18. Wahlperiode

Deutscher Bundestag
Innenausschuss

Wortprotokoll
der 113. Sitzung

Innenausschuss
Berlin, den 24. April 2017, 10:30 Uhr
10557 Berlin, Konrad-Adenauer-Str. 1
Paul-Löbe-Haus, Raum 4 900

Vorsitz: Ansgar Heveling, MdB

Öffentliche Anhörung

Einziger Tagesordnungspunkt

Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Förderung des elektronischen Identitätsnachweises

BT-Drucksache 18/11279

Federführend:
Innenausschuss

Mitberatend:
Ausschuss für Recht und Verbraucherschutz
Ausschuss Digitale Agenda

Gutachtlich:
Parlamentarischer Beirat für nachhaltige Entwicklung

Berichterstatter/in:
Abg. Heinrich Zertik [CDU/CSU]
Abg. Mahmut Özdemir (Duisburg) [SPD]
Abg. Ulla Jelpke [DIE LINKE.]
Abg. Dr. Konstantin von Notz [BÜNDNIS 90/DIE GRÜNEN]

Inhaltsverzeichnis

		Seite
I.	Anwesenheitslisten	3
II.	Sachverständigenliste	9
III.	Sprechregister der Sachverständigen und Abgeordneten	10
IV.	Wortprotokoll der Öffentlichen Anhörung	11
V.	Anlagen	35

Stellungnahmen der Sachverständigen zur Öffentlichen Anhörung

Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Bonn	18(4)868 A
Prof. Dr. Marian Margraf	18(4)868 B
Prof. Dr. Bernd Holznagel, LL.M.	18(4)868 C
Dr. Constanze Kurz	18(4)868 D

Gutachterliche Stellungnahme des Parlamentarischen Beirates für nachhaltige Entwicklung

zu BT-Drucksache 18/11279	18(4)773

4.

18. Wahlperiode

Deutscher Bundestag

Sitzung des Innenausschusses (4. Ausschuss)

Montag, 24. April 2017, 10:30 Uhr

Ordentliche Mitglieder des Ausschusses	Unterschrift	Stellvertretende Mitglieder des Ausschusses	Unterschrift
CDU/CSU		CDU/CSU	
Baumann, Günter		Albsteiger, Katrin	
Binninger, Clemens		Berghegger Dr., André	
Bosbach, Wolfgang		Brähmig, Klaus	
Frieser, Michael		Brandt, Helmut	
Hellmuth, Jörg		Fabritius Dr., Bernd	
Heveling, Ansgar		Feiler, Uwe	
Hoffmann (Dortmund), Thorsten		Giousouf, Cemile	
Lindholz, Andrea		Gröhler, Klaus-Dieter	
Mayer (Altötting), Stephan		Harbarth Dr., Stephan	
Ostermann Dr., Tim		Hauer, Matthias	
Schäfer (Saalstadt), Anita		Heck Dr., Stefan	
Schuster (Weil am Rhein), Armin		Liebing, Ingbert	
Veith, Oswin		Luczak Dr., Jan-Marco	
Warken, Nina		Monstadt, Dietrich	
Wendt, Marian		Sensburg Dr., Patrick	
Wichtel, Peter		Ullrich Dr., Volker	
Woltmann, Barbara		Wellenreuther, Ingo	
Zertik, Heinrich		Wittke, Oliver	

Referat ZT 4 - Zentrale Assistenzdienste, Tagungsbüro
Luisenstr. 32-34, Telefon: +49 30 227-32251, Fax: +49 30 227-36339

18. Wahlperiode

Sitzung des Innenausschusses (4. Ausschuss)
Montag, 24. April 2017, 10:30 Uhr

Ordentliche Mitglieder des Ausschusses	Unterschrift	Stellvertretende Mitglieder des Ausschusses	Unterschrift
SPD		**SPD**	
Castellucci Dr., Lars		Esken, Saskia	
Frograscher, Gabriele		Fechner Dr., Johannes	
Grötsch, Uli		Gerster, Martin	
Gunkel, Wolfgang		Högl Dr., Eva	
Hartmann, Sebastian		Juratovic, Josip	
Lischka, Burkhard		Kolbe, Daniela	
Mittag, Susanne		Lühmann, Kirsten	
Özdemir (Duisburg), Mahmut		Poschmann, Sabine	
Reichenbach, Gerold		Rix, Sönke	
Schmidt (Berlin), Matthias		Spinrath, Norbert	
Veit, Rüdiger		Yüksel, Gülistan	
DIE LINKE.		**DIE LINKE.**	
Jelpke, Ulla	Ulla Jelpke	Dağdelen, Sevim	
Korte, Jan		Hahn Dr., André	
Renner, Martina		Karawanskij, Susanna	
Tempel, Frank		Pau, Petra	

04

18. Wahlperiode

Sitzung des Innenausschusses (4. Ausschuss)
Montag, 24. April 2017, 10:30 Uhr

Ordentliche Mitglieder des Ausschusses	Unterschrift	Stellvertretende Mitglieder des Ausschusses	Unterschrift
BÜ90/GR		**BÜ90/GR**	
Amtsberg, Luise		Haßelmann, Britta	
Beck (Köln), Volker		Künast, Renate	
Mihalic, Irene		Lazar, Monika	
Notz Dr., Konstantin von		Mutlu, Özcan	

Tagungsbüro

Deutscher Bundestag

Sitzung des Innenausschusses (4. Ausschuss)
Montag, 24. April 2017, 10:30 Uhr

	Fraktionsvorsitz	Vertreter
CDU/CSU		
SPD		
DIE LINKE.		
BÜNDNIS 90/DIE GRÜNEN		

Fraktionsmitarbeiter

Name (Bitte in Druckschrift)	Fraktion	Unterschrift
Buczyk, Pirk	LINKE	
Alexander Lemm	SPD	
M. Gopalai	Grüne	

Stand: 20. Februar 2015
Referat ZT 4 – Zentrale Assistenzdienste, Luisenstr. 32-34, Telefon: +49 30 227-32659, Fax: +49 30 227-36339

Tagungsbüro

Sitzung des Innenausschusses (4. Ausschuss)
Montag, 24. April 2017, 10:30 Uhr

Bundesrat

Land	Name (bitte in Druckschrift)	Unterschrift	Amts-bezeich-nung
Baden-Württemberg			
Bayern	Lyderschmid	Lindner-a	RD
Berlin			
Brandenburg			
Bremen			
Hamburg			
Hessen			
Mecklenburg-Vorpommern	DAUCH	Rauch	
Niedersachsen			
Nordrhein-Westfalen			
Rheinland-Pfalz			
Saarland			
Sachsen			
Sachsen-Anhalt			
Schleswig-Holstein			
Thüringen			

Stand: 20. Februar 2015
Referat ZT 4 – Zentrale Assistenzdienste, Luisenstr. 32-34, Telefon: +49 30 227-32659, Fax: +49 30 227-36339

Tagungsbüro

Sitzung des Innenausschusses (4. Ausschuss)
Montag, 24. April 2017, 10:30 Uhr

Ministerium bzw. Dienststelle (bitte in Druckschrift)	**Name** (bitte in Druckschrift)	**Unterschrift**	**Amts-bezeich-nung**
BfDI	Edith Weber	Weber	ORR'in
BMI	Batt, Peter	Batt	MDir
BMJV	Sommer, Nino	Sommer	BMJV
BMI	Wolkin, Göran	Wolkin	DMI
BMI	Kiejel, Irmela	v. Kiejel	PD
BMI Amt	Struve, Isabel	Struve	ORR'in

Stand: 20. Februar 2015
Referat ZT 4 – Zentrale Assistenzdienste, Luisenstr. 32-34, Telefon: +49 30 227-32659, Fax: +49 30 227-36339

Liste der Sachverständigen

Öffentliche Anhörung am Montag, 24. April 2017, 10.30 Uhr

Jens Fromm
IT-Dienstleistungszentrum Berlin

Prof. Dr. Bernd Holznagel, LL.M.
Universität Münster

Dr. Constanze Kurz
Chaos Computer Club, Berlin

Prof. Dr. Marian Margraf
Freie Universität Berlin

Arne Schönbohm
Präsident des Bundesamtes
für Sicherheit in der Informationstechnik, Bonn

MDg J. H. Müller
Referatsgruppenleiter 2,
Bundesbeauftragte für den Datenschutz
und die Informationsfreiheit, Bonn

Sprechregister der Sachverständigen und Abgeordneten

Sachverständige	Seite
Jens Fromm	11, 26, 30
Prof. Dr. Bernd Holznagel	12, 24, 30, 32
Dr. Constanze Kurz	14, 22, 23, 24, 31
Prof. Dr. Marian Margraf	15, 22,31
Arne Schönbohm	17, 21, 32
MDg J. H. Müller	17, 20, 33

Abgeordnete	
Vors. Ansgar Heveling (CDU/CSU)	11, 12, 14, 15, 17, 19, 20, 21 22, 24, 26, 27, 28
Abg. Marian Wendt (CDU/CSU)	19, 27
BE Abg. Mahmut Özdemir (Duisburg) (SPD)	20, 28, 32
BE Abg. Ulla Jelpke (DIE LINKE.)	19, 28
BE Abg. Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN)	20, 23, 29

Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Förderung des elektronischen Identitätsnachweises

BT-Drucksache 18/11279

Vors. **Ansgar Heveling** (CDU/CSU): Meine sehr geehrten Damen und Herren, liebe Kolleginnen und Kollegen, ich eröffne die 113. Sitzung des Innenausschusses, die heute als öffentliche Anhörung zum Entwurf eines Gesetzes zur Förderung des elektronischen Identitätsnachweises stattfindet. Ich danke Ihnen sehr herzlich, sehr geehrte Damen und Herren Sachverständige, dass Sie unserer Einladung nachgekommen sind, um die Fragen der Kolleginnen und Kollegen aus dem Innenausschuss und den mitberatenden Ausschüssen zu beantworten. Die Ergebnisse der Anhörung dienen dazu, die Beratungen zu diesem Gesetzentwurf der Bundesregierung vorzubereiten. Ich darf auch sehr herzlich die weiteren Gäste und Zuhörer begrüßen.

Schriftliche Stellungnahmen hatten wir trotz der Kürze der Vorbereitungszeit erbeten. Für die eingegangenen Stellungnahmen darf ich mich ganz herzlich bedanken. 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, sehr geehrte Damen und Herren Sachverständige, dass Ihr Einverständnis zur öffentlichen Anhörung auch die Aufnahme der Stellungnahmen in eine Gesamtdrucksache umfasst. Ich sehe keinen Widerspruch.

Die heutige Sitzung wird im Parlamentsfernsehen des Deutschen Bundestags weltweit überragen.

Von der heutigen Anhörung wird für ein Wortprotokoll eine Bandabschrift gefertigt. Das Protokoll wird Ihnen zur Korrektur übersandt. Im Anschreiben werden Ihnen die Details zur weiteren Behandlung mitgeteilt. Die Gesamtdrucksache bestehend aus Protokoll und schriftlichen Stellungnahmen werden wir dann auch ins Internetangebot des Deutschen Bundestags einstellen.

Zum zeitlichen Ablauf darf ich anmerken, dass insgesamt eine Zeit von 10.30 Uhr bis 12.30 Uhr für die Durchführung der Anhörung vorgesehen ist. Einleitend erhält jeder und jede Sachverständige die Gelegenheit in einem Eingangsstatement, das bitte 5 Minuten nicht überschreiten sollte, zum Gesetzentwurf Stellung zu beziehen. Maßgeblich ist die Uhr des Vorsitzenden. Ich werde durch dezentes Hüsteln darauf aufmerksam machen, wenn die Zeit überschritten ist und behalte mir auch weitere Maßnahmen vor.

Danach würden wir mit der Befragung der Damen und Herren Sachverständigen durch die Berichterstatterinnen und Berichterstatter sowie weiterer Abgeordneter beginnen. Ich bitte, dass die Fragesteller diejenigen Sachverständigen ausdrücklich benennen, an die die Frage gerichtet ist, wobei es im Interesse möglichst vieler Kolleginnen und Kollegen ist, die Fragen so knapp und limitiert wie möglich zu stellen, damit auch bei Bedarf die Möglichkeit vieler Fragen besteht.

Wenn Sie damit einverstanden sind, verfahren wir so.

Entsprechend der alphabetischen Reihenfolge darf ich zunächst Herrn Fromm vom IT-Dienstleistungszentrum Berlin um sein Eingangsstatement bitten.

SV **Jens Fromm** (IT-Dienstleistungszentrum Berlin): Vielen Dank für die Einladung. Erst einmal entschuldige ich mich ganz förmlich, dass ich es nicht geschafft habe, eine Stellungnahme einzureichen. Mir wurde schon gesagt, es bringt nichts, dass ich mich hier entschuldige, aber so viel dazu.

Warum bin ich hier geladen? Ich hatte die Freude, zehn Jahre bei der Fraunhofer-Gesellschaft zu arbeiten und habe in dem Rahmen intensiv die Einführung des damals neuen Personalausweises 2008/2009 und die Einführung 2010 zu begleiten. Damals bestand zumindest bei einigen, auch bei mir, eine riesige Euphorie, weil wir dachten, wir könnten mit der eID-Funktion ganz viele Probleme, die wir – immer noch – in der virtuellen Welt haben, nämlich die Identifikation, lösen. Wir haben dann relativ schnell oder über Jahre gemerkt: Naja, so richtig angenommen wird der nicht. Ich habe vor zwei, drei Jahren noch einmal eine „Lessons Learned-Publikation“ veröffentlicht, in der wir bestimmte Vorschläge gemacht haben, was man daran machen könnte. Ein, zwei, drei Vorschläge finden sich heute glücklicherweise hier in diesem Gesetz wieder. Aber, sieben Jahre nach der Einführung sehen wir immer noch eine Landschaft,

eine virtuelle Welt, in der wir immer noch privatwirtschaftlich dominierte Identitätsnachweise haben. In der wir kaum Datenschutz, kaum Datensicherheit bei den Identitätslösungen haben, die wir so bei Facebook und allen möglichen anderen Plattformen finden. Wir haben einen Wildwuchs an Lösungen, die die Etablierung von Identitätslösungen erschweren. Wir haben dadurch auch kaum die E-Government-Lösungen, also kaum Möglichkeiten, mit denen die Verwaltung den Bürgerinnen und Bürgern oder Unternehmen komplexe Lösungen anbieten kann.

Ich glaube, dass die Technik des Personalausweises nach wie vor State of the Art ist, es ist immer noch eine tolle Technik. Wir haben aber damals ein Stückweit vergessen, den Nutzer mitzunehmen. Andere Länder haben das klüger gemacht und sind schrittweise vorgegangen. Wir haben – 2010 glaube ich – sofort einen komplex zu bedienenden Mercedes hingestellt. Ich glaube, einige Elemente des Gesetzes dienen dazu, dies wieder zu vereinfachen.

Ich will vier Aspekte herausgreifen. Erstens: Einschalten versus Ausschalten. Das ist sicher ein Thema, das man hier diskutieren kann und auch muss. Man könnte das philosophisch diskutieren: Wird der Bürger, wenn das eingeschaltet bleibt, gezwungen, ist das ein Zwang hin zum E-Government? Ich glaube, dass man versuchen sollte, das hier entsprechend eingeschaltet zu lassen. Der Bürger, die Bürgerin, kann das durch einen Anruf sperren. Ob das gleich im Bürgeramt passiert oder nicht sehe ich jetzt nicht wirklich als relevant an. Es birgt aber eine größere Chance, dass die eID-Funktion vorankommt.

Thema zwei, Berechtigungszertifikate. Ich glaube, dass eine Vereinfachung der Beantragung der Berechtigungszertifikate sehr wohl Sinn ergibt. Dadurch werden nicht die datenschutzrechtlichen Vorschriften ausgehebelt, diese bleiben unberührt. Zudem hat die Vergabestelle, wenn Verstöße erfolgen, auch im Nachhinein die Möglichkeit, das Berechtigungszertifikat und damit auch die Erlaubnis zu entziehen, auf die eID-Funktion des Ausweises zuzugreifen.

Der dritte Punkt, Speicherung durch Identifizierungsanbieter, also Etablierung eines Postident. Technisch gesehen kann man sagen: Endlich. Das sind Sachen die wir bei Fraunhofer seit 10, 15 Jahren diskutiert haben. Man könnte hier sogar noch viel weiter gehen. Das ist im privatwirtschaftlichen Raum auf jeden Fall der Fall, dass Daten auch langfristig gespeichert werden. Der Gesetzgeber sieht hier im neuen Gesetz vor, dass das nur für den jeweiligen Zweck ist. Das finde ich eine relativ humane und sinnvolle Lösung, um hier erst einmal die Etablierung des Ausweises voranzubringen.

Vierter Aspekt, der mir sehr gut in dem Gesetz gefallen hat, ist das Vor-Ort-Auslesen dergestalt, dass im Endeffekt, wenn der Ausweisinhaber dabei ist, entsprechend der Chip mit Eingabe der Zugangsberechtigung, der Zugangsnummer, ausgelesen werden kann.

Zu den Kosten und den polizeilichen Maßnahmen kann und will ich mich nicht äußern. Das ist nicht meine Expertise. Das möchte ich ganz klar sagen.

Alle diese Maßnahmen, die Aspekte, die ich gerade herausgegriffen habe, sind für mich kleine Bausteine um das Thema sichere Identifikation für die Menschen voranzubringen. Die sind aber nur ein Baustein. D. h., wenn man das wirklich seriös voranbringen möchte, müsste man hier noch weitere Projekte starten, Werbung schalten, vielleicht auch verpflichtende Maßnahmen dahingehend, dass Verwaltungen stärker elektronische Anwendungen anbieten und hier den Ausweis oder andere Identifikationsmöglichkeiten bieten.

Vors. **Ansgar Heveling** (CDU/CSU) vielen Dank Herr Fromm. Als nächster hat Herr Prof. Dr. Holznagel das Wort.

SV **Prof. Dr. Bernd Holznagel**, LL.M. (Universität Münster): Herr Vorsitzender, meine Damen und Herren, herzlichen Dank für die Einladung. Ich bin ganz auf der Linie von Herrn Fromm. Zunächst einmal ist es sehr zu begrüßen, dass der erneute Versuch unternommen wird, diese Sicherheitsinfrastruktur zu etablieren und zu fördern. Ich hätte mir ein bisschen mehr gewünscht, dass in der Begründung oder auch in einzelnen Vorschriften deutlich wird, dass die Zukunft im Mobilfunk und beim Fingerscan liegt. Wer zufällig am Wochenende die FAZ gelesen hat, der sieht noch einmal, dass diese mobilfunkbasiert eingeführten Bezahlsysteme endlich auch in Deutschland die Zukunft sind. Ich war kürzlich auf Forschungsreise in Kanada, dort kann ich schon

jetzt mein Konto mit dem Mobilfunk bedienen. Ich habe ein bisschen das Gefühl, dass wir, obwohl die Infrastruktur steht, in der Umsetzung wirklich inzwischen weit zurück liegen. Ich habe mich aber auch belehren lassen, dass das System mobilfunkfähig und zumindest auf Android-Geräten einsatzfähig ist. Aber dann muss es auch umgesetzt werden. Ich hatte gehört, dass der Werbeetat in der letzten Runde von 21 Mio. Euro auf 3 Mio. Euro heruntergekürzt wurde. Das geht natürlich nicht. Ich meine, dass sich solche Veränderungen in den Köpfen verankern müssen. An der Universität wissen wir, dass es sich nur durch ein Prinzip verankert: Wiederholung, Wiederholung und Wiederholung. Es gibt gar keinen anderen Weg. Die Leute müssen mit dieser Situation konfrontiert werden. Es müssen Schulungsprogramme gemacht werden und das alles ergibt nur Sinn, wenn es entsprechende Dienste gibt, die man auch vernünftig nutzen kann. Da bin ich ganz auf der Linie, aber, ich hoffe – und das ist ja das, was die Bundesregierung verspricht – dass es zu einer riesigen Initiative im Bereich von E-Government kommt. Dann hat man genügend Anwendungsmöglichkeiten.

Zu den Details. Erst ein frauenpolitisches Thema. Ich bin etwas über den § 7 Absatz 1 Nr. 11 – Versagungsgründe – gestolpert. Da ist bisher nur genannt, dass der Pass versagt werden kann, wenn ein Verstoß gegen § 226a StGB – Verstümmelung weiblicher Genitalien – vorliegt. Mir ist jetzt nicht klar, warum § 237 StGB – Ausreisen zum Zwecke der Zwangsverheiratung – nicht auch unterbunden werden können. Da sehe ich einen Wertungswiderspruch. Beides sind krasse Menschenrechtsverletzungen oder, um genauer zu sein, Verletzungen des Würdeprinzips. Hier besteht glaube ich fraktionsübergreifend eine gute Möglichkeit, noch eine kleine Nachbesserung zu vollziehen.

Zweiter Punkt ist der automatische Lichtbildabruf für Sicherheitsbehörden und Nachrichtendienste. Ich bin persönlich der Auffassung, dass die Erweiterung des Kreises auf die Nachrichtendienste angesichts der Terrorgefährdung oder auch anderer Gefährdungen sinnvoll ist. Ich komme aus Dortmund, diese Aktion mit dem Anschlag, die wir gerade beim BVB erlebt haben, zeigt, dass der Kreis der Verrückten heutzutage sehr weit gezogen ist. Ich glaube, dass dort Nachrichtendienste insgesamt so eine Ermächtigung brauchen und dass der Kreis auch ausgeweitet gehört. Ich bin aber nicht der Auffassung, dass das nur im Rahmen der Aufgaben der Nachrichtendienste erfolgen soll. Ich sehe keinen Grund, warum nicht erst die zuständigen Behörden angefragt werden sollen. Da bin ich ganz auf der Linie der Bundesdatenschutzbeauftragten.

Es gibt aber noch einen systematischen Grund. In § 26 Absatz 4 PAuswG ist das Verbot der Errichtung einer nationalen Lichtbilddatenbank vorgesehen. Heute ist die Vernetzung so gut, dass, wenn ich aus den eigenen Aufgaben heraus jederzeit und egal wo ich bin einen Abruf machen kann, das faktisch so etwas ist wie eine nationale Datenbank für Lichtbilder. Ich denke, dass das so beschränkt werden muss, wie das auch bei den Sicherheits- und Ordnungsbehörden der Fall ist. Die Entwurfsbegründung zu § 25 Absatz 2 Satz 3 PAuswG-E ist da sehr ausführlich und man muss sie sehr ernst nehmen. Es wird etwa gesagt, dass die Gefahr besteht, dass, wenn ich z. B. bei uns im Bürgeramt in Dortmund bin, es sein kann, dass eine Anfrage an jemanden im Meldebereich adressiert ist, der den kennt oder dass ein verdeckter Ermittler existiert. Das ist natürlich eine reale Gefahr und in der Begründung nicht schlicht fabuliert. Es muss zudem Möglichkeiten geben, auch tatsächlich direkt, ohne noch mal im Einzelnen den Weg mit den Meldebehörden zu gehen, die Informationen automatisch direkt zu bekommen. Das darf aber nicht der Regelfall sein, sondern sollte als Ausnahmefall formuliert werden, der immer begründet werden muss. Solche begründungsfähigen Akte finden sich z. B. im BKA-Gesetz in § 10 Absatz 7. Wenn man das auf die Nachrichtendienste überträgt, könnte man solche Ausnahmen z. B. bei schutzwürdigen Interessen der Betroffenen – also V-Leuten oder sonstigen wichtigen Leuten – oder auch bei Eilbedürftigkeit vorsehen, wenn die zuständigen Behörden am Wochenende geschlossen sind. Da findet man sicher einen Weg.

Zusammengefasst finde ich die Ausweitung auf die Nachrichtendienste positiv, aber nicht nur im Rahmen ihrer Aufgaben, sondern entsprechend den Vorgaben nach dem BKA-Gesetz sollten erst die zuständigen Behörden angesprochen werden, anschließend kann es Ausnahmen geben, nach denen man einen automatisierten Abruf direkt durchführen darf.

Der letzte Punkt ist die ex-ante-Kontrolle, die wir bisher hatten, wenn es bei den Diensteanbietern um die Zertifikatsverleihung geht. Das soll jetzt zu einer ex-post-Kontrolle ausgebaut werden. Der Grund ist eine Vereinfachung. Bei näherer Betrachtung denke ich aber, dass das ein Scheineffekt ist. Denn die Neuregelung enthält keine Vereinfachung im Standard. Die Datenschutz- und Datensicherheitsstandards sind einzuhalten. Die Unternehmen müssen auch im Vorfeld wissen, welche Rechtsregeln auf sie zukommen. Tun wir doch nicht so, als wäre heute noch jemand alleine in der Lage, das komplizierte Datenschutzrecht zu durchschauen. Wenn diese keine Beratung haben, setzt man sie automatisch der Gefahr aus, von den Behörden sanktioniert zu werden. Die Sanktionen, die dann kommen können, sind nicht nur finanzieller Art. Die Diensteanbieter können auch einen erheblichen Imageschaden durchlaufen, wenn diese ganze Angelegenheit an die Medien geht. Die jetzt vorgeschlagene Regelung finde ich nicht akzeptabel. Man sollte zurück zur alten Regelung, zur Präventivkontrolle und diese Präventivkontrolle – wie es jetzt auch ist – zum Gespräch mit den Unternehmen und zu Schulungen nutzen.

Ich bin jetzt, glaube ich, seit 15 Jahren bei der Bundesnetzagentur im wissenschaftlichen Arbeitskreis. Ich habe mehrfach erlebt, dass im Bereich der Telekommunikation Geschäftsmodelle erst zwischen Behörden und Unternehmen entwickelt worden sind. An vielen Stellen ist das Recht heute so kompliziert, dass es ohne eine Hilfe gar nicht mehr zu machen ist.

Was ich dabei unterstelle, ist, dass der Bundestag nicht davon ausgeht, dass er den Standard hinunterregelt und sagt: Naja, das wird dann sowieso nicht kontrolliert. Wenn wir Recht haben, muss Recht auch vollzogen werden, sonst reißen wir den Stuhl um, auf dem wir sitzen.

Zum letzten Punkt das Plädoyer: Belassen Sie es bei der Zertifizierung bei der alten Regelung. Das ist erprobt und ist gut so.

Vors. **Ansgar Heveling** (CDU/CSU) vielen Dank Herr Prof. Dr. Holznagel. Frau Dr. Kurz, bitte.

SVe **Dr. Constanze Kurz** (Chaos Computer Club, Berlin): Vielen Dank. Sie werden es vermuten, ich sehe den Gesetzentwurf doch ein bisschen kritischer als meine Vorredner. Ich werde nur auf die Aspekte eingehen, die ich kritisch sehe und nicht auf die Aspekte des Gesetzes, die ich für durchaus sinnvoll halte. „Die Euphorie ist verflogen“, hier sprach Herr Fromm übrigens auch für die Hacker: Schlicht aufgrund der Nichtnutzung der eID hat sich keine nennenswerte Schadsoftware herausgebildet. Es wurden nicht einmal Versuche unternommen, die bestehenden Probleme bei der Sicherheit auszunutzen. Das ist insofern ein positiver Aspekt der Nichtnutzung.

Herr Prof. Dr. Holznagel hat eben schon angesprochen, dass es Alternativen gibt, insbesondere solche, die auf internationalen Standardisierungen beruhen. Die will ich hier besonders erwähnen. Ich habe es auch in der Stellungnahme kurz angesprochen: Wenn wir über dieses Gesetz sprechen wollen, müssen wir die Mobile Identity, die von der GSMA – also der internationalen Vereinigung der Mobilfunkanbieter – demnächst angeboten wird, betrachten. Denn die Förderung, die hier beabsichtigt ist, muss auch hinsichtlich der Frage, ob das Gesetz das erreicht, gestellt werden. Aus meiner Sicht sind die internationalen Lösungen, die es derzeit gibt, aber vor allen Dingen auch die Geplanten, für privatwirtschaftliche Anbieter sehr viel attraktiver und werden marktgängig sein. Insofern ist meine Befürchtung, dass die hinter dem Gesetzentwurf stehende Idee in Bezug auf die Förderung der eID so nicht erfolgreich umgesetzt wird. Nur die Tatsache, dass man die eID dauerhaft aktiviert, wird zu keiner Form von neuen Anwendungen führen und natürlich auch nicht dazu, dass die Bürger sie plötzlich benutzen. Die Anreizsetzung für die Anbieterseite besteht eigentlich nur darin, dass man den Prozess bei der Beantragung der Zertifikate ein bisschen erleichtert. Das sehe ich allerdings insofern kritischer als Herr Prof. Dr. Holznagel, als diese Prozeduren bei der Beantragung auch ein Vertrauensanker sind und die Nichtnutzung der eID gerade mit dem Nichtvertrauen der Bürger zu tun hat. Ich halte die Idee, mit der Vereinfachung des Beantragungsverfahrens eine gewisse Incentivierung für Anbieter zu setzen, ebenfalls für verfehlt. Ich denke, sie wird leider auch scheitern. Es gibt aber aus meiner Sicht durchaus eine Alternative, um diese durch den Gesetzentwurf versuchte Incentivierung auch tatsächlich zu erreichen, nämlich – wie das auch in einigen

anderen Staaten angegangen wird – die Angebote staatlicherseits zu verbessern.

Von Anfang an gab es einige Kritik an der eID, insbesondere, weil man mit der durch diese Online-Funktion im Ausweis gegebenen staatlichen Garantie eine gewisse Vermischung zwischen hoheitlichen Aufgaben und Anbietern im privatwirtschaftlichen Sektor hat. Diese Kritik hat der CCC lange geäußert und wir äußern sie auch heute. Ich denke, im Sinne des Datenschutzes für normale Netznutzer ist es eine gute Sache, dass im privatwirtschaftlichen Sektor – mit einigen Ausnahmen – die Identitätsprofile mit der eID nicht staatlich garantiert angelegt werden können. Insofern habe ich eine gewisse Kritik an der generellen Idee des Gesetzentwurfs.

Ein Aspekt, der noch nicht erwähnt wurde, der mir aber wichtig ist, ist das Zulassen von Ausweis- und Passkopien. In Fragen der IT-Sicherheit halte ich das für gefährlich, denn dazu gehört auch die Kopie der MRZ, der Maschinen lesbaren Zone. Wie Sie wissen, ist diese MRZ gleichzeitig der Schlüssel für Daten auf dem Chip. Insofern halte ich die Idee, die Ausweiskopie zu erleichtern, für kritikwürdig, auch weil bei einer Ausweiskopie regelmäßig sehr viel mehr Daten kopiert werden, als für die Verträge oder Dienstleistungen, die man abschließen will, nötig sind. Das liegt vor allen Dingen daran, dass die typischen Daten wie Namen, Anschrift und Geburtsdatum auf zwei Seiten des Ausweises sind und man deshalb in der Regel für eine Ausweiskopie beide Seiten kopiert. Das bedeutet, dass man alle aufgedruckten Angaben damit auch mitkopiert. Dazu gehört übrigens auch die Zugangsnummer, die gleichzeitig für einen hoheitlichen Bereich des Chips mitkopiert würde.

Außerdem sehe ich die mittelbar in diesem Gesetzentwurf vorgesehene Reduzierung der Information der Bürger kritisch. Mit der dauerhaften Aktivierung und der Nichtmöglichkeit der Deaktivierung soll gleichzeitig die Information an den Bürger reduziert werden. Die Formulierung in dem Gesetzentwurf ist ein bisschen schwammig, es soll den Stellen vor allen Dingen selbst überlassen werden. Das halte ich aber deswegen für den falschen Weg, weil nach wie vor der Grund für den Vertrauensmangel in diese eID darin besteht, dass auf die mit der Benutzung einhergehenden Risiken nicht handfest und ehrlich hingewiesen wird, insbesondere was die Lesegeräte betrifft.

Ich glaube, es wäre eine Pflicht für den Staat, der diese eID ausgibt, die Bürger darüber sinnvoll zu informieren, was die Unterschiede bei der Benutzung der verschiedenen Lesegeräte in Bezug auf die IT-Sicherheit sind und vor allen Dingen auch darüber, welche Risiken eigentlich bestehen. Es gibt zwei Angriffswege, oder zwei wesentliche Angriffsparameter gegen diese eID. Die bestehen vor allen Dingen auf Seiten des benutzenden Ausweisbesitzers, also bei seinem privaten PC, und beim Lesegerät. Ich denke, darauf muss der Staat hinweisen und das tut er nach wie vor nicht. Die dazu ausgegebenen Broschüren sind nicht hinreichend. Diese Informationspflichten noch zu reduzieren, halte ich für den falschen Weg. Das würde dazu führen, dass wir ganz viele aktivierte Ausweise haben, aber ein minimiertes Vertrauen. Sie werden es erahnen, ich setze mich daher dafür ein, dass die Wahlfreiheit für den Bürger weiterhin bestehen sollte.

Was die Berechtigungszertifikate angeht, kann ich mich ansonsten dem, was Herr Prof. Dr. Holznagel sagte, anschließen. Dass ein Teil dieser Prüfung wegfällt, halte ich natürlich für kritisch.

Ein letzter Satz zu der Frage der Geheimdienste, die Herr Prof. Dr. Holznagel ansprach. Der automatisierte Abruf ist für die Polizei bereits heute möglich. Ich sehe überhaupt keinen Grund, warum man das auf Geheimdienste ausweiten sollte. Wir lehnen das seit vielen Jahren ab. Es ist vor allen Dingen ein Szenario, vor dem lange gewarnt wurde, dass man nämlich nach und nach die Türen öffnet. Wenn wir gleichzeitig sehen, wie im öffentlichen Bereich die Gesichtserkennung und die Videoüberwachung und vor allem die technischen Möglichkeiten damit ausprobiert werden, sehe ich diesen Bereich natürlich sehr kritisch. Vielen Dank.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank Frau Dr. Kurz. Dann gebe ich nun Herrn Prof. Dr. Margraf das Wort.

SV **Prof. Dr. Marian Margraf** (Freie Universität Berlin): Danke schön. Ich möchte mich auch noch einmal für die Einladung bedanken. Ähnlich wie Herr Fromm bin ich schon seit über einem Jahrzehnt mit der eID-Funktion des neuen Personalausweises beschäftigt und kann noch einmal wiederholen, was Herr Fromm gesagt hat:

Wir waren 2010 alle enttäuscht, dass sich das nicht so richtig durchgesetzt hat, wir haben da viel mehr erwartet. Umso mehr begrüße ich, dass jetzt mit dem Gesetzentwurf Änderungsvorschläge gemacht werden, um die eID-Funktion noch einmal zu befördern. Ob das alles ausreichend ist kann zum jetzigen Zeitpunkt, glaube ich, keiner sagen. Zumindest will ich einige Punkte herausgreifen, bei denen ich denke, dass sie das befördern werden, gleichzeitig aber auch nicht denke, dass das den Datenschutz und die Datensicherheit schwächt. Ich glaube, eine wichtige Funktion ist, dass man zukünftig die eID-Funktion auch vor Ort nutzen kann. Das wird wahrscheinlich dazu führen, dass die Nutzerinnen und Nutzer einmal sehen wie so etwas überhaupt funktioniert, also dass man mit dieser eID- Funktion tatsächlich etwas machen kann, bevor man sich selbst einen Kartenleser kauft. Ich glaube, das ist die größte Hürde, die es gibt.

Ich kann dazu eine kleine Geschichte darüber erzählen, dass die Funktion eigentlich gar nicht so schlecht ist und von Leuten auch genutzt werden kann, die wenig technischen Sachverstand haben. Meine Frau ist Heilpraktikerin und wollte kurzfristig unser Auto abmelden, weil sie dem Käufer des Autos nicht vertraut hat. Dadurch, dass wir die ganze Infrastruktur zu Hause haben, hat sie es innerhalb einer halben Stunde geschafft, das Auto abzumelden, also die Ausweis-App herunterzuladen, den Kartenleser zu installieren, die richtige Pin einzustellen und dann die Abmeldung durchzuführen. Das zeigt, das funktioniert, wenn die Infrastruktur zu Hause vorhanden ist. Insofern noch einmal, dieser Punkt vor Ort Diensteanbieter wird die Leute wahrscheinlich überzeugen, dass die eID-Funktion funktioniert. Ich halte die automatische und dauerhafte Einschaltung der eID-Funktion, wie Herr Fromm auch, für nicht so kritisch. Nutzerinnen und Nutzer haben nach wie vor die Möglichkeit, den Personalausweis in der Sperrhotline zu sperren oder bspw. ihren Pinbrief nicht zu öffnen oder zu vernichten, so dass eine zweifache Authentisierung auch nicht missbraucht werden kann. Man könnte ein bisschen den Eindruck gewinnen, dass die Vereinfachung der Vergabe von Berechtigungszertifikaten – das was geändert wird – und gleichzeitigen Löschung der Abwahlmöglichkeiten einzelner Datenfelder kritisch ist. Das habe ich am Anfang auch gedacht. Die Berechtigungszertifikate werden jetzt nicht mehr zweckgebunden sondern organisationsgebunden vergeben. Dadurch kann es durchaus sein, dass eine Organisation für einen Geschäftsprozess weniger Daten benötigt als für einen anderen Geschäftsprozess, aber laut Berechtigungszertifikat natürlich die Möglichkeit hat, für diesen einen Geschäftsprozess mehr Daten auszulesen. Ein typisches Beispiel wäre, ich mache eine Altersverifikation, also Video-on-demand, um da noch einmal zu überzeugen, dass ich über 16 Jahre oder über 18 Jahre alt bin. Ein anderer Geschäftsprozess wäre: Ich will einen Mobilfunkvertrag abschließen, aber auf der einen Seite braucht man viel mehr Daten, als auf der anderen. Allerdings ist die Technik des Personalausweises nicht darauf beschränkt, was im Berechtigungszertifikat steht, sondern der Diensteanbieter hat durchaus auch technisch die Möglichkeit, weniger Daten aus dem Personalausweis auszulesen. Ich denke, dass er das auch aufgrund der bestehenden Datenschutzgesetze machen muss. Das ändert überhaupt nichts: Nur weil das plötzlich im Personalausweisgesetz nicht mehr enthalten ist, ist diese Verpflichtung für den Diensteanbieter nicht entfallen. Deswegen sehe ich das auch nicht so kritisch.

Auch die neue Idee, Identifizierungsdienste-anbieter zu erlauben – also Diensteanbieter, die für andere Diensteanbieter die Identifizierung mit der eID-Funktion vollziehen können – ist auf der einen Seite kritisch, weil man damit erlaubt, dass das Tracking von Nutzerinnen und Nutzern ermöglicht wird. Allerdings hat auch hier das Personal-ausweisgesetz ganz fest vorgeschrieben, dass diese Identifizierungsdiensteanbieter Mehrver-pflichtungen haben, als normale Diensteanbieter. Die Daten müssen sofort gelöscht werden, wenn die Identifizierung erbracht wurde und sie müssen auch mehr hinsichtlich Datenschutz und Datensicherheit erfüllen, was zukünftig in der Rechtsverordnung geschrieben wird. Die Rechtsverordnung liegt zum heutigen Zeitpunkt noch nicht vor. Deswegen ist in meiner Stellungnahme auch der Vorschlag, dass in dieser Rechtsverordnung diese Identifizierungs-diensteanbieter verpflichtet werden, ein IT-Sicherheitskonzept zu erarbeiten, vorzulegen und regelmäßig zu aktualisieren. Was dann eventuell auch geprüft werden sollte.

Soweit von mir. Ich möchte mich auch nicht zu den anderen Gesetzänderungen äußern, sondern nur zu den Änderungen zum elektronischen Identitätsnachweis.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank Herrn Prof. Dr. Margraf. Dann gebe ich das Wort an Herrn Müller weiter.

SV **MDg Jürgen Müller** (Referatsgruppenleiter 2, Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Bonn): Vielen Dank, sehr geehrter Vorsitzender, meine Damen und Herren Abgeordnete, auch ich bedanke mich im Namen von Frau Voßhoff für die Gelegenheit, hier noch einmal Stellung nehmen zu können.

Wir haben im Rahmen der Gesetzesabstimmung auch in der Ressortabstimmung schon einmal Gelegenheit gehabt, unsere datenschutzrechtliche Bewertung einzubringen und Änderungsvorschläge vorzubringen. Die sind allerdings leider nicht unbedingt berücksichtigt worden. Deswegen ist unser Gesamtvotum nach wie vor so, dass wir sagen: Der Gesetzentwurf beeinträchtigt das Recht auf informationelle Selbstbestimmung und unterläuft auch bestimmte, den Datenschutz sichernde Standards. Es gibt auch eine Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder von Anfang des Jahres, auf die ich aufmerksam machen möchte. Auch in dieser Entschließung sind bestimmte Punkte noch einmal konkret angesprochen worden. Ich möchte jetzt nur die wichtigsten aufgreifen.

Zum Teil sind die Punkte alle durch meine Vorredner schon angesprochen worden. An erster Stelle ist natürlich die obligatorische Aktivierung der eID-Funktion zu nennen. Hier sind wir nur dann bereit mitzugehen, wenn es tatsächlich keine verpflichtende Nutzung gibt. In der Gesetzesbegründung wird zwar angesprochen, dass es keine verpflichtende Nutzung geben soll, allerdings plädiere ich dafür, dass man das auch im Gesetz selber noch einmal zum Ausdruck bringt. Nur dadurch, dass die Verankerung im Gesetz selbst erfolgt, kann aus meiner Sicht das informationelle Selbstbestimmungsrecht gewahrt bleiben.

Der zweite Punkt ist auch schon angesprochen worden. Die Umstellung durch die vorgesehene Einführung auf die organisationsbezogenen Berechtigungszertifikate. Damit entfällt die bisherige Zweckbindung. Wir sehen schon die Gefahr, dass jetzt natürlich wesentlich mehr Daten erhoben werden. Ob das tatsächlich so richtig ist, weil man sagt: „Der Datenschutz und die Datensicherheit sollen ja unverändert geltend bleiben“, und ob das im Einzelfall so erfolgt, daran haben wir durchaus unsere Zweifel. Deswegen sind wir der Auffassung, dass man es beim bisherigen § 21 belassen sollte. Außerdem halten wir es für wichtig, dass die Bürgerinnen und Bürger tatsächlich auch immer wieder über den Zweck der Datenübermittlung Kenntnis erhalten. Nur dann kann man nachvollziehen, in welchem konkreten Kontext Identitätsdaten übermittelt werden. Auch der § 18 sollte aus unserer Sicht beibehalten bleiben.

Der nächste Punkt ist das Ablichten. Auch hier wird nur gefordert, dass eindeutig erkennbar ist, dass es eine Ablichtung ist. Aber die Erforderlichkeit dafür, überhaupt eine Ablichtung durchzuführen – also die Beschränkung auf den jeweiligen Zweck oder auch eine Regelung, nach der nach Zweckerreichung die Kopie oder die Ablichtung vernichtet wird – fehlt. Das sollte aus unserer Sicht noch entsprechend ergänzt werden.

Zum letzten Punk: Der aus unserer Sicht fast voraussetzungslose Abruf eines Lichtbildes im automatisierten Verfahren durch die Polizeien und die Nachrichtendienste, § 25. Hier ist die Begründung aus unserer Sicht nicht überzeugend, so dass wir eher dafür plädieren würden, es beim bisherigen § 25 zu belassen. Eine Notwendigkeit hier wirklich alle Nachrichtendienste fast voraussetzungslos in diesem automatisierten Abruf mit aufzunehmen, sehen wir nicht. Demzufolge würden wir uns freuen, wenn wir aufgrund unserer Empfehlungen noch verschiedene Änderungen des Gesetzentwurfs erreichen könnten.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank Herr Müller. Nun geht das Wort an den Präsidenten des Bundesamtes für die Sicherheit in der Informationstechnik Herrn Schönbohm.

SV **Arne Schönbohm** (Präsident des Bundesamtes für Sicherheit in der Informationstechnik, Bonn): Sehr geehrter Herr Vorsitzender, meine sehr geehrten Damen und Herren. Haben Sie herzlichen Dank, dass ich hier heute mit Ihnen gemeinsam über das wichtige Thema: Förderung des

elektronischen Identitätsausweises sprechen darf.

Ich glaube uns ist allen klar, die sichere Identifizierung, Authentisierung ist notwendige Voraussetzung für sicheres E-Government und E-Business. Ohne sichere Identifizierung der Transaktionspartner sind keine sicheren Transaktionen möglich. Das ist offensichtlicher und allgemeiner Konsens. Es ist bereits auch von Frau Dr. Kurz angesprochen worden, es gibt zahlreiche privatwirtschaftliche Initiativen zur sicheren Authentisierung. Ich denke z. B. auch an die FIDO-Allianz, an der Google, Microsoft, Intel, zahlreiche andere und auch das BSI intensiv arbeiten. Diese Initiativen sind natürlich auch besonders wichtig. Wir unterstützen sie und sie werden auch sehr positiv gesehen. All das soll letzten Endes die sichere Authentisierung im Netz fördern. Das ist eines der wesentlichen Themen, die wir auch politisch gesehen vorantreiben.

Der elektronische Identitätsnachweis des Personalausweises ist aber das einzige System – um es klar zu sagen – das staatlich verifizierte Identitätsdaten bietet, hoch sicher ist und anwendungsunabhängig vom Staat als Basis in einer Struktur zur Verfügung gestellt wird. Der Staat hat die Verpflichtung, dem Bürger sichere elektronische Identitäten so zur Verwendung per Behörden und im privatwirtschaftlichem Bereich zur Verfügung zu stellen, wie er das in der physischen Welt auch durch den klassischen Pass oder Ausweis tut.

Ich möchte gerne noch einmal auf das Thema Sicherheit eingehen, weil das unsere Kerndomäne ist, aber auch, weil wir glauben, dass es besonders wichtig ist, zu sagen, warum der Ausweis mit diesen Funktionalitäten zur Förderung gegenüber den marktgetriebenen Verfahren wesentliche Vorteile hat.

Erstens: Nur der elektronische Identitätsnachweis bietet eine Identifizierung auf Basis staatlich verifizierter Identitätsdaten. Andere Verfahren bieten meistens nur eine reine Authentisierung.

Zweitens: Der elektronische Identitätsnachweis wird vom Bund als anbieterunabhängige Basis in einer Struktur zur Verfügung gestellt, das habe ich bereits ausgeführt.

Drittens: Der Ausweis basiert auf einem sicheren Kryptochip und die Nutzerkontrolle durch eine Pin bietet ein hohes Sicherheitsniveau.

Viertens: Der elektronische Identitätsnachweis ist nach unserer Einschätzung datenschutzfreundlich gestaltet. Der Nutzer hat die volle Kontrolle darüber, ob und welche Identitätsdaten an einen Dienstanbieter weitergeben werden. Ebenso wird – anders als in Österreich oder Estland – keine zentrale Datenbank benötigt. Viele andere Identifizierungsverfahren basieren auf zentralen Datenbanken, das ist hier nicht der Fall.

Es wurde gerade auch von dem Thema der Incentivierung gesprochen. Man kann das vielleicht auch umgangssprachlich anders mit dem Henne-Ei-Problem beschreiben. Ich glaube, dass hier ein guter Ansatz gefunden wurde, um die Verwendungsbreite zu intensivieren.

Um das zu erreichen, muss man auf der einen Seite eine Vereinfachung für Diensteanbieter um Mehranwendungen durch Verringerung der Einstiegsförderung schaffen und auf der anderen Seite Vereinfachungen bei der Ausweisausgabe für den Bürger.

Dazu gibt es zwei Seiten. Einmal die Anbieterseite. Dort geht es um die Vereinfachung des Verwaltungsverfahrens zur Erlangung einer Berechtigung: Weniger Dokumentationspflichten für den Anbieter – das ist hier Gewährleistung – Verringerung der Einstiegshürde bei Wahrung des hohen Sicherheitsdatenschutzniveaus, darauf habe ich gerade hingewiesen.

Die andere ist die Bürgerseite. Sie haben im Gesetzentwurf in der Präambel geschrieben, dass ungefähr nur ein Drittel der Ausweise mit eingeschalteter eID ausgegeben wird. Es wird natürlich von den Diensteanbietern erheblich problematisiert, entsprechende Leistungen zur Verfügung zu stellen, weil die Flächendeckung der eID reduziert ist. Wir glauben, dass die im Gesetzentwurf vorgesehene Abschaffung der Abschaltmöglichkeit keine Reduzierung des Datenschutzes, der Datensicherheit, ist, da der Bürger über die Transport-Pin, die Sperrmöglichkeit der Pineingabe, weiterhin die volle Kontrolle hat, ob er die eID nutzen will oder nicht. Insgesamt wird hiermit nur die Kundenmöglichkeit deutlich erhöht.

Zusammenfassend bleibt nach Einschätzung im BSI zu sagen, dass der elektronische Identitätsnachweis

ein wichtiges Instrument für die Sicherheit für den Bürger im Netz ist. Er kann staatlich verifizierte Identitätsdaten auf hohem Sicherheitsniveau bieten. Der Gesetzentwurf reagiert auf die praktischen Erfahrungen seit Einführung der eID, um die Verwendungsbreite für die Bürger zu erhöhen. Die Änderungen behalten das hohe Sicherheitsniveau der eID bei. Das Aufrechterhalten dieses hohen Sicherheitsniveaus ist für uns als BSI, als nationale Cybersicherheitsbehörde, Aufgabe und Verpflichtung. Von daher würden wir dem Gesetzentwurf voll zustimmen.

Vors. **Ansgar Heveling** (CDU/CSU): Herzlichen Dank, Herr Schönbohm. Ganz herzlichen Dank an die Damen und Herren Sachverständigen für die Einführungsstatements.

Wir kommen damit jetzt zur Fragerunde. Ich bitte noch einmal die Kolleginnen und Kollegen die Fragen an Sachverständige zu adressieren. Die Sachverständigen bitte ich, die an Sie gerichteten Fragen erst einmal zu notieren, denn wir gehen eine Runde durch bevor wir dann zur Beantwortung kommen.

Als Erstem darf ich Herrn Kollegen Wendt das Wort geben.

Abg. **Marian Wendt** (CDU/CSU): Vielen Dank, meine Damen und Herren Sachverständigen, dass Sie sich zu diesem wichtigen Thema für unsere Fragen zur Verfügung stellen. Ich habe zwei Fragen. Einmal an Herrn Schönbohm vom BSI.

Der Gesetzentwurf reformiert das Verfahren, das ein Unternehmer oder eine Behörde durchlaufen muss, um eine Berechtigung zur Benutzung der Online-Funktion nach § 21 Abs. 2 zu erhalten. Die rechtlichen Hürden sollen jetzt durch den Gesetzentwurf abgebaut werden. Bedeutet dies aus Ihrer Sicht weniger Sicherheit für die persönlichen Daten der Bürgerinnen und Bürger? Wie könnten schwarze Schafe, die hier Datendiebstahl begehen wollen, besser ausfindig gemacht werden?

Die zweite Frage geht an Herrn Fromm. Es wird neben dem Gesetzentwurf auch darüber nachgedacht, in den Verwaltungen eine Öffentlichkeitskampagne zu starten. Oft haben wir das Phänomen, dass man den Personalausweis von dem örtlichen Einwohnermeldeamt der Stadt bekommt, und dort dahingehend beraten wird, dass die Bürger diese Funktion auch abschalten könnten und nicht nutzen müssten. Welche Kampagne wäre hier zielführend? Wie könnte man dahingehend sensibilisieren, dass wir diesem Ausweis stärkere Nutzung bringen und die Möglichkeiten darstellen? Wir lassen die eID-Funktion jetzt angeschaltet, wollen aber, dass die Leute sie auch nutzen. Was müssten wir hierzu noch Besseres tun?

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank Herr Kollege Wendt, Frau Kollegin Jelpke bitte.

BE Abg. **Ulla Jelpke** (DIE LINKE.): Danke Herr Vorsitzender. Meine Fragen richten sich an Frau Dr. Kurz und Herrn Müller.

Ich würde gerne genauer wissen, welche Sicherheitslücken Sie insbesondere für Bürgerinnen und Bürger sehen, die diese kennen müssten, wenn sie den elektronischen Identitätsnachweis haben. Worauf können die Bürger überhaupt noch Einfluss nehmen? Wir haben mitbekommen, dass etwa 51 Millionen Deutsche einen neuen Personalausweis bekommen haben und zwei Drittel die Online-Funktion nicht haben aktivieren lassen. Das hat auch etwas damit zu tun, dass hier ein großer Aufklärungsbedarf darüber besteht, was damit passieren kann. Die Angst vor Missbrauch mit den Daten ist recht groß und ich würde gerne wissen, was man noch tun kann, um aufzuklären.

Hier ist auch wichtig, welche günstigeren und sichereren Alternativen aus Ihrer Sicht denkbar wären. Immerhin wird sich das Ganze enorm verteuern. Vielleicht können Sie uns einfach ein bisschen verdeutlichen, was man sich unter den Identifizierungsdiensteanbietern vorstellen muss. Was sind das für Unternehmen? Wie arbeiten die eigentlich? Was muss ich mir als Bürgerin darunter vorstellen, was dort passiert und welche Bedeutung haben diese Unternehmen für den Markt?

Dann würde ich gerne noch ein bisschen mehr über andere EU-Staaten wissen. Ich weiß nicht, ob Sie beide das beantworten können, wenn andere Sachverständige das wüssten, wäre das auch gut: Gibt es dort ähnliche Erfahrungen oder hat man dort überhaupt die elektronische Identitätsbestätigung?

Zum Schluss interessiert mich noch ein bisschen genauer, welche Vorschläge Sie haben. Wir haben von Frau Dr. Kurz, aber auch von Herrn Prof. Dr.

Holznagel gehört: Verfassungsschutz. Ich finde den automatisierten Zugriff, der jetzt auf die Lichtbilder stattfinden kann, außerordentlich problematisch. Was müsste passieren, um hier entsprechende Einschränkungen vorzunehmen?

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank Frau Kollegin Jelpke, Herr Kollege Özdemir bitte.

BE Abg. **Mahmut Özdemir** (Duisburg) (SPD): Sehr verehrter Herr Vorsitzender, verehrte Sachverständige, ich glaube, aus der Anhörung ist deutlich geworden, dass der Staat Präsenz im Internet zeigen muss und dass wir hier eine Entwicklung haben, in der wir im IT-Bereich relativ zügig unterwegs sind und als Gesetzgeber relativ behäbig, wenn ich an 2010 denke und an die Akzeptanz innerhalb der letzten sieben Jahre.

Meine Fragen richten sich allerdings auf drei Komplexe. Herr Prof. Dr. Holznagel hat gerade dargestellt, dass wir über nachrichtendienstliche Zugänge zu den Lichtbildern entsprechend des BKA-Gesetzes konkrete Zeichnungen des Tatbestandes vornehmen müssten. Entsprechend würde ich fragen: Halten Sie die derzeitige Regelung für eine Art Ermächtigungsgrundlage, die derzeit anlasslos ist und auch ein grundrechtliches Risiko hat, obwohl man auf der anderen Seite nicht das entsprechende Sicherheitsbedürfnis bekommt?

Wir haben gerade auch über das Opt-Out gesprochen, Frau Dr. Kurz und Herr Müller haben diese Frage aufgeworfen. Halten Sie ein echtes Opt-Out für zielführender oder wären Sie mit der derzeitigen Regelung einverstanden, wenn man entsprechend bei der staatlichen Aufklärung noch einmal nachsteuern würde, sprich eine entsprechende staatliche Schutzpflicht im Hinblick auf weitere Informationen gebe?

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank Herr Kollege Özdemir, dann gebe ich Herrn Kollegen Dr. von Notz das Wort.

BE Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Erst einmal ganz herzlichen Dank für den Sachverstand und dessen Einbringen. Ich darf vielleicht vorweg schicken, dass ich mich bezüglich der Unschärfe, des Punktes so ein bisschen wundere, dass hier eine Zwangsbeglückung stattfinden soll. All diese tollen und coolen Features: Die Leute wollen das nicht. Jetzt macht man eine Pflicht daraus. Das ist erst einmal ein sehr unliberaler Ansatz, an dem ich mich grundsätzlich störe. Man muss sich das erst einmal vorstellen.

Ich würde an Herrn Müller die Frage stellen, wie Sie die datenschutzrechtliche Seite und die grundrechtliche Dimension dieser voraussetzungslosen Abrufmöglichkeit der Lichtbilder im automatisierten Verfahren durch die Polizeien, das Bundesamt für Verfassungsschutz, die Landesämter für Verfassungsschutz, den Militärischen Abschirmdienst und den Bundesnachrichtendienst beurteilen. Denn so lese ich das und finde das grundrechtlich ziemlich skandalös. Das wirft eine ganze Reihe von grundrechtlichen Fragen auf, wenn ich die letzten Bundesverfassungsgerichtsurteile vor Augen habe.

Vielleicht an den Präsidenten des BSI die Frage – weil zuständig für Sicherheit und auch in Risikoszenarien denkend – man wundert sich insgesamt, wie in dieser ganzen unsicheren, eID missenden Internet-Welt auch nur ein Geschäft zustande kommen kann. Es funktioniert aber und ist ein Milliarden Markt, bisher auch ohne diesen Ausweis.

Wenn man den jetzt schafft, dann hat der schöne Features, aber es birgt auch ein gewisses Risiko. Wenn ich jetzt das Szenario von Frau Margraf nehme, die ihren Wagen online abgemeldet hat: Man kann auch viel Unfug damit machen. Man kann dann natürlich auch Wagen abmelden, wenn man davon ausgeht, dass IT hackbar ist, was bisher jede IT ist. Vielleicht hat das BSI einmal so ein Horrorszenario, ein Worst-Case-Szenario darüber, was passieren kann, wenn man vom schlimmsten Fall ausgeht – von dem sollten wir ja denken – dass man glaubt, es aufgrund dieser Technik tatsächlich mit jemandem zu tun zu haben, mit dem man es faktisch aber nicht zu tun hat.

Vors. **Ansgar Heveling** (CDU/CSU): Wir kommen jetzt zur ersten Antwortrunde. Herr Schönbohm, bitte.

SV **Arne Schönbohm** (Präsident des Bundesamtes für Sicherheit in der Informationstechnik, Bonn): Ich fange mit Herrn Wendt an. Ich hatte dankenswerter Weise zwei Fragen bekommen.

Die erste Frage war nach § 21 und wie hier mit schwarzen Schafen umgegangen werden soll.

Zunächst einmal ist es relativ wichtig, eine Sache zu verstehen. Bei der Vergabe der Berechtigung erfolgt die Offenlegung der internen Organisation, also wofür das benötigt wird, etwa für Kontoeröffnung, oder was man im Einzelnen damit tut. Wenn man dann feststellt, dass es ein Schwarzes Schaf, wie sie es genannt haben, ist, dann ist jederzeit ein Abschalten von Diensteanbietern über Berechtigungszertifikate machbar und möglich. Durch das Berechtigungszertifikat ist der Diensteanbieter inklusive der Geschäftsadresse eindeutig identifiziert, so dass im Missbrauchsfall auch ein Rückgriff auf diesen Diensteanbieter möglich ist. Dies natürlich auch durch die jeweils zuständige Datenschutzaufsichtsbehörde. Diese Entziehung der Berechtigung ist nach wie vor vorgesehen. Über die Sperrung der Ausgabe von Berechtigungszertifikaten kann das auch umgehend erfolgen. Von daher glaube ich, dass das gut gewährleistet ist. Damit haben wir kein Problem.

Zur anderen Frage von dem Abgeordneten Dr. von Notz. In der Tat haben Sie Recht, es gibt eine Vielzahl von Geschäften und Möglichkeiten im Internet. Jeder geht da gerne hin und kauft gerne bei Online-Anbietern ein. Da funktioniert das. Jetzt ist es aber so, dass der Staat dadurch, dass es hier um hoheitliche Dokumente geht, eine besondere Aufgabe hat. Von daher ist es hier wichtig – darum habe ich das aufgeführt – uns noch einmal vorzuhalten, dass sich die Wirtschaft kontinuierlich weiter entwickelt. Natürlich erkennt man auch, dass der Missbrauch von elektronischen Identitäten ein boomender Markt ist, nicht nur im Guten, sondern auch im Schlechten, so wie wir es auch im Lagebericht zu IT-Sicherheit 2016 vorgestellt und dargestellt haben. Dort ist das natürlich ein klassisches Thema, was dementsprechend helfen würde.

Jetzt bitte ich um Verständnis, dass ich bei einer öffentlichen Anhörung ungerne ein Horrorszenario, wie Sie es geschildert haben oder Worst-Case-Szenario hier darstellen würde. Das, glaube ich, kann man dann später noch einmal entsprechend nachholen.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank Herr Schönbohm. Herr Müller bitte.

SV **MDg Jürgen Müller** (Referatsgruppenleiter 2, Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Bonn): Vielen Dank, Herr Vorsitzender. Ich fange von hinten an. Herr Abg. Dr. von Notz, aber auch Frau Abg. Jelpke, hatte die Frage des Lichtbildabgleiches angesprochen. Ich hatte in meiner Stellungnahme schon deutlich zum Ausdruck gebracht, dass wir eine Erweiterung der Befugnisse der Nachrichtendienste, auf Daten zuzugreifen, auf die sie normalerweise zumindest nicht automatisiert zugreifen können, grundsätzlich ablehnen; die Nachrichtendienste müssen den normalen, ordnungsgemäßen Weg wählen und sich an die Behörden wenden. Dass sich nun tatsächlich die Sachlage, die Bedrohungslage, die von Ihnen dargestellt worden ist, derart geändert hat? Wir sehen ganz einfach nicht, dass diese das jetzt rechtfertigt. Dafür ist aus meiner oder unserer Sicht die Begründung auch nicht derart nachvollziehbar, dass man sagt: Jawohl, das kann man machen. Es ist nach wie vor zumindest uns bisher auch nicht dargelegt worden, dass es auf Grund der bisher nicht vorhandenen Möglichkeit, diesen automatisierten Lichtbildabruf so durchzuführen, wie ihn der Gesetzgeber jetzt vorsieht, zu irgendwelchen nennenswerten Problemen gekommen ist. Das ist aus unserer Sicht immer Voraussetzung, um die Erforderlichkeit für eine Ausweitung gesetzlicher Befugnisse darzulegen. Wie gesagt, da ist uns zumindest nichts bekannt.

Zum Thema von Ihnen, Herr Abg. Özdemir, was die Frage Opt-Out angeht. Auch da hatte ich gesagt, dass wir es so, wie die gesetzliche Regelung jetzt ausgestaltet ist, schon für denkbar halten. In der Begründung findet sich dann der Hinweis, dass durch die gesetzliche Regelung die freiwillige Nutzung natürlich nicht tangiert werden soll. Die Sicherheitsmechanismen, die hier auch mehrfach angesprochen worden sind, existieren nach wie vor. Ich muss als Bürger nach wie vor mit der Pin freischalten. Nichtsdestotrotz ist es für uns auch ein generelles Problem, wenn eine Regelung von einer bisher nicht vorhandenen Freischaltung der eID-Funktion nun auf eine gesetzlich vorgegebene geändert wird, dann ist die Gefahr vorhanden, dass es nicht lange dauert, bis auch eine gesetzliche Nutzungsverpflichtung entsteht. Dem wollen wir entgegen wirken, indem wir meinen, dass dann zumindest auch im Gesetzestext die freiwillige Nutzung noch einmal ausdrücklich verankert wird.

Rein theoretisch lässt sich auch dieser Halbsatz oder Satz natürlich im Gesetz wieder streichen. Aber es wäre ein deutlicheres Signal des Gesetzgebers, dass er deutlich macht: Bitteschön, wir wollen hier nach wie vor an der freiwilligen Nutzung nichts ändern, sondern wir wollen nur die Nutzungsmöglichkeit und -häufigkeit der Bürger versuchen zu aktivieren.

Zu den anderen Fragen von Ihnen, Frau Abg. Jelpke, kann ich nicht ganz so viel beitragen. Ich hoffe, dass Frau Dr. Kurz, die diese Fragen auch gestellt bekommen hat, dazu etwas mehr sagen kann, Ich persönlich habe überhaupt keinen Überblick, wie es in anderen EU-Staaten aussieht.

Zum Thema Aufklärung. Auch das halten wir für existenziell wichtig. Die bisher vorgesehene Aufklärung, die Übergabe der Broschüren, soll abgeschafft werden. Da finden wir: Gerade im Gegenteil. Es ist nach wie vor erforderlich, dass man die Bürgerinnen und Bürger aufklärt, welche Möglichkeiten sie haben. Am einfachsten wäre aus unserer Sicht nach wie vor auch eine bundesweite, einheitliche Aufklärung für die Bürger. Ich denke, das ist auch in den Eingangsstatements genannt worden, dass man die Bürger mitnehmen muss. Das geht in der Tat nur, indem man sie jetzt konkret nochmal entsprechend aufklärt.

Der letzte Punkt war, glaube ich, Diensteanbieter bezogen die Frage, dass die in der Tat natürlich eine Datenmenge bekommen, die eventuell gar nicht erforderlich ist. Wie nun konkret das Risiko aussieht, welcher Missbrauch dort betrieben werden kann, ist im Augenblick schwer abzuschätzen. Es ist immer auch die generelle Problematik, wenn Daten die nicht erforderlich sind, an Stellen vorliegen, dass dann irgendwelche Hackerangriffe passieren können, dass dann irgendwelche sonstigen Missbrauchsszenarien, sei es durch interne Täter, passieren. Das ist alles erst einmal nur relativ theoretisch. Da liegen uns auch keine Erkenntnisse darüber vor, was jetzt die Vergangenheit angeht. Das ist auch ein Punkt, den man noch einmal ehrlich sagen muss: Wir plädieren dafür, verschiedene gesetzliche Vorschriften so beizubehalten, wie sie bisher waren, insbesondere was die Frage der zweckgebundenen Berechtigungszertifikate angeht. Es gibt aber wirklich ganz wenige praktische Erfahrungen. Dadurch, dass die Funktion des Ausweises derart selten genutzt wird, kann man auch nicht wirklich sagen, ob es sich in der Praxis bewährt hat. Es lässt sich einfach gar nicht richtig sagen, ob sich dieses Verfahren in der Praxis derart bewährt hat, so dass man jetzt sagen müsste: Nein, weil es sich nicht bewährt hat, muss man es ändern.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank Herr Müller. Frau Kollegin Jelpke hatte die Frage nach EU-Erfahrungen allgemein gestellt. Deswegen, Herr Prof. Dr. Margraf, an Sie hatte sich keine konkrete Frage gerichtet, aber wenn Sie zu dieser Frage Stellung nehmen könnten, dann dürften Sie das.

SV **Prof. Dr. Marian Margraf** (Freie Universität Berlin): Wir kennen einige Verfahren innerhalb der EU, die aber eine ähnliche Problematik haben, was den Durchsatz betrifft. Ich meine jetzt gerade von staatlichen Identifizierungsmitteln, also vom Staat ausgegebene eID-Funktionen haben ein ähnliches Problem wie in Deutschland. Sie werden von den Bürgerinnen und Bürgern nicht so richtig angenommen und haben auch, wie ich finde, zwei große Nachteile.

Zum einen ist es immer nur eine einseitige Authentisierung, also die Bürgerinnen und Bürger authentisieren sich gegenüber den Diensteanbietern, aber nicht umgekehrt, so z. B. die österreichische Lösung.

Das zweite ist: Nur mit dieser in Deutschland vorgenommenen Konstruktion der gegenseitigen Authentisierung kann man festlegen, welche Datenkategorien aus dem Ausweis ausgelesen werden. Das steht im Berechtigungszertifikat. Das ist innerhalb der EU häufig gar nicht umgesetzt. Deswegen halte ich die Lösung, die eID-Funktion, die wir hier in Deutschland haben, insgesamt schon für die datenschutzfreundlichste.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank Herr Prof. Dr. Margraf, Frau Dr. Kurz, bitte.

SVe **Dr. Constanze Kurz** (Chaos Computer Club, Berlin): Ich habe versucht, mir die Fragen aufzuschreiben. Wenn ich jetzt welche vergesse, dann hoffe ich, jemand weist mich daraufhin. Ich bin natürlich sehr traurig, dass Herr Abg. Dr. von Notz nicht mir die Worst-Case-Szenario-Frage gestellt hat, sondern Herrn Schönbohm.

BE Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Diese Frage können Sie gerne übernehmen.

SVe **Dr. Constanze Kurz** (Chaos Computer Club, Berlin): Ich werde tatsächlich ein paar Sachen zu der IT-Sicherheit sagen.

Zunächst einmal ist mir keine Schadsoftware bekannt – und ich denke, sie wäre mir bekannt – die sich auf die eID oder auf Lesegeräte spezialisiert hat. Was aus meiner Sicht absolut mit der Benutzung und der Marktdurchdringung zu tun hat, denn die Zahlen die wir da haben, die auch in der Gesetzesbegründung noch einmal aufgezählt sind – dass sich zwei Drittel ohnehin dagegen entschieden haben – haben nichts mit der Nutzung zu tun. Es sind sehr viel weniger, als ein Drittel, die diesen Chip überhaupt einmal benutzt haben und noch viel weniger, die sich überhaupt das Equipment gekauft haben, geschweige denn ein ordentliches Lesegerät. Es hat sich einfach für niemanden gelohnt, Schadsoftware zu entwerfen. Dennoch gibt es eine gewisse akademische Forschung. Auch die ist zum Erliegen gekommen. Zwei, drei Jahre vor Beginn und nach der Einführung gab es akademische Forschungen im universitären Bereich, die sich mit diesen Sicherheitslücken beschäftigt hat, insbesondere mit sogenannten Relay-Angriffen. Mit diesen versucht man, die Pin auszuspähen oder – generell gesprochen – den Rechner oder das Lesegerät anzugreifen. Das sind die beiden Einfallstore, die überhaupt möglich sind. Von Seiten des Chaos Computer Clubs gab es natürlich Kritik an der Sicherheit. Aber das Grundkonzept technischer Art ist zwar komplex und sicherlich für den normalen Bürger, der jetzt diesen aktivierten Chip bekommt, schwer zu verstehen, es ist aber natürlich sehr durchdacht und eine gute Lösung.

Natürlich, wie das bei Hackern oder generell jemanden ist, der angreifen will, nimmt man immer den Weakest-Link, also die schwächste Stelle, und die ist hier entweder das Lesegerät oder der PC des Anwenders.

Es gibt auch keine akademische Forschung mehr. Es interessiert sich einfach niemand mehr dafür. Das wird sich vielleicht ändern, aber sicherlich nicht durch diesen Gesetzentwurf.

Zu dieser Mobile-Identity oder generellen Alternativen. Ich glaube, der größte Vorteil der Alternativen ist die Internationalität. Ich bin deshalb der Überzeugung, dass diese sich durchsetzen und marktgängig werden. Es sind aber auch die Konzerne, die sich dahinter gestellt haben, die mit der Incentivierung überhaupt keine Probleme haben, weil sie selbst die Anbieter sind. Sie bieten Lösungen an, die man nicht national technisch und mit Kosten umsetzen muss, sondern die einfach für europäische oder darüber hinausgehende Märkte wie bei der Mobile-Identity gelten. Sie haben vergleichbare IT-Sicherheitslösungen gefunden. Richtig ist sicher, dass in Punkto präventiver Datenschutz bei diesen internationalen Lösungen vieles nicht so perfektioniert ist wie bei der deutschen. Aber das wird auch, zumindest teilweise, durch den Gesetzentwurf eher wieder abgebaut, etwa indem man bei der Beantragung bestimmte Notwendigkeitsprüfungen sein lässt.

Die Frage stellt sich insofern nicht für mich, dass schlicht mit der Marktmacht dieser Anbieter die Durchdringung gegeben sein wird, die der Staat mit seinem Alternativangebot so nicht erreichen kann.

Noch eine andere Sache. Dieses Wort von flächendeckend haben wir hier viel gehört. Flächendeckend ist der Ausweis nicht, schon gar nicht mit einer aktivierten eID. Aber flächendeckend haben wir mindestens ein Mobiltelefon. Wenn sich z. B. die Mobile-Identity an die SIM-Karte bindet ist die Flächendeckung bereits gegeben, die wir beim Ausweis so überhaupt nie haben können. Wir haben den Aufenthaltstitel und den Ausweis. Wir haben natürlich auch eine ganze Menge Leute, die beides nicht haben und damit auch mit einem aktivierten Chip nichts haben würden.

Im Übrigen kurz zu der Deaktivierung, die angesprochen wurde. Man hat jetzt nicht mehr die Möglichkeit, die eID auf dem Amt zu deaktivieren. Aber die Deaktivierung ist natürlich denkbar einfach, man kann den Chip einfach ausmachen. Das kann natürlich jemand tun, der das möchte und diese datenschutzfreundliche Lösung sucht.

Ich will nur kurz etwas zu den anderen EU-Staaten und Lösungen sagen. Mir sind nicht alle bekannt. Aber mit dem Fall Österreich habe ich mich länger beschäftigt und es gibt eine Vergleichsstudie zwischen den Nutzungen, die sehr interessant ist. Aus meiner Sicht sind im Vergleich zu Österreich

die Angebote, die von staatlicher Seite gemacht werden, die Incentivierung für die Bürger, teilweise sehr praktisch. Ich glaube, das Beispiel mit der Anmeldung ist da sicherlich pragmatisch.

Ein zweites immer genanntes Beispiel ist natürlich Estland. Aber Estland hat nicht vergleichbare Sicherheitslösungen. Sie sind nicht derselbe Standard wie in Deutschland. Aber hier ist ebenfalls die Lösung gewählt worden, dass man versucht hat, von behördlichen Anwendungen her diese Attraktivität der Nutzung der Identifizierung einzuleiten, und nicht indem man etwas aktiviert und hofft, dass jemand das benutzt.

Diese Opt-Out-Frage. Es ist keine Nutzungsverpflichtung und Opt-Out kann man natürlich machen, indem man einfach den Chip deaktiviert.

Kurz noch zu den Geheimdiensten. Meine ganz faktische Befürchtung ist, dass sich hier Schattendatenbanken bilden. In § 26 Abs. 4 Personalausweisgesetz ist ganz klar geregelt, dass keine zentrale biometrische Datenbank errichtet werden soll. Das sollte auch nicht hinten herum über Geheimdienste entstehen. Herr Prof. Dr. Holznagel hatte den Dortmunder Anschlag argumentativ erwähnt. Dazu muss ich sagen: Es ist eine klassische Zuständigkeit der Polizei, wenn wir hier von Börsenterrorismus reden, der in Dortmund offenbar passiert ist. Da ergründet sich für mich nicht, warum das eine Begründung dafür sein soll, sämtlichen Geheimdiensten einen Zugriff zu erlauben, der zudem mit einer Protokollierung auf der abfragenden Seite erfolgt. Das wären zwei Forderungen, die ich hätte: Protokolliert werden sollte nicht nur bei der abfragenden Stelle, so dass überhaupt eine Kontrolle gegeben sein kann. Zweitens sollte jede dauerhafte Speicherung und Weitergabe dieser erlangten Daten, erst Recht ins Ausland, untersagt werden.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank Frau Dr. Kurz. Herr Prof. Dr. Holznagel, bitte.

SV **Prof. Dr. Bernd Holznagel**, LL.M. (Universität Münster): Im Dortmunder Fall hat das BKA gehandelt.

SVe **Dr. Constanze Kurz** (Chaos Computer Club, Berlin): Das ist doch eine Polizei.

SV **Prof. Dr. Bernd Holznagel**, LL.M. (Universität Münster): Ja, die werden aber jetzt erst ermächtigt, hier oben nicht. Aber das ist eine juristische Frage.

Lassen Sie mich kurz zur internationalen Frage etwas sagen. Ich kenne auch, wie Herr Prof. Dr. Margraf das schon ausgeführt hat, kein System, das staatlich vorgeschlagen oder aufgebaut wird, und das besser, datenschutzfreundlicher ist als das deutsche. Insofern sind wir da, glaube ich, sehr gut. Die andere Frage ist: Wo liegt das Worst-Case-Szenario? Wir wissen alle, dass Europa über keine relevanten Internetkonzerne verfügt. Die sind alle entweder in China oder den USA. Am weitesten in diesem Bereich, den wir hier diskutieren, ist China, und zwar seit Jahren. Ich war einmal drüben, das ist schon ein paar Jahre her, da waren wir bei Alibaba und haben mit der Regulierungsabteilung gesprochen. Die Regulierungsabteilung ist damals gerade von dem ehemaligen Staatssekretär aus dem Bereich der Informatisierung beschickt worden. Sie können sich vorstellen, dass in China die Verbindung von Staat und Wirtschaft sehr eng ist. Da brauchen Sie nicht solche Regelungen. In der Praxis ist es aber so – das ist jetzt ironisch formuliert – weil der direkte Zugriff des Staates unmittelbar ist. In China haben sie Alipay als jede Art von Bezahlung verfügbar. Wir haben schon vor sieben Jahren im Taxi mit unserem Mobiltelefon bezahlt. Sie mieten sich in Peking Fahrräder mit Alipay und diesen Geräten an. Meine Freunde, die hier aus Deutschland dort wohnen, sagen, dass es praktisch keinen alltäglichen Vorgang mehr gibt, der mit Bargeld bedient wird. Das alles setzt diese Identifizierung voraus.

Jetzt machen wir einmal ein Realexperiment. Ich habe jetzt parallel auf die App der Royal Bank of Canada gedrückt. Ich habe in Kanada studiert und bin immer wieder einmal zu Forschungsaufenthalten da. Ich habe allein jetzt Zugang zu meinem Konto und kann sofort eine Banküberweisung durchführen. Wir sind in den Möglichkeiten der Identifizierung sehr weit zurück. Die Möglichkeiten der öffentlichen Sicherheitsbehörden, darauf Zugriff zu nehmen, sind in China evident. Wie das in den USA genau ist, weiß ich nicht. Da hatten wir diese Großdiskussion, ob man hier überhaupt Apple mit dem normalen Pin-Code öffnen kann. Das weiß nur Apple, nicht die Sicherheitsbehörden. Damals ging das zu den Gerichten. Es ist nicht ausgeurteilt

worden, weil das Risiko seitens Apple zu hoch war, dass die Richter den Sicherheitsbehörden folgen und dann ihr Authentifizierungssystem durchlagen würden.

Das alles – Alipay, Apple – bezieht sich nur auf den privaten Bereich. Das sind alles private Transaktionen. Sie haben von der Seite des BSI ausgeführt. Sobald das in die hoheitlichen Transaktionen geht, können wir unmöglich eine Sicherheitsinfrastruktur nutzen, die irgendwie in privaten Händen ist. Wir enthaupten jede Art von Schutzfunktion des Deutschen Sozialstaates, wenn wir diesen Weg hier nicht gehen und irgendwie private Unternehmen einschalten. Ich denke, wir sind auf dem Weg, das Worst-Case-Szenario für unser Land zu realisieren. Wir haben – wie das vorhin einer der Kollegen gesagt hat – jetzt die letzte Möglichkeit, um das überhaupt noch auf national vernünftige Bahnen zu bringen.

Zur verfassungsrechtlichen Lage. Hier soll dauerhaft diese Funktion eingeschaltet werden. Jetzt schreibt der Datenschutzbeauftragte, das sei ein Eingriff in das Recht auf informationelle Selbstbestimmung. Ich sehe das gar nicht. Warum ist das Recht denn überhaupt tangiert? Wenn etwas tangiert ist, dann ist das die allgemeine Handlungsfreiheit, weil ich als Bürger gezwungen bin, diese Funktion dauerhaft aktiviert erleben zu müssen. Aber der Grundrechtseingriff ist doch an der Grenze der Bagatellschwelle, wenn ich überhaupt einen annehme. Weil ich einfach jederzeit die Sache sperren kann. Die Nutzung ist frei, das ist ausgeführt worden. Dass die Benutzung frei bleiben soll, schreibt die Begründung, da brauche ich aus meiner Sicht keine gesetzliche Klarstellung. Diese Sache ist rechtlich vollständig klar. Ich sehe in diesem Bereich überhaupt gar kein Problem.

Ein Problem fängt bei § 25 Absatz 2 des Entwurfs an. Frau Abgeordnete Jelpke, Sie hatten das gefragt. Wenn Sie einmal den § 25 Absatz 2 mitlesen, dann ist da enthalten, dass bisher nur die Polizei- und Ordnungsbehörden von den – ich nenne sie jetzt mal – Ausweisbehörden die Informationen bekommen können. Da ist immer noch gedacht, dass die Ausweisbehörden diejenigen sind, die diese Ausweisinformationen verwalten, sichern, speichern usw. Der nächste Schritt ist jetzt: Gibt es Möglichkeiten des automatisierten Verfahrens? Kann ich das direkt bekommen? In einer vernetzten Welt ist eigentlich naheliegend, dass ich das irgendwie auch automatisiert bekomme. Dennoch sagt das Gesetz schon für die Polizei- und Ordnungsbehörden: Nein, wir wollen keine bundesweite Datenbank für biometrische Daten haben – das wäre nämlich die Alternative – sondern wir wollen, dass das bei den Meldebehörden bleibt. Ihr könnt einen automatisierten Abruf bekommen, aber nur in besonderen Fällen, z. B. wenn die Meldebehörden nicht mehr erreichbar sind, also am Wochenende, ich nehme den einfachsten Fall. Jetzt ist das Interessante, dass dieser Fall – wann man die Meldebehörden nicht mehr erstmals kontaktieren muss und wann man automatisiert verfahren darf, nämlich dann, wenn die geschlossen haben – gerade nicht für die Nachrichtendienste aufgeführt ist. Wenn Sie nämlich den neuen § 25 Satz 2 Satz lesen, dann ist der vom Wortlaut her so abgefasst, dass diese Behörden jederzeit automatisch Zugriff zu den Lichtbildern bekommen. Dieser Regelfall: Geht erst zu den Meldebehörden, dann am Wochenende oder wenn es besondere Gründe gibt, dürft ihr automatisiert verfahren – diese Regelung gibt es gerade nicht, sondern sie können immer sofort automatisiert zugreifen. Das wird hier von den Sachverständigen kritisiert. Warum? Wegen § 26 Absatz 4, in dem klar steht: „Eine bundesweite Datenbank der biometrischen Merkmale wird nicht errichtet.“ Diese Norm wird quasi ausgehöhlt. Das ist jetzt vielleicht kein Verfassungsverstoß. Ich bin aber, weil der gesetzgeberische Wille, eigentlich keine bundesweite Datenbank haben zu wollen, so klar ist, gar nicht auf die verfassungsrechtliche Lage eingegangen. Sie wissen, dass das Bundesverfassungsgericht immer sehr vorsichtig ist, wenn der Staat solche zentrale Datenbanken aufbaut, wenn es daraus möglich werdende Profilbildungen gibt. Das hängt natürlich immer von den Einzelfällen ab. Es hängt auch von der Gefährdungslage ab, gerade wenn die Nachrichtendienste involviert sind. Ich glaube aber, man muss hier gar nicht in die verfassungsrechtliche Prüfung eintreten, weil einfach der Gesetzgeber so eine bundesweite Datenbank gar nicht aufbauen will. Eine Automatisierung, die ich beliebig – nur wenn ich sage: Hier ist eine Aufgabe, die von mir erfüllt werden muss – durchführe, damit komme ich zu solchen Datenbanken und das ist ein Widerspruch im Gesetz, der behoben werden muss.

Im Übrigen, ganz vorsichtig – Herr Abg. Özdemir, Sie hatten das gefragt – habe ich schon verfassungsrechtliche Bedenken, wenn man über diesen automatisierten Abruf faktisch so eine bundesweite Datenbank erstellen würde. Das ist dann in mehrerer Hinsicht problematisch: Ist das noch bestimmt? Wenn in § 26 Abs. 4 genau das Gegenteil steht, haben Sie schon das Bestimmtheitsproblem. Ist das mit dem Recht auf informationelle Selbstbestimmung vereinbar? Da wird es schwierig, das zu beurteilen. Das müsste man genauer prüfen. In der Tendenz würde ich sagen, das Verfassungsgericht wäre da kritisch. Ich vermute, dass man da hohe Risiken eingeht, die man, glaube ich, gar nicht eingehen muss, weil ich an sich finde, dass dieses Gesetz der richtige Ansatz ist. Ich finde auch, dass hier „alt“ diskutiert wird, Herr Abg. Dr. von Notz, das ist doch kein neues Denken. Das neue Denken ist: Wie bekommen wir das als staatliche sichere Infrastruktur auf die Mobiltelefone. Dann haben wir erst einmal Zugang zu 75 Prozent der Bevölkerung. Dann haben wir noch ein Digital-Divide-Problem: Was machen wir mit den älteren, mit denen, die sich das nicht leisten können? Wir wissen auch nicht, ob die Mobiltelefontarife immer so günstig bleiben. Da entstehen viele Folgefragen. Die sind nicht banal, aber wir müssen den Weg gehen, weil wir nicht zulassen können, dass alle unsere Identifikationsabläufe, Transaktionen primär durch Google oder Amazon gesteuert werden oder – wenn wir mit diesen aufgrund der bestehenden Regierung jetzt Probleme haben – dass wir dann chinesische Systeme verwenden. Das macht doch alles keinen Sinn.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank, Herr Prof. Dr. Holznagel. Dann gebe ich jetzt Herrn Fromm das Wort.

SV **Jens Fromm** (IT-Dienstleistungszentrum Berlin): Herr Abg. Wendt, vielen Dank für die Frage zu dem, was man über das Gesetz hinaus tun kann. Das ist mir ein großes Anliegen. Ich glaube, wir haben letztes oder vorletztes Jahr für den NKR eine spannende Studie zum Thema E-Government gemacht, die nicht besonders gut ausgefallen ist. Da ist der Personalausweis oder die eID-Funktion, über die wir heute reden, nur ein ganz kleiner Baustein. Was aber vom Bund, vom Parlament und den Verwaltungen insgesamt unterschätzt wird ist, dass man für E-Government oder für Anwendungen generell auch Werbung machen muss. Es ist nun einmal leider kein Selbstläufer, dass man irgendeine Anwendung ins Netz stellt und dann denkt, der Bürger fängt an es sofort begeistert zu nutzen. Das klappt in keiner Firma – es gibt vielleicht ein, zwei Beispiele – aber man muss hier schon auch Kampagnen fahren. Wichtig ist hierbei – das wurde in der Vergangenheit auch manchmal falsch gemacht – dass so eine Kampagne auch mit klaren Anwendungen unterlegt sein muss. Was meine ich: Wenn man für ein Produkt Werbung macht, dann muss man auch eine Anwendung dahinter haben. Man kann nicht einfach Werbung machen: „Wir haben jetzt E-Government“ – und dann geht der Bürger auf eine Webseite und findet nur irgendwelche Informationen. Der Bürger muss schon einen subjektiven Mehrwert spüren.

Ich habe ein paar Bespiele. Ich wundere mich nach wie vor, nach vielen Jahren Elster – das ist die elektronische Steuererklärung – dass man sich mittlerweile mit dem Personalausweis ein Elsterzertifikat machen lassen kann, das man herunterlädt, um sich eine Pin zu generieren und sich dann bei Elster mit diesem Zertifikat, das von dem Personalausweis mit einem eigens kreierten Pin generiert worden ist, einloggen kann. Das ist absurd.

Zweites Beispiel. Ich habe vor einiger Zeit, nämlich im Dezember, ein polizeiliches Führungszeugnis gebraucht. Das braucht man nicht so häufig, aber vielleicht doch ab und zu einmal. Das kann man mittlerweile mit dem Personalausweis beantragen. Ich war glücklich und habe das gemacht, denn ich habe die Infrastruktur, Frau Dr. Kurz, ich habe natürlich auch einen teuren Komfortkartenleser, ich kenne meine Pin noch, logge mich ein, registriere mich, identifiziere mich mit dem weltweit fast sichersten Dokument, um mir ein Führungszeugnis machen zu lassen. Im Prozess auf der Website des, glaube ich, Bundesjustizministeriums, steht plötzlich, dass ich ein Dokument, eine Datenschutzerklärung, ausdrucken, diese unterschreiben und dann wieder einscannen müsse, die könne ich dann gleich wieder hochladen. Das musste ich bei zwei Dokumenten machen. Ich hatte also dann für einen Prozess zwei Medienbrüche, wie man neudeutsch sagt. Da sollte man sich auch überlegen, wenn man dafür Werbung macht, das auch zu optimieren.

Drittes Beispiel könnte Kindergeld sein. Hier könnte man sicher auch etwas machen. Wir in Berlin werden außerdem – ich möchte noch kein Datum nennen, aber alsbald – die Parkraumbewirtschaftung angehen. Aufgrund unserer neuen Regierung in Berlin ist das Thema Parkraumbewirtschaftung im Ring, im Zentrum, wichtig. Das werden wir über die eID-Funktion etablieren. Hier ist auch eine konkrete Anwendung, die etwas bringen kann, und die man dann wiederum bewerben muss.

Frau Abg. Jelpke, wir haben uns vor zwei, drei Jahren intensiv mit ausländischen Lösungen im eID-Bereich beschäftigt. Wir haben uns alle EU-weiten eID-Lösungen angeschaut. Ausnahmslos alle kämpfen mit Akzeptanzproblemen. Es gibt verschiedene Ansätze, auf die ich keine Zeit habe einzugehen. Andere Länder haben es etwas cleverer gemacht, sie haben nämlich einfach angefangen. Z. B. die Niederlande haben mit ihrer DigiD vor drei, vier Jahren einfach gesagt, sie fangen langsam mit einem Nutzername-Passwort-Konzept an. Das ist extrem unsicher, aber so wurde der Bürger an eine Identität gewöhnt. Die Niederlande hatten innerhalb weniger Jahre extrem gute Nutzerzahlen.

Estland hat, was kritisiert worden ist, durch eine privatwirtschaftliche Lösung Erfolg gehabt. Sie haben nämlich gesagt: In Estland kann man ein öffentliches Nahverkehrsticket kaufen und hat da dann 20 Prozent Reduktion, quasi einen Discount. Das war sehr erfolgreich, hat sich dann aber auch nicht weiter durchgesetzt. Man kann aber festhalten, es wurde schon von Herrn Prof. Dr. Margraf gesagt: Keins dieser Länder hat ein ähnlich hohes Datenschutz- oder Sicherheitsniveau wie hier in Deutschland. Kein Land hat eine Vergabestelle für Berechtigungszertifikate. Darum noch einmal, denke ich, eine Absenkung von dem gegenwärtig extrem hohen Niveau würde nicht dazu führen, dass wir unter dem Niveau liegen. Wir würden immer noch weit über den Datenschutzanforderungen der anderen europäischen Länder liegen. Trotzdem plädiere ich dafür – das sieht das Gesetz glaube ich auch vor – eine Evaluierung nach fünf Jahren durchzuführen. Wenn man in den nächsten fünf Jahren merkt, dass es datenschutzrechtliche Probleme gibt, kann man das entsprechend wieder verschärfen.

Herr Abg. Dr. von Notz, ich könnte mich sogar amüsieren über Ihre Schilderung der tollen Features des neuen Personalausweises, wenn ich nicht so lange an dem Projekt gearbeitet hätte. Dann würde ich sicher auch darüber lächeln. Für mich war und ist immer die Frage gewesen – ich hatte auch 2009 in meinem Freundeskreis immer wieder diese Diskussion – brauchen wir so ein Dokument? Brauchen wir so eine staatliche Identität? Soll der Staat uns überwachen? Alles was man in Diskussionen nach dem ersten, zweiten Bier hört. Für mich war immer die Frage: Was ist der Fall, wenn wir keine virtuelle staatliche Identität haben? Das ist die spannende Frage. Ich will darauf keine Antwort geben, darüber kann man stundenlang drüber diskutieren. Für mich war immer entscheidend zu hinterfragen, ob wir wirklich im Bereich der Identifikation von großen Firmen abhängig sein wollen. Daher denke ich, ist das meine implizite Antwort, aber ich weiß, dass es hier ganz viele Antworten darauf gibt.

Frau Dr. Kurz hat die Mobile-Identity oder andere Lösungen in den Raum gestellt. Ich möchte hier noch einmal erläuternd sagen, dass wir auch stark unterscheiden müssen – das wurde bei dem Personalausweis getan – zwischen der Identifikation und der Authentifizierung. Bei dem Personalausweis rede ich in erster Linie immer von der Erstidentifikation. Diese Erstidentifikation in der virtuellen Welt ist wichtig. Wir brauchen – das ist zumindest die Hoffnung gewesen – eine staatliche, eine vertrauenswürdige Identität, die der Bürger, die Bürgerin nutzen kann, um dann auf kommerzielle Anwendungen wie z. B. Mobile-Identity oder FIDO oder sonstigen genannten Anwendungen aufbauen zu können. Darum finde ich eine kombinierte Lösung gut, die es zukünftig übrigens geben muss und wird, das ist unvermeidbar. Für mich war immer ein stückweit wichtig, eine sichere, vertrauenswürdige Identität zu haben, die für die Identifikation da ist.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank Herr Fromm. Dann könnten wir noch zu einer zweiten Runde kommen. Herr Kollege Wendt, bitte.

Abg. **Marian Wendt** (CDU/CSU): Das sind schon zwei spannende Themen, insgesamt eine spannende Diskussion.

Ich habe noch eine Frage an Herrn Fromm und Herrn Prof. Dr. Margraf. Inwieweit wirkt sich das gegenwärtige Verfahren für die Vergabe von

Berechtigung und Berechtigungszertifikaten auf die Verbreitung der online Ausweisfunktion aus? Wir haben jetzt auch ein Verfahren. Wenn Sie spezifizieren könnten, was vielleicht über den Gesetzentwurf hinaus aus Ihrer fachlichen Sicht noch möglich wäre?

Der zweite Bereich geht an Herrn Prof. Dr. Margraf. Er klang in ihrer Diskussion schon an und ist aus meiner Sicht auch eine Kernfrage, die wir uns stellen müssen. Wir haben mit dem Kerndatensystem bei Asylbewerbern ein einheitliches Personalmanagement, bei dem es eine ID-Funktion gibt, die sogar online ist und mit der ich jemanden deutschlandweit durch den Fingerabdruck durch verschiedene Behörden identifizieren kann. Bei der Frage Personalausweis und eID haben wir natürlich 16 verschiedene Datenbanken, das ist ja nur auf die Länder beschränkt. Die Frage wäre in Zukunft: Wie können wir, wenn wir zu einer einheitlichen eID-Funktion bzw. mit einer einheitlichen auch Personal- oder Bevölkerungsmanagementfunktion kommen wollen, diese Datenbanken miteinander verknüpfen, zentralisieren, um auch zu dieser österreichischen Lösung zu kommen. Diese basiert darauf, dass man seine Pass- oder Personalausweisnummer eingibt, die dann beim Benutzernamen angefragt wird – also Amazon Österreich fragt dann bei der Bundesdruckerei Österreich an, ob es diese Person gibt, ob die hinterlegt ist. Dann erfolgt die Freischaltung und wird die Transaktion über ein SMS-Tan-Verfahren noch einmal in einem zwei Faktorverfahren genehmigt. Vielleicht könnten Sie uns da noch einmal eine Hilfestellung geben, wie nötig das wäre, erst einmal diese Grundlagen zu schaffen. Der Personalausweis ist nicht nur ein Ausweisdokument, sondern wir wollen dahinter ein einheitliches System, ein einheitliches Bevölkerungsdatenmanagement haben.

Wenn Sie dazu noch ein paar Ausführungen machen könnten, wäre das sicherlich sehr hilfreich, auch für die nächste Wahlperiode.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank Herr Kollege Wendt. Frau Kollegin Jelpke, bitte.

BE Abg**. Ulla Jelpke** (DIE LINKE.): Vielleicht wäre es auch für die Änderung dieses Gesetzes hilfreich, wir diskutieren hier ja gerade über einen Gesetzentwurf.

Ich möchte auf jeden Fall Herrn Müller noch einmal die Möglichkeit geben, zu dem Punkt: „Verletzung informationelles Selbstbestimmungsrecht“ eine Antwort zu geben. Dann fand ich die Vorschläge, die auch Herr Prof. Dr. Holznagel hier gemacht hat, sehr interessant. Dazu würde ich gerne noch einmal ein kurzes Statement von Frau Dr. Kurz, Herrn Müller und Herrn Schönbohm hören. Sie, Herr Schönbohm, sind zwar kein unabhängiger Sachverständiger, weil Sie aus dem Haus kommen, aber Sie haben die Vorschläge mit erarbeitet und deswegen würde mich Ihr Statement insbesondere zu Herrn Prof. Dr. Holznagel interessieren.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank Frau Kollegin Jelpke. Herr Kollege Özdemir, bitte.

BE Abg. **Mahmut Özdemir** (Duisburg) (SPD): Ich würde gerne auch noch einmal auf die Frage der Zertifizierung zurückkommen und da Herrn Prof. Dr. Margraf ansprechen.

Wenn wir jetzt eine universelle Vergabe eines Zertifikates hätten, wäre das technisch, wirtschaftlich ein höherer Aufwand, als wenn man dienstebezogen mehrere Zertifikate ausstellt? Würde das einen höheren Aufwand darstellen?

Die Frage die sich daran anknüpft ist: Ich gebe jetzt einem Konzern ein einziges Zertifikat. Der münzt dann seine entsprechenden Dienste – etwa ein Konzern, 22 verschiedene Dienste – im gesamten Portfolio ein, und ein Dienst von diesen 22 hat einen Mangel, einen Hackerangriff, datenschutzrechtliche Probleme, wirtschaftliche Verknüpfungen oder Wirtschaftskriminalität. Entziehe ich dann ein einziges Zertifikat und mache das gesamte Geschäftsportfolio des Konzerns kaputt? Wäre das die Konsequenz aus dem Gesetzentwurf? Könnte man das dadurch regeln, dass man – darauf möchte ich hinaus – dienstebezogen verschiedene Zertifikate ausstellt und dann sagt, okay, du hast in deinem Konzern ein schwarzes Schaf, das machen wir dir kaputt, wir lassen dich aber wirtschaftlich mit deinen restlichen Geschäftsmodell auch weiterleben.

Die zweite Frage ist ein bisschen durch Herrn Prof. Dr. Holznagel angestoßen und richtet sich auch an Herrn Schönbohm. Wir haben gerade gehört, dass eine Erstauthentifizierung Richtung Mobilfunk und mobilfunkbasierter Dienste die Zukunft ist. Wenn wir hier einen Gesetzentwurf schaffen wollen und

heute schon in die Zukunft schauen, die die Lebensrealität der Menschen abdecken soll, inwieweit sind wir da im Hinblick auf Sicherheitstechnik gewappnet, dass sich nach dieser Erstauthentifizierung auch der von uns perpetuierte staatliche Identifikationsanspruch auch in diesen Diensten weiter wiederspiegelt? Welche Möglichkeiten haben wir, hier auch die Sicherheit der Bürgerinnen und Bürger zu gewährleisten?

Der letzte Komplex würde sich da noch einmal auf das EU-Recht und die Datenschutzgrundverordnung richten. Wir hatten eine relativ vernünftige Einwilligungsregelung im Hinblick auf Übernahme und Speicherung bei elektronischen Formularen. Da hat die EU einen abschließenden Katalog von sechs weiteren Bedingungen. Dadurch würde man, wenn man sich nur auf eine Einwilligungslösung versteift, den Rückgriff auf die EU-Regelung nationalrechtlich sperren.

Ich fand unsere Regelung grundsätzlich eine datenschutzrechtlich begrüßenswerte Lösung und mich würde interessieren, Herr Prof. Dr. Holznagel, aber auch Herr Müller, ob Sie das weiter problematisieren würden oder einfach nach derzeitigem Stand dann einfach unterpflügen. Mir wäre einfach an einer kurzen juristischen Expertise gelegen.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank Herr Kollege Özdemir. Herr Kollege Dr. von Notz, bitte.

BE Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Erst einmal ganz kurz bezugnehmend auf das, was Herr Prof. Dr. Holznagel gesagt hat. Das ist genau der Spagat der hier stattfinden soll. Es soll liberale Netzpolitik und das Leben praktisch gemacht werden, so dass wir von hier aus bei unserer kanadischen Bank eine Überweisung machen können. Ich meine, ich kann hier während dieser Sitzung auch ohne diese Technik eine Überweisung machen, das geht auch mit der Kreissparkasse Herzogtum Lauenburg, aber das Bedürfnis ist da. Dieses Ziel teilen wir ausdrücklich. Nur die Schwierigkeit ist, wie bei so vielen Dingen die aus dem BMI kommen: Zwei Herzen schlagen in Ihrer Brust. Sie können es dann nicht lassen, in dieses Gesetz auch diesen automatischen biometrischen Datenabgleich zu schreiben. Damit zerschießen Sie alles. Ich sage Ihnen nach acht Jahren Erfahrungen mal, wie das hier läuft und was kommen wird. Es wird auf Behördenseite maximale Sicherheitsbedenken geben, jemand wird falsch abgemeldet werden oder ähnliches. Und dann ist es genauso wie bei ELENA und der elektronischen Gesundheitskarte, in die wir schon Milliarden von Euro gesteckt haben, Herr Fromm – auch ohne Bier sehen die Leute das einfach kritisch. Dann bleibt am Ende nur der biometrische Datenabgleich von diesem schönen Gesetz. In der Praxis verändert sich nichts, denn im Einwohnermeldeamt Mölln besteht überhaupt kein Bedürfnis, diese Technik einzuführen. Die Anmeldezahlen liegen natürlich auch daran, dass in den kommunalen Behörden Leute sitzen, die sagen: „Ach, wissen Sie was Frau Müller, das brauchen Sie gar nicht, was wollen Sie denn damit? Lassen Sie das mal weg.“

Das haben wir nicht überwunden. Weil wir keine schönen Features geschaffen haben, die die Leute da selbst hineinlocken. Deswegen, glaube ich, droht uns hier wirklich dieses Problem und dieser Spagat. Dafür können der PSt Dr. Ole Schröder oder das BSI nichts, aber es ist in der Struktur angelegt, dass im BMI beide Interessen – datenschutzfreundliche Lösungen und die Dienste sollen schön hacken können – vorhanden sind. Das ist ein offener Widerspruch.

Ich will noch einmal einen Gedanken zu der wie ich finde relevanten Frage der Weitergabe von biometrischen Daten aus dieser Rasterung bringen. Vielleicht kann das auch Herr PSt Dr. Schröder beantworten. Nach welchen Kriterien soll da abgeglichen werden? Kann es dazu kommen, dass dann diese Daten ins Ausland an befreundete Dienste gegeben werden? Wie erklärt sich das eigentlich mit ihrem Umsetzungsgesetz – was wir auch gerade diskutieren – der Datenschutzgrundverordnung, hier kann vielleicht Herr Müller noch einmal etwas zu sagen, dass die BfDI zukünftig bei Diensten, insbesondere beim Bundesnachrichtendienst, explizit vor der Tür bleiben muss. Die darf uns gar nicht mehr berichten, was der BND für Dateien ansammelt. Ich sehe da wirklich krasse verfassungsrechtliche Probleme und teile trotzdem, das will ich an der Stelle noch einmal deutlich sagen, dieses Grundbedürfnis, dass es schön wäre, eine solche Technik hier zu implementieren. Allerdings auf

freiwilliger Basis: Überzeugen durch Technik. Aber genau das ist das, was hier auf dem Tisch liegt, gerade nicht.

Vors. **Ansgar Heveling** (CDU/CSU): Wir kämen dann zur Antwortrunde. Ich bitte, bei der Beantwortung die Uhr im Blick zu haben, denn in 20 Minuten schließe ich die Anhörung, deswegen bitte kurze und knappe Antworten. Wir beginnen jetzt mit Herrn Fromm.

SV **Jens Fromm** (IT-Dienstleistungszentrum Berlin): Ich hatte nur die eine Frage, ich mache es ganz kurz.

Wenn man sich anschaut, was gibt es eigentlich für Anwendungen? Nicht viele. Ich glaube, ich habe hier die Zahl gesehen, es gibt derzeit 233 Zertifikate die vergeben wurden oder 243, das ist schon einmal eine sehr überschaubare Zahl. Da stecken natürlich teilweise ganze Bundesländer dahinter. Es gibt auch Berechtigungszertifikate, bei denen dann ein ganzes Bundesland die Dienste nutzen kann. Daher ist es schwierig, diese Zertifikate dann Richtung Anwendung zu übertragen.

Ansonsten gibt es gerade im Verwaltungsbereich einige ehemals Bürger-, jetzt Servicekonten. Das ist die Idee, dass der Bürger über ein Konto auf Anträge zugreifen kann. Es gibt so ein paar Leuchtturmanwendungen wie ich gesagt habe: Elster mit beschränkter Handlungsfähigkeit oder das Kraftfahrt-Bundesamt, KBA, da kann man sogar live seine Punkte abfragen. Es war jahrelang so, dass einem mitgeteilt worden ist, dass man einen Brief bekommt, in dem die Punkte aufgeführt sind. Das kann man jetzt live abfragen. Es gibt aber auch ein paar wenige Versicherungen, auf die man zugreifen und entsprechend Verträge kündigen oder Ähnliches kann.

Zu den Fragen was man noch tun kann. Ich glaube, es wurde schon so viel versucht. Das Thema Normscreening z. B., wo auch auf Länderebene, Bundesebene geschaut wurde, wo Gesetze sind, die vereinfacht werden können, die elektronisch einfacher abgewickelt werden können. Aber das muss man sicher noch einmal forcieren. Es gab schon vor Jahren – aber es ist vielleicht auch an der Zeit, das zu wiederholen – den Versuch, Pilotprojekte zu schaffen. Es gab vor 10, 15, zu Media@com Zeiten noch die Idee für fünf konkrete Projekte, Kfz oder Meldewesen war z. B. so ein Thema. Was ist dabei herausgekommen? Ich glaube, man muss das dann wirklich vereinfachen und nicht das Elektronische so umsetzen, wie der derzeitige reale Prozess war.

Was mir heute in der Debatte ein bisschen zu kurz kommt ist: Es gibt so viele Menschen, die ihre Sachen elektronisch abwickeln wollen. Ja, es gibt auch welche, die das nicht können oder wollen. Aber zumindest diejenigen, die das nicht wollen, werden immer weniger. Es werden immer mehr, die bei uns anrufen und fragen: Warum kann ich das noch nicht elektronisch machen? Ich finde, wenn wir daran denken, was für Durchlaufzeiten wir haben. Wenn wir jetzt etwas am Gesetz ändern oder Sie, das Parlament, dann reden wir über eine Zeit von 10 Jahren, bis das den letzten Bürger, die letzte Bürgerin erreicht hat. Das sollte man auch ein bisschen im Blick haben.

Vors**. Ansgar Heveling** (CDU/CSU): Vielen Dank Herr Fromm, Herr Prof. Dr. Holznagel, bitte.

SV **Prof. Dr. Bernd Holznagel**, LL.M. (Universität Münster): Ich bin zu der europarechtlichen Vereinbarkeit dieses Regelwerkes gefragt worden. Ich sehe keine europarechtlichen Bedenken. Man könnte überlegen, ob das, wenn ich einen Bereich fördere, eine staatliche Beihilfe ist. Daran könnte man durchaus denken, weil man einen eigenständigen Sektor aufbaut. Man fördert diese Diensteanbieter. Das würde ich insgesamt dann verneinen, wenn es darum geht, dass man eine insbesondere auf den hoheitlichen Sektor bezogene Sicherheitsinfrastruktur aufbaut. Europarechtlich sehe ich vom Grundansatz keine Bedenken, auch nicht im Hinblick auf die Datenschutzgrundverordnung. Insofern denke ich, dass bis auf dieses Problem mit den Geheimdiensten – dazu habe ich hinreichend Stellung bezogen – keine grundlegenden verfassungs- oder europarechtlichen Bedenken bestehen.

Das was Herr Fromm sagte, spricht mir völlig aus dem Herzen – wir waren auf Sachverständigenseite ja eigentlich an keinem Punkt in irgendeinem Dissens: Man muss eben fördern und es liegt an dem Hohen Haus, das zu tun. Ich glaube, wir investieren jetzt an die 20 Mrd., oder auch 10 Mrd. Euro, in den Breitbandausbau. Wenn wir dann darüber diskutieren, dass wir nicht einmal 20 Millionen Euro haben, um so eine Infrastruktur sicherzustellen, dann passt da etwas nicht

zusammen. Woran es liegt, haben Sie soeben aufgeführt: Die Meldeämter, die Länder, haben da nur ein bedingtes Interesse, für den Identitätsnachweis zu werben. Es ist eine Frage, wie sich der Staat als Ganzes in Bund-Länder-Einheit organisiert. Wenn der Staat schon die ländlichen Infrastrukturen ausbaut – denn selbst im schönen Schleswig-Holstein werden Sie bald überall ein schnelles Internet haben – was machen Sie dann damit? Nur eine Infrastruktur zu finanzieren für Netflix und Amazon-Prime ist keine so ganz große Idee. Da wird man dem Bürger schon auch solche Anwendungen präsentieren müssen, sonst lohnt das Investment nicht. Aber da muss man vielleicht auch ein bisschen aus diesem Bereich für so eine Infrastruktur investieren, das ist jedenfalls meine Sicht. Das ist mehr eine politische Willensfrage als eine verfassungsrechtliche oder europarechtliche Frage. Vielen Dank.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank, Herr Prof. Dr. Holznagel. Frau Dr. Kurz, bitte.

SVe **Dr. Constanze Kurz** (Chaos Computer Club, Berlin): Ich würde nur noch kurz auf die letzte Problematik eingehen. Ich bin auch der Meinung, dass das Angebot bestehen bleiben sollte, es ist da und auch das Geld ist da. Ich glaube aber, dass es nicht nur an diesem Hohen Haus liegt, Angebote zu machen, sondern dass es sicherlich auch Angebote aus den Ländern, aus Landesbehörden sein werden, die interessante, attraktive Angebote machen müssen.

Ich fürchte, dass dieser Gesetzentwurf dieses Ziel mit einer bloßen, noch nicht zu einer Nutzung führenden Zwangsaktivierung und mit einem geringen Abbau bei der Berechtigungsbeantragung nicht erreichen wird. Ich glaube aber, dass dieses Ziel sehr wohl zu erreichen ist, nämlich in dem Sinne, dass manche Bürger für manche Bereiche diese eID benutzen werden. Sie ist nun einmal da. Ich glaube, mit dem Gesetz wird es nicht erreicht, aber das Ziel teilen wir durchaus.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank Frau Dr. Kurz. Herr Prof. Dr. Margraf bitte.

SV **Prof. Dr. Marian Margraf** (Freie Universität Berlin): Ganz kurz die Erklärung, Herr Abg. Wendt, wie das Verfahren heute bei der Vergabestelle für Berechtigungszertifikate aussieht.

Jetzt werden die Berechtigungszertifikate zweckgebunden vergeben. Es wird schon diskutiert, welche Datenkategorien aus dem Ausweis dann bezüglich dieses Zweckes ausgelesen werden dürfen. Das soll ja zukünftig dann in die zuständigen Datenschutzaufsichtsbehörden – wenn ich das Gesetz richtig interpretiere – verlagert werden. Zukünftig kann ein Diensteanbieter ein organisationsbezogenes Berechtigungszertifikat oder eine Berechtigung beantragen, sollte aber vorab mit seiner zuständigen Datenschutzaufsichtsbehörde klären, welche Daten er dann auslesen darf oder nicht. Das ist die Änderung.

Ich bin mir nicht ganz sicher, ob ich Ihre zweite Frage richtig verstanden habe. Ich beantworte sie so, wie ich sie interpretiere.

Die eID-Funktion ist so konstruiert, dass sie keine zentrale Datenbank braucht, weil die personenbezogenen Daten auf dem Chip des Ausweises gespeichert sind. Wenn man jetzt zukünftig andere Use Cases oder andere Endgeräte nutzen will, wie z. B. Smartphones in Österreich, dann kann man sich durchaus – jetzt mache ich ein bisschen Werbung, denn meine Arbeitsgruppe forscht daran – das Thema abgeleitete Identitäten anschauen, also wie bekomme ich die Daten vom Personalausweis sicher in das Smartphone. Da haben wir auch Sicherheitselemente drin und muss man sich anschauen, wie das dann alles funktioniert. Auch da sind die Daten dann eben aufgehoben, also lokal beim Nutzer, was datenschutzrechtlich immer deutlich besser ist, als eine zentrale Datenbank. Die Forschung geht eher in diese Richtung.

Herr Abg. Özdemir, die Fragen mit diesen organisationsbezogenen Zertifikaten habe ich mir auch gestellt. Ich habe das auch in meiner Stellungnahme problematisiert. Was passiert eigentlich, wenn ein großer Konzern eine Berechtigung bekommt, aber eine Abteilung damit Schindluder betreibt, wird dann unabhängig von den Folgen für den ganzen Konzern die Berechtigung zurückgezogen oder nicht? Das kann man heute nicht entscheiden. Auf der anderen Seite – so interpretiere ich zumindest das Gesetz – ist organisationsbezogen ein weitgefasster Begriff, d. h., in einem Konzern kann es 20 verschiedene Organisationen geben. Die Diensteanbieter sind weiterhin in der Lage, für verschiedene

Organisationseinheiten oder verschiedene Geschäftsprozesse auch verschiedene Berechtigungen zu beantragen. So könnte man das Problem vielleicht lösen. Wenn er nur eine Berechtigung hat, könnte man im Nachgang sagen, dass er dafür keine mehr bekommt, jetzt muss er für eine andere Organisation ein Berechtigungszertifikat beantragen. Das kann ich nicht entscheiden. Da kann ich das Gesetz nicht richtig interpretieren, ich bin Techniker. Ich denke, technische Lösungen gibt es, das habe ich da auch hineingeschrieben.

BE Abg. **Mahmut Özdemir** (Duisburg) (SPD): Also sollte es gesetzlich präzisiert werden?

SV **Prof. Dr. Marian Margraf** (Freie Universität Berlin): Ja, für mich ja. Das ist genau der Fall: Was passiert da eigentlich rein rechtlich, wenn die Berechtigung zurückgezogen werden muss, dass dann plötzlich 20 Geschäftsprozesse von einem Diensteanbieter betroffen sind, das weiß ich nicht. Wird man dann zurückziehen? Das kann ich nicht sagen.

SV **Prof. Dr. Bernd Holznagel**, LL.M. (Universität Münster): Das wird in einer Rechtsverordnung geregelt, so dass man das derzeit noch gar nicht sagen kann.

BE Abg. **Mahmut Özdemir** (Duisburg) (SPD): Es bedarf also einer gesetzlichen Präzisierung, darauf will ich hinaus.

SV **Prof. Dr. Marian Margraf** (Freie Universität Berlin): Es gibt jedenfalls technische Lösungen.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank Herr Prof. Dr. Margraf. Herr Müller, bitte.

SV **MDg Jürgen Müller** (Referatsgruppenleiter 2, Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Bonn): Es gab mehrere Fragen bzw. Zwischenfragen. Ich hoffe, ich habe das alles richtig verstanden.

Bei Herrn Abg. Özdemir hatte ich die Frage so verstanden, wie auch Herr Prof. Dr. Holznagel sie schon beantwortet hat, inwiefern sich aufgrund der europäischen Datenschutzgrundverordnung noch irgendwelche Komplikationen ergeben könnten. Da sehe ich, ähnlich wie Herr Prof. Dr. Holznagel, auch keine Probleme. Herr Abg. Dr. von Notz, Sie hatten im Zusammenhang mit dem Lichtbildabgleich die BND-Problematik angesprochen. Da hoffe ich nun auf den Innenausschuss, der jetzt am Mittwoch das Datenschutzanpassungsgesetz berät. In der Tat, da gibt es eine große Gefahr, dass durch eine dort vorhandene Regelung unsere Behörde, die BfDI, in bestimmten Bereichen das Parlament nicht einmal unterrichten darf. Das ist eine Regelung, die wir und insbesondere Frau Voßhoff, ganz konkret auch in der Anhörung schon thematisiert haben. Ob das noch Erfolg hat, werden Sie hier am Mittwoch beraten. Aber das ist in der Tat ein Bereich, der auch dazu führt, dass wir diesen automatisierten Lichtbildabgleich für die Nachrichtendienste generell ablehnen, weil man nicht weiß, was danach noch passiert. Das ist die eine Frage, ob der Abgleich erfolgt. Wer dann nachher noch welche Daten bekommt, das ist dann aus unserer Sicht völlig ungeklärt.

Frau Abg. Jelpke, Sie hatten wegen des informationellen Selbstbestimmungsrechts nachgefragt. Da ist zum einen das, was hier Herr Prof. Dr. Margraf bei der Frage der Berechtigungszertifikate ausgeführt hat: Die Bürger wissen nicht mehr, welche Daten wo von wem erhoben werden, weil die Zweckbindung fehlt. Aber das ist gerade das Essenzielle des Selbstbestimmungsrechts, dass jeder Bürger und jede Bürgerin wissen muss, welche Daten von wem für welche Zwecke wofür erhoben und übermittelt werden.

Was jetzt die Eingangsfrage angeht, die Frage der obligatorischen Aktivierung. Da gebe ich in gewisser Weise Herrn Prof. Dr. Holznagel auch recht: Allein durch die Tatsache, dass im Gesetz enthalten ist, dass die obligatorische Aktivierung nun zu erfolgen hat, ist der Eingriff noch nicht erfolgt. Dieser wird dann aber, und das ist dann unsere Sorge, spätestens dann erfolgen, wenn die freiwillige Nutzung nicht wirklich garantiert wird und ich dann als Bürgerin oder Bürger nicht mehr anders kann, als diese eID-Funktion zu nutzen. Deswegen wäre aus unserer Sicht eine Klarstellung im Gesetz erforderlich. Eine Begründung ist schön und gut, aber das fällt leider oft in Vergessenheit.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank Herr Müller. Herr Schönbohm, bitte.

SV **Arne Schönbohm** (Präsident des Bundesamtes für Sicherheit in der Informationstechnik, Bonn): Ich hatte zwei Fragen. Eine von Frau Abg. Jelpke, eine von Herrn Abg. Özdemir.

Frau Abg. Jelpke hatte gefragt, ob ich es genauso sehen, wie Herr Prof. Dr. Holznagel. Ich gehe davon aus, das war sehr stark auf das Thema Alibaba und anderes gerichtet, ob hier auch etwas Staatliches benötigt wird. Ja, das sehen wir so, dass man da bestimmte Infrastrukturen anbieten muss.

Vielleicht nur noch ein Thema. Wir reden das auch immer gerne schlecht. Ich habe mein Abitur in Nordrhein-Westfalen gemacht. Bei 51 Mio. neuen ausgegebenen Ausweisen und einem Drittel, das das nutzt, muss man nicht immer sagen, dass es zwei Drittel nicht nutzen. Ein Drittel sind 15 Mio., also mehr, als Österreich Einwohner hat, und die nutzen das. Von daher sind wir gar nicht mal so schlecht. Ich glaube, das ist so ein Thema, bei dem man auch mal sagen kann, dass man schon einmal eine Grundlage geschaffen hat. Ich glaube, das ist ein ganz wichtiges Thema, dass man darauf aufbaut und das auch dementsprechend weiter entwickelt.

Herr Abg. Özdemir, Sie haben das Thema angesprochen, wie zukunftssicher wir eigentlich sind. Vielleicht in Kurzform: Ich finde mit der Neuerung, z. B. NFC Schnittstelle, dass man das auch darüber nutzen und das mit dem Handy, mit dem Smartphone kombinieren kann, gut. Mir ist gerade die AusweisApp2 freigeschaltet worden für Android basierte Mobilegeräte. Es sind dort bereits mehr als 40 verschiedene Modelle bereit. Es geht natürlich darum, auch die Attraktivität zu steigern und dafür zu sorgen, dass dieses zunehmend auch weiter entwickelt wird. Darum ist es, glaube ich, notwendig, dass es hier so eine Art Initialzündung gibt, um dann eine stärkere Geschwindigkeit aufzunehmen. Das ist ein grundsätzliches Thema, wie der Lauf zwischen Hase und Igel, an dem man natürlich arbeiten muss. Ich denke, da hat man die ersten Grundlagen für gelegt.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank Herr Schönbohm. Meine sehr geehrten Damen und Herren Sachverständige, liebe Kolleginnen und Kollegen, ich darf mich ganz herzlich für die Statements und die Beantwortung der Fragen bedanken. Wir werden in die weitere Beratung einsteigen. Für heute darf ich die Anhörung und die Sitzung des Innenausschusses schließen.

Schluss der Sitzung: 12.25 Uhr

Ansgar Heveling, MdB

Vorsitzender

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
18(4)868 A

Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Andrea Voßhoff
Bundesbeauftragte für den Datenschutz
und die Informationsfreiheit

POSTANSCHRIFT Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Postfach 1468, 53004 Bonn

Vorsitzenden des Innenausschusses
des Deutschen Bundestages
Herrn Ansgar Heveling
ansgar.heveling@bundestag.de

Mitglied des Deutschen Bundestages
Herrn Stephan Mayer (Altötting)
stephan.mayer@bundestag.de

Mitglied des Deutschen Bundestages
Herrn Burkhard Lischka
burkhard.lischka@bundestag.de

Mitglied des Deutschen Bundestages
Frau Ulla Jelpke
ulla.jelpke@bundestag.de

Mitglied des Deutschen Bundestages
Frau Irene Mihalic
irene.mihalic@bundestag.de

Mitglied des Deutschen Bundestages
Herrn Heinrich Zertik
heinrich.zertik@bundestag.de

Mitglied des Deutschen Bundestages
Herrn Mahmut Özdemir (Duisburg)
mahmut.oezdemir@bundestag.de

Mitglied des Deutschen Bundestages
Herrn Dr. Konstantin von Notz
konstantin.notz@bundestag.de

nachrichtlich:
Sekretariat des Innenausschusses
des Deutschen Bundestages

HAUSANSCHRIFT Husarenstraße 30, 53117 Bonn
VERBINDUNGSBÜRO Friedrichstraße 50, 10117 Berlin

TELEFON (0228) 997799-100
TELEFAX (0228) 997799-550
E-MAIL referat13@bfdi.bund.de

INTERNET www.datenschutz.bund.de

DATUM Bonn, 13.04.2017
GESCHÄFTSZ. **21-206-6/002#0003**

Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.

Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

 innenausschuss@bundestag.de

BETREFF **Personalausweisgesetz**

Sehr geehrter Herr Vorsitzender, sehr geehrte Damen und Herren Abgeordnete,

für die Gelegenheit, mich im Rahmen der öffentlichen Anhörung im Innenausschuss des Deutschen Bundestages am Montag, den 24. April 2017, zum Entwurf eines Gesetzes zur Förderung des elektronischen Identitätsnachweises äußern zu dürfen, bedanke ich mich ausdrücklich. Aus terminlichen Gründen ist mir eine persönliche Teilnahme jedoch leider nicht möglich. Für mein Haus wird Herr Ministerialdirigent Müller an der Anhörung als Sachverständiger teilnehmen.

Im Rahmen der Ressortabstimmung zu diesem Gesetzentwurf hatte ich bereits Gelegenheit, meine datenschutzrechtliche Bewertung und Änderungswünsche zu äußern. Diesen ist mit dem jetzt vorliegenden Entwurf jedoch nur zum Teil Rechnung getragen worden. Daher nehme ich gerne die Gelegenheit wahr, Ihnen meine datenschutzrechtlichen Bedenken aufzuzeigen und meine Formulierungsvorschläge zum Gesetzentwurf zur Kenntnis zu geben. Die Einzelheiten finden Sie in dem anliegenden Positionspapier.

Mit freundlichen Grüßen

Andrea Voßhoff

Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Bonn, den 13. April 2017

Stellungnahme

der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

zur öffentlichen Anhörung des Innenausschusses des Deutschen Bundestages

am 24. April 2017

zum

Entwurf eines Gesetzes
zur Förderung des elektronischen Identitätsnachweises

Bundestags-Drucksache 18/11279

Das Bundeskabinett hat am 9. Dezember 2016 den Entwurf eines Gesetzes zur Förderung des elektronischen Identitätsnachweises verabschiedet. Hierzu führt der Innenausschuss des Deutschen Bundestages am 24. April 2017 eine öffentliche Anhörung durch.

Im Rahmen der Ressortabstimmung zu diesem Gesetzentwurf hatte ich bereits Gelegenheit, meine datenschutzrechtliche Bewertung und Änderungswünsche zu äußern. Diesen ist mit dem jetzt vorliegenden Entwurf jedoch nur zum Teil Rechnung getragen worden. Nach meiner Auffassung werden mit dem vorliegenden Gesetzentwurf nach wie vor das Recht auf informationelle Selbstbestimmung der Bürgerinnen und Bürger übergangen und Datenschutz sichernde Standards unterlaufen. Dies gilt insbesondere für die Regelungen zur Nutzung der eID-Funktion sowie das Verfahren zur Vergabe sogenannter Berechtigungszertifikate nach § 21 PAuswG-E.

Wie nachfolgend aufgeführt, halte ich daher Änderungen des Entwurfs eines Gesetzes zur Förderung des elektronischen Identitätsnachweises (Bundestags-Drucksache 18/11279) für notwendig:

I. Artikel 1
Änderung des Personalausweisgesetzes (PAuswG)

I.1. § 10 Absatz 1 PAuswG-E

§ 10 Absatz 1 PAuswG-E lautet:

(1) Der Personalausweis wird mit einer Funktion zum elektronischen Identitätsnachweis nach § 18 ausgegeben.

Vorschlag BfDI:

(1) Der Personalausweis wird mit einer Funktion zum elektronischen Identitätsnachweis nach § 18 ausgegeben. ***Die Nutzung dieser Funktion durch den Ausweisinhaber ist freiwillig.***

Begründung:
Die obligatorische Aktivierung der Funktion zum elektronischen Identitätsnachweis (eID-Funktion) ist nur dann hinnehmbar, wenn dauerhaft sichergestellt ist, dass daraus keine verpflichtende Nutzung der eID-Funktion resultiert. Die Entscheidung über die Nutzung der eID-Funktion muss allein bei den Bürgerinnen und Bürgern liegen. Nur so kann deren informationelles Selbstbestimmungsrecht gewahrt bleiben.

I.2. § 11 Absatz 3 PAuswG-E

§ 11 Absatz 3 PAuswG-E lautet:

(3) Die Personalausweisbehörde hat die antragstellende Person bei Antragstellung über den elektronischen Identitätsnachweis nach § 18 und das Vor-Ort-Auslesen nach § 18a sowie über Maßnahmen zu unterrichten, die erforderlich sind, um die Sicherheit der Nutzung des elektronischen Identitätsnachweises zu gewährleisten. Sie soll der antragstellenden Person die Übergabe von entsprechendem Informationsmaterial anbieten.

Vorschlag BfDI:

(3) Die Personalausweisbehörde hat die antragstellende Person bei Antragstellung ***schriftlich nach bundesweit einheitlicher Vorgabe*** über den elektronischen Identitätsnachweis nach § 18 und das Vor-Ort-Auslesen nach § 18a sowie über Maßnahmen zu unterrichten, die erforderlich sind, um die Sicherheit der Nutzung des elektronischen Identitätsnachweises zu gewährleisten. ***[…]***

Begründung:
Das Angebot von Informationsmaterial ist nicht ausreichend. Die bisherige Verpflichtung, über die eID-Funktion des Personalausweises schriftlich zu unterrichten, sollte daher beibehalten werden. Nur durch eine bundesweit einheitliche Vorgabe zu einer solchen Information wird sichergestellt, dass alle Bürgerinnen und Bürger in hinreichend verständlicher Form aufgeklärt werden.

I.3. § 18 Absatz 4 und 5 PAuswG-E

§ 18 Absatz 4 und 5 PAuswG-E lauten:

(4) Die Daten werden nur übermittelt, wenn der Diensteanbieter ein gültiges Berechtigungszertifikat an den Personalausweisinhaber übermittelt und dieser in der Folge seine Geheimnummer eingibt. Vor Eingabe der Geheimnummer durch den Personalausweisinhaber muss der Diensteanbieter dem Ausweisinhaber die Gelegenheit bieten, die folgenden Daten einzusehen:
1. Name, Anschrift und E-Mail-Adresse des Diensteanbieters,
2. Kategorien der zu übermittelnden Daten nach Absatz 3 Satz 2,
3. (aufgehoben)
4. Hinweis auf die für den Diensteanbieter zuständigen Stellen, die die Einhaltung der Vorschriften zum Datenschutz kontrollieren,
5. letzter Tag der Gültigkeitsdauer des Berechtigungszertifikats.

(5) Die Übermittlung ist auf die im Berechtigungszertifikat genannten Datenkategorien beschränkt.

Vorschlag BfDI:

(4) Die Daten werden nur übermittelt, wenn der Diensteanbieter ein gültiges Berechtigungszertifikat an den Personalausweisinhaber übermittelt und dieser in der Folge seine Geheimnummer eingibt. Vor Eingabe der Geheimnummer durch den Personalausweisinhaber muss der Diensteanbieter dem Ausweisinhaber die Gelegenheit bieten, die folgenden Daten einzusehen:
1. Name, Anschrift und E-Mail-Adresse des Diensteanbieters,
2. Kategorien der zu übermittelnden Daten nach Absatz 3 Satz 2,
3. ***Zweck der Übermittlung*****,**
4. Hinweis auf die für den Diensteanbieter zuständigen Stellen, die die Einhaltung der Vorschriften zum Datenschutz kontrollieren,
5. letzter Tag der Gültigkeitsdauer des Berechtigungszertifikats.

(5) Die Übermittlung ist auf die im Berechtigungszertifikat genannten Datenkategorien beschränkt. ***Der Personalausweisinhaber kann die Übermittlung auch dieser Datenkategorien im Einzelfall ausschließen.***

Begründung:
Vor einer Datenübermittlung aus dem Personalausweis müssen die Bürgerinnen und Bürger Kenntnis über den Zweck der Übermittlung erhalten. Zur Wahrung des Rechts auf informationelle Selbstbestimmung müssen die Betroffenen stets nachvollziehen können, in welchem konkreten Kontext ihre Identitätsdaten übermittelt werden. Dies war nach der bisherigen Fassung des § 18 Absatz 4 Satz 2 Nummer 3 PAuswG möglich. Daher sollte Nummer 3 weiter beibehalten werden. Zudem sollte die bisherige Möglichkeit, die Übermittlung einzelner Datenkategorien ausschließen zu können (§ 18 Absatz 5 Satz 2 PAuswG), auch weiter gelten.

I.4 § 20 Absatz 2 PAuswG-E

§ 20 Absatz 2 PAuswG-E lautet:

(2) Der Ausweis darf nur vom Ausweisinhaber oder von anderen Personen mit Zustimmung des Ausweisinhabers in der Weise abgelichtet werden, dass die Ablichtung eindeutig und dauerhaft als Kopie erkennbar ist. Andere Personen als der Ausweisinhaber dürfen die Kopie nicht an Dritte weitergeben. Werden durch Ablichtung personenbezogene Daten aus dem Personalausweis erhoben oder verarbeitet, so darf die datenerhebende oder -verarbeitende Stelle dies nur mit Einwilligung des Ausweisinhabers tun. Die Vorschriften des allgemeinen Datenschutzrechts über die Erhebung und Verwendung personenbezogener Daten bleiben unberührt.

Vorschlag BfDI:

(2) Der Ausweis darf nur vom Ausweisinhaber oder von anderen Personen mit Zustimmung des Ausweisinhabers in der Weise abgelichtet werden, dass die Ablichtung eindeutig und dauerhaft als ***Ablichtung*** erkennbar ist. ***Vor der Ablichtung ist die Erforderlichkeit der Ablichtung zu prüfen. Die Ablichtung darf ausschließlich zu Identifizierungszwecken verwendet werden und ist auf die hierfür notwendigen Daten zu beschränken. Die Ablichtung ist unverzüglich zu vernichten, sobald der mit der Ablichtung verfolgte Zweck erreicht ist***. Andere Personen als der Ausweisinhaber dürfen die Ablichtung nicht an Dritte weitergeben.
Werden durch Ablichtung personenbezogene Daten aus dem Personalausweis erhoben oder verarbeitet, so darf die datenerhebende oder -verarbeitende Stelle dies nur mit Einwilligung des Ausweisinhabers tun. Die Vorschriften des allgemeinen Da-

tenschutzrechts über die Erhebung und Verwendung personenbezogener Daten bleiben unberührt.

Begründung:
Nach der vorgesehenen Änderung im PAuswG-E ist das Ablichten (als Oberbegriff für Kopieren, Fotografieren und Scannen) mit Einwilligung des Inhabers erlaubt. Neben der Einwilligung ist lediglich erforderlich, dass die Ablichtung eindeutig und dauerhaft als Kopie erkennbar ist.
Es ist zu vermuten, dass unter Anwesenden das Ablichten zwar regelmäßig nicht erforderlich, allerdings „praktisch“ ist. Es besteht daher die Gefahr, dass aus Gründen der Praktikabilität auf die Prüfung der Erforderlichkeit verzichtet wird.

I.5. § 21 PAuswG-E

§ 21 PAuswG-E lautet:

(1) Um Daten im Wege des elektronischen Identitätsnachweises anzufragen, benötigen Diensteanbieter eine Berechtigung. Die Berechtigung lässt datenschutzrechtliche Vorschriften unberührt. Das Vorliegen einer Berechtigung ist durch die Vergabe von Berechtigungszertifikaten technisch abzusichern.

(2) Die Berechtigung wird auf Antrag erteilt. Die antragstellende Person muss die Daten nach § 18 Absatz 4 Satz 2 Nummer 1, 2 und 4 angeben. Die Berechtigung ist zu erteilen, wenn

1. *der Diensteanbieter seine Identität gegenüber der Vergabestelle für Berechtigungszertifikate nachweist,*
2. *der Diensteanbieter das dem Antrag zu Grunde liegende Interesse an einer Berechtigung darlegt und*
3. *der Vergabestelle für Berechtigungszertifikate keine Anhaltspunkte für eine missbräuchliche Verwendung der Daten vorliegen.*

(3) Die Berechtigung ist zu befristen. Die Gültigkeitsdauer darf einen Zeitraum von drei Jahren nicht überschreiten. Die Berechtigung darf nur von dem im Berechtigungszertifikat angegebenen Diensteanbieter verwendet werden. Sie wird auf Antrag wiederholt erteilt.

(4) Die Berechtigung ist zurückzunehmen, wenn der Diensteanbieter diese durch Angaben erwirkt hat, die in wesentlicher Beziehung unrichtig oder unvollständig waren. Sie ist zu widerrufen, wenn sie nicht oder nicht im gleichen Umfang hätte erteilt werden dürfen. Die Berechtigung soll zurückgenommen oder widerrufen werden, wenn die für den Diensteanbieter zuständige Datenschutzaufsichtsbehörde die Rücknahme oder den Widerruf verlangt, weil Tatsachen die Annahme rechtfertigen, dass der Diensteanbieter die auf Grund der Nutzung des Berechtigungszertifikates erhaltenen personenbezogenen Daten in unzulässiger Weise verarbeitet oder nutzt

(5) Mit Bekanntgabe der Rücknahme oder des Widerrufs der Berechtigung darf der Diensteanbieter vorhandene Berechtigungszertifikate nicht mehr verwenden. Dies gilt nicht, solange und soweit die sofortige Vollziehung (§ 30) ausgesetzt worden ist.

(6) Der Diensteanbieter hat Änderungen der Angaben nach § 18 Absatz 4 Satz 2 Nummer 1 und 4 der Vergabestelle für Berechtigungszertifikate unverzüglich mitzuteilen.

(7) Öffentliche Stellen anderer Mitgliedstaaten der Europäischen Union sind berechtigt, Daten im Wege des elektronischen Identitätsnachweises anzufragen.

(8) Die Vergabestelle für Berechtigungszertifikate führt ein Register über die erteilten Berechtigungen.

Vorschlag BfDI:

(1) ***Diensteanbieter erhalten unter den Voraussetzungen des Absatzes 2 auf schriftlichen Antrag die Berechtigung, die für die Wahrnehmung ihrer Aufgaben oder Geschäftszwecke erforderlichen Daten im Wege des elektronischen Identitätsnachweises beim Inhaber des Personalausweises mittels eines Berechtigungszertifikats anzufragen. Die zuständige Stelle nach § 7 Abs. 4 Satz 1 stellt hierzu den Diensteanbietern Berechtigungen nach den nachstehenden Bestimmungen aus und stellt den Diensteanbietern entsprechende Berechtigungszertifikate über jederzeit öffentlich erreichbare Kommunikationsverbindungen zur Verfügung. In dem Antrag sind die Daten nach § 18 Abs. 4 Satz 2 Nr. 1 bis 4 anzugeben.***

(2) ***[…]*** Die Berechtigung nach Absatz 1 ist zu erteilen, wenn

***1. der angegebene Zweck nicht rechtswidrig ist**,*
2. der antragstellende Diensteanbieter die Erforderlichkeit der zu übermittelnden Angaben für den beschriebenen Zweck nachgewiesen hat,
3. die Anforderungen, insbesondere an Datenschutz und Datensicherheit, gemäß der Rechtsverordnung nach § 34 Nr. 7 erfüllt sind und
4. keine Anhaltspunkte für eine missbräuchliche Verwendung der Berechtigung vorliegen.

Der Diensteanbieter hat durch Selbstverpflichtung die Anforderungen nach Nummer 3 schriftlich zu bestätigen und auf Anforderung nachzuweisen.

(3) Die Berechtigung ist zu befristen. Die Gültigkeitsdauer darf einen Zeitraum von drei Jahren nicht überschreiten. Die Berechtigung darf nur von dem im Berechtigungszertifikat angegebenen Diensteanbieter ***und nur zu dem darin vorgesehenen Zweck*** verwendet werden. ***Die Berechtigung kann mit Nebenbestimmungen versehen*** und auf entsprechenden Antrag wiederholt erteilt werden.

(4) Änderungen der ***Daten*** und Angaben ***nach Absatz 1 Satz 3*** sind der ***zuständigen Stelle gemäß § 7 Abs. 4 Satz 1*** unverzüglich mitzuteilen.

(***5***) Die Berechtigung ist zurückzunehmen, wenn der Diensteanbieter diese durch Angaben erwirkt hat, die in wesentlicher Beziehung unrichtig oder unvollständig waren. Sie ist zu widerrufen, wenn sie nicht oder nicht im gleichen Umfang hätte erteilt werden dürfen. Die Berechtigung soll zurückgenommen oder widerrufen werden, wenn die für den Diensteanbieter zuständige Datenschutzaufsichtsbehörde die Rücknahme oder den Widerruf verlangt, weil Tatsachen die Annahme rechtfertigen, dass der Diensteanbieter die auf Grund der Nutzung des Berechtigungszertifikates erhaltenen personenbezogenen Daten in unzulässiger Weise verarbeitet oder nutzt

(***6***) Mit Bekanntgabe der Rücknahme oder des Widerrufs der Berechtigung darf der Diensteanbieter vorhandene Berechtigungszertifikate nicht mehr verwenden. Dies gilt nicht, solange und soweit die sofortige Vollziehung (§ 30) ausgesetzt worden ist

(7) Öffentliche Stellen anderer Mitgliedstaaten der Europäischen Union sind berechtigt, Daten im Wege des elektronischen Identitätsnachweises anzufragen.

(8) Die Vergabestelle für Berechtigungszertifikate führt ein Register über die erteilten Berechtigungen.

Begründung:
Die bisherige Praxis der Vergabe von Berechtigungszertifikaten erfährt mit dem PAuswG-E eine grundsätzliche Änderung. Die Vergabestelle für Berechtigungszertifikate soll zukünftig nur noch die Identität des Diensteanbieters prüfen und ob Anhaltspunkte für eine missbräuchliche Verwendung der Daten vorliegen. Die Daten nach § 18 Absatz 4 Satz 2 Nummer 1, 2 und 4 PAuswG (Name, Anschrift und E-Mail-Adresse des Anbieters, die Kategorien der zu übermittelnden Daten nach § 18 Absatz 3 Satz 2 PAuswG und der Hinweis auf die für den Diensteanbieter zuständigen Stellen, die die Einhaltung der Vorschriften zum Datenschutz kontrollieren) müssen zwar im Antrag an die Vergabestelle für Berechtigungszertifikate übermittelt werden, aber eine irgendwie geartete inhaltliche Prüfung ist damit nicht mehr verbunden.

Um sicherzustellen, dass Diensteanbieter nur die für den jeweiligen Geschäftsprozess erforderlichen Angaben übermittelt bekommen, sollte an der aktuellen Rechtslage festgehalten werden, nach der der antragstellende Diensteanbieter die Erforderlichkeit der aus der eID-Funktion des Personalausweises zu übermittelnde Angaben nachweisen muss und an den jeweils festgelegten Zweck gebunden ist.
Im Übrigen sollten Berechtigungszertifikate nur an Diensteanbieter erteilt werden, die Datenschutz und Datensicherheit gewährleisten. Daher sollten antragstellende Diensteanbieter wie bisher durch eine Selbstverpflichtung die Erfüllung dieser Anforderungen schriftlich bestätigen und nachweisen müssen.

Außerdem weise ich darauf hin, dass sich nach der von der Bundesregierung geplanten Gesetzesänderung möglicherweise ein zusätzlicher – nicht bezifferbarer - Mehraufwand bei der repressiven Verfolgung von Verstößen bei meinem Hause und insbesondere bei den Landesdatenschutzbeauftragten entstehen kann, da eine inhaltliche Vorabprüfung der Diensteanbieter seitens der Vergabestelle für Berechtigungszertifikate nach der vorgesehenen Änderung des PAuswG nicht mehr erfolgt.

II. Artikel 2
Weitere Änderung des Personalausweisgesetzes zum 1. Mai 2021

§ 25 Absatz 2 PAuswG-E

§ 25 Absatz 2 PAuswG-E lautet:

(2) Die Ordnungsbehörden, die Steuerfahndungsstellen der Länder sowie die Behörden der Zollverwaltung dürfen das Lichtbild zum Zweck der Verfolgung von Straftaten und Verkehrsordnungswidrigkeiten im automatisierten Verfahren abrufen, wenn die Personalausweisbehörde auf andere Weise nicht erreichbar ist und ein weiteres Abwarten den Ermittlungszweck gefährden würde. Zuständig für den Abruf sind die Polizeivollzugsbehörden auf Ebene der Landkreise und kreisfreien Städte, die durch Landesrecht bestimmt werden. Die Polizeien des Bundes und der Länder, das Bundesamt für Verfassungsschutz, der Militärische Abschirmdienst, der Bundesnachrichtendienst sowie die Verfassungsschutzbehörden der Länder dürfen das Lichtbild zur Erfüllung ihrer Aufgaben im automatisierten Verfahren abrufen. Die abrufende Behörde trägt die Verantwortung dafür, dass die Voraussetzungen der Absätze 1 und 2 Satz 1 vorliegen. Alle Abrufe sind von den beteiligten Behörden so zu protokollieren, dass eine Kontrolle der Zulässigkeit der Abrufe möglich ist. Die Protokolle enthalten:

1. *Familienname, Vornamen sowie Tag und Ort der Geburt der Person, deren Lichtbild abgerufen wurde,*
2. *Tag und Uhrzeit des Abrufs,*
3. *die Bezeichnung der am Abruf beteiligten Stellen,*
4. *die Angabe der abrufenden und der den Abruf anordnenden Person sowie*
5. *das Aktenzeichen.*

§ 24 Abs. 3 Satz 5 gilt entsprechend.

Vorschlag BfDI:

(2) Die ***Polizei- und*** Ordnungsbehörden, die Steuerfahndungsstellen der Länder sowie die Behörden der Zollverwaltung dürfen das Lichtbild zum Zweck der Verfolgung von Straftaten und Verkehrsordnungswidrigkeiten im automatisierten Verfahren abrufen, wenn die Personalausweisbehörde auf andere Weise nicht erreichbar ist und ein weiteres Abwarten den Ermittlungszweck gefährden würde. Zuständig für den Abruf sind die Polizeivollzugsbehörden auf Ebene der Landkreise und kreisfreien Städte, die durch Landesrecht bestimmt werden. ***[...]*** Die abrufende Behörde trägt die Verantwortung dafür, dass die Voraussetzungen der Absätze 1 und 2 Satz 1 vorliegen. Alle Abrufe sind von den beteiligten Behörden so zu protokollieren, dass eine Kontrolle der Zulässigkeit der Abrufe möglich ist. Die Protokolle enthalten:

1. Familienname, Vornamen sowie Tag und Ort der Geburt der Person, deren Lichtbild abgerufen wurde,
2. Tag und Uhrzeit des Abrufs,
3. die Bezeichnung der am Abruf beteiligten Stellen,

4. die Angabe der abrufenden und der den Abruf anordnenden Person sowie
5. das Aktenzeichen.

§ 24 Abs. 3 Satz 5 gilt entsprechend.

Begründung:

Mit § 25 Abs. 2 Satz 3 PAuswG-E soll ein nahezu voraussetzungsloser Abruf des Lichtbildes im automatisierten Verfahren durch die Polizeibehörden des Bundes und der Länder, das Bundesamt für Verfassungsschutz, die Landesämter für Verfassungsschutz, den Militärischen Abschirmdienst und den Bundesnachrichtendienst eingeführt werden. Dies wird aus datenschutzrechtlicher Sicht abgelehnt.
Bisher dürfen zur Verfolgung von Straftaten und Verkehrsordnungswidrigkeiten insbesondere die Polizeibehörden Lichtbilder automatisiert abrufen, wenn die Personalausweisbehörde nicht erreichbar ist und ein weiteres Abwarten den Ermittlungszweck gefährdet. Diese gesetzlichen Einschränkungen für das Abrufverfahren sollen nun entfallen und zusätzlich sollen alle Nachrichtendienste zukünftig voraussetzungslos Lichtbilder abrufen können.
Die bisherige Rechtslage ist jedoch völlig ausreichend.

III. Artikel 3
Änderung des Passgesetzes

§ 18 Absatz 3 Passgesetz-E

§ 18 Absatz 3 Passgesetz-E lautet:

(3) Der Pass darf nur vom Passinhaber oder von anderen Personen mit Zustimmung des Passinhabers in der Weise abgelichtet werden, dass die Ablichtung eindeutig und dauerhaft als Kopie erkennbar ist. Andere Personen als der Passinhaber dürfen die Kopie nicht an Dritte weitergeben. Werden durch Ablichtung personenbezogene Daten aus dem Pass erhoben oder verarbeitet, so darf die datenerhebende oder -verarbeitende Stelle dies nur mit Einwilligung des Passinhabers tun. Die Vorschriften des allgemeinen Datenschutzrechts über die Erhebung und Verwendung personenbezogener Daten bleiben unberührt.

Vorschlag BfDI:

(2) Der Pass darf nur vom Passinhaber oder von anderen Personen mit Zustimmung des Passinhabers in der Weise abgelichtet werden, dass die Ablichtung eindeutig und dauerhaft als Ablichtung erkennbar ist. ***Vor der Ablichtung ist die Erforderlichkeit der Ablichtung zu prüfen. Die Ablichtung darf ausschließlich zu Identifizierungszwecken verwendet werden und ist auf die hierfür notwendigen Daten zu beschränken. Die Ablichtung ist unverzüglich zu vernichten, sobald der mit der Ablichtung verfolgte Zweck erreicht ist.*** Andere Personen als der Passinhaber dürfen die Ablichtung nicht an Dritte weitergeben.
Werden durch Ablichtung personenbezogene Daten aus dem Pass erhoben oder verarbeitet, so darf die datenerhebende oder -verarbeitende Stelle dies nur mit Einwilligung des Passinhabers tun. Die Vorschriften des allgemeinen Datenschutzrechts über die Erhebung und Verwendung personenbezogener Daten bleiben unberührt.

Begründung:
Siehe Begründung unter Ziffer I.4 zu § 20 Absatz 2 PAuswG.

IV. Artikel 4
Weitere Änderung des Passgesetzes zum 1. Mai 2021

§ 22a Absatz 2 Passgesetz-E

§ 22a Absatz 2 Passgesetz-E lautet:

(2) Im Fall der Übermittlung von Lichtbildern durch Passbehörden gemäß § 19 Abs. 1 Satz 1 an die Ordnungsbehörden im Rahmen der Verfolgung von Straftaten und Verkehrsordnungswidrigkeiten sowie an die Steuerfahndungsstellen der Länder und an die Behörden der Zollverwaltung im Rahmen der Verfolgung von Straftaten und Ordnungswidrigkeiten kann der Abruf des Lichtbildes im automatisierten Verfahren erfolgen. Der Abruf ist nur zulässig, wenn die Passbehörde nicht erreichbar ist und ein weiteres Abwarten den Ermittlungszweck gefährden würde. Zuständig für den Abruf sind die Polizeivollzugsbehörden auf Ebene der Landkreise und kreisfreien Städte,

die durch Landesrecht bestimmt werden. Die Polizeien des Bundes und der Länder, das Bundesamt für Verfassungsschutz, die Landesämter für Verfassungsschutz, der Militärische Abschirmdienst und der Bundesnachrichtendienst dürfen das Lichtbild zur Erfüllung ihrer Aufgaben im automatisierten Verfahren abrufen. Die abrufende Behörde trägt die Verantwortung dafür, dass die Voraussetzungen der Absätze 1 und 2 Satz 2 vorliegen. Über alle Abrufe sind von den beteiligten Behörden Aufzeichnungen zu fertigen, die eine Kontrolle der Zulässigkeit der Abrufe ermöglichen. Die Aufzeichnungen enthalten:

1. *Vor- und Familiennamen sowie Tag und Ort der Geburt der Person, deren Licht bild abgerufen wurde,*
2. *Tag und Uhrzeit des Abrufs,*
3. *die Bezeichnung der am Abruf beteiligten Stellen,*
4. *die Angabe der abrufenden und verantwortlichen Person sowie*
5. *das Aktenzeichen.*

§ 22 Abs. 3 Satz 5 gilt entsprechend.

Vorschlag BfDI:

(2) Im Fall der Übermittlung von Lichtbildern durch Passbehörden gemäß § 19 Abs. 1 Satz 1 an die ***Polizei- und*** Ordnungsbehörden im Rahmen der Verfolgung von Straftaten und Verkehrsordnungswidrigkeiten sowie an die Steuerfahndungsstellen der Länder und an die Behörden der Zollverwaltung im Rahmen der Verfolgung von Straftaten und Ordnungswidrigkeiten kann der Abruf des Lichtbildes im automatisierten Verfahren erfolgen. Der Abruf ist nur zulässig, wenn die Passbehörde nicht erreichbar ist und ein weiteres Abwarten den Ermittlungszweck gefährden würde. Zuständig für den Abruf sind die Polizeivollzugsbehörden auf Ebene der Landkreise und kreisfreien Städte, die durch Landesrecht bestimmt werden. ***[…]*** Die abrufende Behörde trägt die Verantwortung dafür, dass die Voraussetzungen der Absätze 1 und 2 Satz 2 vorliegen. Über alle Abrufe sind von den beteiligten Behörden Aufzeichnungen zu fertigen, die eine Kontrolle der Zulässigkeit der Abrufe ermöglichen.
Die Aufzeichnungen enthalten:

1. Vor- und Familiennamen sowie Tag und Ort der Geburt der Person, deren Licht bild abgerufen wurde,
2. Tag und Uhrzeit des Abrufs,
3. die Bezeichnung der am Abruf beteiligten Stellen,
4. die Angabe der abrufenden und verantwortlichen Person sowie
5. das Aktenzeichen.

§ 22 Abs. 3 Satz 5 gilt entsprechend.

Begründung:

Siehe Begründung unter Ziffer II zu § 25 Absatz 2 PAuswG.

Bonn, den 13. April 2017

Andrea Voßhoff

Freie Universität Berlin

Fachbereich Mathematik und Informatik
ID-Management

Prof. Dr. Marian Margraf
Takustraße 9
14195 Berlin

+49 30 838 75-245
marian.margraf@fu-berlin.de

Innenausschuss des
Deutschen Bundestages

nur per E-Mail

Betr.: Öffentliche Anhörung zum Gesetzentwurf der Bundesregierung „Entwurf eines Gesetzes zur Förderung des elektronischen Identitätsnachweises"

Sehr geehrte Damen und Herren,

vielen Dank für die Einladung zur öffentlichen Anhörung zum Gesetzentwurf. Gern übersende ich Ihnen vorab meine Stellungnahme in schriftlicher Form. Dabei beziehe ich mich ausdrücklich nur auf die im vorliegenden Gesetzentwurf aufgeführten Änderungen des aktuellen Gesetzes über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisgesetz - PAuswG) vom 18.06.2009 mit dem Ziel, den elektronischen Identitätsnachweis (auch eID-Funktion genannt) zu fördern. Darüber hinaus bewerte ich die im Gesetzentwurf vorgeschlagenen Änderungen hinsichtlich ihrer sicherheitstechnischen Folgen. Dies betrifft die folgenden Änderungsvorschläge:

1) Automatische und dauerhafte Einschaltung der eID-Funktion, Neufassung §10.
2) Löschung der Abwahlmöglichkeit einzelner im Rahmen der eID-Funktion übermittelbaren Daten, Neufassung §18.
3) Nutzung der eID-Funktion ohne Eingabe der PIN für Vor-Ort-Diensteanbieter, neuer §18a.
4) Nutzung der eID-Funktion über einen Identifizierungsdiensteanbieter, neuer §19a.
5) Vereinfachung der Vergabe von Berechtigungszertifikaten, Neufassung §21.

zu 1) Aus sicherheitstechnischer Sicht ergibt sich in Bezug auf eine automatische und dauerhafte Einschaltung der eID-Funktion keine Gefährdung. Nutzerinnen und Nutzer können weiterhin verhindern, dass die eID-Funktion ihres Ausweisdokuments missbraucht wird, indem sie z.B. diese Funktion über die Sperrhotline sperren lassen. Selbst wenn diese Maßnahme nicht durchgeführt wird, die eID-Funktion also nicht gesperrt ist, können Angreifer die eID-Funktion nur missbrauchen, wenn sie im Besitz

von Ausweisdokument und der für die Nutzung der eID-Funktion notwendigen PIN sind (2-Faktor-Authentisierung). Eine weitere Maßnahme, die Nutzerinnen und Nutzer umsetzen können, besteht also darin, den PIN-Brief sicher zu verwahren oder die hiermit übermittelte PIN unkenntlich zumachen.

zu 2) Das derzeit aktuelle PAuswG sieht vor, dass Nutzerinnen und Nutzer einzelne Datenfelder für die Übermittlung ausschließen können. Diensteanbieter müssen eine Berechtigung bei der Vergabestelle für Berechtigungszertifikate (VfB) beantragen. Diese prüft insbesondere, abhängig vom Zweck der Datenübermittlung, auf welche Datenkategorien der Diensteanbieter zugreifen darf. Ein Abwählen einzelner Datenkategorien wird also im Allgemeinen dazu führen, dass der Dienst nicht erbracht werden kann. Vor diesem Hintergrund ergibt ein Abwählen einzelner Datenkategorien keinen Sinn.

Dies ändert sich aber, wenn, wie in der Neuregelung in §21 vorgesehen (siehe auch Punkt 5) zukünftig Berechtigungen nicht mehr zweck-, sondern organisationsgebunden vergeben werden. Damit erhält ein Dienstanbieter eine Berechtigung für unterschiedliche Geschäftsprozesse, die aber auch, abhängig vom Zweck, unterschiedliche Anforderungen hinsichtlich der hierfür benötigten Datenkategorien haben können. Technisch ist es möglich, dass sich der Diensteanbieter in solchen Fällen nicht alle laut Berechtigung erlaubten Datenkategorien aus dem Ausweis übermitteln lässt, sondern nur die für diesen Geschäftsprozess benötigten. Meines Wissens ist dies auch in der heutigen Infrastruktur technisch so umgesetzt.

Da Diensteanbieter, unabhängig von den Regelungen im Personalausweisgesetz an das geltende Datenschutzrecht gebunden sind (z.B. Erforderlichkeitsgrundsatz und Gebot der Datensparsamkeit), müssen sie die oben aufgeführte technische Lösung umsetzen, um diesen gesetzlichen Verpflichtungen nachzukommen. Die zuständigen Datenschutz-aufsichtsbehörden sollten dies zukünftig stichprobenartig prüfen.

zu 3) Mit diesem Änderungsvorschlag werden weitere Anwendungsfälle für die eID-Funktion ermöglicht. Für Vor-Ort-Diensteanbieter wird ein spezielles Berechtigungszertifikat benötigt, das den Zugriff auf die Datenkategorien der eID-Funktion ohne Eingabe einer geheimen PIN ermöglicht. Der Zugriff setzt auf Seiten der Vor-Ort-Diensteanbieter die Kenntnis der auf dem Ausweis aufgedruckten Zugangsnummer voraus. Weiter muss der Vor-Ort-Diensteanbieter die Ausweisinhaberin bzw. den Ausweisinhaber eindeutig über das auf dem Ausweis aufgedruckte Lichtbild identifizieren.

All diese Maßnahmen führen dazu, dass ein Missbrauch der eID-Funktion in diesem Einsatzszenario verhindert wird. Nutzerinnen und Nutzer müssen bewusst ihren Ausweis einem Vertreter des Vor-Ort-Diensteanbieters übergeben, damit dieser die nach Berechtigung erlaubten Datenkategorien aus dem Ausweis auslesen kann.

zu 4) Identifizierungsdiensteanbieter sollten in der aktuellen Fassung des Gesetzes verhindert werden. Dazu heißt es in §21 Absatz 2: „Die Berechtigung nach Absatz 1 ist zu erteilen, wenn der Zweck nicht in der geschäftsmäßigen Übermittlung der Daten besteht und keine Anhaltspunkte für die geschäftsmäßige oder unberechtigte Übermittlung der Daten vorliegen". Dies hat aber dazu geführt, dass gerade kleine Diensteanbieter die eID-Funktion nicht einsetzen und weiterhin auf das potentiell unsichere Authentisierungsverfahren Benutzername/Passwort zurückgreifen.

Da Identifizierungsdiensteanbieter in der Regel die Identifizierung von Nutzerinnen und Nutzern für viele Diensteanbieter übernehmen können, kann das Verhalten der Nutzerinnen und Nutzer von diesen nachverfolgt werden. Die besonderen Anforderungen an Identifizierungsdiensteanbieter hinsichtlich Datenschutz und Datensicherheit trägt das Gesetz aber Rechnung. So heißt es in §19a Absatz 2: „Der Identifizierungsdiensteanbieter hat die personenbezogenen Daten des Ausweisinhabers zu löschen...". Weiter muss er nach §21b Absatz 2 Nummer 2 weitere Anforderungen hinsichtlich Datenschutz und Datensicherheit umsetzen, die in einer Rechtsverordnung geregelt werden. Eine aktualisierte VO, die Identifizierungsdiensteanbieter berücksichtig, liegt nicht vor. Diese sollte aber beinhalten, dass der Identifizierungsdiensteanbieter für seinen Dienst IT-Sicherheitsmaßnahmen umsetzt, die nach einem standardisierten Vorgehensmodellen erarbeitet wurden und regelmäßig aktualisiert werden.

zu 5) Berechtigungen sollen zukünftig nicht mehr zweckgebunden, sondern organisationsgebunden vergeben werden. Ein Nachteil, der bereits unter Punkt 2) diskutiert wurde, ist, dass hier für einen Geschäftszweck Daten im Rahmen der eID-Funktion erhoben werden könnten, die nicht benötigt werden (Verstoß gegen die Datensparsamkeit). Wie unter Punkt 2) erläutert, muss der Diensteanbieter dieses Gebot aber umsetzen und hat dazu auch die technischen Möglichkeiten.

Ein weiteres Problem könnte sich ergeben, wenn der Diensteanbieter für einen seiner Geschäftsprozesse die laut Berechtigungszertifikat übermittelten personenbezogenen Daten in unzulässiger Weise verarbeitet oder nutzt. In diesem Fall wird die Berechtigung widerrufen (§21 Absatz 5). Dieser Widerruf gilt dann für alle Geschäftsprozesse, in denen die eID-Funktion genutzt wird. Ob dieser Widerruf zukünftig tatsächlich vollzogen wird, trotz der für den Diensteanbieter erwarteten Folgen aus diesem Schritt, wird die Praxis zeigen.

Alternativ haben Diensteanbieter zukünftig immer noch die Wahl, für verschiedene Geschäftsprozesse verschiedene Berechtigungen zu beantragen. Dies wird durch den Gesetzentwurf hiesigen Erachtens nicht ausgeschlossen.

Zusammenfassung

Grundsätzlich ist die Entscheidung, die eID-Funktion weiter zu fördern, begrüßenswert. Mit der eID-Funktion des Personalausweises und des elektronischen Aufenthaltstitels ist grundsätzlich eine Authentifizierung der Nutzerinnen und Nutzer

ohne einen vorab häufig aufwendigen, weil nicht medienbruchfreien Erstregistrierungsprozess, möglich. Die vorgeschlagenen Änderungen führen nicht zu einer Schwächung der eID-Funktion hinsichtlich Datenschutz und Datensicherheit. Eine Verbreitung dieser Funktion würde darüber hinaus die IT-Sicherheit in vielen Einsatzgebieten deutlich erhöhen. Auch Firmen wie Apple und Google haben erkannt, dass eine Anmeldung allein über Benutzername/Passwort nicht mehr dem heutigen Sicherheitsstandard genügt und führen Verfahren ein, die auf mehr als einem Authentisierungsfaktor basieren.

Ob die oben aufgeführten Änderungen an der eID-Funktion die gewünschte Wirkung zeigen, kann zum jetzigen Zeitpunkt noch nicht mit Sicherheit gesagt werden. Gerade die Abschaffung des Ausschalten der eID-Funktion und die vereinfachte Beantragung von Berechtigungszertifikaten könnten aber hierzu beitragen. Darüber hinaus ermöglicht die Einführung von Identifizierungsdiensteanbietern die Nutzung der eID-Funktion auch für kleinere Diensteanbieter.

Mit freundlichen Grüßen

Prof. Dr. Marian Margraf

WESTFÄLISCHE
WILHELMS-UNIVERSITÄT
MÜNSTER

Institut für
Informations-,
Telekommunikations-
und Medienrecht

ITM | Leonardo-Campus 9 | 48149 Münster

Prof. Dr.
Bernd Holznagel, LL.M.
Direktor

Dr. Marius Stracke
Geschäftsführer

Leonardo-Campus 9
48149 Münster

Tel. +49 251 83-38641
Fax +49 251 83-9038644
holznagel@uni-muenster.de
http://itm.uni-muenster.de

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
18(4)868 C

Datum 21.04.2017

STELLUNGNAHME

ZUR ÖFFENTLICHE ANHÖRUNG ZUM ENTWURF EINES GESETZES ZUR FÖRDERUNG DES ELEKTRONISCHEN IDENTITÄTSNACHWEISES

I. Elektronischen Identitätsnachweis nachhaltig fördern

Im Jahre 2010 ist den Bürgerinnen und Bürgern die Möglichkeit eröffnet worden, sich mittels ihres Personalausweises online auszuweisen. Hierzu müssen sie bei der Aushändigung des Personalausweises gegenüber der Personalausweisbehörde erklären, dass sie den elektronischen Identitätsnachweis nutzen wollen. Die Einrichtung einer Funktion zum elektronischen Identitätsnachweis soll elektronische Transaktionen im Verhältnis zu Behörden und Unternehmen sicherer machen. Bisher erfolgt der Nachweis der Identität vor allem im Geschäftsleben durch die Eingabe und online-Übermittlung von Passworten. Diese Vorgehensweise ist jedoch anfällig für Angriffe Dritter. Die Kriminalstatistiken zeigen, dass der „Passwortdiebstahl“ in den letzten Jahren sprunghaft zugenommen hat.[1] Mit Einführung der eID-Funktion wird staatlicherseits der Versuch unternommen, eine sichere und verlässliche Infrastruktur zur gegenseitigen Identifikation im Internet zur Verfügung zu stellen. Sie basiert auf

[1] Siehe *Bundeskriminalamt,* Cybercrime / Bundeslagebild 2010-2015.

dem Prinzip einer Zwei-Faktoren-Authentifizierung, welches sich bei der Umsetzung im Alltag bewährt hat.

In der Praxis ist jedoch die Akzeptanz dieser 2010 eingeführten Sicherheitsinfrastruktur gering. Nur ein Drittel der Antragsteller macht von der bereitgestellten Opt-In-Möglichkeit Gebrauch. Mit dem Entwurf eines Gesetzes zur Förderung des elektronischen Identitätsnachweises in seiner derzeitigen Fassung (BT-Drs. 18/11279) soll nun die Nutzung der eID-Funktion gefördert werden. Dieses gesetzgeberische Ziel ist nachhaltig zu unterstützen. Die Digitalisierung von Wirtschaft und Gesellschaft hat in den letzten Jahren rasant an Fahrt aufgenommen. Sichere Vernetzungen und Transaktionen sind eine zentrale Voraussetzung dafür, dass der notwendige Transformationsprozess erfolgreich durchgeführt werden kann. Darüber hinaus bedarf es eines angemessenen Schutzes der Bürgerinnen und Bürger, aber auch der Unternehmen, wenn sie online kommunizieren und Transaktionen durchführen. Die Förderung des elektronischen Identitätsnachweises ist hierfür grundsätzlich eine wichtige Maßnahme.

Eine andere Frage ist, ob der hierfür im Gesetzesentwurf gefundene Steuerungsansatz weit genug geht. Schaut man sich das Geschäftsleben außerhalb Europas – zum Beispiel in China oder den USA – an, stellt man fest, dass die Identifizierung immer mehr per Mobiltelefon und vorwiegend auf Basis von Fingerprints erfolgt. Dem Gesetzgeber wäre zu raten, sich auf diese technologische Entwicklung rechtzeitig einzustellen und hierfür zeitnah besondere Förderansätze zu entwickeln. Des Weiteren dürfte die mangelnde Akzeptanz der eID-Funktion in der Bevölkerung auch damit zu tun haben, dass ihr Nutzen für die Bürgerinnen und Bürger nicht hinreichend erkenntlich ist. Es fehlt an Diensten von Wirtschaft und Verwaltung, die erkennbar durch den Einsatz der eID-Funktion einfacher und besser in Anspruch genommen werden können. Schließlich müssen die neuen technologischen Möglichkeiten auch „in den Köpfen“ verankert werden. Hierfür bedarf es permanenter Information und Schulung. Auf diesen Feldern weist die an sich lobenswerte Strategie der Bundesregierung ein deutliches Defizit auf.

II. Opt-In oder Opt-out ?

Um den Gebrauch der eID-Funktion zu fördern, soll nach dem neu gefassten § 10 Abs. 1 PAuswG-E der Personalausweis zukünftig standardmäßig mit dieser Funktion

ausgegeben werden. Der Bürger kann aber jederzeit durch einen Anruf eine sofortige Sperrung des elektronischen Identitätsnachweises veranlassen (§ 10 Abs. 6 PAuswG-E). Die Regelung wird damit im Ergebnis von einer „Opt-In"-Lösung auf ein „Opt-Out"-Modell umgestellt.

In verfassungsrechtlicher Hinsicht ist diese Umstellung hin zu einer dauerhaften Einstellung der eID-Funktion unbedenklich. Es handelt sich wenn überhaupt um einen marginalen Eingriff in die Allgemeine Handlungsfreiheit, da Bürgerinnen und Bürger das „Opt-Out" jederzeit durch Sperrung formlos vornehmen können und zudem im Alltag weiterhin selbst entscheiden, ob und wie sie die Funktion nutzen (vgl. § 18 PAuswG-E). Vor übertriebenen Erwartungen in diese Maßnahme ist jedoch zu warnen, weil die übrigen tatsächlichen Hindernisse für den Gebrauch der eID-Funktion – zum Beispiel unzureichende Mobilfunkanwendungen, zu wenig attraktive Dienste und mangelnde Verankerung im Bewusstsein – weiterhin bestehen.

III. Ex-Ante- oder Ex-Post-Kontrolle des Dienstanbieters?

Derzeit setzt die Prüfung für Berechtigungszertifikate durch die Vergabestelle ex-ante an. Die Vergabestelle muss detailliert klären, zu welchen Aufgaben oder Geschäftszwecken Daten im Wege des elektronischen Identitätsnachweises beim Inhaber des Personalausweises mittels eines Berechtigungszertifikats angefragt werden können. Hierbei ist auch der Frage nachzugehen, ob den Anforderungen an Datenschutz und Datensicherheit Rechnung getragen wird (vgl. § 21 Abs. 1 und 2 PAuswG). Das bisherige Verfahren mag zwar auf den ersten Blick umständlich erscheinen, dient aber in der Praxis auch der frühzeitigen Sensibilisierung der Antragsteller für die Belange des Datenschutzes und damit proaktiv der Vermeidung datenschutzrechtlicher Beanstandungen. Die Unternehmen werden darüber aufgeklärt, wie der Rechtsrahmen ihrer zukünftigen Tätigkeit in diesem Bereich aussieht. Oft können so die Geschäftsmodelle auf das bestehende Recht von Anfang an eingestellt werden und spätere Konflikte mit dem Datenschutzrecht verhindert werden.

Zukünftig soll anstelle der bisherigen zweckgebundenen Vergabe eine organisationsbezogene Vergabe erfolgen. Der Antragsteller muss nicht mehr den Zweck der Abfrage der Daten aus dem elektronischen Identitätsnachweis benennen. Es soll vielmehr ausreichen, dass der Diensteanbieter das dem Antrag zugrunde liegende Interesse an einer Berechtigung darlegt. Begründet wird dieser Systemwechsel mit dem

Ziel der Vereinfachung. Die Praxis habe gezeigt, dass die Diensteanbieter den bisherigen Zertifizierungsgang scheuten und stattdessen auf alternative Identifizierungsmittel zurückgriffen.[2]

Die angestrebte „Vereinfachung“ erweist sich bei genauer Betrachtung indessen als ein Scheineffekt. Die Neuregelung ist nämlich nicht mit einer Absenkung der Standards für den Datenschutz und die Datensicherheit verbunden. Die Unternehmen müssen sie selbstverständlich weiterhin einhalten und gehen zukünftig zusätzlich das Risiko ein, dass sie bei einer Unterschreitung von den Datenschutzbehörden ex-post sanktioniert werden. Vieles, was präventiv durch die Vorprüfung an Unsicherheiten aus dem Wege geräumt werden konnte, wird nun nachträglich infolge einer Kontrolle durch die Datenschutzbehörden auf die Unternehmen zurückfallen. Kommt es zu einer Sanktionierung, ist diese für die Diensteanbieter regelmäßig mit erheblichen Belastungen finanzieller Art und mit einem massiven Imageschaden verbunden, der auf die eID-Funktion selbst zurückfallen kann. Die Vermeidung dieser Risiken dürfte den Aufwand, der von den Diensteanbietern im bisherigen Zertifizierungsverfahren aufzubringen ist, im Ergebnis rechtfertigen. Aus diesem Grunde sollte an dem bisherigen Verfahren zur Erteilung der Berechtigungszertifikate festgehalten werden.

IV. Automatisierter Lichtbildabruf für Sicherheitsbehörden und Nachrichtendienste beschränken

Der neu eingefügte § 25 Abs. 2 S. 3 PAuswG-E, der zum 1. Mai 2021 in Kraft treten soll, berechtigt „die Polizeien des Bundes und der Länder, das Bundesamt für Verfassungsschutz, der Militärische Abschirmdienst, den Bundesnachrichtendienst sowie die Verfassungsschutzbehörden der Länder“ dazu, im Hinblick auf Reisepässe und Personalausweise „das Lichtbild *zur Erfüllung ihrer Aufgaben* im automatisierten Verfahren abrufen“. Der automatisierte Abruf wird an keine weiteren Voraussetzungen geknüpft. Die Subsidiaritätsklausel des § 25 Abs. 2 S. 1 2.HS PAuswG soll hier nicht gelten. Hiernach sind die Polizei- und Ordnungsbehörden zum Abruf im automatisierten Verfahren nur dann befugt, wenn die Personalausweisbehörde auf

[2] BT-Drs. 18/11279, 28

andere Weise nicht erreichbar ist und ein weiteres Abwarten den Ermittlungszweck gefährden würde.

Für die Erweiterung des Kreises der zum Abruf im automatisierten Verfahren befugten Behörden, die § 25 Abs. 2 S. 3 PAuswG-E vorsieht, werden in der Gesetzesbegründung gewichtige Gründe angeführt.[3] So wird u.a. darauf hingewiesen, dass die Ermittlung und die Kontaktaufnahme mit der örtlich zuständigen Behörde, die den Pass oder Personalausweis ausgestellt hat, oft zu zeitaufwendig oder zum Beispiel in den Abendstunden oder am Wochenende gar nicht möglich ist. Es ist nachvollziehbar, dass in Eilfällen gleichwohl ein automatisierter Abruf angezeigt ist. Zutreffend ist auch der Hinweis darauf, dass mit der Einzelabfrage der das Lichtbild liefernden Behörde unweigerlich bekannt wird, dass eine Person Gegenstand von Ermittlungen der Sicherheitsbehörden oder Nachrichtendienste ist. Dies ist ein Umstand, der durchaus nicht allen Betroffenen angenehm sein dürfte und im Wege des automatisierten Abrufs vermieden werden kann.

Andererseits wird eine Abfrage des Lichtbildes im automatisierten Verfahren nur daran geknüpft, dass dies für die Erfüllung der Aufgaben der Nachrichtendienste bzw. der Sicherheitsbehörden erforderlich ist. Damit wird das automatisierte Verfahren zu einem Standardverfahren erhoben. Da die Vernetzung der Behörden untereinander heute sehr weit gediehen ist, wird damit eine Situation geschaffen, die funktional dem der Einrichtung einer bundesweiten Datenbank für bestimmte biometrische Merkmale (Lichtbilder) entspricht. § 25 Abs. 6 PAuswG-E, der ein Verbot der Errichtung einer solchen Datenbank vorsieht, wird damit in seinem Sinngehalt unterlaufen. Aus diesem Grunde sollte die Subsidiaritätsklausel beibehalten werden und auch für die Nachrichtendienste gelten. Sie müsste allerdings auf die besonderen Interessenlagen der Nachrichtendienste und Sicherheitsbehörden zugeschnitten werden. So wäre zu berücksichtigen, ob bei einer vorherigen Anfrage bei den zuständigen Behörden die Gefahr der Enttarnung von Personen oder auch der Weitergabe der Nachfrage durch Unbefugte entstünde.

Subsidiaritätsklauseln dieser Art sind im geltenden Recht nicht unbekannt. Ein Beispiel findet sich u.a. in § 10 Abs. 7 BKAG. Die Abfrage des Lichtbildes im automatisierten

---

[3] 18/11279, 32.

Verfahren könnte etwa daran geknüpft werden, dass gerade diese Form der der Datenübermittlung „zur Wahrung des Zwecks der Abfrage unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen oder wegen ihrer besonderen Eilbedürftigkeit“ angemessen ist.

Daneben gilt es, einen Personenkreis zu definieren, der bei den Sicherheitsbehörden oder Nachrichtendiensten zur Abfrage berechtigt ist. Eine solche Regelung wäre allerdings nicht im Gesetz selbst zu treffen, sondern müsste Gegenstand einer noch zu entwerfenden Rechtsverordnung oder einer Verwaltungsvorschrift sein. Der Gesetzgeber sollte erwägen, dazu Leitlinien mindestens in der Begründung des vorliegenden Gesetzesentwurfs vorzugeben.

V. Passversagung

Zu begrüßen ist, dass in § 7 Abs. 1 Nr. 11 PassG-E ein neuer Passversagungsgrund eingeführt werden soll, um die Ausreise von Person zu unterbinden, denen im Ausland gravierende Menschenrechtsverletzungen drohen. Der Gesetzesentwurf verweist insoweit allerdings nur auf § 226a StGB (Verstümmelung weiblicher Genitalien). Es läge nahe, den Gesetzentwurf dieser Stelle um einen Verweis auch auf § 237 StGB zu ergänzen, um auch Ausreisen zum Zwecke der Zwangsverheiratung unterbinden zu können. Eine Ausreise zum Zweck der Herbeiführung einer Zwangsehe kann ebenso wenig hingenommen werden wie eine Ausreise zum Zwecke einer sogenannten „Beschneidung“. Die Gefahren für die von diesen Menschenrechtsverletzungen betroffenen Mädchen und jungen Frauen und deren Schutzbedürftigkeit sind in beiden Fällen gleichwertig.

Bernd Holznagel

Marius Stracke

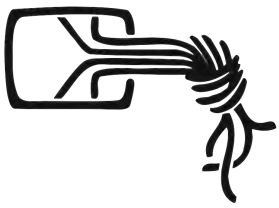
Prof. Dr. Bernd Holznagel

Dr. Marius Stracke

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
18(4)868 D

Chaos Computer Club



Stellungnahme eID

Gesetz zur Förderung des elektronischen Identitätsnachweises
(PAuswG-E, Passgesetz)

19. April 2017

Constanze Kurz
Jan Krissler, Linus Neumann, Frank Rieger

Dauerhafte Aktivierung der eID-Funktion

Das Ziel des Gesetzes zur Förderung des elektronischen Identitätsnachweises (eID) spricht bereits aus dem Titel: Die Nutzung der eID-Funktion soll sowohl beim elektronischen Personalausweis (ePA) als auch beim elektronischen Aufenthaltstitel (eAT) flächendeckend ausgebaut werden. Das soll vor allem dadurch erreicht werden, dass die Funktion standardmäßig und dauerhaft eingeschaltet wird, „bürokratische Hürden“ abgebaut und mögliche Anwendungsfelder erweitert werden.

Mit dem vorliegenden Gesetzentwurf wird also eine Förderung der Nutzung der eID-Funktion im Personalausweis versucht. Der elektronische Ausweis enthält einen Chip mit einer drahtlosen Schnittstelle, der drei verschiedene Funktionen anbietet. Eine davon ist der elektronische Identitätsnachweis (eID). Zur Nutzung dieser eID sind prinzipiell zwei Faktoren notwendig: der Besitz der Ausweis-Karte und die Kenntnis eines Geheimnisses (Zwei-Faktor-Authentisierung). Diese Zwei-Faktor-Authentisierung ist für den Nutzer ein technischer Vorteil in Fragen der Sicherheit, aber kein Alleinstellungsmerkmal gegenüber nicht-staatlichen Alternativen zur eID im Ausweis. Mittlerweile setzt eine Vielzahl von Anbietern Verfahren ein, die auf mehreren Authentisierungsfaktoren beruhen.

Verbreitung der eID-Nutzung

Die eID-Funktion hat nach ihrer kostenintensiven Einführung im November 2010 keine nennenswerte Verbreitung gefunden. In der Begründung des Gesetzentwurfes wird dies offenbar der bisherigen Möglichkeit zugeschrieben, diese eID-Funktion gar nicht erst zu aktivieren oder später zu deaktivieren. Kern des Gesetzentwurfes ist daher deren automatische Aktivierung.

Insgesamt liegt die eID-Nutzung deutlich unter den Erwartungen, die Aktivierungsquote hat nicht einmal ein Drittel der Ausweisbesitzer erreicht.

Die Aktivierung ist aber nur eine Seite der Medaille, denn die tatsächliche Nutzung liegt noch weit darunter, da sinnvolle Angebote rar sind. Nur etwa fünfzehn Prozent der Besitzer mit aktivierter eID-Funktion haben den Einsatz überhaupt getestet. Die Zahl der Test-Nutzer darunter, die zudem ein sicheres Lesegerät nutzen, ist statistisch nahe Null.

Die Hoffnung ist, dass die zwangsweise Aktivierung einen Anreiz zur Implementierung von eID-Diensten setzen könnte. Während behördliche Angebote zur Nutzung der eID-Funktion seitens der Bundes- und Landesregierungen stimuliert werden könnten, ergibt sich bei Angeboten aus der Wirtschaft eine Art Henne-Ei-Problematik: Angebote werden nicht gemacht, wenn niemand die eID nutzt; niemand nutzt die eID, wenn es keine guten Angebote gibt.

Doch bisher haben sich selbst staatliche Stellen in den letzten sieben Jahren dem überwältigendem Votum der Bürger gegen die eID angeschlossen: Leuchtturmprojekte, die als potentielle Zugpferde Werbung für die Benutzung machen könnten, sind quasi nicht existent.

Selbst das mit großem Rummel angekündigte besondere elektronische Anwaltspostfach (beA) lässt die eID links liegen, obwohl deren Notarsfunktion quasi ein Heimspiel wäre.

Welche Vorteile die Nutzung der eID-Funktion gegenüber anderen alltäglichen und marktgängigen Identifikationsmethoden haben soll, konnte bisher nicht überzeugend dargestellt werden. Die damit ganz praktisch befassten Mitarbeiter in den Meldeämtern sind weder dafür ausgebildet noch zeitlich in der Lage, Fragen der Ausweisbesitzer nach Vor- und Nachteilen zu beantworten. Der Begründung des neuen Gesetzentwurfes gelingt das auch nicht. Warum bestehende Lösungen bei Online-Diensten durch die vergleichsweise komplexe Nutzung der eID ersetzt werden soll, erschließt sich nicht.

Es drängt sich der Eindruck auf, dass die mit vielen Versprechungen und hohen finanziellen Investitionen an den Start gegangene Digitalisierung des Ausweises von einem Angebot an die Bürger nun per Gesetz zu einem Zwang ausgebaut werden soll, obgleich sich der besondere Nutzen weder aus Sicht des Bürgers noch aus Sicht von Anbietern nicht begründen lässt.

Es ist nicht das erste Mal, dass durch ein derartiges Nachbesserungsgesetz ein teures und aus guten Gründen nie benutztes totes Pferd wiederbelebt werden soll. Die mangelnde Verbreitung und Nutzung der eID-Funktion dürfte vielmehr dem mangelnden Vertrauen und Interesse der Bürger zuzuschreiben sein als der Möglichkeit der Aktivierung und Deaktivierung. Dieses fehlende Vertrauen lässt sich auch durch eine zwangsweise Aktivierung nicht zurückgewinnen. Es stellt sich zudem die einfache Frage: Warum sollte jemand eID nutzen wollen, nur weil sie dann verpflichtend eingeschaltet ist?

Es sollte anerkannt werden, dass sich auch die Online-Welt in den vergangenen sieben Jahren weitergedreht hat. Heute wird das eID-Verfahren den Anforderungen der mobilen Welt kaum gerecht. Identitätsabgleiche verlagern sich mehr und mehr auf Smartphones, wofür auch nach Jahren so gut wie keine Angebote gemacht werden.

Das ausbleibende Interesse betrifft dabei sowohl die Ausweisbesitzer als auch die Anbieter. Offenbar konnten auch potentielle Anbieter von der Sinnhaftigkeit der eID-Funktion gegenüber bestehenden Alternativen nicht überzeugt werden. Von den ausgestellten Berechtigungszertifikaten vom Bundesverwaltungsamt sind derzeit mit 233 Zertifikaten etwa die Hälfte für den behördlichen oder eGovernment-Bereich vergeben worden, die andere Hälfte für kommerzielle Anbieter.

Beantragungsverfahren für Zertifikate

Unternehmen zögern mit der Nutzung der eID-Funktion auch aufgrund des aufwendigen Beantragungsverfahrens, allerdings sichert das bisherige Vorgehen auch gegen Missbrauch. Das betrifft vor allem Haftungsfragen sowie die Vorlage von Sicherheitskonzepten.

Die Notwendigkeitsprüfung vor der Erstellung eines Berechtigungszertifikats soll künftig entfallen, ebenso der Dienstbezug und die Bußgeldhöhe bei Verstößen. Damit soll die Bürokratie vor Erteilung eines Berechtigungszertifikats abgebaut werden. Die Befürchtung ist dabei, dass diese bürokratischen Pflichten die eID-Nutzung behindern. Allerdings war die Prüfung auch ein wichtiges Versprechen an den Bürger im Sinne seiner Datenschutzinteressen, das vor Missbrauch schützen sollte. Obwohl gar nicht belegt ist, dass die Prüfung tatsächlich ausschlaggebend oder gar ursächlich für die klägliche Anzahl an Berechtigungszertifikaten ist, soll nun darauf verzichtet werden. Um Anbietern eine zweifelhafte Incentivierung für eID-Anwendungen anzubieten, wird letztlich beim präventiven Datenschutz zurückgesteckt.

Dass durch den Wegfall der Notwendigkeitsprüfung das mangelnde Vertrauen in die eID seitens der Nutzer gestärkt wird, ist nicht zu erwarten. Wenn das Gegenüber im Netz bei der Beantragung des Zertifikats kaum mehr geprüft wird, fiele ein Vertrauensaspekt der eID weg. Bisher kann jeder bei Interesse die notwendigen Daten sichten und sich auf die Prüfung verlassen, die bei Erstellung der Berechtigungszertifikate erfolgte.[1] Mindestens das Bußgeld bei Verstoß sollte wesentlich erhöht werden, um Missbrauch entgegenzuwirken.

[1] Vgl. Erteilte Berechtigungszertifikate: http://download.gsb.bund.de/VfB/npavfb.pdf

Inflationärer Einsatz der eID führt zu Überidentifizierung

Die Vermischung von hoheitlichen Identifizierungsaufgaben mit den Erfordernissen der Wirtschaft zur Identifizierung im Rechtsverkehr ist konzeptionell problematisch. Es steht zu erwarten, dass die einfache Verfügbarkeit eines Identitätsdienstes auf Basis des Personalausweises zu einer Überidentifizierung führt: Die einfache Identifizierung könnte dann für immer mehr Services und Angebote verlangt werden, was wiederum die Verknüpfung mit anderweitig gewonnenen Profilinformationen zu einem eindeutig zuzuordnenden Persönlichkeitsprofil ermöglicht. An separaten Stellen von verschiedenen Anbietern gesammelte Daten würden so sehr viel einfacher kombinier- und abgleichbar.

Bisher ist der Großteil der bei Anbietern gesammelten Profilinformationen nicht eindeutig mit einer hoheitlich garantierten Identität verknüpft. Durch eine einfache staatlich verifizierte und vertrauenswürdige Personalisierung dieser Profilinformationen entstünden daher umfängliche Probleme in Fragen des Datenschutzes und der Privatsphäre. Während derzeit etwa zu einem alltäglichen Social-Media-Profil fast nie Adressinformationen gespeichert werden, könnte dies mit einem niederschwelligen quasi-hoheitlichen Identitätsservice zum Standard werden. Dies wäre beispielsweise für Stalking-Opfer im Netz gefährlich.

Eine Lösungsmöglichkeit hierfür wäre eine rechtliche und preisliche Gestaltung, die die Nutzung der Personalausweis-basierten Identität nur möglich und attraktiv macht, wenn für Zwecke eines Vertragsabschlusses eine solche Identifizierung wirklich benötigt wird. Das widerspräche aber gerade dem Ziel des Gesetzentwurfes, der die Nutzung der eID explizit fördern will und die Beantragung der Zertifikate zu erleichtern.

Alternativen: größere Einsatzmöglichkeiten und geringere Einstiegshürden

Es bestehen bereits Alternativen zur Identifikation, die vom privaten Sektor angeboten werden bzw. kurz vor ihrer Einführung stehen. Ein Beispiel ist das von der weltweiten Mobilfunk-Vereinigung GSMA spezifizierte „Mobile Identity“-System. Dieses verwendet die bei den Netzanbietern vorhandenen Kundenbeziehungen über das Mobiltelefon des Nutzers zur Identifikation in verschiedenen Sicherheitsstufen. Dieses Verfahren ermöglicht insbesondere das selektive Preisgeben von Identitätsinformationen, um Datensparsamkeit sicherzustellen. Theoretisch denkbar ist dabei auch die pseudonyme Nutzung, bei der einem Anbieter gegenüber nur versichert wird, dass es sich um eine dem Mobilfunkanbieter bekannte Identität handelt, bei der dieser einzugsermächtigt ist.

Dieses alternative Verfahren hat dank globaler Standardisierung und der länderübergreifenden Struktur der großen Mobilfunkanbieter (Vodafone, Telefonica, Telekom etc.) eine hohe Chance auf umfassende Akzeptanz und Marktdurchdringung. Als Vertrauensanker dient dabei die SIM-Karte, welche über weitgehend vergleichbare Sicherheitsattribute wie für eID verwendeten SmartCards verfügt. Es offeriert den Anbieter vor allem eine internationale Lösung, die von nationalen Eigenheiten wie bei der deutschen eID frei ist.

Es ist davon auszugehen, dass solche in ihrer Konzeption nicht national begrenzten Ansätze eine schnellere und größere Akzeptanz finden. Grund dafür ist auch, dass die Anbieter weniger Kosten erwartet, wenn sie eine internationale Lösung statt einer nationalen umsetzen.

Zugriff auf biometrische Lichtbilder

Der Gesetzentwurf enthält auch mit der Förderung der eID nicht in Zusammenhang stehende Inhalte, die den Zugriff auf biometrische Passbilder betreffen. Die digitalisierten biometrischen Pass- und Ausweisbilder stehen der Polizei zum automatisierten Abruf zur Verfügung. Der nun vorgesehene automatisierte Zugriff von Geheimdiensten auf die biometrischen Passbilder in elektronischer Form wäre ein Schritt in eine umfassende und kaum kontrollierte Überwachung. Der Gesetzentwurf sieht diese Möglichkeit der automatisierten Übermittlung der biometrischen Passbilder vor, also einen unmittelbaren geheimdienstlichen Zugriff auf die Daten in den Meldeämtern. Die Protokollierung dieser Zugriffe soll aber nur bei der abfragenden Stelle, also den Geheimdiensten selbst, erfolgen.

Dieser Datenzugriff weitet die Nutzung in einem kaum überschaubaren und wenig kontrolliertem Maße aus und sollte unterbleiben, mindestens aber sollte jede dauerhafte Speicherung und Weitergabe der so erlangten Daten untersagt werden.

Die Möglichkeit des automatisierten Zugriffs sowohl für Polizeien als auch für Geheimdienste muss im Kontext des immer weiteren Ausbaus der Videoüberwachung und der laufenden Tests der Behörden mit automatischer Gesichtserkennung in Videoüberwachungs-Streams gesehen werden. Die einfache elektronische Abfrage großer Mengen Gesichtsbilder erlaubt den Aufbau von Überwachungssystemen, bei denen die Eingabe eines Namens und eines Geburtsdatums in die entsprechende Abfragemaske ausreicht, um das persönliche Passbild abzurufen und direkt in automatischen Gesichtserkennungssysteme einzuspeisen. Auch die umgekehrte Abfrage persönlicher Daten zu einem automatisch identifizierten Gesichtsbild wird für die abgerufenen und bei Polizei oder Geheimdienst gespeicherten Gesichtsbildern dadurch technisch ermöglicht. Die schon heute gegebene Vollüberwachung der digitalen Welt erhält so mittelfristig Einzug in die „reale Welt“ und macht auch diese zu einer digital überwachten Sphäre.

Da die Videoüberwachung des öffentlichen Raums immer weiter ausgebaut wird und die Erprobung automatischer Gesichtserkennung bereits erklärtes Ziel der Behörden ist, muss dieses Szenario für die Bewertung des Gesetzentwurfes bedacht werden.

Ein weiteres Problem ist der weitgehend unkontrollierte Datenaustausch der Geheimdienste mit ausländischen Partnerdiensten. Die jüngsten Aktivitäten türkischer Geheimdienste in Deutschland im Kontext des Präsidial-Referendums offenbarten, dass auch als „befreundet“ klassifizierte Dienste alle Mittel nutzen, um politische Ziele zu verfolgen und Opposition gegen ihre Regierung auch in Deutschland zu unterdrücken. Über den Weg der deutschen Geheimdienste ist hier also von einem Zugriff solcher Partnerdienste auf die gespeicherten deutschen Meldedaten zu warnen, die elektronischen Aufenthaltstitel eingeschlossen. Mit der kontinuierlich zunehmenden Intensität und Automatisierung des Datenaustauschs unter Behörden in Europa und darüber hinaus ist davon auszugehen, dass auch die Gewährung des Zugangs für ausländische Geheimdienste und Polizeien innerhalb weniger Jahre Realität wird.

Dass der Zugriff erst ab dem Jahr 2021 vorgesehen ist, ändert nichts daran, dass ein Einfließen der Meldedaten in die geheimdienstlichen Kreisläufe eine Zweckentfremdung der Daten darstellt.

Vertrauen in das eID-Verfahren

Bei der Betrachtung des Erfüllungsaufwands durch den Normenkontrollrat werden Einsparpotentiale unter anderem dadurch gesehen, dass erstens die Bürger nicht mehr über eine Möglichkeit der Deaktivierung aufgeklärt werden müssen, zweitens die Deaktivierung grundsätzlich nicht mehr angeboten wird und damit auch drittens die Reaktivierung wegfällt. Aus diesem Grund soll auch auf fünfzig Prozent der Informationsmaterialien verzichtet werden. Die erhofften Kosteneinsparungen sind allerdings praxisfern.

Laut dem vorliegenden Gesetzentwurf soll es der ausstellenden Behörde überlassen bleiben, „in welcher praxisgerechten Form“ eine Unterrichtung der Bürger über die eID-Funktion stattfindet. Dies lässt entweder den Schluss zu, dass die durch diesen Zeitaufwand entstehenden Kosten bei der Betrachtung nicht berücksichtigt werden, oder dass ein Verzicht auf diese Unterrichtung billigend in Kauf genommen wird.

Es zeugt vom Geist dieses Gesetzes, dass den Bürgern in Zukunft eine Funktionalität aufgezwungen wird, gegen die sich bisher mehr als zwei Drittel der Bürger entschieden haben, nachdem sie darüber informiert wurden. Diese Bürger sollen nun nicht nur zur Nutzung zwangsweise animiert, sondern über die Funktion auch nicht mehr vollständig und einheitlich aufgeklärt werden. Es bleibt schleierhaft, wie das Vertrauen in eine Funktion dadurch gesteigert werden soll, geschweige denn in deren Anwendung.

Es ist eine langjährige Forderung des Chaos Computer Clubs, die Informationen für den Ausweisnutzer verständlicher, umfassender und risikobezogener zur Verfügung zu stellen. Statt bunter Broschüren sollte eine ehrliche und auch die Risiken betrachtende Information mit dazu geschulten Mitarbeitern erfolgen. Das Gegenteil sieht der Gesetzentwurf vor, obgleich die eID und auch der elektronische Personalausweis insgesamt ein anspruchsvolles und technisch komplexes Angebot ist.

Nach wie vor sollte der Bürger darauf hingewiesen werden, dass der elektronische Personalausweis nicht länger als notwendig in ein Lesegerät gesteckt werden sollte, um etwa Relay-Angriffe zu vermeiden. Handfeste Informationen über die Unterschiede in Fragen der IT-Sicherheit, die zwischen den angebotenen Lesegeräten („Basisleser“, „Komfortleser“ usw.) bestehen, sollten ebenso an den Bürger gegeben werden. Dazu sind bei Interesse weitergehende Behördeninformationen zu Lesegeräten und Software sowie zur IT-Sicherheit im Alltag, insbesondere zu Schadsoftware auf den heimischen Rechnern der Nutzer, anzubieten.

Dass noch keine speziell auf den Missbrauch der eID zugeschnittenen Trojaner im Umlauf sind, dürfte an der spärlichen Verbreitung liegen. Wenn sich die Erfahrungen der Missbrauchsmöglichkeiten nur ähnlich langsam durchsetzen, wie in der Vergangenheit bei Online-Banking oder den PINs der EC-Karten, wären gerade unter den frühzeitigen Anwendern die von Identitätsdiebstahl Betroffenen – auch in Hinsicht auf das deutlich höhere Schadpotential – einem mühsamen Kampf zum Nachweis des Missbrauchs ausgesetzt. Ein weiteres Beschneiden der Aufklärungsarbeit in den Meldeämtern würde diese Schieflage noch verschlimmern.

Ausweis- und Passkopien

Bisher ist das Erstellen einer Ausweiskopie an die Erforderlichkeit gebunden. Wenn der Ausweis vor Ort vorgezeigt und geprüft werden kann, liegt diese Erforderlichkeit nicht vor. Das automatisierte Speichern von Personalausweiskopien durch nicht-öffentliche Stellen ist bisher nach dem Personalausweisgesetz nicht möglich.

Der Gesetzentwurf soll die Erstellung von Kopien des elektronischen Personalausweises nun erlauben. Kopien sollen auch für den elektronischen Pass möglich werden. Damit wird zugleich die Kopie der aufgedruckten maschinenlesbaren Zone (MRZ) zum Problem, da der Zugang zu den Daten auf dem Chip damit verbunden ist.

Diese Kopien sollen künftig dann hergestellt werden dürfen, wenn der Ausweisbesitzer darin freiwillig einwilligt. Die Kopien sollen aber nicht an Dritte weitergegeben werden dürfen. Die Freiwilligkeit ist aber regelmäßig in der Praxis keine echte, wenn etwa ein Dienstleister schlicht danach verlangt und den Besitzer zu einer Ausweiskopie drängt, um eine Dienstleistung oder einen Vertragsabschluss durchzuführen. Die Vermietung von Wohnraum, Fahrzeugvermietungen oder Hotelübernachtungen sind typische Beispiele dafür.

Ob und wie lange eine Kopie gespeichert wird, entzieht sich im Regelfall der Kenntnis des Ausweisbesitzers, auch eine Weitergabe kann er praktisch kaum erfahren noch verhindern.

Zudem gibt die Kopie regelmäßig mehr Daten preis als für den Vertrag oder die Dienstleistung nötig wäre, inklusive der MRZ. Zwar wird empfohlen, nicht erforderliche Daten zu schwärzen. Dass aber in der Praxis tatsächlich Bereiche wie die maschinenlesbare Zone aus Sicherheitsgründen physisch abgeklebt werden, ist lebensfremd und schlicht unpraktisch.

Generell wird statt der heute üblichen Vorlage und Einsichtnahme die Ausweiskopie durch die neue Regelung wieder häufiger werden und damit – anders als bei den aus dem Chip freigegebenen eID-Datenfeldern – die aufgedruckten Informationen vollständig preisgeben. Das sind auf der Vorderseite typischerweise neben Lichtbild, Name und Vorname: das Geburtsdatum und der Geburtsort, die Seriennummer des Ausweises, das Gültigkeitsdatum, die Staatsangehörigkeit sowie die Zugangsnummer (für den hoheitlichen Bereich des Chips). Wird auch die Rückseite kopiert, sind zusätzlich die Anschrift, die Körpergröße, die Augenfarbe, eventuelle Künstler- und Ordensnamen, die ausstellende Behörde sowie die MRZ aufgedruckt.

Erforderlich sind hingegen bei typischen Identitätsnachweisen nur Vorname, Nachname, Anschrift und häufiger auch das Geburtsdatum. Da beim Ausweis jedoch Name und Anschrift auf unterschiedlichen Seiten aufgedruckt sind, besteht eine Ausweiskopie regelmäßig aus beiden Seiten und damit aus den vollständigen aufgedruckten Informationen. Als besonders sensibel kann dabei die MRZ und die Zugangsnummer gelten. Der Gesetzgeber sollte daher das Abkleben vorschreiben. Da das im Alltag nicht besonders praktisch ist, wird das zugleich nicht unbedingt notwendigen Ausweiskopien entgegenwirken.

Fazit

Nachdem das Desinteresse von Bürgern und Anbietern an der eID nun seit Jahren besteht und auch keine Art der Selbstverpflichtung der Industrie erreicht werden konnte, soll die Nutzung der eID jetzt mit dem gesetzlichen Holzhammer verordnet werden. Statt mit attraktiven behördlichen Angeboten aufzuwarten, die Vertrauen und Nutzungszufriedenheit fördern könnten, wird eine Methode gewählt, die mit hoher Wahrscheinlichkeit erneut scheitern wird.

Die vorgesehene Erlaubnis für Kopien von Ausweis und Pass birgt Gefahren für den Datenschutz und die IT-Sicherheit, insbesondere durch die Kopie der MRZ.

Bei der Nutzung des elektronischen Personalausweises sollte auf Sicherheitsprobleme hingewiesen werden anstatt die Aufklärung in den Meldeämter weiter zu reduzieren. Die Benutzung des elektronischen Identitätsnachweises ist technisch komplex, auf Risiken sollten die Bürger aufmerksam gemacht werden, insbesondere wenn sie keine der teureren Lesegeräte benutzen.

Der automatisierte Zugriff auf die biometrischen Lichtbilder aus den elektronischen Personalausweisen und Pässen für die Geheimdienste ist kaum kontrollierbar und daher abzulehnen.

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
18(4)773

Deutscher Bundestag
Parlamentarischer Beirat
f. nachhaltige Entwicklung

Ausschussdrucksache
18(23)94-21

Deutscher Bundestag

Parlamentarischer Beirat für
nachhaltige Entwicklung

Gutachtliche Stellungnahme/Prüfbitte

Entwurf eines Gesetzes zur Förderung des elektronischen Identitätsnachweises

Bundesrats-Drucksache 787/16

Im Rahmen seines Auftrags zur Überprüfung von Gesetzentwürfen und Verordnungen der Bundesregierung auf Vereinbarkeit mit der nationalen Nachhaltigkeitsstrategie hat sich der Parlamentarische Beirat für nachhaltige Entwicklung gemäß Einsetzungsantrag (Drs. 18/559) am 30. Januar 2017 mit dem Entwurf eines Gesetzes zur Förderung des elektronischen Identitätsnachweises (BR.-Drs. 787/16) befasst.

Folgende Aussagen zur Nachhaltigkeit wurden in der Begründung des Gesetzentwurfes getroffen:

„Das Vorhaben entspricht den Zielen der Nationalen Nachhaltigkeitsstrategie. Die Managementregeln und Indikatoren der Nationalen Nachhaltigkeitsstrategie sind nicht einschlägig."

Formale Bewertung durch den Parlamentarischen Beirat für nachhaltige Entwicklung:

Eine Nachhaltigkeitsrelevanz des Gesetzentwurfes ist gegeben. Der Bezug zur nationalen Nachhaltigkeitsstrategie ergibt sich hinsichtlich folgenden Indikators:

Indikator 15 (Kriminalität - Persönliche Sicherheit weiter erhöhen)

Die Darstellung der Nachhaltigkeitsprüfung ist nicht plausibel.
Das Ausweisrecht dient der Sicherheit in Deutschland, somit ist der Indikatorenbereich 15 durch das vorliegende Gesetz durchaus betroffen. Das sollte geprüft und dargestellt werden.

Prüfbitte:
Der Parlamentarische Beirat für nachhaltige Entwicklung bittet daher den federführenden Innenausschuss, bei der Bundesregierung nachzufragen, warum der o.g. Bezug zur nationalen Nachhaltigkeitsstrategie nicht hergestellt wurde und welche konkreten Auswirkungen auf die nachhaltige Entwicklung in diesem Bereich zu erwarten sind und die Ergebnisse in den Bericht des Ausschusses aufzunehmen.

Berlin, 30. Januar 2017

Dr. Lars Castellucci, MdB
Berichterstatter

Dr. Valerie Wilms, MdB
Berichterstatterin