Deutscher Bundestag **Protokoll Nr. 17/100**
17. Wahlperiode

Innenausschuss
Wortprotokoll
100. Sitzung

Öffentliche Anhörung

am Mittwoch, 20. März 2013, von 12.00 Uhr bis 14.00 Uhr
im Paul-Löbe-Haus, Raum 4.400
Konrad-Adenauer-Straße 1, 10557 Berlin

Vorsitz: Frank Hofmann (Volkach), MdB

Öffentliche Anhörung von Sachverständigen
zum

Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften

BT-Drucksache 17/11473

sowie **Ausschussdrucksache 17(4)688**

Seite

I. Anwesenheitsliste Mitglieder des Deutschen Bundestages

Bundesregierung

Bundesrat

Fraktionen und Gruppen

II. Liste der Sachverständigen für die Öffentliche Anhörung am 20. März 2013

1.	Reinhard Dankert	Der Landesbeauftragte für den Datenschutz Mecklenburg-Vorpommern, Schwerin
2.	Dr. Helmut Fogt	Deutscher Städtetag, Berlin
3.	Prof. Dr. Ralf Müller-Terpitz	Universität Passau
4.	Linus Neumann	Chaos Computer Club
5.	Dr. Bernhard Rohleder	BITKOM, Berlin
6.	Dirk Stocksmeier	]init[AG, Berlin

III. Sprechregister der Sachverständigen und Abgeordneten

IV. Protokollierung der Anhörung

Stv. Vors. **Frank Hofmann (Volkach)**: Meine sehr verehrten Damen und Herren, wir haben heute eine öffentliche Anhörung, in der es um die Förderung der elektronischen Verwaltung geht. Ich eröffne die 100. Sitzung des Innenausschusses. Meine sehr verehrten Damen und Herren, ich begrüße Sie alle sehr herzlich. Mein Name ist Frank Hofmann. Ich bin stellv. Vorsitzender des Innenausschusses und werde die öffentliche Anhörung von Sachverständigen leiten. Ich danke Ihnen, sehr geehrte Herren Sachverständige, dass Sie unserer Einladung nachgekommen sind, um die Fragen der Kolleginnen und Kollegen aus dem Innenausschuss und den mitberatenden Ausschüssen zu beantworten. Weiter begrüße ich alle anwesenden Gäste und Zuhörer. Für die Bundesregierung wird auch noch Herr PSt Dr. Ole Schröder, ich habe mit ihm schon im Innenausschuss gesprochen, er wird also auch mit anwesend sein. Trotz der Kürze der Zeit, sehr geehrte Herren Sachverständige, haben wir Sie gebeten, eine schriftliche Stellungnahme zu dem Gesetzentwurf und den damit verbundenen Fragestellungen abzugeben. Für die eingegangenen Stellungnahmen bedanke ich mich deshalb um so mehr. Sie sind an die Mitglieder des Innenausschusses und der mitberatenden Ausschüsse verteilt worden und werden dem Protokoll über diese Sitzung beigefügt. Ich gehe davon aus, dass Ihr Einverständnis zur öffentlichen Durchführung der Anhörung auch die Aufnahme der Stellungnahmen in eine Gesamtdrucksache umfasst. Von der heutigen Sitzung wird für ein Wortprotokoll eine Bandabschrift gefertigt. Das Protokoll wird Ihnen zur Korrektur übersandt. Im Anschreiben werden Ihnen Details zur Behandlung mitgeteilt. Die Gesamtdrucksache bestehend aus Protokoll und schriftlichen Stellungnahmen wird im Übrigen auch ins Internet eingestellt. Wie man schon der Einladung bzw. der Tagesordnung entnehmen konnte, ist insgesamt eine Zeit von zwei Stunden, also bis 14.00 Uhr vorgesehen. Einleitend möchte ich jedem Sachverständigen die Gelegenheit geben, in einer Erklärung, die fünf Minuten nicht überschreiten sollte, zum Beratungsgegenstand Stellung zu beziehen. Danach werden wir mit der Befragung der Sachverständigen durch die Berichterstatter sowie weiterer Abgeordneter beginnen, wobei ich jetzt schon darum bitte, dass die Fragesteller diejenigen Sachverständigen benennen, an die die Frage gerichtet ist. Wenn Sie damit einverstanden sind, würden wir so verfahren. Vielen Dank. Entsprechend alphabetischer Reihenfolge darf ich deshalb Herrn Reinhard Dankert, Landesbeauftragter für den Datenschutz Mecklenburg-Vorpommern um sein Einführungsstatement bitten.

SV **Reinhard Dankert** (Der Landesbeauftragte für den Datenschutz Mecklenburg-Vorpommern, Schwerin): Vielen Dank, Herr Vorsitzender! Meine Damen und Herren, ich werde mich bemühen, das kurz zu machen. Mecklenburg-Vorpommern ist auch federführend im AK-Technik der Datenschutzkonferenz der Landes- und Bundesbeauftragten für den Datenschutz. Insofern ist unsere

Stellungnahme auch eher auch etwas techniklastig, wo ich von vorneherein ein bisschen um Entschuldigung bitte, aber im Einzelfall können Sie ja nachfragen. Es wird Sie nicht wundern, dass wir aus unserer Sicht die kritischen Punkte herausgearbeitet haben. Im Großen und Ganzen begrüßen auch die Datenschützer so ein Vorhaben der Bundesregierung, was für die Bürgerinnen und Bürger Vereinfachung bringen soll, auch für die Verwaltung, aber trotzdem muss es auf einem hohen Standard bleiben und nicht hinter die klassischen Standards zurückgehen. Natürlich steht bei uns die Kritik der fehlenden Ende-zu-Ende-Verschlüsselung oben an, aber wir weisen auch daraufhin, dass sich im Gesetzentwurf – wir hatten auch nur zwei Tage Zeit, uns darauf vorzubereiten, ich bitte um Nachsicht, wenn wir vielleicht etwas zugespitzt diskutieren, Sie können es dann auch wieder verwerfen – nach unserer Meinung viele technische Sachverhalte vermischen, sogar Widersprüche zu bestehenden Gesetzen tun sich uns auf. Ich würde ganz kurz auf diese einzelnen Punkte in einem Schnelldurchlauf eingehen. Technisch dürfte es für die Dienstanbieter kein Problem sein, dieses anzubieten. Uns erschließt sich nicht, – oder nur mit großer Fantasie – warum es nicht gemacht wird und es kollidiert auch mit dem Bundesdatenschutzgesetz, nämlich mit dem Prinzip der Vertraulichkeit, denn wenn sensible Daten über das Netz per De-Mail übertragen werden, dann werden hier nach unserer Meinung die bestehenden Sicherheitslücken im jetzigen gewählten Verfahren per Gesetz weg-definiert. Das finden wir nicht besonders gut. Deswegen sollten Sie, insbesondere die Bitte an die federführenden oder regierenden Fraktionen, in den Anforderungskatalog dann doch verankern, dass die Anbieter die Ende-zu-Ende-Verschlüsselung anbieten müssen und nicht nur können. In Deutschland – jetzt komme ich zu unserem Punkt 2 – werden Pseudonyme verwendet. Pseudonyme sind ein wichtiges Instrument des technischen, aber auch des persönlichen Datenschutzes. Pseudonyme sind eindeutig, die Klarnamen stehen im Inhalt und deswegen sollten Sie auch bitte die Pseudonyme als absenderbestätigte De-Mail zulassen. Zwei Punkte, die wir herausgefunden haben, wo wir glauben, dass die nötige Klarheit aufgrund von technischen Vermischungen fehlt. Da geht es um qualifizierte Signatur, die der De-Mail-Anbieter beim Empfang der E-Mail empfängt und dann an den anderen weitergibt, der für den Empfänger zuständig ist. Normalerweise werden qualifizierte Signaturen durch natürliche Personen aufgebracht und nicht durch juristische Personen. Das ist ein Widerspruch, der sich uns nicht erklärt. Vielleicht sind wir da zu sehr Techniker. Es gibt auch im Signaturgesetz festgesetzte Kriterien für Signaturen, für den Anspruch, der in diesem Fall das De-Mail-Gesetz verlangt und im Signaturgesetz gibt es keine adäquaten Lösungen. Wir empfehlen daher eine eher rein technische Signatur, die entwickelt werden müsste und für den Fall, dass Sie dort willens sind, etwas zu verändern, stehen wir gerne zur Beratung zur Verfügung. Das Thema Zugangs-eröffnung ist sicherlich juristisch sauber geregelt, aber für die Bürger insgesamt ist es undurchsichtig. Im jetzigen Gesetzentwurf wird abgestellt darauf, dass es ein öffentliches Verzeichnis mit besonderem Zusatz gibt und für den Bürger ergibt sich

fast nur die Möglichkeit, den pauschalen zu wählen, wenn er nicht weiß, dass es auch andere Möglichkeiten gibt, also die Spezialzugänge zu den einzelnen Sachen. Wir sehen es eher aus der Sicht der Bürger heraus. Wir sind nach wie vor der Meinung, dass der konkrete Zugang zu einem bestimmten Dienst einer Behörde dem Bürger überlassen sein muss, es nicht erst schwierig herauszufinden ist und dieser pauschale Zugang eher die Ausnahme ist. Ich weiß, dass das möglicherweise aus Verwaltungssicht anders gesehen wird, aber das Selbstbestimmungsrecht des Bürgers sollte dabei nicht hintanstehen. Die Erklärung dazu sollte zumindest sein – wenn Sie diesen pauschalen Zugang nicht als Ausnahmelösung definieren –, dass die Anbieter dazu verpflichtet werden, die Bürgerinnen und Bürger, also die Kunden der Verwaltung, normenklar und transparent darauf hinweisen. Das wäre das Wenigste, was Sie machen sollten, damit der Bürger weiß, dass es neben dieser pauschalen Zugangsmöglichkeit auch andere Möglichkeiten gibt. Zur Georeferenzierung können wir kurz sagen: Das sollte nicht für das Personenstandswesen, den Meldepass und das Personalausweiswesen verwendet werden. Soweit zu unserer Kritik. Bei Punkt 6 unserer Stellungnahme geht es um die Formen der Einsichtnahme. Da gibt es einen eklatanten Widerspruch zum IFG, also zum Ansinnen der Transparenz und zum Wahlrecht. Hier wird durch eine starke Reglementierung erzeugt, dass de facto die Behörde die Wahl der Form der Einsichtnahme vorgibt. Sie sollten das so regeln, dass das Wahlrecht ähnlich wie im IFG, also dem Informationsfreiheitsgesetz, geregelt, dem Bürger überlassen wird und Abweichungen durch die Behörde nur bei triftigen Gründen erfolgen können. Punkt 7: Da haben wir herausgefunden, dass für die Schriftform als Ersatz auch elektronische Formulare eingesetzt werden sollen. Der Bürger kann am Bildschirm sicherlich Daten eingeben, die für die Behörde wichtig sind. Wir verstehen nicht, warum man an dieser Stelle sehr offen lässt, wie das technisch geregelt ist. Wenn im Signaturgesetz und auch im De-Mail-Gesetz klare technische Vorgaben sind, sollten Sie das in diesem Fall auch tun, weil hier auch das Schriftformerfordernis gilt. Insofern wäre es sehr gut, wenn an dieser Stelle nachgearbeitet werden würde. Es sind zwar Hinweise drauf, dass der Anbieter und der Betreiber und auch die Behörde entsprechende Regelungen schaffen müssen, aber wenn das so ist, dass Formulare schriftformersetzend sind, dann müssen sie auf dem gleichen technischen Standard sein wie z. B. De-Mail- oder auch nach Signaturgesetz. Unter Punkt 8 unserer Stellungnahme geht es um Identitätsdaten aus dem neuen Personalausweis. Sie schreiben, dass Sie u. a. verhindern wollen, dass Daten für Geschäftszwecke übermittelt werden. Dann machen Sie es im Gesetz auch so und lassen nicht irgendeine Öffnungsklausel zu, die dann heißt „nicht ausschließlich geschäftsmäßige Übermittlung“. Wir bitten Sie, diese Änderung zu streichen. Dann wird in dem Gesetzentwurf auch darauf hingewiesen, dass die elektronische Gesundheitskarte in die Identitätsprüfung genommen werden soll. Das halten wir vom Standard her nicht für gerechtfertigt. Die elektronische Gesundheitskarte entspricht nicht dem Standard wie beim neuen Personalausweis und sollte deswegen als Identifizierungsmittel ausgeschlossen werden. Dann haben

wir uns erlaubt, für die Kollegen des DBSV noch ein bisschen mit in die Bresche zu springen: Das Thema Barrierefreiheit. Es ist sicherlich in der Begründung erwähnt, dass für Barrierefreiheit zu sorgen ist, aber im Grunde gehört so etwas in die Spezialgesetze oder in das E-Gov-G als eigener Artikel. Da haben wir die Stellungnahme des DBSV übernommen und würden Sie bitten, das auch zu unterstützen. Diese ganzen Stellungnahmen haben wir in Abstimmung mit dem Bundesbeauftragten für Datenschutz und Informationsfreiheit abgegeben. Vor Ort stellen wir fest, dass es inzwischen einen Trend gibt, dass Sicherheit per Gesetz definiert wird, dass Abstriche in der IT-Sicherheit aufgrund fehlenden Geldes gemacht werden, insbesondere im kommunalen Sektor. Hier sollten wir alle zusammen gegensteuern. Ich bedanke mich für die Aufmerksamkeit.

Stv. Vors. **Frank Hofmann (Volkach)**: Ich danke Ihnen, Herr Dankert. Herr Dr. Fogt, bitte.

SV **Dr. Helmut Fogt** (Deutscher Städtetag, Berlin): Herr Vorsitzender, meine Damen und Herren, wir bedanken uns seitens des Städtetages für die Gelegenheit, hier noch einmal zu dem EGovG-E Stellung nehmen zu können. Ich darf vorausschicken, dass wir als Städtetag derselben Auffassung sind, was das Gesetz angeht, wie die beiden anderen kommunalen Spitzenverbände, Landkreistag und Städte- und Gemeindebund. Ich darf nochmals unterstreichen, dass wir diesen Gesetzentwurf insgesamt positiv betrachten. Wir sehen ihn als einen wichtigen Schritt für mehr bundeseinheitliches Angebot an elektronischen Verwaltungsdienstleistungen. Das haben wir bereits vor Jahresfrist – im vergangenen April – gegenüber dem federführenden Bundesinnenministerium erklärt. Wir haben uns erlaubt, im Dezember noch einmal die Fraktionsvorsitzenden der Regierungsfraktionen anzuschreiben, mit der Aufforderung, alles zu tun, dass dieses Gesetz bald im Gesetzblatt stehen kann. Das möchte ich noch einmal ausdrücklich für die Kommunen in diesem Land unterstreichen: Wir sehen durch das Gesetz einen erheblichen Fortschritt eröffnet, für elektronische Kommunikation, durch die De-Mail, in der Kombination aus elektronisch angebotenen Formularen und der ID-Funktion des elektronischen Personalausweises mit der jeweiligen Verwaltung, auch der Kommunalverwaltung unmittelbar in Austausch treten zu können, Online-Verwaltungsverfahren betreiben zu können. Wir sehen auch ein erhebliches Potential, über Einzelvorgänge hinausgehen und auch miteinander verbundene Verwaltungsvorgänge integriert dem Bürger anbieten zu können.

Das Stichwort Bürgerfreundlichkeit ist in diesem Zusammenhang für uns von großer Bedeutung, auch deswegen, weil der Bürger heute eine Erwartungshaltung mitbringt, wenn er sich mit öffentlichen Stellen auseinandersetzt und zwar vor dem Hintergrund dessen, was die private Wirtschaft – denken Sie an die Versicherungen oder andere Zweige, mit denen der Bürger zu tun hat – heute elektronisch anbieten kann. Das sind Standards, die da gesetzt sind und ich denke, dass sich die

öffentliche Verwaltung in Deutschland insgesamt an diesen Standards wird messen lassen müssen – auch ein Stück jenseits von Wirtschaftlichkeitsbetrachtungen. Man kann natürlich ausrechnen, was der Bürger spart, wenn er das entsprechende Angebot elektronisch wahrnimmt und nutzt. Ich denke, es ist über die Frage von Kostenersparnis und Wirtschaftlichkeit hinaus für den Bürger von hoher grundsätzlicher Bedeutung, dass er in der öffentlichen Verwaltung nicht anders behandelt wird und dasselbe Angebot präsentiert bekommt, wie es in der privaten Wirtschaft heute der Fall ist. Es hat immense Bedeutung auch in der Verwaltung intern, weil Hand in Hand mit dem elektronischen Abwickeln von Verwaltungsvorgängen auch eine Überprüfung der Vorgänge als solche verbunden sein muss. Wir erwarten uns auch einen gehörigen Schub in Richtung Verwaltungsmodernisierung, Optimierung von Geschäftsprozessen und dergleichen. Das Ganze wird, wie Sie wissen, systematisch durch die Einrichtung des IT-Planungsrates betrieben, der auch im Grundgesetz verankert worden ist, als Schaltstelle, an der der Bund, die Länder und die Kommunen bei diesem Vorgang E-Government-Angebot und elektronische Verwaltungsvorgänge zusammenarbeiten. Das E-Government ist sicher ein entscheidender Rahmen, in dem sich auch Weiteres abspielen wird.

Natürlich fragt jede Verwaltungsebene nach dem Aufwand und den Kosten, die mit dem Angebot elektronischer Verwaltungsdienstleistungen verbunden sind. Das gilt für den Bund, für die Länder und die Kommunen genauso. Wir haben perspektivisch durchaus Erwartungen an Investitionen, die wir tätigen, die wir als Kommunen im Übrigen schon seit 15 Jahren tätigen. Wir fangen nicht auf der grünen Wiese an, sondern wir haben auch selbstständig als Städte und Gemeinden in Deutschland entsprechende Angebote entwickelt. Wir haben nicht gewartet, bis der Bund und die Länder uns Vorgaben gemacht haben, sondern wir sind da ein erhebliches Stück in diesen 15 Jahren vorangekommen. In der Erwartung, dass sich diese Investitionen auch langfristig lohnen werden und dass wir auch Kostenersparnisse realisieren können. Ich darf auch sagen, dass das, was durch dieses Gesetz an zusätzlichen Anforderungen am Ende auch an die Kommunen gestellt wird, diese im Grunde längst erfüllt haben, oder wir sind gemeinsam mit den Ländern längst auf gutem Wege, das zu realisieren. Also auch die ambitionierten E-Government-Bausteine, die in diesem Gesetz angesprochen sind, sind längst in der Entwicklung. Ich denke, wir müssen zusehen, dass dieser einheitliche gesetzliche Rahmen rasch realisiert wird. Das Gesetz ist im Grunde genommen überfällig. Entsprechende Gesetze sind in einzelnen Bundesländern bereits realisiert. Anderswo wartet man darauf, dass das Bundesgesetz kommt, um das Landesgesetz auf den Weg bringen zu können. Wir appellieren, dieses Gesetz jetzt zügig zu verabschieden.

Stv. Vors. **Frank Hofmann (Volkach)**: Vielen Dank, Herr Dr. Fogt. Herr Prof. Dr. Müller-Terpitz, bitte.

SV **Professor Dr. Ralf Müller-Terpitz** (Universität Passau): Vielen Dank, Herr Vorsitzender. Ich erlaube mir einige Anmerkungen aus rechtswissenschaftlicher Perspektive, wobei diese Anmerkungen natürlich in keiner Weise abschließend sind. Zunächst einmal denke ich – das ist bei meinen Vorrednern auch schon deutlich zum Ausdruck gekommen –, ist der Gesetzentwurf in der Tendenz sehr zu begrüßen. Die Mehrzahl der rechtlichen Regeln ist meines Erachtens unproblematisch und eröffnet dem Gesetzgeber einen weiten Gestaltungsspielraum. Im Detail gibt es allerdings Probleme. Was den Regelungsort anbelangt, ist es kein wirkliches Problem, sondern eher eine rechtsästhetische Frage. Ich habe mir immer die Frage gestellt, warum man das in einem eigenständigen EGovG regelt? Wir haben die schöne Kodifikation des Verwaltungsverfahrensgesetzes. Man könnte meines Erachtens die Mehrzahl der Regelungen dort problemlos integrieren. Das würde mehr Transparenz schaffen, das würde den Kodifikationsgedanken – die Schlüssigkeit des Gesetzes – stärken, und es würde meines Erachtens einem Leitbild einer elektronischen Verwaltung viel eher entsprechen, also dem Leitbild neue Impulse geben. Was den Anwendungsbereich des EGovG anbelangt, muss ich als Außenstehender sagen – und ich formuliere das jetzt bewusst als Außenstehender, sozusagen als Bürger –, dass man sich bei der Lektüre etwas wundert, dass das Gesetz im Anwendungsbereich zwischen Bestimmungen mäandert, die auf den Bund anwendbar sein sollen, und solchen, die sowohl für die Bundes- als auch für die Landesebene gelten. Zum Teil gibt es dort Regelungen, wie § 2, wo man im Abs. 1 Regelungen findet, die für beide Behördenebenen gelten; im Abs. 2 und 3 dann wieder nur Regelungen für den Bund. Es stellt sich also die Frage, warum das so ist. Es gibt mit Sicherheit politische Gründe dafür. Die sollten aber meines Erachtens transparenter werden. Das gleiche gilt auch für die Frage der Zustimmungsbedürftigkeit. Im Moment gehen die Entwurfsverfasser davon aus, dass das Gesetz zustimmungsbedürftig ist. Das ist im Ergebnis wohl richtig. Es wird allerdings nicht luzide erläutert, warum Zustimmungsbedürftigkeit besteht. Sollte man sich auf den Art. 84 Abs. 1 S. 5 und 6 stützen, müsste das meines Erachtens dringend in die Begründung mit aufgenommen werden, damit sich der Bundesrat bzw. die im Bundesrat vertretenden Länder hierüber im Klaren sind, denn die Inanspruchnahme dieser Kompetenz würde eine Abweichungskompetenz sperren. Darüber muss meines Erachtens Klarheit geschaffen werden. Was die Zugangseröffnung anbelangt, kann ich mich den Vorrednern anschließen. Hier ist meines Erachtens eine zwingende Verpflichtung nicht aus dem Gesetz herauszunehmen, wie es der Bundesrat vorgeschlagen hat. Allerdings sollte man in Bezug auf die Verpflichtung, den Zugang auch über die De-Mail zu eröffnen, eine etwas technikoffenere und wettbewerbsneutrale Regelung formulieren. Ich werde auf den Gesichtspunkt der Technikoffenheit sogleich noch einmal zu sprechen kommen. Was die elektronische Aktenführung anbelangt, ist diese meines Erachtens ebenfalls nachdrücklich zu begrüßen. Ich würde die Einschränkung, die jetzt in dem Gesetzentwurf in § 6 S. 2 aufgenommen worden ist, wieder herausnehmen. Sie ist meines Erachtens überflüssig. Eine Soll-Vorschrift reicht hier völlig. Ich würde

allerdings – und dies scheint mir ein verfassungsrechtliches Desiderat zu sein – die Regelung bzgl. der Datensicherheit noch deutlich ausbauen. Bislang heißt es dort, dass die Akten nach dem Stand der Technik elektronisch geführt werden sollen. Wenn man sich die Vorratsdatenspeicherungsentscheidung des Bundesverfassungsgerichts anschaut und in Rechnung stellt, dass es hier um eine Querschnittsregelung geht, die eine Fülle von Daten erfasst, z. T. auch hochsensitive Daten, wie Gesundheitsdaten oder Betriebs- und Geschäftsgeheimnisse, dann müssen hier meines Erachtens gesetzgeberische Nachbesserungen auf der gesetzlichen Ebene vorgenommen werden, bspw. der Gestalt, dass der Gesetzgeber schon für bestimmte Daten das Niveau der Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität und Revisionsfähigkeit im Gesetz selbst zumindest abstrakt vorgibt. Das kann meines Erachtens nicht auf die Ebene der Verwaltung delegiert werden. Was die elektronische Substituierung des Schriftformerfordernisses anbelangt, muss man sagen, dass die qualifizierte elektronische Signatur nach wie vor das beste Mittel ist, um hier Authentizitäts- und Integritätsschutz sicherzustellen. Auf der anderen Seite erscheint es mir auch durchaus nachvollziehbar, dass man hier über alternative Schriftformerfordernisse nachdenkt, da sich die qualifizierte elektronische Signatur in der Praxis nicht als sehr erfolgreich, zumindest bei den Bürgern, erwiesen hat. Allerdings – und dies ist eine Kritik an dem § 3a Verwaltungsverfahrensgesetz – sollte man hier keine abschließende Regelung treffen der Gestalt, dass man bestimmte Substitute für Schriftformerfordernisse vorschreibt. Vielmehr sollte die Regelung technikoffen, zukunftsoffen und „rechtsraumoffen“ – so möchte ich das einmal formulieren – sein, vor allem im Hinblick auf die Europäische Union, die ja bekanntlich gegenwärtig an einem Entwurf für eine Verordnung über elektronische Identifizierungs- und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt arbeitet und diese Verordnung wird dann ggf. vorsehen, dass man einen Identifikationsdienst aus anderen Mitgliedstaaten anerkennen muss. Dem würde eine in sich geschlossene „Insellösung“ widersprechen. Als Vorbild mag hier der § 130a ZPO bzw. § 32a Abs. 3 StPO dienen, der gerade im Rahmen des E-Justice-Gesetzgebungsprozesses beraten wird. Abschließend noch zur Open-Data: Meines Erachtens sollte man in der Tat in den Gesetzentwurf oder in das jetzige Gesetzgebungsverfahren eine Aufforderung an die Verwaltung integrieren, Daten auch tatsächlich bereit zu stellen, sozusagen nicht nur zu regeln, was passieren muss, wenn Daten bereitgestellt werden, wie sie bereitgestellt werden sollen, sondern auch das „Ob“ der Bereitstellung stärker akzentuieren. Man sollte sich dabei auch nicht auf die reine Maschinenlesbarkeit beschränken, sondern auch vorgeben, dass nicht-proprietäre, d. h. technikoffene und zukunftsoffene Standards bei der Bereitstellung verwendet werden sollten. Allerdings muss ich auch sagen, dass ich skeptisch bin, ob das EGovG oder ggf. das Verwaltungsverfahrensgesetz hierfür der richtige Regelungsort ist. Meines Erachtens müssten diese Fragen eher im Informationsfreiheitsgesetz bzw. allgemein in den Informationsfreiheitsgesetzen, Umweltinformationsgesetzen usw. geregelt werden. Um es abschließend noch

einmal zusammenzufassen: Meines Erachtens handelt es sich um einen Schritt in die richtige Richtung. Allerdings brauchen wir bei der Datensicherheit verstärkte Regelungen. Bei der Technikoffenheit muss meines Erachtens nachgebessert werden, ebenso bei der Datenoffenheit und insgesamt sollte der Entwurf auch besser auf den Gesetzgebungsprozess im Rahmen von E-Justice abgestimmt werden. Vielen Dank!

Stv. Vors. **Frank Hofmann (Volkach)**: Ich danke Ihnen. Ich habe bisher festgestellt, dass wir sehr gut in der Zeit geblieben sind. Ich hoffe, dass das für die nächsten Sachverständigen auch gilt. Herr Neumann, Sie haben das Wort.

SV **Linus Neumann** (Chaos Computer Club): Guten Morgen! Ich bedanke mich für die Einladung. *[Zwischenrufe: „Guten Morgen? Wir haben 14 Uhr!“]* Wunderbar, jetzt habe ich genau den Aufhänger, auf den ich hinaus wollte. Ich bin Mitglied des Vereins Digitale Gesellschaft und des Chaos Computer Clubs. Hier stehen alle ein bisschen später auf, aber da man als „Chaot“ aus dem Computer Club in so einem Gremium natürlich einen gewissen Rechtfertigungsdrang hat, möchte ich kurz darauf hinweisen, dass ich als Berater in einem Unternehmen für IT-Sicherheit tätig bin, wo ich mich täglich mit der Risikoanalyse zukünftiger Hacking-Angriffe auseinandersetze und täglich forensische Untersuchungen erfolgreicher Einbrüche bei DAX 30-Unternehmen vornehme. Entsprechend möchte ich auch den Fokus meiner Stellungnahme legen und zwar auf die Risiken, die Sie mit dem Schritt jetzt eingehen.

Es ist eigentlich seit zwei Jahren bekannt, dass De-Mail nicht den maximalen Sicherheitsmaßnahmen und Sicherheitsstandards genügt. Ich würde gerne beleuchten, was jetzt nun die Entscheidung zu Folge hat. *[An Gerold Reichenbach gewendet:]* Ich kann mich gar nicht konzentrieren. Machen wir es so: Ich fasse mich kurz, aber dafür hören Sie auch zu. Wunderbar, Sie wollen jetzt Steuer- und Sozialdaten über dieses System abwickeln. Wir haben relativ wenig De-Mail-Server heutzutage. Es gibt relativ wenige Anbieter. Das liegt momentan wahrscheinlich daran, dass es eigentlich keinen Anwendungsfall gibt. Mit dem vorliegenden Gesetz wollen Sie einen solchen Fall schaffen. Was haben wir also für eine Situation in dem Moment, wo wir wenige De-Mail-Server haben, auf denen diese hochsensiblen Daten abgewickelt werden? Wir haben einzelne Server im Internet, die eine enorme Attraktivität für Angriffe bieten. Wir sagen, De-Mail ist ein sicheres System. Ich kenne relativ viele Systeme, die als sicher gelten, und ich kann aus meiner beruflichen Erfahrung heraus sagen, dass keines davon absolut sicher ist. RSA, Yahoo, Google sind alles riesige Konzerne, die alle schon Sicherheitslecks hatten. Wir müssen davon ausgehen, dass wir bei De-Mail irgendwann auch eines haben werden. Deshalb wird heute eigentlich im aktuellen Stand der Sicherheit darauf geachtet, dass man sich an keiner Stelle auf nur eine Sicherheitsmaßnahme ver-

lässt, sondern sich bemüht, durch mehrere Schutzschilde selbst die Kompromittierung eines Systems in den Folgen relativ gering zu halten.

Wenn wir uns das De-Mail-System anschauen, haben wir aufgrund der fehlenden Ende-zu-Ende-Verschlüsselung als besonderen Schwachpunkt diese Server. Ich kenne da mehrere häufig trainierte und in der Wildbahn gesehene Angriffsszenarien, z. B. den „Man-in-the-middle-Angriff“ oder persistente Infektionen auf dem Server. Das Ganze haben wir als Angriffsszenarien für unsere De-Mails verwandt. Die Frage ist, und die müssen Sie sich stellen: Wollen Sie ein solches System mit dieser Angriffsattraktivität belasten, oder wollen Sie dafür sorgen, dass Sie ein System schaffen, das zumindest Sicherheitsvorkehrungen hat oder über Sicherheitsvorkehrungen verfügt, die diesem enormen Angriffsrisiko irgendwie etwas entgegensetzen? Das ist momentan nicht der Fall. Aus diesem Grunde halte ich es für absolut geboten, bei De-Mail die Ende-zu-Ende-Verschlüsselung nicht nur als Option anzubieten, sondern wirklich als Standard zu erzwingen. Nur dann haben Sie eine Möglichkeit, ein System zu „bauen“, was überhaupt an die Sicherheitserfordernisse, die heute schon in der Privatwirtschaft Anwendung finden, heranreicht.

Ich erzähle wahrscheinlich nichts Neues. Wenn ich mir diesen Gesetzentwurf anschaue, wollen Sie ja bewusst die Erfordernisse der bestehenden Gesetze senken, um mit De-Mail kompatibel zu werden. Sie weichen schon aktuell bestehenden Sicherheitsvorkehrungen auf, damit Sie Ihre Verwaltung über De-Mail abwickeln können. Ich denke, das ist ein relativ großes Risiko, und ich gehe davon aus, dass sich – sollte das so beschlossen werden – in wenigen Jahren jemand dafür rechtfertigen muss. Insofern sehe ich nach dem aktuellen Entwurf drei realistische Zukunftsszenarien.

Erstens: Das Ganze setzt sich nicht durch. Sie verbrennen ein Heidengeld und Deutschland bleibt Schlusslicht in Fragen des E-Governments. Das wäre aus Nutzerperspektive nach dem momentanen Stand der wünschenswerte Fall.

Zweitens: Das Ganze setzt sich durch. Sie schaffen diese riesig attraktiven Daten-Silos im Internet mit weniger Sicherung, als sie heute schon Standard ist, und in absehbarer Zeit kommt es dort zu einer Datenextraktion, die dann für alle Beteiligten – seien es die Bürger, sei es die Regierung, seien es die Behörden – sehr peinlich werden kann.

Drittens: Ich sehe jetzt die Gelegenheit zur Nachbesserung des De-Mail-Gesetzes. Das Ganze nutzt noch niemand. Der Standard kann jetzt noch nachgebessert werden, davon sind wenige Menschen betroffen. Da die Gelegenheit für die Bundesregierung besteht, tatsächlich in eine Vorreiterrolle in Sachen des E-Governments zu gehen, möchte ich Sie eindrücklich warnen, hier jetzt Sicherheits-

vorkehrungen aufzuweichen, um diesem De-Mail-System gerecht werden. Ich danke Ihnen!

Stv. Vors. **Frank Hofmann (Volkach)**: Ich danke Ihnen! Herr Dr. Rohleder, bitte.

SV **Dr. Bernhard Rohleder** (BITKOM, Berlin): Vielen Dank, Herr Vorsitzender. Meine Damen, meine Herren, guten Tag. Sie haben mich als Vertreter der Wirtschaft eingeladen. Wir stehen für 2.000 Unternehmen aus dem IT-Telekommunikationsbereich – alle großen Serviceprovider, alle großen Netzbetreiber und mehr als 1.000 kleine, mittelständische gründergeführte Unternehmen. Wir begrüßen den Gesetzentwurf sehr. Wir würden sogar darüber hinausgehen und sagen, dass er längst überfällig ist. Wenn wir uns ansehen, worüber wir in der Wirtschaft sprechen, dann reden wir über Cyber Physical Systems, über das Internet der Dinge und der Dienste, über Maschinen, die mit Bauteilen kommunizieren. Dann gehen wir in die Verwaltung und haben eine komplett andere, nämlich eine anachronistische Welt vor uns, die steinzeitartig organisiert ist, und führen jetzt hier eine Diskussion, wo wir Sicherheitsfragen in den Mittelpunkt stellen, die wir uns in der analogen Kommunikation nie gestellt haben. Das, was wir jetzt diskutieren, ist eine ähnliche Frage, als ob ich ein Amtsschreiben in Geheimschrift verfasse und dieses im Metalltresor verschicke. Das ist das, was gefordert wird. Ist es das, was wir wirklich wollen, oder nutzen wir Technologien, die wir verfügbar haben und die aufgrund von Sicherheitsbedenken – ich halte dies für absolut kontraproduktiv überzogen – jetzt nicht zum Einsatz bringen? Das können wir nachher sicherlich gerne noch diskutieren. Anachronismus auch insofern, als die Bürger natürlich gewohnt sind, in ihrem privaten und in ihrem Arbeitsumfeld komplett digital und zwar unterbrechungs- und friktionsfrei zu kommunizieren. Sie haben im Jahr im Schnitt 1,5 Behördenkontakte, und der eine Behördenkontakt ist das Elster-Formular. Dann gibt es noch 0,5 weitere Behördenkontakte und dann stellt sich die Frage, welche Sicherheitsanforderungen wollen wir hier diesem 0,5 Behördenkontakt mitgeben? Kann die qualifizierte elektronische Signatur, die es in Deutschland seit mittlerweile 15 Jahren gibt, und die seit 15 Jahren niemand anwendet, wirklich eine zusätzliche Sicherheit bringen? Oder überfordert sie nicht den normalen Nutzer mit der Schlüsselverwaltung, der schon seine Probleme hat, sich seine vielen Passwörter zu merken und die sicher zu verwalten? Insofern begrüßen wir sehr, dass jetzt gesetzliche Grundlagen geschaffen werden, die wir uns sehr, sehr viel weitergehend vorstellen würden und die dafür sorgen, dass Bürger nicht nur in ihrem Wirtschafts- und privaten Lebensumfeld elektronisch kommunizieren können, sondern das auch mit Behörden tun können und dafür ein Instrument an die Hand bekommen, das 99,9-prozentige Sicherheit liefert, nämlich eine komplette Transportverschlüsselung, und in Teilen des Transports auch eine Ende-zu-Ende-Verschlüsselung liefert, die darüber hinaus sicherstellt, dass ein Befall und ein Angriff auf die Integrität der Daten weitestmöglich ausgeschlossen wird, und wo es jetzt schon zusätzliche Dienste im Markt gibt, die dem profes-

sionellen Nutzer natürlich eine Ende-zu-Ende-Verschlüsselung sehr einfach möglich machen, vom Verfassen der ersten Mail oder vom Einstellen eines Dokuments bis zu dessen Entschlüsselung. Insofern ist es aus unserer Sicht ein gelungener Entwurf, den man sicherlich in einzelnen Details verbessern kann. Wenn hier Details verbessert werden, würden wir uns eher noch einen weiteren Schritt nach vorne als einen Schritt zurück wünschen. Vielen Dank!

Stv. Vors. **Frank Hofmann (Volkach)**: Vielen Dank, Herr Dr. Rohleder. Ich glaube, das kann spannend werden. Herr Stocksmeier, Sie haben das Wort.

SV **Dirk Stocksmeier** (Vorstandsvorsitzender der]init[AG, Berlin): Herzlichen Dank, Herr Vorsitzender. Meine Damen und Herren, schätzungsweise 18 Mrd. Euro investiert die Deutsche Verwaltung jährlich in Informations- und Kommunikationstechnologien. Das tut sie seit vielen Jahren, auch mit großem Erfolg, in vielen Bereichen. Herr Dr. Fogt hat das eben schon angesprochen.
Die Bürger sind es heute gewohnt, eine Vielzahl von Dingen online über das Internet zu erledigen, vor allem im Bereich der Wirtschaft. Das betrifft etwa das Einkaufen oder die Bankgeschäfte und vieles mehr. Vergleichbares wünschen sich die Bürger natürlich auch von ihrer Verwaltung. Für den Aufbau entsprechender Angebote fehlen aber in vielen Fällen heute noch die rechtlichen Voraussetzungen, und genau hier setzt das EGovG an. Im Bereich der Schriftformerfordernisse können wir mit dem EGovG tatsächlich den nächsten Schritt gehen, um Online-Angebote an die Bürger zu bringen. Das ist ein wichtiger Schritt, den wir hier zusammen gehen können, und insofern freue ich mich, dass das Gesetz zu all diesen Dingen wichtige Punkte und Regelungen enthält und zudem Klarstellungen über vieles, was sich im Rahmen der Verwaltung entwickelt hat. Beispielsweise, dass auf Formularen häufig ein Unterschriftsfeld vorgesehen, obwohl es gar nicht notwendig und auch nicht gesetzlich vorgeschrieben ist. Auch hier kann mehr Effizienz geschaffen werden. Es ist schon vieles zu der allgemeinen Wahrnehmung des Gesetzes gesagt worden, der ich mich anschließen kann. Ich denke, wir gehen mit den EGovG einen guten Schritt in die richtige Richtung, und ich glaube, es ist wichtig, dass wir es schaffen, hier die letzten Hürden aus dem Weg zu räumen. Ich würde jetzt noch kurz etwas zum Thema De-Mail sagen, weil das hier in der heutigen Diskussion auch eine große Rolle spielt. Aus meiner Sicht ist mit der De-Mail eine technische Lösung geschaffen worden, die eine Verlässlichkeit im Bereich der Zustellung sicherstellt. Absender und Empfänger können über ihre gegenseitige Identität sicher sein. Es ist auch sichergestellt, dass eine Nachricht nachweisbar zugestellt worden ist. Zusätzlich wird ein höheres Maß an Vertraulichkeit durch die verschiedenen Verschlüsselungsmechanismen angeboten. Ergänzend – und das ist auch für den Privatbürger besonders wichtig – enthält das Verfahren die Erkennung von Schadstoffsoftware. Es ist also sehr unwahrscheinlich, dass man beim De-Mail-Transfer Viren auf seinen Rechner bekommt. Das Sicherheitsniveau von De-Mail ist auch mit Blick auf die öffentliche Verwaltung

entwickelt worden. Die Experten haben sich mit deren Anforderungen auseinandergesetzt und für eine große Zahl von Anwendungen des öffentlichen Bereichs ist De-Mail zweifelsohne sehr geeignet und angemessen. Selbstverständlich gibt es auch Anwendungsbereiche, in denen man zusätzliche Sicherheitstechnologie einsetzen sollte, z. B. die sogenannte Ende-zu-Ende-Verschlüsselung. Das ist völlig unstrittig. Akkreditierte De-Mail-Anbieter unterstützen diese Ende-zu-Ende-Verschlüsselung zum Beispiel dadurch, dass sie ein Schlüsselverzeichnis zur Verfügung stellen und die Kommunikationspartner entsprechend diese Schlüsselinfrastruktur nutzen können. Das Konzept der rechtssicheren Zustellung auf der Basis von De-Mail besticht durch die einfache Bedienbarkeit. Die meisten Nutzer im Privatbereich nutzen E-Mail heute über den Browser, d. h. sie haben keine Komponenten auf ihrem PC installiert, sondern können mit sehr geringem Aufwand die E-Mail-Funktion nutzen. Das Gleiche ist natürlich auch mit De-Mail möglich. Für die Ende-zu-Ende-Verschlüsselung braucht man aber zusätzliche Komponenten auf den Rechnern der Nutzer. Wenn man hier das Anforderungsniveau zwingend erhöht, führt das dazu, dass jeder der De-Mail nutzen möchte, auch Anwendungen installieren muss. Und das ist gar nicht so unkompliziert. Nicht nur die Installation, auch das Schlüsselmanagement stellt gewisse Anforderungen an den Nutzer, und man muss sich sehr gut überlegen, welches Niveau man wählt, damit man eine rechtssichere, verbindliche Kommunikation mit einem gewissen Sicherheitsniveau im Internet erreichen kann, und damit auch möglichst viele Bürgerinnen und Bürger erreicht. Ich sehe hier die Gefahr – und möchte da auch ausdrücklich noch einmal auf die Erfahrungen zum Signaturgesetz verweisen –, dass wir möglicherweise in der jetzigen Phase ein Sicherheitsniveau definieren, das so hoch ist, dass ein Großteil der Bürger die Anwendung nicht nutzen wird. Dann wird, wie in vielen anderen Fällen, häufig auf alternative Verfahren zugegriffen, die dann aber ggf. gar keine Sicherheit mehr bieten. Insofern gilt es in der jetzigen Phase, ein gesundes Augenmaß zu finden, in welcher Form man das eigentlich sehr durchdachte De-Mail-Verfahren noch um weitere Komponenten erweitert. Natürlich kann ich mich dem anschließen, was Sie auch zur Gefahrensituation gesagt haben und zu der Bedrohung der Server. Die De-Mail-Server stellen natürlich eine Versuchung für die Hacker dar, das ist gar keine Frage. Das ist aber von Anfang an bekannt gewesen. Diejenigen, die die De-Mail entwickelt haben und auch hier die technischen Festlegungen getroffen haben, haben das natürlich auch im Blick gehabt und eine Vielzahl von technischen und organisatorischen Maßnahmen vorgesehen, die sicherstellen, dass diese Risiken reduziert werden. Man hat es hier geschafft, ein gutes Gleichgewicht zwischen Funktionalität, Einfachheit und Sicherheit zu finden, und ich denke, man könnte das Verfahren so in Betrieb nehmen. Es ist ja auch so, dass jeder selbst bestimmen kann, ob er einen Zugang eröffnen möchte: Bürger, die der Meinung sind, sie möchten De-Mail gar nicht nutzen, müssen das auch nicht tun. Bürger, die der Meinung sind, sie möchten nur mit bestimmten Behörden über De-Mail kommunizieren, können das ebenfalls selbst entscheiden. Wenn sich der Markt

dahin entwickeln wird, dass die De-Mail-Anbieter sehen, dass es einen großen Bedarf an Ende-zu-Ende-Verschlüsselung gibt, dann werden sie im Ergebnis sicher auch zusätzlich – und optional – diese Funktionalität zur Verfügung stellen. Es ist übrigens auch eine Stärke des De-Mail-Verfahrens, dass hier nicht der Staat die Infrastruktur zur Verfügung stellt, sondern auch die Kräfte der Wirtschaft nutzt. Es wird sich ein Markt entwickeln, und wenn sich neue technische Möglichkeiten ergeben, die Sicherheit zu erhöhen, dann wird es hier vermutlich auch entsprechende Marktentwicklungen auf Seiten der Anbieter geben, um vielleicht besonders sicherheitsaffine Nutzer auch mit einem besonderen Service bedienen zu können. Soviel zum Thema De-Mail. Ansonsten möchte ich auch noch erwähnen, dass sich zahlreiche Vertreter aus Wirtschaft und Wissenschaft seit Langem dafür eingesetzt haben, dass dieses E-Gov-G jetzt verabschiedet wird. Wir sehen natürlich die Komplexität des Verfahrens, denn es betrifft am Ende ja in Summe ca. 20.000 Verwaltungen in Deutschland. Einige Verwaltungen müssen etwas tun, andere bekommen lediglich neue Möglichkeiten. Insofern bin ich froh, dass das Gesetz trotz dieser komplexen Abstimmungsthemen inzwischen so einen reifen Stand erreicht hat. Viele setzen sich dafür ein – oder haben es schon getan –, dass das Gesetz nun schnellstmöglich verabschiedet wird. Das sind nicht nur die IT-Unternehmen, sondern eben auch die Anwender, z. B. der Deutsche Landkreistag, die sich davon viel versprechen. Und ich würde mich freuen, wenn Sie sich auch dafür einsetzen und dieses Gesetz in dieser Legislaturperiode noch zur Verabschiedung bringen. Danke schön!

Stv. Vors. **Frank Hofmann (Volkach)**: Vielen Dank den Sachverständigen für die Eingangsstatements. Wir kommen nun zur Berichterstatterrunde. Als Erstes hat Herr Binninger für die CDU/CSU-Fraktion das Wort.

BE **Clemens Binninger** (CDU/CSU): Vielen Dank an die Sachverständigen. Ich hätte an drei Herren noch einmal eine Frage. Herr Dr. Fogt, wir haben ja die Kommunalen Spitzenverbände intensiv mit eingebunden. Trotzdem wird immer ein bisschen die Sorge geäußert, was da an Kosten auf die Kommunen zukommt. Der Gesetzentwurf ist ja so weit gefasst, wie man ihn machen könnte, oder wie sich Herr Rohleder wünschen würde, dass eben auch die Kommunen verpflichtet sind, das gleich anzubieten, wenn sie Bundesrecht ausführen. Könnten Sie uns trotzdem, sofern es geht, eine grobe Hausnummer nennen, welche Ihnen auf eine Gemeinde mittlerer Größe bis 20.000 Einwohner – und das dürften ja die meisten sein – zukommen, wenn sie jetzt das EGovG umsetzen muss wegen neuer Infrastruktur, Anmelden eines De-Mail-Kontos bei irgendeinem Provider? Das müssen sie ja machen. Wenn Sie uns dazu etwas sagen könnten. Oder ist es so, wie wir einmal vermutet haben, dass es eher organisatorischer und personeller Aufwand innerhalb der Kommunen ist, und weniger eine tatsächliche große Haushaltsbelastung. Dann habe ich noch eine Frage an Herrn Dankert. Mir war etwas nicht ganz klar – sowohl

in Ihrer schriftlichen Stellungnahme als auch in der mündlichen Sie haben ja sehr stark zum De-Mail-G gesprochen, das wir punktuell ändern, aber über das wir heute nicht mehr beraten, dazu hatten wir vor langer Zeit auch schon Anhörungen, aber trotzdem die Frage: Was meinen Sie damit, dass der Provider verpflichtet werden muss, die Ende-zu-Ende-Verschlüsselung anzubieten? Reicht Ihnen das, was wir im Gesetz schon drin haben, also die Information über die verschiedenen Verschlüsselungen? Dass Transportverschlüsselung das normale ist, im Unterschied zur Ende-zu-Ende-Verschlüsselung, wo dann auch der mündige Kunde selber entscheiden kann, was er will, nachdem ihm sein Provider, auch auf die Unterschiede hingewiesen hat. Meinen Sie damit, dass nur die Ende-zu-Ende-Verschlüsselung erfolgen muss, obwohl wir ja wissen, dass da alle Schwierigkeiten hinzukommen, dann wird das der Ladenhüter, den wir bei der Signatur seit 15 Jahren habe. Da würde mich noch einmal interessieren, was Sie mit dieser Verpflichtung meinen. Halten Sie das, was wir im § 5, im § 9 des De-Mail-G schon stehen haben, nicht auch schon für ausreichend und aufklärend gegenüber dem Kunden? Noch eine Frage an Herrn Dr. Rohleder. Könnten Sie uns auch einen Eindruck von der Dimension geben, wenn das jetzt Verbreitung findet, aber auch De-Mail Verbreitung findet, wie viel Millionen an Briefsendungen, die heute eben noch aus unterschiedlichsten Gründen kuvertiert ausgedruckt, teils maschinell unterschrieben in den Versand gehen müssen, wie sich das auswirken könnte, wenn man sagt, dass ein Großteil des Briefmarktes jetzt eben durch das E-Gov-G durch den Schriftformersatz elektronisch versandt werden haben, ob man das irgendwie quantifizieren kann, was es eben an Erleichterungen auslöst oder auch mengenmäßig? Von der Reihenfolge vielleicht so, wie ich die Fragen gestellt habe.

Stv. Vors. **Frank Hofmann (Volkach)**: So machen wir das. Herr Dr. Fogt, bitte.

BE **Clemens Binninger** (CDU/CSU): Herr Vorsitzender, das wird je nach Anhörung unterschiedlich gehandhabt: Sind ganz kurze Nachfragen erlaubt, wenn man es präzisieren möchte? Sonst müsste man ewige Schlaufen drehen, bis man in 20 Minuten wieder rankommt, und dann habe ich es meistens wieder selber vergessen. Es ist im Interesse aller besser, wenn man es gleich stellt.

Stv. Vors. **Frank Hofmann (Volkach)**: Herr Binninger, wir machen das.

SV **Dr. Helmut Fogt** (Deutscher Städtetag, Berlin): Es wird Sie vielleicht überraschen – die Kommunalen Spitzenverbände sind natürlich immer vorn, wenn es darum geht, Kostenerstattung für Aufwände zu fordern, die durch die Gesetzgebung von Bund und Ländern ausgelöst werden. Aber ich darf sagen, dass durch die Regelungen, die jetzt im Entwurf des EGovG stehen, die Kommunen so gut wie gar nicht belastet werden. Es ist ja so, dass im Wesentlichen drei Voraussetzungen zu erfüllen sind: Das eine ist der elektronische Zugang. Da sind wir zunächst nur

genötigt, einen normalen E-Mail-Zugang anzubieten. Ich kenne keine Kommune in Deutschland, die keinen zentralen E-Mail-Account besitzt. Wir müssen zum Zweiten Kontaktdaten und Verfahrensangaben präsentieren. Kontaktdaten als Muss-Vorschrift, Verfahrensangaben lediglich als Soll-Vorschrift. Jede Kommune in Deutschland verfügt über einen Internetauftritt, wo die elementaren Angaben zur Erreichbarkeit selbstverständlich enthalten sind. Wenn in diesem Zusammenhang Kosten entstehen, so betreffen sie eher die Länder. Es sind nach meiner Kenntnis sämtliche Bundesländer auf dem Weg, landesweit Behördenfinder zu installieren, wo Sie problemlos die zuständige Behörde adressiert bekommen, auch die der Kommunalverwaltung. Dies wird gegenwärtig mit dem System Leika verknüpft. Das ist ein System, in dem die entsprechenden Verwaltungsleistungen standardisiert aufgeführt sind, so dass dieser Behördenfinder dann auch mit dem Nachweis, für welche spezielle Verwaltungsleistung welche Behörde zuständig ist, verknüpft werden kann. Dann gibt es noch Formularserver und dergleichen. Wir haben demnach mit den Vorgaben, wie sie auch als Soll-Vorschrift enthalten sind, auf kommunaler Ebene kein wirkliches Problem. Der dritte Punkt betrifft die Angaben zu elektronischer Bezahlung. Da genügt die Angabe des Bankkontos der entsprechenden Kommune. Auch das ist selbstverständlicher Standard. Wir sind im Gegenteil dabei – es gibt das System ePay/Bund, Länder – wirkliche Online-Bezahlplattformen zu entwickeln und diese dann auch im kommunalen Bereich einzuführen. Die Anforderungen für die Pflege dieser Dienste ist sehr überschaubar. Es ist erforderlich, Kontaktdaten à jour zu halten, Leistungskataloge evtl. zu überprüfen. Das sind aber alles Dinge, die zu vernachlässigen sind, und selbst die Einrichtung eines De-Mail-Accounts bewegt sich nach unserem Eindruck in Größenordnungen von einigen tausend Euro. Nichts, was jetzt tatsächlich ein Kostenhindernis wäre, so dass wir sagen könnten, von Seiten der Kommunen hätten wir irgendwo Schwierigkeiten mit diesem Gesetz. Natürlich steht auch im Gesetz, dass weitere Aufgaben im Zweifel über das Landesrecht an die Kommunen adressiert werden müssen, aber wie ich schon sagte, da sind alle Länder mit ihren Kommunen längst unterwegs und es werden auch entsprechende Regelungen für Verwaltungsaufwand gefunden werden.

BE **Clemens Binninger** (CDU/CSU): Eine kurze Nachfrage von mir: Die Kosten sind kein Faktor, wirklich keiner, das haben wir jetzt gehört, obwohl es immer wieder behauptet wird. Gehen Sie eher im Gegenteil, wenn die Dinge dann etabliert sind, und ja in der Behörde, in der Kommune, in der Verwaltung weniger kuvertiert und ausgedruckt werden muss, von einer auf mittlerer Sicht zumindest realen spürbaren Entlastungswirkung aus? Ganz banal beim Porto beginnend bis hin, dass es schneller geht.

SV **Dr. Helmut Fogt** (Deutscher Städtetag, Berlin): Selbstverständlich erwarten wir uns Verwaltungsentlastungen. Wir haben natürlich den Tatbestand, dass auch bei der Verbreitung, die das Internet in der Bevölkerung gefunden hat, wir einen Teil der

Bevölkerung auch perspektivisch weiter im konventionellen Sinne als Verwaltung betreuen müssen, und insofern entsteht auch in Teilen ein Doppelaufwand. Aber jede Bürgerin und jeder Bürger, die/der online rasch und schnell, auch für die Verwaltung schnell und einfach, mit uns Verwaltungsprozesse abwickeln kann, ist eine Entlastung für konventionelle Verwaltungsverfahren und wirkt sich perspektivisch auch finanziell entlastend aus.

Stv. Vors. **Frank Hofmann (Volkach)**: Vielen Dank. Herr Dankert, bitte.

SV **Reinhard Dankert** (Der Landesbeauftragte für den Datenschutz Mecklenburg-Vorpommern, Schwerin): Eine kurze Antwort auf Ihre knappe Frage. Vermutlich beziehen Sie sich auf den Satz: „Ein Ende-zu-Ende-Verschlüsselungsverfahren müssen Sie anbieten.“ Das impliziert ein bisschen, dass wenigstens eines angeboten muss. Das Ganze steht im Zusammenhang mit dem Satz im vorletzten Absatz: „Faktisch und technisch stellen diese Vorgehensweise jedoch keine Ende-zu-Ende-Sicherheit her“. Das heißt, wir wollen, dass ein wirkliches Ende-zu-Ende-Verschlüsselungsverfahren – das müssen Sie sich jetzt einmal denken – angeboten wird. Wir glauben, dass das technisch möglich ist und die De-Mail-Anbieter nicht groß überfordern dürfte. Wie kompliziert das dann wird, wenn man das jetzige De-Mail-Verfahren datenschutzgerecht anwenden will, zeigt die aktuelle Handreichung des Kollegen Peter Schaar und seiner Behörde zum datenschutzgerechten Umgang mit besonders schützenswerten Daten beim Versand mittels De-Mail vom 1. März 2013, was ich Ihnen freundlicherweise mit in die Unterlagen gelegt habe. Da sehen Sie, wie schwierig es ist, wenn man sich tatsächlich sicherheitsgerecht verhalten will, vielleicht nicht ganz so, wie das der Chaos Computer Club fordert und wir fordern, aber wir sind schon sicher, dass das die Mehrheiten sind. Da muss man nicht drum herum diskutieren.

BE **Clemens Binninger** (CDU/CSU): Was macht Sie so sicher, dass Sie sich mit dieser doch aufwändigeren Technik anders als in vergleichbaren Fällen – Stichwort Signatur ist ja ein paar Mal gefallen, die sich in 15 Jahren nicht durchsetzen konnte –, durchsetzen? Wir können den Bürger nicht vergattern. Wenn er das nicht anwendet, dann wendet er es nicht an, und dann ist das alles für die Katz. Was macht Sie so sicher, dass Sie mit Ihrem komplizierterem Verfahren dann auf einmal die Masse der Bürger erreichen?

SV **Reinhard Dankert** (Der Landesbeauftragte für den Datenschutz Mecklenburg-Vorpommern, Schwerin): Das muss für den Bürger seitens der De-Mail-Anbieter sehr komfortabel gemacht werden. Das ist genau der Punkt. Das ist bisher nicht passiert. Wenn Sie einen neuen Personalausweis mit der ganzen Funktion nutzen wollen, also mit den ganzen Signaturen, dann ist das viel zu kompliziert für

den Bürger. Es muss das gesamte Verfahren implementiert werden, und dann wird es richtig rund und wird dann auch angenommen.

Stv. Vors. **Frank Hofmann (Volkach)**: Herr Dr. Rohleder, bitte.

SV **Dr. Bernhard Rohleder** (Hauptgeschäftsführer, BITKOM, Berlin): Zu den Briefsendungen: Es werden in Deutschland etwa 70 Mio. Briefe am Tag und 25 Mrd. im Jahr verschickt. Davon sind 4 Mio. nicht zustellbar. Auch da haben wir ein kleines Sicherheitsthema, um das sich überhaupt niemand kümmert – 4 Mio. jedes Jahr. Das meiste sind Massensendungen, das wenigste sind Urlaubsgrüße oder private Briefe. Es geht um Schreiben von Versicherungen, um die Lohn- und Gehaltsabrechnung oder ähnliche Dinge, und es geht auch um Werbebriefe. Wie viel davon genau dann zu De-Mail oder zum E-Post Brief abwandern wird, das lässt sich nicht sagen. Es hängt davon ab, ob wir das System zu einem Hindernisparcours umbauen, oder ob wir es sehr einfach nutzbar machen auf das Sicherheitsniveau, das wir jetzt haben. Das können 50 % sein, möglicherweise 60 % oder 70 %, vielleicht auch nur 30 % oder 2 %, wenn wir es ganz kompliziert machen. An der Stelle gibt es auch eine ganz andere Frage, nämlich die der Nachhaltigkeit der Kommunikation, wo die Umweltbelastungen, die aus dem Papierversand von Briefen entstehen, ganz andere sind als die, die aus dem elektronischen Versand entstehen.

Stv. Vors. **Frank Hofmann (Volkach)**: Vielen Dank! Gerold Reichenbach für die SPD-Fraktion, bitte.

BE **Gerold Reichenbach** (SPD): Ich habe Fragen zu drei Komplexen. Einmal die Frage der Kosten an Sie, Herr Dr. Fogt. Es geht durch den Schriftlichkeitsersatz nicht nur darum, einen E-Mail-Account einzurichten und erreichbar zu sein, sondern Sie müssen die jeweiligen unterschiedlichen Aufbewahrungsfristen, die wir auch für rechtsverbindliche Vorgänge gegenüber der Verwaltung haben, entsprechend digital umstellen. Deswegen meine Frage an Sie: Haben Sie einen Überblick, welche Kosten entstehen, dass ich entsprechende elektronische Archivierung für die dann per De-Mail elektronisch durchgeführte Verwaltungskommunikation brauche? Sie können ja nicht sagen, ich drucke die E-Mail, die per De-Mail kam, aus und hefte sie ab, dann fehlt in der Signatur der Schriftlichkeitsersatz, d. h., Sie brauchen ein Archivierungssystem. Die erste Frage, welche Kosten durch Anlegung der Archivierungssysteme bei den Kommunen entstehen, an Dr. Fogt, weil das etwas ist, was bei den Kommunen aufläuft.

Die zweite Frage: Welche Kosten und welche Verfahren sind überhaupt vonseiten der Kommunen anwendbar, um dann Löschungsfristen einzuhalten, und zwar durch Löschungen, die konform dem Bundesdatenschutzgesetz sind, also eine endgültige Löschung der Daten und nicht nur eine Löschung der Verzeichnisse?

Das waren die beiden Fragen der Kosten, die an Herrn Dr. Fogt gehen.

Die nächste Frage, weil darauf ein bisschen fokussiert wird, war die Frage der Sicherheitslücke bei De-Mail. Wir haben es mit einem Artikelgesetz zu tun, d. h., wir ändern auch das De-Mail-Gesetz im Bereich des § 5 De-Mail-G. In dem Zusammenhang wird das De-Mail-G dahin geändert, dass bei der Übermittlung von Sozialdaten und später noch einmal an anderer Stelle beim Thema Finanzdaten, die Entschlüsselung des Überprüfens auf Schadsoftware und die Wiederverschlüsselung bei den Providern, wenn ich Sie richtig verstanden habe, Herr Neumann, war das die Sicherheitslücke, die Sie angesprochen haben, nicht mehr als Übermittlung gilt. Da schließen sich zwei Fragen an, einmal an Herrn Dankert: Welche Auswirkungen hat diese Wegdefinition dieses Vorgangs aus dem Übermittlungsfaktor im De-Mail-G nicht nur auf die Kommunikation zwischen Bürger und Verwaltung, sondern auch auf andere Kommunikationsvorgänge, etwa die zwischen Versicherern und Versicherten bei der Übermittlung von Sozial- oder Gesundheitsdaten? Würde das heißen, dass dann nicht nur an der Stelle die Kommunikation zwischen Staat und Bürger, sondern auch die Kommunikation zwischen Bürger und seinen Versicherungen über seine Sozial- und Krankheitsdaten oder Sonstiges dann auch über diese „wegdefinierte“ Sicherheitslücke gängig gemacht werden könnte?

Meine nächste Frage geht an Herrn Neumann: Ist die Änderung im De-Mail-G, die vorgenommen worden ist, ein Sicherheitsgewinn und machen wir dadurch De-Mail sicherer, oder definieren wir einfach gesetzlich ein „Loch in der Wand“ weg?

Die anschließende zweite Frage: Es wurde ja wieder gesagt, im normalen Verkehr wird das auch alles relativ unsicher gemacht. Ist die Sicherheitslücke, die dadurch entstehen könnte, dass ich innerhalb eines kurzen Zeitraumes elektronisch Millionen von Daten abgreifen kann, vergleichbar mit der Sicherheitslücke, dass ich Millionen von Akten und Gesundheitsdaten im analogen Bereich aus den Tresoren und Aktenarchiven der Gemeinden und der Versicherungen entwenden kann?

Meine dritte Frage geht an Herrn Prof. Müller-Terpitz. Sie haben die europarechtlichen Fragen angesprochen. Wir haben in vielen Verordnungen Richtlinien des Prinzips des „One-Stop-Shop“, wo ich mit einer Verwaltung bestimmte Zulassungsverfahren u. ä. im europäischen Wettbewerbsbereich durchführen kann. Halten Sie die Festlegung auf den De-Mail Standard im Behördenverkehr vor dem Hintergrund der europäischen Wettbewerbsgleichheit überhaupt für europarechtlich konform? Oder kann es uns passieren, dass bei der ersten Klage eines polnischen oder sonstigen Anbieters vor dem Europäischen Gerichtshof (EuGH), der sagt, ich möchte genau so wie meine deutschen Kollegen meinen nationalen Standard innerhalb des europäischen Rechtsverkehrs nutzen können, dieser dann erfolgreich ist und wir an der Stelle sozusagen „mit Zitronen gehandelt haben“?

Stv. Vors. **Frank Hofmann (Volkach)**: Vielen Dank, Herr Reichenbach. Herr Dr. Fogt, bitte.

SV **Dr. Helmut Fogt** (Deutscher Städtetag, Berlin): Herr Reichenbach, zum von Ihnen angesprochenen Thema Aufbewahrungs- und Löschungsfristen und veränderte Bedingungen: Wenn man all dieses elektronisch abbildet, ich glaube nicht, dass das die Kommunen besonders beschwert. Wir müssen uns vor Augen halten, dass wir von der Papierverwaltung wegwollen. Wir haben in Deutschland eine Vielzahl von Städten und Gemeinden, die Dokumentenmanagementsysteme einführen oder einführen wollen, mit Kostenansätzen, die sich durchaus zunächst beträchtlich auswirken. Aber dabei soll der gesamte Verwaltungsprozess vom Eingang bis zur Archivierung elektronisch organisiert und abgebildet werden. Aufbewahrung und Löschung sind da nur ein kleiner Baustein am Ende der Kette. Wenn ich diesen Baustein zu dem, was uns Papierverwaltung, Archivierung und Löschung heute kosten, in Relation setze, steht das in gar keinem Verhältnis mehr. Sie brauchen viel Platz und Personal, um den heutigen gesetzlichen Vorschriften für Archivierung und Löschung von Akten und Daten gerecht zu werden. Dagegen löst der elektronische Vorgang mit hoher Sicherheit nur einen Bruchteil an Kosten aus.

Stv. Vors. **Frank Hofmann (Volkach)**: Herr Reichenbach hat eine Nachfrage.

BE **Gerold Reichenbach** (SPD): Glauben Sie das jetzt, oder ist es erhoben worden? Ich bin deswegen überrascht, weil sowohl die Regierung in ihrer Gesetzesbegründung als auch das Statistische Bundesamt, bezogen auf die Einwände des Bundesrates, beide gesagt haben: Die Kosten für diesen Bereich lassen sich bisher noch nicht abschätzen. … Dann hätte drin gestanden „unerheblich“, Herr Kollege Binninger.

Stv. Vors. **Frank Hofmann (Volkach)**: Herr Dr. Fogt, Sie haben das Wort.

SV **Dr. Helmut Fogt** (Deutscher Städtetag, Berlin): Was wir haben, sind Zahlenangaben, z. B. für den Gesamtbaustein Dokumentenmanagementsysteme in großen Städten. So etwas gibt es auch für kleinere Städte, bis zu den Gemeinden hinunter. Dann kann man daraus errechnen, wie hoch der Anteil Archivierung und Löschung etc. am Ende des Vorgangs ist. Das müsste man bundesweit hochrechnen. Ich nehme an, dabei wird kein Betrag herauskommen, der insgesamt sehr beachtlich sein wird, vor allem in Relation zu den Ersparnissen an Aufwand, die ich bei konventioneller Aktenführung heute habe. Sie müssen sich Registraturen vorstellen und den Platz dafür. Ich gehe davon aus, dass die Miete oder die Gebäudekosten für die Archivierung bei Tausenden von Mitarbeitern in einer Kommunalverwaltung höher sind, als das, was wir an Umstellungsaufwand konkret haben würden.

Stv. Vors. **Frank Hofmann (Volkach)**: Ich danke Ihnen, Herr Dr. Fogt. Herr Dankert, bitte.

SV **Reinhard Dankert** (Der Landesbeauftragte für den Datenschutz Mecklenburg-Vorpommern, Schwerin): Sozial- und Gesundheitsdaten erfordern naturgemäß ein sehr hohes Schutzniveau und das ist technisch nur mit einer Ende-zu-Ende-Verschlüsselung zu machen. Einen anderen Standpunkt haben wir nicht dazu.

Stv. Vors. **Frank Hofmann (Volkach)**: Vielen Dank!

BE **Gerold Reichenbach** (SPD): Darf ich noch einmal nachfragen: Was bedeutet die gesetzliche Regelung, wenn ich die Entschlüsselung aus dem Übermittlungsvorgang juristisch-systematisch herausnehme?

SV **Reinhard Dankert** (Der Landesbeauftragte für den Datenschutz Mecklenburg-Vorpommern, Schwerin): Für Techniker bedeutet das Unsicherheit per Gesetz.

Stv. Vors. **Frank Hofmann (Volkach)**: Vielen Dank! Herr Neumann, bitte.

SV **Linus Neumann** (Chaos Computer Club, Berlin): Bei der ersten Frage geht es um die Gesetzesänderung, bei der für De-Mail eine Ausnahmeregelung für die kurzzeitige automatische Entschlüsselung bei De-Mail geschaffen werden soll. Dadurch wird nicht die Sicherheit erhöht, ganz im Gegenteil. Ich interpretiere diesen Paragraphen so, dass damit explizit der Straftatbestand *[Zwischenruf: Nachfrage nach dem Paragraphen]*… es geht hier um Art. 7 Abs. 2 zur Änderung der Abgabenordnung. Ich kann noch einmal kurz vorlesen: „Dem Absatz 1 wird folgender Satz hinzugefügt: ‚Die kurzzeitige automatisierte Entschlüsselung, die beim Versenden einer De-Mail Nachricht durch den akkreditierten Diensteanbieter zum Zweck der Überprüfung auf Schadsoftware und zum Zweck der Weiterleitung an den Adressaten der De-Mail-Nachricht erfolgt, verstößt nicht gegen das Verschlüsselungsgebot des Satzes 3.‘“ Das heißt, hier wird eine definierte Ausnahmeregelung geschaffen und dient nach meiner Interpretation dem Zweck, an dieser Stelle den Vorwurf des eventuellen Falles des Geheimnisverrates aus dem Wege zu räumen, der beim Verstoß gegen den Satz 3 dann nämlich zur Anwendung käme. Hier wird eine explizite Ausnahmeregelung geschaffen, die den Unzulänglichkeiten des De-Mail-Systems Rechnung trägt und daher die Sicherheit explizit senkt.

Die zweite Frage betrifft die Vergleichbarkeit dieser Sicherheitsschwäche auf den Servern mit dem Entwenden von Daten aus dem Tresor der Verwaltung. Hierzu ist festzustellen, dass, wenn der De-Mail-Standard vernünftig eingehalten wird, durch eine persistente Infektion auf dem Server immer nur laufende Kommunikation abzuschöpfen ist. Das heißt, man könnte sich das wie eine Kamera am Eingang dieses

Tresors vorstellen, durch die jedes Dokument gescannt wird. Bei vernünftigen Sicherheitsvorkehrungen, wie ich sie da definiert sehe, sollte allerdings eine nachwirkende Extraktion nicht möglich sein. Das ist allerdings bei heutigen E-Mail-Systemen ebenso der Fall. Wenn ich einmal kurz noch auf die eingebrachten Argumente eingehen darf: Das wichtigste Argument war, dass die Ende-zu-Ende-Verschlüsselung als Option angeboten wird. Diese Option haben wir als E-Mail-Nutzer seit genau 22 Jahren – seit 1991. Diese Option findet in der Wirtschaft beinahe flächendeckend Anwendung. Bei den kleineren und mittelständischen Unternehmen nicht. Bei den Dax-Unternehmen ist das absolut „Best Practice“, auf eine Ende-zu-Ende-Verschlüsselung zu setzen. Das Verfahren, was zur Anwendung kommt, nennt sich S/MIME und ist auch in der Bedienbarkeit besonders einfach. Deshalb hat es sich auch gegen den früheren Standard PGP gerade in der Unternehmenskommunikation so gut durchgesetzt. Bei Privatpersonen ist das nicht der Fall. Das liegt vor allem daran, dass es an einer zentralen Authority fehlt, die diese Zertifikate, die zur Verschlüsselung zum Einsatz kommen, auch signiert. Das wäre genau die Position, die hier die Bundesregierung einnehmen könnte, wenn sie Ende-zu-Ende-Verschlüsselung zum Standard erhebt. Das wäre der einzige Zugewinn, den eine De-Mail zum aktuellen Stand bei E-Mail hat. Wir wissen, bei Privatanwendern findet Ende-zu-Ende-Verschlüsselung hauptsächlich bei besonders paranoiden oder eben kriminellen Anwendung. In der Wirtschaft jedoch auf jeden Fall.

Die vierte Kategorie, die Regierung. Sie erheben den Standard, der aktuell bei sicheren E-Mail-Systemen existiert, und definieren ihn als sicheren Standard für die Zukunft. Sie müssen sich aber, wenn Sie ein neues System erstellen, von den existierenden Standards abgrenzen, um überhaupt eine Rechtfertigung für dieses System zu haben. Das ist momentan nicht der Fall. Das zweite Argument ist die Bedienbarkeit, da wurde auch von Herrn Binninger angebracht, dass Ende-zu-Ende-Verschlüsselung eine zusätzliche Komponente verlangt. Das ist bei E-Mail der Fall, ja, ich muss erst einmal drei oder vier Klicks zusätzlich machen mit meinem E-Mail-Programm, wenn ich S/MIME nutzen möchte. Dieses Argument entfällt, wenn Sie das automatisch in den De-Mail-Setup-Prozess mit aufnehmen. Aus diesem Grund plädiere ich dafür, dass Ende-zu-Ende-Verschlüsselung nicht eine Option sein soll, die dann eine erhöhte Bedienbarkeitshürde stellt, indem noch die Ende-zu-Ende-Verschlüsselung eingerichtet werden muss, sondern dass sie zum Standard wird beim einmaligen Aufsetzungsprozess – Ende-zu-Ende-Verschlüsselung. Zwei Klicks mehr, und das Thema ist erledigt. Sie haben dann einen riesigen Zugewinn an Sicherheit.

Drittens: Kurzzeitige Entschlüsselung geschieht aus zwei Gründen – eine Entschlüsselung, egal ob kurz- oder langfristig, wenn es einmal entschlüsselt ist, habe ich den Plaintext. Der erste Grund ist die Überprüfung auf Schadsoftware, das ist ein hehres Anliegen. Sie wollen vermeiden, dass über De-Mail Vireninfektionen von Bürgern stattfinden. Das ist ein absolut schönes Ziel. Sehen wir uns einmal an,

wie Schadsoftware heute verbreitet wird. Wir haben einmal die Massenangriffe, das sind Spams per E-Mail, die an viele Menschen gehen und wo es dem Angreifer hauptsächlich darum geht, eine hohe Anzahl an Geräten zu infizieren. Diese Schadsoftware wird von Virenscannern in der Regel innerhalb von wenigen Stunden nach dem ersten Auftreffen erkannt. Das heißt, vor genau dieser Masseninfektion können Sie die Bürger mit einem automatisierten Virenscannen schützen. Jetzt ist es aber so, dass das Versenden einer De-Mail Geld kostet und ich den Absender-Account auf meinen persönlichen Namen registriere, d. h. für eine Masseninfektion eignet sich das Kommunikationsmedium De-Mail nicht. Wenn ich Leute massenhaft infizieren möchte, werde ich weiterhin auf E-Mail setzen.

Die zweite Klasse von Schadsoftware ist die gezielte Infektion einer spezifischen Person, von der ich besondere Unterlagen haben möchte. Das heißt, ich mache eine maßgeschneiderte Software, mit der ich Personen angreife, eine, die nicht für die Masseninfektion geeignet ist. Menschen, die in der Lage sind, so etwas zu bauen, sind auch in der Lage, sich z. B. Zugang zum De-Mail-Konto einer anderen Person zu verschaffen und dann damit ihre gezielte Infektion vorzunehmen. Dagegen sind Sie mit einem Virenscannen machtlos. Um das zu verdeutlichen: Ich infiziere bspw. einen Rechner über E-Mail und schicke dann über den infizierten Rechner eine De-Mail mit einer Schadsoftware an eine andere Person. Das heißt, die Überprüfung der Schadsoftware ist letztendlich eine Augenwischerei, Sie können den Bürger nicht von der Notwendigkeit befreien, seinen Rechner selber von Schadsoftware freizuhalten. Insbesondere wenn er gleichzeitig E-Mails nutzt oder Dateien aus dem Internet herunterlädt. Da können Sie keinen Zusatz an Sicherheit leisten durch das Prüfen auf Schadsoftware.

Ein viertes Argument, was ich sehe, ist die Entschlüsselung der Nachricht zum Zwecke der Weiterleitung. Hierzu ist technisch anzumerken, dass es keine technische Notwendigkeit gibt für das Entschlüsseln des Nachrichteninhalts zum Zwecke der Weiterleitung. Die Systeme, die wir seit 20 Jahren zur E-Mail Verschlüsselung Ende-zu-Ende nutzen, erfordern dies ebenso wenig. Sie können sich das wie einen Briefumschlag vorstellen. Der Postbote muss meinen Brief nicht öffnen, um auf den Umschlag zu sehen und festzustellen, wo er diesen Brief hintragen soll. „End-to-End-Encryption“ als Standard definieren und nicht als Option. Nur so können Sie einen Zusatzgewinn zu dem schaffen, was Sie bei E-Mail kritisieren und was Sie eigentlich als Rechtfertigung für den gesamten De-Mail an Aufwand hier heranziehen.

Stv. Vors. **Frank Hofmann (Volkach)**: Vielen Dank, Herr Neumann. Herr Prof. Müller-Terpitz, bitte.

SV **Professor Dr. Ralf Müller-Terpitz** (Universität Passau): Es ging um die Frage der Europarechtskonformität des De-Mail-Gesetzes. Ich möchte Sie nicht erschrecken, aber das wird im Schrifttum diskutiert, von Wenigen als Frage

aufgeworfen, allerdings nicht beantwortet. Sie wollen von mir eine Antwort, ich würde sagen: nein. Wir haben hier zwar eine Beeinträchtigung der Dienstleistungsfreiheit, so gesehen eine Binnenmarktrelevanz; die scheint mir aber gerechtfertigt zu sein dadurch, dass man für die Bürger ein Instrument zur sicheren Kommunikation schaffen will und es noch keine Alternative gibt. Von daher würde ich dahin tendieren zu sagen, europarechtskonform ist es im Moment – zumal wir auch in § 19 De-Mail-G die Möglichkeit haben, dass sich ausländische Provider im Inland akkreditieren können. Ich denke, da ist man rechtlich auf einer sicheren Basis. Mein Punkt ist ein anderer, er ist derjenige, dass die EU bestrebt ist, grenzüberschreitende Standards zu etablieren. Wenn man das Gesetz eng definiert, so wie es im Moment vorgesehen ist, dann müsste man an diesen Punkt in zwei bis fünf Jahren wieder heran. Den Zeitpunkt kennt keiner, er ist ungewiss. Deswegen würde ich es jetzt schon in das Gesetz mit einbauen.

BE **Gerold Reichenbach** (SPD): Die Frage ist nicht beantwortet, die Frage war: Ob die Eröffnung bei Behörden nur durch den De-Mail Zugang nicht eine Wettbewerbsbeschränkung ist, weil ein ausländisches Unternehmen, das mit deutschen Behörden Schriftverkehr hat, sagen könnte, ich bestehe darauf, meinen eigenen nationalen Standard zu nehmen.

*Einwurf BE **Dr. Konstantin von Notz**: Sechs Fragen und sechs Nachfragen, das kann wohl nicht sein.*

SV **Professor Dr. Ralf Müller-Terpitz** (Universität Passau): Entschuldigung, dann habe ich Sie falsch verstanden. Das würde ich aus den genannten Gründen auch noch für europarechtskonform halten. Es ist eine Beeinträchtigung, aber sie ist im Moment noch legitimiert.

Stv. Vors. **Frank Hofmann (Volkach)**: Herr von Notz, ich würde bei Ihnen auch eine Nachfrage zulassen, wenn sie so wie hier jetzt gestellt ist. Es war notwendig. Herr Höferlin, bitte.

BE **Manuel Höferlin** (FDP): Auch wiederholtes Nachfragen führt manchmal nicht zur erwünschten Antwort. Ich habe interessiert festgestellt, dass ein Großteil der Sachverständigen mehr über das De-Mail-G spricht, obwohl das nur ein kleiner Teil des EGovG ist. Deshalb stelle ich jetzt erst einmal zwei Fragen über E-Government. Ich komme, weil das Interesse so groß ist, doch noch zu De-Mail und werde konkret nachfragen, auch wenn es dann vielleicht technisch wird.

Herr Dr. Rohleder, Sie haben gesagt, die Wirtschaft fordert es und Sie von Ihrer Seite aus freuen sich, dass es jetzt passiert, denn es sei längst überfällig. Was glauben Sie, ist ein gemeinsamer Standard, wie man damit kommuniziert, Behörden, Kunden, Unternehmen untereinander kommunizieren, halten Sie es für richtig, dass man dort

Standards definiert, auf die aufgebaut werden kann und neben denen es auch noch anderes Standards geben kann? Ist das eine Art und Weise, wie man Rahmenbedingungen schaffen kann und sollte?

Herr Stocksmeier, Sie hatten gesagt, es gäbe neben dem mittleren Sicherheitsniveau der De-Mail auch die Option, weiteres Sicherheitsniveau aufzubauen. Als wir De-Mail angehört und auch verabschiedet haben, haben wir immer gesagt: Ende-zu-Ende-Verschlüsselung mit De-Mail ist möglich. Wir haben auch den Verzeichnisdienst, den die Provider vorhalten müssen, genannt. Können Sie sagen, wo Sie Anwendungsgebiete sehen, wo dann ein höherer Standard vielleicht zusätzlich stattfinden kann und sollte?

Beim Thema Ende-zu-Ende-Verschlüsselung wurde viel auch von der S/MIME-Verschlüsselung gesprochen. Herr Dr. Fogt, können Sie uns sagen, wie viele Behörden derzeit in der Lage sind, S/MIME nicht nur zu ver- und entschlüsseln, oder wie viele es auch praktizieren – wenn sie E-Mails rausschicken – sie zu signieren, das wäre ja die Vorstufe der Ende-zu-Ende-Verschlüsselung? Wie viele Behörden in Deutschland signieren ihre ausgehenden E-Mails, damit sie wenigstens wissen, dass die E-Mail, die versendet wurde, nicht auf dem Weg verändert wurde? Was machen die Kommunen und Behörden vor Ort mit Verschlüsselung? Kann ich derzeit mit S/MIME verschlüsselte E-Mails zu Behörden schicken? Ich habe noch nie eine Behörde nach ihrem S/MIME-Schlüssel gefragt, das könnte ich ja einmal tun. Was würden Sie sagen, wenn wir den Behörden und den Verwaltungen insgesamt sagen würden, Ihr müsst Euch jetzt flächendeckend S/MIME-Zertifikate zulegen, damit das flächendeckend funktioniert?

Herr Neumann, an Sie geht meine nächste Frage. Sie reden vom S/MIME-Zertifikat so, dass das eine Ende-zu-Ende-Verschlüsselung ist. Die Frage technisch: Wie soll das funktionieren, wenn De-Mail gerade auch in der Verwaltung so gedacht ist, dass man ortsunabhängig von verschiedenen Endgeräten auch über Web-Oberflächen hinaus auf seine Daten zugreifen kann? Können Sie uns da technisch etwas aufklären? Wo muss da der private Schlüssel liegen? Liegt er dann noch beim Bürger und Kunden, oder ist es nicht vielmehr so, dass der private Schlüssel, um den es dann letztlich geht, doch wieder beim Provider liegt? Wenn ich nämlich Mobilität und Flexibilität im Empfang dieser Nachrichten haben will, führt kein Weg daran vorbei, dass ich den privaten Schlüssel, der die Sicherheit gewährleistet, doch wieder zum Provider lege. Da gibt es vielleicht weitere Sicherungsmechanismen, dass der private Schlüssel nicht abgefangen werden kann. Ziel war ja gerade, dass man diese Nachrichten eben nicht nur auf seinem PC, sondern auch im Urlaub von anderen Rechnern aus empfangen kann. Beim Thema Weiterleitung, weil Sie gesagt haben, das sei ja völlig überflüssig, möchte ich daran erinnern, dass wir im De-Mail-G Vertreterregelungen eingebaut haben. Wenn wir De-Mails an einen Empfänger schicken und der einen Vertreter definiert, hilft das nicht wirklich, wenn der Vertreter

dann die E-Mail nicht lesen kann, weil sie Ende-zu-Ende verschlüsselt wurde für den ursprünglichen Empfänger. Das ist nicht Sinn und Zweck der De-Mail gewesen. Sie haben das mit dem Briefumschlag verglichen. Aber was Sie wollen, ist eine Verschlüsselung des Inhalts. Sie haben gesagt, der Postbote braucht auch nicht den Brief aufzumachen, wenn er ihn weiterschickt. Da ist aber genau der Unterschied. Bei der De-Mail reden wir von Transportverschlüsselung, also vom Umschlag. Sie verlangen eine S/MIME Verschlüsselung, das ist eine Verschlüsselung des Inhalts.

Stv. Vors. **Frank Hofmann (Volkach)**: Vielen Dank, Herr Höferlin. Herr Dr. Rohleder, bitte.

SV **Dr. Bernhard Rohleder** (Hauptgeschäftsführer, BITKOM, Berlin): Ich würde jetzt lieber, als die Frage von Herrn Höferlin zu beantworten, zu einer 10-minütigen Replik auf die Einlassung von Herrn Neumann ausweichen. Herr Höferlin, Standards haben herausragende Bedeutung für die Verbreitung von Technologien, gerade in unserer Branche. Das ist das eine, und dazu ist die De-Mail als offener Standard besonders gut geeignet. Das kann von jedem, der es kann, auch entsprechend eingesetzt und in eigene Produkte umgesetzt werden. Das ist erstens bei einem solchen Massenprodukt schon herausragend. Zweitens, die Technologien müssen auch einfach zu nutzen sein. Darum geht es. Das ist die Lektion, die wir aus den letzten 15 Jahren gelernt haben. Insofern habe ich das Gefühl, die Diskussion geht ein wenig in eine andere Richtung. Wenn wir im Jahr 1997 wären und würden das KDG vor uns haben, mit dem ich mich damals schon beschäftigt habe, dann würde ich das verstehen. Aber ich verstehe es heute nicht. Das Ganze muss „easy to use“ sein, es muss jeder nutzen können, ohne sich groß mit irgendetwas auseinandersetzen zu müssen. Ich denke, da liefert der De-Mail Standard eine herausragend gute Basis.

Stv. Vors. **Frank Hofmann (Volkach)**: Herr Stocksmeier, bitte.

SV **Dirk Stocksmeier** (Vorstandsvorsitzender der]init[AG, Berlin): Herr Neumann, Sie hatten ja schon darauf hingewiesen, dass Business-User und Privat-User mit den Mailtechnologien ganz anders umgehen. Es hat ja auch Gründe, warum ein Privat-User vielleicht eine komplexe Technologie nicht auf seinem PC installieren möchte. Große Unternehmen verfügen über komplexe Firewall-Infrastrukturen, haben zentrale Viruserkennungssysteme etc. Das sieht auf dem heimischen PC nicht zwingend identisch aus. Dort ist vielleicht keine so leistungsstarke Firewall installiert, und auch die Viruserkennung ist nicht zwingend immer auf dem neuesten Stand. Insofern liefert die De-Mail Infrastruktur an dieser Stelle einen ganz wichtigen Sicherheitsbeitrag. Gerade für den Bürger, der einen nicht so sicheren PC hat oder sich nicht ganz sicher ist, ob er alle Voraussetzungen getroffen hat. IN diesem Fall ist es auch nützlich, selbst wenn man eine Viruserkennung auf dem eigenen PC hat –, wenn der Provider dies noch durch ein weiteres Verfahren zur Viruserkennung ergänzt. Ich möchte noch einmal beim Schlüsselmanagement ansetzen: Wenn der

heimische PC nicht so sicher ist, dass man den Schlüssel als Software installieren möchte, kann man alternativ eine Hardwarelösung nehmen, bei der der Schlüssel in einer Smartcard abgelegt ist. Dies würde aber wiederum eine zusätzliche Investition auf Seite der Anwender bedeuten. Das heißt, im Ergebnis werden vielleicht viele Anwender sagen, sie wünschen sich eher eine sichere De-Mail-Übertragung als all die Investitionen selber zu tätigen, um für den PC zu Hause die gleiche Sicherheitsinfrastruktur zu schaffen, wie das in einem Unternehmen möglich ist.

BE **Manuel Höferlin** (FDP): Geht es dann bei mobilen Anwendungen?

SV **Dirk Stocksmeier** (Vorstandsvorsitzender der]init[AG, Berlin): Bei mobilen Anwendungen ist das sicher nicht einfacher. Eine bessere Lösung wäre, wenn ein Kryptoprozessor im Mobilgerät integriert ist, als wenn man noch eine zusätzliche Smartcard verwenden muss. Aber insgesamt und so haben Sie es auch dargestellt: Der Privatbürger nutzt seit vielen Jahren noch nicht die Ende-zu-Ende-Verschlüsselung und das hat seine Gründe. Diesem Umstand wird mit der De-Mail an entscheidenden Punkten entsprochen. Auch wenn nicht das identische Niveau erreicht wird, wie wenn man eine vollständige Sicherheitsinfrastruktur auf dem heimischen PC installiert hat, die alle Komponenten einer Verschlüsselung von einem bis zum anderen Ende enthält.

Zum Thema, welche Verfahren einer Ende-zu-Ende-Verschlüsselung bedürfen, gibt es keine pauschalen Aussagen. Es besteht ja auch auf der Seite des Verfahrensverantwortlichen die Aufgabe, jeweils eine Schutzbedarfsfeststellung durchzuführen und zu prüfen, ob die Grenze, ab der die von De-Mail angebotenen Sicherheitsmechanismen nicht mehr ausreichen, überschritten wird - das ist die eine Hälfte der Medaille. Die andere Hälfte ist das, was sich die Bürger wünschen: Hier sollte man die Anforderungen auch von gesetzgeberischer Seite nicht unnötig hoch setzen, sondern denjenigen, die bevorzugen, die Dinge digital zu erhalten, auch die Möglichkeit zu geben, selbst darüber zu bestimmen, ob sie einen Zugang über De-Mail aktivieren möchten.

Stv. Vors. **Frank Hofmann (Volkach)**: Herr Dr. Fogt, bitte.

SV **Dr. Helmut Fogt** (Deutscher Städtetag, Berlin): Herr Höferlin, auf die Frage des Einsatzes bisheriger Mittel in der kommunalen Verwaltung kann ich Ihnen nur sagen, dass die qualifizierte elektronische Signatur fast nur im Bereich der sog. Power-User bisher zum Einsatz gekommen ist. Das sind Architektenbüros oder Notare, Anwälte usw. die einen regelmäßigen Austausch mit der Verwaltung pflegen. Ich kann nicht genau sagen, wie der Prozentsatz von Städten und Gemeinden ist, die entsprechend aufgestellt sind, um mit diesen Power-Usern einschließlich qualifizierter elektronischer Signatur zu kommunizieren. Aber der springende Punkt für mich ist der, dass es bei diesen Power-Usern geblieben ist. Ich beobachte auch heute hier wieder eine

ähnliche Diskussion, wie wir sie seinerzeit im Vorfeld der Einführung der qualifizierten elektronischen Signatur hatten. Am Schluss waren die Techniker, die Sicherheitsleute und auch die Juristen zufrieden, aber es kam nicht zum Laufen. Weil der Aufwand, das haben wir uns damals auch angesehen, die technischen Vorgaben immens waren, die von den akkreditierten Anbietern zu erledigen waren. Ähnliches an Diskussion erleben wir jetzt wieder. Wir haben uns auch das angesehen. Wir halten die De-Mail und ihre Sicherheitsvorkehrungen für ausreichend. Bei den Providern musste bereits ein erheblicher Aufwand getätigt werden, um diesen Anforderungen gerecht zu werden, weil jeder Versuch gemacht worden ist, die Server entsprechend zu schützen, bis hin zur Schulung des Personals. Die technischen Aufwände sind viele Seiten lang, und es gibt Kataloge von Anforderungen, die erfüllt sind. Dass in der Hackerszene die Überzeugung besteht, es gibt keinen Server auf dieser Welt, den ich nicht knacken kann und deren Lieblingsobjekte die Geheimdienste, NASA usw. sind, das mag schon sein. Aber danach kann ich nicht einen vernünftigen Standard für einen Alltagsaustausch der Kommunikation etablieren. Die Ende-zu-Ende-Verschlüsselung hat für uns zwei große Nachteile: Das eine ist die Schlüsselverwaltung privat. Wenn Sie sehen, welche Schwierigkeiten der Privatmann heute hat, mit seinen Passwörtern zurechtzukommen, dann sehe ich nicht, wie diese Schlüsselverwaltung in einem Massengeschäft gut funktionieren kann. Das Zweite ist die Zusatzsoftware. Unsere Befürchtung ist, dass die De-Mail schon einiges an Werbung, niedrigschwelligem Angebot und Überzeugungskraft von Verwaltungsseite braucht, damit sie, so wie sie jetzt ausgestaltet ist, tatsächlich ins Laufen kommt. Wenn ich das jetzt noch mit einer Zusatzsoftware belaste, die ich brauche, dann machen wir denselben Fehler wie mit der qualifizierten elektronischen Signatur: Das Angebot wird nicht zum Laufen kommen. Wir sollten es auch nicht von Anfang an schlecht reden. Wenn ich als Bürger höre, das ist vielleicht nicht ganz sicher, das behaupten die zwar, aber das stimmt nicht, dann werde ich den beabsichtigten Werbeeffekt nicht erzielen. Im Vergleich dazu, dass der Bürger heute per völlig ungeschützter E-Mail mit seiner Verwaltung kommuniziert, halte ich die De-Mail für einen großen Fortschritt. Wir würden sehr dafür werben, nicht auf dieser Ende-zu-Ende-Verschlüsselung so lange zu insistieren, bis man zu einem angeblich perfekten Ergebnis kommt, aber dann die Schwellen so hoch gesetzt zu haben, dass wir keine Chance haben werden, daraus das Massengeschäft zu machen, das wir dringend brauchen.

Stv. Vors. **Frank Hofmann (Volkach)**: Herr Neumann, mit der Bitte um eine kurze Antwort.

SV **Linus Neumann** (Chaos Computer Club, Berlin): Erstens möchte ich sagen, dass wir nicht die Überzeugung haben, dass jedes System unsicher ist, sondern die Erfahrung. Zweitens wollte ich darauf hinweisen, dass Sie schon wieder auf den Aspekt eingegangen sind, dass eine Zusatzsoftware notwendig ist. Das ist nicht der Fall. Wenn Sie sagen, Sie wollen ein System nicht schlechtreden: Ich weiß nicht, ob

es sinnvoll ist, dieses Argument bei Sicherheit anzubringen, wenn sie einfach nicht vorhanden ist.

Zur Frage von Herrn Höferlin: Wie gehe ich damit um, wenn ich verschiedene Endgeräte habe, wo liegt der private Schlüssel, wie machen wir es mit Mobilität und Flexibilität? Sie haben mich noch einmal nach dem Beispiel S/MIME gefragt. Wenn Sie sich ein normales Smartphone ansehen, dann unterstützt das S/MIME bereits. Wenn Sie eine De-Mail-App dafür bauen, wie Sie es sicherlich irgendwann vorhaben, ist es kein Problem, dieses Verfahren zu nutzen. Sie haben sich gefragt, wie die sichere Übertragung meines S/MIME-Zertifikats von meinem Rechner auf mein Mobiltelefon passiert. Dafür wird im Schlüsselverwaltungsmodul, das in jedem Betriebssystem bereits vorhanden ist, das Zertifikat ausgewählt und gesagt, ich möchte dieses exportieren. Ich werde nach einem temporären Passwort für die Übertragung gefragt. Übertrage das Zertifikat dann auf das nächste Endgerät, gebe das Passwort ein und installiere das Zertifikat dort. Bei modernen Smartphones ist es so, dass es sich dann in einem sicheren Schlüsselspeicher befindet, bspw. beim BlackBerry oder sonst etwas, und mit dem Telefon mit gesperrt wird, so dass, wenn ich mein Telefon verliere, dieses Zertifikat nicht in fremde Hände gerät. Ich habe das technisch erklärt.

BE **Manuel Höferlin** (FDP): Und bei Web-Anwendungen?

SV **Linus Neumann** (Chaos Computer Club, Berlin): Bei Web-Anwendungen sind Sie natürlich gezwungen, dieses Zertifikat auf dem Endgerät vorzuhalten, welches Sie zum Zugriff auf Ihre E-Mails nutzen.

BE **Manuel Höferlin** (FDP): Wenn ich im Urlaub in der Türkei in einen Internetshop gehe und meine De-Mail abrufen möchte, wie geht das? Kann ich mir das praktisch so vorstellen, ich rufe mein Web-De-Postfach oder mein E-Postfach ab, wenn De-Mail zertifiziert sind oder ich rufe sonst irgendjemanden an?

SV **Linus Neumann** (Chaos Computer Club, Berlin): Es ist Ihr Ziel, in der Türkei im Urlaub in einem Internetcafe De-Mails abzuholen?

BE **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Das ist doch der Sinn der De-Mail, es geht doch um Mobilität. Ersetzen wir die Türkei durch Kiel, ein Internetcafe in Kiel.

SV **Linus Neumann** (Chaos Computer Club, Berlin): Ich frage noch einmal nach, weil der Begriff sicher nicht mehr darin vorkam. Wenn Sie sagen, es soll nicht sicher sein …

BE **Manuel Höferlin** (FDP): Meine Frage war, wie das mit dem S/MIME-Zertifikat in solchen Fällen ist und wo der private Schlüssel liegt.

SV **Linus Neumann** (Chaos Computer Club, Berlin): Wollen Sie sicher Ihre E-Mails auf einem nicht vertrauenswürdigen Gerät abholen oder nicht?

BE **Manuel Höferlin** (FDP): Die Frage ist: Wo liegt der Schlüssel bei S/MIME-Verschlüsselung, der private Schlüssel, in solchen Fällen?

Stv. Vors. **Frank Hofmann (Volkach)**: Ihr schafft es, das Ganze zu verlängern, indem Ihr Euch auch noch quer unterhaltet. Ich würde es für besser halten, wenn wir die Sachverständigen dazu hören. Herr Neumann, bitte.

SV **Linus Neumann** (Chaos Computer Club, Berlin): Ich würde jedem davon abraten, dies zu tun. Aber er wäre natürlich gezwungen, das Zertifikat in Verbindung mit diesem nicht vertrauenswürdigem Endgerät zu bringen. Das ist im Allgemeinen schon eine schlechte Idee. Aber wenn er das tun wollte, müsste er dieses Zertifikat auf dem zu nutzenden Gerät entschlüsseln und zur Anwendung bringen. Dazu sollte unter keinen Umständen irgendjemandem geraten werden.

BE **Manuel Höferlin** (FDP): Würden Sie mir recht geben, dass die zweite Alternative wäre, dass man die privaten Schlüssel beim entsprechenden Web-Provider hinterlegt? Das wäre die zweite Variante.

SV **Linus Neumann** (Chaos Computer Club, Berlin): Das ist dann leider keine Ende-zu-Ende-Verschlüsselung mehr. Ich bin allerdings noch nicht ganz mit Ihrer zweiten Frage durch. Sie wissen aus Erfahrung, Sie sind an der Regierung beteiligt, Sie kennen das System des Staatstrojaners. Das heißt, Sie sind ungefähr mit der Funktion von Trojanern vertraut und wissen, dass Sie auf einem nicht vertrauenswürdigen Endgerät ohnehin keine E-Mails entschlüsseln sollten. Die Anwendung im Internetcafe oder im Urlaub, davon ist absolut abzuraten. Gab es noch eine Frage?

BE **Manuel Höferlin** (FDP): Die Frage der Weiterleitung hatte ich noch gestellt.

SV **Linus Neumann** (Chaos Computer Club, Berlin): Da bringen Sie das Beispiel eines Briefumschlags. Ja, ich habe das Beispiel gebracht und Sie haben gesagt, das Beispiel träfe nicht zu, sondern es wäre der Fall der Übertragungsverschlüsselung. Übertragungsverschlüsselung heißt: Ich nehme meine Nachricht, sei sie verschlüsselt oder nicht, und schiebe sie durch ein dunkles Rohr zu meinem Provider. Das ist die Analogie zur Übertragungsverschlüsselung. Die Analogie ist nicht ein Briefumschlag. Ein Briefumschlag bleibt geschlossen, und zwar von meinem Verschließen bis zum Öffnen durch den Empfänger. Was wir hier haben, ist ein

dunkles Rohr von mir zu meinem Provider. Dort wird mein unverschlüsselter Brief ausgepackt, umgepackt in ein neues dunkles Rohr, wieder woanders hingeschoben und dann wieder durch ein neues dunkles Rohr geschoben. Jeder Einzelne, der an dem Schieben meines Briefes ohne Umschlag in das dunkle Rohr beteiligt ist, kann den Inhalt einsehen.

Stv. Vors. **Frank Hofmann (Volkach)**: Vielen Dank, Herr Neumann. Was hier gruppendynamisch stattfindet, finde ich sehr interessant. Trotzdem geht das Fragerecht jetzt weiter an Herrn Tempel.

BE **Frank Tempel** (DIE LINKE.): Ich versuche auch, mit der noch nach mir folgenden Fraktion der Grünen etwas solidarischer umzugehen und sie innerhalb der zwei Stunden auch noch drankommen zu lassen. Herr Neumann war so freundlich und hat viele meiner Fragen schon fleißig abgearbeitet.

Ich habe Fragen zu zwei Komplexen. Es liegt im Grund der Sache, dass zwei Experten zwei Meinungen haben, wenn unterschiedliche subjektive Blickwinkel da sind. Was völlig normal ist, das will ich nicht kritisieren. Mein erster Komplex ist noch einmal die Frage der Kommunen, und zwar an Herrn Dr. Fogt. Hier haben wir in der Expertenrunde nicht diese zwei Seiten, sondern nur ein Statement dazu, was ich durchaus respektiere. Ich habe mit Bürgermeistern und Landräten im Vorfeld dieser Anhörung telefoniert und es ist absolut zu begrüßen im Sinne einer bevölkerungs- und bürgerfreundlichen Verwaltung, auf E-Government zuzugreifen und die Möglichkeit, Flexibilität zu haben, gerade im ländlichen Raum ist das enorm wichtig und wird begrüßt. Da ist sicherlich eine einhellige Meinung da. Nicht so einhellig scheint die Meinung zu sein, was die kommunalen Finanzen in dieser Sache angeht. Sie haben beschrieben die Aktenarchivhaltung, die wegfällt, auch sehr langfristige Effekte. Langfristig kann das sogar preisgünstiger sein. Die großen Sorgen, die mir angetragen worden sind, sind die kurzfristigen Investitionen. Die Aktenführung, die bisher da ist, fällt ja nicht sofort weg und auch die Mieten fallen nicht sofort weg. Das sind Investitionsposten. Ich komme aus dem Kreistag, wo gerade mit Stimmen von SPD, FDP und CDU Investitionsmittel im IT-Bereich komplett aus dem Haushalt 2013 aufgrund der Haushaltslage gestrichen, also komplett herausgestrichen wurden. Jetzt reden wir davon, neue Systeme hineinzubringen und da sagen mir Landräte und Bürgermeister, sie haben keine Ahnung, wie sie das, was hier in Berlin beschlossen wird, umsetzen sollen. Deswegen auch noch einmal im Vergleich was die kurzfristig anstehenden Kosten zu den langfristigen Kosten betreffen würde. Ich bedauere es sehr, dass es nicht in den Unterausschuss Kommunales gegangen ist, da hätte das auch noch einmal diskutiert werden können. Ich bitte, auf diese Diskrepanz von der kommunalen Seite noch einmal einzugehen, da kamen mir große Bedenken und ich war über Ihr Statement überrascht in dieser Beziehung.

Ich komme aus dem Bereich der Kriminalpolizei, d. h. man ist häufiger aus unterschiedlichen Blickwinkeln mit derselben Sachlage befasst, wenn es um die Bewertung des Sicherheitsrisikos geht. Der Chaos Computer Club beschäftigt sich hauptsächlich mit diesen Sicherheitsrisiken und hat einen Fokus darauf. Da ist mir die Motivlage völlig klar. Deshalb meine Frage an Herrn Neumann: Sie haben beschrieben, bei den Szenarien, die anstehen würden, welche möglichen Szenarien es für den Nutzer selbst gibt und was für den Bürger passieren könnte. Mir geht es aber auch um den Bereich, was kann in der Behörde passieren und was passiert mit den Daten, die dort sind. Gibt es dabei Einfallsrisiken? Ist dasselbe Szenario, was Sie für den Bürger beschrieben haben, auch für die Daten der Behörde zu sehen?

An Dr. Rohleder, und bitte nicht falsch verstehen, Wirtschaftsförderung ist sicherlich auch sinnvoll, aber da Sie auf den Blick zur Sicherheitslage bei dieser Umsetzung eine völlig andere Position als Herr Neumann bezogen haben, würde ich gerne wissen, aus welchem Blickwinkel heraus welche wirtschaftliche Bedeutung die Umsetzung dieses Gesetzes für Anbieter hätte. Das muss auch einmal beziffert werden, zumindest grob umrissen würde es mir reichen.

Stv. Vors. **Frank Hofmann (Volkach)**: Vielen Dank, Herr Tempel. Herr Dr. Fogt, bitte.

SV **Dr. Helmut Fogt** (Deutscher Städtetag, Berlin): Herr Tempel, ich muss ein Missverständnis ausräumen. Ich bin zu den Kosten von Archivierung und Löschung von elektronisch geführten Akten gefragt worden. Ich habe da nur den Vergleich, den Rahmen deutlich gemacht, dass bei uns, wenn in den Kommunen etwas in der Richtung angegangen wird, das komplexe System Dokumentenmanagement insgesamt ins Auge gefasst wird, und dass ich in Relation zur konventionellen Archivierung von Akten die Kosten für die elektronische Verwaltung für überschaubar halte. Wir sind durch das Gesetz als Kommunen nicht verpflichtet zur elektronischen Aktenführung, das richtet sich an die Behörden des Bundes. Das Gesetz versteht sich allenfalls als vorbildgebend. Aber dieses Vorbilds bedarf es nicht, weil in den Kommunen über dieses Thema bereits intensiv diskutiert wird, und dies schon seit geraumer Zeit. Wenn da Besorgnisse bestehen bei einzelnen Kommunen und Landkreisen: Durch dieses Gesetz werden wir nicht unmittelbar verpflichtet, elektronische Aktenführung einzuführen. Wir wissen auch, dass elektronisches Dokumentenmanagement kostenintensiv ist und nur perspektivisch angegangen werden kann. Selbstverständlich auch unter Würdigung von Haushaltslagen. Das zur Richtigstellung.

Stv. Vors. **Frank Hofmann (Volkach)**: Herr Neumann, wieder mit der Bitte um eine kurze Antwort.

SV **Linus Neumann** (Chaos Computer Club, Berlin): Es geht um das Angriffsrisiko für die Behörde anstelle der Privatanwender. Für den Privatanwender gilt: Wenn der Inhalt der Nachricht egal ist, nutze ich das kostenlose E-Mail unverschlüsselt. Wenn der Inhalt der Nachricht nicht egal ist, nutze ich das kostenlose E-Mail Ende-zu-Ende verschlüsselt mit PGP oder S/MIME. Wenn ich mit einer Behörde kommunizieren muss, dann nutze ich in Ermangelung einer Alternative eben De-Mail. Das macht dann die Behörde zu dem eigentlich attraktiven fetten Angriffsziel für den Angreifer. In dem Gesetzentwurf wird aus Kostengründen angeraten, ein zentrales Gateway für De-Mail zu machen, wo dann unabhängig von den Providern – die können sich freuen, dass sie nicht ganz so fette und attraktive Ziele bieten wie das eine Gateway für die Behörden – klar ist: Dort ist die gesamte Behördenkommunikation des Bundes. Ich denke, was ich mehrfach schon betont habe, dass die De-Mail Sicherheit diesem Angriffsrisiko und der Angriffsattraktivität sowie dieser Zentralisierung der Kommunikation einfach nicht gerecht wird.

Stv. Vors. **Frank Hofmann (Volkach)**: Vielen Dank, Herr Neumann. Herr Dr. Rohleder, bitte.

SV **Dr. Bernhard Rohleder** (Hauptgeschäftsführer, BITKOM, Berlin): Herr Tempel, ich weiß nicht, ob wir eine so unterschiedliche Perspektive auf dieses Thema haben. Wir verwechseln nur das Thema Datenschutz nicht mit der IT-Sicherheit. Die Entschlüsselung führt zu einem Mehr an Sicherheit. Zu Lasten des Datenschutzes, aber zu Gunsten des Komforts. Hier gibt es eine Güterabwägung und in dieser Güterabwägung entscheiden wir uns für mehr Sicherheit und für mehr Komfort, das ist alles.

Zur Frage der Wirtschaftlichkeit: Unser Mitglied, die Deutsche Post AG, verdient mit Papier unglaublich gutes Geld. Die bei uns organisierten Drucker- und Kopiereranbieter sowie die Hersteller von Postbearbeitungs- und Frankiermaschinen ebenfalls. Der Markt wird sich etwa dadurch halbieren, dass diese Verfahren elektronifiziert und digitalisiert werden. Das ist kein Markt, der dadurch explodiert, sondern im Gegenteil, der Kommunikationsmarkt wird dadurch unter dem Strich schrumpfen.

Stv. Vors. **Frank Hofmann (Volkach)**: Vielen Dank, Herr Dr. Rohleder. Herr von Notz, Sie haben das Wort.

BE **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Danke, Herr Vorsitzender. Zunächst einmal zwei Dinge: Dass wir hier über De-Mail reden, das darf hier niemand verwundern. Ich erinnere an die Anhörung, die wir zu De-Mail gemacht haben. Die fehlende Ende-zu-Ende-Verschlüsselung ist ein Geburtsfehler von De-Mail, den wir seither mit uns herumschleppen, und es ist kein Wunder, dass das hier

wieder aufschlägt. Das haben Sie damals von anderen Sachverständigen gehört, das wollten Sie auch nicht hören. Jetzt haben wir das Problem.

Ich komme zum zweiten Punkt, der mich doch sehr verwundert, auch wenn das hier so gesagt wird, im Hinblick auf dieses „‚easy to use' und den Datenschutz nicht so hoch hängen." Wir haben einige IT-Großprojekte gehabt, und die sind alle implodiert. ELENA, n-Perso usw., da war immer derselbe Spruch: „easy to use", und es muss nutzerfreundlich sein, aber irgendwie spielt der Datenschutz für die Leute doch eine große Rolle. Deswegen kann ich nur sagen: „Vorsicht an der Bahnsteigkante!" Ich bin bereit, viel darauf zu wetten, dass das nichts und wieder ein Milliardengrab wird. Ich verstehe nicht, warum auch von Industrieseite immer noch so gedacht wird, nachdem man so oft „gegen die Wand" gelaufen ist. Das ist bemerkenswert. Ansonsten verstehe ich die ganzen Aussagen hier zu den Kosten nicht, Herr Dr. Fogt, das muss ich Ihnen sagen. Man hört an allen Ecken und Enden, dass es unendlich teuer wird. Das ist auch die Erfahrung, die man mit solchen Umstellungen, mit der gesamten IT-Umstellung gemacht hat, dass das unendlich teuer wird. Deswegen findet die Industrie das ja auch total interessant. Wenn das alles ein Kosteneinsparprogramm wäre und niemand damit Geld verdienen würde …
Das wollte ich zu meiner Verwunderung vorwegschicken.

Aber ich habe auch Fragen. Zuerst an Herrn Prof. Müller-Terpitz: Sie führen in Ihrem Absatz 23 aus, im Hinblick auf die Zusammenhänge zwischen dem § 8 EGovG-E und den Fragen zum Informationsfreiheitsgesetz, die Zusammenhänge, die da bestehen. Ich wäre Ihnen dankbar, wenn Sie das ein bisschen näher erläutern könnten, was in dem Bereich problematisch sein könnte.

Meine nächste Frage geht an Sie und an Herrn Dankert: Es wurde noch nicht angesprochen, es gibt in dem Bereich nicht nur das BVerfG-Urteil zur Vorratsdatenspeicherung, sondern auch die Entscheidung zum IT-Grundrecht im Hinblick auf die grundlegenden Datensicherheitsanforderungen, die verfassungsfest zu machen im Hinblick auf die IT-Infrastruktur, das Integrationsgrundrecht. Macht es Sinn, sich hier nur auf das veraltete Bundesdatenschutzgesetz (BDSG) zu beziehen, oder müsste man nicht auch im Hinblick auf diese Verfassungsrechtsprechung im Hinblick auf die Integrität von IT noch ein Stück weiterdenken, um wirklich etwas auf den Weg zu bringen, was zukünftig funktioniert? Vielen Dank!

Stv. Vors. **Frank Hofmann (Volkach)**: Vielen Dank, Herr von Notz. Herr Prof. Müller-Terpitz, bitte.

SV **Professor Dr. Ralf Müller-Terpitz** (Universität Passau): Zu § 8 IFG, denke ich, hat Herr Dankert etwas gesagt, was ich auch so sehen würde, und das ich im Aufsatz, auf den Sie Bezug nehmen, schon einmal publiziert habe. Dieser § 8 wird zur Friktion mit dem IFG führen, dergestalt, dass es dort heißt: Die Behörden des

Bundes können bestimmen, wie sie die Akteneinsicht gewähren, durch Aktenausdruck, elektronische Dokumente usw. Wenn man in den § 1 Abs. 2 IFG hineinsieht oder in die Informationsfreiheitsgesetze der Länder, die ähnlich gestrickt sind, stellt man fest, da steht genau das Gegenteil. Es steht drin: Der Bürger kann bestimmen, wie er Akteneinsicht nehmen will. Nur wenn das nicht zumutbar ist, kann die Behörde einen anderen Vorschlag machen. Hier wird das bisherige Prinzip umgedreht. Ich unterstelle, dass das von den Entwurfsverfassern so gar nicht beabsichtigt ist, aber es wird zumindest Auslegungsprobleme in der Praxis hervorrufen. Ich habe Ihr Statement, Herr Dankert, auch so verstanden, dass Sie ebenfalls in diese Richtung argumentieren.

Zum zweiten Punkt, die Datensicherheit: Da ist Herr Dankert wahrscheinlich der bessere Ansprechpartner. Trotzdem möchte ich das eine oder andere noch dazu sagen. Wir haben das Problem und das stellt sich vor allen Dingen bei der elektronischen Aktenführung, auch wenn meine technischen Kenntnisse da eher laienhaft sind. Wir werden dann elektronische Akten bei Behörden haben, die zahlreiche Daten ganz unterschiedlicher Art enthalten. Herr Neumann, ich vermute, das ist ein interessantes Angriffsziel für Hacker; da sind hochinteressante Daten, an die möchte man herankommen. Wenn wir eine Regelung haben wie in § 6 Satz 3 EGovG, wo lediglich drinsteht, das muss dem Stand der Technik entsprechen, dann delegieren wir das gesamte Problem auf die Verwaltungsebene und stellen der Verwaltungsebene anheim, wie sie die Datensicherung umsetzen möchte. Das scheint mir nach dem neuen Diktum des BVerfG aus dem Jahr 2010, das auch einen Schutzanspruch auf Datensicherheit zugunsten des Bürgers begründet, zu wenig zu sein. Da brauchen wir eine gesetzliche Definition, für welche Daten möglicherweise ein höheres Maß an Sicherheit vorzusehen ist, und wie diese Sicherheit dann auszusehen hat. Da kann man sich an § 9 BDSG orientieren. Ich vermute nur, dass das nicht ausreicht. Meines Erachtens wäre es interessant, aber offensichtlich gibt es da noch keine Entwürfe, einmal zu sehen, was macht man im Bereich des Telekommunikationsgesetzes, wo das Problem der Vorratsdatenspeicherung ursprünglich herkommt. Wie sind da konkret die Überlegungen, das vom BVerfG eingeforderte Maß an Datensicherheit auf gesetzgeberische Ebene sicherzustellen. Diese Gedanken sollte man auch nutzen, um sie für das EGovG nutzbar zu machen. Vielen Dank!

Stv. Vors. **Frank Hofmann (Volkach)**: Vielen Dank! Herr Dankert, bitte.

SV **Reinhard Dankert** (Der Landesbeauftragte für den Datenschutz Mecklenburg-Vorpommern, Schwerin): Ich bin kein Jurist, aber die Integrität von technischen Systemen ist beim BVerfG-Urteil ein hohes Gut. Ich denke, das widerspricht sich auch nicht mit den möglicherweise etwas veralteten und verstaubten Paragraphen aus dem BDSG, weil die Forderung der Integrität von Daten durchaus darauf bezogen werden kann. Ich bin kein Verfassungsrechtler, aber am besten ist es im

Gesetz zu regeln und nicht durch Verordnung und durch Erklärung und Absichtserklärung. Ich habe an anderen Stellen auch gesagt, dass gerade wir als Techniker merken, dass sehr unterschiedlich mit verschiedenen Instrumenten umgegangen wird und Dinge vermengt werden. Da kann man im Einzelfall sicher noch einmal darüber diskutieren, wenn es gewollt ist. Wenn nicht, dann ist unsere Stellungnahme eben da. Wir decken das durch gesetzliche Anforderungen, und wir haben auch ein paar Hinweise gegeben, wie ein höherer Standard erreicht werden kann als nur durch Absichtserklärung. Vielleicht reicht das erst einmal.

Stv. Vors. **Frank Hofmann (Volkach)**: Vielen Dank! Gibt es noch weitere Fragen? Keine mehr. Dann darf ich mich recht herzlich bedanken bei Ihnen, den Sachverständigen, für Ihr Engagement. Wir wünschen Ihnen einen guten Nachhauseweg und meinen Kolleginnen und Kollegen wünsche ich eine gute Beratung. Herzlichen Dank.

Ende der Sitzung: 13.51 Uhr