, Sie hatten sich auch gemeldet. Worauf gucken Sie?

SV **Harald Welte**: Ich möchte zu zwei Sachen noch ergänzende Hinweise loswerden. Zum einen eben auch nochmal die Frage der Portierbarkeit und dann die Frage Domain-Namen. Ich stimme dem Herrn Vossius ausdrücklich zu, dass eine De-Mail-Adresse als solches sofort eindeutig erkennbar und identifizierbar sein muss. Wenn wir den Namensraum von der existierenden E-Mail-Kommunikation überladen, wie man das technisch betreibt, und sozusagen im gleichen Namensraum sowohl die De-Mail als auch E-Mail-Adressen anbieten, das ist eine Verwechslung sondergleichen. Niemand weiß mehr, was ist das eine, was ist das andere. Und wenn Sie dann, wie vorgeschlagen wurde, in der gleichen Software einfach nur ein Häkchen setzen, ist es eine De-Mail oder eine herkömmliche E-Mail, so etwas wurde ja gerade angeraten, wenn so etwas dann passiert, dann haben Sie wieder das Problem von falschen Absenderadressen, weil, wenn keine De-Mail, sondern eine reguläre E-Mail reinkommt, in der vom Namen her beispielsweise De-Mail drinsteht, dann können Sie ja diese Unterscheidung anhand dessen gar nicht mehr vornehmen.

BE **Clemens Binninger** (CDU/CSU): Wir reden hier ja über geschlossene Systeme. Und Sie können keine E-Mail, egal wie sie heißt, deshalb hat der Name auch nicht die Bedeutung, wie immer suggeriert wird, nicht versehentlich an ein De-Mail-Postfach eines anderen zustellen. Das geht einfach nicht.

SV **Harald Welte**: Nein, das können Sie nicht.

BE **Clemens Binninger** (CDU/CSU): Dann gibt es an dieser Stelle auch keine Verwechslungsgefahr.

SV **Harald Welte**: Sie drucken die De-Mail aus. Jemand liest die Adresse.

Nicht rekonstruierbare Zwischenrufe der Zuhörerschaft

SV **Harald Welte**: Nein.

Vors. **Wolfgang Bosbach**: Das ist auch ein schöner Fall.

SV **Harald Welte**: Ist doch egal, was Sie nehmen. Sie haben eine Adresse, die aussieht wie eine E-Mail-Adresse, jedermann sieht zuerst diesen Klammeraffen darin. Sie sehen, aha, das ist eine E-Mail-Adresse. Ich möchte da eine Nachricht hinschicken. Sie wissen aber nicht nur anhand dessen, dass Sie die Adresse sehen, ist es De-Mail oder ist es herkömmliche E-Mail. Ich sehe da eine ganz erhebliche Verwechslungsgefahr im Kommunikationsverhalten der Anwender. Ich sehe nicht, warum man die nicht eindeutig kennzeichnen kann.

Vors. **Wolfgang Bosbach**: So, Clemens? Nein! Resignation für das Protokoll Herr Reichenbach tut mir leid, Ladys first, Frau Wawzyniak.

Abg. **Halina Wawzyniak** (DIE LINKE.): Ich muss jetzt leider nochmal an der von Herrn Rohleder als Phantom-Diskussion bezeichneten Debatte weitermachen. Das liegt aber daran, dass Herr Spindler mich provoziert hat. Es tut mir leid. Sie haben vorhin auf die Frage von Herrn von Notz gesagt, Herr Spindler, der Staat hat einen Abwägungsspielraum bei der Etablierung neuer Schutzstandards, und haben angedeutet, es könnte passieren, dass bei dem Brief-, Post- und Fernmeldegeheimnis bei unterschiedlichem Stand der technischen Entwicklung auch unterschiedliche Standards akzeptiert werden und haben dann immer von konkurrierenden Interessen gesprochen. Jetzt frage ich mich, auch ich will jetzt mal ein bisschen provozieren, bin im Osten geboren, ich weiß, dass da Post- und Fernmeldegeheimnis nichts wert war. Da ist quasi alles nachgeguckt worden und habe jetzt die Hoffnung, dass in diesem Rechtstaat dieses Post- und Fernmeldegeheimnis sehr hoch gewichtet ist. Die einzigen konkurrierenden Interessen, die mir einfallen würden, warum das Post- und Fernmeldegeheimnis infrage gestellt werden könnte, wären Strafverfolgung und Sicherheitsinteressen. Dann würde ich doch aber sagen, das kann doch aber nicht bei einer Standardentwicklung ein entscheidender Punkt sein. Welche konkurrierenden Interessen sollten hier in Rede stehen, die dieses Post- und Fernmeldegeheimnis – ich sag es jetzt einmal – relativieren? Das ist mir nicht verständlich.

Vors. **Wolfgang Bosbach**: Das ist dann nur ein Missverständnis.

SV **Prof. Dr. Gerald Spindler**: Das Zwinkern deute ich dann schon mal darauf, dass Sie sagen kurzfassen. An sich gehört diese Frage schon fast eher in die Enquete-Kommission hinein, weil sie den ganzen Sektor der IT-Sicherheit berührt. Gestatten Sie mir drei Sätzen zum Ausholen. Das Problem besteht darin, dass wir oftmals Botnetze haben, die sich auf privaten PCs etc. etablieren, oftmals eben durch E-Mail, egal, wie die mit irgendwelchen Anhängen versehen wird, wo Viren, Trojaner,

Sonstiges drauf sitzen. Und die Frage ist eben die, wo setzt man vernünftigerweise an, um möglichst so etwas auszuschalten. Ich will nicht sagen, dass man das an der Stelle machen muss. Ich sage nur, es ist ein Gedankenszenario, dass man unter Umständen bei Providern anknüpft, die dann die digitalen Inhalte an den Endnutzer weitertransportieren, um möglichst so etwas schon vorher auszuschalten. Das Vorbild haben Sie dafür in der jetzt schon existierenden Welt. Wenn Sie in die entsprechenden juristischen Ausarbeitungen zum Vertragsverhältnis zwischen Providern und Kunde schauen, dann sollte eigentlich ein ordentlicher Provider für Sicherheit sorgen, durchaus auch beim Eingang von entsprechenden E-Mails. Und das ist auch etwas, was Sie in den meisten Allgemeinen Geschäftsbedingungen vorfinden. Es ist etwas, was meine Zunft generell vertritt, durchaus als Schutzpflicht sogar gegenüber dem Kunden, aber wohlgemerkt vertraglich. Natürlich muss der Datenschutz gewahrt bleiben, so dass eine vorherige Einwilligung erforderlich ist. Das soll hier nicht ein Schutz- und Überwachungsstaat oder irgendwie was werden. Die Frage ist eben nur, wo setzen wir unter Umständen an welchen Stellen an, um diese Probleme zu beheben, die dann wiederum auch Bürger, Verbraucher, Nutzer überall treffen. Aber das ist Teil eben dieses Gesamtkonzeptes, was ich vorhin gemeint hatte. Herr Schallbruch, Sie wissen ja, da hatten wir ja auch diverse Diskussionen schon, mit BSI usw. darüber. Wie man sowas machen könnte und wo sozusagen da Schnittstellen sind. Ich hoffe, das ist jetzt klar. Also nochmals, ich plädiere hier keineswegs für irgendwelche überwachungsstaatlichen Maßnahmen oder sonst irgendetwas, sondern es geht nur um das Problem IT-Sicherheit, auch im Sinne vom Schutz kritischer Infrastrukturen etc.

Vors. **Wolfgang Bosbach**: Herr Reichenbach.

BE **Gerold Reichenbach** (SPD): Ich glaube, ein Problem ist, dass wir immer versuchen, Kategorien aus der analogen Welt in die digitale zu übertragen. Deswegen klappt das auch nicht. Klar, meine Briefe zu Hause mit den vielen Postwurfsendungen und der wichtigen Mitteilung der Versicherung sortiere ich nicht nur anhand der Adresse, sondern anhand des Gesamterscheinungsbildes aus. Das ist bei einer Extension einer E-Mail einfach so nicht mehr machbar, die muss ich aufmachen, um zu sehen, was da drin ist.

Nicht rekonstruierbare Zwischenrufe der Zuhörerschaft

BE **Gerold Reichenbach** (SPD): Es ist nun glücklicherweise so, dass Werbung heute noch relativ eindeutig als solche zu identifizieren ist, jedenfalls in den meisten Fällen. Ich habe zwei Fragen. Für mich war die Frage der einheitlichen Kennung eigentlich keine Sicherheitsfrage, sondern eher eine des Wettbewerbs. Und dann erinnere ich mich an die Zeiten, als man beim Anbieter im Telekommunikationsbereich noch die Telefonnummer wechseln wollte, wenn man den Provider

gewechselt hat und dann war das schon einmal eine Frage, wenn man sich über die Dienstleistungen des Providers geärgert hat, nehme ich jetzt in Kauf, alle meine Bekannten, trallala und sonst was viel mehr Ärger mit der neuen Telefonnummer. Das scheint mir, das Entscheidende zu sein. Jetzt sage ich auch mal ganz offen in Richtung Herrn Dr. Rohleder: Mein Glaube in die Regulierung von Preis-Leistung-Angebot durch den Markt verliere ich jede Woche einmal an der Tankstelle, aber das vielleicht nur mal am Rande. Deswegen schon nochmal die Frage: Erstens an Herrn Hülsmann, Herrn Bobrowski und vielleicht auch an Sie, Herr Dr. Rohleder, wie hoch wäre denn der Aufwand? Weil, wenn ich tatsächlich eine einheitliche Adresse machen würde, die was weiß ich, vorne lautet, Gerold Reichenbach Punkt, dann hinten noch eine Kennziffer, weil es vielleicht ein paar Gerold Reichenbachs, die auch so einen Dienst haben, und am Ende nur De-Mail.de. Das würde, wie bei der Telefonnummer heute bedeuten, ich kann dann mit meiner Telefonnummer wechseln von A nach B. Und wenn das mit geringem Aufwand zu machen ist, warum macht man das nicht?

Zweite Frage: Wie hoch wäre der Aufwand, wenn ich solch ein Plug-in wirklich installieren würde, so dass ich bei einfachem Klick bei jeder De-Mail dann auch eine verschlüsselte Variante vornehmen kann? Das ist die eine Frage und die zweite Frage, die geht eher so in das, was Sie sagten, Eingriffsverwaltung.

Vors. **Wolfgang Bosbach**: An wen?

BE **Gerold Reichenbach** (SPD): Ja, an die Rechtsgelehrten, also „to whom it may concern“, vielleicht der Notarverein, an Herrn Dr. Spindler, vielleicht aber auch an Herrn Dr. Stefan Brink. Das ist die Frage, De-Mail-Dienste werden behandelt nach dem TKG, das heißt, der Zugriff von Strafverfolgungsbehörden, Diensten und und und richtet sich nach dem TKG, und wenn ich den § 113 richtig gelesen habe, kann ich ohne richterliche Anordnung dann die Herausgabe von Passwort Anschluss nehmen, das heißt, damit bin ich im Postfach drin. Das wäre eine wesentlich niedrigere Hürde zum Eingriff, im Vergleich zum normalen Postbereich und meine Frage ist: Wie beurteilen Sie die Tatsache, dass hier eine Verschiebung zu Lasten des Eingriffsschutzes des Betroffenen stattfindet oder sehen Sie das anders?

Vors. **Wolfgang Bosbach**: Herr Bobrowski. Herr Kollege Reichenbach orientiert sich nicht am Gesamteindruck der Tankstelle, sondern am Preis. Was sagen Sie dazu?

SV **Michael Bobrowski**: Dann könnte ich vielleicht damit beginnen, dass ich sage, ich mache ähnliche Erfahrungen an der Tankstelle, obwohl ich relativ wenig fahre, aber hin und wieder kriegt man dann doch mal eine Chance und dann, wenn man rechtzeitig am Ort ist, kann man da auch vielleicht ein bisschen beim Tanken gegenüber dem Wettbewerber sparen, bei dem einen oder andern. Aber ich will hier keine

Werbung machen für irgendwelche Tank- oder Benzinfirmen. Wir sprechen ja über die De-Mail. Herr Reichenbach, ich will die Frage indirekt beantworten. Ich denke mal, dass es gar nicht so entscheidend ist, wer jetzt welchen Aufwand auf der Provider-Seite oder auf der Nutzerseite hat. Denn die ganze Diskussion über die einheitliche und nach unserer Diktion auch providerfreie Domain-Kennzeichnung von De-Mail orientiert sich doch an ganz anderen Aspekten. Da geht es doch nicht darum, ob es für den Nutzer jetzt teurer oder nicht teurer wird, sondern es ist einfach eine Frage des Marktstatuts bestimmter Unternehmen, der Marktdurchsetzung bestimmter Produkte. Und wir hatten es ja vor einiger Zeit auch deutlich aus einem bestimmten Hause gehört, es geht darum, ein bestimmtes Produkt auch eindeutig am Markt zu platzieren und zu kennzeichnen. Und dann sage ich, und wiederhole mich da, dass das De-Mail-Gesetz, so wie ich es verstehe, auch von der Intention und der zentralen Zielsetzung her, dazu dient, eine sichere Infrastruktur für sichere oder sicherere elektronische Kommunikation zu schaffen, das heißt, der Staat stellt sich hier auf und sagt, ich werde mal Bedingungen formulieren, dass ihr, die Wirtschaft, daraufhin, auf diesem Fundament, bestimmte Dienstleistungen anbieten könnt.

Zwischenruf von Abg. Dr. Dieter Wiefelspütz: Das ist ja wie Straßen mit Leitplanken bauen.

SV **Michael Bobrowski**: Zum Beispiel. Vielen Dank für diese Formulierungshilfe, Herr Dr. Wiefelspütz. Aus dieser Zielsetzung ist für mich völlig klar, dass die De-Mail-Adresse, die das – ich wiederhole mich – physische Postfach und sozusagen die Postkommunikation elektronisch abbilden soll, dass die dem Bürger, dem Verbraucher, oder einem Unternehmen gehört und nicht demjenigen, der diesen Dienst anbietet. Der kann sein Produkt auch anderweitig noch bewerben und es schön bunt machen und so im Wettbewerb bestehen. Aber – ich sage mal – das, was uns ganz wichtig ist, ist, dass ich diese Adresse auch notfalls im Providerwechsel einfach transportieren kann zum nächsten. Ich kann nicht mit einer Provideradresse – ich nenne jetzt mal einfach, ohne jedoch Werbung machen zu wollen – t-online.De-Mail.de zu 1&1 gehen oder zur ePost und sagen, jetzt möchte ich gern diese Adresse bei euch platzieren. Die werden sagen, nein, bei uns kriegst du eine neue. Das machen wir nicht, wir machen doch nicht Reklame oder Werbung für das Konkurrenzunternehmen. Das würde ich auch verstehen. Und damit dieses nicht passiert, sage ich, und das ist keine Frage des Aufwandes, der Aufwand ist im Wesentlichen niedriger beim Nutzer, davon bin ich überzeugt. Wenn wir eine einheitliche Kennzeichnung ohne Providerbezeichnung haben, ist der Nutzer wesentlich besser dran. Das gilt für den privaten Nutzer, würde ich mal behaupten, wie insbesondere auch für die Wirtschaft, die noch ganz andere Kosten bei einem entsprechenden Providerwechsel hat. Das wäre meine Antwort auf die Frage, wie

hoch denn der Aufwand ist. Beziffern kann ich ihn nach Cent und Euro derzeit nicht, weil es keine Erfahrungen damit gibt.

Vors. **Wolfgang Bosbach**: Herr Hülsmann.

SV **Dipl. Inf. Werner Hülsmann**: Ich halte den Aufwand für E-Mail-Adressen, wie ich es ja auch in meiner Stellungnahme vorgeschlagen habe, Vorname.Nachname., was weiß ich, vier- oder fünfstellige zufällige Ziffer @De-Mail.de für im Vergleich zu den anderen Sicherheitsanforderungen und ähnlichen Anforderungen an die technischen Systeme für sehr gering. Wir haben erprobte Verfahren über die Netzagentur, Rufnummern zu verwalten. Wir haben erprobte Verfahren im Sinne der Portierung, weil ich auch bei den Mobilnummern inzwischen nicht mehr an der 0172 erkennen kann, dass es Vodafone ist oder an der 0171 T-Mobile oder naja gut, ich muss jetzt nicht alle nennen. Es sollte jetzt keine Werbung gewesen sein. Da könnte ich es genauso sagen, dass, wenn ein Werner Hülsmann eine De-Mail-Adresse haben will, dann gibt es eine automatische Anfrage an die Bundesnetzagentur, also vollautomatisiert wird eine Zufallsziffer erzeugt. Die wird bei der Bundesnetzagentur in ein entsprechendes Verzeichnis eingetragen und ich bekomme dann Werner. Hülsmann, was weiß ich, 4708@De-Mail.de und wenn dann irgendjemand, der am De-Mail-System angeschlossen ist, an Werner.Hülsmann.4708@De-Mail.de eine Nachricht schickt, dann wird kurz geguckt, welcher Werner Hülsmann ist das, bei welchem Provider ist dieser Werner Hülsmann mit dieser Kennziffer und zack bum, wird dann diese E-Mail an den richtigen Provider zugestellt. Das heißt der Aufwand ist auf alle Fälle händelbar. Und wenn man jetzt Aufwände abwägt, weil wir ja nicht nur die Aufwände bei den Providern sehen dürfen, sondern, wie schon gesagt, die Aufwände beim Verbraucher werden immens, wenn ich bei einem Wechsel des Providers auch meine De-Mail-Adresse wechseln müsste. Wer Wettbewerb will, wer Wettbewerb unter den De-Mail-Providern haben will, der kann nicht wirklich einen Provider-Namen in der De-Mail-Adresse akzeptieren, weil dann haben wir keinen Wettbewerb. Die ersten Drei, die auf dem Markt sind, die haben die ersten so und so viel Hunderttausend oder wie viel auch immer Kunden, und nur weil der andere ein bisschen billiger ist oder ach, der andere bietet die Verschlüsselung standardmäßig im Preis mit an, da wechsel ich doch nicht meine komplette Kommunikationsstruktur. Von daher brauchen wir auf alle Fälle providerfreie De-Mail-Adressen. Der Aufwand für das Plug-in für eine Ende-zu-Ende-Verschlüsselung, wenn ich – ich sag mal – von 500.000 De-Mail-Kunden nach einem gewissen Anfangszeitraum ausgehe, ist das pro Kunde im Cent-Bereich, so dass selbst, wenn man das auf den Kundenpreis draufschlägt, das nicht wirklich irgendwie relevant sein wird. Die eine Abgeordnete ist leider schon raus, bezüglich der anderen Interessen. Ich hatte interessanterweise, kurz nachdem auf der Webseite des Bundestages, also des Innenausschusses, meine Stellungnahme veröffentlicht wurde, eine E-Mail erhalten, wo ein Firmeninhaber aussagte, dass er an dem Vorgängersystem namens „Julia“ gear-

beitet habe und in diesem Vorgängersystem namens „Julia“ natürlich eine Schnittstelle enthalten sei, damit leicht, während dieser millisekundenhaften Entschlüsselung bei dem Provider die E-Mails und dann den entsprechenden Strafverfolgungs- und Sicherheitsbehörden übermittelt werden können. Aufgrund der Kürze der Zeit – wie gesagt – die E-Mail ist am Samstag oder am Sonntag eingegangen, konnte ich das nicht verifizieren, aber nur so viel zu weiteren Interessen.

Vors. **Wolfgang Bosbach**: Deshalb sollte man das auch nicht gleich für bare Münze nehmen. Herr Dr. Rohleder.

SV **Dr. Bernhard Rohleder**: Zum Aufwand: Es gibt natürlich noch einen ganz anderen Aufwand, der dadurch entsteht, dass man das System bedienen muss. Die Mail muss verschlüsselt werden und sie muss vor allem beim Empfänger auch wieder entschlüsselt werden. Es braucht also auch der Empfänger einen Schlüssel, um eine solche Mail, einen solchen Text, ein solches Dokument auch wieder entschlüsseln zu können und damit auslesen zu können. Und dahinter muss ein TrustCenter liegen, das die entsprechenden Schlüssel zertifiziert. Die TrustCenter sind im Betrieb erstens hochsicher und zweitens sehr teuer. Das wird auch der Kollege von der Notarkammer bestätigen können. Wir reden hier sicherlich nicht über Cent-Beträge. Ich kann Ihnen keinen Betrag nennen, aber wir reden auch hier wieder über steigende Preise und einen Verlust an Komfort. Und da müssen wir uns einfach fragen, was wollen wir? Wollen wir diese Höchstsicherheit mit dem Verlust an Komfort mit den höheren Preisen für alle, für jede beliebige Kommunikation, auch wenn sie diese Höchstsicherheit gar nicht braucht? Oder sagen wir, es genügt uns ein sehr hohes Maß an Sicherheit, das deutlich hinausgeht über das, was ein normaler Postbrief bietet, was eine normale E-Mail bietet…

Nicht rekonstruierbare Zwischenrufe der Zuhörerschaft

SV **Dr. Bernhard Rohleder**: Es gibt ja durchaus nicht nur schwarz und weiß, sondern auch Zwischenwelten, wo Sie mehr Sicherheit brauchen.

Vors. **Wolfgang Bosbach**: Rechtsgelehrte sind gefragt worden, Herr Reichenbach, sollen alle antworten oder genügt Ihnen eine sachkundige Auskunft von Herrn Dr. Brink?

BE **Gerold Reichenbach** (SPD): Wenn ich es richtig gesehen habe, steht die De-Mail oder das System nach TKG und nach § 113 TKG Manuelles Auskunftsverfahren, unter keinem Richtervorbehalt, um an die Passwörter und die Domain heranzukommen, das heißt dann könnte ich ja eigentlich die E-Mail lesen. Das wäre gegenüber dem klassischen Brief- und Postgeheimnis eine Abschwächung der Eingriffstiefe.

SV **Prof. Dr. Gerald Spindler**: Würde ich Ihnen jetzt prima vista zustimmen. Müsste ich mir nochmal genauer anschauen, ehrlich gesagt. Darf ich aber ganz kurz die Gelegenheit nutzen, mich nochmal zu den betroffenen EU-Grundfreiheiten zu äußern. Denn das Ganze soll ja auch für ausländische Dienste machbar sein, also aus dem EU-Ausland. Aber wenn wir über Fragen Portierbarkeit und Ähnliches im Hinblick auf zwingende einheitliche Domain-Namen reden, dann haben Sie einen Eingriff in die entsprechenden Grundfreiheiten, nämlich von ausländischen Anbietern. Und dann brauchen Sie wirklich zwingende Gründe dafür – und bitte an dieser Stelle nicht mit dem TK-Recht und der Portierbarkeit von Rufnummern argumentieren, denn wir haben in den TK-Richtlinien die Portierbarkeit entsprechend vorgesehen, nicht aber im Bereich der Domain-Namen. Also deswegen sehe ich ehrlich gesagt auch aus europarechtlichen Primärfreiheiten erhebliche Probleme.

Das Zweite, was man dann wirklich noch einmal genauer ausloten müsste, ob nicht unter Umständen auch die E-Commerce-Richtlinie zu berücksichtigen ist – Stichwort Herkunftslandprinzip. Da müssten Sie dann nämlich auch erst einmal die Ausnahmen bedenken bzw. heranziehen. Allein der Verbraucherschutz wird hier nicht verfangen. Da würde ich doch zur Vorsicht mahnen, dann greifen wir hier wirklich in den EU-Bereich ein.

Vors. **Wolfgang Bosbach**: Herr Dr. Brink, versuchen Sie es doch noch einmal.

SV **Dr. Stefan Brink**: Ja, ich versuche es noch mal. Würde es aber genau so sehen, wie Herr Prof. Spindler. Es gibt je nach dem, was für ein Kommunikationsmedium Sie nutzen, unterschiedliche Eingriffsschwellen für staatliche Erhebungseingriffe. Das können Sie nur als Nutzer steuern, indem Sie halt jeweils unterschiedliche Kommunikationswege nehmen. Sie haben vorhin schon Vorschläge hier aus dem Kreis der Sachverständigen zur Änderung im Bereich § 16 Auskunftsanspruch gehört, mit dem Appell an den Bundesgesetzgeber dann möglicherweise eine höhere Schwelle einzuziehen. Die andere Möglichkeit, auf das Bundesverfassungsgericht zu schauen, ist im Moment eher problematisch. Der erste Senat ist sehr innovativ, sogar auch im Erfinden von neuen Grundfreiheiten in dem Bereich. Der zweite Senat hält sich sehr zurück. Die letzte Entscheidung zur Beschlagnahme von E-Mails bei Rechtsanwälten stammt aus dem August 2010 und das war aus Datenschutzsicht und auch – glaube ich – aus genereller Sicht nicht erfreulich.

Vors. **Wolfgang Bosbach**: Ich habe jetzt noch jede Menge Wortmeldungen. Zunächst einmal Herr Dr. von Notz.

BE **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank, Herr Vorsitzender. Ich wollte vielleicht auch nochmal auf zwei andere Aspekte eingehen, die

wir bisher nur gestreift haben und zwar nochmal bezüglich des Missbrauchsrisikos und folgendem Gedanken. Bisher ist es ja so, dass im Internet so eine gewisse – es klang vorhin schon an – Grundunsicherheit herrscht. Es ist zutreffend, man ist beim E-Mail-Verkehr nicht so hundertprozentig sicher und bei anderen Sachen auch nicht. Man lebt damit. Im Grunde diese Problematik beim nPerso übertragend, verursacht es nicht auch Probleme, wenn ich jetzt ein System implementiere, was 99,9 prozentige Sicherheit suggeriert, und damit eine Erwartungshaltung irgendwie fördert, die die normalen – ich sag mal – Schutzmechanismen, die inzwischen das Internet entwickelt hat, bezüglich Bezahlung und all dieser Dinge, eben konterkariert. Entstehen nicht aus dieser Suggerierung der Sicherheit nicht ganz neue Missbrauchspotentiale. Die Frage würde ich gerne an Herrn Hülsmann und vielleicht an Sie, Herr Vossius richten. Wie das aus Ihrer Sicht ist. Und der zweite Punkt geht eher ins philosophische. Aber es sind ja lauter Gelehrte da. Vielleicht an Herrn Welte: Diese grundsätzliche Überlegung – und das klang hier schon ein-, zweimal an – zu sagen, wir versuchen praktisch das analoge Briefpost-System eins zu eins in die elektronische Welt zu übertragen oder nicht eins zu eins, aber wir versuchen das über – ich will fast sagen – Jahrhunderte herausgebildete Postwesen irgendwie jetzt in das Internet zu implementieren. Ist das überhaupt machbar, umsetzbar? Ist das überhaupt der richtige Ansatz, so irgendwie entstandene, auch rechtliche Handhabungen, vielleicht das dann auch wieder an Herrn Prof. Spindler, wie die Zustellungsfiktion, die wenn man sie - ich will jetzt hier nicht bei Adam und Eva anfangen - aber die Zustellungsfiktion, wie wir sie heute kennen – ich sag das jetzt mal steil – die wär mit PIN nicht gekommen, sondern die haben wir juristisch entwickelt, weil wir Beamte hatten, die sozusagen mit preußischer deutscher Beamtenmentalität den Brief bis in den letzten Haushalt getragen haben, egal welches Wetter, egal was. Und jetzt versuchen wir praktisch diese Zustellungsfiktion, die auf diesem geschichtlichen Fundament irgendwie, und die man heutzutage für den analogen Postdienst wegen all der Probleme, die es da jetzt gibt, seitdem das eben so gemacht wird geradezu infrage stellen könnte. Die es eben gemacht wird, die versuchen wir jetzt, ins Internet zu übertragen. Ist das überhaupt der grundsätzlich richtige Ansatz? Also kann man das eigentlich vom Gefühl …

Vors. **Wolfgang Bosbach**: Wollen wir mal schauen.

BE **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank.

Vors. **Wolfgang Bosbach**: Aber gern. Beim Brief kann nichts passieren, der kann nicht unterschlagen, nicht geöffnet, nicht in den falschen Briefkasten eingeworfen werden, der Briefträger kann nicht überfallen werden, das ist das einzige, was zu Hundert Prozent sicher ist, der Brief. Wir bewegen uns jetzt in ein hochriskantes Zeitalter, wo das alles sehr unsicher wird und jetzt müssen wir gucken, ob wir da Analogien zum sicheren Leben im vergangenen Jahrhundert herstellen können, wo

jeder Brief aber just-in-time im richtigen Briefkasten war, und dieser schwierigen Lage, der wir jetzt taumelnd als völlig überforderter Gesetzgeber entgegen streben. Der philosophische Teil ging an Herrn Welte und an Herrn Prof. Spindler. Wo der erste Teil hinkommt, habe ich jetzt nicht verstanden.

BE **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Das Missbrauchsrisiko an Herrn Vossius und Herrn Hülsmann.

Vors. **Wolfgang Bosbach**: Dann fangen wir jetzt mit dem Herrn Dr. Vossius und Herrn Hülsmann an.

SV **Dr. Oliver Vossius**: Das Missbrauchsrisiko, da werde ich mich nicht auf das Glatteis der Technik hier führen lassen. Das Missbrauchsrisiko kommt dadurch, dass die falschen Leute das System benutzen. Ich habe versucht, mit dem Beispiel zu zeigen, dass sich Betrüger relativ leicht einschleichen können, dass sie sich eine Adresse verschaffen können. Der Grund ist der, dass sich einmal die Verhältnisse schnell wandeln. Firmen können sich ändern, können verkauft werden, können zumachen – keiner merkt es. Die sitzen irgendwo im Ausland, die haben irgendwo ein Büro mal gehabt und haben jetzt keins mehr. Ein schönes Beispiel war vor einigen Jahren eine Recherche – ich glaube bei „Report“ oder „Monitor“ – über diese Betrüger, die diese Handelsregisterrechnungen verschickten, wo sie dann versucht haben mit der Kamera tatsächlich an den Adressen jemanden ausfindig zu machen und jemanden vor die Kamera zu bekommen. Und das haben wir hier auch. Die zusätzliche Gefahr ist die, beim Brief hat man es relativ schnell erkannt, aber auch da nicht vollkommen. Gut, seit zehn Jahren belehre ich darüber, zumindest hat seitdem kein Mandant mehr zugegeben, dass er bezahlt hat, zumindest das. Vorher haben einige dann doch gestanden, dass sie solche Rechnungen bezahlt haben. Beim Internet ist es schneller mal irgendwie rein geklickt, wenn Sie selber sehen, was Sie da an fiser.com oder an postbank.de oder anderen Versuchen so bekommen. Da ist die Gefahr größer, der Bildschirm ist kleiner, man hält nichts in der Hand, und man darf nicht übersehen, man macht das Ganze ja nicht für Leute wie Sie, die kommen damit zurecht, aber ich nicht. Das haben Sie zurecht vorher gesagt. Da sehe ich das Missbrauchsrisiko, dass man sich über diesen Schein von Sicherheit die ganzen Unwägbarkeiten oder ich hätte jetzt gesagt, den ganz normalen Wahnsinn des internationalen Gesellschaftsrechts ins Haus holt.

SV **Dipl. Inf. Werner Hülsmann**: Ich sehe da auch schon sehr hohe Risikopotentiale durch diese Suggerierung von Sicherheit. Denn wenn wir ganz ehrlich sind, wird durch das De-Mail-System tatsächlich nur im Prinzip von meinem PC zum Ziel-system, Ziel-PC oder - von mir aus - der Firmen-Mail-Server eine Sicherheit angeboten, die sich auch auf die Integrität, also auf die Echtheit der Mail und auch auf die Authentizität des Absenders bezieht. Das heißt, da ja davon ausgegangen

wird, dass aber die benutzten PCs, mit denen das De-Mail-System verwendet wird, zu einem großen Teil mit Bots verseucht sind, das ist ja die Begründung für das Entschlüsseln zwischendurch beim Dienstleister, entschlüsselt wird, wenn wir also das als gegeben hinnehmen und es ist tatsächlich so, das zumindest im privaten Sektor man davon ausgehen kann, dass die Hälfte bis zwei Drittel der privaten PCs und auch im – ich sag mal – gewerblichen Bereich – bei Mittelstand und kleineren Unternehmen wir auch auf die ähnliche Zahl von PCs kommen, verseucht sind, da wird suggeriert, die De-Mail ist sicher. Zum einen haben wir, was mein Vorredner Herr Dr. Vossius gesagt hat, dass sich eventuell Betrüger in das System einschleichen können. Da hat jemand eine De-Mail-Adresse, ja der wird schon seriös sein. Und wenn der mir eine Rechnung schickt, dann wird die schon richtig sein und bevor ich jetzt meine ganze Firma abfrage, wer denn das jetzt bestellt hat, bezahl ich mal die 150 Euro. Und wenn das 1.000 Leute gemacht haben, dann ist jemand um 150.000 Euro reicher. Das Risiko ist auf alle Fälle da, weil einfach Sicherheit suggeriert wird. Ein anderer Aspekt ist natürlich, hey ich habe das sichere De-Mail-System, da kann ja gar nichts passieren. Ich kann da eben mal irgendwelche Verträge mit abschließen. Dann ist aber leider mein Rechner verseucht. Und dann wird irgendetwas anderes abgeschlossen. Ich schicke etwas anderes weg, als ich glaube wegzuschicken, und ich schicke es vielleicht auch an einen anderen Empfänger. Ich bekomme vielleicht dann irgendwie eine Zustellbestätigung von irgendeinem Empfänger, dem ich dachte gar nichts gesandt zu haben. Aber er hat eine verbindlich De-Mail von mir bekommen, auf die er sich berufen kann. Wie soll ich beweisen, dass ich diese De-Mail nie willentlich abgeschickt habe, weil mein System hat sie ja abgeschickt. Mein Provider geht davon aus, dass ich sie abgeschickt habe. Der Empfänger darf sich dann natürlich auch darauf berufen, dass ich sie abgeschickt habe. Und das ist natürlich ein hohes Sicherheitspotential. Das haben wir beim ePerso auch, gut er soll ja nPerso genannt werden. Also beim neuen Personalausweis hat das BSI sehr deutlich gesagt, ja, der Personalausweis ist natürlich nur sicher, wenn das System, auf dem er eingesetzt wird, sicher ist. Das heißt eine sichere De-Mail bekommen wir nicht mit irgendeinem Kartenleser. Ich rede jetzt von der sicheren Anmeldung. Ich habe also Benutzername und Passwort, und dann muss ich vielleicht meinen nPerso noch in den Kartenleser packen, dann haben wir noch nicht wirklich eine sichere Anmeldung, wenn ich nicht genau weiß, dass es tatsächlich jetzt die Anmeldung am De-Mail-System ist, die da vom Perso abgefragt werden, weil das System vielleicht verseucht ist. Ich müsste im Prinzip mit meinem Perso jede einzelne Mail, die ich rausschicke freischalten, und ich müsste auf diesem Lesegerät die Mail, den Text, den Empfänger und den Absender sehen, um sicher zu sein, dass die Mail, die ich gerade mit meiner PIN für den nPerso, also für die entsprechende Funktion auf dem nPerso, freigebe, tatsächlich die Mail ist, die bei mir auf dem Bildschirm ist. Diese Sicherheit ist nämlich weder durch das De-Mail-System noch durch den nPerso gegeben.

Vors. **Wolfgang Bosbach**: Herr Welte.

SV **Harald Welte**: Dann komme ich zu der philosophischen Frage, ob wir denn die etablierten Verfahren, Normen, Rechte, Standards und dergleichen aus der Postwelt übernehmen können. Es ist sicherlich eine schwierige Frage. Aus meiner Sicht heraus ist das wesentliche Kriterium hier, dass der Schutz, den die Information genießt, die ich kommuniziere und das ist nicht nur der Schutz gegenüber Viren, Botnetzen und irgendwelchen Angreifern jeglicher Art, sondern das ist eben auch der Schutz vor staatlicher Überwachung, dass der ein gleiches Niveau erreicht. Und wie wir ja auch schon im Laufe dieser Diskussion gehört haben, ist der Schutz, den das De-Mail-System genießt, mit der Herausgabe der Zugangsdaten nach TKG ohne richterlichen Vorbehalt ein deutlich geringerer Schutz als die klassische Briefpost eben innehat. Die Diskussion hier scheint sich zwischen zwei Polen zu bewegen. Auf der einen Seite, ja es ist doch aber besser als die E-Mail und auf der anderen Seite, aber es ist doch nicht irgendwo vergleichbar von der rechtlichen Sicherheit wie die Briefpost. Und jetzt ist eben die Frage, wollen wir quasi eine Alternative zur Briefpost haben mit dem gleichen Schutz für den Anwender oder wollen wir einfach nur die E-Mail ein bisschen besser machen. Danke.

Vors. **Wolfgang Bosbach**: Die Bundesregierung.

MinDir **Martin Schallbruch** (BMI): Zwei Aspekte, die in der Diskussion angesprochen worden sind. Das eine, das Telekommunikationsgeheimnis: Die E-Mail ist Telekommunikation im Sinne des Telekommunikationsgesetzes und fällt deshalb unter das Telekommunikationsgeheimnis. Deshalb bestimmt sich die Möglichkeit des Zugriffs auf Inhalte nach den Regeln wie sie auch für Telekommunikation oder Briefverkehr gelten. Da ist also nichts unsicherer. Das ist ganz genau so geregelt. Der Verweis auf § 112, 113 TKG, da geht es um die Auskunft zu Bestandsdaten bei Telekommunikationsverhältnissen. Dieses Bestandsdatenauskunft umfasst nicht die Herausgabe des Passworts, die die Einsichtnahme des Inhaltes der Kommunikation dann ermöglicht. Weil das nun gerade unter das Telekommunikationsgeheimnis nach § 88 TKG fällt, das zur Klarstellung. § 112, 113 TKG verweisen auf die Daten nach § 111 TKG und wenn man sich § 111 TKG anguckt, dass sind die Bestandsdaten, also die Rufnummer, Name, Anschrift usw. Da gibt es die klassische Bestandsdatenauskunft, die auch für TK-Provider beispielsweise gilt. Was die Sicherheit der Kommunikation angeht, will ich noch ergänzend sagen, dass die von einigen Sachverständigen ein bisschen in Frage gezogene Transportverschlüsselung im Vergleich zu sonstiger elektronischer Kommunikation ein großer Sicherheitsgewinn ist, weil es um die Strecke vom Endkunden zum Provider, die Lagerung der De-Mails im Postfach bei dem Provider, die Übermittlung von einem Provider zum anderen Provider, die Lagerung im Postfach beim Empfänger und die Übermittlung vom Empfänger-Provider zum Empfänger geht, dass heißt alle diese Strecken werden

durch eine Verschlüsselung abgesichert. Und das ist zunächst einmal ein Vorteil, weil das völlig ohne jeglichen Aufwand für den Endanwender läuft, ohne dass er irgendetwas tun muss. Wenn man Ende-zu-Ende, das ist ja auch gefragt worden, beim Endanwender eine Ende-zu-Ende-Verschlüsselung generieren will, ganz abgesehen von der zu Recht von Herrn Hülsmann angesprochenen Problematik der Sicherheit des Rechners des Endanwenders, die wir für Ende-zu-Ende-Verschlüsselung auch haben, dann müsste man dort einen Aufwand treiben. Das kann auch durch eine Browser-Lösung sein. Dann sagt mir das BSI aber sehr deutlich für den Endanwender eine sichere Browser-Lösung, wo Schlüsselgenerierung möglicherweise beim Provider erfolgt und der Schlüssel im Einzelfall dem Endanwender geliefert wird, das ist ein zusätzlicher Aufwand für den Endanwender. Dieser Aufwand ist einfach da. Man kann ihm das nicht einfach abnehmen. Und insofern möchte ich das unterstreichen, was Herr Dr. Rohleder gesagt hat. Man kann immer hundertprozentige Sicherheit fordern, aber was De-Mail an dieser Stelle generiert, ist ein hohes Sicherheitsniveau ohne das der Kunde irgendetwas dazu tun muss. Er kriegt einfach mehr Sicherheit geliefert, ohne irgendetwas zu tun. Und an der Stelle wollten wir auch nicht die Verantwortung für diese Sicherheitsmaßnahmen auf den Endkunden verlagern, das wäre so, wenn man Ende-zu-Ende-Sicherheit verpflichtend vorsähe, sondern wir wollten die Verantwortung beim Provider lassen. Eine zweite Anmerkung noch. Es wurde hier ein Vorgängerprojekt „Julia“ oder so etwas erwähnt. So etwas gab es nicht, das vielleicht nur als Anmerkung. Es gab kein Vorläuferprojekt „Julia“, ist mir nicht bekannt. Und eine dritte Bemerkung. Im Zusammenhang mit der Domain ist gesagt worden, dass die Tatsache, dass eine E-Mail nun eine einheitliche Kennzeichnung durch eine einheitliche Domain erhält, dass man daran die Sicherheit irgendwie erkennen kann. Die Tatsache, dass eine eingehende Nachricht eine De-Mail ist, wird und muss durch den Provider durch eine entsprechende Zuordnung in das jeweilige De-Mail-Postfach des Endkunden sichergestellt werden. Daran erkennt der Endkunde, dass das eine vernünftig, richtig zugestellte De-Mail ist, nicht an irgendwelchen Adressen. Internet-E-Mail-Adressen kann man fälschen. Wenn wir eine einheitliche Domain vorsehen würden, wäre es möglich, natürlich diese Adresse als Internet-E-Mail-Adresse auch fälschlich zu verwenden. Und das würde dann aber natürlich im normalen E-Mail-Postfach landen, das heißt unabhängig von der Domainfrage, die Sicherheitseigenschaft knüpft sich an das Protokoll der Kommunikation zwischen dem Providern und an die Zuordnung dieser Nachricht in das gesonderte De-Mail-Postfach des Empfängers.

Vors. **Wolfgang Bosbach**: Herr Kollege Höferlin.

BE **Manuel Höferlin** (FDP): Vielen Dank. Ich glaube De-Mail kann nicht lösen, dass Computer gesichert sein müssen. Das Thema von Herrn Hülsmann, ich glaube, wir werden mit De-Mail nicht gesetzlich eine Lösung finden, sie technisch so verankern

und durch Verfahren so abwickeln. Dass ersetzt nicht die Notwendigkeit, dass ein Nutzer seinen Rechner absichern muss. Das ist so, sowohl beim neuen Personalausweis wie auch bei der De-Mail. Die Frage ist, wie kann man bestimmte Dinge sicherer machen. Und bei der Ende-zu-Ende-Verschlüsselung – ich lass mich da gerne nochmal berichtigen –, aber meine Vorstellung ist ja die, es ist auch bisher nicht besonders schwierig, sich eine Ende-zu-Ende-Verschlüsselung per E-Mail aufzubauen. Es ist nicht besonders schwierig. Es gibt zahllose, auch kostenlose Anbieter, bei denen ich Möglichkeiten bekomme, sofern der Empfänger natürlich ein entsprechendes System benutzt, eine verschlüsselte E-Mail zu verschicken. Und das wird ja auch weiterhin mit De-Mail möglich sein. Sie können genauso, wie bisher mit Ihren bestehenden, ich nehme an, Sie benutzen wahrscheinlich PGP oder so, würde ich Sie jetzt mal einschätzen, und dann können Sie darüber genauso auch die E-Mails PGP-verschlüsseln und eine PGP-verschlüsselte De-Mail versenden. Das steht Ihnen völlig frei. Und das können Sie wahrscheinlich sogar in Ihrem Thunderbird auch automatisieren. Ich verstehe nicht, wie man es schaffen soll und das war letztlich der Punkt, warum wir davon abgesehen haben, wie man es einfach so gestalten soll, dass, wenn man Provider verpflichtet, eine Ende-zu-Ende-Verschlüsselung anzubieten, dass der Nutzer ohne Probleme das plötzlich ohne Aufwand können soll, weil das hat sich seit – naja seit wann gibt es PGP, ich glaub 1995 oder so oder 1994 – hat sich nicht wirklich breit durchgesetzt. Weil letztlich, es fängt damit an, dass ich eben meinen privaten Schlüssel beim mir haben muss und ihn eben auch mit mir herumschleppen muss und das BMI hat uns gesagt, dass ja viele Provider, das haben auch die Provider selbst gesagt, bewusst auch die Web-Lösung haben wollten, weil sie die Erfahrung gemacht haben, dass der Nutzer eben mobil auf sein Postfach zugreifen möchte. Und da stellt sich mir halt die Frage, ich stelle sie mal an alle Sachverständigen, weil es antworten ja eh immer alle dann auch zu jeder Frage, von daher suche ich mir da auch keinen bestimmten raus. Das Verfahren so etwas sicher zu machen, ohne das jetzt zusätzliche Hürden, wie zum Beispiel ich muss meinen Schlüssel mitnehmen, weil daran scheitert es nämlich im Zweifel, hat es auch in der Vergangenheit, funktioniert nicht. Und wenn ich den Schlüssel beim Provider platziere, habe ich ja genau die gleiche Situation. Dann habe ich ein Vertrauensverhältnis, dass ich dem Provider entgegenbringen müsste, dass er den Schlüssel nicht herausgibt. Das ist mit Sicherheit nicht die Lösung, weil dann ist sozusagen das System konterkariert, wenn also der Provider meinen privaten Schlüssel vorhält, damit ich wieder darauf zugreifen kann. Da würde ich gern noch einmal eine Antwort haben. Warum jetzt plötzlich Ende-zu-Ende-Verschlüsselung von allen Nutzern akzeptiert wird, wenn es vorher 16 Jahre nicht

Vors. **Wolfgang Bosbach**: Herr Höferlin, das haben wir verstanden.

BE **Manuel Höferlin** (FDP): Das Zweite, die Domain-Frage. Ich habe mir das jetzt auch nochmal von Herrn Hülsmann angeguckt. Dieser Vorschlag Vorname

Nachname.xxxx@.De-Mail.de, das geht natürlich sehr stark dann so ein bisschen in Richtung Staats-De-Mail. Mir ist schon klar, man müsste dann irgendwie einen zentralen Server haben, der das dann verteilt an die Provider. Aber wir haben doch jetzt die Situation: Ich habe eine normale E-Mail-Adresse, Manuel.Höferlin@bundestag.de oder Manuel.Höferlin@t-online.de oder web.de und wenn mir das nicht passt – und es hat mir nicht gepasst – habe ich mir eben eine Domain registriert. Und deswegen habe ich eben eine Adresse, die heißt Manuel@höferlin.de. Wenn ich das bei De-Mail mache, habe ich doch genau das Gleiche erreicht, was ich auch bei der E-Mail immer geschafft habe. Ich habe eine Portierbarkeit meiner Adresse zu jeglichem Provider. Wenn das nicht so ist, möge mir das bitte erklärt werden.

Vors. **Wolfgang Bosbach**: An wen geht die Frage?

BE **Manuel Höferlin** (FDP): An alle. Herr Bosbach, Sie haben doch die Runde hier aufgemacht. Ich würde auf jeden Fall gerne Herrn Hülsmann fragen.

Vors. **Wolfgang Bosbach**: Um halb sechs ist hier Schluss!

BE **Manuel Höferlin** (FDP): Es durfte sich jeder melden. Also ich weiß nicht…

Vors. **Wolfgang Bosbach**: Hat ja nicht jeder nichts mehr zu tun.

BE **Manuel Höferlin** (FDP): Herr Hülsmann möchte auf jeden Fall antworten, weil den habe ich jetzt einfach gefragt und ansonsten gerne nochmal Herr Spindler, der hatte auch etwas dazu gesagt.

Vors. **Wolfgang Bosbach**: In Ordnung, Herr Hülsmann.

SV **Dipl. Inf. Werner Hülsmann**: Wenn das De-Mail-System, um jetzt diese Portierbarkeit kurz zu beantworten, tatsächlich Adressen wie Werner@Hülsmann.net, was auch eine meiner privaten Adressen ist, unterstützt, dann ist die Portierbarkeit natürlich gegeben. Wenn aber jetzt erzwungenermaßen De-Mail.de Teil des Namens sein muss, und wir haben nicht den zentralen Server, der allerdings nur verwaltet wohin, welcher Provider hostet jetzt diese Adresse, die E-Mail muss nicht darüber laufen, sondern die Information, wohin muss sie. Dann haben wir nämlich das Problem, dass wir Adressen bekommen, wie was weiß ich Werner.Hülsmann@t-online-De-Mail.de und die ist nicht portierbar, da müsste man in den Gesetzentwurf nochmal reingucken. Und der Gesetzentwurf sagt, De-Mail.de sollte Bestandteil sein und dieser Satz

Zwischenruf Abg. Clemens Binninger (Berichterstatter) nicht rekonstruierbar

SV **Dipl. Inf. Werner Hülsmann**: Da steht doch von der Kennzeichnung.

Zwischenruf Abg. Clemens Binninger (Berichterstatter): Ja, eine Kennzeichnung, eine…

Vors. **Wolfgang Bosbach**: Ja, da hat er Recht.

SV **Dipl. Inf. Werner Hülsmann**: Okay, gut. Also wie gesagt, wenn wir beliebige E-Mail-Adressen verwenden können, dann haben wir die Portierbarkeit sichergestellt. Wenn wir das so sehen, ich hatte das jetzt, wahrscheinlich aufgrund anderer Sachen, anders verstanden. Dann sind wir ja dacore. Wenn wir De-Mail.de vorschreiben, was irgendwo auch mal, vielleicht im Änderungsvorschlag gefordert war, da hätten wir das Problem, wenn diese providerabhängig ist, dass wir die Portierbarkeit verlieren. Was jetzt die Ende-zu-Ende-Verschlüsselung angeht, wenn die Provider verpflichtet würden, was anzubieten, dass ich sie benutzen kann, auch web-basierend. Es ist ja nicht so, wenn der Schlüssel beim Provider liegt, dass das System konterkariert ist. Wenn Sie da zum Beispiel als Passphrase sagen, „der Verzeichnisdienst eröffnet dem Nutzer gleichzeitig allein dadurch, dass“ einstellt und Sie sich das merken können. Das waren jetzt hier Anfänge von drei Absätzen. Es wäre nicht sehr geschickt, es genau so zu machen. Und dann kann auf den Schlüssel zugegriffen werden, wenn Sie diese Passphrase haben, und wenn Sie dann einen vertrauens-würdigen Provider haben… so eine Passphrase zu knacken, ist schon sehr sehr aufwendig.

Zwischenruf Abg. Manuel Höferlin (Berichterstatter) : Und wenn auf meinem Rechner ein Trojaner ist?

SV **Dipl. Inf. Werner Hülsmann**: Da benutzen Sie dann einfach die von Ihren Provider hoffentlich angebotene Möglichkeit der Bildschirmtastatur. Also ING-DIBA zum Beispiel als Bank, die macht das. Wenn ich mich dort anmelde, muss ich über eine Bildschirmtastatur noch einen sechsstelligen Pin-Code eingeben, den kann kein Trojaner abgreifen, weil an der Stelle die SSL-Verschlüsselung nämlich schon aktiviert ist. Die technischen Möglichkeiten wären also gegeben, so etwas einigermaßen sicher zu machen. Auch wenn der Rechner nicht hundertprozentig sicher ist. Wir haben also die technischen Möglichkeiten und deswegen, ich kann mit Thunderbird und PGP, ich verwende die offene Gnu-PGP-Version, ich kann damit dann einen webbasierten De-Mail-Dienst ja gar nicht nutzen, weil ich den nicht mit meinem Thunderbird gekoppelt kriege. Da müsste dann zumindest die Verpflichtung der Provider sein, dass sie entsprechende Schnittstellen für die Standard-E-Mail-Programme anbieten. Das wäre dann vielleicht die kleine Lösung.

Vors. **Wolfgang Bosbach**: So prima, das hätten wir jetzt geklärt. Jetzt zum Schluss, Herr Prof. Spindler. Jetzt noch etwas Nettes zum Schluss, etwas Erbauendes, nichts Kompliziertes. Zumal Herr Dr. Vossius hat ja zu Beginn gesagt, er würde seinen Klienten die neue Möglichkeit nicht empfehlen. Da stellt sich natürlich für alle Provider die Frage, ob da noch genug Kunden übrig bleiben.

SV **Prof. Dr. Gerald Spindler**: Okay gut. Meines Erachtens ist das jetzt mit der Portierbarkeit – ich denke mal – einigermaßen geklärt. Ich möchte nur nochmals auf die verfassungsrechtlichen Vorgaben kurz hinweisen. Wir haben es hier mit der Zurverfügungstellung von bestimmten Standards zu tun, die einem bestimmten Interesse dienen, wie gesagt, möglichst der Sicherheit. Und da gilt immer noch das Prinzip der Verhältnismäßigkeit, insbesondere des mildesten Mittels, was ich habe. Und wenn ich eben potenzielle Eingriffe in Rechte Dritter habe, muss ich dies beachten; ich beziehe mich jetzt nochmal auf die Domain-Namen, die auch unter Umständen in Persönlichkeitsrechte eingreifen, wenn Sie jetzt, Herr Höferlin zum Beispiel, nicht mehr Ihren Domain-Namen dafür verwenden können. Das wäre eine Konsequenz, wenn ich nur eine einheitliche Kennzeichnung hätte. Angesichts alternativer Möglichkeiten stellt sich aus verfassungsrechtlicher Sicht immer die Frage, wieso habt ihr nicht bei der Sache das mildeste Mittel genommen, insbesondere hinsichtlich von Persönlichkeitsrechten, aber auch Unternehmenskennzeichen etc. Und jetzt im Sinne der sozusagen bosbachschen Anforderungen ein nettes Schlusswort, aber ich mach es nicht im kölschen Dialekt.

Vors. **Wolfgang Bosbach**: Hätte der Sache Charme gegeben.

SV **Prof. Dr. Gerald Spindler**: Aber ich kann es nicht so gut. Ganz kurz, Scherz beiseite. Nochmals, was dieses Gesamtkonzept angeht, und es ist ja hier von Herrn Hülsmann auch schon, glaube ich, sehr eindringlich nochmal geschildert worden. Wir haben es hier mit einem komplexen System zu tun. Was hier gemacht wird, ist ein guter Sprung nach vorn. Aber er wird mit Sicherheit nie ausreichen. Und darüber muss man sich eben gewiss sein. Es ist die Frage, ob das Glas halbleer ist oder halbvoll ist. Das ist eine Frage der Perspektive. Es ist mit Sicherheit ein guter Schritt in die richtige Richtung, aber Sie dürfen auf gar keinen Fall dabei stehenbleiben. Und es ist absolut richtig, was Herr Hülsmann gesagt hat. Es ist ein komplexes System, was ineinandergreift. Und ich kann nur noch einmal sagen: Wir haben alle möglichen Produkte bestimmten Sicherheitsanforderungen unterworfen, ob das Autos sind, ob das irgendwelche Eierkocher sind...

Zwischenruf Abg. Dr. Dieter Wiefelspütz: Immer Schritt für Schritt!

SV **Prof. Dr. Gerald Spindler**: Richtig. Aber die Schritte müssen irgendwann kommen, Herr Dr. Wiefelspütz. Man darf nicht warten.

Zwischenruf Abg. Dr. Dieter Wiefelspütz: Es ist wie im Bereich der Straßensicherheit. Wir sind beim Internet am Anfang, aber jetzt geht es los! Wir brauchen neue Ethik, wir brauchen Sicherheitsfragen, viele viele Fragen…

Vors. **Wolfgang Bosbach**: Deshalb haben wir ja die Enquete-Kommission.

SV **Prof. Dr. Gerald Spindler**: Deswegen, Herr Dr. Wiefelspütz, haben wir die Enquete-Kommissionen, das zum einen. Zum anderen dürfen Sie bitte nicht vergessen, dass der Anstieg des Straßenverkehrs, wenn Sie den vergleichen mit dem Anstieg des Internets, überhaupt nicht vergleichbar ist.

Nicht rekonstruierbare Zwischenrufe der Zuhörerschaft

Vors. **Wolfgang Bosbach**: Das war auch ein schönes Schlusswort.

SV **Prof. Dr. Gerald Spindler**: Ich denke, im rheinischen Sinne: „Jetzt mach ich Schluss“.

Vors. **Wolfgang Bosbach**: Ich darf mich sehr herzlich bedanken bei ausnahmslos allen Sachverständigen, die heute hier gewesen sind, bei den Kollegen, aber auch bei den Besucherinnen und Besuchern. Kommen Sie gut nach Hause und ein schönes Wochenende.

Ende der Anhörung: 17:25 Uhr